RENDICONTI
*del*
SEMINARIO MATEMATICO
*della*
UNIVERSITÀ DI PADOVA

FEDERICO MENEGAZZO

# On index preserving projectivities of finite groups

*Rendiconti del Seminario Matematico della Università di Padova*, tome 52 (1974), p. 227-242

<http://www.numdam.org/item?id=RSMUP_1974__52__227_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 52 (1974)

# 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 $\sigma\colon G \to H$ is index preserving if $|U^\sigma : V^\sigma| = |U : V|$ for every pair $U \geqslant V$ 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 $G$, $\sigma\colon G \to H$ 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 $G$, $\sigma\colon G \to G^\sigma$ an index preserving projectivity, and assume that $A$ is generated by its $p$-elements, while $B = O^p(B)$. If $B \leqslant \mathcal{N}_G(A)$, then $B^\sigma \leqslant \mathcal{N}_{G^\sigma}(A^\sigma)$; if $B \leqslant \mathcal{C}_G(A)$, then $B^\sigma \leqslant \mathcal{C}_{G^\sigma}(A^\sigma)$. (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 $A \vee \langle x \rangle$ is in $A$, i.e. $A$ is the union of the cyclic subgroups of $A \vee \langle x \rangle$ whose orders are a power of $p$. Since $\sigma$ is index preserving, $A^\sigma$ is the union of the cyclic subgroups of $(A \vee \langle x \rangle)^\sigma$ whose orders are a power of $p$, so $A^\sigma \trianglelefteq (A \vee \langle x \rangle)^\sigma$; as $x$ describes all the elements of $B$ whose orders are prime to $p$ we get $B^\sigma \leqslant \mathcal{N}_{G^\sigma}(A)$. If furthermore $B \leqslant \mathcal{C}_G(A)$, for every element $x$ of $B$ such that $p \nmid |x|$ and for every $p$-element $y$ of $A$ $\langle x \rangle \vee \vee \langle y \rangle = \langle x \rangle \times \langle y \rangle$ 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 $\mathcal{N}_G(P)$. If $\sigma\colon G \to G^\sigma$ is an index preserving projectivity, then $P^\sigma$ is a $p$-Sylow subgroup of $G^\sigma$, $\mathcal{N}_{G^\sigma}(P^\sigma) = \mathcal{N}_G(P)^\sigma = P^\sigma Q^\sigma$, $[P, Q]^\sigma = [P^\sigma, Q^\sigma]$, $\mathcal{C}_P(Q)^\sigma = \mathcal{C}_{P^\sigma}(Q^\sigma)$.

PROOF. The only thing to prove is that $[P, Q]^\sigma = [P^\sigma, Q^\sigma]$. $[P, Q]$ is the intersection of $P$ with $O^p(\mathcal{N}_G(P))$; 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 $[G, \operatorname{Aut} G] \leqslant M$ or $\Phi(G)[M, \operatorname{Aut} G] < M$.

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 $[G/H, \operatorname{Aut} G/H] \leqslant M/H$ (in which case $[G, \operatorname{Aut} G] \leqslant M$ would follow) or

$$\Phi(G/H)[M/H, \operatorname{Aut} G/H] < M/H ,$$

i.e. $\Phi(G)[M, \operatorname{Aut} G] < M$. In particular $G' \wedge \Omega_1(Z(G)) \geqslant G'$, i.e. $G' \leqslant \Omega_1(Z(G))$. So $G = A\langle b \rangle$ with $A$ abelian, $a^b = a^{1+p^s}$ for every $a \in A$, $\exp A = p^{s+1}$, $p^s > 2$. We now prove that we may choose $A$, $b$ such that $|b| \leqslant \exp A$: thus, if $|b| > p^{s+1}$, then $1 \neq \langle (ab^i)^{p^{s+1}} | a \in A \rangle = \langle b^{ip^{s+1}} \rangle = \mho_{s+1}(G) \leqslant \mho_1(G) = \Phi(G)$, whence $G' \leqslant \langle b \rangle$ and $G'$ is cyclic; on the other hand $G' = [A, b] = \mho_3(A)$, so $A = \langle t \rangle \times U$ with $\exp U \leqslant p^s$, $|t| = p^{s+1}$; $V = U\langle b \rangle$ is now abelian, and $t$ normalizes every cyclic subgroup of $V$, because if $i \equiv 0 \pmod{p}$ $[ub^i, t] = 1$ and if $i \not\equiv 0 \pmod{p}$ $[ub^i, t] = [b^i, t] \in \langle b^{p^{s+1}} \rangle = \langle (ub^i)^{p^{s+1}} \rangle \leqslant \langle ub^i \rangle$; 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 $x = ab^{ip} \in M$ $x^{p^s} = a^{p^s}$, so $x^b = a^{1+p^s} b^{ip} = xa^{p^s} = x^{1+p^s}$. If $M$ is a characteristic subgroup of $G$, then for every $x \in M$, $\alpha \in \operatorname{Aut} G$ $(x^\alpha)^b = (x^\alpha)^{1+p^s} = (x^{1+p^s})^\alpha = (x^b)^\alpha$, i.e. $[b, \alpha] \in \mathfrak{C}_G(M) = M$; and $[G, \operatorname{Aut} G] \leqslant M$. If $M$ is not characteristic in $G$, then $|G/Z(G)| = p^2$, $\Phi(G) \leqslant Z(G)$, and since $Z(G) = \Omega_s(A)\langle b^p \rangle$, $Z(G) < AZ(G) = M < G$, we get $|A : \Omega_s(A)| = p$, i.e. $A = \langle u \rangle \times V$ with $p^s \geqslant \exp V$, $p^{s+1} = |u|$. 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 $|g| \leqslant p^s$; it follows $\langle u \rangle \wedge \langle b \rangle = 1$, since otherwise $1 \neq b^{p^s} = u^{ip^s}$ and $(u^{-i} b)^{p^s} = 1$, contradicting the former assumption, for a suitable $i \not\equiv 0$ (mod. $p$); hence $\langle u \rangle \wedge \langle u^k b \rangle = 1$ 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 $Z(G) < N < G$, $N \neq M$, $N/Z(G) = \langle u^k bZ(G) \rangle$ with $k$ a suitable integer, and since $[u^k b, u] = [b, u] = u^{-p^s} \notin \langle u^k b \rangle$ $N$ contains $\langle u^k b \rangle$ which is not normal in $G$. So assume we chose $b$ such that $|b| \leqslant p^s$; for every $x \in G$, $x = ab^i$, $x^{p^s} = (ab^i)^{p^s} = a^{p^s}$, $x^b = a^{1+p^s} b^i = a^{p^s} x = x^{1+p^s}$: $b$ induces on $G$ a homogeneous power automorphism, hence $[b, \operatorname{Aut} G] \leqslant Z(G)$. Furthermore $\Omega_s(G) = \langle u^p, V, b \rangle = Z(G)\langle b \rangle$, $|G : \Omega_s(G)| = |\Omega_s(G) : Z(G)| = p$, and eventually $\Phi(G)[\Omega_s(G), \operatorname{Aut} G] = \Phi(G)[Z(G)\langle b \rangle, \operatorname{Aut} G] \leqslant Z(G)$, 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 $A \leqslant G$ be an abelian $p$-group, $Q \leqslant \mathcal{N}_G(A)$, $p \nmid |Q|$. If $\sigma : G \to G^\sigma$ is an index-preserving projectivity, then $A^\sigma = [A^\sigma, Q^\sigma] \times \mathfrak{C}_{A^\sigma}(Q^\sigma)$, and $[A^\sigma, Q^\sigma]$ is in the centre of $A^\sigma$.

PROOF. Put $H = O^p(AQ)$; then $H^\sigma = O^p(A^\sigma Q^\sigma)$. $[A^\sigma, Q^\sigma] = [A, Q]^\sigma = (A \wedge H)^\sigma = A^\sigma \wedge H^\sigma \trianglelefteq A^\sigma Q^\sigma$;

$$\mathfrak{C}_{A^\sigma}(Q^\sigma) = \mathfrak{C}_A(Q)^\sigma = \mathfrak{C}_A(H)^\sigma = \mathfrak{C}_{A^\sigma}(H^\sigma) \trianglelefteq A^\sigma Q^\sigma \ ;$$

so $A^\sigma = ([A, Q] \times \mathfrak{C}_A(Q))^\sigma = [A^\sigma, Q^\sigma] \times \mathfrak{C}_{A^\sigma}(Q^\sigma)$. Moreover $[A^\sigma, Q^\sigma, Q^\sigma] =$

$=[A, Q, Q]^\sigma = [A, Q]^\sigma = [A^\sigma, Q^\sigma]$: by lemma 1.3, since $[A^\sigma, Q^\sigma]$ is a modular non-Hamiltonian $p$-group, $[A^\sigma, Q^\sigma]$ is abelian, q.e.d.

COROLLARY 1.5. Let $A$ be a 2-generator abelian $p$-subgroup of $G$, $\sigma\colon G \to G^\sigma$ an index-preserving projectivity. If $A^\sigma$ is not abelian, then $\mathcal{N}_G(A)/\mathcal{C}_G(A)$ is a $p$-group.

PROOF. Let $Q$ be a subgroup of $\mathcal{N}_G(A)$ such that $p \nmid |Q|$. $A^\sigma$ is a 2-generator modular non-abelian non-Hamiltonian $p$-group, so $A^\sigma$ is not directly decomposable; by 1.4 $[A^\sigma, Q^\sigma] < A^\sigma$, whence $[A^\sigma, Q^\sigma] = 1 = [A, Q]$, 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

$$H = \langle a, b \mid a^p = b^q = 1,\ a^b = a^r,\ \exists r \not\equiv 1,\ r^q \equiv 1 \ (\mathrm{mod.}\, p)\rangle$$

where $p$, $q$ are prime numbers, $p \equiv 1$ (mod. $q$); $K = \langle c, d \mid c^{p^2} = d^p = 1, [c, d] = 1\rangle$; $L = \langle e, f \mid e^{p^2} = f^p = 1,\ e^f = e^{1+p}\rangle$. For every element $he^x f^y$ of $H \times L$ ($h \in H$; $x$, $y$ integers) put $(he^x f^y)^\tau = hc^x d^y \in H \times K$; since $he^x f^y = h' e^{x'} f^{y'}$ ($h, h' \in H$; $x, x', y, y'$ integers) if and only if $hc^x d^y = h' c^{x'} d^{y'}$, $\tau$ is a well defined bijection of $H \times L$ onto $H \times K$. Moreover if $he^y f^x$, $h' e^{x'} f^{y'} \in H \times L$, with $[e^{x'}, f^{-y}] = e^{p\alpha(x', y)}$, we get

$$\big((he^x f^y)(h' e^{x'} f^{y'})\big)^\tau = hh' c^{x+x'+p\alpha(x',y)} d^{y+y'} \in \langle (he^x f^y)^\tau, (h' e^{x'} f^{y'})^\tau\rangle =$$
$$= \langle hc^x d^y, h' c^{x'} d^{y'}\rangle\,;$$

in fact, this is true if and only if $c^{p\alpha(x',y)} \in \langle hc^x d^y, h' c^{x'} d^{y'}\rangle$, but if $x' \equiv 0$ (mod. $p$), then $\alpha(x', y) \equiv 0$ (mod. $p$) and $c^{p\alpha(x',y)} = 1$, whereas if $x' \not\equiv 0$ (mod. $p$)

$$c^{p\alpha(x',y)} \in \langle c^p\rangle = \langle c^{pqx'}\rangle = \langle (h' c^{x'} d^{y'})^{pq}\rangle \leqslant \langle hc^x d^y, h' c^{x'} d^{y'}\rangle\,.$$

So $\tau$ induces a bijection of $\mathfrak{L}(H \times L)$ onto $\mathfrak{L}(H \times K)$ 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 $G$, $A^\sigma = \langle a\rangle \times L$ is no longer abelian, but $\mathcal{N}_G(A)/\mathcal{C}_G(A) = G/A \simeq \langle b\rangle$ 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 $P$, $\sigma\colon G\to G^\sigma$ 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 $Z^\sigma\trianglelefteq G^\sigma$; 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 $G$ $[P^\sigma, Z^\sigma]\leqslant A^\sigma\wedge B^\sigma=1$, 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 $G/\mathrm{C}_G(Z)\neq 1$. As $(p, |G/\mathrm{C}_G(Z)|)=1$ $Z=[Z,G]\times\mathrm{C}_Z(G)$; both factors are normal subgroups of $G$, $\mathrm{C}_Z(G)\neq Z$ and by what we have just pointed out $Z=[Z,G]$, $\mathrm{C}_Z(G)=1$. 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 $Z^\sigma=[Z^\sigma,\langle h\rangle]\times\mathrm{C}_{Z^\sigma}(h)$ with abelian $[Z^\sigma,\langle h\rangle]$, whence $\mathrm{C}_{Z^\sigma}(h)\geqslant(Z^\sigma)'$; $G^\sigma=O^p(G^\sigma)$, so $(Z^\sigma)'$ 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 $M\leqslant\mathrm{C}_G(Z)$ and by 1.1 $M^\sigma\leqslant\mathrm{C}_{G^\sigma}(Z)$, and since $L=PM$, $L^\sigma=P^\sigma M^\sigma$, then $L^\sigma/\mathrm{C}_{L^\sigma}(Z^\sigma)$ is a $p$-group. It follows that $\mathrm{C}_{Z^\sigma}(L^\sigma)\neq 1$ 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 $T\trianglelefteq G$. $|G/\mathrm{C}_G(\Omega_1(Z))|$ is not divisible by $p$, hence $T$ has a complement $S$ in $\Omega_1(Z)$ which is normal in $G$; an earlier remark shows $T=\Omega_1(Z)$, i.e. $\Omega_1(Z^\sigma)$ is contained in the centre of $P^\sigma$ and of every conjugate of $P^\sigma$. Therefore $p^n=\exp Z>p$; the minimality of $G$ then implies $[P^\sigma,Z^\sigma]\leqslant\Omega_1(Z^\sigma)$, $[\Phi(P^\sigma),Z^\sigma]=[P^\sigma,\Phi(Z^\sigma)]=1$ (for every group $\Phi(X)=$ Frattini subgroup of $X$). Define $G^*=G^\sigma/M^\sigma$, $\bar G=G^\sigma/\mathrm{C}_{G^\sigma}(Z^\sigma)$ (for every $x\in G^\sigma$, $x^*=xM^\sigma$ and $\bar x=x\mathrm{C}_{G^\sigma}(Z^\sigma)$); $\bar G$ is isomorphic to a quotient group of $G^*$. Since $L^\sigma=P^\sigma M^\sigma\trianglelefteq G^\sigma$, the $p$-Sylow subgroup $P^*=P^\sigma M^\sigma/M^\sigma$ of $G^*$ is normal in $G^*$, and $\bar P=P^\sigma\mathrm{C}_{G^\sigma}(Z^\sigma)/\mathrm{C}_{G^\sigma}(Z^\sigma)\trianglelefteq\bar G$; $\bar P\neq 1$ by our choice of $G$; let $Q^*$, $\bar Q$ be complements of $P^*$, $\bar P$ in $G^*$, $\bar G$ respectively. Since $G^*=O^p(G^*)$ and $\bar G=O^p(\bar G)$, it follows that $P^*=[P^*,Q^*]$, $\bar P=[\bar P,\bar Q]$; moreover if $H^*=H^\sigma/M^\sigma$ is a proper subgroup of $Q^*$ then $[P^*,H^*]\neq P^*$, since otherwise $O^p(P\vee H)=P\vee H<G$ 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 $\bar{Q}$ both operate in a natural way on $\Omega_1(Z^\sigma)$ and $G^* = Q^*\mathfrak{C}_{G^*}(\Omega_1(Z^\sigma))$, $\bar{G} = \bar{Q}\mathfrak{C}_{\bar{G}}(\Omega_1(Z^\sigma))$, 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 $\mho_{n-1}(Z^\sigma) = \Omega_1(Z^\sigma)$, 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 $\mathfrak{C}_{\bar{P}}(\bar{Q}) = 1$, $\bar{a} = 1$: 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 $\bar{Q}$) 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 $\langle h_i^* | i \in I\rangle = Q^*$. By an earlier remark $[P^*, h_i^*] < P^*$, and, if $h_i^* = h_i M^\sigma$ with $(|h_i|, p) = 1$, $O^p([P^\sigma, h_i]M^\sigma\langle h_i\rangle) = [P^\sigma, h_i]M^\sigma\langle h_i\rangle < G^\sigma$, which implies, by our choice of $G$, that $[Z^\sigma, h_i] \leqslant Z^\sigma \wedge ([P^\sigma, h_i]M^\sigma\langle h_i\rangle)$ is contained in the centre of $P^\sigma \wedge [P^\sigma, h_i]M^\sigma\langle h_i\rangle$, whence $[Z^\sigma, h_i] \leqslant \mathfrak{C}_{Z^\sigma}([L^\sigma, h_i])$.

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

$$\mathfrak{C}_{Z^\sigma}(h_i) = \mathfrak{C}_Z(g_i)^\sigma = \mathfrak{C}_Z(O^p(L\langle g_i\rangle))^\sigma = \mathfrak{C}_{Z^\sigma}(O^p(L^\sigma\langle h_i\rangle)) \leqslant \mathfrak{C}_{Z^\sigma}([L^\sigma, h_i])\,.$$

It then follows that $[L^\sigma, h_i, Z^\sigma] = 1$ and since $\langle h_i^* | i \in I\rangle = Q^*$, $[P^*, Q^*, Z^\sigma] = [P^*, Z^\sigma] = 1$, a contradiction. So assume $\bar{Q} = \langle \bar{h}\rangle$ with $|\bar{h}| = q^\tau$, $\tau \geqslant 1$; we have already seen that $\bar{h}$ has no invariant subspace on either $Z^\sigma/\Phi(Z^\sigma)$ or $\Omega_1(Z^\sigma)$ and that $[\bar{h}^q, \bar{P}] < \bar{P}$; we presently shall prove that $\bar{P}$ is $\bar{h}$-irreducible. Thus, suppose $\bar{P} = \bar{P}_1 \times \bar{P}_2$ is a proper $\bar{h}$-factorization; if $\bar{P}_i = P_i^\sigma/\mathfrak{C}_{G^\sigma}(Z^\sigma)$, $\bar{Q} = Q^\sigma/\mathfrak{C}_{G^\sigma}(Z^\sigma)$, $\bar{h} = h\mathfrak{C}_{G^\sigma}(Z^\sigma)$ with $p \nmid |h|$, then $Z^\sigma = [Z^\sigma, h] \leqslant O^p(P_i^\sigma Q^\sigma)$, so $Z$ is in the centre of $P \wedge O^p(P_iQ)$, a $p$-Sylow subgroup of $O^p(P_iQ)$, which implies $[Z^\sigma, P^\sigma \wedge O^p(P_i^\sigma Q^\sigma)] = 1$ (because $O^p(P_iQ)$ is normal and proper in $G$); if now $\bar{x} = x\mathfrak{C}_{G^\sigma}(Z^\sigma)$ with $x \in P^\sigma$ is any element of $\bar{P}_i$, there exists $\bar{y} = y\mathfrak{C}_{G^\sigma}(Z^\sigma)$ with $\bar{y} \in \bar{P}_i$, $\bar{x} = [\bar{y}, \bar{h}]$ and $[y, h] \in P^\sigma$: this means that $x = [y, h]c$ with $c \in \mathfrak{C}_{G^\sigma}(Z^\sigma)$, and eventually $[\bar{P}_i, Z^\sigma] = 1$, again a contradiction; in particular, $[\bar{h}^q, \bar{P}] = 1$. For the next step, we choose $y \in P^\sigma$, $y \notin \mathfrak{C}_{G^\sigma}(Z^\sigma)$, and we start with a detailed investigation of which are the possible structures for $\langle y\rangle Z^\sigma$. First of all, if $\langle x\rangle^\sigma = \langle y\rangle$, then $\langle x\rangle \wedge Z \neq 1$, since otherwise for every $z \in Z^\sigma$, $\langle z, y\rangle \wedge Z^\sigma = \langle z\rangle \lhd \langle z, y\rangle$, i.e. $y$ would operate on $Z^\sigma$ as a non-trivial power automorphism; further, $p^m = |x| \leqslant p^n$ would imply that every $z \in \Omega_1(Z)$, $z \neq 1$, has the same height in $Z$ as in $Z\langle x\rangle$, hence we could assume $Z\langle x\rangle = Z \times \langle x\rangle$

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 $\langle x\rangle \wedge Z \neq 1$; $\langle x\rangle$ is a direct factor of $Z\langle x\rangle$ and for $z \neq 1$ in a complement $S$ of $\langle x\rangle \wedge \Omega_1(Z)$ 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 $\langle v_i\rangle^\sigma = \langle w_i\rangle$, $\langle c\rangle^\sigma = \langle d\rangle$. We can also manage to get $v_0 = x^{p^{m-n}}c$ and $w_0 = y^{p^{m-n}}d$. $\langle y\rangle Z^\sigma$, 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 $u^t = u^{1+p^l}$ where $p^{l+1} = \exp A$, so that $(\langle y\rangle Z^\sigma)' = \mho_l(A)$ and $\langle y\rangle Z^\sigma$ has class 2. Suppose first that $\exp A > p^n$; in this case $(\langle y\rangle Z^\sigma)' = \Omega_1(\langle y\rangle)$, $\langle y\rangle \lhd \langle y\rangle Z^\sigma$, $|Z^\sigma : \mathfrak{C}_{Z^\sigma}(y)| = p$, and the matrix of $y$ on $Z$ (with entries from $\boldsymbol{Z}/p^n\boldsymbol{Z}$), for a suitable choice of the basis, is either

$$\text{(I)} \qquad \left(\begin{array}{c|c} 1+p^{n-1} & 0 \\ \hline 0 & \text{identity} \end{array}\right)$$

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

$$\text{(II)} \qquad \left(\begin{array}{c|c} \text{identity} & 0 \\ \hline p^{n-1}\ 0\ 0 \ldots 0 & 1 \end{array}\right)$$

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 $1 \leqslant i < k$ (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 $Z\langle x\rangle / A^{\sigma^{-1}}$ being cyclic implies that $v_1 = x^r g$ with $g \in A^{\sigma^{-1}}$, so that $1 \neq v_1^{p^{n-1}} = x^{rp^{n-1}} \in \langle v_0\rangle \wedge \wedge \langle v_1\rangle$. We now assume that $\exp A = p^n$, and remark that from $|t| \leqslant |y|$ and $y = t^r u$ with $u \in A$ it follows that $|y| = |t^r|$ and we can substitute $y$ for $t$. Moreover, we can replace $A$ with $U = A\langle y^{p^{m-n+1}}\rangle$: thus, $U$ is abelian and $u^y = u^{1+p^{n-1}}$ for every $u \in U$; but now $U$ has index $p$ in $\Omega_n(\langle y\rangle Z^\sigma) = U\langle y^{p^{m-n}}\rangle$, $Z^\sigma \nleqq U$, so that $|Z^\sigma : Z^\sigma \wedge U| = p$, and the last $k$ elements of a basis for $Z^\sigma$ can be chosen in $Z^\sigma \wedge U$ (remember that $\dim Z^\sigma = k+1$, and that $y^{p^{m-n}} \notin U$). The missing element of the basis of $Z^\sigma$ has the form $z = y^{rp^{m-n}} u$, with $p \nmid r$, $u \in U$, and we try to arrange the things so that $u^{p^{n-1}} \in \Omega_1(\langle y \rangle)$. Since $\Omega_1(Z^\sigma) = \langle y^{p^{m-1}} \rangle \times \mho_{n-1}(Z^\sigma \wedge U)$, we have $[z, y] = [u, y] = u^{p^{n-1}} = y^{sp^{m-1}} w^{p^{n-1}}$ with $w \in Z^\sigma \wedge U$, so $zw^{-1} = y^{rp^{m-n}}(uw^{-1})$ is congruent to $z$ modulo $Z^\sigma \wedge U$, $uw^{-1} \in U$, 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 $\mho_{n-1}(\langle z \rangle) = \Omega_1(\langle y \rangle) \geqslant \mho_{n-1}(\langle u \rangle)$, so that $[z, y] = [u, y] = u^{p^{n-1}} =: z^{\lambda p^{n-1}}$, and the matrix of $y$ on $Z^\sigma$ can be written either as

$$\text{(III)} \qquad \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & 1 + p^{n-1} \end{array}\right)$$

or as

$$\text{(IV)} \qquad \left(\begin{array}{c|c} 1 + \lambda p^{n-1} & 0 \\ \hline 0 & 1 + p^{n-1} \end{array}\right)$$

with $\lambda \not\equiv 0$, $\lambda \not\equiv 1 \pmod{p}$, where the right lower corner corresponds to the action of $y$ on $U \wedge Z^\sigma$. 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 $S \leqslant \mathfrak{C}_1(y) = \{z \in Z^\sigma | z^y = z^{1+p^{n-1}}\}$ there is nothing to prove; otherwise $|S: \mathfrak{C}_1(y) \wedge S| = p$, and we may assume that $u = w_0 c$, $w_0^y = w_0^{1+\lambda p^{n-1}}$ (where $\lambda \equiv 0$ under (III), $\lambda \not\equiv 0$, $\lambda \not\equiv 1$ under (IV)) $c \in \mathfrak{C}_1(y)$, $v \in \mathfrak{C}_1(y)$. $[u, y] = (w_0^\lambda c)^{p^{n-1}} \in S$, so $\langle w_0^{p^{n-1}} \rangle = \langle (w_0^{\lambda^{-1}})^{p^{n-1}} \rangle \leqslant \Omega_1(S)$; $w_0^{p^{n-1}} = (w_0 c)^{rp^{n-1}} v^{sp^{n-1}}$ and $\Omega_1(Z^\sigma) = \Omega_1(\langle w_0 \rangle) \times \mho_{n-1}(\mathfrak{C}_1(y))$ imply that $(c^r v^s)^{p^{n-1}} = 1$, $r \equiv 1 \pmod{p}$, whence $[u^r v^s, y] = w_0^{r\lambda p^{n-1}} = (u^r v^s)^{\lambda p^{n-1}}$, and $S = \langle u^r v^s \rangle \times \langle v \rangle$ with both factors $y$-invariant. We also remark that, if we look at the clements of $\bar{P}$ as linear $\mathbf{Z}/p^n\mathbf{Z}$ maps on $Z^\sigma$, then their determinant is 1, otherwise we would get $O^p(G^\sigma) < G^\sigma$; 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 $z_0, z_1$;

clearly we can choose $z_1 = z_0^h$, 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 $\alpha \equiv 0$, $\beta \not\equiv 0$ (mod. $p$), so if $a_i \in P^\sigma$ is such that $\overline{a_i} = \overline{a^i a^h}$ then $a_i$ is represented by

$$\begin{pmatrix} 1 & \beta p^{n-1} \\ i p^{n-1} & 1 \end{pmatrix} \quad ((i \not\equiv 0 (\text{mod.}\, p))$$

$\langle z_0^r z_1^s \rangle$ is $a_i$-invariant if there is $\mu$ such that $(z_0^r z_1^s)\mu p^{n-1} = [z_0^r z_1^s, a_i] = (z_0^{is} z_1{}^r)^{p^{n-1}} \cdot \mu \equiv 0$ implies $s \equiv 0 \equiv r$ (mod. $p$), i.e. $\mathfrak{C}_{Z^\sigma}(a_i) = \Phi(Z^\sigma)$; for $\mu \not\equiv 0$ we get $si\beta \equiv s\mu^2$ (mod. $p$), and either $s \equiv 0 \equiv r$ or $i\beta$ is a square in $F_p = \mathbf{Z}/p\mathbf{Z}$; 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 $\bar{a} \neq 1$ 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 $\alpha + \delta \equiv 0$ (mod. $p$); $a^h$ induces $1 + p^{n-1}$ on some

$\langle z_0^r z_1^s \rangle$ with $(r, s) \not\equiv (0, 0)$, i.e. $[z_0^r z_1^s, a^h] = (z_0^{r\alpha} z_1^{r\beta} z_0^{s\gamma} z_1^{s\delta})^{p^{n-1}} = (z_0^r z_1^s)^{p^{n-1}}$, which means that the linear system

$$\begin{cases} r(\alpha - 1) + s\gamma \equiv 0 \\ r\beta + s(\delta - 1) \equiv 0 \end{cases}$$

has a non trivial solution, and

$$\det\begin{pmatrix} \alpha - 1 & \gamma \\ \beta & \delta - 1 \end{pmatrix} \equiv \alpha\delta - \beta\gamma + 1 \equiv 0 \ (\text{mod.}\, p)\,.$$

Now take $a_i \in P^\sigma$ such that $\overline{a_i} = \overline{a^i a^h}$; it is represented by

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

it has to normalize two independent cyclic subgroups of $Z^\sigma$, so $[z_0^r z_1^s, a_i] = (z_0^{r(\alpha-i)} z_1^{r\beta} z_0^{s\gamma} z_1^{s(\delta+i)})^{p^{n-1}} = (z_0^r z_1^s)\mu p^{n-1}$ must be solvable with $(r, s) \not\equiv (0, 0)$ for two choices of $\mu$ not congruent mod. $p$, i.e.

$$\begin{pmatrix} \alpha - i & \beta \\ \gamma & \delta + i \end{pmatrix}$$

must have two distinct eigenvalues in $F_p$. The characteristic polynomial

$$\chi(\mu) = \det\begin{pmatrix} \alpha - i - \mu & \beta \\ \gamma & \delta + i - \mu \end{pmatrix} = \mu^2 - i^2 - 2\delta i - 1$$

has distinct roots in $F_p$ if and only if $\Delta(i) = i^2 + 2\delta i - 1 \in (F_p - \{0\})^2$; $\Delta(i) \equiv \Delta(j)$ if and only if $(i - j)(i + j + 2\delta) \equiv 0$ (mod. $p$), so the partition $\mathfrak{T}_\Delta$ associated with $\Delta$ is $\{\{-\delta\}, \{j, -j - 2\delta\}_{j \not\equiv -\delta}\}$ and has $(p+1)/2$ elements; $\Delta(0) = 1 \in (F_p - \{0\})^2$. If $0 \not\equiv -\delta$, then $|\Delta(F_p - \{0\})| = (p+1)/2$; if $0 \equiv -\delta$, then $|\Delta(F_p - \{0\})| = (p-1)/2$, but $1 \notin \Delta(F_p - \{0\})$: in any case, we can find $i \not\equiv 0$ (mod. $p$) 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 $a \in P^\sigma$ satisfying (II); since $[a, Z^\sigma] \wedge [a^h, Z^\sigma] = 1$, $\mathfrak{C}_{Z^\sigma}(a_i) = \mathfrak{C}^{\sim\vee}(a) \wedge \mathfrak{C}_{Z^\sigma}(a^h)$ 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 $P^\sigma$ satisfying either (III) or (IV), $\mathcal{C}_{Z^\sigma}(a^{-1}a^h) \geqslant \mathcal{C}_1(a) \wedge \mathcal{C}_1(a^h)$, where $\mathcal{C}_1(y) = \{z \in Z^\sigma | z^y = z^{1+p^{n-1}}\}$, which has index $p^2$ in $Z^\sigma$, so: if $|Z^\sigma : \mathcal{C}_{Z^\sigma}(a^{-1}a^h)| = p$, $a^{-1}a^h$ satisfies (II) and we have just proved that $\dim Z = 3$ in this case; if $|Z^\sigma : \mathcal{C}_{Z^\sigma}(a^{-1}a^h)| = p^2$, then $a^{-1}a^h$ satisfies (III) and once more $\dim Z = 3$. Suppose now that $a \in P^\sigma$, $\bar{a} \neq 1$, $a$ satisfies (II); with respect to a basis $z_0, z_1, z_2$ such that $\langle z_0 \rangle \geqslant \langle a \rangle \wedge Z^\sigma$, $\langle z_0, z_1 \rangle \Phi(Z^\sigma) = \mathcal{C}_{Z^\sigma}(a)$, $\langle z_2 \rangle = \langle z_0^h \rangle$, $a$ is represented by

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

$a^h$ 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 $\langle z_0, z_2 \rangle \wedge \mathcal{C}_{Z^\sigma}(a) \wedge \mathcal{C}_{Z^\sigma}(a^h) = \langle z_0, z_2^p \rangle$, i.e. $\alpha \equiv 0$, $\beta \not\equiv 0$ (mod. $p$); or $\langle z_0, z_2 \rangle \wedge \mathcal{C}_{Z^\sigma}(a) \wedge \mathcal{C}_{Z^\sigma}(a^h) = \Phi(\langle z_0, z_2 \rangle)$: if we choose $z_1$ such that $\langle z_1, \Phi(Z^\sigma) \rangle = \mathcal{C}_{Z^\sigma}(a) \wedge \mathcal{C}_{Z^\sigma}(a^h)$, then $\alpha \not\equiv 0$, $\beta \equiv 0$ (mod. $p$). In the former case $a_i$ is represented by

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

(symbols are as usual; $a_i$ must satisfy (III)); it centralizes $\langle z_0 \rangle$ and normalizes no other (independent) cyclic subgroup of $Z^\sigma$ of order $p^n$, a contradiction. In the latter case $a_i$ is represented by

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

it centralizes $\langle z_1 \rangle \Phi(Z^\sigma)$, and it should work as a power automorphism, $1 + \mu p^{n-1}$ say, $\mu \not\equiv 0$ (mod. $p$), on a direct product $S$ of two cyclic subgroups of order $p^n$; but $\langle z_0^r z_1^s z_2^t \rangle \leqslant S$ if and only if $(z_0^r z_1^s z_2^t)^{\mu p^{n-1}} = [z_0^r z_1^s z_2^t, a_i] = (z_2^{\alpha r} z_0^{it})^{p^{n-1}}$, i.e. if and only if $(r, s, t)$ is a solution of

$$\begin{cases} r\mu - it \equiv 0 \\ s\mu \equiv 0 \\ r\alpha - \mu t \equiv 0 \end{cases}$$

whose rank is $\geqslant 2$: there is one independent solution at most, a contradiction. So case (II) is ruled out. Now we assume $a \in P^{\sigma}$, $\bar{a} \neq 1$, $a$ satisfies (III); $\det a = 1 = 1 + 2p^{n-1}$ forces $p = 2$. $\mathfrak{C}_1(a)$ has index 2 in $Z^{\sigma}$; the same occurs to $\mathfrak{C}_1(a^h)$, so we can put $\mathfrak{C}_1(a) \wedge \mathfrak{C}_1(a^h) = \mathfrak{C}_{Z^{\sigma}}(aa^h) = \langle z_2 \rangle \Phi(Z^{\sigma})$; $aa^h$ also satisfies (III). With respect to a basis $z_0, z_1, z_2$ 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 $\langle z_0, z_0^h \rangle \Phi(Z^{\sigma}) = \langle z_0, z_2 \rangle \Phi(Z^{\sigma})$; we can choose $z_2$ so that $S = \langle z_0, z_0^h \rangle = \langle z_0, z_2 \rangle = \langle z_0^h, z_2 \rangle$. $S$ is $\langle a, a^h \rangle$-invariant, $\langle z_0^h \rangle \wedge \langle z_2 \rangle = 1$, so $z_0 = (z_0^h)^{\alpha} z_2$, $[z_0, a^h] = z_2^{2^{n-1}}$, $aa^h$ is represented on $S$ by

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

so $\langle z_2^{2^{n-1}} \rangle \leqslant [aa^h, Z^{\sigma}] \wedge \mho_{n-1}(\mathfrak{C}_{Z^{\sigma}}(aa^h))$: but under (III) this intersection is trivial. So we can assume that $\langle z_0^h \rangle \wedge \langle z_0, z_2 \rangle = 1$, and take $z_1' = z_0^h$ instead of $z_1$ in the basis (later on, we shall drop the apex); since we can always arrange that $z_0^h = z_0^{\delta} z_1$, 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 $\langle z_0 z_1^s z_2^t \rangle$: $(z_0 z_1^s z_2^t)^{2^{n-1}} = [z_0 z_1^s z_2^t, a^h] = (z_0 z_1^{\beta} z_2^{\gamma+t})^{2^{n-1}}$, so $\gamma + t \equiv t$, $\gamma \equiv 0 \pmod{2}$. $aa^h$, 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 $(z_0^r z_1^s z_2^t)^{2^{n-1}} = [z_0^r z_1^s z_2^t, aa^h] = (z_0^{r+s\delta} z_1^{r\beta-s})^{2^{n-1}}$ for $z_0^r z_1^s z_2^t \in S$, so that the system: $s\delta \equiv 0, r\beta \equiv 0, t \equiv 0$ has two independent solutions; this only happens if $\beta \equiv \delta \equiv 0$. 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

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

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

$$z_0\Phi(Z^\sigma) = \big(z_0\Phi(Z^\sigma)\big)^{h^2},$$

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

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

and on $Z^\sigma$ 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 $z_0, z_1 = z_0^h$, $z_2 = z_1^h$; moreover $\lambda = \det h = 1$. An easy calculation shows that $a^{h^2}$ 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 $b \in P^\sigma$, $\bar{b} = \overline{aa^{h^2}}$, $b$ 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 $z_1^h \equiv z_0 z_2 \ (\text{mod.}\ \Phi(Z^\sigma))$, a similar argument proves that $h$ is represented on $Z^\sigma/\Phi(Z^\sigma)$ by

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

and on $Z^\sigma$ by

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

where we refer to the basis $z_0$, $z_1 = z_0^h$, $z_2 = z_0^{h^{-1}}$; moreover $\nu = \det h = 1$. In this case $a^{h^2}$ 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 $p^\sigma$ satisfies (I), (II) nor (III); but if $a$ satisfies (IV), then $a^{-1}a^h$ 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 $Z(P)^\sigma$ of the centre $Z(P)$ of the $p$-Sylow-subgroup $P$ of $G$ is not contained in the centre of $P^\sigma$, then $\mathcal{N}_G(Z(P))$ has a proper normal subgroup $K$ such that $\mathcal{N}_G(Z(P))/K$ is a $p$-group.*

PROOF. Apply lemma 2.1 to $N = \mathcal{N}_G(Z(P))$.

**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 $P^\sigma$, then $O^p(G) \neq G$; in particular $G$ is not simple.*

Proof. Call $Z(P)$ the centre of $P$; 2.2 and the second theorem of Grün imply that $G/O^p(G) \cong \mathcal{N}_G(Z(P))/O^p\big(\mathcal{N}_G(Z(P))\big) \neq 1$, 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 $\sigma\colon G \to G^\sigma$ 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, $Z(P)^\sigma \leqslant Z(P^\sigma)$: 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 $\bar{\sigma}\colon G/A \to G^\sigma/B$ and by the minimality of $G$ (we now put $Z = Z(P)$)

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

so $[P^\sigma, Z^\sigma] \leqslant A^\sigma \wedge P^\sigma = 1$ against our choice of $G$. There exists a proper normal subgroup $N$ of $G$ such that $p \nmid |G:N|$; put $M = O^p(N)$, and let $Q$ be a complement of $P$ in $\mathcal{N}_G(P)$. $G = [P,Q]QM$: thus, $P \leqslant N$ and by the Frattini argument $G = \mathcal{N}_G(P)N = QPN = QN$; furthermore $N = PM$, whence $G = PQM$; but $[P,Q]Q = Q^P$, so $P \leqslant \mathcal{N}_G([P,Q]QM)$, i.e. $[P,Q]QM \trianglelefteq G$; $G/[P,Q]QM \cong P/[P,Q]QM \wedge P$ is a $p$-group, and eventually $G = [P,Q]QM$. Since $M \trianglelefteq QM$ and $p \nmid |QM:M|$, 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, $[P,Q]Q = O^p([P,Q]Q)$, $\mathfrak{C}_Z(Q)$ is a $p$-group contained in the centralizer of $[P,Q]Q$ so by 1.1 $\big[([P,Q]Q)^\sigma, \mathfrak{C}_Z(Q)^\sigma\big] = 1$; in particular $[[P,Q]^\sigma, \mathfrak{C}_Z(Q)^\sigma] = 1$. Furthermore $[Z,Q] \leqslant Z([P,Q])$; $[P,Q]$ is a $p$-Sylow subgroup of $[P,Q]Q$, so by 2.1 $[Z,Q]^\sigma \leqslant Z([P,Q]^\sigma)$; we can conclude that $[P,Q]^\sigma$ centralizes $\mathfrak{C}_Z(Q)^\sigma \vee [Z,Q]^\sigma = Z^\sigma$. Next we prove that $Z \nleqq M$; assume $Z \leqslant M$: then $Z \leqslant Z(P \wedge M)$ and, by the minimality of $G$, as $P \wedge M$ is a $p$-Sylow subgroup of $M < G$, $Z^\sigma \leqslant Z\big((P \wedge M)^\sigma\big)$: this fact, together with an earlier statement, implies the contradiction $[Z^\sigma, P^\sigma] = 1$. Let $F$ be the Fitting subgroup of $G$; under our assumptions $F$ is a nontrivial $p$-group, and $F \geqslant \mathfrak{C}_G(F)$ [1]. We also have $F \leqslant P \leqslant N$ and $[Z,F] = 1$ implies $Z \leqslant Z(F) \leqslant F$; whence $Z^G$ 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 $p \nmid |V_i/V_{i-1}|$ for $i = 1, \ldots, k$). We shall prove by induction that $[V_i, Z^G] = 1$. $V_1$ is a $p$-group, so $V_1 \leqslant F$ and $[V_1, Z^G] = 1$. Assume next $[V_r, Z^G] = 1$; if $p \nmid |V_{r+1}/V_r|$ we can write $Z^G = [Z^G, V_{r+1}] \times \mathcal{C}_{Z^G}(V_{r+1})$ where both factors are normal $p$-subgroups of $G = O^p(G)$; 1.1 then tells that $[Z^G, V_{r+1}]^\sigma$ and $\mathcal{C}_{Z^G}(V_{r+1})^\sigma$ are both normal in $G^\sigma$; if both are non-trivial by the minimality of $G$ $[P^\sigma, Z^\sigma] \leqslant [Z^G, V_{r+1}]^\sigma \wedge \mathcal{C}_{Z^G}(V_{r+1})^\sigma = 1$ against our choice of $G$. But if $\mathcal{C}_{Z^G}(V_{r+1}) = 1$, then $Z \leqslant Z^G = [Z^G, V_{r+1}] \leqslant V_{r+1} \leqslant M$ contradicting an earlier statement, so in this case $[Z^G, V_{r+1}] = 1$. In case $V_{r+1}/V_r$ is a $p$-group, $V_{r+1} = (P \wedge V_{r+1})\, V_r$; for every $x \in G$

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

$$= [P \wedge V_{r+1}, Z^{v^{-1}}]^{vx} = [P \wedge V_{r+1}, Z]^{vx} = 1$$

for a suitable $v \in V_r$; hence in this case too $[Z^G, V_{r+1}] = 1$. It follows that $[Z^G, M] = [Z^G, V_k] = 1$; $Z^G$ is a $p$-group, $M = O^p(M)$, so by 1.1 $[(Z^G)^\sigma, M^\sigma] = 1$, $\mathcal{C}_{G^\sigma}(Z^\sigma) \geqslant [P, Q]^\sigma M^\sigma \geqslant [P, Q]^\sigma (P \wedge M)^\sigma = P^\sigma$: 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

[1] D. GORENSTEIN, *Finite groups,* 1968.

[2] G. M. SEITZ - C. R. B. WRIGHT, *On finite groups whose Sylow subgroups are modular or quaternion-free,* Journal of Algebra, **13** (1969), 374-381.

[3] M. SUZUKI, *Structure of a group and the structure of its lattice of subgroups,* 1956.

Manoscritto pervenuto in redazione il 23 aprile 1974.