NORMAL p-SUBGROUPS OF SOLVABLE LINEAR GROUPS

JOHN D. DIXON

(Received 24 June 1966)

1. Introduction

In his paper [8], N. Itô gives an elegant proof that the Sylow p-group of a finite solvable linear group of degree n over the field of complex numbers is necessarily normal if $p > n+1$. Moreover he shows that this bound on p is the best possible when p is a Fermat prime (i.e. a prime of the form $2^{2^k}+1$), but that the bound may be improved to $p > n$ when p is not a Fermat prime.

The object of this paper is to prove the following generalization of Itô's theorem.

THEOREM. *Let p be a given prime, and let G be a finite solvable completely reducible subgroup of the general linear group $GL(n, \mathscr{F})$ over a perfect field $\mathscr{F}$. Let P be a Sylow p-group of G, and let K denote the p-core of G (i.e. K is the largest normal p-subgroup of G). If $|P:K| = p^\lambda$, then $\lambda \leqq \lambda_p(n)$ where*

$$\lambda_p(n) = \begin{cases} \sum_{i=0}^{\infty} \left[\dfrac{n}{p^i(p-1)}\right] & \text{if } p \text{ is a Fermat prime,} \\ \sum_{i=1}^{\infty} \left[\dfrac{n}{p^i}\right] & \text{if } p \text{ is odd and not a Fermat prime,} \\ \left[\dfrac{4n}{3}\right] - 1 & \text{if } p = 2. \end{cases}$$

(Here $[x]$ denotes the greatest integer $\leqq x$, and so the formally infinite sums each only have a finite number of nonzero terms.)

REMARK. Evidently Itô's theorem is an immediate consequence of this theorem since $\lambda = 0$ implies that P is normal in G. We shall later show that the values for $\lambda_p(n)$ ($p \neq 2$) are best possible in the sense that for each value of n there is a group G satisfying the hypotheses of the theorem with $\lambda = \lambda_p(n)$. The value for $\lambda_2(n)$ is less precise; it is attained for infinitely many n but not for all n.

There are two simple corollaries to the Theorem.

Corollary 1. *Let G be a finite solvable completely reducible subgroup of* $GL(n, \mathscr{F})$ *where* $\mathscr{F}$ *is a perfect field of characteristic* p. *If the Sylow* p-*group of G has order* p^μ, *then* $\mu \leqq \lambda_p(n)$.

Corollary 2. *Let G be a finite solvable subgroup of* $GL(n, \mathscr{F})$ *where* $\mathscr{F}$ *is a perfect field of characteristic* p. *Let P be a Sylow* p-*group of G, K be the* p-*core of G, and put* $p^\lambda = |P : K|$. *Then* $\lambda \leqq \lambda_p(n)$. (*Thus when the field has characteristic* p *we may drop the hypothesis of complete reducibility.*)

Remark. Corollary 1 is a substantial improvement on results of B. Huppert ([6] Satz 13, Satz 14). Huppert shows that, if $\mathscr{F}$ is the finite field with p^f elements, then $\mu \leqq f(3n/p-1)$ if p is odd, and $\mu \leqq f(n-1)$ if $p = 2$. Since any finite field is perfect, our Corollary 1 gives a better estimate (independent of f) except when $\mathscr{F}$ has two elements.

2. The proof of the Theorem in the primitive case

We begin with the observation that G remains completely reducible in any finite normal extension of $\mathscr{F}$ (see [2] Theorem (70.15)), and hence that G is completely reducible over the algebraic closure of $\mathscr{F}$. Thus, without loss in generality, we shall assume that $\mathscr{F}$ *is algebraically closed.*

We now proceed to the proof of the Theorem. The technique is similar to that used in [3], and in fact the connexion between these results is even more obvious when we note that p^λ is just the order of the Sylow p-groups of $G/F(G)$ (where $F(G)$ is the Fitting subgroup of G). Once again the critical case hinges on an analysis of the primitive solvable groups, and we begin with that.

We shall use the theorem of Suprunenko ([9] Theorem 11) quoted in [3]:

Let G be a solvable primitive subgroup of $GL(n, \mathscr{F})$ *where* $\mathscr{F}$ *is an algebraically closed field. Let* $n = q_1^{l_1} \cdots q_k^{l_k}$ *be the cannonical decomposition of n into prime factors. Then G has a normal nilpotent subgroup A such that G/A is isomorphic to a subgroup of the direct product of the symplectic groups* $Sp(2l_i, q_i)$ $(i = 1, \cdots, k)$.

Now let G be a solvable primitive group satisfying the hypotheses of our Theorem. Since the Sylow p-group of the group A (defined above) is a normal p-subgroup of G, it is clear that p^λ divides $|G/A|$. If p^{ν_i} is the highest power of p dividing $|Sp(2l_i, q_i)|$ $(i = 1, \cdots, k)$, then $\lambda \leqq \nu_1 + \cdots + \nu_k$ by Suprunenko's theorem. This means that, if we can prove $\nu_i \leqq \lambda_p(q_i^{l_i})$ for each i, then $\lambda \leqq \sum_{i=1}^{k} \lambda_p(q_i^{l_i}) \leqq \lambda_p(n)$ as required. Thus, in order to show that our Theorem holds in the case G is primitive, it is sufficient to prove the following lemma.

LEMMA. *If q is a prime, l is an integer $\geqq 1$, and p^ν is the highest power of p dividing $|Sp(2l, q)|$, then $\nu \leqq \lambda_p(n)$.*

PROOF. We recall that

$$|Sp(2l, q)| = (q^{2l}-1)(q^{2l-2}-1)\cdots(q^2-1)q^{l^2}$$

(see [1] page 147). If $p = q$, then $\nu = l^2 \leqq p^{l-1}+p^{l-2}+\cdots+1 \leqq \lambda_p(p^l)$ if $p \geqq 3$, and $\nu = l^2 \leqq [4.2^l/3]-1 = \lambda_2(2^l)$ if $p = 2$. This proves the result in this case.

Now suppose that $p \neq q$. Then p^ν divides

$$(q^l+1)(q^l-1)(q^{l-1}+1)\cdots(q+1)(q-1).$$

Since $q^i-1 \neq q^{i-1}+1$ unless $q = 2$ and $q^i-1 = 3$, p^ν divides $3\cdot(q^l+1)!$. It is well known that the exponent of the highest power of p dividing $m!$ is $\sum_{i=1}^{\infty}[m/p^i]$, and so, by direct calculation;

(i) $$\nu \leqq \sum_{i=1}^{\infty}\left[\frac{q^l+1}{p^i}\right] = \sum_{i=1}^{\infty}\left[\frac{q^l}{p^i}\right] = \lambda_p(q^l)$$

if p is odd and not a Fermat prime;

(ii) $$\nu \leqq \sum_{i=1}^{\infty}\left[\frac{q^l+1}{p^i}\right] \leqq \sum_{i=1}^{\infty}\left[\frac{q^l}{p^{i-1}(p-1)}\right] = \lambda_p(q^l)$$

if p is a Fermat prime and $p \neq 3$;

(iii) $$\nu \leqq 1+\left[\frac{q^l+1}{3}\right]+\sum_{i=2}^{\infty}\left[\frac{q^l+1}{3^i}\right] \leqq \left[\frac{q^l}{2}\right]+\sum_{i=1}^{\infty}\left[\frac{q^l}{2\cdot 3^i}\right] = \lambda_3(q^l)$$

if $p = 3$ and $l \geqq 2$ (and $\nu \leqq \lambda_3(q)$ if $l = 1$);

(iv) $$\nu \leqq \sum_{i=1}^{\infty}\left[\frac{q^l+1}{2^i}\right] \leqq q^l \leqq \left[\frac{4q^l}{3}\right]-1 = \lambda_2(q^l)$$

if $p = 2$ (since $q \geqq 3$).

This completes the proof of the lemma, and hence completes the proof of the Theorem for the case G primitive.

3. The proof of the Theorem in the general case

We shall proceed by induction on the degree n. The reduction to the primitive case (considered in § 2) is very similar to the corresponding reduction in the proof of Theorem 1 of [3]. Therefore we shall outline the steps and refer to [3] for details.

https://doi.org/10.1017/S1446788700004481 Published online by Cambridge University Press

We begin with a few observations. Let us write $\lambda_p(G) = \lambda$ when p^λ is the index of the p-core of G in a Sylow p-group of G. Then it is easily seen that for a direct product of finite groups we have

$$\lambda_p(G_1 \times \cdots \times G_d) = \lambda_p(G_1) + \cdots + \lambda_p(G_d).$$

Similarly, if H is a subgroup of G, then $\lambda_p(H) \leqq \lambda_p(G)$.

We now proceed to the proof of the Theorem. Since we have already dealt with the primitive case in § 2, we have two cases to consider.

(a) *Suppose that G is reducible.* Then G is isomorphic to a subgroup of a direct product $G_1 \times G_2$ where G_i is a finite solvable completely reducible subgroup of $GL(n_i, \mathscr{F})$ and $n_1 + n_2 = n$. (Compare [3].) Hence, by the observations above and the induction hypothesis,

$$\lambda = \lambda_p(G) \leqq \lambda_p(G_1) + \lambda_p(G_2) \leqq \lambda_p(n_1) + \lambda_p(n_2) \leqq \lambda_p(n_1 + n_2) = \lambda_p(n).$$

(b) *Suppose that G is irreducible but imprimitive.* Then there is a divisor $d > 1$ of n such that G has a normal subgroup N with the following properties. (See [2] Theorem (50.2).) First G/N is isomorphic to a subgroup of the symmetric group S_d. Secondly N is isomorphic to a subgroup of the direct product $N_1 \times \cdots \times N_d$ where the N_i are each isomorphic to a finite solvable completely reducible subgroup of $GL(m, \mathscr{F})$ (with $m = n/d$). (Compare [3].) Therefore, from the observations above and the induction hypothesis,

$$\lambda = \lambda_p(G) \leqq \rho + \sum_{i=1}^{d} \lambda_p(N_i) \leqq \rho + d\lambda_p(m)$$

where p^ρ is the highest power of p dividing $d!$. Thus, it remains to prove that

$$\rho + d\lambda_p(m) \leqq \lambda_p(md). \tag{1}$$

The proof of (1) is trivial if $p = 2$. In the other cases it is convenient to put $p' = p - 1$ or p depending on whether p is or is not a Fermat prime. (1) is obvious if $m < p'$, so suppose that $m \geqq p'$ and choose the integer $j \geqq 0$ so that $p^j p' \leqq m < p^{j+1} p'$. Then

$$\rho = \sum_{i=1}^{\infty} \left[\frac{d}{p^i}\right] \leqq \sum_{i=1}^{\infty} \left[\frac{md}{p^{i+j} p'}\right]$$

and

$$d\lambda_p(m) = \sum_{i=0}^{j} d \left[\frac{m}{p^i p'}\right] \leqq \sum_{i=0}^{j} \left[\frac{md}{p^i p'}\right].$$

Hence, by addition, (1) follows.

This completes the proof of the Theorem.

4. Limiting cases of the Theorem

We shall give examples in terms of matrix groups over the field $\mathscr{C}$ of complex numbers, but of course there are corresponding examples in terms of linear transformations.

If p is a Fermat prime, then Itô gives an example in [7] of a finite solvable matrix group of degree $p-1$ over $\mathscr{C}$ with a Sylow p-group which is not normal. On the other hand, if p is not a Fermat prime, then the matrix group of degree p generated by the permutation matrix

$$\begin{pmatrix} \cdot & 1 & \cdot & & \\ \cdot & \cdot & 1 & & \\ & & & \ddots & \\ \cdot & \cdot & & & 1 \\ 1 & \cdot & & & \cdot \end{pmatrix}$$

together with all diagonal matrices with diagonal entries ± 1 is a finite solvable group with a Sylow p-group which is not normal. These examples show that the bound $\lambda_p(n)$ is exact when $n = p-1$ or p depending on whether p is a Fermat prime or not.

We now show that if $p \neq 2$ then there is a finite solvable matrix group G of degree n over $\mathscr{C}$ for which $\lambda_p(G) = \lambda_p(n)$. For convenience we write $p' = p-1$ or p depending on whether p is or is not a Fermat prime, and we put $m = [n/p']$. Since $\lambda_p(n) = \lambda_p(mp')$, it is sufficient to construct G of degree mp'. Let G_0 be a finite solvable matrix group of degree p' over $\mathscr{C}$ which has a nonnormal Sylow p-group (see above). We define N as the matrix group of degree mp' consisting of all block diagonal matrices diag $(x_1, \cdots, x_m)$ with each $x_i \in G_0$. Let H be a group of block permutation matrices of degree mp' (with blocks of degree p' of the form 0 or 1) such that H is isomorphic to a Sylow p-group of the symmetric group S_m. It is clear that N is normalized by H, and that $G = HN$ is a finite solvable group. It is easily verified that G has no nontrivial normal p-subgroup (compare with [3] § 4), and that the Sylow p-group of G has order p^λ where

$$\lambda = \lambda_p(N) + \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right].$$

(The latter sum is the largest exponent to which p divides $m!$.) Since $\lambda_p(N) = m$ and $[m/p^i] = [n/p'p^i]$ for each $i \geqq 0$,

$$\lambda = \sum_{i=0}^{\infty} \left[\frac{n}{p'p^i}\right] = \lambda_p(n)$$

as required.

5. The proof of the Corollaries

Proof of Corollary 1. The p-core K of G is completely reducible by Clifford's theorem ([2] Theorem (49.2)). Since the only completely reducible linear p-group over a field of characteristic p is the trivial group ([2] Theorem (27.28)), therefore $K = 1$ and $|P| = p^\lambda$. Hence $\mu = \lambda \leqq \lambda_p(n)$ by the Theorem.

Proof of Corollary 2. We may choose a basis for the underlying vector space so that (for some integers $n_i \geqq 1$ with $n_1 + \cdots + n_s = n$) each element x in G has a corresponding matrix of the form

$$\begin{pmatrix} x_1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ * & & & \cdot \\ & & & x_s \end{pmatrix} \tag{2}$$

where the $n_i \times n_i$ blocks x_i on the diagonal correspond to the irreducible components of G, and all entries above these blocks are zero. In particular, the group

$$G_i = \{x_i \text{ in } (2) \, | x \in G\}$$

is an irreducible matrix group of degree n_i over $\mathscr{F}$ $(i = 1, \cdots, s)$. It follows from Corollary 1 that, if the order of the Sylow p-group of G_i is p^{μ_i}, then $\mu_i \leqq \lambda_p(n_i)$. On the other hand, the subgroup

$$H = \{x \in G \mid x_i = 1 \text{ for } i = 1, \cdots, s \text{ in } (2)\}$$

is a normal subgroup of G, and H is a p-subgroup because $\mathscr{F}$ is of characteristic p. Hence H is the p-core of G, and

$$\lambda \leqq \mu_1 + \cdots \mu_s \leqq \lambda_p(n_1) + \cdots + \lambda_p(n_s) \leqq \lambda_p(n).$$

6. Comments

(a) The theorem of Suprunenko used in § 2 also allows us to make a more detailed analysis of the structure of the factor group P/K in the Theorem. For example, if p is odd and $n < p(p-1)$, then it is not hard to show that P/K is an elementary abelian p-group.

(b) Itô points out in [8] that his theorem is equally true for p-solvable groups. In the same way it may be shown that the Theorem of the present paper remains true under the hypothesis that G is p-solvable (rather than solvable) — provided we add the condition that the factor group P/K is cyclic. I do not known what the situation is without this additional condition. On general grounds (e.g. using Jordan's theorem [2]

Theorem (36.13)) it can be seen that a theorem analogous to the Theorem proved here must hold even when there is no solvability condition imposed on G. From the results of Feit and Thompson [5] and Feit [4] it might be conjectured that the corresponding bounds will be about twice $\lambda_p(n)$, but the proof would certainly be much more difficult.

References

[1] E. Artin, *Geometric Algebra*, (Interscience 1957).
[2] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, (Interscience 1962).
[3] J. D. Dixon, "The Fitting subgroup of a linear solvable group", *J. Australian Math. Soc.* 7 (1967), 417–424.
[4] W. Feit, "Groups which have a faithful representation of degree less than p—1", *Trans. Amer. Math. Soc.* 112 (1964), 287—303.
[5] W. Feit and J. G. Thompson, "On groups which have a faithful representation of degree less than (p—1)/2", *Pacific J. Math.* 11 (1961), 1257—1262.
[6] B. Huppert, "Lineare auflösbare Gruppen", *Math. Z.* 67 (1957), 479—518.
[7] N. Itô, "On the characters of soluble groups", *Nagoya Math. J.* 3 (1951), 31—48.
[8] N. Itô, "On a theorem of H. Blichfeldt", *Nagoya Math. J.* 5 (1953), 75—78.
[9] D. Suprunenko, "Soluble and Nilpotent Linear Groups", *Amer. Math. Soc. Transl. Math. Monographs* vol. 9, 1963.

University of New South Wales