Federico Menegazzo

On index preserving projectivities of finite groups


<http://www.numdam.org/item?id=RSMUP_1974__52__227_0>
On Index Preserving Projectivities of Finite Groups.

FEDERICO MENEGAZZO (*)

If $G$ is a group, a projectivity of $G$ is an isomorphism of the lattice $\mathcal{L}(G)$ of subgroups of $G$ onto the lattice $\mathcal{L}(H)$ of subgroups of a group $H$; the projectivity $\sigma: G \to H$ is index preserving if $|U^\sigma: V^\sigma| = |U: V|$ for every pair $U > V$ of subgroups of $G$. As a motivation for this research one might look at these well known facts: if $G$ is finite simple (non abelian) then every projectivity of $G$ is index preserving; if $A$ is an abelian subgroup of the group $G$, $A^\sigma$ may be non abelian (thus projectivities, generally speaking, do not preserve centres nor centralizers) [3]. In this paper the following problem is investigated: let $P$ be a $p$-Sylow subgroup of $G$, $\sigma: G \to H$ an index preserving projectivity; under which assumptions can we assert that $\sigma$ sends the centre of $P$ into a central subgroup of $P^\sigma$? We prove that if $P^\sigma$ is not centralized by the image of the centre of $P$, and if $G$ is either $p$-normal or $p$-soluble, then $G$ has a proper normal subgroup $K$ such that $G/K$ is a $p$-group.

The notation is standard; by « group » we shall mean « finite group ».

1. This section includes some introductory results and remarks.

LEMMA 1.1. Let $A$ and $B$ be subgroups of $G$, $\sigma: G \to G^\sigma$ an index preserving projectivity, and assume that $A$ is generated by its $p$-elements, while $B = O_p^p(B)$. If $B \triangleleft N_p^g(A)$, then $B^\sigma \triangleleft N_{g^\sigma}^g(A^\sigma)$; if $B \triangleleft C_g^g(A)$, then $B^\sigma \triangleleft C_{g^\sigma}^g(A^\sigma)$. (Here, and in the rest of the paper, if $X$ (*) Indirizzo dell’A.: Seminario Matematico dell’Università di Padova. Lavoro eseguito nell’ambito dei gruppi di ricerca afferenti al Comitato per la matematica del C.N.R.
is any group, \( O^p(X) \) denotes the subgroup of \( X \) generated by all the elements in \( X \) whose orders are prime to \( p \).

**Proof.** Let \( x \) be any element of \( B \) with \( p \nmid |x| \); every \( p \)-element of \( A \triangleleft \langle x \rangle \) is in \( A \), i.e. \( A \) is the union of the cyclic subgroups of \( A \triangleleft \langle x \rangle \) whose orders are a power of \( p \). Since \( \sigma \) is index preserving, \( A^\sigma \) is the union of the cyclic subgroups of \( (A \triangleleft \langle x \rangle)^\sigma \) whose orders are a power of \( p \), so \( A^\sigma \leq (A \triangleleft \langle x \rangle)^\sigma \); as \( x \) describes all the elements of \( B \) whose orders are prime to \( p \) we get \( B^\sigma \leq N^\sigma_{\sigma}(A) \). If furthermore \( B \leq C^\sigma_{\sigma}(A) \), for every element \( x \) of \( A \) such that \( p \nmid |x| \) and for every \( p \)-element \( y \) of \( A \) \( \langle x \rangle \triangleleft \langle y \rangle = \langle x \rangle \times \langle y \rangle \) where the decomposition is both group- and lattice-theoretical; it follows that \( \langle x, y \rangle^\sigma = \langle x \rangle^\sigma \times \langle y \rangle^\sigma \). Letting \( x, y \) describe all the elements of \( B \) with an order prime to \( p \) and all the \( p \)-elements of \( A \) respectively, we get \( [A^\sigma, B^\sigma] = 1 \).

**Lemma 1.2.** Let \( P \) be a \( p \)-Sylow subgroup of \( G \), \( Q \) a complement of \( P \) in \( N^\sigma_{\sigma}(P) \). If \( \sigma : G \rightarrow G^\sigma \) is an index preserving projectivity, then \( P^\sigma \) is a \( p \)-Sylow subgroup of \( G^\sigma \), \( N^\sigma_{\sigma}(P^\sigma) = N^\sigma_{\sigma}(P) = P^\sigma Q^\sigma \). Letting \( x, y \) describe all the elements of \( B \) with an order prime to \( p \) and all the \( p \)-elements of \( A \) respectively, we get \( [A^\sigma, B^\sigma] = 1 \).

**Proof.** The only thing to prove is that \( [P, Q] = [P^\sigma, Q^\sigma] \). \( [P, Q] \) is the intersection of \( P \) with the same is true for \( [P^\sigma, Q^\sigma] \) and the equality follows.

**Lemma 1.3.** Let \( G \) be a non-abelian non-Hamiltonian modular \( p \)-group. \( G \) has a maximum subgroup \( M \) which is characteristic and such that either \( [G, \text{Aut } G] \leq M \) or \( \Phi(G)[M, \text{Aut } G] \leq M \).

**Proof.** Let \( G \) be a counterexample of least possible order. Every non-trivial characteristic subgroup \( H \) of \( G \) which is contained in \( \Phi(G) \) contains \( G' \); thus, should \( G/H \) be non-abelian, by the minimality of \( G \) there would exist a maximum subgroup \( M \) of \( G \), characteristic and such that either \( [G/H, \text{Aut } G/H] \leq M/H \) (in which case \( [G, \text{Aut } G] \leq M \) would follow) or

\[
\Phi(G/H)[M/H, \text{Aut } G/H] \leq M/H ,
\]

i.e. \( \Phi(G)[M, \text{Aut } G] \leq M \). In particular \( G' \cap \Omega_1(Z(G)) \geq G' \), i.e. \( G' \leq \Omega_1(Z(G)) \). So \( G = A \langle b \rangle \) with \( A \) abelian, \( a^{\exp A} = a^{1+\epsilon} \) for every \( a \in A \), \( \exp A = p^{\epsilon+1} \), \( p^\epsilon > 2 \). We now prove that we may choose \( A, b \) such that \( |b| < \exp A \); thus, if \( |b| > p^{\epsilon+1} \), then \( 1 \neq \langle ab \rangle^{p^{\epsilon+1}} \), \( a \in A \) \( = \langle b^{p^{\epsilon+1}} \rangle = \langle b \rangle^\epsilon \langle b \rangle \). Letting \( b \) describe all the elements of \( B \) with a power prime to \( p \) and all the \( p \)-elements of \( A \) respectively, we get \( [A^\epsilon, B^\epsilon] = 1 \).

**Proof.** The only thing to prove is that \( [P, Q] = [P^\sigma, Q^\sigma] \). \( [P, Q] \) is the intersection of \( P \) with the same is true for \( [P^\sigma, Q^\sigma] \) and the equality follows.

**Lemma 1.3.** Let \( G \) be a non-abelian non-Hamiltonian modular \( p \)-group. \( G \) has a maximum subgroup \( M \) which is characteristic and such that either \( [G, \text{Aut } G] \leq M \) or \( \Phi(G)[M, \text{Aut } G] \leq M \).

**Proof.** Let \( G \) be a counterexample of least possible order. Every non-trivial characteristic subgroup \( H \) of \( G \) which is contained in \( \Phi(G) \) contains \( G' \); thus, should \( G/H \) be non-abelian, by the minimality of \( G \) there would exist a maximum subgroup \( M \) of \( G \), characteristic and such that either \( [G/H, \text{Aut } G/H] \leq M/H \) (in which case \( [G, \text{Aut } G] \leq M \) would follow) or

\[
\Phi(G/H)[M/H, \text{Aut } G/H] \leq M/H ,
\]

i.e. \( \Phi(G)[M, \text{Aut } G] \leq M \). In particular \( G' \cap \Omega_1(Z(G)) \geq G' \), i.e. \( G' \leq \Omega_1(Z(G)) \). So \( G = A \langle b \rangle \) with \( A \) abelian, \( a^{\exp A} = a^{1+\epsilon} \) for every \( a \in A \), \( \exp A = p^{\epsilon+1} \), \( p^\epsilon > 2 \). We now prove that we may choose \( A, b \) such that \( |b| < \exp A \); thus, if \( |b| > p^{\epsilon+1} \), then \( 1 \neq \langle ab \rangle^{p^{\epsilon+1}} \), \( a \in A \) \( = \langle b^{p^{\epsilon+1}} \rangle = \langle b \rangle^\epsilon \langle b \rangle \). Letting \( b \) describe all the elements of \( B \) with a power prime to \( p \) and all the \( p \)-elements of \( A \) respectively, we get \( [A^\epsilon, B^\epsilon] = 1 \).

**Proof.** The only thing to prove is that \( [P, Q] = [P^\sigma, Q^\sigma] \). \( [P, Q] \) is the intersection of \( P \) with the same is true for \( [P^\sigma, Q^\sigma] \) and the equality follows.

**Lemma 1.3.** Let \( G \) be a non-abelian non-Hamiltonian modular \( p \)-group. \( G \) has a maximum subgroup \( M \) which is characteristic and such that either \( [G, \text{Aut } G] \leq M \) or \( \Phi(G)[M, \text{Aut } G] \leq M \).

**Proof.** Let \( G \) be a counterexample of least possible order. Every non-trivial characteristic subgroup \( H \) of \( G \) which is contained in \( \Phi(G) \) contains \( G' \); thus, should \( G/H \) be non-abelian, by the minimality of \( G \) there would exist a maximum subgroup \( M \) of \( G \), characteristic and such that either \( [G/H, \text{Aut } G/H] \leq M/H \) (in which case \( [G, \text{Aut } G] \leq M \) would follow) or

\[
\Phi(G/H)[M/H, \text{Aut } G/H] \leq M/H ,
\]

i.e. \( \Phi(G)[M, \text{Aut } G] \leq M \). In particular \( G' \cap \Omega_1(Z(G)) \geq G' \), i.e. \( G' \leq \Omega_1(Z(G)) \). So \( G = A \langle b \rangle \) with \( A \) abelian, \( a^{\exp A} = a^{1+\epsilon} \) for every \( a \in A \), \( \exp A = p^{\epsilon+1} \), \( p^\epsilon > 2 \). We now prove that we may choose \( A, b \) such that \( |b| < \exp A \); thus, if \( |b| > p^{\epsilon+1} \), then \( 1 \neq \langle ab \rangle^{p^{\epsilon+1}} \), \( a \in A \) \( = \langle b^{p^{\epsilon+1}} \rangle = \langle b \rangle^\epsilon \langle b \rangle \). Letting \( b \) describe all the elements of \( B \) with a power prime to \( p \) and all the \( p \)-elements of \( A \) respectively, we get \( [A^\epsilon, B^\epsilon] = 1 \).
other hand $G' = [A, b] = \mathcal{O}_t(A)$, so $A = \langle t \rangle \times U$ with $\exp U < p^t$, $|t| = p^{r+1}$; $V = U \langle b \rangle$ is now abelian, and $t$ normalizes every cyclic subgroup of $V$, because if $i \equiv 0 \pmod{p}$, $[ub^i, t] = 1$ and if $i \not\equiv 0 \pmod{p}$, $[ub^i, t] = [b^i, t] \in \langle b^{2ri} \rangle = \langle ub^i \rangle = \langle ub \rangle$; hence $t$ induces on $V$ a power automorphism, and a suitable generator of $\langle t \rangle$ induces exactly the power $1 + p^r$ for some $r$; since $\exp V > p^2$, we get $p^r > 2$, and $V$, $t$ satisfy the condition we asked for. Put $M = A \langle b^p \rangle$; $M$ is a maximum subgroup of $G$, and $M$ is abelian. Remark that for every $x = ab^{ip} \in M$, $x^* = a^x$, so $x^* = a^{1+p^t} b^{ip} = x a^p = a^{1+p^t} b^{ip}$. If $M$ is a characteristic subgroup of $G$, then for every $x \in M$, $\alpha \in \text{Aut } G$, $G(x^\alpha) = (x^\alpha)^p = (x^{1+p^t})^{\alpha} = (x^{1+p^t})^{\alpha} = (x^p)^\alpha$, i.e. $[b, \alpha] \in C_0(M) = M$; and $[G, \text{Aut } G] \subseteq M$. If $M$ is not characteristic in $G$, then $|G[Z(G)]| = p^2$, $\Phi(G) < Z(G)$, and since $Z(G) = \mathcal{O}_t(A)/\langle b \rangle$, $Z(G) < AZ(G) = M < G$, we get $|A : \mathcal{O}_t(A)| = p$, i.e. $A = \langle u \rangle \times V$ with $p^r > \exp V$, $p^{r+1} = |u|$. We prove next that under these assumptions we can choose $b$ such that $|b| < \exp A$. Thus, assume there is no $g \in Ab$ with $|g| < p^t$; it follows $\langle u \rangle \times \langle b \rangle = 1$, since otherwise $1 \neq b^p = u^p a^p$, and $\langle u^{-1} b \rangle = 1$, contradicting the former assumption, for a suitable $i \equiv 0 \pmod{p}$; hence $\langle u \rangle \times \langle b \rangle = 1$ for every integer $k$. But we have so proved that $M$ is the only maximum subgroup of $G$ containing $Z(G)$ all whose subgroups are normal in $G$; hence $M$ is characteristic, against a former assumption: thus, if $Z(G) < N < G$, $N \not\subseteq M$, $N/Z(G) = \langle u^k b Z(G) \rangle$ with $k$ a suitable integer, and since $[u^k b, u] = [b, u] = u^{-p^t} \not\subseteq \langle u^k b \rangle$ $N$ contains $\langle u^k b \rangle$ which is not normal in $G$. So assume we chose $b$ such that $|b| < p^t$; for every $x \in G$, $x = ab^i$, $x^* = (ab^i)^p = a^{p^t}$, $x^* = a^{1+p^t} b^i = a^{1+p^t} x = a^{1+p^t} x$; $b$ induces on $G$ a homogeneous power automorphism, hence $[b, \text{Aut } G] < Z(G)$. Furthermore $\mathcal{O}_t(G) = \langle \mathcal{O}_t, V, b \rangle = Z(G)/\langle b \rangle$, $|G : \mathcal{O}_t(G)| = |\mathcal{O}_t(G) : Z(G)| = p$, and eventually $\Phi(G)[\mathcal{O}_t(G), \text{Aut } G] = \Phi(G)[Z(G)/\langle b \rangle, \text{Aut } G] < Z(G)$, q.e.d.

**Remark.** Lemma 1.3 is in some way a refinement of a result in [2] which would however be enough for the needs of this paper.

**Lemma 1.4.** Let $A < G$ be an abelian $p$-group, $Q < N'_G(A)$, $p \not\mid |Q|$. If $\sigma : G \to G^\sigma$ is an index-preserving projectivity, then $A^\sigma = [A^\sigma, Q^\sigma] \times \times C_{A^\sigma}(Q^\sigma)$, and $[A^\sigma, Q^\sigma]$ is in the centre of $A^\sigma$.

**Proof.** Put $H = O^p(AQ)$; then $H^\sigma = O^p(A^\sigma Q^\sigma)$. $[A^\sigma, Q^\sigma] = [A, Q]^\sigma = (A \wedge H)^{\sigma} = A^\sigma \wedge H^\sigma \subseteq A^\sigma Q^\sigma$; $C_{A^\sigma}(Q^\sigma) = C_A(Q) = C_A(H) = C_{A^\sigma}(H^\sigma) \subseteq A^\sigma Q^\sigma$; so $A^\sigma = ([A, Q] \times C_A(Q))^{\sigma} = [A^\sigma, Q^\sigma] \times C_{A^\sigma}(Q^\sigma)$. Moreover $[A^\sigma, Q^\sigma, Q^\sigma]$ =
\[ [A, Q, Q]^v = [A, Q]^v = [A^v, Q^v] \]: by lemma 1.3, since \([A^v, Q^v]\) is a modular non-Hamiltonian \(p\)-group, \([A^v, Q^v]\) is abelian, q.e.d.

**Corollary 1.5.** Let \(A\) be a 2-generator abelian \(p\)-subgroup of \(G\), \(\sigma : G \to G^v\) an index-preserving projectivity. If \(A^v\) is not abelian, then \(\mathcal{N}_\sigma(A) / C_\sigma(A)\) is a \(p\)-group.

**Proof.** Let \(Q\) be a subgroup of \(\mathcal{N}_\sigma(A)\) such that \(p \mid |Q|\). \(A^v\) is a 2-generator modular non-abelian non-Hamiltonian \(p\)-group, so \(A^v\) is not directly decomposable; by 1.4 \([A^v, Q^v] < A^v\), whence \([A^v, Q^v] = 1 = [A, Q]\), q.e.d.

**Remark 1.6.** The hypothesis on the number of generators of \(A\) in 1.5 cannot be dispensed with, as the following example shows. We first look at the groups

\[ H = \langle a, b | a^p = b^q = 1, a^b = a^r, \exists r \neq 1, r^q = 1 \pmod{p} \rangle \]

where \(p, q\) are prime numbers, \(p \equiv 1 \pmod{q}\); \(K = \langle e, d | e^p = d^q = 1, [e, d] = 1 \rangle\); \(L = \langle e, f | e^p = f^q = 1, e' = e^{1+p} \rangle\). For every element \(he^xf^y\) of \(H \times L\) (\(h \in H\); \(x, y\) integers) put \((he^xf^y)^x = he^x \bar{d}^y \in H \times K\); since \(he^xf^y = h' e^{x'} \bar{d}^{y'} (h, h' \in H; x, x', y, y'\) integers) if and only if \(he^x \bar{d}^y = h' e^{x'} \bar{d}^{y'}\), \(\tau\) is a well defined bijection of \(H \times L\) onto \(H \times K\). Moreover if \(he^xf^y, h' e^{x'} \bar{d}^{y'} \in H \times L\), with \([e^x, f^y] = e^{p\alpha(x', y)}\), we get

\[
((he^xf^y)(h' e^{x'} \bar{d}^{y'}))^x = hh' e^{x+x'+p\alpha(x', y)} \bar{d}^{y+y'} \in \langle he^xf^y \rangle^x, (h' e^{x'} \bar{d}^{y'})^y = \\
= \langle he^x \bar{d}^y, h' e^{x'} \bar{d}^{y'} \rangle ;
\]

in fact, this is true if and only if \(e^{p\alpha(x', y)} \in \langle he^x \bar{d}^y, h' e^{x'} \bar{d}^{y'} \rangle\), but if \(x' \equiv 0 \pmod{p}\), then \(\alpha(x', y) \equiv 0 \pmod{p}\) and \(e^{p\alpha(x', y)} = 1\), whereas if \(x' \not\equiv 0 \pmod{p}\)

\[
e^{p\alpha(x', y)} \in \langle e^p \rangle = \langle e^{p\alpha} \rangle = \langle (h' e^{x'} \bar{d}^{y'})^{pq} \rangle < \langle he^x \bar{d}^y, h' e^{x'} \bar{d}^{y'} \rangle .
\]

So \(\tau\) induces a bijection of \(\mathcal{L}(H \times L)\) onto \(\mathcal{L}(H \times K)\) which clearly is an index-preserving projectivity. Now put \(\sigma = \tau^{-1}\), \(G = H \times K\), \(A = \langle a \rangle \times K\); \(A\) is a 3-generator abelian \(p\)-subgroup of \(G\), \(A^v = \langle a \rangle \times L\) is no longer abelian, but \(\mathcal{N}_\sigma(A) / C_\sigma(A) = G / A \cong \langle b \rangle\) has order \(q\).

2. The following lemma is the crucial step in the proof of the results of this paper.
LEMMA 2.1. Let $P$ be a $p$-Sylow subgroup of the group $G$, $Z$ a normal subgroup of $G$ contained in the centre of $P$, $\sigma : G \to G^\sigma$ an index-preserving projectivity. If $G = O_p(G)$, then $Z^\sigma$ is in the centre of $P^\sigma$.

PROOF. Let $G$ be a counterexample of least possible order. Since $G^\sigma = O_p(G^\sigma)$ lemma 1.1 implies $Z^\sigma \leq G^\sigma$; moreover if $A$, $B$ are normal subgroups of $G$ contained in $Z$ such that $A \wedge B = 1$, then $A^\sigma$ and $B^\sigma$ are both normal in $G^\sigma$ and if both are non-trivial by the minimality of $G$ $[P^\sigma, Z^\sigma] \leq A^\sigma \cap B^\sigma = 1$, i.e. $Z^\sigma$ would be in the centre of $P^\sigma$, contradicting our choice of $G$; so our assumptions imply that either $A$ or $B$ is trivial. Should $Z$ be in the centre of $G$, then by 1.1 $Z^\sigma$ would be in the centre of $G^\sigma$; hence $G/C_{G^\sigma}(Z) \neq 1$. As $(p, |G/C_{G^\sigma}(Z)|) = 1$ $Z = [Z, G] \times C_{G^\sigma}(Z)$; both factors are normal subgroups of $G$, $C_{G^\sigma}(G) \neq Z$ and by what we have just pointed out $Z = [Z, G]$, $C_{G^\sigma}(G) = 1$. We can now prove that $Z^\sigma$ is abelian: since otherwise for every $h \in G^\sigma$ such that $(|h|, p) = 1$ by 1.4 $Z^\sigma = [Z^\sigma, \langle h \rangle] \times C_{G^\sigma}(h)$ with abelian $[Z^\sigma, \langle h \rangle]$, whence $C_{G^\sigma}(h) > (Z^\sigma)^\prime$; $G^\sigma = O_p(G^\sigma)$, so $(Z^\sigma)^\prime$ would be in the centre of $G^\sigma$ contradicting an earlier statement. Call $L$ the subgroup of $G$ generated by its $p$-elements, $M = O_p(L)$. Then $[L, Z] = 1$; in particular $M < C_{G^\sigma}(Z)$ and by 1.1 $M^\sigma < C_{G^\sigma}(Z)$, and since $L = PM$, $L^\sigma = P^\sigma M^\sigma$, then $L^\sigma/C_{G^\sigma}(Z^\sigma)$ is a $p$-group. It follows that $C_{G^\sigma}(L^\sigma) \neq 1$ and in particular the intersection $T^\sigma$ of $\Omega_1(Z^\sigma)$ with the centre of $L^\sigma$ is a non-trivial normal subgroup of $G^\sigma$; $T^\sigma$ is a $p$-group, $G^\sigma = O_p(G^\sigma)$, so by 1.1 $T \leq G$. $|G/C_{G^\sigma}(\Omega_1(Z^\sigma))|$ is not divisible by $p$, hence $T$ has a complement $S$ in $\Omega_1(Z^\sigma)$ which is normal in $G$; an earlier remark shows $T = \Omega_1(Z^\sigma)$, i.e. $\Omega_1(Z^\sigma)$ is contained in the centre of $P^\sigma$ and of every conjugate of $P^\sigma$. Therefore $p^\sigma = \exp Z > p$; the minimality of $G$ then implies $[P^\sigma, Z^\sigma] < \Omega_1(Z^\sigma)$, $[\Phi(P^\sigma), Z^\sigma] = [P^\sigma, \Phi(Z^\sigma)] = 1$ (for every group $\Phi(X) = Frattini subgroup of X$). Define $G^* = G^\sigma/M^\sigma$, $\tilde{G} = G^\sigma/C_{G^\sigma}(Z^\sigma)$ (for every $x \in G^\sigma$, $x^* = xM^\sigma$ and $\tilde{x} = xC_{G^\sigma}(Z^\sigma)$); $\tilde{G}$ is isomorphic to a quotient group of $G^\sigma$. Since $L^\sigma = P^\sigma M^\sigma < G^\sigma$, the $p$-Sylow subgroup $P^* = P^\sigma M^\sigma/M^\sigma$ of $G^*$ is normal in $G^*$, and $\tilde{P} = P^\sigma C_{G^\sigma}(Z^\sigma)/C_{G^\sigma}(Z^\sigma) \leq \tilde{G}$; $\tilde{P} \neq 1$ by our choice of $G$; let $Q^*$, $\tilde{Q}$ be complements of $P^*$, $\tilde{P}$ in $G^*$, $\tilde{G}$ respectively. Since $G^* = O_p(G^*)$ and $\tilde{G} = O_p(\tilde{G})$, it follows that $P^* = [P^*, Q^*]$, $\tilde{P} = [\tilde{P}, \tilde{Q}]$; moreover if $H^* = H^\sigma/M^\sigma$ is a proper subgroup of $Q^*$ then $[P^*, H^*] \neq P^*$, since otherwise $O_p(P \cap H) = P \cap H < H$ would imply, by the minimality of $G$, $[Z^\sigma, P^\sigma] = 1$; from

$[\Phi(P^\sigma), Z^\sigma] = 1$
follows that $\bar{P}$ is elementary abelian. $Q^*$ and $Q$ both operate in a natural way on $\Omega_1(Z^\sigma)$ and $G^* = Q^* C_{\sigma}(\Omega_1(Z^\sigma))$, $\bar{G} = \bar{Q} C_{\sigma}(\Omega_1(Z^\sigma))$, so $\Omega_1(Z^\sigma)$ is both $Q^*$- and $\bar{Q}$-irreducible; thus, if $\Omega_1(Z^\sigma) = A^\sigma \times B^\sigma$ with $Q^*$ (or $\bar{Q}$-) invariant $A^\sigma, B^\sigma$, then $A^\sigma, B^\sigma$ are normal $p$-subgroups of $G^\sigma$, whence $A, B$ are normal subgroups of $G$ with trivial intersection both contained in $Z$; an earlier remark implies that one of them is trivial. In particular $\bar{G}_{n-1}(Z^\sigma) = \Omega_1(Z^\sigma)$, i.e. $Z$ is a direct product of cyclic groups of the same order $p^n$. Choose now $a \in P^\sigma$, and assume $a$ induces a power automorphism on $Z^\sigma$; then $\bar{a}$ is in the centre of $\bar{G}$ and, as $C_{\sigma}(\bar{Q}) = 1$, $\bar{a} = 1$: i.e. if an element of $P^\sigma$ induces a power automorphism on $Z^\sigma$, then it centralizes $Z^\sigma$; in particular $Z$ cannot be cyclic. We shall now prove that $Q^*$ (and of course $Q$) is a cyclic $q$-group for some prime $q \neq p$; so assume, by way of contradiction, that there is a family $\{h_i^*\}_{i \in I}$ of elements of $Q^*$ such that $\langle h_i^* \rangle < Q^*$ for every $i$, while $\langle h_i^* \rangle \neq Q^*$. By an earlier remark $[P^* , h_i^*] < P^*$, and, if $h_i^* = h_i M^\sigma$ with $(|h_i|, p) = 1$, $O^\sigma([P^* , h_i^*] M^\sigma \langle h_i^* \rangle) = [P^*, h_i^*] M^\sigma \langle h_i^* \rangle \neq G^\sigma$, which implies, by our choice of $\sigma$, that $[Z^\sigma , h_i^*] < Z^\sigma \neq ([P^*, h_i^*] M^\sigma \langle h_i^* \rangle)$ is contained in the centre of $P^\sigma \cap [P^*, h_i^*] M^\sigma \langle h_i^* \rangle$, whence $[Z^\sigma , h_i^*] < C_{\sigma^2}(\langle L^\sigma , h_i^* \rangle)$.

Furthermore, if $\langle g_i^* \rangle = \langle h_i^* \rangle$,

$$C_{\sigma^2}(h_i) = C_{\sigma} (g_i^*) = C_{\sigma} (O^\sigma(L^\sigma \langle g_i^* \rangle))^\sigma = C_{\sigma^2} (O^\sigma(L^\sigma \langle h_i^* \rangle))^\sigma \subset C_{\sigma^2}(\langle L^\sigma , h_i^* \rangle).$$

It then follows that $[L^\sigma , h_i^* , Z^\sigma] = 1$ and since $\langle h_i^* \rangle \neq Q^*$,

$$[P^*, Q^*, Z^\sigma] = [P^*, Z^\sigma] = 1,$$ a contradiction. So assume $Q = \langle h^\tau \rangle$ with $|h^\tau| = q^\tau, \tau > 1$; we have already seen that $h^\tau$ has no invariant subspace on either $Z^\sigma \Phi(Z^\sigma)$ or $\Omega_1(Z^\sigma)$ and that $[h^\tau, P] < P$; we presently shall prove that $P$ is $h^\tau$-irreducible. Thus, suppose $P = P_1 \times P_2$ is a proper $h^\tau$-factorization; if $P_i = P_i/\langle C_{\sigma^2}(Z^\sigma) \rangle$, $\bar{Q} = Q^\sigma/\langle C_{\sigma^2}(Z^\sigma) \rangle$, $h_i = h C_{\sigma^2}(Z^\sigma)$ with $p | |h||$, then $Z_i = [Z^\sigma , h_i] < O^\sigma(P_i^\sigma Q^\sigma)$, so $Z$ is in the centre of $P \cup O^\sigma(P_i^\sigma Q^\sigma)$, a $p$-Sylow subgroup of $O^\sigma(P_i^\sigma Q)$, which implies $[Z^\sigma, P^\sigma \cup O^\sigma(P_i^\sigma Q)] = 1$ (because $O^\sigma(P_i^\sigma Q)$ is normal and proper in $G$); if now $\bar{x} = x C_{\sigma^2}(Z^\sigma)$ with $x \in P^\sigma$ is any element of $P_i^\sigma$, there exists $\bar{y} = y C_{\sigma^2}(Z^\sigma)$ with $\bar{y} \in P_i^\sigma$, $\bar{x} = [\bar{y}, \bar{h}^\tau]$ and $[y, h^\tau] \in P^\sigma$: this means that $x = [y, h^\tau] \in C_{\sigma^2}(Z^\sigma)$, and eventually $[P_i^\sigma, Z^\sigma] = 1$, again a contradiction; in particular, $[\bar{h}^\tau, \bar{P}] = 1$. For the next step, we choose $y \in P^\sigma$, $y \notin C_{\sigma^2}(Z^\sigma)$, and we start with a detailed investigation of which (and of course $Q$) is a cyclic $q$-group for some prime $q \neq p$; so assume, by way of contradiction, that there is a family $\{h_i^*\}_{i \in I}$ of elements of $Q^*$ such that $\langle h_i^* \rangle < Q^*$ for every $i$, while $\langle h_i^* \rangle \neq Q^*$, $\langle h_i^* \rangle \neq Q^*$. By an earlier remark $[P^* , h_i^*] < P^*$, and, if $h_i^* = h_i M^\sigma$ with $(|h_i|, p) = 1$, $O^\sigma([P^* , h_i^*] M^\sigma \langle h_i^* \rangle) = [P^*, h_i^*] M^\sigma \langle h_i^* \rangle \neq G^\sigma$, which implies, by our choice of $\sigma$, that $[Z^\sigma , h_i^*] < Z^\sigma \neq ([P^*, h_i^*] M^\sigma \langle h_i^* \rangle)$ is contained in the centre of $P^\sigma \cap [P^*, h_i^*] M^\sigma \langle h_i^* \rangle$, whence $[Z^\sigma , h_i^*] < C_{\sigma^2}(\langle L^\sigma , h_i^* \rangle)$.
and we would get the same contradiction as before. In view of the particular structure of $Z$, we can find a cyclic direct factor $\langle v_0 \rangle$ of $Z$ containing $\langle x \rangle \cap Z \neq 1$; $\langle x \rangle$ is a direct factor of $Z\langle x \rangle$ and for $z \neq 1$ in a complement $S$ of $\langle x \rangle \cap \Omega_1(Z)$ in $\Omega_1(Z)$, the heights of $z$ in $Z \langle x \rangle$ and in $Z$ are the same, so we may construct a decomposition $Z\langle x \rangle = \langle x \rangle \times \langle v_1 \rangle \times \ldots \times \langle v_k \rangle \times \langle c \rangle$, where $\langle v_0 \rangle \times \langle v_1 \rangle \times \ldots \times \langle v_k \rangle = Z$ and $|c| < p^n$; we fix the notation such that $\langle v_1 \rangle^\sigma = \langle w_1 \rangle$, $\langle c \rangle^\sigma = \langle d \rangle$. We can also manage to get $v_0 = x^{p^n-k}$ and $w_0 = y^{p^n-k}$. $\langle y \rangle Z^\sigma$, as a modular non-Hamiltonian group, has the form $A\langle t \rangle$, where $t$ induces a power automorphism on the abelian group $A$; under our assumptions $t$ can be chosen such that $u^t = u^{1+p^i}$ where $p^i = \exp A$, so that $(\langle y \rangle Z^\sigma)' = \Omega_1(A)$ and $\langle y \rangle Z^\sigma$ has class 2. Suppose first that $\exp A > p^n$; in this case $(\langle y \rangle Z^\sigma)' = \Omega_1(\langle y \rangle)$, $\langle y \rangle < \langle y \rangle Z^\sigma$, $|Z^\sigma: C_{Z^\sigma}(y)| = p$, and the matrix of $y$ on $Z$ (with entries from $Z/p^n Z$), for a suitable choice of the basis, is either

$$
\begin{pmatrix}
1 + p^{n-1} & 0 \\
0 & \text{identity}
\end{pmatrix}
$$

if $w_0$ is normalized but not centralized by $y$; or

$$
\begin{pmatrix}
\text{identity} & 0 \\
0 & 1
\end{pmatrix}
$$

if $[w_0, y] = 1$, in which case we may assume that $[w_k, y] = w_0^{p^{n-1}}$ and $[w_i, y] = 1$ for $1 < i < k$ (it is understood that to get precisely these coefficients we may have to choose another generator for $\langle y \rangle$). The exponent of $A$ cannot be $p^n$, for in this case $Z\langle x \rangle / A^\sigma$ being cyclic implies that $v_1 = x^y g$ with $g \in A^\sigma$, so that $1 = v_1^{p^n-1} = x^{y^{p^n-1}} \in \langle v_0 \rangle \setminus \langle v_1 \rangle$. We now assume that $\exp A = p^n$, and remark that from $|t| < |y|$ and $y = t'u$ with $u \in A$ it follows that $|y| = |t'|$ and we can substitute $y$ for $t$. Moreover, we can replace $A$ with $U = A\langle y^{p^{n-1}} \rangle$: thus, $U$ is abelian and $u^t = u^{1+p^{n-1}}$ for every $u \in U$; but now $U$ has index $p$ in $\Omega_n(\langle y \rangle Z^\sigma) = U\langle y^{p^n-k} \rangle$, $Z^\sigma \cong U$, so that $|Z^\sigma: Z^\sigma \setminus U| = p$,
and the last \( k \) elements of a basis for \( Z^\sigma \) can be chosen in \( Z^\sigma \cap U \) (remember that \( \dim Z^\sigma = k + 1 \), and that \( y^{p^{\sigma - n}} \notin U \)). The missing element of the basis of \( Z^\sigma \) has the form \( z = y^{p^{\sigma - n}} u \), with \( p \nmid r \), \( u \in U \), and we try to arrange the things so that \( w^{p^{n-1}} \in \Omega_1(\langle y \rangle) \). Since \( \Omega_2(Z^\sigma) = \langle y^{p^{n-1}} \rangle \times \sigma_{-1}(Z^\sigma \cap U) \), we have \([z, y] = [u, y] = w^{p^{n-1}} = y^{p^{\sigma - n}} \cdot w^{p^{n-1}} \) with \( w \in Z^\sigma \cap U \), so \( zw^{-1} = y^{p^{n-1}}(uw^{-1}) \) is congruent to \( z \) modulo \( Z^\sigma \cap U \), \( uw^{-1} \in U \), and \((uw^{-1})^{p^{n-1}} \in \Omega_1(\langle y \rangle) \), as required. For such a choice of the first element \( z \) of the basis \( \sigma_{-1}(\langle z \rangle) = \Omega_1(\langle y \rangle) \times \sigma_{-1}(\langle u \rangle) \), so that \([z, y] = [u, y] = w^{p^{n-1}} = z^{p^{n-1}} \), and the matrix of \( y \) on \( Z^\sigma \) can be written either as

\[
\begin{pmatrix}
1 & 0 \\
0 & 1 + p^{n-1}
\end{pmatrix}
\]

(III)

or as

\[
\begin{pmatrix}
1 + \lambda p^{n-1} & 0 \\
0 & 1 + p^{n-1}
\end{pmatrix}
\]

(IV)

with \( \lambda \neq 0 \), \( \lambda \neq 1 \) (mod. \( p \)), where the right lower corner corresponds to the action of \( y \) on \( U \cap Z^\sigma \). It is easily checked that, under either (III) or (IV), if \( S = \langle u \rangle \times \langle v \rangle \) is a \( y \)-invariant subgroup of \( Z^\sigma \) and \([u] = [v] = p^n \), then \( S \) is also the product of two \( y \)-invariant cyclic subgroups: if \( S \leq C_1(y) = \{ z \in Z^\sigma | z^p = z^{1 + p^{n-1}} \} \) there is nothing to prove; otherwise \( |S : C_1(y) \cap S| = p \), and we may assume that \( u = w_0 e \), \( w_0 = w_0^{1, b}p^{n-1} \) (where \( \lambda = 0 \) under (III), \( \lambda = 0 \neq 1 \) under (IV)) \( c \in C_1(y) \), \( v \in C_1(y) \). \([u, y] = (w_0 e)^p - 1 \in S \), so \( \langle w_0^{p^{n-1}} \rangle \times \langle w_0^{1, b} \rangle \times \sigma_{-1}(C_1(y)) \) imply that \( (\sigma^v)^{p^{n-1}} = 1 \), \( r = 1 \) (mod. \( p \)), whence \([w_0^{p^{n-1}}, y] = w_0^{1, b}p^{n-1} = (w_0^{p^{n-1}})^{p^{n-1}} \), and \( S = \langle w_0^{p^{n-1}} \rangle \times \sigma_{-1}(C_1(y)) \) with both factors \( y \)-invariant. We also remark that, if we look at the elements of \( \bar{P} \) as linear \( Z/p^nZ \) maps on \( Z^\sigma \), then their determinant is 1, otherwise we would get \( O_\sigma(C^\sigma) \neq G^\sigma \); this remark eliminates case (I). The next step is to prove that \( \dim Z > 2 \): so assume \( \dim Z = 2 \) and take \( a \in P^\sigma \) such that \( \bar{a} \neq 1 \). Suppose \( a \) satisfies (II) with respect to a basis \( z_0, z_1 ; \)

Federico Menegazzo
clearly we can choose \( z_1 = z_0^a \), so \( a \) is represented by

\[
\begin{pmatrix}
1 & 0 \\
p^{n-1} & 1
\end{pmatrix},
\]

\( a^h \) by

\[
\begin{pmatrix}
1 + \alpha p^{n-1} & \beta p^{n-1} \\
0 & 1
\end{pmatrix};
\]

\( \det a^h = 1 \) implies \( \alpha \equiv 0, \beta \not\equiv 0 \pmod{p} \), so if \( a_i \in P^\sigma \) is such that \( \overline{a_i} = \overline{a^h} \) then \( a_i \) is represented by

\[
\begin{pmatrix}
1 & \beta p^{n-1} \\
\gamma p^{n-1} & 1
\end{pmatrix} \quad ((i \not\equiv 0 \pmod{p})
\]

\( \langle z_0^a z_1^a \rangle \) is \( a \)-invariant if there is \( \mu \) such that \( (z_0^a z_1^a) \mu p^{n-1} = [z_0^a z_1^a, a_i] = (z_0^a z_1^a)^{p^{n-1}} \). \( \mu \equiv 0 \) implies \( s \equiv 0 \equiv r \pmod{p} \), i.e. \( C_{\Phi^\sigma}(a_i) = \Phi(Z^2) \); for \( \mu \not\equiv 0 \) we get \( s \beta \equiv s \mu^2 \pmod{p} \), and either \( s \equiv 0 \equiv r \) or \( i \beta \) is a square in \( F_p = Z/pZ \); if \( p \neq 2 \) this leads to a contradiction, and for \( p = 2 \) we check directly that \( a^h \) is represented by

\[
\begin{pmatrix}
1 & 2^{n-1} \\
0 & 1
\end{pmatrix},
\]

and \( aa^h \) does not normalize two independent cyclic subgroups of order \( 2^n \), again a contradiction. So if \( \dim Z = 2 \), then every \( a \in P^\sigma \) with \( \overline{a} \neq 1 \) is represented, with respect to a suitable basis \( z_0, z_1 \), by

\[
\begin{pmatrix}
1 - p^{n-1} & 0 \\
0 & 1 + p^{n-1}
\end{pmatrix}
\]

(i.e. case (IV) with \( \lambda \equiv -1; p \neq 2 \); we possibly have to change the generator of \( \langle a \rangle \). If \( a^h \) is represented by

\[
\begin{pmatrix}
1 + \alpha p^{n-1} & \beta p^{n-1} \\
\gamma p^{n-1} & 1 + \delta p^{n-1}
\end{pmatrix},
\]

\( \det a^h = 1 \) implies \( \alpha + \delta \equiv 0 \pmod{p} \); \( a^h \) induces \( 1 + p^{n-1} \) on some
\[ \langle x_0^r x_1^s \rangle \text{ with } (r, s) \neq (0, 0), \text{ i.e. } [x_0^r x_1^s, a^h] = (x_0^r x_1^s x_0^r x_1^s)^{p-1} = (x_0^r x_1^s)^{p-1}, \]

which means that the linear system

\[
\begin{cases} 
  r(x - 1) + sy = 0 \\
  r\beta + s(\delta - 1) = 0
\end{cases}
\]

has a non trivial solution, and

\[
\det \begin{pmatrix} 
  x - 1 & y \\
  \beta & \delta - 1
\end{pmatrix} = x\delta - \beta y + 1 \equiv 0 \pmod{p}.
\]

Now take \( a_i \in \mathbb{P} \) such that \( a_i \equiv a_i' a_i^h \); it is represented by

\[
\begin{pmatrix}
  1 + (x - i)p^{n-1} & \beta p^{n-1} \\
  \gamma p^{n-1} & 1 + (\delta + i)p^{n-1}
\end{pmatrix};
\]

it has to normalize two independent cyclic subgroups of \( \mathbb{Z}^\sigma \), so \( [x_0^r x_1^s, a_i] = (x_0^{(x+i)} x_1^\beta x_0^{(\delta+i)} x_1^\gamma)^{p-1} = (x_0^r x_1^s)^{p-1} \) must be solvable with \( (r, s) \neq (0, 0) \) for two choices of \( \mu \) not congruent mod. \( p \), i.e.

\[
\begin{pmatrix} 
  x - i & \beta \\
  y & \delta + i
\end{pmatrix}
\]

must have two distinct eigenvalues in \( F_p \). The characteristic polynomial

\[
\chi(\mu) = \det \begin{pmatrix} 
  x - i - \mu & \beta \\
  y & \delta + i - \mu
\end{pmatrix} = \mu^2 - i^2 - 2\delta i - 1
\]

has distinct roots in \( F_p \) if and only if \( \Delta(i) = i^2 + 2\delta i - 1 \in (F_p - \{0\})^2 \); \( \Delta(i) = \Delta(j) \) if and only if \((i - j)(i + j + 2\delta) = 0 \pmod{p} \), so the partition \( \mathcal{P}_d \) associated with \( \Delta \) is \( \{-\delta\}, \{j, -j - 2\delta\}, j=\frac{-p-1}{2} \) and has \((p+1)/2\) elements; \( \Delta(0) = 1 \in (F_p - \{0\})^2 \). If \( 0 \neq -\delta \), then \( |\Delta(F_p - \{0\})| = (p+1)/2 \); if \( 0 = -\delta \), then \( |\Delta(F_p - \{0\})| = (p-1)/2 \), but \( 1 \notin \Delta(F_p - \{0\}) \).

In any case, we can find \( i \neq 0 \pmod{p} \) such that \( \Delta(i) \notin (F_p - \{0\})^2 \): for such an \( i \) \( a_i \) does not satisfy the conditions we asked for. This contradiction proves \( \dim Z > 2 \); we shall show that \( \dim Z = 3 \). Suppose we can choose \( a \in \mathbb{P} \) satisfying (II); since \( [a, Z^\sigma] a^{\mathbb{P}} Z^\sigma = 1 \), \( C_{2\sigma}(a) = C_{2\sigma}^\sigma(a) \setminus C_{2\sigma}^\sigma(a) \) has index \( p^2 \) in \( Z^\sigma \): this is only possible when
dim $Z = 3$, and $a_i$ satisfies (III). If there is $a$ in $P^a$ satisfying either (III) or (IV), $C_{x^a}(a^{-1}a^h) > C_1(a) \cap C_1(a^h)$, where $C_1(y) = \{z \in Z^a | z^a = z^{1+np^{-1}} \}$, which has index $p^2$ in $Z^a$, so: if $|Z^a: C_{x^a}(a^{-1}a^h)| = p$, $a^{-1}a^h$ satisfies (II) and we have just proved that dim $Z = 3$ in this case; if $|Z^a: C_{x^a}(a^{-1}a^h)| = p^2$, then $a^{-1}a^h$ satisfies (III) and once more dim $Z = 3$.

Suppose now that $a \in P^a, a \neq 1$, $a$ satisfies (II); with respect to a basis $z_o, z_1, z_2$ such that $\langle z_o \rangle \cap Z^a, \langle z_o, z_1 \rangle \Phi(Z^a) = C_{x^a}(a), \langle z_2 \rangle = \langle z_0 \rangle$, $a$ is represented by

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
p^{-1} & 0 & 1
\end{pmatrix},
$$

$a^h$ by

$$
\begin{pmatrix}
1 & 0 & \alpha p^{n-1} \\
0 & 1 & \beta p^{n-1} \\
0 & 0 & 1
\end{pmatrix}.
$$

Two cases are possible: either $\langle z_o, z_1 \rangle \cap C_{x^a}(a) \cap C_{x^a}(a^h) = \langle z_o, z_0^2 \rangle$, i.e. $\alpha = 0, \beta \neq 0$ (mod. $p$); or $\langle z_o, z_2 \rangle \cap C_{x^a}(a) \cap C_{x^a}(a^h) = \Phi(\langle z_o, z_2 \rangle)$: if we choose $z_1$ such that $\langle z_1, \Phi(Z^a) \rangle = C_{x^a}(a) \cap C_{x^a}(a^h)$, then $\alpha \neq 0, \beta = 0$ (mod. $p$). In the former case $a_i$ is represented by

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & \beta p^{n-1} \\
p^{-1} & 0 & 1
\end{pmatrix}
$$

(symbols are as usual; $a_i$ must satisfy (III)); it centralizes $\langle z_o \rangle$ and normalizes no other (independent) cyclic subgroup of $Z^a$ of order $p^n$, a contradiction. In the latter case $a_i$ is represented by

$$
\begin{pmatrix}
1 & 0 & \alpha p^{n-1} \\
0 & 1 & 0 \\
p^{-1} & 0 & 1
\end{pmatrix};
$$

it centralizes $\langle z_1 \rangle \Phi(Z^a)$, and it should work as a power automorphism, $1 + \mu p^{n-1}$ say, $\mu \neq 0$ (mod. $p$), on a direct product $S$ of two cyclic subgroups of order $p^n$; but $\langle z_0^r z_1^t z_2^t \rangle < S$ if and only if $(z_0^r z_1^t z_2^t)^{\mu p^{n-1}} = [z_0^r z_1^t z_2^t, a_i] = (z_2^r z_0^t)^{\mu p^{n-1}}$, i.e. if and only if $(r, s, t)$ is a solution of

\begin{align*}
\begin{cases}
rmu - it & = 0 \\
smu & = 0 \\
rz - \mu t & = 0
\end{cases}
\end{align*}
whose rank is \(\geq 2\): there is one independent solution at most, a contradiction. So case (II) is ruled out. Now we assume \(a \in \mathcal{P}_a, a \not= 1\), \(a\) satisfies (III); \(\det a = 1 = 1 + 2p^{n-1}\) forces \(p = 2\). \(\mathcal{C}_1(a)\) has index 2 in \(\mathbb{Z}^a\); the same occurs to \(\mathcal{C}_1(a^h)\), so we can put \(\mathcal{C}_1(a) \cap \mathcal{C}_1(a^h) = = \mathcal{C}_2(a^h) = \langle \tau_2, \Phi(\mathcal{Z}) \rangle; a^h\) also satisfies (III). With respect to a basis \(\tau_0, \tau_1, \tau_2\), let \(a\) be represented by

\[
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 + 2^{n-1} & 0 \\
0 & 0 & 1 + 2^{n-1}
\end{pmatrix}.
\]

Assume further that \(\langle \tau_1, \tau_2 \rangle \Phi(\mathcal{Z}) = \langle \tau_0, \tau_2 \rangle \Phi(\mathcal{Z})\); we can choose \(\tau_2\) so that \(S = \langle \tau_0, \tau_2 \rangle = \langle \tau_0, \tau_2 \rangle = \langle \tau_0, \tau_2 \rangle\). \(S\) is \(\langle a, a^h \rangle\)-invariant, \(\langle \tau_0 \rangle \wedge \wedge \langle \tau_2 \rangle = 1\), so \(\tau_0 = (a^h)^n \tau_2\), \(\tau_0, a^h = \tau_0^{2^{n-1}}, a^h\) is represented on \(S\) by

\[
\begin{pmatrix}
1 & 2^{n-1} \\
0 & 1
\end{pmatrix},
\]

so \(\langle \tau_0^{2^{n-1}} \rangle \subset [a^h, \mathcal{Z}] \cap \mathcal{C}_2^{n-1}(\mathcal{C}_a(a^h))\); but under (III) this intersection is trivial. So we can assume that \(\langle \tau_0 \rangle \wedge \langle \tau_2 \rangle = 1\), and take \(\tau_1 = \tau_0\) instead of \(\tau_1\) in the basis (later on, we shall drop the apex); since we can always arrange that \(\tau_0 = \tau_0^n \tau_2\), this means that \(a\) is represented by

\[
\begin{pmatrix}
1 & 0 & 0 \\
\delta 2^{n-1} & 1 + 2^{n-1} & 0 \\
0 & 0 & 1 + 2^{n-1}
\end{pmatrix},
\]

and \(a^h\) by

\[
\begin{pmatrix}
1 + \alpha 2^{n-1} & \beta 2^{n-1} & \gamma 2^{n-1} \\
0 & 1 & 0 \\
0 & 0 & 1 + 2^{n-1}
\end{pmatrix},
\]

\(\det a^h = 1 + (\alpha + 1)2^{n-1} = 1\) forces \(\alpha \equiv 1 \pmod{2}\); \(a^h\) must induce the power \(1 + 2^{n-1}\) on a cyclic subgroup \(\langle \tau_0, \tau_1 \rangle = \langle \tau_0, \tau_1 \rangle \rangle = \langle \tau_0, \tau_1 \rangle \rangle = \langle \tau_0^2, \tau_1^2 \rangle^{2^{n-1}} = \langle \tau_0^2, \tau_2^2 \rangle, \ a^h = \rangle = \langle \tau_0^2, \tau_2^2 \rangle^{2^{n-1}}\), so \(\gamma + t = t, \ \gamma \equiv 0 \pmod{2}\). \(a^h\), which should satisfy (III), is represented by

\[
\begin{pmatrix}
1 + 2^{n-1} & \beta 2^{n-1} & 0 \\
\delta 2^{n-1} & 1 + 2^{n-1} & 0 \\
0 & 0 & 1
\end{pmatrix};
\]
it has to induce the power automorphism $1 + 2^{n+1}$ on a complement $S$ of $\langle z_2 \rangle$; this means that $(z_0^a z_1 z_2^a) z_2^{-1} = [z_0^a z_1 z_2^a, a a^h] = (z_0^a z_1 z_2^a)^{z_2^{-1}}$ for $z_0^a z_1 z_2^a \in S$, so that the system: $s \delta = 0$, $r \beta = 0$, $t = 0$ has two independent solutions; this only happens if $\beta = \delta = 0$. So $a$ is represented by

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 + 2^{n-1} & 0 \\
0 & 0 & 1 + 2^{n-1}
\end{pmatrix},
$$

$a^h$ by

$$
\begin{pmatrix}
1 + 2^{n-1} & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 + 2^{n-1}
\end{pmatrix};
$$

$z_0^h \in \langle z_1, \Phi(Z^a) \rangle$, $\langle z_1, z_2 \rangle^h \Phi(Z^a) = \langle z_0, z_2 \rangle \Phi(Z^a)$. We look at the way $h$ operates on $Z^a/\Phi(Z^a)$: if $z_1^h \equiv z_0 \pmod{\Phi(Z^a)}$, then

$$
z_0 \Phi(Z^a) = (z_0 \Phi(Z^a))^h,
$$

a contradiction; suppose $z_1^h \equiv z_2$ (the other possibility is $z_1^h \equiv z_0 z_2$) (mod. $\Phi(Z^a)$); then from $z_0^h \equiv z_0 \pmod{\Phi(Z^a)}$ it follows that $(z_0 \Phi(Z^a))^h = z_0 \Phi(Z^a)$, so $\langle h^a \rangle < \bar{Q}$, and, as $\bar{Q}$ is isomorphic to a subgroup of $GL(3, 2)$, $h^a = 1$ and $h$ cannot be irreducible on $\Omega_1(Z^a)$ which has dimension 3; clearly $z_2^a \not\equiv z_2$ (mod. $\Phi(Z^a)$), so $h$ is represented on $Z^a/\Phi(Z^a)$ by

$$
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 1
\end{pmatrix},
$$

and on $Z^a$ by

$$
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
\lambda & 2 \mu & \nu
\end{pmatrix}
$$

with $\lambda \equiv \nu \equiv 1 \pmod{2}$, where we are using the basis $z_0, z_1 = z_0$, $z_2 = z_1$; moreover $\lambda = \det h = 1$. An easy calculation shows that $a^h$ is represented by

$$
\begin{pmatrix}
1 + 2^{n-1} & 0 & 2^{n-1} \\
0 & 1 + 2^{n-1} & 0 \\
0 & 0 & 1
\end{pmatrix}
$$
and if \( b \in P^a, \overline{b} = \overline{a}a^i \), \( b \) should satisfy (III), which contrasts to the fact that it normalizes \( \langle z_0, z_2 \rangle \) and \( \langle z_2 \rangle \), but no complement of \( \langle z_2 \rangle \) in \( \langle z_0, z_2 \rangle \). If instead \( z_2^i \equiv z_0 z_2 \) (mod. \( \Phi(Z^a) \)), a similar argument proves that \( h \) is represented on \( Z^a/\Phi(Z^a) \) by

\[
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 1 \\
1 & 0 & 0
\end{pmatrix}
\]

and on \( Z^a \) by

\[
\begin{pmatrix}
0 & 1 & 0 \\
\lambda & 2\mu & \nu \\
1 & 0 & 0
\end{pmatrix},
\]

where we refer to the basis \( z_0, z_1 = z_0^b, z_2 = z_0^{b^{-1}} \); moreover \( \nu = \det h = 1 \). In this case \( a^b \) is represented by

\[
\begin{pmatrix}
1 + 2^{n-1} & 0 & 0 \\
0 & 1 + 2^{n-1} & 0 \\
2^{n-1} & 0 & 1
\end{pmatrix},
\]

and \( b \) as above normalizes \( \langle z_0 \rangle \) and \( \langle z_0, z_2 \rangle \), but no complement of \( \langle z_0 \rangle \) in \( \langle z_0, z_2 \rangle \). So far we showed that no element \( a \) in \( p^a \) satisfies (I), (II) nor (III); but if \( a \) satisfies (IV), then \( a^{-1}a^b \) should satisfy (III): this, last contradiction proves the lemma.

**Corollary 2.2.** Let \( \sigma: G \to H \) be an index-preserving projectivity. If the image \( Z(P)^a \) of the centre \( Z(P) \) of the \( p \)-Sylow-subgroup \( P \) of \( G \) is not contained in the centre of \( P^a \), then \( N^a_\sigma(Z(P)) \) has a proper normal subgroup \( K \) such that \( N^a_\sigma(Z(P))/K \) is a \( p \)-group.

**Proof.** Apply lemma 2.1 to \( N = N^a_\sigma(Z(P)) \).

3. We shall now use the propositions proved in section 2 in order to derive the results announced in the introduction.

**Theorem 3.1.** Let \( G \) be \( p \)-normal, \( P \) a \( p \)-Sylow subgroup of \( G \), \( \sigma: G \to H \) an index-preserving projectivity. If the image under \( \sigma \) of the centre of \( P \) is not contained in the centre of \( P^a \), then \( O^a(\sigma(G)) \neq G \); in particular \( G \) is not simple.
PROOF. Call $Z(P)$ the centre of $P$; 2.2 and the second theorem of Grün imply that $G/O^{p}(G) \cong N^{p}_{\sigma}(Z(P))/O^{p}\left(N^{p}_{\sigma}(Z(P))\right) \neq 1$, q.e.d.

THEOREM 3.2. Let $G$ be a $p$-soluble group with $O^{p}(G) = G$. For every $p$-Sylow subgroup $P$ of $G$ and every index-preserving projectivity $\sigma: G \to G^\sigma$ the image under $\sigma$ of the centre of $P$ is the centre of $P^\sigma$.

PROOF. For any group $X$ let $Z(X)$ be its centre. It will be enough if we prove that, under our assumptions, $Z(P)^\sigma < Z(P^\sigma)$: the opposite inclusion is then proved looking at $\sigma^{-1}$. Let $G$ be a counterexample of least possible order. Call $A$, $B$ respectively $O_{p'}(G)$, $O_{p'}(G^\sigma)$: they are the intersection of all subgroups of $G$, $G^\sigma$ maximal with respect to the property of having an order prime to $p$, so $B = A^\sigma$. Assume $A \neq 1$: $\sigma$ induces an index-preserving projectivity $\bar{\sigma}: G/A \to G^\sigma/B$ and by the minimality of $G$ (we now put $Z = Z(P)$)

$$(ZA/A)^{\bar{\sigma}} = Z(PA/A)^{\bar{\sigma}} = Z^{\sigma}A^{\sigma}/A^{\sigma} < Z((PA/A)^{\bar{\sigma}}) = Z(P^{\sigma}A^{\sigma}/A^{\sigma}),$$

so $[P^{\sigma}, Z^{\sigma}] \not< A^{\sigma}\cap P^{\sigma} = 1$ against our choice of $G$. There exists a proper normal subgroup $N$ of $G$ such that $p^{\nu}|G:N|$; put $M = O^{p}(N)$, and let $Q$ be a complement of $P$ in $N_{\sigma}(P)$. $G = [P, Q]QM$: thus, $P < N$ and by the Frattini argument $G = N_{\sigma}(P)N = QPN = QN$; furthermore $N = PM$, whence $G = PQM$: but $[P, Q]Q = Q^{p}$, so $P < N_{\sigma}([P, Q]QM)$, i.e. $[P, Q]QM \leq G$; $G/[P, Q]QM \cong P/[P, Q]QM \wedge P$ is a $p$-group, and eventually $G = [P, Q]QM$. Since $M \leq QM$ and $p^{\nu}|QM: M|$, we get $P\wedge QM = P\wedge M$; it follows that

$$P = P\wedge [P, Q]QM = [P, Q](P\wedge QM) = [P, Q](P\wedge M).$$

We shall now prove that $[P, Q]^{\sigma}$ centralizes $Z^{\sigma}$; thus, $[P, Q]Q = \cdots = O^{p}(P, Q)Q$, $C_{p}(Q)$ is a $p$-group contained in the centralizer of $[P, Q]Q$ so by 1.1 $([P, Q]Q)^{\sigma}, C_{p}(Q)^{\sigma} = 1$; in particular $[[P, Q]^{\sigma}, C_{p}(Q)^{\sigma} = 1$. Furthermore $[Z, Q] < Z([P, Q])$; $[P, Q]$ is a $p$-Sylow subgroup of $[P, Q]Q$, so by 2.1 $[Z, Q]^{p} < Z([P, Q]^{p})$; we can conclude that $[P, Q]^{\sigma}$ centralizes $C_{p}(Q)^{\sigma}\cup [Z, Q]^{\sigma} = Z^{\sigma}$. Next we prove that $Z \leq M$: assume $Z < M$: then $Z < Z(P\wedge M)$ and, by the minimality of $G$, as $P\wedge M$ is a $p$-Sylow subgroup of $M < G$, $Z^{p} < Z((P\wedge M)^{p})$: this fact, together with an earlier statement, implies the contradiction $[Z^{p}, P^{\sigma}] = 1$. Let $F$ be the Fitting subgroup of $G$: under our assumptions $F$ is a nontrivial $p$-group, and $F \supset C_{p}(F)$ [1]. We also have $F < P < N$ and $[Z, F] = 1$ implies $Z < Z(F) < F$; whence $Z^{p}$ is an abelian subgroup
of $Z(F)$. Let $1 = V_0 < V_1 < \ldots < V_k = M$ be a $p$-series of $M$ whose elements are normal in $G$ (i.e. $V_i/V_{i-1}$ is either a $p$-group or $p
mid |V_i/V_{i-1}|$ for $i = 1, \ldots, k$). We shall prove by induction that $[V_i, Z^o] = 1$. $V_1$ is a $p$-group, so $V_1 \leq F'$ and $[V_1, Z^o] = 1$. Assume next $[V_r, Z^o] = 1$; if $p \nmid |V_{r+1}/V_r|$, we can write $Z^o = [Z^o, V_{r+1}] \times C_{Z^o}(V_{r+1})$ where both factors are normal $p$-subgroups of $G = O^p(G)$; 1.1 then tells that $[Z^o, V_{r+1}]^o$ and $C_{Z^o}(V_{r+1})^o$ are both normal in $G^o$; if both are non-trivial by the minimality of $G [P^o, Z^o] < [Z^o, V_{r+1}]^o \cap C_{Z^o}(V_{r+1})^o = 1$ against our choice of $G$. But if $C_{Z^o}(V_{r+1}) = 1$, then $Z < Z^o = [Z^o, V_{r+1}] < V_{r+1} < M$ contradicting an earlier statement, so in this case $[Z^o, V_{r+1}] = 1$. In case $V_{r+1}/V_r$ is a $p$-group, $V_{r+1} = (P \cap V_{r+1}) V_r$; for every $x \in G$ 

$$[P \cap V_{r+1}, Z^o] = [(P \cap V_{r+1})^{v^{-1}}, Z^o] = [(P \cap V_{r+1})^{v}, Z^o] = [P \cap V_{r+1}, Z]^{v^{-1}} = [P \cap V_{r+1}, Z]^{v} = 1$$

for a suitable $v \in V_r$; hence in this case too $[Z^o, V_{r+1}] = 1$. It follows that $[Z^o, M] = [Z^o, V_r] = 1$; $Z^o$ is a $p$-group, $M = O^p(M)$, so by 1.1 $[Z^o]^o, M^o] = 1$, $C_{Z^o}(Z^o) > [P, Q]^o M^o > [P, Q]^o (P \cap M)^o = P^o$: this contradiction ends the proof.

(Theorem 3.2 dealt originally with soluble groups; the author is grateful to prof. F. Napolitani who pointed out to him that the proof worked for $p$-soluble groups too).

REFERENCES


Manoscritto pervenuto in redazione il 23 aprile 1974.