PROCEEDINGS OF
SYMPOSIA IN PURE MATHEMATICS
VOLUME VI

1960 INSTITUTE ON FINITE GROUPS

Held at California Institute of Technology
Pasadena, California
August 1—August 28, 1960

EDITOR
Marshall Hall, Jr.

AMERICAN MATHEMATICAL SOCIETY
190 HOPE STREET, PROVIDENCE, RHODE ISLAND
1962

This Institute was
Sponsored by the
AMERICAN MATHEMATICAL SOCIETY,
and supported by
THE NATIONAL SCIENCE FOUNDATION
under grant NSF-G 10091

Library of Congress Catalog Card Number 62-10812

CONTENTS

p-LENGTH THEOREMS

BY

G. HIGMAN

As motivation and introduction, I begin with a self-contained account of

1. Finite groups of exponent six. Such a group, G say, is soluble.

(i) *G has a normal series $G \supset H \supset K \supset 1$, such that G/H, K are 3-groups, and H/K is a 2-group.*

We take K to be the largest normal 3-subgroup of G, and H/K to be the largest normal 2-subgroup of G/K.

H contains the centraliser of H/K.

Otherwise there exists M normal in G, in the centraliser of H/K, such that M/H is a 3-group. Then M/K is the direct product of its Sylow subgroups, and if T/K is the Sylow 3-subgroup, T/K is characteristic in M/K and so normal in G/K, whence T is a larger normal 3-subgroup than K.

It follows that every 2-element of G belongs to H. For a Sylow 2-subgroup of G is abelian; and since H/K is a 2-group we may choose coset representatives for K in H out of a preassigned Sylow 2-subgroup and hence to commute with any 2-element. This proves (i).

(ii) *G has a normal series $G \supset L \supset M \supset 1$ such that G/L, M are 2-groups, and L/M is a 3-group.*

This, though formally similar to (i), is more difficult.

We choose M, L, N in turn so that M is the largest normal 2-subgroup of G, L/M the largest normal 3-subgroup of G/M, and N/L the largest normal 2-subgroup of G/L, so that we have to show $N = G$. Almost as in (i) we have

L contains the centraliser of L/M.

N contains the centraliser of N/L.

But we cannot finish as in (i), because a Sylow 3-subgroup of G is not necessarily abelian. L/M is a 3-group, and we let F/M be its Frattini subgroup. Then

L is the centraliser of L/F.

If the centraliser is greater than L, it contains an element not in L of order 2, by the choice of L. Such an element induces in L/M a non-trivial automorphism, of order prime to 3, which is the identity on L/F. This is impossible.

L/F is an elementary abelian 3-group, and so can be identified with a vector space over the field of three elements. The automorphisms induced by elements of G are linear transformations of the vector space. They form a representation of G, or since the kernel is L, a faithful representation of G/L. Consider first the way N/L is represented. N/L is a 2-group, so the representation is completely reducible; however, N/L is abelian and of exponent 2, so that the irreducible components are of dimension 1. Putting together isomorphic summands into one block, we express V as a direct sum

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

where, on each summand V_i, each element n of N is represented by a scalar multiplication $v \rightarrow \chi^{(i)}(n)v$. If N is not the whole of G, there is an element g in G, not in N, of order 3. Then operation by g permutes the summands V_i, because $gNg^{-1} = N$. Suppose that for some i, $V_i g = V_i$. Then, for v in V_i, n in N,

$$\chi^{(i)}(gng^{-1})v = vgng^{-1} = (vg)ng^{-1} = \chi^{(i)}(n)v \,.$$

Thus $\chi^{(i)}(gng^{-1}) = \chi^{(i)}(n)$ and so $\chi^{(i)}(n^{-1}gng^{-1}) = 1$. Now g does not centralise N/L, so that we can choose n so that $n^{-1}gng^{-1}$ is not in L; and then $n^{-1}gng^{-1}$ does not centralise L/F, so that for some i, $\chi^{(i)}(n^{-1}gng^{-1}) \neq 1$. This implies that $V_i g \neq V_i$. Since g is of order 3, there are three V_i permuted cyclically by g, and hence a vector v such that v, vg, vg^2 are linearly independent; in particular $vg^2 + vg + v \neq 0$.

Reverting to multiplicative notation, this means that there is an element y of L such that

$$(gy)^3 = g^{-2}yg^2 \cdot g^{-1}yg \cdot y$$

is not in F, whence gy is of order 9 at least. This contradiction proves that $N = G$, and establishes (ii).

Either (i) or (ii) is sufficient to establish the restricted Burnside conjecture for exponent 6. Together they can be used to establish the order of the largest finite k-generator group of exponent 6.

2. The general problem. Abstracting from the above, one considers, for any finite group G and for any prime p, *the upper p-series of G*:

$$1 \subset N_0 \subset P_1 \subset N_1 \subset P_2 \subset \cdots \subset P_i \subset N_i \subset P_{i+1} \cdots$$

where $P_0 = 1$, N_i/P_i is the largest normal subgroup of G/P_i of order prime to p (p'-subgroup) and P_{i+1}/N_i the largest normal p-subgroup of G/N_i. This will be of real interest only if, for some l, $N_l = G$. The condition for this is that every chief-factor (or equivalently every composition-factor) of G is either a p-group or a p'-group. If so G is *p-soluble* and $l = l_p = l_p(G)$, the *p-length of G*, is the least integer l for which $N_l = G$.

Then the fundamental results on exponent six say that, if G is of exponent 6, then $l_2 \leqq 1$ and $l_3 \leqq 1$. The general problem is to find conditions, and particularly conditions on the Sylow p-subgroup of G, which imply bounds for the p-length. This can be pursued at three levels of difficulty, the first two of which correspond to the cases $l_2 = 1$ and $l_3 = 1$ for exponent 6, while in the third a different kind of difficulty occurs.

In all cases, the fundamental lemma is:

For $i \geqq 1$, P_i contains the centraliser of P_i/N_{i-1}; and N_i contains the centraliser of N_i/P_i.

If, for instance, the centraliser Z of P_1 is not in P_1, let M be a normal subgroup of G with $P_1 \subset M \subset ZP_1$, the first inequality being strict, and M being minimal. Then M/P_1 is a p'-group, by the definition of P_1. By the

Schur-Zassenhaus theorem, P_1/N_0 is complemented in M/N_0, say by X/N_0. Elements of X induce inner automorphisms in P_1/N_0, because $X \subset ZP_1$, and automorphisms of order prime to p because X/N_0 is a p'-group. That is, M/N_0 is the direct product of P_1/N_0 and X/N_0, whence X is normal in G, contrary to the definition of N_0.

The simplest level of attack on p-length theorems uses this result within the Sylow p-subgroup of G. For instance:

If S is a Sylow p-subgroup of G, the centre of S is contained in P_1.

Since P_1/N_0 is a p-group, $P_1 \subset SN_0$, so that we may choose elements of S as coset representatives in P_1/N_0. The elements of the centre of S commute with these representatives, so that a fortiori they centralize P_1/N_0, hence $S \subset P_1$.

If the Sylow p-subgroup has class c_p, then $l_p \leqq c_p$.

Proof by induction on l_p. G/P_1 has p-length $l_p - 1$, and its Sylow subgroup is isomorphic to $S/S \cap P_1$. Since the centre of S is in $S \cap P_1$, this has class at most $c_p - 1$; thus the induction hypothesis gives $l_p - 1 \leqq c_p - 1$, as required. The case $l_p = 1$ being trivial, the result follows.

3. Second level attack. This begins by improving the "centraliser" theorem slightly for the p-factors, P_i/N_{i-1}.

If F_i/N_{i-1} is the Frattini subgroup of the p-group P_i/N_{i-1}, then P_i is the centraliser of P_i/F_i.

The centraliser contains P_i, because P_i/F_i is abelian; and if it were larger, there would be p'-elements which centralise the Frattini factor group P_i/F_i of P_i/N_{i-1} but not P_i/N_{i-1} itself, which is impossible.

Thus G/P_i is represented faithfully as a group of automorphisms of the elementary abelian p-group P_i/F_i; that is, as a linear group over a field of characteristic p. At the second level of attack we seek to exploit this (in particular with $i = 1$) but, to avoid the worst difficulties, we make the assumption that *Sylow q-subgroups of G, for primes q other than p, are abelian.* We observe that, in addition to being a linear group over a field of characteristic p, G/P_1 is a p-soluble group with no non-trivial normal p-subgroup.

If, changing the notation, G is any linear group over a field of characteristic p, and g is an element of order p^n in G, then $g^{p^n} = 1$, so that $(g-1)^{p^n} = 0$, but $g^{p^{n-1}} \neq 1$, so that $(g-1)^{p^{n-1}} \neq 0$. Thus the minimal equation of g is $(x-1)^r$, for some r in the range $p^{n-1} < r \leqq p^n$. In general, no more can be said; but one of the most important weapons used in proving p-length theorems, and a fact that has proved useful in other directions, is that if G is p-soluble with no non-trivial normal p-subgroup, much more can be said.

If G is a p-soluble linear group over a field of characteristic p, has no non-trivial normal p-subgroup, and has abelian Sylow q-subgroups for $q \neq p$, then the minimal equation of an element of order p^n is $(x-1)^{p^n} = 0$.

Let g be an element of G of order p^n, and let N be the largest normal p'-subgroup of G. We show first that there exists a Sylow q-subgroup Q of N for some prime q, such that g normalises Q, but $g^{p^{n-1}}$ does not centralise it. Indeed, for each prime q dividing the order of N, there is a Sylow q-subgroup normalised by g, since the number of such subgroups is prime to p. If this group were centralised by $g^{p^{n-1}}$ for all q, the order of the centraliser of $g^{p^{n-1}}$ in N would equal the order of N, so that $g^{p^{n-1}}$ would centralise N, which it does not. Q, by our basic assumption, is abelian.

Now consider Q as a linear group. Its order is prime to p, so that it is completely reducible. We can, if necessary, extend the base field so that the irreducible components of Q are absolutely irreducible, and so one-dimensional. This will not alter the minimal equation of g. Then V, the vector space on which G operates, can be written as a direct sum

$$V = V_1 \oplus \cdots \oplus V_k$$

of minimal characteristic Q-modules, and any element x of Q acts, on V_i, as a scalar multiplier: $v \to \chi^i(x)v$.

Because Q is normalised by g, operation by g permutes the summands V_i. We shall show that this permutation has at least one p^n-cycle. If not, $g^{p^{n-1}} = h$ maps each V_i into itself, whence, for each i, and for each x in Q, $\chi^i(h^{-1}xh) = \chi^i(x)$, and $\chi^i(x^{-1}h^{-1}xh) = 1$. But this means $x^{-1}h^{-1}xh = 1$, so that h centralises Q, which is not so.

Hence the permutation of the V_i induced by g includes at least one p^n-cycle, whence the degree of the minimal equation of g is at least p^n, proving the theorem.

As an illustration of the way this yields p-length theorems:

Let G be a p-soluble group, with abelian Sylow q-subgroups, $q \neq p$, such that, for elements x in a Sylow p-subgroup, $x^{p^e} = 1$. Then its p-length is at most e.

Proof by induction on the p-length of G. If, as usual, the upper series is

$$1 \subset N_0 \subset P_1 \subset N_1 \subset \cdots ,$$

then G/P_1 has p-length $l_p(G) - 1$; if we can show that its p-elements satisfy $x^{p^{e-1}} = 1$ we are clearly home. If not, there is an element x in G, whose order modulo P_1 is p^e. Applying the theorem, the minimal equation of the transformation of P_1/F_1 induced by x has degree p^e, so that for some y in P_1 (which we can assume belongs to the same Sylow p-subgroup as x)

$$y \cdot x^{-1}yx \cdot x^{-2}yx^2 \cdot \cdots \cdot x^{-p^e+1}yx^{p^e-1} \neq 1$$

indeed, is not in F_1. But then

$$(yx^{-1})^{p^e} x^{p^e} \neq 1$$

whence either yx^{-1} or x has order p^{e+1}, proving the result.

4. Top level attack. Preliminaries. We now see what happens if we try to throw out the condition that Sylow subgroups for $p \neq q$ are abelian. We begin with an example to show that, as they stand, the theorems do not remain valid in this case.

Put $G = TQ$, Q a normal quaternion subgroup, T a cycle of order 3 which induces in Q an automorphism of order 3. It is easily verified that G has a representation of degree 2, over the field of three elements. Thus if i, j, k

are the quaternion units, and $t^{-1}(i, j, k)t = (j, k, i)$, we may take

$$i \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad j \rightarrow \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}, \quad k \rightarrow \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad t \rightarrow \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Clearly, the minimal equation of t is $(t-1)^2 = 0$, not $(t-1)^3 = 1$; and if we extend G by an elementary abelian 3-group $\mathscr{H}$, so that G operates in the above way on it, $G\mathscr{H}$ has 3-length 2, but contains no elements of exponent 9. Thus the theorems above have to be modified if there exist non-abelian q-groups, $q \neq p$, in G.

Before indicating the modifications, we prove:

THEOREM. *Let $G = PN$, where P is a Sylow p-subgroup, N a normal p'-subgroup, and let g be an element of P which does does not centralise N. Then for some prime $q \neq p$, N contains a q-subgroup Q, normalised by P but not centralised by g, such that* (i) *Q is either elementary abelian, or has $Q' = Z(Q) = \Phi(Q)$; and* (ii) *Q/Q' is transformed irreducibly by P, and Q' trivially.*

We take Q to be any subgroup of N which is normalised by P but not centralised by g, and which is minimal subject to this. Then for some prime q, Q is a q-group. For Q is certainly of order prime to p, so that, for each prime dividing its order, P normalises some Sylow subgroup. If Q is no q-group, these Sylow subgroups are proper subgroups, so that by the minimality of Q, g centralises them, and hence centralises Q itself, a contradiction.

Then $Q/\Phi(Q)$ is a direct product of groups transformed irreducibly by P; if there is more than one of these we have a contradiction to the minimality of Q. Moreover g does not centralise $Q/\Phi(Q)$. Now let X be a subgroup of Q normalised by P. which contains $x^{-1}g^{-1}xg$ for all x in Q. Because g does not centralise $Q/\Phi(Q)$, $X\Phi(Q)$ is greater than $\Phi(Q)$; and because P transforms $Q/\Phi(Q)$ irreducibly, this implies that $X\Phi(Q) = Q$. By the fundamental property of the Frattini subgroup, this implies $X = Q$.

We use this fact twice. First, let X be the subgroup of Q consisting of those elements whose qth powers are in Q'. X is characteristic in Q, so it admits P. But, modulo Q', we have

$$(x^{-1} \cdot g^{-1}xg)^q \equiv x^{-q}g^{-1}x^q g .$$

Now $\Phi(Q)$ is a proper subgroup of Q which admits P, so that, by the minimality of Q, g centralises $\Phi(Q)$, whence $x^{-q}g^{-1}x^q g = 1$. Thus X satisfies our conditions, and $X = Q$, which is to say $\Phi(Q) = Q'$. Second, consider C, the centraliser of $\Phi(Q)$. Obviously, C admits P. But if y belongs to $\Phi(Q)$ so does $x^{-1}yx$ for any x in Q, and so

$$y = g^{-1}yg , \quad x^{-1}yx = g^{-1}x^{-1}yxg .$$

Taken together, these imply that $x^{-1}g^{-1}xg$ belongs to C, so that $C = Q$, which is to say $Z(Q) \supset \Phi(G)$. Because P transforms $Q/\Phi(Q)$ irreducibly, this means that either $Z(Q) = Q$, in which case Q is elementary abelian, or $Z(Q) = \Phi(G)$.

We shall use the term *special q-group* to denote a q-group Q which either is abelian or satisfies $Q' = Z(Q) = \Phi(G)$; an *extraspecial q-group* is a non-abelian special q-group with cyclic centre.

5. Theorems of type 2.1.n. Reduction to special case. We shall be concerned to prove theorems of the following special kind. We shall be given a p-soluble linear group G of linear transformations of a vector space over a field of characteristic p, with no non-trivial normal p-subgroup. We shall be given elements $a, b, \cdots$ of a Sylow p-subgroup of G, and a word $u(a, b, \cdots)$ in these elements and their inverses; and a finite set $w_1, w_2, \cdots$ of linear combinations of such words. We may also be given a side-condition $\mathscr{C}$, such that if it holds for a group G it also holds for subgroups and factor groups of G. Then our theorem will be: *If G satisfies $\mathscr{C}$, and $u(a, b, \cdots) \neq 1$, at least one of $w_1, w_2, \cdots$ is not* 0.

For instance, "*If all q-subgroups of G are abelian, for $q \neq p$, and a is of order p^r, its minimal equation is* $(x-1)^{p^r} = 0$" is a theorem of this sort which we already know to be true. Another, which we shall prove later, is "*If a, b are of orders p^r, p^s, and the elements of orders p in the cyclic groups $\{a\}$ and $\{b\}$ do not commute, then either a has minimal equation $(x-1)^{p^r} = 0$ or b has minimal equation* $(x-1)^{p^s} = 0$."

Then we have:

In proving any theorem of this kind we may suppose

(i) *$G = PQ$, where P is a Sylow p-subgroup generated by $a, b, \cdots$, and Q is a normal special q-group, such that P transforms Q/Q' irreducibly and Q' identically.*

(ii) *G is absolutely irreducible.*

In the cases we deal with, we shall be able to strengthen (ii) to the assertion: *Q is absolutely irreducible*, but I do not know any reason to suppose this is true in general.

Assuming the special case to hold, we establish the general case. Let N be the greatest normal p'-subgroup of G, P the subgroup generated by $a, b, \cdots$, so that P acts faithfully as a group of automorphisms of N. This implies in particular that $u(a, b, \cdots)$ acts non-trivially on N. Then by the previous theorem, we can choose a special q-group Q in N which is normalised by P but not centralised by $u = u(a, b, \cdots)$, such that N acts irreducibly on Q/Q' and trivially on Q'. Let V be the vector space on which G, and so PQ, acts, and let

$$0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$$

be a composition series for V as PQ-module. The set of elements which act trivially on each factor V_{i+1}/V_i is a normal p-subgroup of PQ. Now u acts non-trivially on Q, so that the normal subgroup it generates is not a p-group. Hence we can choose i so that u acts non-trivially on V_{i+1}/V_i. Let $\bar{P}, \bar{Q}, \bar{u}$, etc., be the restrictions of P, Q, u, etc., to V_{i+1}/V_i. Then $\overline{PQ}$ is a p-soluble linear group, which is irreducible, and hence contains no non-trivial normal p-subgroup. $\bar{P}$ is a Sylow p-subgroup, generated by $\bar{a}, \bar{b}, \cdots$, elements such that $\bar{u} = u(\bar{a}, \bar{b}, \cdots) \neq 1$. $\bar{Q}$, as the maximal normal p'-subgroup of $\overline{PQ}$, is not centralised by any element outside it, in particular not by $\bar{a}$. But any proper subgroup of $\bar{Q}$ invariant under $\bar{P}$ is centralised by $\bar{u}$ (since its inverse image (in Q) is already centralised by u). Hence $\bar{Q}$ is a special q-group, and $\bar{P}$

transforms $\bar{Q}/\bar{Q}'$ irreducibly and $\bar{Q}'$ trivially. Thus we are in the special case envisaged in the theorem, except that $\bar{P}\bar{Q}$ is irreducible rather than absolutely irreducible, a matter that can be dealt with by a preliminary extension of the ground field. Thus one of $\bar{w}_1 = w_1(\bar{a}, \bar{b}, \cdots)$, $\bar{w}_2, \cdots$ is non-zero; and since these are images of $w_1, w_2, \cdots$ under a ring-homomorphism, one of $w_1, w_2, \cdots$ is non-zero.

6. Statement of theorems.

1) *Let G be a p-soluble group of linear transformations of a vector space over a field of characteristic p, with no non-trivial normal p-subgroup. Let g be an element of G of order p^n. Then the minimal equation of g is $(x-1)^r = 0$ where $r = p^n$, unless there is an integer $n_0 \leqq n$ such that $p^{n_0} - 1$ is a power of a prime q, and G has non-abelian Sylow q-subgroups, in which case, if n_0 is the smallest such integer, $p^{n-n_0}(p^{n_0} - 1) \leqq r \leqq p^n$.*

Obviously if $p^{n_0} - 1 = q^n$, either p or q is 2. If $q = 2$, $p - 1$ divides q^n, so that $p = 1 + 2^{n_0}$ is a *Fermat prime*. If $p = 2$, then $n_0 > 1$, so that $q^m \equiv 3(4)$. Thus m is odd, and from $p^{n_0} = 1 + q^n$ it follows that $1 + q$ is a power of 2 and $q = 2^t - 1$ is a *Mersenne prime*. Thus

(1) *If p is neither 2 nor a Fermat prime, $r = p^n$ always.*

(2) *If p is an odd Fermat prime $r = p^n$ if G has abelian Sylow 2-subgroups, and $r \geqq p^{n-1}(p-1)$ anyway.*

(3) *If $p = 2$, $r = p^n$ if G has abelian Sylow q-subgroups for all Mersenne primes less than 2^n; if $q = 2^{n_0} - 1$ is the least Mersenne prime for which this is not so, $r \geqq 2^{n-n_0}q$, and in any case $r \geqq 2^{n-2}3$.*

It will emerge from our argument that these results are best possible. An element g with $r < p^n$ will be called *exceptional*. The second theorem we shall require is:

2) *If, under the conditions of* 1), *g, h are elements of the same Sylow subgroup of G such that $(g^{p^{m-1}}, h^{p^{n-1}}) \neq 1$, then either $(g-1)^{p^{m-1}} \neq 0$, or $(h-1)^{p^{n-1}}(g-1)^{p^{m-1}} \neq 0$.*

This includes, but goes beyond, the statement that if g, h are both exceptional, then the elements of order p in $\{g\}$ and $\{h\}$ commute. *In proving* 1) *and* 2) *we can assume $G = PQ$, etc., and that Q is absolutely irreducible.* As usual we establish irreducibility, and assume the ground field chosen large enough for this to imply absolute irreducibility. We assume that the proof is by induction on the parameters n, or m and n, that enter into the theorem.

Q is certainly completely reducible; assume first that not all irreducible Q-components are equivalent, so that, if V is the vector space on which everything operates,

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_u$$

where the V_i are minimal characteristic Q-submodules, and $u > 1$. P operates as a permutation group on the V_i, and since PQ transforms V irreducibly, P permutes $V_1, \cdots, V_u$ transitively, and so P_1, the subgroup of P leaving V_1 fixed, is a proper subgroup.

If we are dealing with 1), P is the cyclic group $\{g\}$ of order p^n, so that P_1

is the cyclic group $\{g^{p^a}\}$ of order p^{n-a}, $a > 0$. If $a = n$, then (as in the second level attack) $(g-1)^{p^n-1} \neq 0$, so we may assume $k = g^{p^{n-1}}$ belongs to P_1. We can find x in Q so that $k^{-1}x^{-1}kx = y \neq 1$, and we can assume V_1 so chosen that $y \neq 1$ on V_1. It is clear that P_1Q, restricted to V_1, is a p-soluble group of linear transformations. It has no normal p-subgroup not 1; for if it did, this subgroup would have to contain $g^{p^{n-1}}$, and therefore y, a contradiction. Thus the minimal equation of g^{p^a} on P_1Q, by the induction hypothesis, is $(x-1)^{r_0} = 0$, where $r_0 = p^{n-a}$ if Q is abelian, or if no power p^b with $b \leqq n-a$ is $1 + q^c$, and where $0 \geqq p^{n-a-b}(p^b - 1)$ if p^b is the least power. Now for $i = 1, \cdots, p^a - 1$, and for v in V_1, vg^i belongs to V_{i+1}; so that for any integer s

$$v(g-1)^{p^a s-1} = v(g-1)^{p^a(s-1)+p^a-1} = v(g^{p^a}-1)^{(s-1)}(1 + g + g^2 + \cdots + g^{p^a-1})$$
$$= w + wg + wg^2 + \cdots + wg^{p^a-1}\,,$$
$$w = v(g^{p^a}-1)^{s-1}\,,$$

where the different terms are in different summands Then if $(g^{p^a}-1)^{s-1} \neq 0$ on V_1, we have $(g-1)^{p^a s-1} \neq 0$. Thus the minimal equation of g is $(g-1)^r$ with $r \geqq p^a r_0$. In the non-exceptional case this gives $r = p^n$, and in the exceptional, $r \geqq p^{n-b}(p^b-1)$ as required.

Now turn to 2), when P is generated by g, h, with $k = (g^{p^{m-1}}, h^{p^{n-1}}) \neq 1$. We can find x in Q so that $k^{-1}x^{-1}kx = y \neq 1$, and we can suppose that y restricted to V_1 is not 1. If the permutation of the V_i induced by g includes at least one p^m-cycle then as usual $(g-1)^{p^m-1} \neq 0$, and we are home. Thus $V_i g^{p^{m-1}} = V_i$ for all i. Suppose next that V_1 belongs to a cycle under h which contains at least p^n elements. Then for v in V_1

$$v(h-1)^{p^n-1} = v + vh + vh^2 + \cdots + vh^{p^n-1}$$

where the terms belong to different direct summands, and as v varies over V_1, so does vh^j over the corresponding V_{j+1} say. Thus if on any of these $g^{p^{m-1}}$ is not 1, we can choose v so that

$$v(h-1)^{p^n-1}(g-1)^{p^m-1} = v(g^{p^{m-1}}-1) + vh(g^{p^{m-1}}-1) + \cdots + vh^{p^m-1}(g^{p^{m-1}}-1)$$
$$\neq 0\,,$$

and again we are home. If, however, $g^{p^{m-1}}$ is 1 on all V_1h^r (even on V_1 and $V_1h^{-p^{n-1}}$) one shows easily that $k = (g^{p^{m-1}}, h^{p^{n-1}})$ is 1 on V_1, and hence that $y = k^{-1}x^{-1}kx$ is 1 on V_1, contrary to choice of V_1.

That is, we may assume that not only $g^{p^{m-1}}$ but also $h^{p^{n-1}}$ belongs to P_1, and we are now in a position to apply induction on m and n. Since P_1 is a proper subgroup of P, the first powers of g, h in P_1 are g^{p^a}, h^{p^b} where one of a, b is at least 1. Let U be an irreducible P_1Q-submodule of V_1. The restriction of P_1Q to U is a p-soluble linear group, and by irreducibility it has no non-trivial normal p-subgroup. Because V_1 is a sum of equivalent irreducible Q-modules, the fact that y is not 1 on V_1 implies that it is not 1 on U, and hence that k is not 1 on U. Thus if $\bar{g}, \bar{h}$ are the restrictions to U of g^{p^a} and g^{p^b}, $(\bar{g}^{p^{m-a-1}}, \bar{h}^{p^{n-b-1}}) \neq 1$. Since at least one of a, b is positive, we can apply induction to deduce that either $(\bar{g}-1)^{p^{m-a}-1}$ or $(\bar{h}-1)^{p^{n-b}-1}(\bar{g}-1)^{p^{m-a}-1}$

is not zero. That is, that either $(g-1)^{p^m-p^a}$ or $(h-1)^{p^m-p^b}(g-1)^{p^{m-1}}$ is non-zero on U. The argument is concluded exactly as in the case of 1), by remarking that for v in V_1 (or in particular in U), $v, vg, \cdots, vg^{p^a-1}$ belong to distinct direct summands, as do $v, vh, \cdots, vh^{p^b-1}$. It follows that if $v(g-1)^{p^m-p^a} \neq 0$ then even $v(g-1)^{p^{m-1}} \neq 0$, and if $v(h-1)^{p^n-p^b}(g-1)^{p^{m-1}} \neq 0$, then even $v(h-1)^{p^{n-1}}(g-1)^{p^{m-1}} \neq 0$.

We have, finally, to deal with the case in which the decomposition $V = V_1 \oplus \cdots \oplus V_u$ is trivial; that is, V is a direct sum of isomorphic irreducible Q-modules. In this case we show that there is only one such module, that is, Q is irreducible. Suppose in fact that

$$V = V_1 \oplus \cdots \oplus V_d$$

where $V_1, \cdots, V_d$ are now irreducible isomorphic Q-modules. Since we are dealing with an irreducible group PQ, there is no loss of generality in supposing that the base field is finite, say with p^e elements. Then we prove that V contains $1 + p^e + \cdots + p^{(d-1)e}$ irreducible Q-modules. This is obvious if $d = 1$, so we use induction on d. Then we have to show that the number of submodules *not* contained in $V_2 \oplus \cdots \oplus V_d$ is $p^{(d-1)e}$. But such a submodule consists of all elements

$$(v_1, v_1\alpha_2, \cdots, v_1\alpha_d)$$

where α_i, $i = 2, \cdots, d$, is a fixed homomorphism of V_1 into V_i. But V_1 is an (absolutely) irreducible module, so that there are p^e such homomorphisms, and $p^{(d-1)e}$ choices for $\alpha_2, \cdots, \alpha_d$ as required. Since P permutes these $1 + p^e + \cdots + p^{(d-1)e}$ submodules, it must leave at least one of them, say U fixed (since it is a p-group); and then U is a PQ-submodule. But V was irreducible, so that $U = V$ and $d = 1$.

This completes the proof that we can suppose Q absolutely irreducible.

7. Extraspecial q-groups. We have, then, to consider linear groups PQ, where Q is a normal, absolutely irreducible q-group, and P is a Sylow p-group, which we may assume transforms Q/Q' irreducibly.

The first stage is to investigate Q abstractly. Q/Q' is a vector space over the field F_q of q elements, say W. If c is a generator of Q', and x, y belong to Q, we can write $(x, y) = c^{\rho(x,y)}$. Here $\rho(x, y)$ can be considered as an element of F_q; and it depends only on the cosets mod Q' to which x, y belong. That is, it is a function from $W \times W$ to F_q. The usual commutator identities show that it is bilinear and skew-symmetric; and the fact that $Q' = Z(Q)$ shows that, given $x \neq 0$ in W, we can find y so that $\rho(x, y) \neq 0$. Thus $\rho(x, y)$ is a skew-symmetric form of maximum rank; and so W is a symplectic space. It follows that W is of even dimension, say $2l$, and that Q has order q^{2l+1}.

If x, y are elements of Q which do not commute, they generate a non-abelian group, Q_1 say, of order q^3. The centraliser of x has index q, since the only conjugates are xc^i, and similarly that of y, so that the centraliser Q_2 of Q_1 has index at most q^2. But $Q_1 \cap Q_2$ is the centre $\{c\}$ of Q_1; hence Q_2 has index q^2, and $Q = Q_1Q_2$. Thus, if $l > 1$, Q can be written as a central product of two proper subgroups. (G is the central product of its subgroups A, B if $G = AB$ and every element of A commutes with every element of B; then $A \cap B$ belongs to the centre of G, and G is isomorphic to a factor group $(A \times B)/K$ of the direct product of A and B, K being isomorphic to $A \cap B$.) We notice that Q_2, like Q_1, is extraspecial, since an element in its centre is in the centre of Q. More generally if Q_1 is any extraspecial subgroup of Q, and Q_2 is its centraliser, Q_2 is also extraspecial, and Q is the central product Q_1Q_2.

The advantage of expressing a group as a central product is in the hold it gives us over its representations. Consider first a direct product $A \times B$. We recall that if U, V are vector spaces over the same field, we can form their product space $U \otimes V$ (e.g., if $u_1, \cdots, u_m$ are a basis of U, and $v_1, \cdots, v_n$ are a basis of V, $u_i \otimes v_j$ can be taken as a basis of $U \otimes V$). If s, t are transformations of U, V into themselves we can form the transformation $s \otimes t$ of $U \otimes V$ into itself; and the map $(s, t) \rightarrow s \otimes t$ is bilinear in each of s and t, and $(s_1 \otimes t_1)(s_2 \otimes t_2) = s_1s_2 \otimes t_1t_2$. In matrix terms, if $S = (s_{ij})$ is the matrix of s, and T the matrix of t, the matrix of $s \otimes t$, if the basis vectors are properly ordered, is

$$\begin{bmatrix} s_{11}T & \cdots & s_{1m}T \\ \vdots & & \vdots \\ s_{m1}T & \cdots & s_{mm}T \end{bmatrix}.$$

Evidently, if $a \rightarrow s(a)$ and $b \rightarrow t(b)$ are representations of A, B as transformations of U and V, then $(a, b) \rightarrow s(a) \otimes t(b)$ is a representation of $A \times B$ as a transformation of $U \otimes V$. If the representations we start from are absolutely irreducible, so is the representation we finish with, since then the enveloping algebras are full matrix algebras. And conversely, every (classical) absolutely irreducible representation of $A \times B$ is obtained in this way (which we call forming the Kronecker product). Suppose indeed that we have such a representation, operating on a space U, and let U_0 be a subspace admitting B (absolutely) irreducibly. Then for each a in A, U_0a is a B-module isomorphic to U_0 so that the sum of such modules is the whole of U. Thus we can choose a basis for U so that the representation, for B, takes the form

$$b \rightarrow \begin{bmatrix} T(b) & & 0 \\ & \ddots & \\ 0 & & T(b) \end{bmatrix}.$$

A matrix representing an element a of A commutes with all these, and since the $T(b)$ span a full matrix algebra it has the form

$$\begin{bmatrix} s_{11}(a)I & \cdots & s_{1m}(a)I \\ \vdots & & \vdots \\ s_{m1}(a)I & \cdots & s_{mm}(a)I \end{bmatrix}.$$

Then the mapping $a \rightarrow [s_{ij}(a)]$ is a representation of A, and the representation we started with was the Kronecker product of $a \rightarrow (s_{ij}(a))$ and $T \rightarrow T(b)$.

If we are concerned with a central product $G = AB$, we can regard it as obtained from the direct product $A \times B$ by the homomorphism which identifies $(c, 1)$ with $(1, c)$ if c belongs to $A \cap B$; so that a representation of AB is just a representation of $A \times B$ which represents $(c, 1)$ and $(1, c)$ in the same way. Now c is a central element, both of A and of B, so that an absolutely irreducible representation represents it by a scalar, and it makes sense to say that two representations represent $A \cap B$ in the same way. Thus: *The absolutely irreducible representations of a central product AB can be obtained as Kronecker products of absolutely irreducible representations of A and of B which represent $A \cap B$ in the same way.*

Now, let Q be an extraspecial q-group; and let F be a field whose characteristic is not q, which contains a primitive q-root of unity ω, and also, if $q = 2$ and char $(F) = 0$, a primitive 4th root. Then *Q has just one absolutely irreducible representation in which the generator c of Q' is represented by ωI, and this can be written in the field F.*

Let Q have order q^{2l+1}. If $l = 1$, Q is a non-abelian group of order q^3, and the result is well known. If $l > 1$, Q is the central product of two proper extraspecial subgroups Q_1, Q_2, for which, by induction, we may assume the result proved. Any absolutely irreducible representation of Q representing c by ωI is a Kronecker product of absolutely irreducible representations of Q_1, Q_2 which represent c by ωI. By assumption, there is just one choice for each of Q_1, Q_2 and this representation can be written in F. Hence the same is true of Q.

8. Linear groups PQ with Q absolutely irreducible. Now continue the same assumptions, but add the hypothesis that F is finite and of characteristic p, and that Q is a normal subgroup of the group PQ (where P is a Sylow p-subgroup) which has a faithful representation in which Q is represented irreducibly. If V is the space on which PQ acts, we would like to be able to lay hands on V as a P-module. This there seems no way of doing. However (denoting the representation by ρ) we can lay our hands on the *enveloping algebra of $\rho(Q)$ considered as a P-module under $\rho(x) \to \rho(g^{-1}xg)$*, by means of the theorem of the previous section.

Let $\mathcal{Q}$ be the group-algebra of Q over F, and consider the factor algebra $\mathcal{Q}/\mathcal{Q}(c - \omega 1)$ where ω is the qth root such that $c = \omega I$, as a linear transformation. Since Q has just one absolutely irreducible representation, in which c is represented by ωI, and this can be written in the field F, $\mathcal{Q}/\mathcal{Q}(c - \omega 1)$ has just one absolutely irreducible representation and this can be written in F. Since $\mathcal{Q}/\mathcal{Q}(c - \omega 1)$ is semi-simple, this implies that it is a full matrix algebra over F. Since its dimension is q^{2l}, it is a $(q^l \times q^l)$ matrix algebra, which incidentally implies that the representation of PQ is of degree q^l. If g is an element of P then g acts, by transformation, both on $\mathcal{Q}/\mathcal{Q}(c - \omega 1)$ and also on the enveloping algebra of Q (as a linear group). Its mode of action in the two cases is precisely the same, since it has the same effect on the elements of Q, which span the algebra. We prove the special case of Theorem 1, to which it has been reduced, by comparing the dimensions of the centraliser of g in $\mathscr{Q}/\mathscr{Q}(c-\omega 1)$ and in the enveloping algebra.

We have an absolutely irreducible linear group PQ, where Q is absolutely irreducible and extraspecial, P is cyclic of order p^n and transforms Q/Q' irreducibly. Let q^{2l+1} be the order of Q. Because Q/Q' is transformed irreducibly (and faithfully) by P, it is isomorphic to the additive group of $\mathscr{F}_q(\theta)$, θ a p^nth root of 1, a generator of P acting as multiplication by θ. It follows that the elements of Q/Q' other than the identity are permuted by the generator in cycles all of length p^n. Since these elements form a basis for $\mathscr{Q}/\mathscr{Q}(c-\omega 1)$ we have: *The centraliser of P in $\mathscr{Q}/\mathscr{Q}(c-\omega 1)$ has dimension* $(q^{2l}-1)/p^n+1$.

The generator g of P is a linear transformation over a field of characteristic p satisfying $g^{p^n}-1=0$. Thus the Jordan canonical form of the corresponding matrix is

$$\begin{bmatrix} J_{\lambda_1} & & \\ & \ddots & \\ & & J_{\lambda_i} \end{bmatrix}$$

where J_λ is the $\lambda\times\lambda$ matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ & & \ddots & 1 \\ 0 & & \cdots & 1 \end{bmatrix};$$

here we may assume $p^n \geqq \lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_i \geqq \cdots$ (where superfluous λ_i's are put equal to 0, and the first inequality springs from the fact that $g^{p^n}-1=0$). Also, since we are dealing with a $q^l\times q^l$ matrix, we have $\lambda_1+\lambda_2+\cdots+\lambda_i+\cdots=q^l$. The centraliser of P is then the set of matrices which commute with the matrix above.

The centraliser of P has dimension $\sum(2i-1)\lambda_i$

This comes by direct computation. One obtain immediately that the dimension is $\sum_{i,j}\xi_{ij}$, where ξ_{ij} is the dimension of the set of matrices X_{ij} satisfying $J_iX_{ij}=X_{ij}J_j$. These matrices form $\operatorname{Hom}(M_i, M_j)$, where M_i is a cyclic $\mathscr{F}[x]$ module satisfying $ux^i=0$. Evidently, an element of $\operatorname{Hom}(M_i, M_j)$ is determined by the image of a generator. If $j\leqq i$, this image can be chosen at will; if $i\leqq j$ it must be chosen from the subset of those elements v satisfying $vx^i=0$. Thus in any case the dimension is $\min(i,j)$. Thus the dimension we are looking for is $\sum_{ij}\min(\lambda_i,\lambda_j)$; which is $\sum_i(2i-1)\lambda_i$, because the λ's have been arranged in descending order.

All but one of the non-zero λ_i's are equal to p^n, the other to p^n-1.

We first show that $q^l\equiv -1(p^n)$. If p^n is odd this is obvious, for q^{2l} is the order of the field generated by a p^nth root of unity, so that $p^n \nmid q^l-1$, but $p^n \mid q^{2l}-1$. Thus $p^n \mid q^l+1$, as asserted. If $p=2$, we have to proceed a little differently. We use the fact that Q/Q' is a symplectic space, and that transformation by g induces in it a symplectic transformation, and so, in particular, one of determinant 1. The determinant of the multiplication by θ is, of course, the norm $N(\theta)$, so that $\theta^{1+q+q^2+\cdots+q^{2l-1}}=1$, whence

$$2^n \mid (q^l - 1)(q^l + 1)/(q - 1) .$$

Since $2^n \nmid (q^l - 1)$, this implies that $q^l + 1$ is divisible by a higher power of 2 than $q - 1$. In particular $4 \mid q^l + 1$, so that $q \equiv 3(4)$ and l is odd. Thus $(q^l - 1)/(q - 1)$ is odd, and $2^n \mid q^l + 1$, as required.

Now if $q^l = ap^n + (p^n - 1)$, and we put $\mu_1 = \cdots \mu_a = p^n$, and $\mu_{a+1} = p^n - 1$, we have

$$\begin{aligned}\sum (2i - 1)\mu_i &= a^2 p^n + (2a + 1)(p^n - 1) \\ &= (a + 1)^2 p^n - (2a + 1)\end{aligned}$$

and

$$\begin{aligned}1 + (q^{2l} - 1)p^n &= 1 + \{[(a + 1)p^n - 1]^2 - 1\}/p^n \\ &= (a + 1)^2 p^n - (2a + 1) .\end{aligned}$$

Thus $\lambda_i = \mu_i$ gives a solution of our equations; that it is the only solution follows from the fact that any λ's satisfying

$$p^n \geqq \lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_i \geqq \cdots$$

and

$$\lambda_1 + \lambda_2 + \cdots + \lambda_i + \cdots = q^l$$

can be reduced to $\mu_1, \cdots, \mu_{a+1}$ by a sequence of moves each of which increases some λ_i at the expense of λ_j, where $j > i$, which decreases the sum $\sum (2i - 1)\lambda_i$.

We obtain (as part of our result):

If $G = PQ$ is a linear group over a field of characteristic p, where Q is an absolutely irreducible normal extraspecial q-group, and P is the cyclic group generated by the element g of order p^n, which transforms Q/Q' irreducibly, then the minimal equation of g is $(x - 1)^{p^n} = 0$ unless $p^n - 1$ is a power of q, in which case it is $(x - 1)^{p^n - 1} = 0$.

This, of course, is a more precise version of the missing special case of Theorem 1.

If we make the same assumptions except that g need no longer transform Q/Q' irreducibly, then g has minimal equation $(x - 1)^r = 0$ with $r < p^n$ only if (i) *$p^n - 1$ is a power of q and* (ii) *Q is the central product $Q = Q_1Q_2$, where g transforms Q_1/Q' irreducibly and Q_2/Q' trivially (here Q_2 may be trivial).*

We can choose a special q-subgroup Q_1 such that g transforms Q_1/Q_1' irreducibly and faithfully; and since $Q_1' \subset Q'$, Q_1 is either abelian or extraspecial. If Q_1 is abelian, the minimal equation of g is certainly $(x - 1)^{p^n} = 0$. If Q_1 is extraspecial, Q is the central product Q_1Q_2, where Q_2 is the centraliser of Q_1. We form groups $G_1 = \{g_1, Q_1\}$ and $G_2 = \{g_2, Q_2\}$, where g_i transforms the group Q_i in the same way as g, and has the appropriate order. If we form the central product of G_1 and G_2, we can evidently identify g with g_1g_2, abstractly; and hence, if we take appropriate irreducible faithful representations of G_1 and G_2, as a linear transformation g is identified with the Kronecker product $g_1 \otimes g_2$. If g centralises Q_2, g_2 is the identity, g_1 and g have the same minimal equation, and we are home. If not, by Theorem 1, g operates on some subspace like $J_{p^n-1} \otimes J_2$, which is to say (the characteristic being p) like $J_{p^n} \otimes J_{p^n-2}$. Thus g has minimal equation $(x-1)^{p^n} = 0$, proving the result.

9. Completion of the proof of Theorem 2. In the special case that remains to us this says: *Let $G = PQ$ be a linear group over a field of characteristic p, where Q is a normal, absolutely irreducible extraspecial q-group, and P is a Sylow p-group which transforms Q/Q' irreducibly and is generated by elements g and h satisfying $(g^{p^{m-1}}, h^{p^{n-1}}) \neq 1$. Then either $(g-1)^{p^{m-1}} \neq 0$ or $(h-1)^{p^{n-1}}(g^{p^{m-1}}-1) \neq 0$.*

We shall assume that $(g-1)^{p^{m-1}} = 0$, so that g is of order p^m and exceptional, and prove that $(h-1)^{p^{n-1}}(g^{p^{m-1}}-1) \neq 0$. The first step is to find out something about how P transforms Q/Q'. Elements of P induce a p-group of symplectic transformations of Q/Q' (with respect to a certain skew-symmetric form), which we may suppose to be a subgroup of some fixed Sylow p-subgroup of the symplectic group on Q/Q'. We shall describe such a Sylow subgroup, taking separately the two possible cases (i) p a Fermat prime, $q = 2$; and (ii) $p = 2$, q a Mersenne prime. We remark that the dimension of Q/Q' must be such that an irreducible symplectic p-group exists; but state the facts without proof.

(i) If $q = 2$, $p = 2^a + 1$ we let $\mathscr{F}^*$ be the field of 2^{2a} elements so that $\mathscr{F}^*$ contains a primitive pth root of unity, θ. Then under our assumption, Q/Q' can be regarded as a vector space over $\mathscr{F}^*$; and we let $x_1, x_2, \cdots$ be an $\mathscr{F}^*$ basis. For α in $\mathscr{F}^*$ let $\alpha' = \alpha^{2^a}$, so that $\alpha \to \alpha'$ is the automorphism of $\mathscr{F}^*$ of order 2. Then $\langle \sum \alpha_i x_i, \sum \beta_i x_i \rangle = \sum_i \mathrm{tr}\,(\alpha_i \beta_i')$ is a (skew-) symmetric form on Q/Q' (as a vector space over $\mathscr{F}_2$), which is easily seen to have top rank; indeed, for fixed i, it has top rank on the subspace of all αx_i, α in $\mathscr{F}^*$; so that the corresponding subgroup Q_i of Q is extraspecial. Since $\theta\theta' = \theta^{2^a+1} = \theta^p = 1$, the transformations

A(i): $$\sum \alpha_i x_i \to \sum \alpha_i \theta^{n_i} x_{\sigma(i)}$$

for all integers n_i, and all permutations σ, are symplectic. If σ is restricted to a Sylow p-subgroup of the symmetric group on $1, 2, \cdots$ they form a Sylow p-subgroup of the symplectic group, as is verified by counting them.

(ii) The results for $q = 2^b - 1$, $p = 2$, are similar but a bit more complicated. $\mathscr{F}^*$ is now the field of q^2 elements; and Q/Q' is again a vector space over $\mathscr{F}^*$ with $\mathscr{F}^*$ basis $x_1, x_2, \cdots$; but θ is now a primitive 2^{b+1}st root so that $\theta\theta' = -1$. The fundamental form is given by

$$\langle \sum \alpha_i x_i, \sum \beta_i x_i \rangle = \sum_i (\alpha_i \beta_i' - \alpha_i' \beta_i) .$$

We now have to define the transformations T_n of $\mathscr{F}^*$ by

$$T_n(\alpha) = \theta^n \alpha' \qquad (n \text{ odd}) ,$$

$$T_n(\alpha) = \theta^n \alpha \qquad (n \text{ even}) .$$

The transformations T_n form a generalized quaternion group; and the Sylow 2-group consists of transformations