CHAPTER II

6. Preliminary Lemmas of Lie Type

Hypothesis 6.1.

(i) *p is a prime, $\mathfrak{P}$ is a normal S_p-subgroup of $\mathfrak{P}\mathfrak{U}$, and $\mathfrak{U}$ is a non identity cyclic p'-group.*

(ii) $C_{\mathfrak{U}}(\mathfrak{P}) = 1$.

(iii) *$\mathfrak{P}'$ is elementary abelian and $\mathfrak{P}' \subseteq \boldsymbol{Z}(\mathfrak{P})$.*

(iv) *$|\mathfrak{P}\mathfrak{U}|$ is odd.*

Let $\mathfrak{U} = \langle U \rangle$, $|\mathfrak{U}| = u$, and $|\mathfrak{P} : D(\mathfrak{P})| = p^n$. Let $\mathscr{L}$ be the Lie ring associated to $\mathfrak{P}$ ([12] p. 328). Then $\mathscr{L} = \mathscr{L}_1^* \oplus \mathscr{L}_2$ where $\mathscr{L}_1^*$ and $\mathscr{L}_2$ correspond to $\mathfrak{P}/\mathfrak{P}'$ and $\mathfrak{P}'$ respectively. Let $\mathscr{L}_1 = \mathscr{L}_1^*/p\mathscr{L}_1^*$. For $i = 1, 2$, let U_i be the linear transformation induced by U on $\mathscr{L}_i$.

LEMMA 6.1. *Assume that Hypothesis 6.1 is satisfied. Let $\varepsilon_1, \cdots, \varepsilon_n$ be the characteristic roots of U_1. Then the characteristic roots of U_2 are found among the elements $\varepsilon_i\varepsilon_j$ with $1 \leqq i < j \leqq n$.*

Proof. Suppose the field is extended so as to include $\varepsilon_1, \cdots, \varepsilon_n$. Since $\mathfrak{U}$ is a p'-group, it is possible to find a basis $x_1, \cdots, x_n$ of $\mathscr{L}_1$ such that $x_iU_1 = \varepsilon_i x_i$, $1 \leqq i \leqq n$. Therefore, $x_iU_1 \cdot x_jU_1 = \varepsilon_i\varepsilon_j x_i \cdot x_j$. As U induces an automorphism of $\mathscr{L}$, this yields that

$$(x_i \cdot x_j)U_2 = x_iU_1 \cdot x_jU_1 = \varepsilon_i\varepsilon_j x_i \cdot x_j\ .$$

Since the vectors $x_i \cdot x_j$ with $i < j$ span $\mathscr{L}_2$, the lemma follows.

By using a method which differs from that used below, M. Hall proved a variant of Lemma 6.2. We are indebted to him for showing us his proof.

LEMMA 6.2. *Assume that Hypothesis 6.1 is satisfied, and that U_1 acts irreducibly on $\mathscr{L}_1$. Assume further that $n = q$ is an odd prime and that U_1 and U_2 have the same characteristic polynomial. Then $q > 3$ and*

$$u < 3^{q/2}$$

Proof. Let ε^{p^i} be the characteristic roots of U_1, $0 \leqq i < n$. By Lemma 6.1 there exist integers i, j, k such that $\varepsilon^{p^i}\varepsilon^{p^j} = \varepsilon^{p^k}$. Raising this equation to a suitable power yields the existence of integers a and b with $0 \leqq a < b < q$ such that $\varepsilon^{p^a + p^b - 1} = 1$. By Hypothesis 6.1 (ii), the preceding equality implies $p^a + p^b - 1 \equiv 0 (\mathrm{mod}\ u)$. Since U_1 acts irreducibly, we also have $p^q - 1 \equiv 0 (\mathrm{mod}\ u)$. Since $\mathfrak{U}$ is a p'-group,

$ab \neq 0$. Consequently,

$$(6.1)\qquad \begin{aligned} &p^a + p^b - 1 \equiv 0 (\mathrm{mod}\ u)\ , \\ &p^q - 1 \equiv 0(\mathrm{mod}\, u),\ 0 < a < b < q\ . \end{aligned}$$

Let d be the resultant of the polynomials $f = x^a + x^b - 1$ and $g = x^q - 1$. Since q is a prime, the two polynomials are relatively prime, so d is a nonzero integer. Also, by a basic property of resultants,

$$(6.2)\qquad d = hf + kg$$

for suitable integral polynomials h and k.

Let ε_q be a primitive qth root of unity over $\mathscr{Q}$, so that we also have

$$(6.3)\qquad \begin{aligned} d^2 &= \prod_{i=0}^{q-1} (\varepsilon_q^{ia} + \varepsilon_q^{ib} - 1) \prod_{i=0}^{q-1} (\varepsilon_q^{-ia} + \varepsilon_q^{-ib} - 1) \\ &= \prod_{i=0}^{q-1} \{3 + \varepsilon_q^{i(a-b)} + \varepsilon_q^{i(b-a)} - \varepsilon_q^{ia} - \varepsilon_q^{ib} - \varepsilon_q^{-ib} - \varepsilon_q^{-ia}\}\ . \end{aligned}$$

For $q = 3$, this yields that $d^2 = (3 - 1 + 1 + 1)^2 = 4^2$, so that $d = \pm 4$. Since u is odd (6.1) and (6.2) imply that $u = 1$. This is not the case, so $q > 3$.

Each term on the right hand side of (6.3) is non negative. As the geometric mean of non negative numbers is at most the arithmetic mean, (6.3) implies that

$$d^{2/q} \leqq \frac{1}{q} \sum_{i=0}^{q-1} \{3 + \varepsilon_q^{i(a-b)} + \varepsilon_q^{i(b-a)} - \varepsilon_q^{ia} - \varepsilon_q^{-ia} - \varepsilon_q^{ib} - \varepsilon_q^{-ib}\}\ .$$

The algebraic trace of a primitive qth root of unity is -1, hence

$$d^{2/q} \leqq 3\ .$$

Now (6.1) and (6.2) imply that

$$u \leqq |d| \leqq 3^{q/2}\ .$$

Since $3^{q/2}$ is irrational, equality cannot hold.

LEMMA 6.3. *If $\mathfrak{P}$ is a p-group and $\mathfrak{P}' = D(\mathfrak{P})$, then $C_n(\mathfrak{P})/C_{n+1}(\mathfrak{P})$ is elementary abelian for all n.*

Proof. The assertion follows from the congruence

$$[A_1, \cdots, A_n]^p \equiv [A_1, \cdots, A_{n-1}, A_n^p] (\mathrm{mod}\ C_{n+1}(\mathfrak{P}))\ ,$$

valid for all $A_1, \cdots, A_n$ in $\mathfrak{P}$.

LEMMA 6.4. *Suppose that σ is a fixed point free p'-automorphism* *of the p-group* $\mathfrak{P}$, $\mathfrak{P}' = D(\mathfrak{P})$ *and* $A^\sigma \equiv A^x (\operatorname{mod} \mathfrak{P}')$ *for some integer* x *independent of* A. *Then* $\mathfrak{P}$ *is of exponent* p.

Proof. Let $A^\sigma = A^x \cdot A^\phi$ so that A^ϕ is in $\mathfrak{P}'$ for all A in $\mathfrak{P}$. Then

$$\begin{aligned}[A_1, \cdots, A_n]^\sigma &= [A_1^\sigma, \cdots, A_n^\sigma] = [A_1^x \cdot A_1^\phi, \cdots, A_n^x \cdot A_n^\phi] \\ &\equiv [A_1^x, \cdots, A_n^x] \equiv [A_1, \cdots, A_n]^{x^n} (\operatorname{mod}\ C_{n+1}(\mathfrak{P})) .\end{aligned}$$

Since σ is regular on $\mathfrak{P}$, σ is also regular on each C_n/C_{n+1}. As the order of σ divides $p-1$ the above congruences now imply that $\operatorname{cl}(\mathfrak{P}) \leqq p-1$ and so $\mathfrak{P}$ is a regular p-group. If $\mho^1(\mathfrak{P}) \neq 1$, then the mapping $A \longrightarrow A^p$ induces a non zero linear map of $\mathfrak{P}/D(\mathfrak{P})$ to $C_n(\mathfrak{P})/C_{n+1}(\mathfrak{P})$ for suitable n. Namely, choose n so that $\mho^1(\mathfrak{P}) \subseteq C_n(\mathfrak{P})$ but $\mho^1(\mathfrak{P}) \nsubseteq C_{n+1}(\mathfrak{P})$, and use the regularity of $\mathfrak{P}$ to guarantee linearity. Notice that $n \geqq 2$, since by hypothesis $\mho^1(\mathfrak{P}) \subseteq \mathfrak{P}'$. We find that $x \equiv x^n (\operatorname{mod} p)$, and so $x^{n-1} \equiv 1 (\operatorname{mod} p)$ and σ has a fixed point on C_{n-1}/C_n, contrary to assumption. Hence, $\mho^1(\mathfrak{P}) = 1$.

7. Preliminary Lemmas of Hall-Higman Type

Theorem B of Hall and Higman [21] is used frequently and will be referred to as (B).

LEMMA 7.1. *If* $\mathfrak{X}$ *is a p-solvable linear group of odd order over a field of characteristic p, then* $O_p(\mathfrak{X})$ *contains every element whose minimal polynomial is* $(x-1)^2$.

Proof. Let $\mathscr{V}$ be the space on which $\mathfrak{X}$ acts. The hypotheses of the lemma, together with (B), guarantee that either $O_p(\mathfrak{X}) \neq 1$ or $\mathfrak{X}$ contains no element whose minimal polynomial is $(x-1)^2$.

Let X be an element of $\mathfrak{X}$ with minimal polynomial $(x-1)^2$. Then $O_p(\mathfrak{X}) \neq 1$, and the subspace $\mathscr{V}_0$ which is elementwise fixed by $O_p(\mathfrak{X})$ is proper and is $\mathfrak{X}$-invariant. Since $O_p(\mathfrak{X})$ is a p-group, $\mathscr{V}_0 \neq 0$. Let

$$\mathfrak{K}_0 = \ker(\mathfrak{X} \longrightarrow \operatorname{Aut} \mathscr{V}_0) , \qquad \mathfrak{K}_1 = \ker(\mathfrak{X} \longrightarrow \operatorname{Aut}(\mathscr{V}/\mathscr{V}_0)) .$$

By induction on $\dim \mathscr{V}$, $X \in O_p(\mathfrak{X} \operatorname{mod} \mathfrak{K}_i)$, $i = 0, 1$. Since

$$O_p(\mathfrak{X} \operatorname{mod} \mathfrak{K}_0) \cap O_p(\mathfrak{X} \operatorname{mod} \mathfrak{K}_1)$$

is a p-group, the lemma follows.

LEMMA 7.2. *Let* $\mathfrak{X}$ *be a p-solvable group of odd order, and* $\mathfrak{A}$ *a p-subgroup of* $\mathfrak{X}$. *Any one of the following conditions guarantees that* $\mathfrak{A} \subseteq O_{p',p}(\mathfrak{X})$:

1. *$\mathfrak{A}$ is abelian and $|\mathfrak{X} : N(\mathfrak{A})|$ is prime to p.*
2. *$p \geqq 5$ and $[\mathfrak{P}, \mathfrak{A}, \mathfrak{A}, \mathfrak{A}, \mathfrak{A}] = 1$ for some S_p-subgroup $\mathfrak{P}$ of $\mathfrak{X}$.*
3. *$[\mathfrak{P}, \mathfrak{A}, \mathfrak{A}] = 1$ for some S_p-subgroup $\mathfrak{P}$ of $\mathfrak{X}$.*
4. *$\mathfrak{A}$ acts trivially on the factor $O_{p',p,p'}(\mathfrak{X})/O_{p',p}(\mathfrak{X})$.*

Proof. Conditions 1, 2, or 3 imply that each element of $\mathfrak{A}$ has a minimal polynomial dividing $(x-1)^{p-1}$ on $O_{p',p}(\mathfrak{X})/\mathfrak{D}$, where $\mathfrak{D} = D(O_{p',p}(\mathfrak{X}) \bmod O_{p'}(\mathfrak{X}))$. Thus (B) and the oddness of $|\mathfrak{X}|$ yield 1, 2, and 3. Lemma 1.2.3 of [21] implies 4.

LEMMA 7.3. *If $\mathfrak{X}$ is p-solvable, and $\mathfrak{P}$ is a S_p-subgroup of $\mathfrak{X}$, then $\mathsf{M}(\mathfrak{P})$ is a lattice whose maximal element is $O_{p'}(\mathfrak{X})$.*

Proof. Since $O_{p'}(\mathfrak{X}) \lhd \mathfrak{X}$ and $\mathfrak{P} \cap O_{p'}(\mathfrak{X}) = 1$, $O_{p'}(\mathfrak{X})$ is in $\mathsf{M}(\mathfrak{P})$. Thus it suffices to show that if $\mathfrak{H} \in \mathsf{M}(\mathfrak{P})$, then $\mathfrak{H} \subseteq O_{p'}(\mathfrak{X})$. Since $\mathfrak{P}\mathfrak{H}$ is a group of order $|\mathfrak{P}|\cdot|\mathfrak{H}|$ and $\mathfrak{P}$ is a S_p-subgroup of $\mathfrak{X}$, $\mathfrak{H}$ is a p'-group, as is $\mathfrak{H}O_{p'}(\mathfrak{X})$. In proving the lemma, we can therefore assume that $O_{p'}(\mathfrak{X}) = 1$, and try to show that $\mathfrak{H} = 1$. In this case, $\mathfrak{H}$ is faithfully represented as automorphisms of $O_p(\mathfrak{X})$, by Lemma 1.2.3 of [21]. Since $O_p(\mathfrak{X}) \subseteq \mathfrak{P}$, we see that $[\mathfrak{H}, O_p(\mathfrak{X})] \subseteq \mathfrak{H} \cap \mathfrak{P}$, and $\mathfrak{H} = 1$ follows.

LEMMA 7.4. *Suppose $\mathfrak{P}$ is a S_p-subgroup of $\mathfrak{X}$ and $\mathfrak{A} \in \mathscr{SCN}(\mathfrak{P})$. Then $\mathsf{M}(\mathfrak{A})$ contains only p'-groups. If in addition, $\mathfrak{X}$ is p-solvable, then $\mathsf{M}(\mathfrak{A})$ is a lattice whose maximal element is $O_{p'}(\mathfrak{X})$.*

Proof. Suppose $\mathfrak{A}$ normalizes $\mathfrak{H}$ and $\mathfrak{A} \cap \mathfrak{H} = \langle 1 \rangle$. Let $\mathfrak{A}^*$ be a S_p-subgroup of $\mathfrak{A}\mathfrak{H}$ containing $\mathfrak{A}$. By Sylow's theorem, $\mathfrak{P}_1 = \mathfrak{A}^* \cap \mathfrak{H}$ is a S_p-subgroup of $\mathfrak{H}$. It is clearly normalized by $\mathfrak{A}$, and $\mathfrak{A} \cap \mathfrak{P}_1 = \langle 1 \rangle$. If $\mathfrak{P}_1 \neq \langle 1 \rangle$, a basic property of p-groups implies that $\mathfrak{A}$ centralizes some non identity element of $\mathfrak{P}_1$, contrary to 3.10. Thus, $\mathfrak{P}_1 = \langle 1 \rangle$ and $\mathfrak{H}$ is a p'-group. Hence we can assume that $\mathfrak{X}$ is p-solvable and that $O_{p'}(\mathfrak{X}) = \langle 1 \rangle$ and try to show that $\mathfrak{H} = \langle 1 \rangle$.

Let $\mathfrak{X}_1 = O_p(\mathfrak{X})\mathfrak{H}\mathfrak{A}$. Then $O_p(\mathfrak{X})\mathfrak{A}$ is a S_p-subgroup of $\mathfrak{X}_1$, and $\mathfrak{A} \in \mathscr{SCN}(O_p(\mathfrak{X})\mathfrak{A})$. If $\mathfrak{X}_1 \subset \mathfrak{X}$, then by induction $\mathfrak{H} \subseteq O_{p'}(\mathfrak{X}_1)$ and so $[O_p(\mathfrak{X}), \mathfrak{H}] \subseteq O_p(\mathfrak{X}) \cap O_{p'}(\mathfrak{X}_1) = 1$ and $\mathfrak{H} = 1$. We can suppose that $\mathfrak{X}_1 = \mathfrak{X}$.

If $\mathfrak{A}$ centralizes $\mathfrak{H}$, then clearly $\mathfrak{A} \lhd \mathfrak{X}$, and so $\ker(\mathfrak{X} \longrightarrow \operatorname{Aut}\mathfrak{A}) = \mathfrak{A} \times \mathfrak{H}_1$, by 3.10 where $\mathfrak{H} \subseteq \mathfrak{H}_1$. Hence, $\mathfrak{H}_1$ char $\mathfrak{A} \times \mathfrak{H}_1 \lhd \mathfrak{X}$, and $\mathfrak{H}_1 \lhd \mathfrak{X}$, so that $\mathfrak{H}_1 = 1$. We suppose that $\mathfrak{A}$ does not centralize $\mathfrak{H}$, and that $\mathfrak{H}$ is an elementary q-group on which $\mathfrak{A}$ acts irreducibly. Let $\mathfrak{B} = O_p(\mathfrak{X})/D(O_p(\mathfrak{X})) = \mathfrak{B}_1 \times \mathfrak{B}_2$, where $\mathfrak{B}_1 = C_{\mathfrak{B}}(\mathfrak{H})$ and $\mathfrak{B}_2 = [\mathfrak{B}, \mathfrak{H}]$. Let $V \in \mathfrak{B}_2$ and $X \in V$, so that $[X, \mathfrak{A}] \subseteq \mathfrak{A}$. Hence, $[X, \mathfrak{A}]$ maps into $\mathfrak{B}_1$, since $[[X, \mathfrak{A}], \mathfrak{H}] \subseteq \mathfrak{H} \cap O_p(\mathfrak{X}) = 1$. But $\mathfrak{B}_2$ is $\mathfrak{X}$-invariant, so $[X, \mathfrak{A}]$ maps into $\mathfrak{B}_1 \cap \mathfrak{B}_2 = 1$. Thus, $\mathfrak{A} \subseteq \ker(\mathfrak{X} \longrightarrow \operatorname{Aut}\mathfrak{B}_2)$, and so $[\mathfrak{A}, \mathfrak{H}]$

centralizes $\mathfrak{B}_2$. As $\mathfrak{A}$ acts irreducibly on $\mathfrak{H}$, we have $\mathfrak{H} = [\mathfrak{H}, \mathfrak{A}]$, so $\mathfrak{B}_2 = 1$. Thus, $\mathfrak{H}$ centralizes $\mathfrak{B}$ and so centralizes $O_p(\mathfrak{X})$, so $\mathfrak{H} = 1$, as required.

LEMMA 7.5. *Suppose $\mathfrak{H}$ and $\mathfrak{H}_1$ are $S_{p,q}$-subgroups of the solvable group $\mathfrak{S}$. If $\mathfrak{B} \subseteq O_p(\mathfrak{H}_1) \cap \mathfrak{H}$, then $\mathfrak{B} \subseteq O_p(\mathfrak{H})$.*

Proof. We proceed by induction on $|\mathfrak{S}|$. We can suppose that $\mathfrak{S}$ has no non identity normal subgroup of order prime to pq. Suppose that $\mathfrak{S}$ possesses a non identity normal p-subgroup $\mathfrak{J}$. Then

$$\mathfrak{J} \subseteq O_p(\mathfrak{H}) \cap O_p(\mathfrak{H}_1) .$$

Let $\bar{\mathfrak{S}} = \mathfrak{S}/\mathfrak{J}$, $\bar{\mathfrak{B}} = \mathfrak{B}\mathfrak{J}/\mathfrak{J}$, $\bar{\mathfrak{H}} = \mathfrak{H}/\mathfrak{J}$, $\bar{\mathfrak{H}}_1 = \mathfrak{H}_1/\mathfrak{J}$. By induction, $\bar{\mathfrak{B}} \subseteq O_p(\bar{\mathfrak{H}})$, so $\mathfrak{B} \subseteq O_p(\mathfrak{H} \bmod \mathfrak{J}) = O_p(\mathfrak{H})$, and we are done. Hence, we can assume that $O_p(\mathfrak{S}) = \langle 1 \rangle$. In this case, $F(\mathfrak{S})$ is a q-group, and $F(\mathfrak{S}) \subseteq \mathfrak{H}_1$. By hypothesis, $\mathfrak{B} \subseteq O_p(\mathfrak{H}_1)$, and so $\mathfrak{B}$ centralizes $F(\mathfrak{S})$. By 3.3, we see that $\mathfrak{B} = \langle 1 \rangle$, so $\mathfrak{B} \subseteq O_p(\mathfrak{H})$ as desired.

The next two lemmas deal with a S_p-subgroup $\mathfrak{P}$ of the p-solvable group $\mathfrak{X}$ and with the set

$\mathscr{S} = \{\mathfrak{H} \mid$ 1. $\mathfrak{H}$ is a subgroup of $\mathfrak{X}$.
2. $\mathfrak{P} \subseteq \mathfrak{H}$.
3. The p-length of $\mathfrak{H}$ is at most two .
4. $|\mathfrak{H}|$ is not divisible by three distinct primes .$\}$

LEMMA 7.6. $\mathfrak{X} = \langle \mathfrak{H} \mid \mathfrak{H} \in \mathscr{S} \rangle$.

Proof. Let $\mathfrak{X}_1 = \langle \mathfrak{H} \mid \mathfrak{H} \in \mathscr{S} \rangle$. It suffices to show that $|\mathfrak{X}_1|_q = |\mathfrak{X}|_q$ for every prime q. This is clear if $q = p$, so suppose $q \neq p$. Since $\mathfrak{X}$ is p-solvable, $\mathfrak{X}$ satisfies $E_{p\,q}$, so we can suppose that $\mathfrak{X}$ is a p, q-group. By induction, we can suppose that $\mathfrak{X}_1$ contains every proper subgroup of $\mathfrak{X}$ which contains $\mathfrak{P}$. Since $\mathfrak{P}O_q(\mathfrak{X}) \in \mathscr{S}$, we see that $O_q(\mathfrak{X}) \subseteq \mathfrak{X}_1$. If $N(\mathfrak{P} \cap O_{q\,p}(\mathfrak{X})) \subset \mathfrak{X}$, then $N(\mathfrak{P} \cap O_p(\mathfrak{X})) \subseteq \mathfrak{X}_1$. Since $\mathfrak{X} = O_q(\mathfrak{X}) \cdot N(\mathfrak{P} \cap O_{q\,p}(\mathfrak{X}))$, we have $\mathfrak{X} = \mathfrak{X}_1$. Thus, we can assume that $O_p(\mathfrak{X}) = \mathfrak{P} \cap O_{q\,p}(\mathfrak{X})$. Since $\mathfrak{P}O_{p,q}(\mathfrak{X}) \in \mathscr{S}$, we see that $O_{p,q}(\mathfrak{X}) \subseteq \mathfrak{X}_1$. If $\mathfrak{P}O_{p\,q}(\mathfrak{X}) = \mathfrak{X}$, we are done, so suppose not. Then $N(\mathfrak{P} \cap O_{p,q\,p}(\mathfrak{X})) \subset \mathfrak{X}$, so that $\mathfrak{X}_1$ contains $N(\mathfrak{P} \cap O_{p,q\,p}(\mathfrak{X}))O_{p\,q}(\mathfrak{X}) = \mathfrak{X}$, as required.

LEMMA 7.7. *Suppose $\mathfrak{M}, \mathfrak{N}$ are subgroups of $\mathfrak{X}$ which contain $\mathfrak{P}$ such that $\mathfrak{H} = (\mathfrak{H} \cap \mathfrak{M})(\mathfrak{H} \cap \mathfrak{N})$ for all $\mathfrak{H}$ in $\mathscr{S}$. Then $\mathfrak{X} = \mathfrak{M}\mathfrak{N}$.*

Proof. It suffices to show that $|\mathfrak{M}\mathfrak{N}|_q \geq |\mathfrak{X}|_q$ for every prime q. This is clear if $q = p$, so suppose $q \neq p$. Let $\mathfrak{Q}_1$ be a S_q-subgroup of

$\mathfrak{M} \cap \mathfrak{N}$ permutable with $\mathfrak{P}$, which exists by $E_{p,q}$ in $\mathfrak{M} \cap \mathfrak{N}$. Since $\mathfrak{X}$ satisfies $D_{p,q}$, there is a S_q-subgroup $\mathfrak{Q}$ of $\mathfrak{X}$ which contains $\mathfrak{Q}_1$ and is permutable with $\mathfrak{P}$, Set $\mathfrak{R} = \mathfrak{P}\mathfrak{Q}$. We next show that

$$\mathfrak{R} = (\mathfrak{R} \cap \mathfrak{M})(\mathfrak{R} \cap \mathfrak{N}) .$$

If $\mathfrak{R} \in \mathscr{S}$, this is the case by hypothesis, so we can suppose the p-length of $\mathfrak{R}$ is at least 3. Let $\mathfrak{P}_1 = \mathfrak{P} \cap O_{p,q,p}(\mathfrak{R})$, and $\mathfrak{L} = N_{\mathfrak{R}}(\mathfrak{P}_1)$. Then $\mathfrak{L}$ is a proper subgroup of $\mathfrak{R}$ so by induction on $|\mathfrak{X}|$, we have $\mathfrak{L} = (\mathfrak{L} \cap \mathfrak{M})(\mathfrak{L} \cap \mathfrak{N})$. Let $\mathfrak{K} = \mathfrak{P} \cdot O_{p,q,p}(\mathfrak{R}) = \mathfrak{P}O_{p,q}(\mathfrak{R})$. Since $\mathfrak{K}$ is in $\mathscr{S}$, we have $\mathfrak{K} = (\mathfrak{K} \cap \mathfrak{M})(\mathfrak{K} \cap \mathfrak{N})$. Furthermore, by Sylow's theorem, $\mathfrak{R} = \mathfrak{K}\mathfrak{L}$. Let $R \in \mathfrak{R}$. Then $R = KL$ with $K \in \mathfrak{K}$, $L \in \mathfrak{L}$. Then $K = PK_1$, with P in $\mathfrak{P}$, K_1 in $O_{p,q}(\mathfrak{R})$. Also, $L = MN$, M in $\mathfrak{L} \cap \mathfrak{M}$, N in $\mathfrak{L} \cap \mathfrak{N}$, and so $R = KL = PK_1MN = PMK_1^M N$. Since $K_1^M \in O_{p,q}(\mathfrak{R})$, we have $K_1^M = M_1N_1$ with M_1 in $\mathfrak{M} \cap \mathfrak{K}$, N_1 in $\mathfrak{N} \cap \mathfrak{K}$. Hence, $R = PMM_1 \cdot N_1N$ with PMM_1 in $\mathfrak{M} \cap \mathfrak{R}$, N_1N in $\mathfrak{N} \cap \mathfrak{R}$.

Since $\mathfrak{R} = (\mathfrak{R} \cap \mathfrak{M})(\mathfrak{R} \cap \mathfrak{N})$, we have

$$|\mathfrak{X}|_q = |\mathfrak{R}|_q = \frac{|\mathfrak{R} \cap \mathfrak{M}|_q \cdot |\mathfrak{R} \cap \mathfrak{N}|_q}{|\mathfrak{R} \cap \mathfrak{M} \cap \mathfrak{N}|_q} .$$

By construction, $|\mathfrak{R} \cap \mathfrak{M} \cap \mathfrak{N}|_q = |\mathfrak{M} \cap \mathfrak{N}|_q$. Furthermore, $|\mathfrak{R} \cap \mathfrak{M}|_q \leqq |\mathfrak{M}|_q$ and $|\mathfrak{R} \cap \mathfrak{N}|_q \leqq |\mathfrak{N}|_q$, so

$$|\mathfrak{M}\mathfrak{N}|_q = \frac{|\mathfrak{M}|_q|\mathfrak{N}|_q}{|\mathfrak{M} \cap \mathfrak{N}|_q} \geqq \frac{|\mathfrak{R} \cap \mathfrak{M}|_q \cdot |\mathfrak{R} \cap \mathfrak{N}|_q}{|\mathfrak{R} \cap \mathfrak{M} \cap \mathfrak{N}|_q} = |\mathfrak{X}|_q ,$$

completing the proof.

LEMMA 7.8. *Let $\mathfrak{X}$ be a finite group and $\mathfrak{H}$ a p'-subgroup of $\mathfrak{X}$ which is normalized by the p-subgroup $\mathfrak{A}$ of $\mathfrak{X}$. Set $\mathfrak{A}_1 = C_{\mathfrak{A}}(\mathfrak{H})$. Suppose $\mathfrak{L}$ is a p-solvable subgroup of $\mathfrak{X}$ containing $\mathfrak{A}\mathfrak{H}$ and $\mathfrak{H} \not\subseteq O_{p'}(\mathfrak{L})$. Then there is a p-solvable subgroup $\mathfrak{K}$ of $\mathfrak{A}C_{\mathfrak{X}}(\mathfrak{A}_1)$ which contains $\mathfrak{A}\mathfrak{H}$ and $\mathfrak{H} \not\subseteq O_{p'}(\mathfrak{K})$.*

Proof. Let $\mathfrak{F} = O_{p',p}(\mathfrak{L})/O_{p'}(\mathfrak{L})$. Then $\mathfrak{H}$ does not centralize $\mathfrak{F}$. Let $\mathfrak{B}$ be a subgroup of $\mathfrak{F}$ which is minimal with respect to being $\mathfrak{A}\mathfrak{H}$-invariant and not centralized by $\mathfrak{H}$. Then $\mathfrak{B} = [\mathfrak{B}, \mathfrak{H}]$, and $[\mathfrak{B}, \mathfrak{A}_1] \subseteq D(\mathfrak{B})$, while $[D(\mathfrak{B}), \mathfrak{H}] = 1$. Hence, $[\mathfrak{B}, \mathfrak{A}_1, \mathfrak{H}] = [\mathfrak{A}_1, \mathfrak{H}, \mathfrak{B}] = 1$, and so $[\mathfrak{H}, \mathfrak{B}, \mathfrak{A}_1] = 1$. Since $[\mathfrak{H}, \mathfrak{B}] = \mathfrak{B}$, $\mathfrak{A}_1$ centralizes $\mathfrak{B}$. Since $\mathfrak{B}$ is a subgroup of $\mathfrak{F}$, we have $\mathfrak{B} = \mathfrak{L}_0/O_{p'}(\mathfrak{L})$ for suitable $\mathfrak{L}_0$. As $O_{p'}(\mathfrak{L})$ is a p'-group and $\mathfrak{B}$ is a p-group, we can find an $\mathfrak{A}$-invariant p-subgroup $\mathfrak{P}_0$ of $\mathfrak{L}_0$ incident with $\mathfrak{B}$. Hence, $\mathfrak{A}_1$ centralizes $\mathfrak{P}_0$. Set

$$\mathfrak{K} = \langle \mathfrak{A}, \mathfrak{P}_0, \mathfrak{H} \rangle \subseteq \mathfrak{L} .$$

As $\mathfrak{L}$ is p-solvable so is $\mathfrak{K}$. If $\mathfrak{H} \subseteq O_{p'}(\mathfrak{K})$, then

$$[\mathfrak{P}_0, \mathfrak{H}] \subseteq \mathfrak{L}_0 \cap O_{p'}(\mathfrak{K}) \subseteq O_{p'}(\mathfrak{L})$$

and $\mathfrak{H}$ centralizes $\mathfrak{B}$, contrary to construction. Thus, $\mathfrak{H} \not\subseteq O_{p'}(\mathfrak{K})$, as required.

LEMMA 7.9. *Let $\mathfrak{H}$ be a p-solvable subgroup of the finite group $\mathfrak{X}$, and let $\mathfrak{P}$ be a S_p-subgroup of $\mathfrak{H}$. Assume that one of the following conditions holds:*

(a) $|\mathfrak{X}|$ *is odd.*

(b) $p \geqq 5$.

(c) $p = 3$ *and a S_2-subgroup of $\mathfrak{H}$ is abelian.*

Let $\mathfrak{P}_0 = O_{p',p}(\mathfrak{H}) \cap \mathfrak{P}$ and let $\mathfrak{P}^*$ be a p-subgroup of $\mathfrak{X}$ containing $\mathfrak{P}$. If $\mathfrak{P}$ is a S_p-subgroup of $N_{\mathfrak{X}}(\mathfrak{P}_0)$, then $\mathfrak{P}_0$ contains every element of $\mathscr{SCN}(\mathfrak{P}^*)$.

Proof. Let $\mathfrak{A} \in \mathscr{SCN}(\mathfrak{P}^*)$. By (B) and (a), (b), (c), it follows that $\mathfrak{A} \cap \mathfrak{P} = \mathfrak{A} \cap \mathfrak{P}_0 = \mathfrak{A}_1$, say. If $\mathfrak{A}_1 \subset \mathfrak{A}$, then there is a $\mathfrak{P}_0$-invariant subgroup $\mathfrak{B}$ such that $\mathfrak{A}_1 \subset \mathfrak{B} \subseteq \mathfrak{A}$, $|\mathfrak{B} : \mathfrak{A}_1| = p$. Hence, $[\mathfrak{P}_0, \mathfrak{B}] \subseteq \mathfrak{A}_1 \subseteq \mathfrak{P}_0$, so $\mathfrak{B} \subseteq N_{\mathfrak{X}}(\mathfrak{P}_0) \cap \mathfrak{P}^*$. Hence, $\langle \mathfrak{B}, \mathfrak{P} \rangle$ is a p-subgroup of $N_{\mathfrak{X}}(\mathfrak{P}_0)$, so $\mathfrak{B} \subseteq \mathfrak{P}$. Hence, $\mathfrak{B} \subseteq \mathfrak{A} \cap \mathfrak{P} = \mathfrak{A}_1$, which is not the case, so $\mathfrak{A} = \mathfrak{A}_1$, as required.

8. Miscellaneous Preliminary Lemmas

LEMMA 8.1. *If $\mathfrak{X}$ is a π-group, and $\mathscr{C}$ is a chain $\mathfrak{X} = \mathfrak{X}_0 \supseteqq \mathfrak{X}_1 \supseteqq \cdots \supseteqq \mathfrak{X}_n = 1$, then the stability group $\mathfrak{A}$ of $\mathscr{C}$ is a π-group.*

Proof. We proceed by induction on n. Let $A \in \mathfrak{A}$. By induction, there is a π-number m such that $B = A^m$ centralizes $\mathfrak{X}_1$. Let $X \in \mathfrak{X}$; then $X^B = XY$ with Y in $\mathfrak{X}_1$, and by induction, $X^{B^r} = XY^r$. It follows that $B^{|\mathfrak{X}_1|} = 1$.

LEMMA 8.2. *If $\mathfrak{P}$ is a p-group, then $\mathfrak{P}$ possesses a characteristic subgroup $\mathfrak{C}$ such that*

(i) $\mathrm{cl}(\mathfrak{C}) \leqq 2$, *and $\mathfrak{C}/Z(\mathfrak{C})$ is elementary.*

(ii) $\ker(\mathrm{Aut}\,\mathfrak{P} \xrightarrow{\text{res}} \mathrm{Aut}\,\mathfrak{C})$ *is a p-group.* (res *is the homomorphism induced by restricting A in* Aut $\mathfrak{P}$ *to* $\mathfrak{C}$.)

(iii) $[\mathfrak{P}, \mathfrak{C}] \subseteq Z(\mathfrak{C})$ *and* $C(\mathfrak{C}) = Z(\mathfrak{C})$.

Proof. Suppose $\mathfrak{C}$ can be found to satisfy (i) and (iii). Let $\mathfrak{K} = \ker$ res. In commutator notation, $[\mathfrak{K}, \mathfrak{C}] = 1$, and so $[\mathfrak{K}, \mathfrak{C}, \mathfrak{P}] = 1$. Since $[\mathfrak{C}, \mathfrak{P}] \subseteq \mathfrak{C}$, we also have $[\mathfrak{C}, \mathfrak{P}, \mathfrak{K}] = 1$ and 3.1 implies $[\mathfrak{P}, \mathfrak{K}, \mathfrak{C}] = 1$, so that $[\mathfrak{P}, \mathfrak{K}] \subseteq Z(\mathfrak{C})$. Thus, $\mathfrak{K}$ stabilizes the chain $\mathfrak{P} \supseteqq \mathfrak{C} \supseteqq 1$ so is a p-group by Lemma 8.1.

If now some element of $\mathscr{SCN}(\mathfrak{P})$ is characteristic in $\mathfrak{P}$, then (i) and (iii) are satisfied and we are done. Otherwise, let $\mathfrak{A}$ be a maximal characteristic abelian subgroup of $\mathfrak{P}$, and let $\mathfrak{C}$ be the group generated by all subgroups $\mathfrak{D}$ of $\mathfrak{P}$ such that $\mathfrak{A} \subset \mathfrak{D}$, $|\mathfrak{D} : \mathfrak{A}| = p$, $\mathfrak{D} \subseteq \boldsymbol{Z}(\mathfrak{P} \bmod \mathfrak{A})$, $\mathfrak{D} \subseteq \boldsymbol{C}(\mathfrak{A})$. By construction, $\mathfrak{A} \subseteq \boldsymbol{Z}(\mathfrak{C})$, and $\mathfrak{C}$ is seen to be characteristic. The maximal nature of $\mathfrak{A}$ implies that $\mathfrak{A} = \boldsymbol{Z}(\mathfrak{C})$. Also by construction $[\mathfrak{P}, \mathfrak{C}] \subseteq \mathfrak{A} = \boldsymbol{Z}(\mathfrak{C})$, so in particular, $[\mathfrak{C}, \mathfrak{C}] \subseteq \boldsymbol{Z}(\mathfrak{C})$ and $\mathrm{cl}(\mathfrak{C}) \leqq 2$. By construction, $\mathfrak{C}/\boldsymbol{Z}(\mathfrak{C})$ is elementary.

We next show that $\boldsymbol{C}(\mathfrak{C}) = \boldsymbol{Z}(\mathfrak{C})$. This statement is of course equivalent to the statement that $\boldsymbol{C}(\mathfrak{C}) \subseteq \mathfrak{C}$. Suppose by way of contradiction that $\boldsymbol{C}(\mathfrak{C}) \not\subseteq \mathfrak{C}$. Let $\mathfrak{E}$ be a subgroup of $\boldsymbol{C}(\mathfrak{C})$ of minimal order subject to (a) $\mathfrak{E} \lhd \mathfrak{P}$, and (b) $\mathfrak{E} \not\subseteq \mathfrak{C}$. Since $\boldsymbol{C}(\mathfrak{C})$ satisfies (a) and (b), $\mathfrak{E}$ exists. By the minimality of $\mathfrak{E}$, we see that $[\mathfrak{P}, \mathfrak{E}] \subseteq \mathfrak{C}$ and $\boldsymbol{D}(\mathfrak{E}) \subseteq \mathfrak{C}$. Since $\mathfrak{E}$ centralizes $\mathfrak{C}$, so do $[\mathfrak{P}, \mathfrak{E}]$ and $\boldsymbol{D}(\mathfrak{E})$, so we have $[\mathfrak{P}, \mathfrak{E}] \subseteq \mathfrak{A}$ and $\boldsymbol{D}(\mathfrak{E}) \subseteq \mathfrak{A}$. The minimal nature of $\mathfrak{E}$ guarantees that $\mathfrak{E}/\mathfrak{E} \cap \mathfrak{C}$ is of order p. Since $\mathfrak{E} \cap \mathfrak{C} = \mathfrak{E} \cap \mathfrak{A}$, $\mathfrak{E}/\mathfrak{E} \cap \mathfrak{A}$ is of order p, so $\mathfrak{E}\mathfrak{A}/\mathfrak{A}$ is of order p. By construction of $\mathfrak{C}$, we find $\mathfrak{E}\mathfrak{A} \subseteq \mathfrak{C}$, so $\mathfrak{E} \subseteq \mathfrak{C}$, in conflict with (b). Hence, $\boldsymbol{C}(\mathfrak{C}) = \boldsymbol{Z}(\mathfrak{C})$, and (i) and (iii) are proved.

LEMMA 8.3. *Let $\mathfrak{X}$ be a p-group, p odd, and among all elements of $\mathscr{SCN}(\mathfrak{X})$, choose $\mathfrak{A}$ to maximize $m(\mathfrak{A})$. Then $\Omega_1(\boldsymbol{C}(\Omega_1(\mathfrak{A}))) = \Omega_1(\mathfrak{A})$.*

REMARK. The oddness of p is required, as the dihedral group of order 16 shows.

Proof. We must show that whenever an element of $\mathfrak{X}$ of order p centralizes $\Omega_1(\mathfrak{A})$, then the element lies in $\Omega_1(\mathfrak{A})$.

If $X \in \boldsymbol{C}(\Omega_1(\mathfrak{A}))$ and $X^p = 1$, let $\mathfrak{B}(X) = \mathfrak{B}_1 = \langle \Omega_1(\mathfrak{A}), X \rangle$, and let $\mathfrak{B}_1 \subset \mathfrak{B}_2 \subset \cdots \subset \mathfrak{B}_n = \langle \mathfrak{A}, X \rangle$ be an ascending chain of subgroups, each of index p in its successor. We wish to show that $\mathfrak{B}_1 \lhd \mathfrak{B}_n$. Suppose $\mathfrak{B}_1 \lhd \mathfrak{B}_m$ for some $m \leqq n-1$. Then $\mathfrak{B}_m$ is generated by its normal abelian subgroups $\mathfrak{B}_1$ and $\mathfrak{B}_m \cap \mathfrak{A}$, so $\mathfrak{B}_m$ is of class at most two, so is regular. Let $Z \in \mathfrak{B}_m$, Z of order p. Then $Z = X^k A$, A in $\mathfrak{A}$, k an integer. Since $\mathfrak{B}_m$ is regular, $X^{-k}Z$ is of order 1 or p. Hence, $A \in \Omega_1(\mathfrak{A})$, and $Z \in \mathfrak{B}_1$. Hence, $\mathfrak{B}_1 = \Omega_1(\mathfrak{B}_m)$ char $\mathfrak{B}_m \lhd \mathfrak{B}_{m+1}$, and $\mathfrak{B}_1 \lhd \mathfrak{B}_n$ follows. In particular, X stabilizes the chain $\mathfrak{A} \supseteq \Omega_1(\mathfrak{A}) \supseteq \langle 1 \rangle$.

It follows that if $\mathfrak{D} = \Omega_1(\boldsymbol{C}(\Omega_1(\mathfrak{A})))$, then $\mathfrak{D}'$ centralizes $\mathfrak{A}$. Since $\mathfrak{A} \in \mathscr{SCN}(\mathfrak{X})$, $\mathfrak{D}' \subseteq \mathfrak{A}$. We next show that $\mathfrak{D}$ is of exponent p. Since $[\mathfrak{D}, \mathfrak{D}] \subseteq \mathfrak{A}$, we see that $[\mathfrak{D}, \mathfrak{D}, \mathfrak{D}] \subseteq \Omega_1(\mathfrak{A})$, and so

$$[\mathfrak{D}, \mathfrak{D}, \mathfrak{D}, \mathfrak{D}] = 1\,,$$

and $\mathrm{cl}(\mathfrak{D}) \leqq 3$. If $p \geqq 5$, then $\mathfrak{D}$ is regular, and being generated by elements of order p, is of exponent p. It remains to treat the case $p=3$, and we must show that the elements of $\mathfrak{D}$ of order at most 3 form a subgroup. Suppose false, and that $\langle X, Y\rangle$ is of minimal order subject to $X^3 = Y^3 = 1$, $(XY)^3 \neq 1$, X and Y being elements of $\mathfrak{D}$. Since $\langle Y, Y^X\rangle \subset \langle X, Y\rangle$, $[Y, X] = Y^{-1}$. $X^{-1}YX$ is of order three. Hence, $[X, Y]$ is in $\Omega_1(\mathfrak{A})$, and so $[Y, X]$ is centralized by both X and Y. It follows that $(XY)^3 = X^3Y^3[Y, X]^3 = 1$, so $\mathfrak{D}$ is of exponent p in all cases.

If $\Omega_1(\mathfrak{A}) \subset \mathfrak{D}$, let $\mathfrak{E} \lhd \mathfrak{X}$, $\mathfrak{E} \subseteq \mathfrak{D}$, $|\mathfrak{E} : \Omega_1(\mathfrak{A})| = p$. Since $\Omega_1(\mathfrak{A}) \subseteq \boldsymbol{Z}(\mathfrak{E})$, $\mathfrak{E}$ is abelian. But $m(\mathfrak{E}) = m(\mathfrak{A}) + 1 > m(\mathfrak{A})$, in conflict with the maximal nature of $\mathfrak{A}$, since $\mathfrak{E}$ is contained in some element of $\mathscr{SCN}(\mathfrak{X})$ by 3.9.

LEMMA 8.4. *Suppose p is an odd prime and $\mathfrak{X}$ is a p-group.*

(i) *If $\mathscr{SCN}_3(\mathfrak{X})$ is empty, then every abelian subgroup of $\mathfrak{X}$ is generated by two elements.*

(ii) *If $\mathscr{SCN}_3(\mathfrak{X})$ is empty and A is an automorphism of $\mathfrak{X}$ of prime order q, $p \neq q$, then q divides $p^2 - 1$.*

Proof. (i) Suppose $\mathfrak{A}$ is chosen in accordance with Lemma 8.3. Suppose also that $\mathfrak{X}$ contains an elementary subgroup $\mathfrak{E}$ of order p^3. Let $\mathfrak{E}_1 = \boldsymbol{C}_{\mathfrak{E}}(\Omega_1(\mathfrak{A}))$, so that $\mathfrak{E}_1$ is of order p^2 at least. But by Lemma 8.3, $\mathfrak{E}_1 \subseteq \Omega_1(\mathfrak{A})$, a group of order at most p^2, and so $\mathfrak{E}_1 = \Omega_1(\mathfrak{A})$. But now Lemma 8.3 is violated since $\mathfrak{E}$ centralizes $\mathfrak{E}_1$.

(ii) Among the A-invariant subgroups of $\mathfrak{X}$ on which A acts non trivially, let $\mathfrak{H}$ be minimal. By 3.11, $\mathfrak{H}$ is a special p-group. Since p is odd, $\mathfrak{H}$ is regular, so 3.6 implies that $\mathfrak{H}$ is of exponent p. By the first part of this lemma, $\mathfrak{H}$ contains no elementary subgroup of order p^3. It follows readily that $m(\mathfrak{H}) \leq 2$, and (ii) follows from the well known fact that q divides $|\mathrm{Aut}\ \mathfrak{H}/\boldsymbol{D}(\mathfrak{H})|$.

LEMMA 8.5. *If $\mathfrak{X}$ is a group of odd order, p is the smallest prime in $\pi(\mathfrak{X})$, and if in addition $\mathfrak{X}$ contains no elementary subgroup of order p^3, then $\mathfrak{X}$ has a normal p-complement.*

Proof. Let $\mathfrak{P}$ be a S_p-subgroup of $\mathfrak{X}$. By hypothesis, if $\mathfrak{H}$ is a subgroup of $\mathfrak{P}$, then $\mathscr{SCN}_3(\mathfrak{H})$ is empty. Application of Lemma 8.4 (ii) shows that $N_{\mathfrak{X}}(\mathfrak{H})/C_{\mathfrak{X}}(\mathfrak{H})$ is a p-group for every subgroup $\mathfrak{H}$ of $\mathfrak{P}$. We apply Theorem 14. 4. 7 in [12] to complete the proof.

Application of Lemma 8.5 to a simple group $\mathfrak{G}$ of odd order implies that if p is the smallest prime in $\pi(\mathfrak{G})$, then $\mathfrak{G}$ contains an elementary subgroup of order p^3. In particular, if $3 \in \pi(\mathfrak{G})$, then $\mathfrak{G}$ contains an elementary subgroup of order 27.

LEMMA 8.6. *Let $\mathfrak{N}_1, \mathfrak{N}_2, \mathfrak{N}_3$ be subgroups of a group $\mathfrak{X}$ and suppose that for every permutation σ of $\{1, 2, 3\}$,*

$$\mathfrak{N}_{\sigma(1)} \subseteq \mathfrak{N}_{\sigma(2)}\mathfrak{N}_{\sigma(3)}$$

Then $\mathfrak{N}_1\mathfrak{N}_2$ is a subgroup of $\mathfrak{X}$.

Proof. $\mathfrak{N}_2\mathfrak{N}_1 \subseteq (\mathfrak{N}_1\mathfrak{N}_3)(\mathfrak{N}_3\mathfrak{N}_2) \subseteq \mathfrak{N}_1\mathfrak{N}_3\mathfrak{N}_2 \subseteq \mathfrak{N}_1(\mathfrak{N}_1\mathfrak{N}_2)\mathfrak{N}_2 \subseteq \mathfrak{N}_1\mathfrak{N}_2$, as required.

LEMMA 8.7. *If $\mathfrak{A}$ is a p'-group of automorphisms of the p-group $\mathfrak{P}$, if $\mathfrak{A}$ has no fixed points on $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$, and $\mathfrak{A}$ acts trivially on $\boldsymbol{D}(\mathfrak{P})$, then $\boldsymbol{D}(\mathfrak{P}) \subseteq \boldsymbol{Z}(\mathfrak{P})$.*

Proof. In commutator notation, we are assuming $[\mathfrak{P}, \mathfrak{A}] = \mathfrak{P}$, and $[\mathfrak{A}, \boldsymbol{D}(\mathfrak{P})] = 1$. Hence, $[\mathfrak{A}, \boldsymbol{D}(\mathfrak{P}), \mathfrak{P}] = 1$. Since $[\boldsymbol{D}(\mathfrak{P}), \mathfrak{P}] \subseteq \boldsymbol{D}(\mathfrak{P})$, we also have $[\boldsymbol{D}(\mathfrak{P}), \mathfrak{P}, \mathfrak{A}] = 1$. By the three subgroups lemma, we have $[\mathfrak{P}, \mathfrak{A}, \boldsymbol{D}(\mathfrak{P})] = 1$. Since $[\mathfrak{P}, \mathfrak{A}] = \mathfrak{P}$, the lemma follows.

LEMMA 8.8. *Suppose $\mathfrak{Q}$ is a q-group, q is odd, A is an automorphism of $\mathfrak{Q}$ of prime order p, $p \equiv 1 \pmod q$, and $\mathfrak{Q}$ contains a subgroup $\mathfrak{Q}_0$ of index q such that $\mathscr{S}\mathscr{C}\mathscr{N}_3(\mathfrak{Q}_0)$ is empty. Then $p = 1 + q + q^2$ and $\mathfrak{Q}$ is elementary of order q^3.*

Proof. Since $p \equiv 1 \pmod q$ and q is odd, p does not divide $q^2 - 1$. Since $\boldsymbol{D}(\mathfrak{Q}) \subseteq \mathfrak{Q}_0$, Lemma 8.4 (ii) implies that A acts trivially on $\boldsymbol{D}(\mathfrak{Q})$.

Suppose that A has a non trivial fixed point on $\mathfrak{Q}/\boldsymbol{D}(\mathfrak{Q})$. We can then find an A-invariant subgroup $\mathfrak{M}$ of index q in $\mathfrak{Q}$ such that A acts trivially on $\mathfrak{Q}/\mathfrak{M}$. In this case, A does not act trivially on $\mathfrak{M}$, and so $\mathfrak{M} \neq \mathfrak{Q}_0$, and $\mathfrak{M} \cap \mathfrak{Q}_0$ is of index q in $\mathfrak{M}$. By induction, $p = 1 + q + q^2$ and $\mathfrak{M}$ is elementary of order q^3. Since A acts trivially on $\mathfrak{Q}/\mathfrak{M}$, it follows that $\mathfrak{Q}$ is abelian of order q^4 If $\mathfrak{Q}$ were elementary, $\mathfrak{Q}_0$ would not exist. But if $\mathfrak{Q}$ were not elementary, then A would have a fixed point on $\Omega_1(\mathfrak{Q}) = \mathfrak{M}$, which is not possible. Hence A has no fixed points on $\mathfrak{Q}/\boldsymbol{D}(\mathfrak{Q})$, so by Lemma 8.7, $\boldsymbol{D}(\mathfrak{Q}) \subseteq \boldsymbol{Z}(\mathfrak{Q})$.

Next, suppose that A does not act irreducibly on $\mathfrak{Q}/\boldsymbol{D}(\mathfrak{Q})$. Let $\mathfrak{N}/\boldsymbol{D}(\mathfrak{Q})$ be an irreducible constituent of A on $\mathfrak{Q}/\boldsymbol{D}(\mathfrak{Q})$. By induction, $\mathfrak{N}$ is of order q^3, and $p = 1 + q + q^2$. Since $\boldsymbol{D}(\mathfrak{Q}) \subset \mathfrak{N}$, $\boldsymbol{D}(\mathfrak{Q})$ is a proper A-invariant subgroup of $\mathfrak{N}$. The only possibility is $\boldsymbol{D}(\mathfrak{Q}) = 1$, and $|\mathfrak{Q}| = q^3$ follows from the existence of $\mathfrak{Q}_0$.

If $|\mathfrak{Q}| = q^3$, then $p = 1 + q + q^2$ follows from Lemma 5.1. Thus, we can suppose that $|\mathfrak{Q}| > q^3$, and that A acts irreducibly on $\mathfrak{Q}/\boldsymbol{D}(\mathfrak{Q})$, and try to derive a contradiction. We see that $\mathfrak{Q}$ must be non abelian. This implies that $\boldsymbol{D}(\mathfrak{Q}) = \boldsymbol{Z}(\mathfrak{Q})$. Let $|\mathfrak{Q} : \boldsymbol{D}(\mathfrak{Q})| = q^n$. Since

$p \equiv 1 \pmod q$, and $q^n \equiv 1 \pmod p$, $n \geqq 3$. Since $D(\mathfrak{Q}) = Z(\mathfrak{Q})$, n is even, $\mathfrak{Q}/Z(\mathfrak{Q})$ possessing a non singular skew-symmetric inner product over integers mod q which admits A. Namely, let $\mathfrak{C}$ be a subgroup of order q contained in $\mathfrak{Q}'$ and let $\mathfrak{C}_1$ be a complement for $\mathfrak{C}$ in $\mathfrak{Q}'$. This complement exists since $\mathfrak{Q}'$ is elementary. Then $Z(\mathfrak{P} \bmod \mathfrak{C}_1)$ is A-invariant, proper, and contains $D(\mathfrak{Q})$. Since A acts irreducibly on $\mathfrak{Q}/D(\mathfrak{Q})$, we must have $D(\mathfrak{Q}) = Z(\mathfrak{Q} \bmod \mathfrak{C}_1)$, so a non singular skew-symmetric inner product is available. Now $\mathfrak{Q}$ is regular, since $\mathrm{cl}(\mathfrak{Q}) = 2$, and q is odd, so $|\Omega_1(\mathfrak{Q})| = |\mathfrak{Q} : \mho^1(\mathfrak{Q})|$, by [14]. Since $\mathrm{cl}(\mathfrak{Q}) = 2$, $\Omega_1(\mathfrak{Q})$ is of exponent q. Since

$$|\mathfrak{Q} : \mho^1(\mathfrak{Q})| \geqq |\mathfrak{Q} : D(\mathfrak{Q})| \geqq q^4 ,$$

we see that $|\Omega_1(\mathfrak{Q})| \geqq q^4$. Since $\mathfrak{Q}_0$ exists, $\Omega_1(\mathfrak{Q})$ is non abelian, of order exactly q^4, since otherwise $\mathfrak{Q}_0 \cap \Omega_1(\mathfrak{Q})$ would contain an elementary subgroup of order q^3. It follows readily that A centralizes $\Omega_1(\mathfrak{Q})$, and so centralizes $\mathfrak{Q}$, by 3.6. This is the desired contradiction.

LEMMA 8.9. *If $\mathfrak{P}$ is a p-group, if $\mathscr{SCN}_3(\mathfrak{P})$ is non empty and $\mathfrak{A}$ is a normal abelian subgroup of $\mathfrak{P}$ of type (p, p), then $\mathfrak{A}$ is contained in some element of $\mathscr{SCN}_3(\mathfrak{P})$.*

Proof. Let $\mathfrak{E}$ be a normal elementary subgroup of $\mathfrak{P}$ of order p^3, and let $\mathfrak{E}_1 = C_{\mathfrak{E}}(\mathfrak{A})$. Then $\mathfrak{E}_1 \lhd \mathfrak{P}$, and $\langle \mathfrak{A}, \mathfrak{E}_1 \rangle = \mathfrak{F}$ is abelian. If $|\mathfrak{F}| = p^2$, then $\mathfrak{A} = \mathfrak{E}_1 = \mathfrak{F} \subset \mathfrak{E}$, and we are done, since $\mathfrak{E}$ is contained in an element of $\mathscr{SCN}_3(\mathfrak{P})$. If $|\mathfrak{F}| \geqq p^3$, then again we are done, since $\mathfrak{F}$ is contained in an element of $\mathscr{SCN}_3(\mathfrak{P})$.

If $\mathfrak{X}$ and $\mathfrak{Y}$ are groups, we say that $\mathfrak{Y}$ *is involved in* $\mathfrak{X}$ provided some section of $\mathfrak{X}$ is isomorphic to $\mathfrak{Y}$ [18].

LEMMA 8.10. *Let $\mathfrak{P}$ be a S_p-subgroup of the group $\mathfrak{X}$. Suppose that $Z(\mathfrak{P})$ is cyclic and that for each subgroup $\mathfrak{A}$ in $\mathfrak{P}$ of order p which does not lie in $Z(\mathfrak{P})$, there is an element $X = X(\mathfrak{A})$ of $\mathfrak{P}$ which normalizes but does not centralize $\langle \mathfrak{A}, \Omega_1(Z(\mathfrak{P}))\rangle$. Then either $SL(2, p)$ is involved in $\mathfrak{X}$ or $\Omega_1(Z(\mathfrak{P}))$ is weakly closed in $\mathfrak{P}$.*

Proof. Let $\mathfrak{D} = \Omega_1(Z(\mathfrak{P}))$. Suppose $\mathfrak{E} = \mathfrak{D}^G$ is a conjugate of $\mathfrak{D}$ contained in $\mathfrak{P}$, but that $\mathfrak{E} \neq \mathfrak{D}$. Let $\mathfrak{D} = \langle D \rangle$, $\mathfrak{E} = \langle E \rangle$. By hypothesis, we can find an element $X = X(\mathfrak{E})$ in $\mathfrak{P}$ such that X normalizes $\langle E, D \rangle = \mathfrak{F}$, and with respect to the basis (E, D) has the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Enlarge $\mathfrak{F}$ to a S_p-subgroup $\mathfrak{P}^*$ of $C_{\mathfrak{X}}(\mathfrak{E})$. Since $\mathfrak{E} = \mathfrak{D}^G$, $\mathfrak{P}^G \subseteqq C_{\mathfrak{X}}(\mathfrak{E})$, so $\mathfrak{P}^*$ is a S_p-subgroup of $\mathfrak{X}$, and $\mathfrak{E} \subseteqq Z(\mathfrak{P}^*)$. Since $Z(\mathfrak{P}^*)$ is cyclic by hypothesis, we have $\mathfrak{E} = \Omega_1(Z(\mathfrak{P}^*))$. By hypothesis, there is an element $Y = Y(\mathfrak{D})$ in $\mathfrak{P}^*$ which normalizes $\mathfrak{F}$ and with respect to the basis (E, D) has the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Now $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate $SL(2, p)$ [6, Sections 262 and 263], so $SL(2, p)$ is involved in $N_{\mathfrak{X}}(\mathfrak{F})$, as desired.

LEMMA 8.11. *If $\mathfrak{A}$ is a p-subgroup and $\mathfrak{B}$ is a q-subgroup of $\mathfrak{X}$, $p \neq q$, and $\mathfrak{A}$ normalizes $\mathfrak{B}$ then* $[\mathfrak{B}, \mathfrak{A}] = [\mathfrak{B}, \mathfrak{A}, \mathfrak{A}]$.

Proof. By 3.7, $[\mathfrak{A}, \mathfrak{B}] \lhd \mathfrak{A}\mathfrak{B}$. Since $\mathfrak{A}\mathfrak{B}/[\mathfrak{A}, \mathfrak{B}]$ is nilpotent, we can suppose that $[\mathfrak{A}, \mathfrak{B}]$ is elementary. With this reduction, $[\mathfrak{B}, \mathfrak{A}, \mathfrak{A}] \lhd \mathfrak{A}\mathfrak{B}$, and we can assume that $[\mathfrak{B}, \mathfrak{A}, \mathfrak{A}] = 1$. In this case, $\mathfrak{A}$ stabilizes the chain $\mathfrak{B} \supseteqq [\mathfrak{B}, \mathfrak{A}] \supseteqq 1$, so $[\mathfrak{B}, \mathfrak{A}] = 1$ follows from Lemma 8.1 and $p \neq q$.

LEMMA 8.12. *Let p be an odd prime, and $\mathfrak{E}$ an elementary subgroup of the p-group $\mathfrak{P}$. Suppose A is a p'-automorphism of $\mathfrak{P}$ which centralizes $\Omega_1(C_{\mathfrak{P}}(\mathfrak{E}))$. Then $A = 1$.*

Proof. Since $\mathfrak{E} \subseteq \Omega_1(C_{\mathfrak{P}}(\mathfrak{E}))$, A centralizes $\mathfrak{E}$. Since $\mathfrak{E}$ is A-invariant, so is $C_{\mathfrak{P}}(\mathfrak{E})$. By 3.6 A centralizes $C_{\mathfrak{P}}(\mathfrak{E})$, so if $\mathfrak{E} \subseteq Z(\mathfrak{P})$, we are done.

If $C_{\mathfrak{P}}(\mathfrak{E}) \subset \mathfrak{P}$, then $C_{\mathfrak{P}}(\mathfrak{E})D(\mathfrak{P}) \subset \mathfrak{P}$, and by induction A centralizes $D(\mathfrak{P})$. Now $[\mathfrak{P}, \mathfrak{E}] \subseteq D(\mathfrak{P})$ and so $[\mathfrak{P}, \mathfrak{E}, \langle A \rangle] = 1$. Also, $[\mathfrak{E}, \langle A \rangle] = 1$, so that $[\mathfrak{E}, \langle A \rangle, \mathfrak{P}] = 1$. By the three subgroups lemma, we have $[\langle A \rangle, \mathfrak{P}, \mathfrak{E}] = 1$, so that $[\mathfrak{P}, \langle A \rangle] \subseteq C_{\mathfrak{P}}(\mathfrak{E})$, and A stabilizes the chain $\mathfrak{P} \supseteqq C_{\mathfrak{P}}(\mathfrak{E}) \supset 1$. It follows from Lemma 8.1 that $A = 1$.

LEMMA 8.13. *Suppose $\mathfrak{P}$ is a S_p-subgroup of the solvable group $\mathfrak{S}$, $\mathscr{SCN}_3(\mathfrak{P})$ is empty and $\mathfrak{S}$ is of odd order. Then $\mathfrak{S}'$ centralizes every chief p-factor of $\mathfrak{S}$.*

Proof. We assume without loss of generality that $O_{p'}(\mathfrak{S}) = 1$. We first show that $\mathfrak{P} \lhd \mathfrak{S}$. Let $\mathfrak{H} = O_p(\mathfrak{S})$, and let $\mathfrak{C}$ be a subgroup of $\mathfrak{H}$ chosen in accordance with Lemma 8.2. Let $\mathfrak{W} = \Omega_1(\mathfrak{C})$. Since p is odd and $\mathrm{cl}(\mathfrak{C}) \leqq 2$, $\mathfrak{W}$ is of exponent p.

Since $O_{p'}(\mathfrak{S}) = 1$, Lemma 8.2 implies that $\ker(\mathfrak{S} \longrightarrow \operatorname{Aut}\mathfrak{C})$ is a p-group. By 3.6, it now follows that $\ker(\mathfrak{S} \xrightarrow{\alpha} \operatorname{Aut}\mathfrak{W})$ is a p-group. Since $\mathfrak{P}$ has no elementary subgroup of order p^3, neither does $\mathfrak{W}$, and so $|\mathfrak{W} : D(\mathfrak{W})| \leqq p^2$. Hence no p-element of $\mathfrak{S}$ has a minimal polynomial $(x - 1)^p$ on $\mathfrak{W}/D(\mathfrak{W})$. Now (B) implies that $\mathfrak{P}/\ker\alpha \lhd \mathfrak{S}/\ker\alpha$. and so $\mathfrak{P} \lhd \mathfrak{S}$, since $\ker\alpha \subseteq \mathfrak{P}$.

Since $\mathfrak{P} \lhd \mathfrak{S}$, the lemma is equivalent to the assertion that if $\mathfrak{L}$ is a $S_{p'}$-subgroup of $\mathfrak{S}$, then $\mathfrak{L}' = 1$. If $\mathfrak{L}' \neq 1$, we can suppose that $\mathfrak{L}'$ centralizes every proper subgroup of $\mathfrak{P}$ which is normal in $\mathfrak{S}$. Since $\mathfrak{L}$ is completely reducible on $\mathfrak{P}/D(\mathfrak{P})$, we can suppose that $[\mathfrak{P}, \mathfrak{L}'] = \mathfrak{P}$

and $[D(\mathfrak{P}), \mathfrak{L}'] = 1$. By Lemma 8.7 we have $D(\mathfrak{P}) \subseteq Z(\mathfrak{P})$ and so $\Omega_1(\mathfrak{P}) = \mathfrak{R}$ is of exponent p and class at most 2. Since $\mathfrak{P}$ has no elementary subgroup of order p^3, neither does $\mathfrak{R}$. If $\mathfrak{R}$ is of order p, $\mathfrak{L}'$ centralizes $\mathfrak{R}$ and so centralizes $\mathfrak{P}$ by 3.6, thus $\mathfrak{L}' = 1$. Otherwise, $|\mathfrak{R} : D(\mathfrak{R})| = p^2$ and $\mathfrak{L}$ is faithfully represented as automorphisms of $\mathfrak{R}/D(\mathfrak{R})$. Since $|\mathfrak{L}|$ is odd, $\mathfrak{L}' = 1$.

LEMMA 8.14. *If $\mathfrak{S}$ is a solvable group of odd order, and $\mathscr{SCN}_3(\mathfrak{P})$ is empty for every S_p-subgroup $\mathfrak{P}$ of $\mathfrak{S}$ and every prime p, then $\mathfrak{S}'$ is nilpotent.*

Proof. By the preceding lemma, $\mathfrak{S}'$ centralizes every chief factor of $\mathfrak{S}$. By 3.2, $\mathfrak{S}' \subseteq F(\mathfrak{S})$, a nilpotent group.

LEMMA 8.15. *Let $\mathfrak{S}$ be a solvable group of odd order and suppose that $\mathfrak{S}$ does not contain an elementary subgroup of order p^3 for any prime p. Let $\mathfrak{P}$ be a S_p-subgroup of $\mathfrak{S}$ and let $\mathfrak{C}$ be any characteristic subgroup of $\mathfrak{P}$. Then $\mathfrak{C} \cap \mathfrak{P}' \lhd \mathfrak{S}$.*

Proof. We can suppose that $\mathfrak{C} \subseteq \mathfrak{P}'$, since $\mathfrak{C} \cap \mathfrak{P}'$ char $\mathfrak{P}$. By Lemma 8.14 $F(\mathfrak{S})$ normalizes $\mathfrak{C}$. Since $F(\mathfrak{S})\mathfrak{P} \lhd \mathfrak{S}$, we have $\mathfrak{S} = F(\mathfrak{S})N(\mathfrak{P})$. The lemma follows.

The next two lemmas involve a non abelian p-group $\mathfrak{P}$ with the following properties:
(1) p is odd.
(2) $\mathfrak{P}$ contains a subgroup $\mathfrak{P}_0$ of order p such that

$$C(\mathfrak{P}_0) = \mathfrak{P}_0 \quad \mathfrak{P}_1 ,$$

where $\mathfrak{P}_1$ is cyclic.
Also, $\mathfrak{A}$ is a p'-group of automorphisms of $\mathfrak{P}$ of odd order.

LEMMA 8.16. *With the preceding notation,*
(i) *$\mathfrak{A}$ is abelian.*
(ii) *No element of $\mathfrak{A}^\#$ centralizes $\Omega_1(C(\mathfrak{P}_0))$.*
(iii) *If $\mathfrak{A}$ is cyclic, then either $|\mathfrak{A}|$ divides $p \quad 1$ or $\mathscr{SCN}_3(\mathfrak{P})$ is empty.*

Proof. (ii) is an immediate consequence of Lemma 8.12.

Let $\mathfrak{B}$ be a subgroup of $\mathfrak{P}$ chosen in accordance with Lemma 8.2, and let $\mathfrak{W} = \Omega_1(\mathfrak{B})$ so that $\mathfrak{A}$ is faithfully represented on $\mathfrak{W}$. If $\mathfrak{P}_0 \not\subseteq \mathfrak{W}$, then $\mathfrak{P}_0\mathfrak{W}$ is of maximal class, so that with $\mathfrak{W}_0 = \mathfrak{W}$, $\mathfrak{W}_{i+1} = [\mathfrak{W}_i, \mathfrak{P}]$, we have $|\mathfrak{W}_i : \mathfrak{W}_{i+1}| = p$, $i = 0, 1, \cdots, n-1$, $|\mathfrak{W}| = p^n$, and both (i) and (iii) follow. If $\mathfrak{P}_0 \subseteq \mathfrak{W}$, then $m(\mathfrak{W}) = 2$. Since $[\mathfrak{W}, \mathfrak{P}] \subseteq Z(\mathfrak{W})$, it follows that $\langle \mathfrak{P}_0, \boldsymbol{Z}(\mathfrak{W})\rangle \lhd \mathfrak{P}$. By Lemma 8.9, $\mathscr{S}\mathscr{C}\mathscr{N}_3(\mathfrak{P})$ is empty. The lemma follows readily from 3.4.

LEMMA 8.17. *In the preceding notation, assume in addition that* $|\mathfrak{A}| = q$ *is a prime, that* q *does not divide* $p - 1$, *that* $\mathfrak{P} = [\mathfrak{P}, \mathfrak{A}]$ *and that* $C_{\mathfrak{P}}(\mathfrak{A})$ *is cyclic. Then* $|\mathfrak{P}| = p^3$.

Proof. Since $q \nmid p - 1$, $\mathfrak{A}$ centralizes $\boldsymbol{Z}(\mathfrak{P})$, and so $\boldsymbol{Z}(\mathfrak{P}) \subseteq \mathfrak{P}'$. Since $C_{\mathfrak{P}}(\mathfrak{A})$ is cyclic, $\Omega_1(\boldsymbol{Z}_2(\mathfrak{P}))$ is not of type (p, p). Hence, $\mathfrak{P}_0 \subseteq \Omega_1(\boldsymbol{Z}_2(\mathfrak{P}))$. Since every automorphism of $\Omega_1(\boldsymbol{Z}_2(\mathfrak{P}))$ which is the identity on $\Omega_1(\boldsymbol{Z}_2(\mathfrak{P}))/\Omega_1(\boldsymbol{Z}(\mathfrak{P}))$ is inner, it follows that $\mathfrak{P} = \Omega_1(\boldsymbol{Z}_2(\mathfrak{P})) \cdot \mathfrak{D}$, where $\mathfrak{D} = C_{\mathfrak{P}}(\Omega_1(\boldsymbol{Z}_2(\mathfrak{P})))$. Since $\mathfrak{P}_1$ is cyclic, so is $\mathfrak{D}$, and so $\mathfrak{D} \subseteq \Omega_1(\boldsymbol{Z}_2(\mathfrak{P}))$, by virtue of $\mathfrak{P} = [\mathfrak{P}, \mathfrak{A}]$ and $q \nmid p - 1$.