CH-GROUPS WHICH ARE FINITE $p$-GROUPS

B. WILKENS

Communicated by Alireza Abdollahi

Abstract. In their paper "Finite groups whose noncentral commuting elements have centralizers of equal size", S. Dolfi, M. Herzog and E. Jabara classify the groups in question- which they call CH-groups- up to finite $p$-groups. Our goal is to investigate the finite $p$-groups in the class. The chief result is that a finite $p$-group that is a CH-group either has an abelian maximal subgroup or is of class at most $p+1$. Detailed descriptions, in some cases characterisations up to isoclinism, are given.

1. Introduction

Following [2], we call the group $G$ a CH-group if the conjugacy class lengths of any two commuting noncentral elements of $G$ are equal. Examples of CH-groups are the CA-groups (also known as AC-groups) in which centralisers of noncentral elements are abelian or finite groups with no more than two distinct conjugacy class lengths.

In [2], CH-groups are classified up to the finite $p$-groups in the class, with some results on the latter. We intend to close the $p$-group-shaped gap, as far as this is possible.

So let $p$ be a prime. For brevity’s sake, a finite $p$ group which is CH shall be referred to as a CH-$p$-group. It is mentioned in [2] that, for $n \in \mathbb{N}$, the wreath product $C_p^n \wr C_p$ is a CA-group - actually, any finite $p$-group with an abelian maximal subgroup is - which shows that CH-$p$-groups may be of arbitrarily large class. However, we show

Keywords: Finite-p-groups; AC-groups; conjugate rank.
Received: 2 July 2012, Accepted: 23 July 2012.
Theorem 1. Let $P$ be a nonabelian CH-$p$-group. Then either $P$ has an abelian maximal subgroup or $\mathcal{U}_1(P) \leq Z(P)$ and $\text{cl}(P) \leq p + 1$. The bound is attainable.

Aside from that theorem, we obtain quite detailed structural information on CH-$p$-groups, to be found in Propositions [1.3, 1.6, 1.9]. To state these, a few preliminaries are needed.

Notation: Let $G$ be a CH-$p$-group, let $Z = Z(G)$ and $\overline{G} = G/Z$. Pick an element $u$ of $Z_2(G) \setminus Z$, and let $|u^G| = p^s$. Using notation as found in [2], we let $\mathcal{M} = \{x \mid x \in G, |x^G| = p^s\}$. Let $\langle \mathcal{M} \rangle = H$.

Let $A$ be a maximal abelian normal subgroup of $G$ with $u \in A$. If $H \leq V \leq G$, then, for $x \in \mathcal{M}$, $C_G(x) \subseteq \mathcal{M} \cup Z \subseteq V$. Hence if $Z(H) > Z$, then, for $x \in \mathcal{M}$, we have $H = C_G(x) = A$. Let $U$ be the inverse image in $G$ if $C_{\overline{G}}(A)$.

Lemma 1.1. [2], Lemma 5.1, [5], Lemma 2] $|H, A| \leq Z$.

Lemma 1.2. [2], Lemma 6.1, [6] If $\exp G > p$, then $|G : A| \leq p$.

Classifying CH-$p$-groups of class 2 seems an impossible task, especially as we can prove:

Proposition 1.3. Let $p$ be a prime, and let $G$ be a finite $p$-group of class 2. Then $G$ is isomorphic to a subgroup of a CH-$p$-group of class 2 if and only if $\mathcal{U}_1(G) \leq Z(G)$.

From now on, let $G$ be a CH-$p$-group with $\exp(G/Z) = p$ and $\text{cl}(G) \geq 3$. Note that this rules out $p = 2$. We describe $G$ according to whether $H$ is abelian (Proposition 1.4), of class 2 (Proposition 1.6) or of class 3 (Proposition 1.9).

Proposition 1.4. If $H$ is abelian, then $G/H$ is elementary abelian of order $p^s$. For $i \in \mathbb{N}$, $a \in A$ and $x \in G \setminus H$, we have $|a, t x| = 1$ if and only if $a \in Z_i(G)$. Furthermore, $\text{cl}(G) \leq p + 1$, and this bound is sharp.

Propositions 1.6 and 1.9 require some more preliminaries:

The groups $S(m, k)$

Let $k, m \in \mathbb{N}$, and let $n = km$. Let $T = GF(p^k)$, regarded as a $GF(p)$-algebra, and let the $T$-module $V$ be the direct sum of $m$ submodules isomorphic to $(T, +)$ with $T$ acting by multiplication. Let $\alpha : V \to V_1$ be a $T$-isomorphism. Let $Z = (V_1 \otimes_T V)/I$ where $I = \langle \alpha(u) \otimes v - \alpha(v) \otimes u \mid u, v \in V \rangle$.

Observe that, for $u, v \in V$ and $t \in T$, we have $(\alpha tu \otimes v) + I = (\alpha(u) \otimes v) + I = (\alpha(u) \otimes tv) + I = (\alpha(tv) \otimes u) + I = (\alpha(v) \otimes tu) + I$. Let $D = V_1 \otimes_T V$, and let $W = V_1 \otimes Z \otimes D$. Let $f : W \times V \to Z$ be given by $(\alpha(u) + z + d, v) \mapsto (\alpha(u) \otimes v) + I$, and let $g : W \times T \to D$ be given by $(\alpha(v) + z + d, t) \mapsto \alpha(v) \otimes t (u, v, z, d \in D)$.

Setting $u(\alpha(v) + d + z) = \alpha(v) + f(\alpha(v), u) + d + z$ and $t(\alpha(v) + d + z) = \alpha(v) + g(\alpha(v), t) + d + z$ makes $W$ into a $V$- and a $T$-module.

Define a multiplication on $V \times W$ by

- $(u, \alpha(v) + d + z)(u', \alpha(v') + z' + d') = (u + u', \alpha(v) + \alpha(v') + z + z' + d + d' + f(\alpha(v), u'))$
- $(u, u', v, v' \in V, z, d, d' \in D)$.
This multiplication (compare [9], Theorem 6.7) defines a group \( H = H(k, m) \) of class 2 in which \([(u, 0), (0, \alpha(v))] = (0, -f(\alpha(v)), u) \) whenever \( u, v \in V \). Identifying \( V, V_1, Z, D \) with the corresponding subgroups of \( H \), we have \( Z(H) = ZD \). Let \( u, v \in V \). If \( u \) and \( v \) belong to the same irreducible \( T \)-submodule of \( V \), then there is \( t \in T \) with \( v = tu \) and \( C_H(ua(v)) = Z(H)\{ua(tw) \mid w \in V\} \), an elementary abelian subgroup of \( H \) of index \( p^n \). If \( u \) and \( v \) do not belong to the same irreducible \( T \)-submodule, then \( C_H(ua(v)) = Z(H)\{ua(v)\} \). In particular, \( H \) is a CA-group.

Let \( \{w_1, \ldots, w_n\} \) be a basis of \( V \) and, for \( h \in \{0, \ldots, k - 1\} \), define \( \delta_{th} : V \to W \oplus Z \) as follows: For \( u = \sum \lambda_i w_i \) with \( \lambda_1, \ldots, \lambda_n \in GF(p) \), let

\[
\delta_{th}(u) = \alpha(u) + \sum_i (\lambda_i^q) f(\alpha(t^h w_i), w_i) + \sum_{i < j} \lambda_i \lambda_j f(\alpha(t^h w_i), w_j).
\]

A straightforward calculation shows that \( \delta_{th} \in Der(V, W) \). The \( GF(p) \)-vector space \( Der(V, W) \) becomes a module for the additive group of \( T \) via \( t(\delta)(u) = d(u) + g(d(u), t) \) \( (u \in V, t \in T, d \in Der(V, W)) \). We extend \( \delta \) to an element of \( Der(T, Der(V, W)) \) as follows: For \( s = \sum \lambda_h t^h \) with \( \lambda_1, \ldots, \lambda_k \in GF(p) \) and \( u \in V \), let

\[
\delta_s(u) = \sum_h \lambda_h \delta_{th}(u) + \sum_h (\lambda_h^q) g(\alpha(u), t^h) + \sum_{h < j} \lambda_h \lambda_j g(\alpha(t^h u), t^h).
\]

For \( s \in T \), define \( y_s : H \to H \) by setting

\[
y_s((u, \alpha(v) + z + d)) = (u, \delta_s(u) + \alpha(v) + g(\alpha(v), s) + z + d) \quad (u, v \in V, z \in Z, d \in D).
\]

A direct calculation shows that \( y_s \in Aut(H) \). For \( s, s' \in T \), and \( u, v \in V \), we have \( y_{s'}((u, \delta_s(u) + \alpha(v) + g(\alpha(v), s))) = (u, \delta_s(u) + \delta_{s'}(u) + \alpha(v) + g(\alpha(v), s) + g(\alpha(v) + \delta_s(u), s')) \). Now \( g(\delta_s(u), s') = \alpha(s(u)) \otimes s' + I = ss' \alpha(u) \otimes I = s' \alpha(u) \otimes s + I = \alpha(s' u) \otimes s + I \), whence \( y_{s'}y_s = y_s y_{s'} = y_{s+s'} \). If \( y_s = id \), then \( \delta_s = 0 \) and \( s = 0 \), so the map \( s \mapsto y_s \) is an embedding of \( (T, +) \) into \( Aut(H) \).

**Definition 1.5.** Let \( S(m, k) = H \rtimes Y \), where \( Y = \{y_s \mid s \in T\} \).

Let \( S(m, k) = S \). To prove that \( S \) is a CH-p-group, let \( t, t' \in T \setminus \{0\} \), \( u, u' \in V \), let \( x = uy_t \), and let \( X = [W, x] \). In additive notation, \( X = \{f(\alpha(v), u) + g(\alpha(v), t) \mid v \in V\} \). The condition

\[
[uy_t, yv_t]X = [uy_t, u']X
\]

translates to \( \delta_{t'}(u) + g(\alpha(t' u), t) + X = -\delta_t(u') + X \), which forces \( t'u = -tu' \). Let \( t^{-1}t' = s \).

The group \( L = GF(p^k)^* \) already acts on \( V \) and on \( V_1 \). Thus \( L \) acts on \( V_1 \otimes T V \) via \( \lambda(\alpha(v) \otimes u) = \lambda\alpha(v) \otimes \lambda u = \lambda^2 \alpha(v) \otimes u \) \( (u, v \in V, \lambda \in L) \) and the ideal \( I \) is \( L \)-invariant with respect to this action. Likewise, \( L \) acts on \( D \) via \( \lambda(\alpha(v) \otimes t) = \lambda\alpha(v) \otimes \lambda t = \lambda^2 \alpha(v) \otimes t \) \( (v \in V, \lambda \in L, t \in T) \).

Now set \( \lambda(u, \alpha(v) + z + d) = (\lambda(u), \lambda(v) + \lambda(z) + \lambda(d)) \) \( (\lambda \in L, u, v \in V, z \in Z, d \in D) \) to obtain an embedding of \( L \) into \( Aut(H) \). It should be noted that \( L \) normalises \( X \). For \( r \in GF(p^k) \), the set \( E_r = \{d : U \to Z + D \mid d(u_1 + u_2) = d(u_1) + d(u_2) + f(\alpha(ru_1), u_2)\} \) is invariant with respect to the natural action of \( L \) on \( (Z + D)^U \). Let \( E = \langle E_r \mid r \in GF(p^k) \rangle \). Then \( E \) is a group with respect to the addition of maps, and both \( \delta_st \) and the map given by \( v \mapsto \delta_t(-sv) \) \( (v \in V) \) are in \( E \), as is
the map $v \mapsto g(\alpha(stv), t)$. Let $\eta_{s,t,u} = \delta_{s}(u) + \delta_{t}(-su) + g(\alpha(stu), t)$. If $\eta_{s,t,u} \in X$ and $\lambda \in L$, then $\lambda(\delta_{s}(\lambda^{-1}u) + \delta_{t}(-s\lambda^{-1}u)) + \lambda g(\alpha(st(\lambda^{-1}u), t)) \in X$, which implies that $\delta_{s}(\mu u) + \delta_{t}(-s\mu u)) + g(\alpha(st(\mu u), t)) \in X$ whenever $\mu \in L$.

Now let $r_{1}, r_{2} \in T$; then $f(\alpha(r_{1}r_{2}(s^{2} + s)tu, u) = \eta_{s,t,(r_{1}+r_{2})u} - \eta_{s,t,r_{1}u} - \eta_{s,t,r_{2}u} \in X$ which implies that $s = -1$.

It is straightforward from the definition of $S$ that if $g \in H \setminus ZD$, then $C_{S}(g) \leq H$ and that, if $y \in Y \setminus \{1\}$, then $C_{S}(y) = Y$. The calculations conducted in the previous paragraph show that for a "diagonal" element $x = gy, g \in H \setminus ZD, y \in Y \setminus \{1\}$, we have $C_{S}(x) = ZD(x)$. Together with the fact that $H$ is a CA-group, this implies that $S$ is a CH-group.

**Proposition 1.6.** If $cl(H) = 2$, then one of the following holds:

a) There are $k, m \in \mathbb{N}, m > 2$, such that $G$ is isoclinic to $K/E$ where $H(m, k) = K \leq S(m, k)$ and $E \leq Z(S(m, k))$. In particular, $cl(G) = 3$.

b) $H = M \cup Z$, and, for $x \in M, \{H, x\} = H'$. If $y \in G \setminus H$, then $C_{H}(y) = Z(G)$ and $G = HC_{G}(y)$; for $i \in \mathbb{N}, Z_{i}(G) \cap H = \{h, h \in H, (h, y) = 1\}$ and $[H_{i}, G] = [H_{i}, h]$.

Finally, $cl(G) \leq p + 1$, and this bound is attainable.

**Proposition 1.9** requires a definition, which will be preceded by two lemmas of which the second seems generally useful for the construction of groups of class $3$. The first is a minimally modified special case of [9], Theorem 6.7 (construction of semiextraspecial groups from a $GF(q)$-symplectic form).

**Lemma 1.7.** Let $n \in \mathbb{N}$, and let $q = p^{n}$. Let $A$ and $B$ be finite $p$-groups of rank $n$, with respective Frattini quotients $\overline{A}$ and $\overline{B}$. Pick isomorphisms $\varphi : (GF(q), +) \to \overline{A}$, and $\psi : (GF(q), +) \to \overline{B}$. Define a multiplication on the set $A \times B \times (GF(q), +)$ via

$$(a, b, \gamma)(a', b', \gamma') = (aa', bb', c + c' - a^{-1}b^{-1}b^{-1})$$

(a, b, c \in GF(q)).

With this multiplication, $A \times B \times GF(q)$ becomes a group which, if $A$ and $B$ are abelian, is isoclinic to a Sylow-$p$-subgroup of $U_{3}(q)$.

**Proof:** The first statement follows as in [9], Theorem 6.7.

The second statement is well-known: A Sylow-$p$-subgroup $Q$ of $U_{3}(q)$ is isomorphic to the group of matrices $Q(a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & -a^{\tau} \\ 0 & 0 & 1 \end{pmatrix}$ where $a, b \in GF(q^{2}), \tau$ is the field automorphism given by $x \mapsto x^{q}$ ($x \in GF(q^{2})$) and $aa^{\tau} + b + b^{\tau} = 0$ ([4], Satz II, 10.12). Then $\{Q(a, b) \mid a \in GF(q), a^{2} + b + b^{\tau} = 0\}$ is an abelian subgroup of $Q$, of which we select a subgroup $A$ such that, for every $a \in GF(q)$, contains exactly one element $Q(a, b)$. Let $\lambda \in GF(q^{2}) \setminus GF(q)$, and let $B = \{Q(\lambda a, \lambda^{-1}b) \mid Q(a, b) \in A\}$. Then $Q = ABZ(Q)$, and if $a, a' \in GF(q)$, and $Q(a, b) \in A$, then $[Q(a, b), Q(\lambda a', \lambda^{-1}b)] = Q(0, aa'(\lambda - \lambda^{7}))$.

**Lemma 1.8.** Let $P_{1}$ and $P_{2}$ be finite $p$-groups, and let $A$ be a $GF(p)$-vector space. Let $A \geq E = E_{1} \oplus E_{2}$.

For $i = 1, 2$, let $g_{i} : A \times P_{i} \to E_{i}$ satisfy the following conditions:

For $a, a' \in A$, and $x_{i} \in P_{i},$ and $b \in E$
With this definition, 
\[ P(a, x_i) + P(a', x_i), \]
\[ g_1(b, x_1) = 0 = g_2(b, x_2) \]  
Then the following hold:

1) Let \( f : P_2 \times P_1 \rightarrow A \) be such that, for \( x, x' \in P_1 \) and \( y, y' \in P_2 \),
\[ f(yy', x) = f(y, x) + f(y', x) + g_2(f(y, x), y'), \]
\[ f(y, xx') = f(y, x) + f(y', x') + g_1(f(y, x), x'), \]
\[ g_2(f(y, x), y') = g_2(f(y', x), y), \]
\[ g_1(f(y, x), x') = g_1(f(y, x'), x). \]  
Define a multiplication on \( P_1 \times P_2 \times A \), by setting
\[ (x, y, a)(x', y', a') = (xx', yy', aa'f(y, x')g_1(a, x')g_2(a, y')g_2(f(y, x'), y')). \]  
With this definition, \( P_1 \times P_2 \times A \) becomes a group \( R \). Identifying \( P_1 \) and \( P_2 \) with the subgroups \( \{(x, 1, 1) \mid x \in P_1\} \), and, respectively, \( \{(1, y, 1) \mid y \in P_2\} \) of \( R \), we obtain
\[ f(y, x) = [y, x] \quad (x \in P_1, y \in P_2). \]

2) Let \( B \) be a complement of \( E \) in \( A \). Let \( h : P_2 \times P_1 \rightarrow B \) be such that, for \( x, x' \in P_1 \) and \( y, y' \in P_2 \),
\[ h(yy', x) = h(y, x) + h(y', x), \]
\[ h(y, xx') = h(y, x) + h(y, x') \]
\[ g_2(h(y, x), y') = g_2(h(y', x), y), \]
\[ g_1(h(y, x), x') = g_1(h(y, x'), x). \]  
Then there is a map \( f : P_2 \times P_1 \rightarrow A \) satisfying (b) and (c), while \( g_1(f(y, x), x') = g_1(h(y, x), x') \)
and \( g_2(f(y, x), y') = g_2(h(y, x), y') \) for \( x, x' \in P_1 \), \( y, y' \in P_2 \).

**Proof:** Let \( P_1 \times P_2 = P \), and let \( w \in P \). There are uniquely determined elements \( x_w \) and \( y_w \) of \( P_1 \) and \( \Phi(P) \), respectively, such that \( w = x_wy_w \). Condition (a) ensures that, setting \( wa = g_1(a, x_w)g_2(a, y_w) \) \((a \in A)\), turns \( A \) into a \( P \)-module. By (b) \([A, P, P] = 0\), in particular \([A, \Phi(P)] = 0\).

Let \( \alpha(xy, x'y') = f(y, x') + g_2(f(y, x'), y') \) \((x, x' \in P_1, y, y' \in P_2)\).

A straightforward calculation shows that \( \alpha \) is a 2-cocycle from \( P \times P \) to \( A \) and that \( R \) is the extension of \( A \) by \( P \) corresponding to \( \alpha \).

Finally, let \( x \in P_1 \) and \( y \in P_2 \). We have
\[ (1, y^{-1}, 1)(x^{-1}, 1, 1)(1, y, 1)(x, 1, 1) = \]
\[ (x^{-1}, y^{-1}, f(y^{-1}, x^{-1}))(1, y, 1)(x, 1, 1) = \]
\[ (y, x, y, x')g_2(f(y^{-1}, x^{-1}, y))g_1(f(y^{-1}, x^{-1}, x)). \]  
As \( f(y^{-1}, x^{-1}) = f(y^{-1}, x)^{-1}g_1(f(y^{-1}, x), x^{-1})^{-1} = f(y, x)g_2(f(y, x), y^{-1}), \) while \( g_2(f(y^{-1}, x^{-1}, y) = g_2(f(y, x), y) \) and \( g_1(f(y^{-1}, x), x^{-1}) = g_1(f(y^{-1}, x^{-1}, x)), \) assertion 1 is proved.

As to 2), let \( \{u_1, \ldots, u_k\} \) and \( \{v_1, \ldots, v_k\} \) be minimal generating set for \( P_1 \) and, respectively, \( P_2 \). For \( i \in \{1, \ldots, k\} \) and \( j \in \{1, \ldots, l\} \) set \( \delta_{v_i}(u_j) = -\eta_{u_j}v_i = h(v_i, u_j), \) and extend \( \delta_{v_i} \) to a derivation from \( P_1 \) to the \( P_1 \)-module \( A \) and \( \eta_{u_j} \) to a derivation from \( P_2 \) to the \( P_2 \)-module \( A \) by the rules
\[ \delta_{v_i}(u + u') = \delta_{v_i}(u) + \delta_{v_i}(u') + g_1(h(v_i, u), u') \quad (u, u' \in P_1), \]
\[ \eta_{u_j}(v + v') = \eta_{u_j}(v) + \eta_{u_j}(v') + g_2(h(v, u_j), v') \quad (v, v' \in P_2). \]
Observe that $\delta_{ij}$ and $\eta_{ij}$ are completely determined by these conditions. Extend $\delta$ and $\eta$ to homomorphisms $P_2 \to \text{Der}(P_1, A)$ and, respectively, $P_1 \to \text{Der}(P_2, A)$. For $v \in P_2$ and $u \in P_1$ let

$$f(v, u) = \delta(v, u) + \eta(v) - h(v, u).$$

For $v, v' \in P_2$ and $u, u' \in P_1$, we have $f(v, v', u) = \delta(v) + \delta(v') + \eta(u) + \eta(u') + g_2(h(v, u), v') - h(v, u) - h(v', u) = f(v, u) + f(v', u) + g_2(h(v, u), v')$, and $f(v, uu') = \delta(v) + \delta(u) + \eta(u) + \eta(u') + g_1(h(v, u), u') - h(v, u) - h(v, u').$

This is 2). Definition: Let $P_1$, $P_2$, $E_1$, $E_2$, $B \cong (GF(q), +)$ with isomorphisms $\varphi_1: (GF(q), +) \to P_1$, $\psi_1: (GF(q), +) \to E_i (i = 1, 2)$ and $\varphi: (GF(q), +) \to B$. Let $A = B \times E_1 \times E_2$ and let $\pi: A \to B$ be the projection map. Define the required maps $h: P_2 \times P_1 \to B$ and $g_i: A \times P_i \to E_i (i = 1, 2)$ by $h(\varphi_2(\mu), \varphi_1(\nu)) = \varphi_3(-\mu \nu)$ and $g_i(a, \varphi_i(\mu)) = \psi_1(\kappa \mu)$, where $\kappa = \varphi^{-1}(\pi(a), (i = 1, 2, \mu, \nu) \in GF(q))$.

Clearly, $h$, $g_1$, and $g_2$ satisfy every requirement of 1.8 2) and we may define a group structure on $P_1 \times P_2 \times A$ as in 1.8 1). The particular choice of any of the isomorphisms involved in the construction does not affect the isomorphism type of the resulting group, which will be denoted by $R(n)$.

We note: $R(n)$ is a CH-p-group.

Indeed, the conjugacy class size of every element of $R(n)$ outside $E_1 \times E_2 = Z(R(n))$ is $p^{2n}$, so $R(n)$ has conjugate rank 2, and in particular is a CH-group.

**Proposition 1.9.** If $H' \leq Z$, then $G = H$ and there is $n \in \mathbb{N}$ such that $G$ is isoclinic to $R(n)$.

Letting $q = p^n$, we thus have $|A| = q$, $G$ is ultraspecial of order $q^3$, and the map $(x, y) \to [\bar{x}, \bar{y}] (x, y \in G)$ induces a $GF(q)$-symplectic form on $G/A$. If $x, y \in M$ with $[\bar{x}, \bar{y}] \neq 1$, and $a \in A \setminus Z$, then

$[A, G] = [a, G] = [A, x] \times [A, y]$, while $|[a, G]| = p^b$, and $[A, v] = q$ whenever $v \in M \setminus A$.

## 2. Auxiliary lemmas

**Notation:** Let $x \in G$. Using the notation of [8], we let $M_x = AC_G(x)$.

**Lemma 2.1.** [8, Lemma 5(a)] Let $a \in A$, $x \in G$. Then $[a, M_x \cap M_{ax}] \leq [A, x]$.

**Notation:** Let $V$ be a vector space and let $M \subseteq GL(V)$. Following [9], we say that $M$ is $D$-independent if every nonzero linear combination of elements of $M$ is a bijection. Analogously, a set $M$ of quadratic matrices is $D$-independent if every nonzero linear combination of its elements has nonzero determinant.

**Lemma 2.2.** Let $n \in \mathbb{N}$, and let $V$ be a vector space over $GF(p)$ of dimension $n$. Let $\{A_1, \ldots, A_n\}$ be a $D$-independent set of commuting $n \times n$-matrices over $GF(p)$. Then there is a Singer cycle $S \in GL_n(p)$ such that, for $i = 1, \ldots, n$, $A_i$ is a power of $S$. Furthermore, every power of $S$ is a $GF(p)$-linear combination of $\{A_1, \ldots, A_n\}$.

**Proof:** Let $\langle A_1, \ldots, A_n \rangle = X$ and let $k$ be a (finite) splitting field for $X$ on $V$. For $i = 1, \ldots, n$, let $A_i = S_i + N_i$ be the Jordan decomposition of $A_i$; i.e., $S_i$ is semisimple, $N_i$ is nilpotent, and both $S_i$ and $N_i$ are polynomials in $A_i$. Since $X$ is abelian, there is a basis of $V_k$ with respect to which every $S_i$ is a diagonal matrix and every $N_i$ is upper triangular with zeros in the diagonal. Let $i \in \{1, \ldots, n\}$
and let \( Q = O_p(X) \). Being polynomials in \( A_i, S_i \) and \( N_i \) are centralised by \( X \). Upon writing \( A_i \) as a product \( A_i = B_i C_i \) with \( B_i \in Q \) and \( C_i \in O_p(X) \), we have \( B_i = S_i \) \((11), 27.9\). In particular, \( Q = (S_1, \ldots, S_n) \).

Consider a \( GF(p) \)-linear combination \( D = \lambda_1 A_1 + \cdots + \lambda_n A_n \). Then \( D = S + N \), where \( S = \lambda_1 S_1 + \cdots + \lambda_n S_n \) and \( N = \lambda_1 N_1 + \cdots + \lambda_n N_n \). Clearly \( S \) is a diagonal matrix, and \( N \) is upper triangular with zeros in the diagonal, whence \( \det D = \det S \). So \( \{ S_1, \ldots, S_n \} \) is a \( D \)-independent set of diagonal matrices over \( k \).

Let \( V = V_1 \oplus \cdots \oplus V_t \) be a decomposition of \( V \) into irreducible \( GF(p)\{|C\}_1 \)-submodules. For \( j \in \{1, \ldots, t\} \), \( Q/C_Q(V_j) \) is cyclic. Let \( m = \dim V_1 \) and let \( Q = \langle T \rangle C_Q(V_1) \). There is \( \mu \in GF(p^n) \) such that the degree of the minimum polynomial of \( T \) over \( GF(p) \) is \( m \) and the eigenvalues of \( T \) on \( V_1 \) are the algebraic conjugates of \( \mu \). Let \( w \in V_1^k \) be an eigenvector for \( S_i \) \((i = 1, \ldots, n) \) with \( T(w) = \mu w \) and let \( \lambda_1, \ldots, \lambda_n \in GF(p) \). There are powers \( \mu^{i_1}, \ldots, \mu^{i_n} \) such that \( S_j(w) = \mu^j w \). As \( \langle \lambda_1 S_1 + \cdots + \lambda_n S_n \rangle = \langle \lambda_1 \mu^{i_1} + \cdots + \lambda_n \mu^{i_n} \rangle \) \( \mu \) is linearly independent over \( GF(p) \), which is possible only if \( GF(p^n) = GF(p)[\mu^{i_1}, \ldots, \mu^{i_n}] \).

Consequently \( Q \) is irreducible on \( V \) and hence is cyclic. For \( i = 1, \ldots, n \), \( N_i \) is (the matrix of) a nilpotent endomorphism of \( V^k \) centralising \( Q \), whence \( N_i = 0 \) for \( i = 1, \ldots, n \).

**Lemma 2.3.** Let \( V \) be a finite-dimensional vector space over \( GF(p) \), and let \( P \leq GL(V) \) be an abelian \( p \)-group. For \( i \in \mathbb{N}_0 \), let \( C_i(P) = \{ v \in V, | [v, i] P = 0 \} \), and, for \( x \in P \), define \( C_i(x) \) accordingly. Suppose that, for \( y \in P \setminus \{1\} \), \( C_V(P) = C_V(y) \). Then \( C_i(P) = C_i(y) \) for \( y \in P \setminus \{1\} \) and \( i \in \mathbb{N}_0 \).

**Proof:** Induction on \( i \). If \( i \in \{0, 1\} \), then the assertion is trivial or, respectively, included in the premise. Let \( i \geq 2 \), \( x, y \in P \setminus \{1\} \) and \( v \in C_i(x) \). Via induction, \( [v, x] \leq C_{i-1}(x) = C_{i-1}(y) \), and \( [v, x, y] \leq C_{i-2}(x) = C_{i-2}(P) \). Let \( C_{i-2}(P) = D \). Since \( P \) is abelian, \( 0 \equiv [v, x, y]^{-1} \equiv [y, v, x] \) \((\mod D) \), whence \( [v, y] \leq C_{i-1}(x) = C_{i-1}(y) \) and \( v \in C_i(y) \).

For the following lemma, we assume familiarity with Marshall Hall’s definition of basic commutators \((13) \) p.165). We take the set of basic commutators as totally ordered by the relation “\(<\)” satisfying \( c < c' \) if \( w(c) < w(c') \) and \( x_i < x_j \) if \( i < j \) \((i, j \in \{1, \ldots, n\}) \).

Since the reader is believed to be familiar with commutator collecting arguments, some details in the proof are left to her/him.

**Lemma 2.4.** Let \( k, n \in \mathbb{N}, k, n \geq 2 \), and let \( F \) be the relatively free group of class \( k \) with free generators \( x_1, \ldots, x_n \). Let \( M \) be the verbal subgroup of \( F \) generated by the word \([w_1, w_2], [w_3, w_4]\).

Then \( M \) is the set of elements \( c_1^{\epsilon_1} \cdots c_s^{\epsilon_s} \) where \( s \in \mathbb{N}, \epsilon_1, \ldots, \epsilon_s \in \mathbb{Z} \), and \( c_1, \ldots, c_s \) are basic commutators in \( \{x_1, \ldots, x_n\} \) of weight less than \( k \) such that \( c_1 \prec \cdots \prec c_s \) and each \( c_i \) is of the form \( c_i = [\eta_i, \gamma_i] \) where \( \eta_i \) and \( \gamma_i \) are basic commutators of weight at least \( 2 \).

**Proof:** We divide the proof into three steps:

a) Let \( \eta \in F, \eta = [u_1, \ldots, u_i, \gamma, v_1, \ldots, v_j, \delta, w_1, \ldots, w_l] \). We shall say that \( \eta \) is an \((*)\)-commutator if \( \gamma \) and \( \delta \) are basic commutators of weight at least \( 2 \) in \( x_1, \ldots, x_n \), and the \( u_i, v_j, \) and \( w_k \) are elements of \( \{x_1, \ldots, x_n\} \). Observe that, for \( 4 \leq l \leq k - 1 \), the subgroup \( N_{\ell} \) generated by the \((*)\)-commutators
of weight at least \( \ell \) is a normal subgroup of \( F \) contained in \( \gamma_\ell(F) \cap M \).

Let \( w(\eta) = \ell \). Repeated application of the commutator identities
\[
[a, b^{-1}, c]^\varepsilon = [a, c][b, c^{-1}, a]^\varepsilon, [a, b^{-1}] = [a, b, b^{-1}]^{-1}[a, b]^{-1}, \text{ and } [a, bc] = [a, c][a, b]c \text{ together with M. Hall’s basis theorem (3, Theorem 11.2.4) shows that } \eta \in \kappa N_{\ell+1} \text{ for some product } \kappa \text{ of terms } [\gamma, \delta]^{\varepsilon},
\]
where \( \varepsilon \in \{1, -1\} \), \( \delta \) and \( \gamma \) are basic commutators such that \( w(\delta) + w(\gamma) = \ell \) and \( w(\delta) \geq 2 \). Without loss, \( \gamma > \delta \). Let \( w(\gamma) + w(\delta) = \ell \leq k - 1 \). We prove that, modulo \( N_{\ell+1}, [\gamma, \delta] \) is in the subgroup generated by basic commutators \( \{\eta, \eta’\} \), such that \( \eta \) and \( \eta’ \) are basic commutators with \( \eta \succ \eta’ \succ \delta \) or \( \eta \succ \eta’ = \delta \). Observe that this implies that \( w(\eta) \geq 2 \leq w(\eta’). \)

If \( [\gamma, \delta] \) is a basic commutator, there is nothing left for us to do. If not, then \( \gamma = [\gamma_1, \gamma_2] \) with basic commutators \( \gamma_1 \) and \( \gamma_2 \) such that \( \gamma_1 \succ \gamma_2 \succ \delta \). If \( \ell \) is even and \( w(\delta) = \frac{\ell}{2} \) or if \( \ell \) is odd and \( w(\delta) = \frac{\ell - 1}{2} \), then, as \( w(\delta) \geq 2 \), this constellation is impossible. If \( \eta \) and \( \eta’ \) are basic commutators with \( w(\eta) > w(\eta’), \) then \( \eta \succ \eta’ \), so we may argue by reverse induction on the position of \( \delta \) in the ordering of basic commutators of weight less than \( \ell \).

Now \( [\gamma, \delta] \in [\gamma_2, \delta, \gamma_1][\delta, \gamma_1, \gamma_2]N_{\ell+1} \). Let \( \{1, 2\} = \{s, t\} \) and \( w([\gamma_s, \delta]) = w, \) observing that \( w > w(\delta) \). Then \( [\gamma_s, \delta] \) is a product of basic commutators of weight no less than \( w \) or the inverses of such. Thus there is an element \( \nu \) of the subgroup generated by terms \( [\eta, \gamma_i], \) where \( \eta \) is a basic commutator with \( w(\eta) = w \), such that \( [\gamma_i, \delta, \gamma_i] \in \nu N_{\ell+1} \). If \( w(\eta) = w, \) then \( \eta \succ \delta \); we know that \( \delta \prec \gamma_i \), so induction applies to \( [\eta, \gamma_i] \) and we are through.

c) Let \( 4 \leq \ell \leq k - 1 \). By a) and b), \( N_{\ell} \) is generated by basic commutators \( [\gamma, \delta] \) with \( w(\gamma) \geq 2 \leq w(\delta) \) and \( w(\gamma) + w(\delta) \geq \ell \). A commutator \( [[\gamma, \delta], [\gamma’, \delta’]] \) is in \( N_{\ell+1} \), so if \( y \) is a product of commutators of this type or their inverses, collecting the terms to the left will produce an element \( y[N_{\ell+1}] \) which is an ordered product of the form \( \epsilon_1 \cdots \epsilon_s \) as required by the lemma and such that \( w(\epsilon_1) = \ell = \ldots = w(\epsilon_s) \).

As a basic commutator of weight \( \ell + 1 \) succeeds a basic commutator of weight \( \ell \) with respect to \( \prec \), reverse induction on \( \ell \) completes the proof.

3. Proof of Proposition 1.3

a) Let \( k \in \mathbb{N} \). We prove that there is \( n \in \mathbb{N} \) such that, if \( A \) and \( B \) are abelian groups of rank \( n \), then the group on \( A \times B \times GF(q) \) constructed as in 1.7 possesses a \( k \)-generated subgroup whose commutator subgroup has rank \( \left(\frac{k}{2}\right) \). Note that it is sufficient to prove this for the groups constructed from elementary abelian groups \( A \) and \( B \), which we shall call \( Q(m), m \) being the rank of \( A \) and \( B \). We proceed by induction on \( k \). If \( k = 1 \), there is nothing to prove. Let \( k > 1 \) and assume that there is \( \langle x_1, \ldots, x_{k-1} \rangle = U \leq Q(p^m) \) such that \( \text{rk } U' = \binom{k-1}{2} \). Let \( n = m \ell \) with \( \ell > 2 \) and let \( Q = Q(p^n) \).

As \( GF(p^m) \) is a subfield of \( GF(p^n) \), the set \( H = \{(a, b, c) | a, b, c \in GF(p^m)\} \) is a subgroup of \( Q \) isomorphic to \( Q(p^m) \). Let \( s, t \in GF(p^m) \) be such that \( \{1, s, t\} \) is linearly independent over \( GF(p^m) \) and let \( u = (s, t, 0) \). Then \( [u, H] = \{(0, 0, at - bs) | a, b \in GF(p^m)\} \), and our choice of \( s \) and \( t \) ensures that \( C_H(u) = H \cap Z(Q) = H' \) and that \( [u, H] \cap H = 1 \). Now let \( x_k = u \) to obtain that
\( \langle x_1, \ldots, x_{k-1}, x_k \rangle \) is a \( k \)-generated subgroup of \( Q \) whose commutator subgroup has rank \( \binom{k}{2} \).

b) Let \( P \) be a \( \text{CH-p} \)-group of class 2 and let \( x \in P \). There is \( y \in P \) with \( [x, y] \neq 1 = [x, y]^p = [x^p, y] \), so if \( U \leq P \), then \( U_1(U) \subseteq Z(U) \).

Conversely, let \( R \) be a finite \( p \)-group of class 2 with \( U_1(R) \subseteq Z(R) \), let \( rk R = k \) and \( \exp R = p^e \). For \( m \in \mathbb{N} \), let \( A(m) \) and \( B(m) \) be homocyclic of exponent \( p^e \) and rank \( m \), and let \( P(m) \) be the group on \( A(m) \times B(m) \times GF(q) \) constructed as in \( \text{1.7} \). By a), we can find \( n \) such that \( P(n) \) has a subgroup \( U = \langle x_1, \ldots, x_k \rangle \) with \( rk U' = \binom{k}{2} \). Let \( P(n) = P \). Note that \( Z(P) = \Phi(P), \) \( rk P/Z(P) = 2n \), and that if \( H \leq P \) and \( i \leq e - 1 \), then \( rk (U_i(H)/P'/P') = rk (H\Phi(P)/\Phi(P)) \). Now \( "rk U' = \binom{k}{2}" \) forces \( U \cap \Phi(P) = \Phi(U) \); moreover, \( U \) is relatively free of class 2 with elementary abelian commutator subgroup, with \( k \) free generators \( x_1, \ldots, x_k \). Accordingly, there is \( N \leq \Phi(U) \) such that \( U/N \cong G \).

Now \( cl(G) = 2 \), and \( G' \cong P'/P' \cap N \neq 1 \). Now \( P \) is ultraspecial, whence \( P/N \) is semiextraspecial and is, in particular, a \( \text{CH-p} \)-group.

4. Proof of Proposition 1.4

Suppose that \( H \) is abelian, i.e. \( H = A \). Since \( G'Z \leq H, G/H \) is elementary abelian, and, as \( H \) is abelian, we have \( H = C_G(x) \) whenever \( x \in M \) and \( |G : H| = p^e \). Let \( y \in G \setminus H \) and, for \( i \in \mathbb{N} \), let \( C_i(y) = \langle h \in H \mid [h, y] = 1 \rangle \). By Lemma 2.3, \( C_i(y) \) is elementary abelian, and, as \( H \) is abelian, we have \( [H, P] = 1 \) so \( H \leq Z_p(G) \) and \( cl(G) \leq p + 1 \).

Let \( n, k \in \mathbb{N} \) and let \( F \) and \( M \) be as defined above Lemma 2.4. Let \( \ell \in 4, \ldots, k - 1 \) and let \( x \in M \cap \gamma(\ell)(F) \). By Lemma 2.4, \( x = c_1^i \ldots c_s^i \) where each \( c_i \) is a basic commutator of the form \( \langle \eta_i, \gamma_i \rangle \) where \( \eta_i \) and \( \gamma_i \) are basic commutators of weight at least 2. By Hall’s basis theorem (3, Theorem 11.2.4), each \( c_i \) is of weight at least \( \ell \). Moreover, the set of basic commutators of the form \( \langle \gamma, x \rangle \) with \( x \in \{ x_1, \ldots, x_n \} \) and \( \gamma \) a basic commutator of weight \( \ell - 1 \) is a basis of \( \gamma(\ell)(F) \) over \( (\gamma(\ell)(F) \cap M)\gamma(\ell+1)(F) \).

Let \( i \in \{1, \ldots, n\} \) and let \( \gamma \) be a basic commutator. Then \( \langle \gamma, x_i \rangle \) is a basic commutator if and only if \( \gamma = \langle \gamma', x_j \rangle \) with \( j \leq i \) and \( \gamma' \succ x_j \). Let \( S \) be the set of terms \( \{ x_{i_1}, x_{i_2}, \ldots, x_{i_w} \} M \) with \( i_1 > i_2 \leq i_3 \leq \ldots \leq i_w \) and \( 2 \leq w \leq k \), \( \nu \). Via induction on \( \ell \), \( (F/M)'/\gamma(\ell+1)(F) \) is free abelian, freely generated by \( S \). Hence the elements of \( F/M \) are in one-to-one correspondence with the words \( c_1^{\epsilon_1} \ldots c_s^{\epsilon_s} \) where \( \epsilon_1, \ldots, \epsilon_s \in \mathbb{Z}, c_1, \ldots, c_s \in S \cup \{ x_1, \ldots, x_n \} \) and \( c_1 < \ldots < c_s \).

Let \( N = M\Omega_3(\gamma(2)(F)) \) and let \( F/N = F \). Observe that \( F \) is the relatively free group on \( n \) free generators with elementary abelian derived subgroup, and that the elements \( \{ x_{i_1}, x_{i_2}, \ldots, x_{i_w} \}, i_1 > i_2 \leq i_3 \leq \ldots \leq i_w, 2 \leq w \leq k \) form a basis of \( F' \) which we shall denote by \( B \). Let \( 1 \leq \ell < k - 1 \) and let \( y = x_n \). If \( \gamma \in B \) has weight \( \ell \), then \( \langle \gamma, y \rangle \in B \). Accordingly, \( |\gamma(\ell)(F)/\gamma(\ell+1)(F)| = |\gamma(\ell)(F)/\gamma(\ell+2)(F)/\gamma(\ell+2)(F)| \), so \( C_F(\bar{y}) = \gamma_{k-1}(F) = Z(F) \). As \( F \) is relatively free, every element of \( F \setminus \Phi(F) \) is the image of \( \bar{y} \) under some automorphism of \( F \). Thus \( C_F(\bar{x}) = \gamma_{k-1}(F) = Z(F) \).

Assume that \( k \leq p + 1 \) and let \( g, h \in F \). As \( F' \) is elementary abelian, \( [g, h^p] = [g, p h] = 1 \). Let \( k = p + 1 \) and \( G = F/I_2(F) \), \( H = G' \), to obtain a \( \text{CH-p} \)-group of the required type and of class \( p + 1 \).
5. Proof of Proposition 1.6

Let \( d(H) = 2 \) remembering that this implies that \( Z(H) = Z \).

Let \( V, W \leq H \). We claim that

For \( i, j \in \mathbb{N}_0 \), \([V, iG], [W, jG] = [V, [W, i+jG]]\).

(0)

True for \( i = 0 \). Suppose \( i > 0 \) and let \( X = [V, G] \). Via induction on \( i \), \([X, i-1G], [W, jG] = [X, [W, j+i-1G]]\).

Letting \( Y = [W, j-i-1G] \), the Three-Subgroups-Lemma says that \([X, Y] = [V, G, Y] = [G, Y, V] = [V, [W, i+jG]]\).

Let \( \ell \in \mathbb{N}_0 \) and let \( x \in M \) with \([x, \ell G] \notin Z \). If \( \ell = 0 \), then \( H = [H, \ell G] = [H, \ell G]C_H(x) \). Now suppose \( H = [H, \ell G]C_H(x) \) and \([x, \ell+1G] \notin Z \). Let \( g \in G \) be such that \([x, g, \ell G] \notin Z \) and let \( v = [x, g] \).

Via induction, \( H = [H, \ell G]C_H(v) \), and \([H, v] = [H, \ell G, v] \). By (0) \([H, \ell G, v] = [H, \ell+1G, x] \), and since \([H, v] = [H, \ell G, v] = [H, x] \), we obtain \([H, x] = [H, \ell+1G, x] \) and \( H = [H, \ell+1G]C_H(x) \), as desired. Thus

If \( v \in M \) and \( \ell \in \mathbb{N}_0 \) with \([v, \ell G] \neq 1 \), then \( H = C_H(v)[H, \ell G] \).

(1)

Let \( \ell \in \mathbb{N} \) be minimal with \([H, 2G] \leq Z \). If \([H, \ell G] \leq Z \), then \( \ell > 2\ell - 2 \) which forces \( \ell = 1 \) and \([H, G] = 1 \), implying \( G' \leq Z(H) = Z \), by the Three-Subgroups-Lemma. Thus \([H, \ell G] \leq Z \). Let \([H, \ell G] = W \). By (0), \( W' \leq [H, 2G, H] = 1 \). Let \( v \in W \setminus Z \). Since \( W \leq G' \subseteq M \cup Z \), \( M \) is the set of elements of \( G \) whose centraliser has order \(|C_G(v)| \).

Since \( W \cap Z \notin Z \), and \( A \) may be any maximal abelian normal subgroup of \( G \) which has nonempty intersection with \( M \), we may without loss take \( W \leq A \).

Let \( x \in H \) such that \([x, \ell G] \neq 1 \). By (1), \( H = [H, \ell G]C_H(x) = M_x \).

The possibilities "\( Ax \notin M' \)" and "\( Ax \subseteq M' \)" need to be considered separately; the first case leads to the groups in (1.6a), the second to those in (1.6b).

a) Suppose that \( Ax \notin M \) and let \( b \in A \) with \( xb \notin M \). If \( C_H(b) > A \), then, as \( H = M_x \), \( C_G(x) \cap C_G(b) = C_G(x) \cap C_G(xb) \leq A \). However, \( C_G(x) \cap A \subseteq M \), so \( xb \in M \), a contradiction. Accordingly,

If \( a \in A \setminus Z \) then \( C_G(a) = A \).

(i)

Let \( a \in A \setminus Z \); by (i), \([H, a] > [H, G, a] = [G, a, H] \). This implies \([G, A] \leq Z \) i.e. \( G = U \).

Furthermore, \(|H : A|=|H, a| = |AC_H(x) : A| = |A : C_A(x)| = |A| \). Let \( y \in G \setminus H \) with \([x, y] \notin Z \), and \( y \) is guaranteed to exist by the choice of \( x \).

As \([H, x] \leq Z \), the Three-Subgroups-Lemma says that \([x, y, H] = [y, H, x] \). As \(|[x, y, H]| = |[x, H]|\), we obtain \([x, H] = [y, H, x] = [x, y, H] \) and \( A = [y, H]C_A(x) = [y, H]Z \). Since \( G = U \), \( \overline{C} \leq \overline{A} = [\overline{y}, \overline{H}] \), whence \( \overline{C} = \overline{H}C_{\overline{G}}(\overline{y}) \). Suppose there are elements \( v \) of \( H \setminus A \) and \( w \) of \( G \setminus H \) with \([v, w] \in Z \).

Without loss, \([w, \overline{y}] \in Z \). Moreover, \([w, H, v] = [H, v, w] = [v, w, H] = 1 \), and, as \( G' \leq A \), (a) yields \([w, H] \leq C_A(v) \). Accordingly, \([x, y, w] = [x, y] = [y, w, x] = 1 \), contradicting (i).

Let \( s \in M \setminus A \) and \( t \in G \setminus H \). We have just seen that \([H, G, G] \leq Z \notin [s, t] \). Accordingly, \( s \) and \( t \) satisfy all the requirements placed on \( x \) and \( y \) in the above, and

\(|H : A| = |A : Z| \), and if \( t \in G \setminus H \), then
Let $D$ be the inverse image of $C_{\overline{G}}(\bar{y})$ in $G$. Let $|G : H| = p^r$ and let $D = \langle y_1, \ldots, y_r \rangle Z / Z$ with $y = y_1$.

Let $C = C_H(x)$, remembering that $\overline{C} \cong H / A$. It will be convenient to regard $\overline{C}$ and $D$ as vector spaces over $GF(p)$.

For $i = 1, \ldots, r$, let $\alpha_i : \overline{C} \to \overline{C}$ be defined by $[c, \bar{y}] = [\alpha_i(c), \bar{y}]$ ($\bar{c} \in \overline{C}$). By (2), the set $\{\alpha_1, \ldots, \alpha_r\}$ is $D$-independent. Let $h \in H$; then $C_{\overline{G}}(\bar{y}^h) = \langle \bar{y}_i \alpha_i(h) \mid i = 1, \ldots, r \rangle$. Let $E$ be the inverse image of $C_{\overline{G}}(\bar{y}^h)$ in $G$; then $E' \leq Z$, and, for $i, j \in \{1, \ldots, r\}$, we have $1 = \langle \bar{y}_i \alpha_i(h), \bar{y}_j \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle [\alpha_i(h), \bar{y}_j]$. Thus $\langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}, \alpha_j(h) \rangle$. By (ii), this implies that

For $i, j \in \{1, \ldots, r\}$, $\alpha_i \alpha_j = \alpha_j \alpha_i$.

Let the equivalence relation $\sim$ on $\overline{C}$ be defined by $\bar{v} \sim \bar{w}$ if $[v, A] = [w, A]$.

Let $\overline{C} \cong H / A$. It will be convenient to regard $\overline{C}$ and $D$ as vector spaces over $GF(p)$.

For $i = 1, \ldots, r$, let $\alpha_i : \overline{C} \to \overline{C}$ be defined by $[c, \bar{y}] = [\alpha_i(c), \bar{y}]$ ($\bar{c} \in \overline{C}$). By (2), the set $\{\alpha_1, \ldots, \alpha_r\}$ is $D$-independent. Let $h \in H$; then $C_{\overline{G}}(\bar{y}^h) = \langle \bar{y}_i \alpha_i(h) \mid i = 1, \ldots, r \rangle$. Let $E$ be the inverse image of $C_{\overline{G}}(\bar{y}^h)$ in $G$; then $E' \leq Z$, and, for $i, j \in \{1, \ldots, r\}$, we have $1 = \langle \bar{y}_i \alpha_i(h), \bar{y}_j \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle [\alpha_i(h), \bar{y}_j]$. Thus $\langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}_i, \alpha_j(h) \rangle = \langle \bar{y}, \alpha_j(h) \rangle$. By (ii), this implies that

For $i, j \in \{1, \ldots, r\}$, $\alpha_i \alpha_j = \alpha_j \alpha_i$.

Let $V_1$ and $V_2$ be subspaces of $\overline{C}$ such that $V_1^2$ and $V_2^2$ are distinct equivalence classes of $\sim$. Let $P = O_p(X)$ and $Q = O_{p'}(X)$. Let $U_1 \leq V_1$ and $U_2 \leq V_2$ be irreducible $Q$-submodules, and pick $u_1 \in U_1^2$, $u_2 \in U_2^2$. If $U_1$ and $U_2$ are inequivalent as $Q$-modules, then the smallest $Q$-submodule of $V$ containing $u_1 + u_2$ is $U_1 + U_2$. However, $u_1 + u_2$ belongs to an equivalence class of $\sim$ disjoint from both $U_1^2$ and $U_2^2$, so that is impossible. According to $U_1$ and $U_2$ are equivalent as $Q$-modules, and $\overline{C}$ splits into a direct sum of inequivalent irreducible $Q$-submodules. In particular, $Q$ is cyclic.

Next, suppose that $[U_1, P] = 0$ and that $W$ is an $X$-submodule of $V_2$ with $[W, P] \neq 0$. Letting $0 \neq u \in U_1$ and $w \in W \setminus CW(\beta)$ for some $\beta \in P$, we obtain $[\bar{u} + \bar{w}, \beta] = [\bar{w}, \beta] = \bar{u} + \bar{w};$ yet $[\bar{w}, \beta] \sim \bar{w}$, so that is not possible. Thus $P = 1$.

For $\gamma \in X$ and $c \in C$ pick $c_\gamma \in C$ with $\gamma(c) = c_\gamma$. Let $\beta \in X$, let $c, c' \in C \setminus Z$, and assume that $[c_\beta, y, c'] = [c'_\beta, y, c]$. Let $i \in \{1, \ldots, r\}$. Then $[c_{\alpha_i} y, c'] = [c_\beta, y_i, c'] = [c', y_i, c_\beta] = [c'_{\alpha_i}, y, c] = [c'_{\alpha_i}, y, c] = [c', y_i, c_\beta]$.

Via induction on the length of a word in the generators $\alpha_1, \ldots, \alpha_r$, we obtain $[c', y, c] = [c'_\gamma, y, c] (c, c' \in C, \gamma \in X)$.
Let $T = GF(p)[X]$; we have seen that there is $k \in \mathbb{N}$ such that (as a $GF(p)$-algebra) $T$ is isomorphic to $GF(p^k)$. Let $\phi : T \to GF(p^k)$ be an isomorphism of $GF(p)$-algebras and let $p^k = q$. Then $\overline{C}$ becomes a $GF(q)$-module via $\phi(\gamma)(\overline{c}) = \gamma \overline{c}$, $[\overline{C}, \overline{y}]$ can be made into a $GF(q)$-module via $\phi(\gamma)[\overline{c}, \overline{y}] = \overline{c} \overline{y}$ and $H'$ becomes a $GF(q)$-module via $\phi(\gamma)[c, y, c'] = [c, y, c']$ $(\gamma \in X, c, c' \in C)$.

Let $f : [\overline{C}, \overline{y}] \times \overline{C} \to H'$ be given by $f([\overline{c}, \overline{y}], c') = [c, y, c']$. Then (v) says that $f$ is a $GF(q)$-bilinear form.

By (iii), $\overline{C} = \overline{HCG}(\overline{y})$. Letting $D$ be the inverse image of $\overline{HCG}(\overline{y})$ in $G$, we have $D' \leq C_H(y) = Z$, which implies

$$[d', c, d'] = [d, c, d'] \quad (c \in C, d, d' \in D).$$

Now (v) shows that $H$ is isoclinic to a central quotient of $H(m, k)$. For $c \in C$ and $d \in D$, the map $c \mapsto [c, d]$ $(c \in C, d \in D)$ induces a derivation $\delta_d : \overline{C} \to H'$, and the map $d \mapsto \delta_d$ is a derivation from $\overline{D}$ into $Der(\overline{C}, A)$. This shows that $G$ is one of the groups described in part $a)$ of the proposition.

b) Now assume that $Ax \subseteq M$.

If $A \not\subseteq Z_{r+1}(G)$, then, as $A \subseteq M \cup Z$, there is $a \in A$ with $H = [H, A]G C_H(a) = A$, a contradiction. Hence, for $a \in A$, $H = M_x = M_{ax}$, and $[A, H] = [A, x]$ by 2.1. Since $|[A, x]| = |[H, x]|$, we obtain that for $v \in M \setminus A$ and $a \in A \setminus Z$, $[A, H] = [a, H] = [A, x] = [H, x]$. Letting $c \in C_G(x)$, either $\overline{c} \not\subseteq Z_{r+1}(G)$ and, since $c \in M$, $[H, c] = [A, c] = [A, x]$, or neither $\bar{x}$ nor $\bar{x}c$ belongs to $Z_{r}(G)$, and $[H, c] \leq [A, x][A, xc] = [A, x]$. Accordingly,

$$H' = [A, h] = [a, H].$$

If $x' \in H \setminus A$, then there are $c \in C_G(x)$ and $a \in A$ with $x' = ca$; by (*), there is $b \in A$ such that $[x, a] = [c, b]$, and $[xb, ca] = 1$. By assumption, $xb \in M$, whence $x' \in M$ and $H = M \cup Z$.

Let $V = \overline{H}$ and let $W$ be a maximal subgroup of $H'$. By (*), the map $(\bar{u}, \bar{v}) \mapsto [u, v]W$ $(u, v \in H)$ induces a $G$-invariant nondegenerate symplectic inner product $f$ on $V$, and $V$ will be regarded as a $GF(p)$-vector space equipped with $f$. We have $C_V(G) = [V, G]^{\perp}$ and $[V, G] = C_V(G)^{\perp}$. Let $\bar{u} \in C_V(G)$; by the Three-Subgroups Lemma, $[u, G'] = 1$, so

$$C_\ell' \leq [V, G].$$

Let $y, y' \in G \setminus H$ and let $\bar{h} \in C_V(y)$. Then $[h, y^{-1}, y']^y = 1$ and $[y, y'^{-1}, h]^y \in H'$, whence $[y', h, y] \in H'$. Let $b = [y, h]$ and assume that $b \not\subseteq Z$; by (*), $H' = [H, b]$; whence there is $x \in H \setminus Z$ with $[b, xy] = 1$, contradicting $b \in M$. Thus $C_V(y) = C_V(G)$, and, since $C_V(K') = [V, K]^{\perp}$ whenever $K \leq G$, this implies $[V, G] = [V, y]$. Thus $G' \leq [H, y]Z$, and therefore $G = \overline{HCG}(\overline{y})$.

By 2.3, $C_i(y) = C_i(G)$ for all $i$ (where $C_i(*))$ is defined as in 2.3), and, since $[V, K] = (C_i(K))^{\perp}$ for every $i$ and every $K \leq G$, we obtain

$$C_i(y) = C_i(G).$$

As $\overline{C}' \leq [V, y]$, and $[V_{p-1}(y)] = 1$ because of $\exp \overline{G} = p$, $cl(\overline{G}) \leq p + 1$.

We display a class of examples proving that the bound on the class is sharp and at the same time paving the way for remark 5.1 just below:

Let $\ell \in \mathbb{N}$ and let $q = p^\ell$. Let $K$ be the central product $E_1 \ast \ldots \ast E_{\ell-1}$, where each $E_i$ is isomorphic to a Sylow-$p$-subgroup of $U_3(q)$ (see 1.7) and let $H = K \times E$ where $E$ is elementary abelian of order $q$. 
The group $C_{Aut(K)}(K')$ is $Sp_{p-1}(q)$ acting on $K/K'$ as the symplectic space $V$ of dimension $p - 1$ over $GF(q)$, its defining module. Furthermore, there is $\tau \in Sp_{p-1}(q)$ such that $o(\tau) = p$ and $\langle \tau \rangle$ is uniserial on $V$. We let $\theta \in C_{Aut(H)}(K')$ be defined by $\theta_E = id$, $\theta_K = \tau$. Let $C_K(\theta) = K' \times D$ with $D$ elementary abelian of order $q$, and let $\psi : D \rightarrow E$ be an isomorphism. Let $L$ be a complement of $D$ in $K$. There is $\eta \in Aut(H)$ given by $\eta_{L \times E} = id$ and $\eta(v) = v\psi(v)$ ($v \in D$). Let $G = H \rtimes \langle \theta\eta \rangle$. Now $H$ is of conjugate rank 1, and, for $x \in G \setminus H$, we have $x^p \in E$ and $C_G(x) = \langle x \rangle EK' = \langle x \rangle Z(G)$, so $G$ is a CH-p-group of class $p + 1$.

Let $P$ be a finite p-group of class 2 with $\exp P = p$. In the proof of [1.3], it was shown that there is $q$ such that $P$ is isomorphic to a subgroup of a central quotient of $E_1$, so is isomorphic to a subgroup of a central quotient of $K$ and therefore also of $G$. Hence

**Remark 5.1.** Let $p$ be an odd prime and let $P$ be a finite p-group of class 2 and exponent $p$. Then there is a CH-p-group of the type described in [1.0 b) which has a subgroup isomorphic to $P$.

### 6. Proof of Proposition 1.9

Assume that $d(H) = 3$. We shall prove the statements following up "in particular" first and then use the information gathered to deduce that $G$ is isoclinic to $R(n)$. For $v \in M$, $C_G(v) \subseteq H \subseteq U$, so $|v^U|$ is independent of the particular choice of $v$. Let $|v^U| = p^b$, and let $D_v$ be the inverse image of $C_{\gamma}(\bar{v})$ in $G$.

Let $x$ and $y$ in $M$ with $[x, y] \notin Z$. Let $w \in U$; then $[x, y, w] = [x, w, y][w, y, x]$, whence $[U, [x, y]] \subseteq [U, y, x][U, x, y] \subseteq [D_x, x][D_y, y]$. Let $|U : D_x| = p^{n_1}$, and $|U : D_y| = p^{n_2}$. For $v \in M$, the map $t \mapsto [t, v]$, $(t \in D_v)$ is a homomorphism, so $|[D_v, v]| = |D_v : C_G(v)|$. Accordingly, $p^b \leq |[D_x, x][D_y, y]| = p^{2^{b-(n_1+n_2)}}$, and $b \geq n_1 + n_2$.

On the other hand, $[x, D_x \cap D_y, y] = 1 = [y, D_x \cap D_y, x]$, and $D_x \cap D_y \subseteq C_G([x, y])$ by the Three-Subgroups-Lemma. As $|G : D_x \cap D_y| = |G : D_x||D_y : D_x|\leq |G : D_x||D_y| = p^{n_1 + n_2}$, we obtain $b \leq n_1 + n_2$.

Accordingly, $b = n_1 + n_2$. This implies that

$$D_x D_y = G,$$  \hspace{1cm} (1)

$$[U, [x, y]] = [U, y, x] \times [U, x, y] = [A, x] \times [A, y] = [D_x, x] \times [D_y, y].$$  \hspace{1cm} (2)

Let $v \in M$; then $[D_v, v] = \{[d, v] | d \in D_v\}$, so (2) implies that, if $v, w \in M$ and $[\bar{v}, \bar{w}] \neq 1$, then

$$D_v = [U, w]C_G(v) = AC_G(v).$$  \hspace{1cm} (3)

Taken together, (1) and (3) yield $U = C_U(x)C_U(y)A = H$.

Assume $Ax \not\subseteq M$. Then $C_A(x) = Z$, and, by (3), $A = Z[U, y]$, implying $|A : Z| = p^{n_2}$. Accordingly, $Ay \subseteq y^U Z \subseteq M$. Since $x A \not\subseteq M$, we know that $[U, x]Z \neq A$, which forces $n_1 < n_2$. We also know that $D_y = D_{ay} = M_y = M_{ax} (a \in A)$ whence Lemma 2.1 says that $[A, D_y] = [A, y]$. Let $c \in D_x \cap D_y$. We have just seen that $[c, A] \leq [y, A]$, and, by the Three-Subgroups-Lemma, $[c, U, x] \subseteq [x, U, c] \leq [A, y] \cap [A, x] = 1$, so $[c, U] \leq Z$, and $c \in Z_2(U)$. Since $A = [U, y]Z = U'Z$, $Z_2(U) \leq C_U(A) = A$. So $D_x \cap D_y = A$.

From $D_x \cap D_y = A$ it follows that $|U : A| = |D_x D_y : D_x \cap D_y| = p^{n_1 + n_2} = p^b$ whence $C_U(a) = A$.
whenever \( a \in A \setminus Z \).

On the other hand, \( ||[U, \bar{g}]|| = p^{n_2} = |A : Z| \), and \( ||[A, y]|| = p^{n_1} < p^{n_2} \). So there is \( a \in C_A(y) \setminus Z \), a contradiction. Accordingly,

\[
D_x \cap D_y = A = C_U(a)\ 
\text{whence}\ 
\text{whenver} \ a \in A \setminus Z. \tag{5}
\]

Let \( a, g \in G \), and \( u \in U \). Then \( [a, g, u][g^{-1}, u^{-1}, a] = 1 \), whence \( [a, g, U] \leq [G, U, a] \). Since \( C_U(a) = A \), and \( [G, U]A \leq U \), this implies \( [a, g, U] \leq [a, U] \) and \( A, G \leq Z \), i.e. \( G = U = H \).

By (1), (3) and (5), \( |D_v : A| = |C_G(v) : C_A(v)| = |G| \) whenever \( v \in \mathcal{M} \). By (2), \( |G : D_x| = p^{n_1} = |D_x : D_x \cap D_y| \), which implies \( n_1 = n_2 \). Let \( n_1 = n \).

Let \( x \in G \setminus A \). By (5), \( [A : C_A(t)] = |[A, t]| = |A : Z| \); in particular, \( |[A, x]| = |[A, t]| \). By (5), \( Z_2(G) \leq A \), so, by (1), \( \overline{A} = \overline{G}, \bar{v} \) for every \( v \in \mathcal{M} \setminus A \). Lastly, let \( c, d \in (D_x \cap \mathcal{M}) \setminus A \). By (4) and 2.1 \( [D_c, A] = [c, A] = [x, A] = [d, A] = [D_d, A] \). If \( [c, \bar{d}] \neq 1 \), then, by (2), \( G = D_cD_d \), whence \( [G, A] = [x, A] \), a contradiction. So \( D_c = D_x \) whenever \( c \in (D_x \cap \mathcal{M}) \setminus A \). Let \( t \in G \setminus A \); since \( t \notin Z_2(G) \), we may assume that \( [\bar{t}, \bar{x}] \neq 1 \). As we have just seen, this implies \( [t, c] \notin Z \) for \( c \in D_x \setminus A \), so that \( [\bar{t}, \overline{G}] = \overline{A} \). So \( \overline{G} \) is ultraspecial of order \( p^{3n} \).

Let \( V = A \), let \( X = D_x / A \), and let \( Y = D_y / A \). We regard \( X, Y \), and \( V \) as vector spaces over \( GF(p) \).

If \( v, w \in G \), then \( [v^p, w, v] = [v^p, w, v] = 1 \), implying \( [v^p, w] = [v, w]p^3[v, w] = 0 \). Accordingly, \( G' \) is elementary abelian, and, as \( A = [G, x]Z, Z \) has an elementary abelian complement \( B \) in \( A \). For \( v \in D_x \) and \( w \in D_y \), let \( h(v, w) \) be the image of \( [v, w] \) under the projection onto \( B \).

Let \( D_x = \langle x_1, \ldots, x_n \rangle A = \langle x_1 \rangle A \). Regarding \( D_y / A \) as a \( GF(p) \)-vector space, define the linear transformation \( \alpha_i : D_y / A \to D_y / A \) by the rule: \( \alpha_i(wA) = w'A \) if and only if \( h(x_i, w) = h(x, w') \) (\( w \in Y, i = 1, \ldots, n \)). If \( \lambda_1, \ldots, \lambda_n \in GF(p) \), \( w \in D_y \), and \( w' A = (\lambda_1 \alpha_1 + \ldots + \lambda_n \alpha_n) w A \), then \( h(x_1, w') = h(x_1^{\lambda_1} \ldots x_n^{\lambda_n}) \), which implies that the set \( \{\alpha_1, \ldots, \alpha_n\} \) is \( D \)-independent.

Let \( i, j \in \{1, \ldots, n\} \) and \( w \in D_y \). Let \( w_i A = \alpha_i(wA), w_j A = \alpha_j(wA), w' A = \alpha_i \alpha_j(wA) \) and \( w'' A = \alpha_j \alpha_i w A \).

Then \( [w, x_i, x_j] = [w_1, x_1, x_j] = [w_i, x_j, x_1] = [w''x_1, x_1] = [w, x_j, x_i] = [w', x_1, x_1] \). As the map \( Y \to |A, x| \) given by \( w \mapsto [x_1, w, x_1] (w \in Y) \) is a bijection, we have \( \alpha_i \alpha_j = \alpha_j \alpha_i \).

Accordingly, Lemma 2.2 becomes applicable to the set \( \{\alpha_1, \ldots, \alpha_n\} \), and there is a Singer cycle \( \sigma \in GL_n(p) \) such that each \( \alpha_i \) is a power of \( \sigma \). Observe that \( \alpha_1 = id \) by definition.

For \( i = 1, \ldots, n \), let \( y_i \) be such that \( y_i A = \alpha_i(yA) \). Then \( D_y = \langle y_1, \ldots, y_n \rangle A \). Let \( i, j \in \{1, \ldots, n\} \) and \( \alpha_i \alpha_j(yA) = y' \). Then, as \( y' A = \alpha_j \alpha_i(yA) \), \( h(x_i, y_j) = h(x, y') = h(x_j, y_i) \). \( \tag{6} \)

Let \( \alpha_i = \sigma^{k_i} \) (\( i = 1, \ldots, n \)). By 2.2, there is a generator \( \lambda \) of \( GF(q)^* \) such that there are linear bijections \( \varphi_2 : GF(q^+) \to D_y / A \) and \( \varphi_1 : GF(p^n, +) \to D_x / A \) defined by \( \psi(\lambda^{k_i}) = y_i A \) and \( \varphi(\lambda^{k_i}) = x_i A \) (\( i = 1, \ldots, n \)). For every \( \mu \in GF(q) \), pick elements \( y(\mu) \) of \( \varphi_2(\mu) \) and \( x(\mu) \) of \( \varphi_1(\mu) \). Define the linear bijection \( \rho : GF(p^n, +) \to B \) by \( \rho(\mu) = h(x, y(\mu)) (\mu \in GF(q)) \). If \( i, j \in \{1, \ldots, n\} \), then
(6) translates to: \( h(x(\lambda^i), y(\lambda^j)) = h(x, y(\lambda^i + \lambda^j)) = h(x(\lambda^i), y(\lambda^j)) \). By the bilinearity of \( h \) (properties (e) and (f) in [1,8 2]) and the fact that the powers \( \lambda^i, i = 1, \ldots, n, \) form a basis of \( (GF(q), +) \), (see [2.2]), we obtain
\[
g(-\mu\mu') = h(y(\mu\mu'), x) = h(y(x(\mu\mu')) = h(y(\mu), x(\mu')) = h(y(\mu'), x(\mu)).
\]
Let \( g_1 : A \times D_x \rightarrow [A, x] = E_1 \) and \( g_2 : A \times D_y \rightarrow [A, y] = E_2 \), be given by \( (a, v) \mapsto [a, v] (a \in A, v \in D_x \cup D_y) \). Observe that \( g_1, g_2 \) satisfy the requirements of [1,8 (a), (b), and (f)]. Let \( P_1 = D_x / A, P_2 = D_y / A \). Let \( \psi_1 : GF(q) \rightarrow E_1, \psi_2 : GF(q) \rightarrow E_2 \), be given by \( \psi_1(\mu) = [y(\mu), x, x], \psi_2(\mu) = \) \( \) \( [y, x(\mu), y]. \) Let \( a \in A, \mu \in GF(q), \kappa = \rho^{-1}\pi(a); \) then \( \psi_1(\kappa\mu) = [y(\kappa\mu), x, x] = [y(\kappa), x, x(\mu)] = [a, x(\mu)] = g_1(a, \varphi_1(\mu)), \) and, analogously, \( \psi_2(\kappa\mu) = [y(\kappa\mu), x, y] = [y(\kappa), x, y(\mu)] = g_2(a, \varphi_2(\mu)). \) This shows that \( G \) is isoclinic to \( R(n) \), and the proof is complete.

We conclude the paper by a remark on \( CH-p \)-and \( CA \)-groups. In [2], the authors provide examples showing that \( CA \subset CH \). It might therefore be interesting to note that, if \( G \) is a \( CH-p \)-group and not of class 2 or one of the groups in part \( b \) of [1,6], \( G \) must be isoclinic to a \( CA \)-group. If \( \ell > 2 \) and \( H = E_1 \ast \ast E_\ell \) where each \( E_i \) isomorphic to a Sylow-\( p \)-subgroup of \( U_3(q) \) for some \( p \)-power \( q \), then \( H \) is \( CH \) but not \( CA \).

References


Bettina Wilkens
Department of Mathematics, University of Botswana, Private Bag 00704, Gaborone, Botswana
Email: wilkensb@mopipi.ub.bw