ON IMPRIMITIVE SOLVABLE RANK 3 PERMUTATION GROUPS

BY

LARRY DORNHOFF[1]

We remind the reader that a permutation group G transitive on a set Ω is said to be of rank m, if the subgroup G_α fixing $\alpha \in \Omega$ has m orbits on Ω. Thus, rank 2 groups are doubly transitive groups. D. A. Foulser and the present author have independently classified primitive solvable rank 3 groups (Foulser's paper has appeared in the Transactions of the American Mathematical Society). Among finite solvable rank 3 groups, many imprimitive groups occur. This paper is a classification of those imprimitive solvable rank 3 permutation groups G with a regular normal subgroup N.

If G is such a permutation group on a set Ω and $\alpha \in \Omega$, then we have $G_\alpha N = G$, $G_\alpha \cap N = 1$. By Theorem 11.2 of [6], G_α is then an automorphism group of N acting with only two orbits on $N^\# = N - \{1\}$. Conversely, if N is any group with a solvable automorphism group A having only two orbits on $N^\#$, then the semidirect product $G = AN$ is a solvable rank 3 permutation group with regular normal subgroup N; G will be imprimitive if and only if A fixes some proper subgroup of N. Thus our problem is to classify those groups N with a solvable automorphism group having only two orbits on $N^\#$ (such an N is clearly solvable). Our main theorem is the following.

THEOREM. *Let N be a finite group, A a solvable automorphism group of N acting with only two orbits on $N^\# = N - \{1\}$. Then we have one of the following:*

(i) *N is an elementary abelian p-group for some prime p.*

(ii) *For some prime p, N is a direct product of cyclic groups of order p^2.*

(iii) *For primes p and q, the polynomial $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$, and N is a Frobenius group of order $qp^{m(q-1)}$ (m an integer). Here N has an elementary abelian Frobenius kernel of order $p^{m(q-1)}$.*

(iv) *For some integer $n > 2$ which is not a power of 2, and some automorphism $\theta \neq 1$ of $GF(2^n)$ of odd order,*

$$N = A(n, \theta)$$
$$= \{(\alpha, \zeta) \in GF(2^n) \times GF(2^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^\theta)\}.$$

Thus $|N| = 2^{2n}$.

(v) *For some integer $n \geqq 1$,*

$$N = B(n)$$
$$= \{(\alpha, \zeta) \in GF(2^{2n}) \times GF(2^n) \mid (\alpha, \zeta)(\beta, \eta)$$
$$= (\alpha + \beta, \zeta + \eta + \alpha\beta^{2^n}\mu + \alpha^{2^n}\beta\mu^{-1})\},$$

Received August 19, 1968.

[1] This work was done at Yale University under a contract from the Army Research Office, Durham, N. C.

where $\mu \in GF(2^{2n})$ *has order* $2^n + 1$. *Here* $|N| = 2^{3n}$, *and N does not depend on* μ.

(vi) *For some odd prime p and integer* $n \geqq 1$, *choose* $\varepsilon \in GF(p^{2n})$ *such that* $\varepsilon + \varepsilon^{p^n} = 0$. *Then*

$$\begin{aligned} N &= C(p, n) \\ &= \{\pi(\alpha, \zeta) \in GF(p^{2n}) \times GF(p^n) \mid (\alpha, \zeta)(\beta, \eta) \\ &\qquad = (\alpha + \beta, \zeta + \eta + \tfrac{1}{2}(\alpha\beta^{p^n} - \alpha^{p^n}\beta)\varepsilon)\}. \end{aligned}$$

Here $|N| = p^{3n}$, *and N does not depend on* ε.

(vii) *N is an extra special* 3*-group of order* 3^5 *and exponent* 3.

(viii) $N = P(\varepsilon)$, *where* $|P(\varepsilon)| = 2^9$, ε *is a multiplicative generator in* $GF(2^6)$, *and*

$$\begin{aligned} P(\varepsilon) = \{(\alpha, \zeta) \in GF(2^6) \times GF(2^3) \mid (\alpha, \zeta)(\beta, \eta) \\ = (\alpha + \beta, \zeta + \eta + \alpha\beta^2\varepsilon + \alpha^8\beta^{16}\varepsilon^8)\}. \end{aligned}$$

Furthermore, all these groups except $|N| = 2$ *have such solvable automorphism groups A; in case* (i), *one orbit of A can be* $H^{\#}$, *any proper subgroup H of N.*

We have thus determined the subdegrees (lengths of orbits of G_α) in each solvable imprimitive rank 3 permutation group G with regular normal subgroup N. If N is elementary abelian, $|N| = p^n$, then all possibilities $p^t - 1$ $p^n - p^t$ for $0 < t < n$ occur as subdegrees. If N is not elementary abelian, then N has an obvious unique characteristic proper subgroup K, and the subdegrees are $|K| - 1$, $|N| - |K|$.

We remark that the groups (iv) and (v) will be identified as among the Suzuki 2-groups of G. Higman [2]. The proof of our Theorem uses the methods of [2] quite heavily, and will begin after three number-theoretic Lemmas.

LEMMA 1. *Let p be a prime,* $n > 1$ *an integer. Then one of the following holds.*

(i) *There exists a prime q,* $q \mid (p^n - 1)$, $q \nmid (p^t - 1)$ *for any* $t < n$.

(ii) $n = 2$ *and* $p = 2^a - 1$ *is a Mersenne prime.*

(iii) $p = 2, n = 6$.

Proof. See [1].

LEMMA 2. *Let p be a prime,* $n \geqq 4$ *an integer. Suppose that integers* e_2, e_3, e_4, a_1, a_2, a_3 *exist, satisfying* $e_i = \pm 1$ *and* $n > a_1 > a_2 > a_3 > 0$, *such that*

$$(p^n - 1) \mid n(p^{a_1} + e_2 p^{a_2} + e_3 p^{a_3} + e_4).$$

Then we have one of the following:

(i) $(5^4 - 1) \mid 4(5^3 + 5^2 + 5 + 1)$.
(ii) $(3^8 - 1) \mid 8(3^6 + 3^4 + 3^2 + 1)$.
(iiia) $(3^4 - 1) \mid 4(3^3 + 3^2 + 3 + 1)$.
(iiib) $(3^4 - 1) \mid 4(3^3 - 3^2 + 3 - 1)$.
(iva) $(2^6 - 1) \mid 6(2^5 - 2^4 + 2^2 + 1)$.
(ivb) $(2^6 - 1) \mid 6(2^5 - 2^3 - 2 - 1)$.
(ivc) $(2^6 - 1) \mid 6(2^5 - 2^3 - 2^2 + 1)$.
(ivd) $(2^6 - 1) \mid 6(2^4 + 2^3 - 2 - 1)$.
(ive) $(2^6 - 1) \mid 6(2^4 + 2^3 - 2^2 + 1)$.
(ivf) $(2^6 - 1) \mid 6(2^4 + 2^2 + 2 - 1)$.

Proof. Denote $k = (n, p^n - 1)$. Then we have an equation

$$t(p^n - 1) = k(p^{a_1} + e_2 p^{a_2} + e_3 p^{a_3} + e_4)$$

for some integer $0 < t < k$. Therefore $t + e_4 k \equiv 0 \pmod{p^{a_3}}$, which implies $p^{a_3} < 2k$. Now set $t + e_4 k = p^{a_3} t_1$, where we see $0 < |t_1| < k$; substituting into the equation, we get

$$-p^{a_3} t_1 \equiv k(p^{a_1} + e_2 p^{a_2} + e_3 p^{a_3}) \pmod{p^n}.$$

This implies $t_1 + e_3 k \equiv 0 \pmod{p^{a_2 - a_3}}$, and therefore $p^{a_2 - a_3} < 2k$. We now set $t_1 + e_3 k = p^{a_2 - a_3} t_2$, and see that $0 < |t_2| < k$; continuing this substitution process also gives us $p^{a_1 - a_2} < 2k$ and $p^{n - a_1} < 2k$. We have now proved that $p^n < 16\,(n, p^n - 1)^4$. The only solutions of this inequality are $p^n = 2^6, 3^4, 3^8, 5^4, 5^6$ or 7^4. It is now easy to verify that (i)–(ivf) are the only cases actually occurring. (Repeat the argument of the proof, with specific values of p and n.)

LEMMA 3. *Let p be a prime, $n > 2$ an integer. If integers $i, j, k, l \geqq 0$ satisfy the congruence*

$$p^i + p^j \equiv p^k + p^l \pmod{(p^n - 1)/(n, p^n - 1)},$$

then we have $i - j \equiv \pm(k - l) \pmod{n}$.

Proof. This congruence is equivalent to the relation

$$(p^n - 1) \mid n(p^i + p^j - p^k - p^l).$$

If some exponent t is $\geqq n$, then since $np^t = np^{t-n}(p^n - 1) + p^{t-n} \equiv np^{t-n} \pmod{p^n - 1}$, we can replace p^t by p^{t-n}. Therefore we may assume $0 \leqq i, j, k, l < n$.

If i, j, k, l are all different, then inspection of Lemma 2 shows that the present lemma holds. If one of the relations $i = k, j = k, i = l, j = l$ holds, then two terms drop out and we are left with a relation $(p^n - 1) \mid n(p^u - 1)$, some $u < n$. $u = 0$ means the conclusion of the Lemma holds, so we may take $0 < u < n$. This now contradicts Lemma 1, unless $p^n = 2^6$. The relation $(2^6 - 1) \mid 6(2^u - 1)$ is impossible for $0 < u < 6$. We conclude that we may assume $i \neq k, j \neq k, i \neq l, j \neq l$ in any counterexample to Lemma 3.

Therefore either $i = j$ or $k = l$; by symmetry we may assume that $i = j$, $k \neq l$, in any counterexample to Lemma 3. We thus have

$$2p^i \equiv p^k + p^l \pmod{(p^n - 1)/(n, p^n - 1)}.$$

If $k < i$ or $l < i$, we replace p^k by p^{k+n} or p^l by p^{l+n}, not destroying the congruence, and then divide by p^i. Hence if Lemma 3 has a counterexample, we have a relation

$$(*) \qquad (p^n - 1) \mid n(p^k + p^l - 2), \qquad 0 < k < l < n.$$

Let $s = (n, p^n - 1)$; we have an equation $t(p^n - 1) = s(p^k + p^l - 2)$, $0 < t < s$, $2s - t \equiv 0 \pmod{p^k}$. Therefore $p^k < 2s$. We set $2s - t = p^k u$, where $0 < u < s$; substituting for t in the equation, we get

$$p^k u \equiv sp^k + sp^l \pmod{p^n}.$$

Therefore $u \equiv s \pmod{p^{l-k}}$, which implies $p^{l-k} < s$. Setting $s - u = p^{l-k}v$ we see $0 < v < s$; substituting for u in the last congruence mod p^n, we get $s + v \equiv 0 \pmod{p^{n-l}}$, implying $p^{n-l} < 2s$. We have proved that $p^n < 4(n, p^n - 1)^3$. The only solutions of this inequality are $p^n = 3^4$ or 2^6, and we easily see that they provide no example of $(*)$, Q.E.D. for Lemma 3.

Proof of the theorem. Clearly, if a group N has an automorphism group with only two orbits on $N^\#$, then N has at most one proper characteristic subgroup and has nonidentity elements of at most two different orders. If N is abelian, this means that N is a p-group, either elementary or a direct product of cyclic groups of order p^2. If N is nonabelian, N may be either a p-group with $\Phi(N) = Z(N) = N'$, or N may be a p, q-group for primes p and q. These four possibilities will be studied separately.

First, let N be elementary abelian of order p^n. If $|N| = 2$, then $|\mathrm{Aut}(N)| = 1$, so $\mathrm{Aut}(N)$ has only one orbit on $N^\#$. If $|N| = p$ and $p > 2$, then Aut (N) has a subgroup A of order $\frac{1}{2}(p - 1)$ having only two orbits on $N^\#$. If $|N| = p^n$ and $n > 1$, choose a proper subgroup H of N, $|H| = p^t$. Automorphisms of N fixing H may be represented by block matrices

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix},$$

where A is $t \times t$, B is $(n - t) \times t$, 0 is a $t \times (n - t)$ zero matrix, and C is $(n - t) \times (n - t)$. Such matrices multiply by the rule

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}\begin{pmatrix} D & 0 \\ E & F \end{pmatrix} = \begin{pmatrix} AD & 0 \\ BD + CE & CF \end{pmatrix}.$$

Let $N = H \times K$ for some subgroup K of H, and let G_1, G_2 be solvable groups of matrices on H and K transitive on $H^{\#}$ and $K^{\#}$, respectively. (Such groups always exist, and are classified in [4]). Define

$$J = \left\{ \begin{pmatrix} A & 0 \\ B & C \end{pmatrix} \middle| \, A \in G_1 \,, C \in G_2 \,, B \text{ any } (n - t) \times t \text{ matrix} \right\}.$$

Then J is certainly solvable, and transitive on $H^{\#}$ and $N - H$. This shows that the group (i) of our theorem exists.

Now suppose $N = H_1 \times H_2 \times \cdots \times H_m$, each H_i cyclic of order p^2. Let $T = \{a \in \text{Aut } (N) \,|a \text{ is trivial on } N/\Phi(N)\}$. Then easy counting arguments show that $|T| = p^{m^2}$, $|\text{Aut } (N)| = p^{m^2} |GL(m, p)|$. This implies that Aut (N) has an element ψ of order $p^m - 1$, by Theorem II.7.3 of [3]. T is transitive on $x\Phi(N)$ for any $x \in N - \Phi(N)$, so we conclude that $T\langle\psi\rangle$ is a solvable automorphism group of N, transitive on $N - \Phi(N)$ and $\Phi(N)^{\#}$. N is case (ii) of our theorem.

We next suppose that N is nonabelian, and that two primes p and q divide $|N|$. Fit (N) is the unique proper characteristic subgroup of N (obviously N is not nilpotent), so let $P =$ Fit (N), an elementary abelian normal Sylow p-subgroup. N has no element of order pq, so N is a Frobenius group. A Sylow q-subgroup Q must be an abelian Frobenius complement of exponent q, so $|Q| = q$ by Theorem V.8.7(a) of [3]. Let A be a solvable automorphism group of N, transitive on $N -$ P and $P^{\#}$. AN/P is transitive on $P^{\#}$ and so certainly primitive as linear group on $P^{\#}$. $Q \cong QP/P \lhd AN/P$, so P is a direct sum of some number m of isomorphic irreducible Q-modules. Since A is transitive on $N - P$, it follows that $N_A(Q)$ is transitive on $Q^{\#}$. It now follows from Lemma II.3.11 of [3] that the irreducible Q-submodules of P must have order p^{q-1}; this means that $|P| = p^{m(q-1)}$, $|N| = qp^{m(q-1)}$, and the polynomial $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$.

Conversely, let p and q be primes such that $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$, m a positive integer. In the field $GF(p^{m(q-1)})$, let μ be a multiplicative generator ($|\langle\mu\rangle| = p^{m(q-1)} - 1$), and set $\lambda \in \langle\mu\rangle$, $|\lambda| = q$. $GF(p^{m(q-1)})$ may be considered an $m(q - 1)$-dimensional vector space over $GF(p)$, and the automorphism $a : x \rightarrow \mu x$ is transitive on $GF(p^{m(q-1)})^{\#}$. If $b : x \rightarrow x^p$, then $|\langle b\rangle| = m(q - 1)$; also, $\langle b, a\rangle = N_{GL(m(q-1), p)}(\langle a\rangle)$ by Lemma II.3.11 of [3], with $\langle b\rangle \cap \langle a\rangle = 1$. Let c be the power of a given by $c : x \rightarrow \lambda x$; $|\langle c\rangle| = q$ and $\langle b\rangle \subseteq N(\langle c\rangle)$. If $b^i c = cb^i$, then we see $xb^i c = \lambda x^{p^i}$ must equal $xcb^i = \lambda^{p^i} x^{p^i}$, so $\lambda = \lambda^{p^i}$. By hypothesis $GF(p)[\lambda] = GF(p^{q-1})$, so $\lambda = \lambda^{p^i}$ only if $(q - 1) \,|\, i$. We conclude that $|\langle b\rangle : C_{\langle b\rangle}(c)| = q - 1$. If we denote $P = GF(p^{m(q-1)})$, then $\langle b, a\rangle$ has the normal subgroup $\langle c\rangle = Q$; $\langle b, a\rangle$ is transitive on $P^{\#}$ and on $(QP/P)^{\#}$. The group I of inner automorphisms of $N = QP$ is transitive on xP, any $x \in N - P$, so we conclude that $\langle b, a\rangle I$ is transitive on $N - P$ and $P^{\#}$. Therefore the group N satisfies the hypotheses of our theorem.

There remains the case when $N = P$ is a nonabelian p-group. Of course, since P has a solvable automorphism group A with only two orbits on $P^{\#}$, we must have $Z(P) = \Phi(P) = P'$, and P is special. P is nonabelian. so if $p = 2$ then all elements of $P - P'$ must have order 4. If p is odd, on the other hand, then the main result of [5] implies that P has exponent p. Denote $|P/P'| = p^m$, $|P'| = p^n$. By Theorem VI.2.3 of [3], we can find a Hall p'-subgroup H of A and a Sylow p-subgroup Q of A such that $A = HQ = QH$.

Let V be either P/P' or P'. $p \nmid |V^{\#}|$, so there is a $v \in V^{\#}$ such that $Q \subseteq A_v$. Then $A = HA_v$ must contain exactly $|H|\cdot|A_v|/|H \cap A_v| = |H : H_v|\cdot|A_v|$ elements, and we see $|A : A_v| = |H : H_v|$. Since A is transitive on $V^{\#}$, then, so is H. We have proved that H is transitive on $(P/P')^{\#}$ and $P'^{\#}$; of course, by Theorem III.3.18 of [3] we know that H is faithful on P/P'.

We first consider the case $m = 2$, so that $|P/P'| = p^2$; clearly $m = 2$ implies that $n = 1$, so P is extra special. If P is the quaternion group of order 8, of course Aut (P) is solvable and has only two orbits on $P^{\#}$; this is the case (v), $n = 1$, of our main theorem. If P is odd and

$$P = \langle x, y, z \mid x^p = y^p = z^p = 1, [x, y] = z, xz = zx, yz = zy\rangle,$$

choose a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, p)$$

of order $p^2 - 1$; such a matrix exists by Theorem II.7.3 of [3]. Then we find that $x^\alpha = x^a y^b$, $y^\alpha = x^c y^d$, $z^\alpha = z^{ad-bc}$ defines an automorphism α of P which is transitive on $(P/P')^{\#}$ and $P'^{\#}$. If I is the inner automorphism group of P, then $\langle\alpha\rangle I$ is transitive on $P - P'$ and $P'^{\#}$, so P is one of the groups of our theorem. P is the case (vi) of our main theorem, $n = 1$.

We may now assume $m > 2$. Since H is transitive on $(P/P')^{\#}$, we know by [4] that either H is a subgroup of the group of semilinear transformations of P/P', or else $|P/P'| = 3^4$ and H is one of the three specific exceptional groups described in [4]. In particular, we know $|H| \mid 2^7\cdot 5$. H is also transitive on $P'^{\#}$ and $|P'| = 3^n$, so certainly $n = 1, 2$, or 4. We shall discuss these three possibilities, and afterward study the general case when H is a subgroup of the group of semilinear transformations on P/P'.

If $|P/P'| = 3^4$, H is an exceptional group of [4], and $n = 2$ or $n = 4$, denote $N = \{h \in H \mid h \text{ is trivial on } P'^{\#}\}$. We see $N \lhd H$, and H/N is transitive on $P'^{\#}$. By [4], $|Z(H)| = 2$; let $Z(H) = \langle w\rangle$. If $x, y \in P - P'$ satisfy $[x, y] \neq 1$, then $(xP')^w = x^2P'$, $(yP')^w = y^2P'$, so $[x, y]^w = [x^w, y^w] = [x^2, y^2] = [x, y]^4 = [x, y]$; this proves that $Z(H)$ is trivial on P', $Z(H) \subseteq N$. We then see that in the case $n = 4$, H/N cannot be transitive on P' by [4], so this case does not occur. In the case $n = 2$, all 5-elements of H are in N, and we see by [4] that $|H/N| \leqq 4$. Thus H/N cannot be transitive on $P'^{\#}$, and this case $n = 2$ does not occur either.

If $|P/P'| = 3^4$, $n = 1$, H an exceptional group of [4], then P is extra special. This case does occur, and is case (vii) of the main Theorem. To see this, we can use the matrices given by Huppert on page 127 of [4]. Let P be extra special of order 3^5 and exponent 3, with generators x, y, u, v, z and relations $\langle z\rangle = Z(P)$, $xy = yx$, $xv = vx$, $yu = uy$, $uv = vu$, $[x, u] = [y, v] = z$. Then we can define automorphisms A, B, C, D, F, G of P as follows: $x^A = y$, $y^A = x^2$, $u^A = v$, $v^A = u^2$, $z^A = z$; $x^B = x$, $y^B = y^2$, $u^B = u$, $v^B = v^2$, $z^B = z$; $x^C = xu$, $y^C = yv$, $u^C = xu^2$, $v^C = yv^2$, $z^C = z$; $x^D = u^2$, $y^D = v^2$, $u^D = x$, $v^D = y$, $z^D = z$; $x^F = x^2yuv$, $y^F = x^2y^2uv^2$, $u^F = yu$, $v^F = y^2u$, $z^F = z$; $x^G = xu$, $y^G = v^2$, $u^G = x^2u$, $v^G = y^2$, $z^G = z^2$. Denote $H = \langle A, B, C, D, F, G\rangle$, I = group of inner automorphisms of P. Then we see from [4] that H is solvable, transitive on $(P/P')^{\#}$ and $P'^{\#}$. I is certainly transitive on wP' for any $w \in P - P'$, so we conclude that HI is transitive on $P - P'$ and $P'^{\#}$.

Now returning to the general case, we have $p^m = |P/P'| > p^2$, where H is a subgroup of the group of semilinear transformations on P/P'. This means that $|H|$ divides $m(p^m - 1)$, and H has a cyclic normal subgroup $\langle\xi\rangle$ such that $|H : \langle\xi\rangle| \mid m$. Since H is transitive on $(P/P')^{\#}$, we see that $|\langle\xi\rangle|$ is divisible by $(p^m - 1)/(m, p^m - 1)$. H is certainly a primitive linear group on (P/P'). Therefore, by Clifford's Theorem, P/P' is a direct sum of faithful isomorphic irreducible $\langle\xi\rangle$-modules. If P/P' is not irreducible as a $\langle\xi\rangle$-module, then we see that $|\langle\xi\rangle|$ divides $p^k - 1$, some $k < m$. Therefore $|H|$ divides $m(p^k - 1)$, and since H is transitive on $(P/P')^{\#}$ we have $(p^m - 1) \mid m(p^k - 1)$. By Lemma 1, this is a contradiction, except possibly when $p^m = 2^6$. If $p^m = 2^6$, we find that 63 divides $6(2^k - 1)$, $k < 6$; this is also impossible. We have proved that P/P' is in all cases an irreducible $\langle\xi\rangle$-module.

Let λ be an eigenvalue of ξ on P/P'. Then ξ has the m distinct eigenvalues $\lambda, \lambda^p, \cdots, \lambda^{p^{m-1}}$; and $|\langle\lambda\rangle| = |\langle\xi\rangle|$. Here we see $GF(p)[\lambda] = GF(p^m)$. Following [2], we now choose a conjugate basis $u_0, u_1, \cdots, u_{m-1}$ for P/P' adapted to ξ. This means that $u_0, u_1, \cdots, u_{m-1}$ are a basis for $P/P' \otimes GF(p^m)$ over $GF(p^m)$, satisfying $u_i\xi = \lambda^{p^i}u_i$; and that if $\langle\sigma\rangle$, $\sigma : x \to x^p$, is the Galois group of $GF(p^m)$, then $u_0^\sigma = u_1, \cdots, u_{m-2}^\sigma = u_{m-1}, u_{m-1}^\sigma = u_0$.

This implies that the elements of P/P' in $P/P' \otimes GF(p^m)$ are precisely the elements $\sum_{i=0}^{m-1} \alpha^{p^i}u_i$, $\alpha \in GF(p^m)$. Denote $\bar{\alpha} = \sum_{i=0}^{m-1} \alpha^{p^i}u_i$. We see that

$$\bar{\alpha}\xi = \left(\sum_{i=0}^{m-1} \alpha^{p^i}u_i\right)\xi = \sum_{i=0}^{m-1} \alpha^{p^i}\lambda^{p^i}u_i = \sum_{i=0}^{m-1} (\alpha\lambda)^{p^i}u_i = \overline{\lambda\alpha},$$

so ξ acts on P/P' as a multiplication by λ.

Let L be the Lie ring of P, $L \otimes GF(p^m)$ its extension to $GF(p^m)$, so that $L \otimes GF(p^m) = (P/P' \otimes GF(p^m)) \oplus (P' \otimes GF(p^m))$. The map

$$[\ ,\ ] : (P/P' \otimes GF(p^m)) \times (P/P' \otimes GF(p^m)) \to P' \otimes GF(p^m)$$

obtained by extending the commutator map is bilinear. We have

$$[u_i, u_j]\xi = [u_i\xi, u_j\xi] = [\lambda^{p^i}u_i, \lambda^{p^j}u_j] = \lambda^{p^i+p^j}[u_i, u_j],$$

so either $[u_i, u_j] = 0$ or $\lambda^{p^i+p^j}$ is an eigenvalue of ξ on P'. Of course, for any i, j we have $[u_j, u_i] = -[u_i, u_j]$ (which equals $[u_i, u_j]$ if $p = 2$).

H is transitive on $P'^{\#}$, so H is certainly a primitive (not necessarily faithful) linear group on P'. Hence P' is a direct sum of isomorphic, irreducible (not necessarily faithful) $\langle\xi\rangle$-modules.

$[u_0, u_r]\xi = \lambda^{1+p^r}[u_0, u_r]$; applying σ^i, this equation implies that $[u_i, u_{i+r}]\xi = \lambda^{p^i(1+p^r)}[u_i, u_{i+r}]$; here the subscripts are taken modulo m. P is not abelian, so some $[u_i, u_j]$ is not 0, and some $[u_0, u_r] \neq 0$; we choose $r > 0$ minimal such that $[u_0, u_r] \neq 0$. Thus λ^{1+p^r} is an eigenvalue of ξ on P', and all eigenvalues of ξ on P' have form $\lambda^{p^s(1+p^r)}$, $0 \leq s < n$. Since $[u_r, u_0] \neq 0$, we can apply σ^{m-r} and see that $[u_0, u_{m-r}] \neq 0$; this proves that $m - r \geq r$, so $0 < r \leq \frac{1}{2}m$.

In any case, $(\lambda^{1+p^r})^{(p^n-1)} = 1$, which implies that $(p^m - 1)/(m, p^m - 1)$ divides $(1 + p^r)(p^n - 1)$. If $p^m = 2^6$, then this asserts that 21 divides $(1 + 2^r)(2^n - 1)$, where $r = 1, 2$ or 3. Any of these imply $7 \mid (2^n - 1)$, so $n = 3$ or $n = 6$; for $n = 3$, we have $r = 1$ or 3. If $p^m \neq 2^6$, let q be the prime of Lemma 1; $q > m$, so $q \nmid (m, p^m - 1)$, and we see that $q \mid (p^n - 1)$ or $q \mid (1 + p^r)$. If $q \mid (p^n - 1)$, then $m \mid n$; since $|H|$ divides $m(p^m - 1)$ and H is transitive on $P'^{\#}$, we see that $n = m$.

Now suppose that $p^m \neq 2^6$ and $q \mid (1 + p^r)$. Then $q \mid (p^{2r} - 1)$, so we must have $m \mid 2r$; but $r \leq \frac{1}{2}m$, so we see $2r = m$. Corresponding to the three cases of Lemma 1, we consider the three possibilities for p^r. If $p^r = 2^6$, then $m = 12$, and we see that 1365 divides $65(2^n - 1)$. In particular, $21 \mid (2^n - 1)$, so $n = 6$ or $n = 12$. If $p^r = p^2$ for a Mersenne prime p, then we see that $(p^4 - 1)/4$ divides $(p^2 + 1)(p^n - 1)$. $|H|$ divides $4(p^4 - 1)$ and H is transitive on $P'^{\#}$, so $(p^n - 1) \mid 4(p^4 - 1)$. These two relations imply that $n = 2$ or $n = 4$, or $n = 1$ with $p = 3$. The group with $p = 3, m = 4, n = 1$ is unique and has been shown to be case (vii) of the theorem, so we can assume $n = 2 = r$ or $n = 4 = m$. Finally, suppose that a prime q_0 divides $p^r - 1$, $q_0 \nmid (p^t - 1)$ for $t < r$. In particular, $q_0 \nmid 2r$, $2r = m$, and $q_0 \nmid (p^r + 1)$, so we must have $q_0 \mid (p^n - 1)$. Therefore $r \mid n$, so $r = n$ or $n = m$.

We have shown that three cases must be studied: (1) $n = r = \frac{1}{2}m$; (2) $m = n$; (3) $p = 2, m = 6, n = 3, r = 1$.

Case 1. Here, the only $[u_i, u_j] \neq 0$ must be $[u_0, u_n]$, $[u_1, u_{n+1}]$, $\cdots$, $[u_{n-1}, u_{2n-1}]$ and their negatives $[u_n, u_0]$, $[u_{n+1}, u_1]$, $\cdots$, $[u_{2n-1}, u_{n-1}]$. If ξ were reducible on P', then for some $t < n$, $t \mid n$, we have $\lambda^{(1+p^r)(p^t-1)} = 0$. $(p^{2n} - 1)/(2n, p^{2n} - 1)$ divides $(1 + p^n)(p^t - 1)$, or in other words

$$(p^n - 1) \mid (2n, p^{2n} - 1)(p^t - 1).$$

This relation is impossible if $p^n = 2^6$, and so must contradict Lemma 1 unless $n = 2$. When $n = 2$ we have $t = 1$, and the relation implies $p = 3$. Thus, except for the possibility $p = 3, n = 2, t = 1$, we have ξ irreducible on P'.

We shall show that this possibility is not really an exception. If it occurs, then $|P/P'| = 3^4$, $|P'| = 3^2$, and ξ fixes two 1-dimensional subspaces of P'. Here, $|H : \langle\xi\rangle|$ divides 4. If λ is an eigenvalue of ξ on P/P', then $|\langle\lambda\rangle| = |\langle\xi\rangle|$; $\lambda^{1+3^2} = \lambda^{10}$ is an eigenvalue of ξ on P', so $\lambda^{10} = \pm 1$, and we see $|\langle\xi\rangle| \mid 20$.

We must therefore have $|H| = 80$, $|\langle\xi\rangle| = 20$, $|H:\langle\xi\rangle| = 4$, and ξ^2 trivial on P'. This forces $H/\langle\xi^2\rangle$ to be regular on $P'^{\#}$, so $H/\langle\xi^2\rangle$ is cyclic or quaternion. $\xi\langle\xi^2\rangle = -1 \in Z(H/\langle\xi^2\rangle)$, so $(H/\langle\xi^2\rangle)/(\langle\xi\rangle/\langle\xi^2\rangle)$ is cyclic of order 4. We conclude that $H/\langle\xi^2\rangle$ is cyclic; this forces H to be cyclic, say $H = \langle\xi_0\rangle$. Replacing ξ by ξ_0, we see that since P' is an irreducible $\langle\xi_0\rangle$-module, P satisfies Case 1 where P' is an irreducible $\langle\xi\rangle$-module.

Returning to the general Case 1, we have seen that λ^{1+p^n} is an eigenvalue of ξ on P'. Let $v_0, v_1, \cdots, v_{n-1}$ be a conjugate basis for P' adapted to ξ, so that $v_i\xi = \lambda^{(1+p^n)p^i}v_i$. $[u_0, u_n]$ and v_0 are both in the one-dimensional subspace

$$\{v \in P' \otimes GF(p^m) \mid v\xi = \lambda^{1+p^n}v\},$$

so we may choose $\varepsilon \in GF(p^{2n})$ such that $[u_0, u_n] = \varepsilon v_0$. Applying σ to this equation repeatedly, we get equations

$$[u_1, u_{n+1}] = \varepsilon^p v_1, \cdots, [u_{n-1}, u_{2n-1}] = \varepsilon^{p^{n-1}}v_{n-1},$$

$$[u_n, u_0] = \varepsilon^{p^n}v_0, \quad [u_{n+1}, u_1] = \varepsilon^{p^{n+1}}v_1, \cdots, [u_{2n-1}, u_{n-1}] = \varepsilon^{p^{2n-1}}v_{n-1}.$$

Since $[u_0, u_n] = -[u_n, u_0]$, we see that $0 = (\varepsilon^{p^n} + \varepsilon)v_0$. Therefore $\varepsilon^{p^n} + \varepsilon = 0$, and ε must be an element of $GF(p^{2n})$ with trace 0 over $GF(p^n)$. If $p = 2$, such elements are found in $GF(p^n)$; if $p \neq 2$, such elements are always available outside $GF(p^n)$.

If $\alpha \in GF(p^n)$, denote $\{\alpha\} = \sum_{i=0}^{n-1} \alpha^{p^i}v_i \in P'$. We can now compute the commutator $[\bar\alpha, \bar\beta]$ of any two elements $\bar\alpha = \sum_{i=0}^{2n-1} \alpha^{p^i}u_i$, $\bar\beta = \sum_{i=0}^{2n-1} \beta^{p^i}u_i$ of P/P'.

$$\begin{aligned}[\bar\alpha, \bar\beta] &= \sum_{i=0}^{2n-1}\sum_{j=0}^{2n-1} \alpha^{p^i}\beta^{p^j}[u_i, u_j] \\ &= \sum_{i=0}^{n-1} \alpha^{p^i}\beta^{p^{n+i}}[u_i, u_{n+i}] + \sum_{j=0}^{n-1} \alpha^{p^{j+n}}\beta^{p^j}[u_{j+n}, u_j] \\ &= \sum_{i=0}^{n-1} (\alpha^{p^i}\beta^{p^{n+i}} - \alpha^{p^{n+i}}\beta^{p^i})[u_i, u_{n+i}] \\ &= \sum_{i=0}^{n-1} (\alpha\beta^{p^n} - \alpha^{p^n}\beta)^{p^i}\varepsilon^{p^i}v_i = \{(\alpha\beta^{p^n} - \alpha^{p^n}\beta)\varepsilon\} \in P'.\end{aligned}$$

Let $\theta : x \to x^{p^n}$ be the Galois automorphism of $GF(p^{2n})$ over $GF(p^n)$. We have shown that $[\bar\alpha, \bar\beta] = \{(\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon\}$.

Assume now, here in Case 1, that p is odd, so that P has exponent p. Let $x_1, x_2, \cdots, x_{2n}$ generate P, $z_1, \cdots, z_n$ generate P'. We can then choose $\alpha_i \in GF(p^{2n})$, $\beta_i \in GF(p^n)$ such that $x_i = \sum_{j=0}^{2n-1} \alpha_i^{p^j}u_j$, $z_i = \sum_{j=0}^{n-1} \beta_i^{p^j}v_j$. We see that $\{\alpha_i\}$ is a basis of $GF(p^{2n})$, $\{\beta_i\}$ a basis of $GF(p^n)$ as additive vector spaces over $GF(p)$. Every element of P has a unique expression $x_1^{i_1}x_2^{i_2} \cdots x_{2n}^{i_{2n}}z_1^{j_1} \cdots z_n^{j_n}$, where all $0 \leq i_k, j_l \leq p - 1$. We can multiply two such expressions if we can identify $x_k x_l$, $l < k$. But $x_k x_l = x_l x_k[x_k, x_l]$, and $[x_k, x_l] = [\bar\alpha_k, \bar\alpha_l] = \{(\alpha_k\alpha_l^\theta - \alpha_l\alpha_k^\theta)\}$ is well defined in P', using the basis $\{\beta_i\}$. This shows that the isomorphism class of P is given by our knowledge of commutators, and for given ε, p, n there is at most one P.

For any odd p, ε, and $n \geq 1$, we now claim that P does exist and have such an automorphism group. Choose $\varepsilon \in GF(p^{2n})$ with $\varepsilon + \varepsilon^{p^n} = 0$, let $\theta : x \to x^{p^n}$, and define P by

$$P = \{(\alpha, \zeta) \in GF(p^{2n}) \times GF(p^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \tfrac{1}{2}(\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon)\}.$$

One easily verifies that P is a group of exponent p, and satisfies

$$[(\alpha, \zeta), (\beta, \eta)] = (0, (\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon).$$

Choose $\lambda \in GF(p^{2n})$ such that $|\langle\lambda\rangle| = p^{2n} - 1$. Then $\lambda^{1+\theta} = \lambda^{1+p^n} \in GF(p^n)$ has order $p^n - 1$. We define $\psi : P \to P$ by $(\alpha, \zeta)\psi = (\lambda\alpha, \lambda^{1+\theta}\zeta)$. ψ is an automorphism of P, because

$$\begin{aligned}\{(\alpha, \zeta)(\beta, \eta)\}\psi &= (\alpha + \beta, \zeta + \eta + \tfrac{1}{2}(\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon)\psi \\ &= (\lambda\alpha + \lambda\beta, \lambda^{1+\theta}\zeta + \lambda^{1+\theta}\eta + \tfrac{1}{2}\lambda^{1+\theta}(\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon) \\ &= (\lambda\alpha, \lambda^{1+\theta}\zeta)(\lambda\beta, \lambda^{1+\theta}\eta) = \{(\alpha, \zeta)\psi\}\{(\beta, \eta)\psi\}.\end{aligned}$$

It is clear that ψ is transitive on $(P/P')^{\#}$ and $P'^{\#}$.

We see that

$$C_P((\alpha, \zeta)) = \{(\beta, \eta) \mid \alpha\beta^\theta - \alpha^\theta\beta = 0\} = \{(\beta, \eta) \mid \alpha\beta^\theta \in GF(p^n)\},$$

which implies that $|C_P((\alpha, \zeta))| = p^{2n}$ for any $(\alpha, \zeta) \in P - P'$. Therefore the group I of inner automorphisms of P is transitive on each coset $(\alpha, \zeta)P' \neq P'$. We conclude that $I\langle\psi\rangle$ is a solvable group of automorphisms of P, transitive on $P - P'$ and $P'^{\#}$.

We finally remark that P does not depend on the choice of ε. For if $\varepsilon_1, \varepsilon_2$ are two nonzero solutions of the equation $X^{p^n} + X = 0$ in $GF(p^{2n})$, then we must have $\varepsilon_2 = \gamma\varepsilon_1$, where $\gamma \in GF(p^n)$ and $\gamma^\theta = \gamma$. Let

$$P_1 = \{(\alpha, \zeta) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \tfrac{1}{2}(\alpha\beta^\theta - \alpha^\theta\beta)\varepsilon_1)\},$$

$$P_2 = \{(\alpha, \zeta) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \tfrac{1}{2}(\alpha\beta^\theta - \alpha^\theta\beta)\gamma\varepsilon_1)\}.$$

We may choose $\tau \in GF(p^{2n})$ such that $\tau^{1+\theta} = \gamma$. If we define $\psi : P_2 \to P_1$ by $(\alpha, \zeta)\psi = (\tau\alpha, \zeta)$, it is easy to verify that ψ is an isomorphism. The group P is the group $C(p, n)$, case (vi) of our theorem.

We still must study $p = 2$ in Case 1. Here we know that ξ is irreducible on P', and all elements of $P - P'$ have order 4. If $u_0, u_1, \cdots, u_{2n-1}$ is our conjugate basis for P/P' adapted to ξ, we see that $[u_0, u_n]^{\sigma^n} = [u_n, u_0] = [u_0, u_n]$. Therefore $v_0 = [u_0, u_n], v_1 = [u_1, u_{n+1}], \cdots, v_{n-1} = [u_{n-1}, u_{2n-1}]$ is a conjugate basis for P' adapted to ξ. These bases satisfy $u_i\xi = \lambda^{2^i}u_i$, $v_i\xi = \lambda^{(1+2^n)2^i}v_i$.

We again denote $\bar{\alpha} = \sum_{i=0}^{2n-1} \alpha^{2^i} u_i \in P/P'$, $\{\gamma\} = \sum_{i=0}^{n-1} \gamma^{2^i} v_i \in P'$. Our calculation of $[\bar{\alpha}, \bar{\beta}]$ shows that $[\bar{\alpha}, \bar{\beta}] = \{\alpha\beta^\theta + \alpha^\theta\beta\}$. This relation is not sufficient to provide defining relations for P, since we need to know x^2 for any

$x \in P - P'$. In P, we have the relations $(x\xi)^2 = (x^2)\xi$ and $(xy)^2 = x^2y^2[x, y]$. Let $\varphi : P/P' \to P'$ be the map $\varphi : xP' \to x^2$. φ satisfies the relations $(\bar{\alpha}\varphi)\xi = (\bar{\alpha}\xi)\varphi$ and $(\bar{\alpha} + \bar{\beta})\varphi = \bar{\alpha}\varphi + \bar{\beta}\varphi + [\bar{\alpha}, \bar{\beta}]$. Following [2], we shall show these relations completely determine φ. For if $\psi : P/P' \to P' \otimes GF(2^{2n})$ also satisfies these relations, we see by subtraction that $\varphi - \psi$ is a ξ-homomorphism. By irreducibility of P/P', this implies that either $(\varphi - \psi)(P/P')$ is ξ-isomorphic to P/P', or else $\varphi = \psi$. ξ-isomorphism is impossible since the eigenvalues $\lambda^{2^i(1+2n)}$ of ξ on $P' \otimes GF(2^{2n})$ are different from the eigenvalues λ^{2^i} of ξ on P/P'. Therefore φ is unique.

We now claim that φ is the map $\bar{\alpha}\varphi = \{\alpha^{1+\theta}\}$. Consider any $\gamma \in GF(2^n)$, and choose $\alpha, \beta \in GF(2^{2n})$ with $\alpha\beta^\theta + \alpha^\theta\beta = \gamma$ (this must be possible, since every element in P' is a commutator). Then

$$\begin{aligned}\{\gamma\}\xi &= [\bar{\alpha}, \bar{\beta}]\xi = [\bar{\alpha}\xi, \bar{\beta}\xi] = [\overline{\lambda\alpha}, \overline{\lambda\beta}] \\ &= \{(\lambda\alpha)(\lambda\beta)^\theta + (\lambda\alpha)^\theta(\lambda\beta)\} = \{\lambda^{1+\theta}\gamma\}.\end{aligned}$$

For any $\alpha, \beta \in GF(2^{2n})$, we now see

$$(\bar{\alpha}\varphi)\xi = \{\alpha^{1+\theta}\}\xi = \{\lambda^{1+\theta}\alpha^{1+\theta}\} = \{(\lambda\alpha)^{1+\theta}\} = (\overline{\lambda\alpha})\varphi = (\bar{\alpha}\xi)\varphi.$$

Also

$$\begin{aligned}(\bar{\alpha} + \bar{\beta})\varphi &= (\alpha + \beta)^-\varphi = \{(\alpha + \beta)^{1+\theta}\} = \{\alpha\alpha^\theta + \alpha\beta^\theta + \alpha^\theta\beta + \beta\beta^\theta\} \\ &= \{\alpha^{1+\theta}\} + \{\beta^{1+\theta}\} + \{\alpha\beta^\theta + \alpha^\theta\beta\} = \bar{\alpha}\varphi + \bar{\beta}\varphi + [\bar{\alpha}, \bar{\beta}].\end{aligned}$$

We have shown that for any $xP' = \bar{\alpha} \in P/P'$, we have $x^2 = \{\alpha^{1+\theta}\} \in P'$. Therefore P is completely determined, and for any n, $p = 2$, Case 1 provides at most one group P.

We do obtain such a group P. For any $n \geq 1$, choose $\mu \in GF(2^{2n})$ of order $2^n + 1$, and define

$$P = \{(\alpha, \zeta) \in GF(2^{2n}) \times GF(2^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^{2^n}\mu + \alpha^{2^n}\beta\mu^{-1})\}.$$

Let $\theta : x \to x^{2^n}$, so $\mu + \mu^{-1} = \mu + \mu^\theta = \varepsilon \in GF(2^n)$. It is easy to verify that P is a group and satisfies the relations

$$(\alpha, \zeta)^2 = (0, \alpha\alpha^\theta\varepsilon), \qquad [(\alpha, \zeta), (\beta, \eta)] = (0, (\alpha\beta^\theta + \alpha^\theta\beta)\varepsilon).$$

Choose $\lambda \in GF(2^{2n})$ such that $|\langle\lambda\rangle| = 2^{2n} - 1$; then $\lambda^{1+\theta}$ satisfies $|\langle\lambda^{1+\theta}\rangle| = 2^n - 1$. If we define $\psi : P \to P$ by $(\alpha, \zeta)\psi = (\lambda\alpha, \lambda^{1+\theta}\zeta)$, it is easy to verify that ψ is an automorphism of P, transitive on $(P/P')^\#$ and $P'^\#$. Just as in the case p odd, the group I of inner automorphisms of P is transitive on each coset $(\alpha, \zeta)P' \neq P'$. Therefore $\langle\psi\rangle I$ is a solvable group of automorphisms of P, transitive on $P - P'$ and $P'^\#$; P is the group of case (v) in the main theorem.

Case 2. In this case, $m = n > 2$, and the integer r is unknown except for the relation $0 < r \leq \frac{1}{2}n$. Again we know that $|H|$ divides $n(p^n - 1)$,

$|H:\langle\xi\rangle|$ divides n, and $\langle\xi\rangle \lhd H$, where $(p^n - 1)/(n, p^n - 1)$ divides $|\langle\xi\rangle|$. H is transitive on $P'^{\#}$, so is certainly a primitive linear group, and P' is a direct sum of isomorphic irreducible $\langle\xi\rangle$-modules. Let

$$K = \{h \in H \mid h \text{ is trivial on } P'\}.$$

$|P'^{\#}| = p^n - 1$, so $(p^n - 1) \mid |H/K|$; if P' were not $\langle\xi\rangle$-irreducible, we would obtain a relation $|H/K| \mid n(p^t - 1)$, $t < n$. This contradicts Lemma 1 if $p^n \neq 2^6$ and is also impossible when $p^n = 2^6$. We conclude that throughout Case 2, P' is an irreducible $\langle\xi\rangle$-module.

r is the smallest positive integer such that $[u_0, u_r] \neq 0$. We have relations

$$|\langle\lambda\rangle| = |\langle\xi\rangle|, \quad u_i\,\xi = \lambda^{p^i}u_i, \quad [u_0, u_r]\xi = \lambda^{1+p^r}[u_0, u_r].$$

If we have $2r = n$, then $\lambda^{1+p^r} \in GF(2^r)$ has only r distinct algebraic conjugates. But P' is an irreducible $\langle\xi\rangle$-module and ξ must have $2r = n$ distinct conjugate eigenvalues on P', so the case $2r = n$ cannot occur, and $0 < r < \frac{1}{2}n$.

For any i, j, suppose that $[u_i, u_j] \neq 0$. Then

$$[u_i, u_j] = \lambda^{p^i+p^j}[u_i, u_j],$$

so $\lambda^{p^i+p^j}$ must be one of the eigenvalues $\lambda^{p^s(1+p^r)}$ of ξ on P'. We therefore have a congruence

$$p^i + p^j \equiv p^s(1 + p^r) \pmod{(p^n - 1)/(n, p^n - 1)}.$$

Lemma 3 now implies that without exception, $i - j \equiv \pm r \pmod{n}$. The only $[u_i, u_j]$ which are not 0 are $[u_0, u_r], [u_1, u_{r+1}], \cdots, [u_{n-r-1}, u_{n-1}], [u_{n-r}, u_0], [u_{n-r+1}, u_1], \cdots, [u_{n-1}, u_{r-1}]$ and their negatives. We denote $[u_0, u_r] = v_0$, $[u_1, u_{r+1}] = v_1, \cdots, [u_{n-1}, u_{r-1}] = v_{n-1}$. $\{v_0, v_1, \cdots, v_{n-1}\}$ must be a conjugate basis for P' adapted to ξ, satisfying $v_i\,\xi = \lambda^{p^i(1+p^r)}v_i$. The elements of P' are denoted, as before, by $\{\gamma\} = \sum_{i=0}^{n-1} \gamma^{p^i} v_i$; let θ denote the automorphism $\theta : x \to x^{p^r}$ of $GF(p^n)$.

We can now compute $[\bar\alpha, \bar\beta]$, for any pair of elements

$$\bar\alpha = \sum_{i=0}^{n-1} \alpha^{p^i} u_i, \qquad \bar\beta = \sum_{i=0}^{n-1} \beta^{p^i} u_i$$

of P/P'.

$$\begin{aligned}[\bar\alpha, \bar\beta] &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \alpha^{p^i}\beta^{p^j}[u_i, u_j] \\ &= \sum_{i=0}^{n-1} \alpha^{p^i}\beta^{p^{i+r}} v_i - \sum_{j=0}^{n-1} \alpha^{p^{j+r}}\beta^{p^j} v_j \\ &= \sum_{i=0}^{n-1} (\alpha\beta^\theta - \alpha^\theta\beta)^{p^i} v_i = \{\alpha\beta^\theta - \alpha^\theta\beta\}.\end{aligned}$$

Assume first that p is odd. Then P is completely determined by the given commutator relation. We know that H is acting on P/P' as a subgroup of the group of semilinear transformations on P/P'. For any $\bar\alpha \in P/P'$, we know that $\bar\alpha\xi = (\lambda\alpha)^-$, so ξ acts on P/P' as a multiplication by λ. P/P' is an irreducible $\langle\xi\rangle$-module. We see, as in the proof of Theorem II.3.11 of [3], that if $h \in H$, then there exist $\tau \in GF(p^n)$ and $\sigma \in \mathrm{Aut}\ (GF(p^n))$ satisfying $\bar\alpha h =$

$(\tau\alpha^\sigma)^-$, all $\bar{\alpha} \in P/P'$. We can now compute the action of H on P'. For any element $\{\alpha\beta^\theta - \alpha^\theta\beta\} \in P'$ and such $h \in H$, we have

$$\begin{aligned}\{\alpha\beta^\theta - \alpha^\theta\beta\}h &= [\bar{\alpha}, \bar{\beta}]h = [\bar{\alpha}h, \bar{\beta}h] = [(\tau\alpha^\sigma)^-, (\tau\beta^\sigma)^-] \\ &= \{(\tau\alpha^\sigma)(\tau\beta^\sigma)^\theta - (\tau\beta^\sigma)(\tau\alpha^\sigma)^\theta\} = \{\tau^{1+\theta}(\alpha\beta^\theta - \alpha^\theta\beta)^\sigma\}.\end{aligned}$$

This shows that for any $\{\gamma\} \in P'$ and any $h \in H$, $\{\gamma\}h$ has form $\{\tau^{1+p^r}\gamma^\sigma\}$, some $\tau \in GF(p^n)$, some $\sigma \in \mathrm{Aut}\ (GF(p^n))$. Define

$$K = \{\gamma \in GF(p^n) \mid \gamma^{(p^n-1)/2} = 1\}.$$

Then $\tau \in GF(p^n)$ implies $\tau^{1+p^r} \in K$; therefore, $\gamma \in K$ implies $\tau^{1+p^r}\gamma^\sigma \in K$. This means H cannot be transitive on $P'^{\#}$; we get no group satisfying our main theorem in Case 2 when p is odd.

Finally, assume $p = 2$. The above methods again show that we get no group unless λ^{1+p^r} is a primitive $(2^n - 1)$-st root of unity. This occurs if and only if λ is a primitive $(2^n - 1)$-st root of unity, and the automorphism $\theta : x \to x^{2^r}$ has odd order (see [2, p. 82]). We know $[\bar{\alpha}, \bar{\beta}] = \{\alpha\beta^\theta + \alpha^\theta\beta\}$, and just as in Case 1 we obtain the square mapping. We find that if $xP' = \bar{\alpha} \in P/P'$, then $x^2 = \{\alpha^{1+\theta}\} \in P'$.

We have obtained the Suzuki 2-groups $P = A(n, \theta)$ of [2]. If $|\langle\lambda\rangle| = 2^n - 1$ and ψ is the automorphism $\psi : (\alpha, \zeta) \to (\lambda\alpha, \lambda^{1+\theta}\zeta)$ of [2], then ψ is clearly transitive on $(P/P')^{\#}$ and $P'^{\#}$. Let

$$T = \{a \in \mathrm{Aut}\ (P) \mid a \text{ is trivial on } P' \text{ and } P/P'\}.$$

Then the p-group T is transitive on every coset $xP' \neq P'$. To see this, choose any $x \in P - P'$, $z \in P'$, and let

$$P = \langle x = x_1, x_2, \cdots, x_n\rangle.$$

Then also $P = \langle \bar{x}_1 = xz, \bar{x}_2 = x_2, \cdots, \bar{x}_n = x_n\rangle$. The sets $\{x_i\}$ and $\{\bar{x}_i\}$ satisfy the same defining relations, so there exists $a \in T$ defined by $x_i^a = \bar{x}_i$, all i. We conclude that the solvable automorphism group $T\langle\psi\rangle$ is transitive on $P - P'$ and $P'^{\#}$, so $P = A(n, \theta)$ is case (iv) of our theorem.

Case 3. We still have this possibility $|P/P'| = 2^6$, $|P'| = 2^3$, $[u_0, u_1] \neq 0$. $|H:\langle\xi\rangle|$ divides 6, and P' is a sum of isomorphic faithful irreducible $\langle\xi\rangle$-modules. If they were one-dimensional, ξ would be trivial on P', an impossibility; therefore ξ is irreducible on P'. Let λ be an eigenvalue of ξ on P/P'. Then λ^3 is an eigenvalue of ξ on P', so $(\lambda^3)^7 = \lambda^{21} = 1$, and irreducibility of ξ on P' shows that indeed $|\langle\xi\rangle| = |\langle\lambda\rangle| = 21$. The eigenvalues of ξ on P' must be λ^3, $(\lambda^3)^2 = \lambda^6$, and $(\lambda^3)^4 = \lambda^{12}$. Using the fact $u_i\,\xi = \lambda^{2^i}u_i$, we see that the only $[u_i, u_j] \neq 0$ are $[u_0, u_1]$, $[u_1, u_2]$, $[u_2, u_3]$, $[u_3, u_4]$, $[u_4, u_5]$ and $[u_0, u_5]$ (here $[u_i, u_j] = [u_j, u_i]$).

Let $\{v_0, v_1, v_2\}$ be a conjugate basis for P' adapted to ξ, so that $v_i\,\xi = (\lambda^3)^{2^i}v_i$, and choose $\varepsilon \in GF(2^6)$ such that $[u_0, u_1] = \varepsilon v_0$. Applying the automorphism $\sigma : x \to x^2$ of $GF(2^6)$ repeatedly, we find that $[u_1, u_2] = \varepsilon^2 v_1$, $[u_2, u_3] = \varepsilon^4 v_2$,

$[u_3, u_4] = \varepsilon^8 v_0$, $[u_4, u_5] = \varepsilon^{16} v_1$, $[u_5, u_0] = \varepsilon^{32} v_2$. We can now compute $[\bar{\alpha}, \bar{\beta}]$, for any $\bar{\alpha}, \bar{\beta} \in P/P'$.

$$\begin{aligned}[\bar{\alpha}, \bar{\beta}] &= [\textstyle\sum_{i=0}^{5} \alpha^{2^i} u_i, \sum_{j=0}^{5} \beta^{2^j} u_j] \\ &= (\alpha\beta^2\varepsilon + \alpha^2\beta\varepsilon + \alpha^8\beta^{16}\varepsilon^8 + \alpha^{16}\beta^8\varepsilon^8)v_0 \\ &\quad + (\alpha^2\beta^4\varepsilon^2 + \alpha^4\beta^2\varepsilon^2 + \alpha^{16}\beta^{32}\varepsilon^{16} + \alpha^{32}\beta^{16}\varepsilon^{16})v_1 \\ &\quad + (\alpha\beta^{32}\varepsilon^{32} + \alpha^4\beta^8\varepsilon^4 + \alpha^8\beta^4\varepsilon^4 + \alpha^{32}\beta\varepsilon^{32})v_2 .\end{aligned}$$

If we let θ denote the automorphism $\theta : x \to x^8$ of $GF(2^6)$, and $\{\gamma\}$ the element $\sum_{i=0}^{2} \gamma^{2^i} v_i$ of P', then this means

$$[\bar{\alpha}, \bar{\beta}] = \{(\alpha\beta^2 + \alpha^2\beta)\varepsilon + (\alpha\beta^2 + \alpha^2\beta)^\theta\varepsilon^\theta\}.$$

Just as in Case 1, we can show that the square mapping $\varphi : P/P' \to P'$ is the unique mapping satisfying $(\bar{\alpha}\varphi)\xi = (\bar{\alpha}\xi)\varphi$ and $(\bar{\alpha} + \bar{\beta})\varphi = \bar{\alpha}\varphi + \bar{\beta}\varphi + [\bar{\alpha}, \bar{\beta}]$, all $\bar{\alpha}, \bar{\beta} \in P/P'$. If we define $\bar{\alpha}\varphi = \alpha^3\varepsilon + \alpha^{3\theta}\varepsilon^\theta$, and use the facts $\bar{\alpha}\xi = (\lambda\alpha)^-$, $\{\gamma\}\xi = \{\lambda^3\gamma\}$, and $(\lambda^3)^\theta = \lambda^3$, we find that $xP' = \bar{\alpha}$ implies $x^2 = \{\alpha^3\varepsilon + \alpha^{3\theta}\varepsilon^\theta\}$.

The group P is now completely determined by knowledge of the square map; for each ε there is at most one group P. P does exist; if we define

$$P(\varepsilon) = \{(\alpha, \zeta) \in GF(2^6) \times GF(2^3) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^2\varepsilon + \alpha^\theta\beta^{2\theta}\varepsilon^\theta)\},$$

we see that $P(\varepsilon)$ is a group and satisfies the relations

$$\begin{aligned}(\alpha, \zeta)^2 &= (0, \alpha^3\varepsilon + \alpha^{3\theta}\varepsilon^\theta), [(\alpha, \zeta), (\beta, \eta)] \\ &= (0, (\alpha\beta^2 + \alpha^2\beta)\varepsilon + (\alpha\beta^2 + \alpha^2\beta)^\theta\varepsilon^\theta).\end{aligned}$$

If $\varepsilon^{21} = 1$, then we can choose $\alpha \in GF(2^6)$ with $\alpha^3 = \varepsilon^2$. We then have $\alpha^3\varepsilon + \alpha^{3\theta}\varepsilon^\theta = \varepsilon^3 + \varepsilon^{3\theta} = 0$ (since $\varepsilon^3 \in GF(2^3)$). Thus some elements of $P(\varepsilon) - P(\varepsilon)'$ have order 2, eliminating this case $\varepsilon^{21} = 1$. Also, suppose $0 \neq \gamma \in GF(2^3)$. We can then choose $\tau \in GF(2^6)$ such that $\tau^3 = \gamma$, and see that the map $\psi : P(\varepsilon\gamma) \to P(\varepsilon)$ given by $(\alpha, \zeta)\psi = (\tau\alpha, \zeta)$ is an isomorphism. Therefore the remaining $\varepsilon \in GF(2^6)$ such that $\varepsilon^9 = 1$ can be replaced by some $\varepsilon\gamma$, $|\langle\varepsilon\gamma\rangle| = 63$. We may assume henceforth that $|\langle\varepsilon\rangle| = 63$.

When $|\langle\varepsilon\rangle| = 63$, define the mappings

$$\psi : P(\varepsilon) \to P(\varepsilon) \quad \text{and} \quad \Phi : P(\varepsilon) \to P(\varepsilon)$$

by $(\alpha, \zeta)\psi = (\lambda\alpha, \lambda^3\zeta)$, $(\alpha, \zeta)\Phi = (\varepsilon\alpha^4, \zeta^4)$, where λ is any element of $GF(2^6)$ with $|\langle\lambda\rangle| = 21$. We find that

$$\{(\alpha, \zeta)(\beta, \eta)\}\psi = \{(\alpha, \zeta)\psi\}\{(\beta, \eta)\psi\}$$

and

$$\{(\alpha, \zeta)(\beta, \eta)\}\Phi = \{(\alpha, \zeta)\Phi\}\{(\beta, \eta)\Phi\},$$

so ψ and Φ are automorphisms, obviously inducing a subgroup of the group of semilinear transformations on P/P'. (Abbreviate $P = P(\varepsilon)$.) On P/P', the orbits of the map $\alpha \to \lambda\alpha$ induced by ψ are

$$\{1, \varepsilon^3, \varepsilon^6, \cdots\}, \quad \{\varepsilon, \varepsilon^4, \varepsilon^7, \cdots\} \quad \text{and} \quad \{\varepsilon^2, \varepsilon^5, \varepsilon^8, \cdots\}.$$

Since the map $\alpha \to \varepsilon\alpha^4$ induced by Φ sends $1 \to \varepsilon$, $\varepsilon \to \varepsilon^5$, we see that $\langle\Phi, \psi\rangle$ is transitive on $(P/P')^{\#}$. $\langle\psi\rangle$ is in fact transitive on $P'^{\#}$.

$(1, 0) \in P - P'$, and

$$\begin{aligned} C_P((1, 0)) &= \{(\beta, \eta) \in P \mid (\beta + \beta^2)\varepsilon + (\beta + \beta^2)^\theta\varepsilon^\theta = 0\} \\ &= \{(\beta, \eta) \in P \mid (\beta + \beta^2)\varepsilon \in GF(2^3)\}. \end{aligned}$$

By looking at $GF(2^6)$, there are 2^3 possibilities for β. Therefore $|C_P((1, 0))| = 2^6$. $\langle\Phi, \psi\rangle$ is transitive on $(P/P')^{\#}$, so for any $\alpha \neq 0$, $|C_P((\alpha, \zeta))| = 2^6$. This means that the inner automorphism group I of P is indeed transitive on any $(\alpha, \zeta)P' \neq P'$. We conclude that $\langle\Phi, \psi\rangle I$ is transitive on $P - P'$ and $P'^{\#}$; $P = P(\varepsilon)$ is the group of case (viii) in our theorem.

This completes the proof of our main Theorem.

Remark. We shall finally show that the group $B(n)$ in case (v) of our main theorem is isomorphic to certain of the Suzuki 2-groups in [2]. We refer to the groups $B(n, 1, \varepsilon)$, for certain ε, in [2]. Choose an element $\chi \in GF(2^{2n})$ such that $|\langle\chi\rangle| = 2^{2n} - 1$, and set $\lambda = \chi^{2^n+1}$, $\mu = \chi^{2^n-1}$. Then $\lambda \in GF(2^n)$. The automorphism $\theta : x \to x^{2^n}$ of $GF(2^{2n})$ satisfies $\mu^\theta = \mu^{-1}$, so $\mu + \mu^{-1} \in GF(2^n)$; let $\varepsilon = \mu + \mu^{-1}$. Then $\varepsilon\mu = \mu^2 + 1$, so $X^2 + \varepsilon X + 1 = 0$ is the irreducible polynomial for μ over $GF(2^n)$. If ε were equal to $\tau + \tau^{-1}$ for some $\tau \in GF(2^n)$, we would have $\tau\varepsilon = \tau^2 + 1$, contradicting the irreducibility of the polynomial. Therefore $\varepsilon \neq \tau + \tau^{-1}$, any τ, and $B(n, 1, \varepsilon)$ exists.

It is shown in [2] that if we find linear transformations $\sigma : GF(2^n) \to GF(2^n)$ and $\rho : GF(2^n) \times GF(2^n) \to GF(2^n) \times GF(2^n)$ satisfying the condition $(u\rho)^{(2)} = u^{(2)}\sigma$, then $P = B(n, 1, \varepsilon)$ will have an automorphism ξ inducing ρ on P/P' and σ on P'. Here ${}^{(2)}$ is the square mapping and satisfies $(\alpha, \beta)^{(2)} = \alpha^2 + \varepsilon\alpha\beta + \beta^2$. We define σ by $\sigma : \zeta \to \lambda^2\zeta$.

To define ρ, we identify $(\alpha, \beta) \in GF(2^n) \times GF(2^n)$ with $\alpha + \beta\mu \in GF(2^{2n})$ and define $\rho : (\alpha, \beta) \to \lambda\mu(\alpha, \beta)$. We see that

$$\begin{aligned} (\alpha, \beta)\rho &= \lambda\mu(\alpha + \beta\mu) = \lambda\alpha\mu + \lambda\beta\mu^2 \\ &= \lambda\alpha\mu + \lambda\beta(1 + \varepsilon\mu) = \lambda\beta + (\lambda\alpha + \varepsilon\lambda\beta)\mu. \end{aligned}$$

Therefore $(\alpha, \beta)\rho = (\lambda\beta, \lambda\alpha + \varepsilon\lambda\beta)$. We find that

$$\begin{aligned} ((\alpha, \beta)\rho)^{(2)} &= \lambda^2\beta^2 + \varepsilon\lambda\beta(\lambda\alpha + \varepsilon\lambda\beta) + \lambda^2\alpha^2 + \varepsilon^2\lambda^2\beta^2 \\ &= \lambda^2(\alpha^2 + \varepsilon\alpha\beta + \beta^2) = ((\alpha, \beta)^{(2)})\sigma. \end{aligned}$$

Therefore the automorphism ξ inducing ρ on P/P' and σ on P' exists. Since

$|\langle\lambda\mu\rangle| = 2^{2n} - 1$ and $|\langle\lambda^2\rangle| = 2^n - 1$, ξ is transitive on $(P/P')^{\#}$ and $P'^{\#}$. Suppose now that $(\alpha, \beta, \zeta) \in P - P'$. Then $(\gamma, \delta, \eta) \in C_P((\alpha, \beta, \zeta))$ if and only if $\alpha\gamma + \varepsilon\alpha\delta + \beta\delta = \gamma\alpha + \varepsilon\gamma\beta + \delta\beta$, which holds if and only if $\alpha\delta = \beta\gamma$. Since $\alpha \neq 0$ or $\beta \neq 0$, this holds if and only if for some $\tau \in GF(2^n)$, $\gamma = \tau\alpha$, $\delta = \tau\beta$. Therefore $|C_P((\alpha, \beta, \zeta))| = 2^{2n}$, which forces the inner automorphism group I of P to be transitive on $(\alpha, \beta, \zeta)P'$.

We conclude that the solvable group $\langle\psi\rangle I$ is transitive on $P - P'$ and $P'^{\#}$. This forces $B(n, 1, \varepsilon)$ to be one of the groups of our main Theorem; at least for $n \neq 3$ the only possibility is the group $B(n)$ in case (v), so $B(n, 1, \varepsilon) \cong B(n)$.

References

1. L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly, vol. 12 (1905), pp. 86–89.
2. Graham Higman, *Suzuki 2-groups*. Illinois J. Math., vol. 7 (1963), pp. 79–96.
3. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
4. ———, *Zweifach transitive, auflösbare Permutations-gruppen*, Math. Zeitschr., vol. 68 (1957), pp. 126–150.
5. Ernest Shult, *The solution of Boen's problem*, Bull. Amer. Math. Soc., vol. 74 (1968), pp. 268–270.
6. Helmut Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

University of Illinois
Urbana, Illinois