TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 180, June 1973

ON LAGRANGIAN GROUPS

BY

J. F. HUMPHREYS AND D. L. JOHNSON

ABSTRACT. We study the class $\mathfrak{L}$ of Lagrangian groups, that is, of finite groups G possessing a subgroup of index n for each factor n of $|G|$. These groups and their analogues were considered by McLain in [4] and the object of the present work is to extend the results in this article. We study the classes $(G) = \{H \mid G \times H \in \mathfrak{L}\}$ and also the closure of $\mathfrak{L}$ under wreath products. We also consider the two classes $\mathfrak{X}$ and $\mathfrak{Y}$ introduced in [2] and [4] respectively.

0. Introduction. Lagrangian groups, that is, finite groups G possessing for every factor of $|G|$ a subgroup of that index, have been studied by many authors. The interesting survey article [3] contains a useful list of references. It is our purpose here to extend some of the ideas developed by McLain in [4] and to prove a number of new results about such groups and their analogues.

Denoting by $\mathfrak{L}$ the class of Lagrangian groups and by s the operation of subgroup closure, then two basic results are that (a) $s\mathfrak{L}$ is the class $\mathfrak{S}$ of supersoluble groups (proved by Zappa [6] in answer to a question of Ore [5]), and (b) soluble groups are characterised as the direct factors of the elements of $\mathfrak{L}$ (proved by McLain in [4]). Extensions of these results will be discussed in §§1 and 2 respectively, while in §3 we prove a result about the wreath product closure of $\mathfrak{L}$.

Finally, in §4 we introduce the following two classes of finite groups: $\mathfrak{Y}$ is the class of groups G such that for every subgroup H of G and every integer n dividing $|G:H|$, there is a subgroup K of G with $H \le K \le G$ and $|G:K| = n$, while $\mathfrak{X}$ is the class of groups all of whose meet-irreducible subgroups have prime-power index. The class $\mathfrak{Y}$ was introduced in [4], while $\mathfrak{X}$ was introduced in [2], where it is proved that $\mathfrak{X} \subseteq \mathfrak{S}$. We prove here that $s\mathfrak{X} \subseteq \mathfrak{Y} \subseteq \mathfrak{X}$ (so that $s\mathfrak{X} = s\mathfrak{Y}$), but we are unable to find a counterexample to the conjecture $\mathfrak{Y} = \mathfrak{X}$.

The authors would like to express their gratitude to the referee for many helpful comments, and in particular for the example following the second corollary of Proposition 2.

Received by the editors August 19, 1971.

AMS (MOS) subject classifications (1970). Primary 20D30.

Key words and phrases. Supersoluble group, wreath product, KG-module, meet-irreducible, subgroup closure.

1. **p-Lagrangian groups.** All groups considered in this article will be finite.

Definition. A group G is called Lagrangian if, for every positive integer n dividing $|G|$, G has a subgroup of index n; we shall denote the class of Lagrangian groups by $\mathfrak{L}$.

Since each $G \in \mathfrak{L}$ contains a Hall p'-subgroup for each prime p dividing $|G|$, the elements of $\mathfrak{L}$ are all soluble, while on the other hand it is easy to show (using the Sylow tower property) that the class $\mathfrak{S}$ of all supersoluble groups is contained in $\mathfrak{L}$, both these inclusions being proper.

Proposition 1. *For a group G to be Lagrangian, it is necessary and sufficient that G have a subgroup of index n for each prime power n dividing $|G|$.*

Proof. The necessity is obvious, while the sufficiency is an immediate consequence of the following elementary result: if H and K are subgroups of G of coprime index, then $|G:H \cap K| = |G:H|\,|G:K|$.

This result leads in a natural way to the

Definition. A group G is said to be p-Lagrangian (where p is a prime) if, for each nonnegative integer α with $p^\alpha \mid |G|$, G contains a subgroup of index p^α. We denote the class of such groups by $\mathfrak{L}_p$. Let the prefix s stand for the operation of subgroup closure; we define the classes of strongly Lagrangian and strongly p-Lagrangian groups to be $s\mathfrak{L}$ and the p-soluble members of $s\mathfrak{L}_p$ respectively.

It follows from Proposition 1 that $\mathfrak{L}$, $s\mathfrak{L}$ are the intersections over all primes p of the classes $\mathfrak{L}_p$ and $s\mathfrak{L}_p$ respectively.

Proposition 2. *A group G is strongly p-Lagrangian if and only if G is a p-soluble group possessing a chain of subgroups,*

$$G = G_0 > \cdots > G_m = H, \tag{1}$$

such that $|G_{i-1}:G_i| = p$, $1 \le i \le m$, and $|H|$ is prime to p.

Proof. The necessity of the condition is obvious, while for the sufficiency it is enough to show that the property (1) is subgroup closed within the class of p-soluble groups. So let G be a p-soluble group possessing property (1) and let K be any subgroup of G. By the p-solubility, we can find a Hall p'-subgroup L of K and an element x of G such that $L \le H^x$. Consider the chain

$$K = K \cap G_0^x \ge \cdots \ge K \cap G_m^x = L \tag{2}$$

of subgroups of K, where, if $r_i = |K \cap G_{i-1}^x : K \cap G_i^x|$, $1 \le i \le m$, we have $r_i \le |G_{i-1}^x : G_i^x| = |G_{i-1}:G_i| = p$ for $1 \le i \le m$. Since each r_i is a divisor of the p-power $|K:L|$, it follows that r_i is 1 or p, $1 \le i \le m$. Thus, deleting the repeated members of (2) leads to a subgroup chain of type (1) for K as required.

Corollary 1. *$G \in s\mathfrak{L}$ if and only if, for each prime p dividing $|G|$, G has a chain of subgroups of type* (1) *above.*

Proof. This follows at once from the proposition and the fact that the existence of these chains entails the solubility of G.

This corollary provides a characterisation of supersoluble groups, since we already know that $\mathfrak{S} = s\mathfrak{L}$ (see §0).

Corollary 2. *Lagrangian groups of cube-free order are supersoluble.*

Consider a chain of subgroups

$$(C) \qquad G = G_0 > \cdots > G_m = H$$

of the p-soluble group G, where H is a Hall p'-subgroup of G, and write $s(C) = \max\{s_1, \cdots, s_m\}$ where $p^{s_i} = |G_{i-1} : G_i|$, $1 \leq i \leq m$. Defining $s_p(G)$ to be the least value of $s(C)$ as (C) ranges over all such chains of subgroups of G, the above corollary simply asserts that if $s_p(G) = 1$ for all primes p dividing $|G|$, then $r_p(G) = 1$ for all p, where $r_p(G)$ is the p-rank of G. It is clear that $s_p(G) \leq r_p(G)$ for all p, however the group G which is the standard wreath product of the symmetric group on three symbols by a cyclic group of order three has $r_3(G) = 3$, but $s_3(G) = 1$, so that $r_p(G) \neq s_p(G)$ in general.

We have the following result for p-soluble groups G satisfying $s_p(G) = 1$.

Proposition 3. *Let G be a p-soluble group with $s_p(G) = 1$ and $|G| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where $\alpha_1, \cdots, \alpha_n$ are all nonzero and $p_1 > p_2 > \cdots > p_i = p > \cdots > p_m$, say; then G possesses a partial Sylow tower, that is, a chain of subgroups*

$$(3) \qquad E = G_0 \leq G_1 \leq \cdots \leq G_{i-1} \leq G$$

where each member is normal in G, $|G_j : G_{j-1}| = p_j^{\alpha_j}$, $1 \leq j \leq i-1$, and $|E| = 1$.

Proof. We proceed by induction on $|G|$ and, to avoid triviality, we assume that $i > 1$. By hypothesis, there is a subgroup H of G with $|G : H| = p$, and $s_p(H) = 1$ by Proposition 2. By induction, H has a normal subgroup G_1, of index $|p_1^{\alpha_1}$, which is normal in G by Sylow's theorem (since $p < p_1$). The result now follows by applying the inductive hypothesis to G/G_1.

2. **Direct products.** If G is a p-soluble group such that $|G| = p^{\alpha}m$, where $\alpha > 0$ and $(p, m) = 1$, then it is obvious that the group $G \times Z_{p^{\alpha-1}}$ is p-Lagrangian. For, if H is a Hall p'-subgroup of G and $Z_{p^{\alpha-1}} = Z_{\alpha-1} > \cdots > Z_0 = E$ is a composition series for $Z_{p^{\alpha-1}}$, then the set $\{H \times Z_\beta, G \times Z_\beta \mid 0 \leq \beta \leq \alpha - 1\}$ forms a collection of subgroups of all possible p-power indices in $G \times Z_{p^{\alpha-1}}$. This

result characterises soluble groups as the direct factors of Lagrangian groups and leads to the following definition.

Definition. For a p-soluble group G, denote by $n_p(G)$ the least value of the integer n for which $G \times Z_{p^n}$ is p-Lagrangian. (By the above remark, such an integer exists, and is less than α, where $p^\alpha \| \, |G|$.)

Lemma 1. *Let G_1 and G_2 be groups such that $G_1 \times G_2$ possesses a subgroup H of index n. Then there exist subgroups $H^1 \le G_1$, $H_2 \le G_2$ such that $H^1 \times H_2$ has index n in $G_1 \times G_2$.*

Proof. Let H^i be the projection of H on G_i and H_i be the intersection of H with G_i, $i = 1, 2$. Then $H_i \lhd H^i$, $i = 1, 2$, and $H^1/H_1 \cong H^2/H_2 \cong H/H_1 \times H_2$. Thus

$$|H^1 \times H_2| = |H^1|\,|H_2| = |H : H_1 \times H_2|\,|H_1|\,|H_2| = |H|,$$

as required.

Proposition 4. *Let G be a p-soluble group and let $\{n_1, \cdots, n_r\}$, where $n_1 < \cdots < n_r$, be the set of integers n such that G has a subgroup of index p^n. Then if $p \mid |G|$,*

$$n_p(G) = \max_{1 \le i \le r-1} (n_{i+1} - n_i) - 1, \tag{4}$$

while $n_p(G) = 0$ otherwise.

Proof. We assume that $p \mid |G|$ to avoid triviality. Denoting the right-hand side of (4) by n, we first show that $G \times Z_{p^n}$ is p-Lagrangian. Let H_i be a subgroup of G of index p^{n_i}, $1 \le i \le r$, so that $H_1 \times Z_{p^n}, \cdots, H_r \times Z_{p^n}, H_r \times E$ are subgroups of $G \times Z_{p^n}$ of indices

$$p^{n_1}, \cdots, p^{n_r}, p^{n_r+1} = p^{n_r+n} \tag{5}$$

respectively. Now let β be any integer such that $p^\beta \mid |G \times Z_{p^n}|$, so that $n_1 \le \beta \le n_{r+1}$, since $n_0 = 0$ and $p^{n_{r+1}} \| \, |G \times Z_{p^n}|$. If β is one of the integers (5) we are finished, and if not we have $n_i < \beta < n_{i+1}$ for some integer i with $1 \le i \le r$. Therefore $\beta - n_i < n_{i+1} - n_i \le n + 1$ and there is a subgroup K of Z_{p^n} of index $p^{\beta - n_i}$, whence $H_i \times K$ is a subgroup of $G \times Z_{p^n}$ of index p^β, as required.

It remains to prove that for any integer $m < n$, $G \times Z_{p^m}$ is not p-Lagrangian. Since m is less than the right-hand side of (4), we can find an i, where $1 \le i \le r - 1$, such that

$$m + 1 < n_{i+1} - n_i. \tag{6}$$

Assume, for a contradiction, that $G \times Z_{p^m}$ is p-Lagrangian, so that $G \times Z_{p^m}$ has a subgroup of index $p^{n_{i+1}-1}$. By Lemma 1, there are subgroups $H \leq G$, $K \leq Z_{p^m}$, such that $|G : H|\,|Z_{p^m} : K| = p^{n_{i+1}-1}$. Setting $|Z_{p^m} : K| = p^s$, we have $0 \leq s \leq m$ and $|G : H| = p^{n_{i+1}-1-s}$. But using (6), $n_i < n_{i+1} - 1 - m \leq n_{i+1} - 1 - s < n_{i+1}$, contradicting the definition of the n_i.

The first and second halves of the preceding proof generalise immediately to yield the two parts of the following result.

Proposition 5. *Let G be a p-soluble group and H a group with $p^\alpha \| \, |H|$; then*

(a) *if $\alpha \geq n_p(G)$ and H is p-Lagrangian, then $G \times H$ is p-Lagrangian,*

(b) *if $G \times H$ is p-Lagrangian, then $\alpha \geq n_p(G)$.*

For any p-soluble group G, we denote by (G) the class of groups $\{H | G \times H$ is p-Lagrangian$\}$. While basic properties of (G) are given in the above two propositions, it would be interesting to know more about this class. For example, can anything be said about those G such that $G \in (G)$? Also is it possible to characterise those elements H of (G) such that (a) H is not p-Lagrangian, and (b) $p^\alpha \| \, |H|$, where $\alpha = n_p(G)$?

We mention one further result of this type.

Proposition 6. *The following three properties of a p-soluble group G with $p^\alpha \| \, |G|$, $\alpha > 0$, are equivalent:*

(a) *some direct power of G is p-Lagrangian,*

(b) *some direct power of G lies in (G),*

(c) *G has subgroups of indices p and $p^{\alpha-1}$.*

Proof. (a) $\Rightarrow$ (b). Obvious.

(b) $\Rightarrow$ (c). Suppose H is a direct power of G lying in (G). Then $G \times H$ is Lagrangian and so contains a subgroup of index p. It follows from the above lemma that either G or H has a subgroup of index p. In the first case we are done, while in the second, we let $H = H_0 = H_1 \times G$, and deduce again that either G or H_1 has a subgroup of index p. Since $H_s = G$ for some s, we can continue in this way until, after finitely many steps, we obtain a subgroup of index p in G. A similar process yields a subgroup of index $p^{\alpha-1}$ in G.

(c) $\Rightarrow$ (a). For $\alpha \leq 3$, G is already p-Lagrangian. We prove that, for $\alpha \geq 4$, the direct product D of $\alpha - 2$ copies of G is p-Langrangian.

Let H, K, L be subgroups of G of indices p^α, $p^{\alpha-1}$, p respectively and let $p^\beta | \, |D|$ so that $0 \leq \beta \leq \alpha(\alpha - 2)$. By Euclid's theorem $\beta = q(\alpha - 1) + r$, $0 \leq r < \alpha - 1$, and since $\beta < (\alpha - 1)^2$, we have $0 \leq q < \alpha - 1$. If $r + q \leq \alpha - 2$, then $L^{\times r} \times K^{\times q} \times G^{\times s}$, where $s = (\alpha - 2) - (r + q)$ is a subgroup of D of index p^β. If, on the other hand, $\alpha - 2 < r + q < 2\alpha - 3$, then $L^{\times(r-s)} \times K^{\times(q-s)} \times H^{\times s}$ has the required index, where $s = r + q - (\alpha - 2)$. Thus, D is p-Langrangian as required.

Note that the results of this section may be stated in terms of Lagrangian, rather than just p-Lagrangian groups.

3. **Wreath products.** In this section, we prove a single result.

Proposition 7. *Let G be a Lagrangian group of exponent e and H be a cyclic group of order p such that e divides $(p - 1)$; then the standard wreath product $W = H \wr G$ is a Lagrangian group.*

Proof. (a) Let k be the field of p elements and B the base group of W. Then B is a right kG-module via conjugation by the elements of G and as such is isomorphic to kG itself. Since $W/B \cong G$, and is therefore Lagrangian, W has subgroups of all possible q-power indices whenever q is a prime different from p (since $p \nmid |G|$ and $|B|$ is a p-power). Thus, it will be sufficient to show that for each integer n between 0 and $|G|$, B contains a G-invariant subgroup of order p^n or, equivalently, that the right regular representation of G over k contains kG-submodules of all possible dimensions. Since e divides $(p - 1)$, k is a splitting field for G, and thus the irreducible modules over kG are in one-to-one degree-preserving correspondence with those of $\mathcal{C}G$, where $\mathcal{C}$ denotes the complex numbers. Thus it will be enough to prove the corresponding assertion for each soluble group G over the field $\mathcal{C}$.

(b) We proceed by induction on the derived length of G, the result being clear for abelian groups. Let $G^{(l)}$ be the last nontrivial term of the derived series of G and let $X_1, \cdots, X_\alpha$ be the irreducible $\mathcal{C}G$-modules obtained by inflation from $G/G^{(l)}$. Denote the remaining irreducibles by $Z_1, \cdots, Z_\beta$, of degrees $z_1, \cdots, z_\beta$, respectively. Since $G^{(l)}$ is abelian, we have by Itô's theorem (see [1]) that $z_i \mid t$ where $t = |G/G^{(l)}|$. Now write $\mathcal{C}G = X \oplus Z$, where X involves only the X_i and Z only the Z_j, so that X contains $\mathcal{C}G$-submodules of all possible dimensions by induction. Now let $Z = Z_\gamma > \cdots > Z_0 = (0)$ be a composition series for Z, and let $Z_{\gamma+1} = \mathcal{C}G$. Then for any integer n between 0 and $|G|$, we can find an m such that $\dim Z_m \leq n \leq \dim Z_{m+1}$, where $n - \dim Z_m \leq \dim Z_{m+1}/Z_m \leq t$, by the above, so that X has a submodule, Y say, of dimension $n - \dim Z_m$. It follows that $\mathcal{C}G$ has a submodule, viz. $Y \oplus Z_m$, of dimension n, and this completes the proof.

Note. It would be interesting to have a purely group-theoretical characterisation of the class $\mathfrak{A}$ of groups possessing the property proved for soluble groups in (b) above. $\mathfrak{A}$ properly contains the class of soluble groups, as the group SL(2, 5) has distinct irreducible characters of degrees 1, 2, 2, 3, 3, 4, 4, 5, 6. On the other hand, $\mathfrak{A}$ contains no nonabelian simple group, since the only complex character of degree 2 for such a group is trivial and so is not in the regular character.

4. **The classes $\mathfrak{X}$ and $\mathfrak{Y}$.** As noted in §0, the class $\mathfrak{X}$ of groups all of whose meet-irreducible subgroups have prime-power index consists solely of supersoluble groups. Since every subgroup of a group G is an intersection of meet-irreducible subgroups of G, it is obvious that $\mathfrak{X}$ consists precisely of those groups G having the property: for every subgroup H of G there exist subgroups $X_1, \cdots, X_n$ of G such that each $|G:X_i|$ is a prime-power and $H = \bigcap_{i=1}^n X_i$. This leads us to define the subclass $\mathfrak{Y}$ of $\mathfrak{X}$ to consist of those groups G having the same property with the restriction that the $|G:X_i|$ are pairwise coprime. Since $\mathfrak{Y} \subseteq \mathfrak{S}$, one easily proves the following result (to be found in [4]).

Lemma. *The following two conditions on a group G are equivalent*:

(a) $G \in \mathfrak{Y}$,

(b) *for any subgroup H of G and any integer n dividing $|G:H|$, there is a subgroup K of G such that $H \leq K$ and $|G:K| = n$.*

It is unknown to us whether or not $\mathfrak{X} = \mathfrak{Y}$; we give three partial results in this direction.

Proposition 8. $s\mathfrak{X} = s\mathfrak{Y}$.

Proof. Since $\mathfrak{Y} \subseteq \mathfrak{X}$ it is sufficient to show that $s\mathfrak{X} \subseteq \mathfrak{Y}$, by standard properties of the operation s. We assume the result to be false and let G be a minimal counterexample. Let H be a subgroup of G such that H is not the intersection of subgroups of pairwise coprime prime-power indices in G and let $|G:H|$ be minimal with respect to this property. Let p be the largest prime dividing $|G|$ and N a minimal normal subgroup of G of order p (such an N exists by the Sylow tower property, since G is supersoluble by [2]). Now if $N \leq H$, the result follows, since $s\mathfrak{X}$ is closed under homomorphic images. Thus we have that $H < NH$ and if $|G:H| = p^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (where the p_i are all distinct and the α_i all nonzero), we deduce by the minimality of $|G:H|$ that NH, and hence H, lies in a subgroup X of G with $|G:X| = p_1$. By the minimality of G and the subgroup closure of $s\mathfrak{X}$, there is a subgroup Y of X such that $H \leq Y$ and $|X:Y| = p^{\alpha}$. If $H \neq Y$, we can find a subgroup Z of G such that $|G:Z| = p^{\alpha}$ and $H < Y \leq Z$, by the minimality of $|G:H|$ again. But NH, and hence H, lies in subgroups $X_1, \cdots, X_r$ of G with $|G:X_i| = p_i^{\alpha_i}$, $1 \leq i \leq r$, by the above, whence $H = Z \cap \bigcap_{i=1}^r X_i$, a contradiction. We conclude that $H = Y$, and so $|G:H| = p^{\alpha} p_1$, where p_1 is a prime less than p. Now let M be a maximal subgroup of X containing H. If $M \neq H$, the minimality of $|G:H|$ entails the existence of a subgroup T of index p in G containing H, which by induction contains a subgroup S containing H with $|T:S| = p^{\alpha-1}$ so that $H = S \cap X$, a contradiction. Thus, $M = H$ and $|G:H| = pp_1$. Since $G \in \mathfrak{X}$, $H = \bigcap_{i=1}^s U_i$ where each $|G:U_i|$ is a prime power, and so $H = H \cap X = \bigcap_{i=1}^s (U_i \cap X)$, so for some i, say $i = 1$, $H = U_i \cap X$. Now $|G:U_1|$ is a prime power and so is either p or p_1. If $|G:U_1| = p_1$, H has p cosets in U_1, implying that X has p cosets in $XU_1 \subseteq G$. This leads to the contradiction $p \leq p_1$, and so $|G:U_1| = p$, which final contradiction proves the proposition.

Proposition 9. *Let $G \in \mathfrak{X}$ be a group of fourth-power-free order, then $G \in \mathfrak{Y}$.*

Proof. Assume that the result is false and let G be a minimal counterexample. As in the preceding proof, let H be a subgroup of minimal index such that H is not the intersection of subgroups of pairwise coprime prime-power indices in G. Let p be the largest prime dividing $|G|$, and N a minimal normal subgroup of G of order p. If $N \leq H$, a contradiction follows by induction, while if $N \not\leq H$, by the minimality of $|G:H|$, NH, and hence H lies in a subgroup X_q of G with $|G:X_q| = q^{\alpha}$, where the prime power $q^{\alpha} \| |G:H|$, for all $q \neq p$. Thus it suffices to show that H is contained as a subgroup of p'-index in some subgroup X of G with $|G:X|$ a p-power. Since $N \not\leq H$, we know that $p \mid |G:H|$, and by Hall's theorem, we have $p \mid |H|$. Thus, by hypothesis, the p-part of $|G:H|$ is either p or p^2. Now let $H = \bigcap_{i=1}^{n} X_i$, with each $|G:X_i|$ a prime power. We claim that p divides $|G:X_i|$ for some i. If not, we use the supersolubility of G to construct chains $X_i = X_{i,0} < X_{i,1} < \cdots < X_{i,\alpha_i} = G$ where each $|X_{i,j}:X_{i,j-1}|$ is a prime smaller than p. These chains intersect to yield a chain from H up to G with the index of each member in the next less than p, which is impossible. Hence we can assume that $|G:X_1|$, say, is a p-power. Since the representation $H = \bigcap_{i=1}^{n} X_i$ can be assumed irredundant, $H < \bigcap_{i=2}^{n} X_i < G$, the last inclusion being proper since otherwise $G = X_1$. By the minimality of $|G:H|$, we can write $\bigcap_{i=2}^{n} X_i = \bigcap_{j=1}^{m} Y_j$ with the $|G:Y_j|$ pairwise coprime prime-powers. If each $|G:Y_j|$ is prime to p, the representation $H = X_1 \cap \bigcap_{j=1}^{m} Y_j$ yields a contradiction. Otherwise, we can assume that p divides $|G:Y_1|$, say. By the above argument with chains of subgroups, we see that $|X_1 \cap Y_1 : H|$ is prime to p, and if $H < X_1 \cap Y_1$ we have a contradiction, again using the minimality of $|G:H|$. Thus, $H = X_1 \cap Y_1$, and this representation is irredundant. Since the p-part of $|G:H|$ is either p or p^2, we must have $|G:X_1| = p = |G:Y_1|$, so that $|G:H| \leq p^2$. But if the p-part of $|G:H|$ is p, X_1 is the required subgroup X of G, while otherwise there is a positive integer k such that $kp^2 = |G:H| \leq p^2$, proving that $|G:H| = p^2$, a contradiction. Thus the proposition is proved.

It follows at once from this that, if G is a minimal counterexample to the assertion $\mathfrak{X} \subseteq \mathfrak{Y}$, then $|G|$ is divisible by p^4, where p is the largest prime dividing $|G|$.

Proposition 10. *Let $G \in \mathfrak{X}$, p be the largest prime dividing $|G|$, P be a Sylow p-subgroup of G and g be an arbitrary element of G. Then there exists an integer n such that, for each $x \in P$, $x^g \equiv x^n \bmod (\Phi(P))$.*

Proof. Since $\mathfrak{X} = q\mathfrak{X}$ and $P \lhd G$, we can assume that $\Phi(P) = E$. We claim that for each $x \in P$, $\langle x \rangle \lhd G$. Suppose this to be false, and choose $g \in G$ such that $x^g \notin \langle x \rangle$. Writing $g = g_1 g_2$, with $g_2 \in P$, and g_1 a p'-element of G, we have that $x^{g_1} \notin \langle x \rangle$. Now write

$$\langle x \rangle = \bigcap_{i=1}^{r} X_i \cap \bigcap_{j=1}^{s} Y_j$$

where each $|G:X_i|$ is a p-power and $|G:Y_j|$ is a prime power coprime to p. Since $P \lhd G$, $P \leq Y_j$ for all j, and we have

$$\langle x \rangle = \langle x \rangle \cap P = \bigcap_{i=1}^{r} X_i \cap \bigcap_{j=1}^{s} Y_j \cap P = \left(\bigcap_{i=1}^{r} X_i\right) \cap P.$$

Now for any i, X_i contains a Hall p'-subgroup of G and so, by Hall's theorem, there is an $a_i \in P$ such that $g_1^{a_i} \in X_i$. We let $g_1^{a_i} = g_i$ and obtain, since P is a normal abelian subgroup of G, that $x^{g_i} = x^{g_1^{a_i}} = x^{g_1} \notin \langle x \rangle$, but x^{g_1} is a member of X_i for all i and also lies in P. Hence, $x^{g_1} \in (\bigcap_{i=1}^{r} X_i) \cap P = \langle x \rangle$, a contradiction.

Thus, for each $x \in P$, $g \in G$, we have $x^g = x^i$ for some integer i; it remains to prove that i is independent of x. Let $x, y \in P \setminus E$ and $g \in G$, and let $x^g = x^i$, $y^g = y^j$ with $0 \leq i, j \leq p-1$. If $y \in \langle x \rangle$, it follows at once that $i = j$, while if not, let $(xy)^g = (xy)^k$, $0 \leq k \leq p-1$, so that $x^i y^j = x^k y^k$, and it now follows from the linear independence of x and y that $i = k$ and $j = k$, as required.

Corollary 1. *Let $G \in \mathfrak{X}$, p be the largest prime dividing $|G|$ and P a Sylow p-subgroup of G. Then $G/PC_G(P)$ is cyclic of order dividing $p-1$.*

Proof. Consider the composite homomorphism

$$G \xrightarrow{\lambda} \mathrm{Aut}(P) \xrightarrow{\mu} \mathrm{Aut}(P/\Phi(P)),$$

where λ is induced by conjugation and μ is the usual canonical homomorphism. By the proposition, $\mathrm{Im}\,\lambda\mu$ lies in the centre of $\mathrm{Aut}(P/\Phi(P))$ (which is cyclic of order $(p-1)$) and since μ is one-to-one on the p'-elements of $\mathrm{Aut}(P)$, it follows that the Hall p'-subgroup of $\mathrm{Im}\,\lambda$ is cyclic of order dividing $(p-1)$. Since $\mathrm{Im}\,\lambda \cong G/C_G(P)$, the corollary is proved.

Corollary 2. *Let G be an element of minimal order in $\mathfrak{X} \setminus \mathfrak{Y}$; then, with the above notation, G/P is cyclic of order dividing $(p-1)$.*

Proof. Let H be a subgroup of minimal index in G such that H is not the intersection of subgroups of pairwise coprime indices in G. Then H is core-free, since $\mathfrak{X} = q\mathfrak{X}$. Since $|HO_p(G):H|$ and $|HO_{p'}(G):H|$ are coprime, it follows from the minimality of $|G:H|$ that at least one of $O_p(G)$, $O_{p'}(G)$ lies in H, and so we deduce that $O_{p'}(G) = E$. But $PC_G(P) = P \times O_{p'}(G)$, and the result follows from Corollary 1.

Addendum. The first author has constructed an example of a group of order $2 \cdot 3^6$ which is in $\mathfrak{X}$ but not in $\mathfrak{Y}$.

REFERENCES

1. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR 37 #302.

2. D. L. Johnson, *A note on supersoluble groups*, Canad. J. Math. 23 (1971), 562–564. MR 43 #7513.

3. D. J. McCarthy, *A survey of partial converses to Langrange's theorem on finite groups*, Trans. New York Acad. Sci. 33 (1971), 586–594.

4. D. H. McLain, *The existence of subgroups of given order in finite groups*, Proc. Cambridge Philos. Soc. 53 (1957), 278–285. MR 19, 13.

5. O. Ore, *Contributions to the theory of groups of finite order*, Duke Math. J. 5 (1939), 431–460.

6. G. Zappa, *Remark on a recent paper of O. Ore*, Duke Math. J. 6 (1940), 511–512. MR 2, 1.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LIVERPOOL, LIVERPOOL, ENGLAND (Current address of J. F. Humphreys)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, URBANA, ILLINOIS 61801

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NOTTINGHAM, NOTTINGHAM, ENGLAND (Current address of D. L. Johnson)