A CHARACTERISATION OF $PSL_2(\boldsymbol{Z}_{p^\lambda})$ AND $PGL_2(\boldsymbol{Z}_{p^\lambda})$

G. E. WALL

(Received 23 June 1967)

1. Introduction

Let $\boldsymbol{F}_q$ denote the finite field with q elements, $\boldsymbol{Z}_m$ the residue class ring $\boldsymbol{Z}/m\boldsymbol{Z}$. It is known that the projective linear groups $G = PSL_2(\boldsymbol{F}_q)$ and $PGL_2(\boldsymbol{F}_q)$ (q a prime-power $\geqq 4$) are characterised among finite insoluble groups by the property that, if two cyclic subgroups of G of even order intersect non-trivially, they generate a cyclic subgroup (cf. Brauer, Suzuki, Wall [2], Gorenstein, Walter [3]). In this paper, we give a similar characterisation of the groups $G = PSL_2(\boldsymbol{Z}_{p^{t+1}})$ and $PGL_2(\boldsymbol{Z}_{p^{t+1}})$ (p a prime $\geqq 5$, $t \geqq 1$).

These satisfy the weaker condition [1] that, if two cyclic subgroups of G intersect in a group of even order, they generate a cyclic subgroup. If $x \in G$, let $\mathscr{R}_G(x)$ denote the subgroup generated by the roots of x, i.e. by the elements of G of which x is a power. Then this condition may also be expressed as follows:

(1.0) $\qquad$ *$\mathscr{R}_G(u)$ is cyclic for every involution $u \in G$.*

A finite group G of even order which satisfies (1.0) will be called an *$\mathscr{R}$-group*.

$PGL_2(\boldsymbol{Z}_{p^{t+1}})$ is an extension of a group, $P_{0,t}(p)$, of order p^{3t} by $PGL_2(\boldsymbol{F}_p)$. If $p \geqq 5$ and $t \geqq 1$, $PGL_2(\boldsymbol{Z}_{p^{t+1}})$ and $PSL_2(\boldsymbol{Z}_{p^{t+1}})$ are insoluble and neither splits over $P_{0,t}(p)$. If $p = 3$, however, both groups are soluble and both split over $P_{0,t}(3)$.

THEOREM 1. *Let G be an insoluble $\mathscr{R}$-group with trivial centre. Suppose that G does not split over its largest normal subgroup of odd order, $O(G)$, and further that, when $G/O(G) \cong PSL_2(\boldsymbol{F}_5)$ or $PSL_2(\boldsymbol{F}_7)$, $O(G)$ is a prime-power group. Then $G \cong PSL_2(Z_{p^{t+1}})$ or $PGL_2(\boldsymbol{Z}_{p^{t+1}})$ (p a prime $\geqq 5$, $t \geqq 1$).*

Although Theorem 1 is actually deduced from the more general Theorem 3, the method of proof is, in effect, to establish successively that $G/O(G)$, $O(G)$ and G are what they should be. The first and last steps present no essential difficulties because the results are at hand for dealing with them — for the former, the powerful theorems of Gorenstein, Walter [3] and Suzuki

[1] I am indebted to Professor Z. Janko for suggesting this condition to me.

[6] and for the latter, detailed information about the cohomology groups of $\boldsymbol{F}_p(PGL_2(\boldsymbol{F}_p))$-modules. The proof in the second step is based on the simple observation that A_4 is a subgroup of $PSL_2(\boldsymbol{F}_p)$. This, and the fact that G is an $\mathscr{R}$-group, imply that A_4 acts as a group of automorphisms on $O(G)$ in such a way that each involution in A_4 has cyclic fixed-point group. Theorem 2 takes care of this situation. Let $P_{s,t}(p)$ (p prime, $0 \leqq s \leqq t$) denote the kernel of the naturally defined epimorphism $PGL_2(\boldsymbol{Z}_{p^{t+1}}) \to PGL_2(\boldsymbol{Z}_{p^{s+1}})$.

THEOREM 2. *Let H be a group of odd order. Suppose that A_4 acts as a group of automorphisms on H in such a way that each involution in A_4 has cyclic fixed-point group. Then H is nilpotent and if S is Sylow subgroup of H, S is either cyclic or a group $P_{s,t}(p)$.*

Theorem 2 points to the chief obstacle in determining all *soluble $\mathscr{R}$-groups*, viz. the determination of the groups of odd order which admit an automorphism of order 2 with cyclic fixed-point group. The detailed structure of such groups is not known, though it has been proved that they have nilpotent derived groups (Kovács, Wall [4]).

In Theorem 3, we determine all $\mathscr{R}$-groups which contain neither a normal Sylow 2-subgroup nor a normal Sylow 2-complement. Some notation is needed before stating the Theorem.

DEFINITION. An $\mathscr{R}$-group G is said to be *reduced* if it satisfies the following two conditions:

(i) G has no non-trivial direct factor of odd order;

(ii) G does not contain two non-trivial normal subgroups of relatively prime odd orders.

A direct product $A \times B$ ($|A|$ even, $|B|$ odd) is an $\mathscr{R}$-group if and only if A is an $\mathscr{R}$-group, B is cyclic and $(|B|, |\mathscr{R}_A(u)|) = 1$ for every involution $u \in A$. A group G with normal subgroups N_1, N_2 of relatively prime odd orders is an $\mathscr{R}$-group if and only if G/N_1, G/N_2 are both $\mathscr{R}$-groups (Lemma 2.3). Thus, in order to determine all $\mathscr{R}$-groups, it is sufficient to determine the reduced ones.

The notation $G = (A; B)$ indicates that the group G is an extension of the group B by the group A, i.e. G has a normal subgroup $\bar{B}$ such that $\bar{B} \simeq B$, $G/\bar{B} \simeq A$. Such an extension is called holomorphic if $\bar{B}$ has a complement $\bar{A}$ in G and $\mathscr{C}_G(\bar{B}) \leq \bar{B}$. We denote the cyclic group of order k by C_k, the direct product of n copies of C_k by $(C_k)^n$ and the dihedral group of order $2k$ by D_{2k}. S_n, A_n denote the symmetric and alternating groups on n letters.

THEOREM 3. *Let G be a group of even order which contains neither a normal Sylow 2-subgroup nor a normal Sylow 2-complement. Then G is a* *reduced $\mathscr{R}$-group if and only if it is isomorphic to one of the following groups*:

(1.1) $PGL_2(\boldsymbol{F}_q)$, $PSL_2(\boldsymbol{F}_q)$ (*q a prime-power* $\geqq 3$);

(1.2) $PGL_2(\boldsymbol{Z}_{p^{t+1}})$, $PSL_2(\boldsymbol{Z}_{p^{t+1}})$ (*p a prime* $\geqq 3$, $t \geqq 1$);

(1.3) *the unique holomorphic extensions* $(PGL_2(\boldsymbol{F}_p); (C_p)^3)$, $(PSL_2(\boldsymbol{F}_p); (C_p)^3)$ (*p a prime* $\geqq 5$);

(1.4) *the unique holomorphic extension* $(PSL_2(\boldsymbol{F}_7); (C_{p^t})^3)$ (*p an odd prime* $\equiv 1, 2$ *or* 4 (*mod* 7), $t \geqq 1$);

(1.5) *the unique holomorphic extension* $(A_5; P_{s,t}(p))$ (*p a prime* $\equiv \pm 1$ (*mod* 5), $0 \leqq s \leqq t$, $t \geqq 1$);

(1.6) *the unique holomorphic extensions* $(A_4; P_{s,t}(p))$, $(S_4; P_{s,t}(p))$ (*p a prime* $\geqq 3$, $0 \leqq s \leqq t$, $t \geqq 1$);

(1.7) *the direct product, amalgamating central subgroups of order* 3, *of* C_{3^t} ($t \geqq 1$) *and the unique non-splitting central extension* $(A_6; C_3)$.

NOTE. A proof of *existence* of groups (1.3)—(1.6) may be constructed along the following lines. Representation theory gives the monomorphisms:

(1.3) $$PGL_2(\boldsymbol{F}_p) \to GL_3(\boldsymbol{F}_p) = \mathrm{Aut}\,((C_p)^3),$$

(1.4) $$PSL_2(\boldsymbol{F}_7) \to GL_3(\boldsymbol{F}_p),$$

(1.5), (1.6) $$S_4, A_5 \to PGL_2(\boldsymbol{F}_p),$$

where p satisfies the appropriate congruences in (1.4), (1.5). The last three monomorphisms may be lifted (essentially by Schur's splitting theorem) to monomorphisms:

(1.4)′ $$PSL_2(\boldsymbol{F}_7) \to GL_3(\boldsymbol{Z}_{p^t}) = \mathrm{Aut}\,((C_{p^t})^3),$$

(1.5′), (1.6)′ $$S_4, A_5 \to PGL_2(\boldsymbol{Z}_{p^{t+1}}).$$

(1.3), (1.4)′ establish the existence of the corresponding groups directly. (1.5)′ (1.6)′ provide them as subgroups of $PGL_2(\boldsymbol{Z}_{p^{t+1}})$. The *uniqueness* of these groups follows from the proof of the Theorem. The verification that they are $\mathscr{R}$-groups is straightforward.

Two problems arise naturally out of these results. The first is to characterise the groups $PSL_2(\Omega/\boldsymbol{p}^{t+1}\Omega)$ and $PGL_2(\Omega/\boldsymbol{p}^{t+1}\Omega)$, where Ω is the ring of integers in an algebraic number field and $\boldsymbol{p}$ a prime ideal of Ω. The second is to determine the groups satisfying suitable generalisations of (1.0). E.g., Suzuki's simple groups have the property that the root groups of all involutions are abelian.

Arrangement of the paper. The deduction of Theorems 1 and 2 from Theorem 3 is described below. The remainder of the paper is devoted to proving Theorem 3. The main steps are as follows. After some preliminary general results, it is shown, in Proposition 2.7, that every non 2-nilpotent $\mathscr{R}$-group G satisfies one of the following conditions:

(i) the Sylow 2-subgroup of G are elementary abelian of order $\geqq 8$;

(ii) $G/O(G) \cong PSL_2(\boldsymbol{F}_q)$ or $PGL_2(\boldsymbol{F}_q)$ for some odd prime-power q.

The Theorem is proved for groups of type (i) in § 3, for groups of type (ii) in Proposition 2.8 ($O(G)$ cyclic) and § 4 ($O(G)$ non-cyclic). The last case is the most complicated and an outline of the method is given at the beginning of § 4.

Deduction of Theorem 1 from Theorem 3. Let G satisfy the conditions of Theorem 1. The list (1.1)-(1.7) shows that the Theorem is true for *reduced* $\mathscr{R}$-groups. Thus, we have only to prove that G is reduced.

By Proposition 4.1.4 and the insolubility of G, $O(G)$ is nilpotent. Let $S(\neq 1)$ be a Sylow subgroup of $O(G)$, T the complement of S in $O(G)$ and $\Gamma = G/T$. By Proposition 4.1.4, Γ is a reduced $\mathscr{R}$-group and since $\mathscr{Z}(G) = 1$, $\mathscr{Z}(\Gamma) \cap O(\Gamma) = 1$. Theorem 3 now shows that one of the following conditions holds (notice that $O(\Gamma) \cong S$ and $\Gamma/O(\Gamma) \cong G/O(G)$):

(a) $G/O(G) \cong A_4$ or S_4;

(b) $G/O(G) \cong A_5$ or $PSL_2(\boldsymbol{F}_7)$;

(c) for some prime p, $G/O(G) \cong PSL_2(\boldsymbol{F}_p)$ or $PGL_2(\boldsymbol{F}_p)$ and S is a p-group.

Case (a) is excluded because G is insoluble. In case (b), the hypotheses of the Theorem ensure that $G = \Gamma$, so that G is reduced. If (c) holds (but neither (a) nor (b)), then every Sylow subgroup of $O(G)$ is a p-group for the one fixed p, so again $G = \Gamma$ and G is reduced. This completes the proof.

Deduction of Theorem 2 from Theorem 3. Let H satisfy the conditions of Theorem 2 and form the splitting extension $G = (A_4; H)$ corresponding to the given action of A_4 on H. Since the involutions in A_4 have cyclic fixed-point groups, G is an $\mathscr{R}$-group. By Proposition 4.1.4., $H = O(G)$ is nilpotent.[1] Let S, T, Γ be as in the previous proof. By Proposition 4.1.4., either S is cyclic or Γ is reduced. In the latter case, Theorem 3 shows that $S(\cong O(\Gamma))$ is a group $P_{s,t}(p)$. This completes the proof.

2. General results

We first consider the factor groups of an $\mathscr{R}$-group.

2.1 Lemma. *Let G be a group of even order, N a normal subgroup of odd order. If u is an involution in G, then $\mathscr{R}_{G/N}(uN) = \mathscr{R}_G(u)N/N$.*

Proof. Clearly, uN is an involution and $\mathscr{R}_G(u)\ N/N \leqq \mathscr{R}_{G/N}(uN)$. It remains to prove that, if xN is a root of uN, then $x \in \mathscr{R}_G(u)N$. Since xN has even order, x has even order; let v be the involution in $\langle x \rangle$. Then vN is the involution in $\langle xN \rangle$, so that $vN = uN$. By Sylow's theorem, $v = nun^{-1}$ for some $n \in N$. Therefore $n^{-1}xn \in \mathscr{R}_G(u)$ and so $x = n^{-1}xn[n, x] \in \mathscr{R}_G(u)N$, as required.

2.2 Corollary. *If G is an $\mathscr{R}$-group and N a normal subgroup of odd order, then G/N is an $\mathscr{R}$-group.*

2.3 Lemma. *Let G be a group of even order and N_1, N_2 normal subgroups of relatively prime odd orders. Then G is an $\mathscr{R}$-group if (and only if) G/N_1, G/N_2 are $\mathscr{R}$-groups.*

Proof. Let u be an involution in G and write $R = \mathscr{R}_G(u)$, $R_i = R \cap N_i$. We prove that R is cyclic by showing (a) that R is abelian and (b) that the Sylow subgroup of R are cyclic.

(a) Since $R/R_i \cong RN_i/N_i = \mathscr{R}_{G/N_i}(uN_i)$, R/R_i is cyclic. Therefore, since $R_1 \cap R_2 = 1$, R is abelian.

(b) Let P be a Sylow p-subgroup of R. Since $(|R_1|, |R_2|) = 1$, we may assume $p \nmid |R_1|$. Then $P \cong PR_1/R_1 \leqq R/R_1$, so that P is cyclic, as required.

Clearly, a group G of even order is an $\mathscr{R}$-group if and only if $\mathscr{C}_G(u)$ is an $\mathscr{R}$-group for each involution $u \in G$. We now determine the structure of $\mathscr{C}_G(u)$.

2.4 Lemma. *Let G be an $\mathscr{R}$-group, u an involution in G and $x \in \mathscr{C}_G(u)$. If x has odd order or order $2^\lambda > 2$, then $x \in \mathscr{R}_G(u)$.*

Proof. If x has odd order, $xu \in \mathscr{R}_G(u)$. Since $u \in \mathscr{R}_G(u)$, $x \in \mathscr{R}_G(u)$. If x has order $2^\lambda > 2$, let v be the involution in $\langle x \rangle$. Then $x \in \mathscr{R}_G(v)$ and $xu \in \mathscr{R}_G(v)$, so that $u \in \mathscr{R}_G(v)$. Since $\mathscr{R}_G(v)$ is cyclic, $u = v$. Hence $x \in \mathscr{R}_G(u)$.

2.5 Lemma. *Let G be an $\mathscr{R}$-group and u an involution in G. Then $\mathscr{C}_G(u)$ has one of the following structures:*

$$C_{2m}\,;\ D_{4m} \times C_n((4m, n) = 1);\quad ((C_2)^t; C_n) \qquad (n \text{ odd}, t \geqq 3).$$

Proof. Write $C = \mathscr{C}_G(u)$, $R = \mathscr{R}_G(u)$ and let K be the subgroup of R formed by its elements of odd order. By lemma 2.4, $K \triangleleft C$ and $C = KQ$, where Q is a Sylow 2-subgroup of C. Again by lemma 2.4, $Q \cap R$ is a cyclic subgroup of Q such that[2] $Q \setminus (Q \cap R)$ consists entirely of involutions. It is well known that this implies either

(a) $Q \cap R = Q$ and Q is cyclic

or (b) $|Q : Q \cap R| = 2$ and Q is dihedral

or (c) Q is elementary abelian.

[2] If $Y \subseteq X$, $X \setminus Y$ denotes the (set) complement of Y in X.

https://doi.org/10.1017/S1446788700006182 Published online by Cambridge University Press

In case (a), $C = KQ = R$ is cyclic. In case (b), $|C : R| = 2$ and $C = R \cup vR$ for some involution $v \in Q$. Let $R_1(R_2)$ be the product of those Sylow subgroups of R whose generators are inverted (centralized) by v. Then $D = R_1 \cup vR_1$ is dihedral, R_2 is cyclic and $C = D \times R_2$; clearly D, R_2 have relatively prime orders. In case (c), $C = KQ$ is evidently an extension $((C_2)^t; C_n)$, n odd. This proves the lemma.

2.6 Corollary. *The Sylow 2-subgroups of an $\mathscr{R}$-group are cyclic, dihedral or elementary abelian.*

2.7 Proposition. *Every $\mathscr{R}$-group G satisfies one of the following conditions:*

(a) *G has a normal Sylow 2-complement;*
(b) *the Sylow 2-subgroups of G are elementary abelian of order $\geqq 8$;*
(c) *G is an extension $(\Gamma; P)$, where P has odd order and $\Gamma \cong PGL_2(\boldsymbol{F}_q)$ or $PSL_2(\boldsymbol{F}_q)$ for some odd prime-power q.*

Proof. If neither (a) nor (b) holds, the Sylow 2-subgroups of G are dihedral. By lemma 2.4, the centralizer of an involution in G has an abelian 2-complement. Therefore, by a theorem of Gorenstein and Walter [3], G is an extension $(\Gamma; P)$, where P has odd order and $\Gamma \cong A_7$, $PGL_2(\boldsymbol{F}_q)$ or $PSL_2(\boldsymbol{F}_q)$ (q an odd prime-power). The first case is excluded by corollary 2.2 because A_7 is not an $\mathscr{R}$-group. This proves the proposition.

We now dispose of the easiest case arising in (c).

2.8 Proposition. *Let G be an extension $(\Gamma; P)$, where P is a non-trivial cyclic group of odd order and $\Gamma \cong PGL_2(\boldsymbol{F}_q)$ or $PSL_2(\boldsymbol{F}_q)$ (q an odd prime-power). Suppose G does not have a normal Sylow 2-subgroup. Then G is a reduced $\mathscr{R}$-group if and only if it is a group (1.7).*

Proof. It is easily verified that (1.7) is a reduced $\mathscr{R}$-group. Conversely, let G be a reduced $\mathscr{R}$-group satisfying the conditions of the proposition. Let G^+ denote the subgroup (of index 1 or 2) such that $G^+/P \cong PSL_2(\boldsymbol{F}_q)$. Since P is cyclic, $G'P$ centralizes P. Now $G'P/P \cong (C_2)^2$ if $G = G^+$ and $q = 3$, and $G'P = G^+$ otherwise. The former case is excluded because G does not have a normal Sylow 2-subgroup. Therefore G^+ centralizes P. Suppose now that $G > G^+$. Let u be an involution in G^+. Since uP has a root in $(G/P)\setminus(G^+/P)$, it follows from lemma 2.1 that u has a root v in $G\setminus G^+$. By lemma 2.4, v centralizes P and so $\mathscr{C}_G(P) = G$. Thus, $P \leqq \mathscr{Z}(G)$ in all cases.

It is easy to see that, if $P \cap G' = 1$, then either $G/P \cong A_4$ and $G' \cong (C_2)^2$ or P is a direct factor of G. Both cases are excluded by assumption. Now $P \cap G'$ is isomorphic to a subgroup of the Schur multiplicator $\mathscr{S}(G/P)$

of G/P. It is known[3] that $|\mathscr{S}(G/P)| = 6$ if $G/P \cong PSL_2(\boldsymbol{F}_q) \cong A_6$ and $|\mathscr{S}(G/P)| = 2$ otherwise. Therefore $G/P \cong A_6$ and $|P \cap G'| = 3$. Since G has no direct factor of odd order > 1, it follows that G' is the non-trivial (central) extension[4] $(A_6; C_3)$ and $P \cong C_{3^t}$. Thus G is the group (1.7).

Finally, we determine the structure of the Sylow 2-normalizers in an $\mathscr{R}$-group.

2.9 Lemma. *Let G be an $\mathscr{R}$-group, Q a Sylow 2-subgroup of G, $N = \mathscr{N}_G(Q)$ and $C = \mathscr{C}_G(Q)$. Then $C = Q \times K$ (K cyclic) and N/C acts as a group of fixed-point free automorphisms*[5] *on Q. Also $N = C$ unless $Q \cong (C_2)^t$ $(t \geqq 2)$.*

Proof. The first and last statements follow at once from lemma 2.4 and corollary 2.6. To prove the second statement we must show that, if $x \in N$ commutes with the involution $u \in Q$, then x commutes with every involution $v \in Q$. By lemma 2.4, $\mathscr{C}_G(u)$ has a cyclic normal Sylow 2-complement K Since $v \in \mathscr{C}_G(u)$ and $x \in K$, v normalizes $\langle x \rangle$. Therefore $[v, x] \in \langle x \rangle \cap Q = 1$, so that v commutes with x, as required.

3. Elementary abelian Sylow 2-subgroups

In this section, we assume that

(A) *G is an $\mathscr{R}$-group,*

(B) *G has a Sylow 2-subgroup $Q \cong (C_2)^t$ $(t \geqq 3)$.*

3.1 Lemma. *Either G has no subgroup of index 2 or G has a normal 2-complement.*

Proof. Lemma 2.9 shows that either $Q \leqq \mathscr{Z}(\mathscr{N}(Q))$ (in which case G has a normal 2-complement by Burnside's theorem) or $Q \leqq \mathscr{N}(Q)'$ (in which case G has no subgroup of index 2).

3.2 Lemma. *If G has a normal 2-complement P, then P is cyclic.*

Proof. By a theorem of Ward [7], P is nilpotent. We may therefore assume that P is a p-group for some prime p. Since $G/\Phi(P)$ is an $\mathscr{R}$-group and since P is cyclic if $P/\Phi(P)$ is cyclic, we may further assume that P is elementary abelian.

Let us regard P as a vector space over $\boldsymbol{F}_p$ on which Q acts as a group of linear transformations. Since $Q \cong (C_2)^t$, the irreducible representations of Q over $\boldsymbol{F}_p$ are all 1-dimensional. Since $p \neq 2$, P is a completely reducible

[3] Schur [5].

[4] The uniqueness of this extension follows from the fact that the "Darstellungsgruppe" of a simple group is unique (Schur, l.c.).

[5] This implies that N/C is metacyclic with cyclic Sylow subgroups.

Q-module. Thus P is a direct sum of 1-dimensional submodules $P_1, \cdots, P_r$. Now, by lemma 2.4, no involution in Q centralizes more than one P_i. On the other hand, if $r > 1$,

$$\mathscr{C}_Q(P_1) \cap \mathscr{C}_Q(P_2) > 1$$

because $|Q : \mathscr{C}_Q(P_i)| = 1$ or 2 and $|Q| \geqq 2^3$. Thus $r = 1$, i.e. P is cyclic as required.

3.3 PROPOSITION. *G satisfies one of the following conditions*:

(a) $Q \trianglelefteq G$;

(b) *G has a cyclic normal 2-complement*;

(c) $G \cong PSL_2(\boldsymbol{F}_{2^t}) \times C_s$ *($t \geqq 3$, s odd)*.

PROOF. Choose an involution $u \in Q$ such that the order of $\mathscr{C}(u)$ $(= \mathscr{C}_G(u))$ is as large as possible. By lemma 2.4, $\mathscr{C}(u)$ has a normal cyclic 2-complement K.

FIRST CASE: Q does not centralize K. Let P be a Sylow subgroup of K which is not centralized by Q. Then $Q_1 = Q \cap \mathscr{C}(P)$ is a subgroup of Q of index 2 and every element of $Q \setminus Q_1$ inverts the elements of P.

We prove that $\mathscr{N}(Q) \leqq \mathscr{N}(P)$. It is sufficient to prove that, if x is an element of $\mathscr{N}(Q)$ of odd order, then $P = P^x$. Since $|Q| \geqq 8$ and $|Q : Q_1| = 2$, $Q_1 \cap Q_1^x > 1$. An involution v in $Q_1 \cap Q_1^x$ centralizes both P and P^x, whence by lemma 2.4, $P = P^x$, as required.

Now, since Q does not centralize P, the cyclic group $\mathscr{N}(P)/\mathscr{C}(P)$ has even order. By lemma 3.1, $\mathscr{N}(P)$ has a normal 2-complement. Since $\mathscr{N}(Q) \leqq \mathscr{N}(P)$, it follows that $Q \leqq \mathscr{Z}(\mathscr{N}(Q))$. Hence, by Burnside's theorem, G has a normal 2-complement (which is cyclic by lemma 3.2).

SECOND CASE: Q centralizes K, i.e. $\mathscr{C}(u)$ is abelian. If v is an involution in Q, then clearly $\mathscr{C}(u) \leqq \mathscr{C}(v)$. Hence, by the choice of $\mathscr{C}(u)$, $\mathscr{C}(u) = \mathscr{C}(v)$. Thus every involution has abelian centralizer. By a theorem of Suzuki [6] (and lemma 3.2), G satisfies one of the conditions in the proposition.

4. Dihedral Sylow 2-subgroups

In this section, we assume that

(A) *G is a reduced $\mathscr{R}$-group*;

(B) *P is a non-cyclic* [6] *normal subgroup of G of odd order*;

(C) $G/P \cong PGL_2(\boldsymbol{F}_q)$ *or* $PSL_2(\boldsymbol{F}_q)$, *where q is an odd prime-power.*

Write $\Gamma = G/P$. Choose a subgroup H/P of Γ isomorphic to A_4 and let

[6] The case where P is cyclic was treated in lemma 2.8.

$T = \{1, u_1, u_2, u_3\}$ be a Sylow 2-subgroup of H. Let $\Gamma_2(p^t)$, $\Gamma_2^+(p^t)$ denote the groups $PGL_2(\boldsymbol{Z}_{p^t})$, $PSL_2(\boldsymbol{Z}_{p^t})$ (p an odd prime).

We prove, in 4.1, that P is a p-group with each G-composition factor [7] of order p^3. Let $|P| = p^{3t}$, $|P : P'| = p^{3s}$ $(0 < s \leqq t)$. We call G a *split group* if P has a complement in G. Two groups satisfying (A)-(C) are said to be *of the same type* if they have the same Γ, p, s, t and both are split groups or both non-split groups. In 4.2, we show that G has the same type as some group listed in Theorem 3. Then, in 4.3, we complete the proof by showing that groups of the same type are isomorphic.

4.1. *Structure of* P.

4.1.1. LEMMA. *If X is an H-subgroup of P, then*

$$X = X_1X_2X_3,\ X_1 \cap X_2 = X_2 \cap X_3 = X_3 \cap X_1 = X_0,$$

where

$$X_i = \mathscr{C}_X(u_i)\ (i = 1, 2, 3),\ X_0 = \mathscr{C}_X(T).$$

X_1, X_2, X_3 are cyclic groups conjugate in H. X_0 is a cyclic Hall subgroup of X and $X_0 \leqq \mathscr{Z}(P)$.

PROOF. The first statement is a known general result (cf. Gorenstein, Walter [3]). The X_i $(i = 1, 2, 3)$ are cyclic because G is an $\mathscr{R}$-group, conjugate in H because the u_i are. Let $1 \leqq i,\ j \leqq 3,\ i \neq j$. Since $u_iu_j = u_ju_i$, u_j normalizes X_i. Therefore, since X_i is cyclic and $u_j^2 = 1$, $X_0\ (= \mathscr{C}_{X_i}(u_j))$ is a Hall subgroup of X_i. This and the first part of the lemma show that X_0 is a cyclic central Hall subgroup of X. $X_0 \leqq P_0\ (= \mathscr{C}_P(T))$ and P_0 is central in P, whence X_0 is central in P.

4.1.2. COROLLARY. *If X is an H-subgroup of P of prime exponent p, then either $X_0 = X \cong C_p$ or $X_0 = 1$, $X = X_1 \times X_2 \times X_3 \cong (C_p)^3$. X is the unique minimal H-subgroup of P of p-power order.*

PROOF. The lemma shows that $X_0 = X \cong C_p$ or $X_0 = 1$, $X = X_1X_2X_3$, $|X| = p^3$. In the second case, $X' < X$ and $(X')_0 \leqq X_0 = 1$, so that $X' = 1$ and thus $X = X_1 \times X_2 \times X_3 \cong (C_p)^3$. X is patently a minimal H-subgroup. Let Y be any H-subgroup of P of exponent p. Since, X, Y are minimal H-subgroups, the H-subgroup XY has exponent p. Hence XY is a minimal H-subgroup and so $XY = X = Y$. Thus X is unique.

4.1.3. LEMMA. *P is nilpotent.*

PROOF. We prove the following result: if X is an H-subgroup of P of

[7] We shall often regard P as a G-group, i.e. a group on which G acts by conjugation. Thus, the G-subgroups of P are those subgroups of P which are normal in G. Where convenient, we will use additive notation and module terminology for abelian G-groups.

prime exponent p and D/C an H-composition factor of P such that C centralizes X, then D centralizes X. Since P is soluble, this implies that $\mathscr{Z}(P) > 1$. This last result and corollary 2.2 then show that the ascending central series of P terminates at P. If Y is an H-subgroup of P, we write $Y_0 = \mathscr{C}_Y(T)$, $Y_i = \mathscr{C}_Y(u_i)$ $(i = 1, 2, 3)$.

Since $X_0 \leqq \mathscr{Z}(P)$, we may assume that $X > X_0$. Then, by corollary 4.1.2, $|X| = p^3$ and X_1, X_2, X_3 are simple T-groups, no two of which are T-isomorphic. Also, if v is an element of H which transforms the u_i cyclically, then X is a simple $\langle v, TD\rangle$-group. Hence, by Clifford's theorem, either X_1, X_2, X_3 are TD-groups or X is a simple TD-group. In the first case, TD induces an abelian group of automorphisms of X, so that $[T, D]$ centralizes X. By lemma 4.1.1, $D = D_0\,[T, D]$ and so D centralizes X. In the second case, consider the groups $X^{(i)} = \mathscr{C}_X(CD_i)$ $(i = 1, 2, 3)$. Since $X_i \leqq D_i$ and $CD_i \lhd TD_i$, $X^{(i)}$ is a non-trivial TD-group. Therefore, since X is a simple TD-group, $X^{(i)} = X$. Thus, $D = D_1 D_2 D_3$ again centralizes X. This proves the lemma.

We break off at this point to prove a general result about $\mathscr{R}$-groups, required in deducing Theorems 1 and 2 from Theorem 3. Notice that the hypotheses that G is reduced and P non-cyclic have not been used in proving Lemmas 4.1.1—4.1.3. Thus, these results apply to any $\mathscr{R}$-group satisfying (c) in Proposition 2.7.

4.1.4. PROPOSITION. *If $\tilde{G}$ is any non 2-nilpotent $\mathscr{R}$-group, then $O(\tilde{G})$ is nilpotent.*

Let S be a Sylow subgroup of $O(\tilde{G})$, U the complement of S in $O(\tilde{G})$ and $\Gamma = \tilde{G}/U$. If S is cyclic, $S \leqq \mathscr{Z}(\tilde{G})$. If S is non-cyclic, $S \cap \mathscr{Z}(\tilde{G}) = 1$ and Γ is a reduced $\mathscr{R}$-group.

PROOF. Since $\tilde{G}$ is not 2-nilpotent, either (b) or (c) of Proposition 2.7 holds. In the former case, $O(\tilde{G})$ is a cyclic central subgroup of $\tilde{G}$ by Proposition 3.3 and Lemma 2.9. In the latter case, $O(\tilde{G})$ is nilpotent by Lemma 4.1.3. Clearly, Γ is an $\mathscr{R}$-group. Since $O(\Gamma) = SU/U \simeq S$ and $O(\Gamma) \cap \mathscr{Z}(\Gamma) = (S \cap \mathscr{Z}(\tilde{G}))U/U \cong S \cap \mathscr{Z}(\tilde{G})$, we may assume for the remainder of the proof that $\Gamma = \tilde{G}$, $S = O(\tilde{G})$.

By the last part of Lemma 4.1.1, either S is cyclic or $S \cap \mathscr{Z}(\tilde{G}) = 1$. In the former case, $S \leqq \mathscr{Z}(\tilde{G})$ by Proposition 2.8. In the latter case, $\tilde{G}$ is reduced because $O(\tilde{G})$ is a prime-power group and $O(\tilde{G}) \cap \mathscr{Z}(\tilde{G}) = 1$. This completes the proof.

We return now to the study of the group G. In the next two corollaries, the assertion that P is a p-group follows from Lemma 4.1.3 and the assumption that G is reduced. The remaining statements follow from Corollary 4.1.2.

4.1.5. COROLLARY. *P is a p-group for some prime p. There is precisely one series*

$$P = P_0 > P_1 \cdots > P_t = 1 \tag{1}$$

of H-subgroups of P such that each factor P_i/P_{i+1} has exponent p; in particular (1) *is the Frattini series of P. For each i, $|P_i : P_{i+1}| = p$ or p^3.*

4.1.6. Corollary. (1) *is the unique G-composition series of P. Every G-subgroup, and in particular every characteristic subgroup, of P is one of the P_i.*

We consider now the power and commutator structure of P.

4.1.7. Lemma. *The rule $xP_i \to x^p P_{i+1}$ ($x \in P_{i-1}$; $0 < i < t$) defines a G-isomorphism $\pi_i : P_{i-1}/P_i \to P_i/P_{i+1}$.*

Proof. By Corollary 4.1.6., $[P_k, \underbrace{P, \cdots, P}_{n}] \leqq P_{k+n}$. Therefore, if $x \in P$ and $y \in P_k$,

$$(xy)^p \equiv x^p y^p [y, x]^{\binom{p}{2}} \pmod{P_{k+2}},$$
$$[y, x]^p \equiv 1 \pmod{P_{k+2}},$$

and so

$$(xy)^p \equiv x^p y^p \pmod{P_{k+2}}. \tag{2}$$

(2) shows that π_i is a well defined G-isomorphism. π_i is non-zero because P_{i-1}/P_{i+1} is not a group of exponent p. Therefore, since P_{i-1}/P_i and P_i/P_{i+1} are irreducible G-modules, π_i is a G-isomorphism.

4.1.8. Corollary. *Every factor P_i/P_{i+1} has order p^3.*

Proof. The lemma shows that all factors have the same order, p or p^3. If the common order were p, $P/\Phi(P) = P/P_1$ would be cyclic and so P would be cyclic, contrary to assumption.

4.1.9. Corollary. *P_{i+1} is the set of p-th powers of the elements of P_i.*

Proof. Let $x \in P$ and $y \in P_k \setminus P_{k+1}$. If $k = t-1$, y is a central element of P of order p and $(xy)^p = x^p$. If $k < t-1$, $y^p \in P_{k+1} \setminus P_{k+2}$ and so, by (2), $(xy)^p \neq x^p$. Thus, $(xy)^p = x^p$ if and only if $y \in P_{t-1}$. It follows that the set S of p-th powers of the elements of P_i has $|P_i|/|P_{t-1}| = |P_{i+1}|$ elements. Thus $S = P_{i+1}$.

4.1.10. Lemma. *If $P' = P_s$, then $[P_i, P_j] = P_{i+j+s}$ (where $P_k = 1$ when $k > t$).*

Proof. Replacing y by $[x, y]$ in (2), we see that, if $x, y \in P$ and $[x, y] \in P_k$, then

$$[x^p, y] \equiv [x, y]^p \pmod{P_{k+2}}. \tag{3}$$

It follows easily from (3) and lemma 4.1.7. that

$$[x^{p^i}, y^{p^j}] \equiv [x, y]^{p^{i+j}} \pmod{P_{i+j+s+1}}.$$

Therefore, since $P_{i+j+s+1} = \Phi(P_{i+j+s})$, the commutators $[x^{p^i}, y^{p^j}]$ $(x, y \in P)$ generate P_{i+j+s}. On the other hand, by corollary 4.1.9, these commutators generate $[P_i, P_j]$.

4.1.11. Lemma. *There exist $u, v \in H$ and $x \in P \setminus P_1$ such that*

(i) $u^2 = v^3 = (uv)^3 = 1$;

(ii) $x^u = x$;

(iii) $x^{p^s} = [x^v, x^{v^2}][x^v, x^{v^2}, u]^{\frac{1}{2}}$.

Proof. Write $N = \mathscr{N}_H(T)$. Clearly, $NP = H$ and since each factor P_i/P_{i+1} is a faithful T-module, $N \cap P = \mathscr{C}_P(T) = 1$. Therefore N is a complement of P in H and so $N \cong A_4$. Choose $u, v \in N$ so that (i) holds.

By Corollary 4.1.2, P/P_1 has a T-module decomposition

$$P/P_1 = \langle yP_1 \rangle \oplus \langle y^v P_1 \rangle \oplus \langle y^{v^2} P_1 \rangle,$$

where $(yP_1)^u = yP_1$. In particular,

$$(y^{v^i})^u \equiv (y^{v^i})^{-1} \pmod{P_1} \quad (i = 1, 2)$$

so that

$$[y^v, y^{v^2}]^u \equiv [y^v, y^{v^2}] \pmod{P_{s+1}}. \tag{4}$$

Here

$$[y^v, y^{v^2}] \not\equiv 1 \pmod{P_{s+1}} \text{ if } s < t, \tag{5}$$

since otherwise $P' \leqq P_{s+1}$, contrary to the definition of s.

Since $|yP_1|$ is odd and $u^2 = 1$, we may assume $y^u = y$. We prove, by induction on $t-s$, that (iii) holds for a suitable generator x of $\langle y \rangle$.

The assertion is obvious for $s = t$. Suppose $s < t$ and $y^{p^s} = abc$, where $a = [y^v, y^{v^2}]$, $b = [y^v, y^{v^2}, u]^{\frac{1}{2}}$, $c \in P_{t-1}$. Now $b^{2u} = (a^{-1}a^u)^u = b^{-2}$, so that $(ab)^u = a^u b^2 b^u = ab$; hence $c^u = c$. By lemma 2.4, c has the form $y^{\mu p^{t-1}}$ and therefore

$$y^{\lambda p^s} = ab, \text{ where } \lambda = 1 + \mu p^{t-1-s}.$$

Since $a \notin P_{s+1}$ and $b \in P_{s+1}$ (by (4) and (5)), $\lambda \not\equiv 0 \pmod{p}$. We choose x so that $x^\lambda = y$. Setting

$$x_2 = x^v, \quad x_3 = x^{v^2}, \quad \xi_2 = x_2^{\lambda-1}, \quad \xi_3 = x_3^{\lambda-1},$$

and using (3), we find that

$$\begin{aligned} a &= [x_2\xi_2, x_3\xi_3] \\ &= [x_2, \xi_3][x_2, x_3][x_2, x_3, \xi_3][x_2, x_3\xi_3, \xi_2][\xi_2, x_3\xi_3] \\ &= [x_2, x_3]^{\lambda^2}. \end{aligned}$$

Then, since

$$[x_2, x_3]^{\lambda^2-1} \in P_{t-1}, \quad [x_2, x_3, u]^{\lambda^2-1} \in P_{t-1},$$

we get $b^2 = [x_2, x_3, u]^{\lambda^2}$ and

$$x^{\lambda^2 p^s} = y^{\lambda p^s} = ab = ([x_2, x_3][x_2, x_3, u]^{\frac{1}{2}})^{\lambda^2}.$$

Thus x satisfies (iii) as required.

4.1.12. COROLLARY. *H is a splitting extension of P by A_4.*

4.1.13. LEMMA. *The Γ-module P/P_1 affords a faithful, absolutely irreducible, unimodular representation ρ of Γ over $\boldsymbol{F}_p$. If P is non-abelian, ρ is self-contragredient.*

PROOF. If $\Gamma \cong A_4$, the lemma follows from Corollary 4.1.2. We may therefore suppose that $\Gamma > H/P$ and that the restriction, ρ', of ρ to H/P satisfies the conclusion of the lemma. Then ρ is absolutely irreducible because ρ' is. ρ is faithful because ρ' is faithful and every non-trivial normal subgroup of Γ contains TP/P.

Suppose ρ were not unimodular. Since $\Gamma > H/P$, Γ is generated by involutions. Thus there exists an involution $uP \in \Gamma$ such that the matrix $U = \rho(uP)$ has determinant -1. U is similar to diag $(-1, -1, -1)$ or diag $(-1, 1, 1)$. The first case is impossible because ρ is faithful and $\mathscr{Z}(\Gamma) = 1$. In the second case, U has a 2-dimensional space of invariant vectors, which means that $\mathscr{C}_{P/P_1}(uP_1)$ has a subgroup $\cong (C_p)^2$. This is impossible by lemma 2.4. Hence ρ is unimodular.

Suppose now that P is non-abelian, i.e. $s < t$. Let $zP \in \Gamma$ and let Z be the matrix of the induced linear transformation on P/P_1 with respect to the basis $xP_1, x^v P_1, x^{v^2} P_1$ in lemma 4.1.11. The relation (iii) and its conjugates under v show that $Z = \text{adj } Z$, i.e. $ZZ' = |Z|I$. Hence $|Z| = 1$ and $ZZ' = I$. This shows that ρ is self-contragredient.

4.2. *Type of G.*

4.2.1. LEMMA. *One of the following holds*:

(a) $q = p \geqq 5$;

(b) $q = 3, p \geqq 3$;

(c) $q = 5$, $\Gamma \cong A_5$ *and* $p \equiv \pm 1$ (*mod* 5);

(d) $q = 7$, $\Gamma \cong \Gamma_2^+(7)$, *$P$ is abelian and* $p \equiv 1, 2,$ *or* 4 (*mod* 7).

In the last 3 *cases, G is a split group.*

PROOF. Let $q = r^\lambda$, where r is prime.

FIRST CASE: $p \neq r$. Let E be an elementary abelian subgroup of Γ of order r^λ and $N = \mathscr{N}_\Gamma(E)$. P/P_1 is a completely reducible E-module; let χ_1, χ_2, χ_3 be the corresponding linear characters of E. Since E is faithfully represented, we may assume χ_1 is not the trivial character. Then χ_1 has

$|N : E|$ conjugates under N because N/E acts fixed-point-free on E. Since each such conjugate is a χ_i, $\frac{1}{2}(q-1) \leqq 3$ if $\Gamma \cong PSL_2(\boldsymbol{F}_q)$ and $q-1 \leqq 3$ if $\Gamma \cong PGL_2(\boldsymbol{F}_q)$. Hence either $q = 3$ or $q = 5$, $\Gamma \cong A_5$ or $q = 7$, $\Gamma \cong \Gamma_2^+(7)$. If $q = 5$, an element of Γ of order 5 is represented by a linear transformation with characteristic roots 1, ε, ε^{-1}, where ε is a primitive 5-th root of 1. Therefore $\varepsilon+\varepsilon^{-1} = -\frac{1}{2}(1+\sqrt{5}) \in \boldsymbol{F}_p$ and so $p \equiv \pm 1 \pmod 5$. If $q = 7$, an element of Γ of order 7 is represented by a linear transformation with characteristic roots ω, ω^2, ω^4, where ω is a primitive 7-th root of 1. In the contragredient representation, the same element is represented by a linear transformation with characteristic roots ω^{-1}, ω^{-2}, ω^{-4}. Hence P is abelian by lemma 4.1.13. Since $\omega+\omega^2+\omega^4 = -\frac{1}{2}(1+\sqrt{-7}) \in \boldsymbol{F}_p$, $p \equiv 1$, 2 or 4 (mod 7). In all these cases, G splits over P because P, Γ have relatively prime orders.

Second case: $p = r$. Let Z be the matrix representing an element of Γ of order $\frac{1}{2}(q+1)$ in the representation ρ. The smallest power p^μ such that $p^\mu \equiv 1 \pmod{\frac{1}{2}(q+1)}$ is q^2. Hence Z has a characteristic root θ such that $\boldsymbol{F}_p(\theta) = \boldsymbol{F}_{q^2}$. Each of the 2λ conjugates of θ over $\boldsymbol{F}_p$ is a characteristic root of Z, so that $2\lambda \leqq 3$. Thus $q = p$ as required. If $q = 3$, P has the complement $\mathscr{N}_G(T)$ in G. This completes the proof.

4.2.2. Lemma. *If $p \geqq 5$ and $G = \Gamma_2^+(p^2)$, G does not split over P.*

Proof. A Sylow p-subgroup S of G is regular because $|S| = p^4$ and $p \geqq 5$. If G were a split group, S would be generated by elements of order p and so would have exponent p. However, it is easily verified that G has elements of order p^2.

Before proving the next lemma, we set down some facts about the representations of $\mathscr{G} = \Gamma_2(p)$ or $\Gamma_2^+(p)$ over $\boldsymbol{F}_q$ (cf. Brauer and Nesbitt [1]). The $\frac{1}{2}(p+1)$ irreducible *unimodular* representations of $\mathscr{G}$ over $\boldsymbol{F}_p$ have degrees $1, 3, 5, \cdots, p$ and all are absolutely irreducible. We denote the corresponding irreducible $\mathscr{G}$-modules by [1], [3], $\cdots$, [p]. Notice that the module [p] is projective because p divides $|\mathscr{G}|$ to the first power.

By lemma 4.1.13, $P/P_1 \cong [3]$ when $q = p$. The representation corresponding to [3] is given by the classical isomorphism $\Gamma_2(p) \rightarrow O_3^+(\boldsymbol{F}_p)$ (or $\Gamma_2^+(p) \rightarrow \Omega_3(\boldsymbol{F}_p)$). It is the only faithful unimodular representation of degree 3 (otherwise such a representation would have all composition factors of degree 1 and $\mathscr{G}$ would be nilpotent, which is clearly not the case).

4.2.3. Lemma. *If $p \geqq 5$, $t \geqq 2$, the group of automorphisms of P/P_2 has no subgroup $\cong \Gamma_2^+(p)$.*

Proof. We may assume without loss of generality that $t = 2$. Choose $x_1 = x$, $x_2 = x^v$, $x_3 = x^{v^2}$ as in lemma 4.1.11. Then either $x_1^p = [x_2, x_3]$,

https://doi.org/10.1017/S1446788700006182 Published online by Cambridge University Press

$x_2^p = [x_3, x_1]$, $x_3^p = [x_1, x_2]$ or $P \cong (C_{p^2})^3$. Thus, if $\bar{G}$ is the $\mathscr{R}$-group $\Gamma_2(p^{t+1})$ $(t \geqq 3)$, $P \cong \bar{P}/\bar{P}_2$ or $\bar{P}_1/\bar{P}_3$. Since $\mathscr{C}_{\bar{G}}(\bar{P}_i/\bar{P}_{i+2}) = \bar{P}_1$, $\bar{G}$ induces a group of automorphisms of $\bar{P}_i/\bar{P}_{i+2}$ isomorphic to $\Gamma_2(p^2)$. Thus, the group of automorphisms, A, of P has a subgroup $X \cong \Gamma_2(p^2)$. Moreover, by the argument in lemma 4.1.13 (applied to $\bar{G}$), we may suppose each $\alpha \in X$ has the property that

$$(x_i P_1)^\alpha = \prod_1^3 (x_j P_1)^{\alpha_{ij}} \qquad (i = 1, 2, 3),$$

where $(\alpha_{ij})'(\alpha_{ij}) = I$, $|\alpha_{ij}| = 1$.

Let B denote the subgroup of A formed by *all* automorphisms α with this property. Then $B = XC$, where C is the group of automorphisms θ of the form

$$x_i^\theta = x_i \prod_1^3 x_j^{p\theta_{ij}} \qquad (i = 1, 2, 3).$$

Clearly, B is an extension of C by $\Gamma_2(p)$ and $\theta \to (\theta_{ij})$ is an isomorphism of C onto the additive group of all 3×3 matrices over $\mathbf{F}_p$. If $\alpha \in B$, $\theta \in C$, then θ^α is the element of C corresponding to the matrix $(\alpha_{ij})^{-1}(\theta_{ij})(\alpha_{ij})$. It follows that C is a $\Gamma_2(p)$-module $\cong [\check{3}] \otimes [3]$ (where $\vee$ denotes the contragredient).

Now, since $p > 3$, C is the direct sum of the $\Gamma_2(p)$-submodules

$$\begin{aligned} C_1 &= \{\theta | (\theta_{ij}) = \lambda I\}, \\ C_3 &= \{\theta | (\theta_{ij}) = -(\theta_{ij})'\}, \\ C_5 &= \{\theta | (\theta_{ij}) = (\theta_{ij})', \ tr(\theta_{ij}) = 0\}. \end{aligned}$$

Since $[3]$ is absolutely irreducible, $[\check{3}] \otimes [3]$ has only the one submodule $\cong [1]$. Since C is self-contragredient and since $[1]$, $[3]$, $[5]$ are its only possible composition factors, it follows easily that C_i are irreducible. Thus, $C \cong [1] \oplus [3] \oplus [5]$ and X is a complement of $C_1 C_5$ in B.

Suppose now that A has a subgroup $Y \cong \Gamma_2^+(p)$. Let τ denote the natural homomorphism of A into the group of automorphisms of P/P_1. Evidently $Y^\tau \cong \Gamma_2^+(p)$, so that $P/P_1 \cong [3]$ as Y^τ-modules. Thus, if P is abelian, Y^τ is conjugate in $GL(P/P_1) = A^\tau$ to a subgroup of B^τ. If P is not abelian, $Y \leqq B$ by the argument in lemma 4.1.13. Hence we may assume that $Y \leqq B$ in both cases.

It now follows that both YC_3 and X^+ are complements of $C_1 C_5$ in YC, where X^+ is the subgroup of X of index 2. Therefore $X^+ \cong YC_3$, contrary to lemma 4.2.2. This proves our result.

4.2.4. Corollary. *If $p = q \geqq 5$ and $t \geqq 2$, then $s = 1$ and G/P_1 does not split over P/P_1.*

Proof. If $s > 1$, P/P_2 is abelian and G induces a group of automorphisms of P/P_2 isomorphic to Γ. If P/P_1 has a complement X/P_1 in G/P_1, X induces

https://doi.org/10.1017/S1446788700006182 Published online by Cambridge University Press

a group of automorphisms of P/P_2 isomorphic to Γ. By the lemma, neither case is possible.

4.2.5. PROPOSITION. *There is a subgroup $\bar{G}$ of a group* (1.2), (1.3) *or* (1.4) *which has the same type as* G.

PROOF. We consider the cases of lemma 4.2.1 in turn.

(a) Here $s = 1$ by lemma 4.2.4. If G is not a split group, we may take $\bar{G} = \Gamma_2(p^{t+1})$ or $\Gamma_2^+(p^{t+1})$ by lemma 4.2.2. If G is a split group, then $t = 1$ by lemma 4.2.4., and we may take $\bar{G}$ as a group (1.3).

In the remaining cases, G is a split group by lemma 4.2.1.

(b) The group $P_{s-1,s+t-1}(p)$ defined in § 1 has order p^{3t} and by lemma 4.1.10, its commutator subgroup is $P_{2s-1,s+t-1}(p)$, of index p^{3s}. Hence we may take $\bar{G}$ as one of the groups

$$(A_4;\, P_{s-1,s+t-1}(p)), \quad (S_4;\, P_{s-1,s+t-1}(p)).$$

(c) Here $p \equiv \pm 1 \pmod 5$. Hence we may take

$$\bar{G} = (A_5;\, P_{s-1,s+t-1}(p)).$$

(d) Here $s = t$ and $p \equiv 1, 2$ or $4 \pmod 7$, by lemma 4.2.1. Hence we may take $\bar{G}$ as the group (1.4).

4.3. *Uniqueness.* In this subsection, G, $\bar{G}$ denote groups which satisfy (A)—(C) and have the same type.

4.3.1. PROPOSITION. *If G is a split group, $\bar{G} \cong G$.*

PROOF. The proof is by induction on t ($\geqq 1$). We may assume that $G/P_{t-1} \cong \bar{G}/\bar{P}_{t-1}$. Choose x, u, v in G as in lemma 4.1.11. We first prove that there is an isomorphism $\alpha : G/P_{t-1} \to \bar{G}/\bar{P}_{t-1}$ such that

$$(xP_{t-1})^\alpha = \bar{x}\bar{P}_{t-1}, \quad (uP_{t-1})^\alpha = \bar{u}\bar{P}_{t-1}, \quad (vP_{t-1})^\alpha = \bar{v}\bar{P}_{t-1},$$

where $\bar{x}$, $\bar{u}$, $\bar{v}$ also satisfy (i)-(iii) in lemma 4.1.11.

Take any isomorphism $\beta : G/P_{t-1} \to \bar{G}/\bar{P}_{t-1}$. We may evidently choose $\tilde{x} \in (xP_{t-1})^\beta$, $\bar{u} \in (uP_{t-1})^\beta$, $\bar{v} \in (vP_{t-1})^\beta$ so that $\tilde{x}$, $\bar{u}$, $\bar{v}$ satisfy (i), (ii). These elements satisfy (iii) modulo $\bar{P}_{t-1}$. Hence, by the proof of lemma 4.1.11, there is a power $\bar{x} = \tilde{x}^\lambda$ such that $\bar{x}$, $\bar{u}$, $\bar{v}$ satisfy (i)-(iii), where $\lambda = 1$ if $s = t$, $(\lambda, p) = 1$ if $s = t-1$ and $\lambda \equiv 1 \pmod{p^{t-1-s}}$ if $s < t-1$. Since $[\bar{P}, \bar{P}_{t-1-s}] = \bar{P}_{t-1}$ by lemma 4.1.10, the mapping $z \to z^\lambda$ is a central automorphism of $\bar{P}/\bar{P}_{t-1}$. Since $\bar{G}$ splits over $\bar{P}$, this can be extended to an automorphism θ of $\bar{G}/\bar{P}_{t-1}$ which fixes $\bar{u}\bar{P}_{t-1}$ and $\bar{v}\bar{P}_{t-1}$. Then $\alpha = \beta\theta :$ $G/P_{t-1} \to \bar{G}/\bar{P}_{t-1}$ satisfies the required conditions.

Let S be the subgroup of $G \times \bar{G}$ formed by the elements (y, z) satisfying $(yP_{t-1})^\alpha = z\bar{P}_{t-1}$. If X, Y are the kernels of the projections

$$\varphi : S \to G,\ (y, z) \to y;\ \psi : S \to \tilde{G},\ (y, z) \to z,$$

and
$$Q_i = \varphi^{-1}(P_i) = \psi^{-1}(\bar{P}_i) \qquad (0 \leqq i \leqq t-1),$$

then
$$1 < X < Q_{t-1} < \cdots < Q_0 = Q$$
$$1 < Y < Q_{t-1} < \cdots < Q,$$

are S-composition series of Q with factors $\cong (C_p)^3$; moreover, $S/Q \cong \Gamma$ and the factors are isomorphic Γ-modules. We note also that Q has a complement K in S. For we may take $K = \mathcal{N}_S(\langle (u, \bar{u}), (v, \bar{v})\rangle)$ if $q = p = 3$, and in all other cases $(|Q|, |S : Q|) = 1$.

If $ks \geqq t > (k-1)s$, the descending central series of P, $\bar{P}$ are $P > P_s > \cdots > P_{(k-1)s} > 1$ and $\bar{P} > \bar{P}_s > \cdots > \bar{P}_{(k-1)s} > 1$ by lemma 4.1.10. Since Q is a subdirect product of P, $\bar{P}$, its descending central series has the form
$$Q = Q^{(0)} > Q^{(1)} > \cdots > Q^{(k-1)} > 1,$$
and

$$Q^{(i)}X = Q^{(i)}Y = Q_{is} \qquad (0 \leqq i \leqq k-1). \tag{1}$$

By the proof of lemma 4.1.7,
$$\mu_i : Q/Q_s \to Q_{(i-1)s}/Q_{is},\ zQ_s \to z^{p^{(i-1)s}}, \qquad (1 \leqq i \leqq k-1)$$
is a well defined S-epimorphism. By (1) and since $X \leqq \mathscr{Z}(Q)$, the natural commutator epimorphism
$$Q/Q^{(1)} \otimes Q^{(i-1)}/Q^{(i)} \to Q^{(i)}/Q^{(i+1)}$$
induces an S-epimorphism
$$\left.\begin{aligned} \gamma_i : (Q/Q_s) \otimes (Q_{(i-1)s}/Q_{is}) &\to Q^{(i)}/Q^{(i+1)} \\ yQ_s \otimes wQ_{is} &\to [y, w]Q^{(i+1)} \end{aligned}\right\} \qquad (1 \leqq i \leqq k-1).$$

The product
$$(1 \otimes \mu_i)\gamma_i : (Q/Q_s) \otimes (Q/Q_s) \to Q^{(i)}/Q^{(i+1)}$$
satisfies
$$\big((1 \otimes \mu_i)\gamma_i\big)(yQ_s \otimes yQ_s) = Q^{(i+1)}$$
and so induces an S-epimorphism of the exterior square
$$\left.\begin{aligned} \lambda_i : (Q/Q_s) \wedge (Q/Q_s) &\to Q^{(i)}/Q^{(i+1)} \\ (yQ_s) \wedge (zQ_s) &\to [y, z^{p^{(i-1)s}}]Q^{(i+1)} \end{aligned}\right\} \qquad (1 \leqq i \leqq k-1).$$

Now $M = (Q/Q_s) \wedge (Q/Q_s)$ is an indecomposable $\mathbf{Z}S$-module with unique composition series $M > pM > \cdots > p^s M = 0$. Therefore $Q^{(i)}/Q^{(i+1)} \cong M/p^{r_i}M$ $(1 \leqq i \leqq k-1)$, where $p^{r_i} \leqq p^s$ is the exponent of $Q^{(i)}/Q^{(i+1)}$. If $1 \leqq i \leqq k-2$, the group $Q_{is}/Q_{(i+1)s}$ of exponent p^s is a homomorphic image of $Q^{(i)}/Q^{(i+1)}$ and so $r_i = s$. If $i = k-1$, $Q^{(k-1)}$ has the same exponent as $Q^{(k-1)}X = Q_{(k-1)s}$, viz. $p^{t-(k-1)s}$, so that $r_{k-1} = t-(k-1)s$. Thus, $|Q'| = p^{3(t-s)}$ and $|Q : Q'| = p^{3(s+1)}$. In other words, Q' is a subgroup of Q_1 of index p^3.

Since $Q/Q_s \cong (C_{p^s})^3$ and since all S-composition factors of Q are isomorphic to $(C_p)^3$, $Q/Q' \cong (C_{p^{s+1}})^3$ or $(C_{p^s})^3 \times (C_p)^3$. Now by the choice of $x, \bar{x}, \cdots$, the elements $x^* = (x, \bar{x})$, $u^* = (u, \bar{u})$, $v^* = (v, \bar{v})$ satisfy (iii) in lemma 4.1.11. Thus $(x^*)^{p^s} \in Q'$. Since

$$Q/Q' = \langle x^*Q', (x^*)^{v^*}Q', (x^*)^{v^{*2}}Q', Q_1/Q' \rangle,$$

Q/Q' has exponent p^s. Therefore $Q/Q' \cong (C_{p^s})^3 \times (C_p)^3$.

Now the Γ-module $Q_1\Phi(Q)/\Phi(Q)$ is a direct summand of $Q/\Phi(Q)$:

$$Q/\Phi(Q) \cong (R/\Phi(Q)) \oplus (Q_1\Phi(Q)/\Phi(Q)).$$

(For either $(p, |\Gamma|) \neq 1$ or $p = q = 3$ and $Q_1\Phi(Q)/\Phi(Q)$ is the injective module [3].) This implies that $R \lhd S$ and $Q/Q' = (R/Q') \times (Q_1/Q')$. Since $Q_1 = Q'X = Q'Y$, R is a common complement of X, Y in Q. Therefore KR is a common complement of X, Y in S. This gives

$$G \cong S/X \cong KR \cong S/Y \cong \bar{G},$$

as required.

For the remaining proofs, we need some information about the cohomology of $\mathscr{G} = \Gamma_2(p)$ or $\Gamma_2^+(p)$ over $\boldsymbol{F}_p$. We assume that $p > 3$. The symbol

$$\begin{bmatrix} a, & b, & \cdots \\ u, & v, & \cdots \\ \cdot & \cdot & \cdots \end{bmatrix}$$

will denote a $\mathscr{G}$-module N with successive Frattini factors

$$N/\Phi(N) \cong [a] \oplus [b] \oplus \cdots,$$
$$\Phi(N)/\Phi(\Phi(N)) \cong [u] \oplus [v] \oplus \cdots, \cdots.$$

Let $[1]'$, $[3]'$, $\cdots$, $[p]'$ denote the principal indecomposable modules corresponding to the irreducible modules $[1], \cdots, [p]$. $[k]'$ is self-contragredient and has a unique maximal submodule M_k, which satisfies $[k]'/M_k \cong [k]$. Using these facts and the known values of the Cartan invariants of $\mathscr{G}$ (cf. Brauer and Nesbitt [1]), we find easily that

$$[1]' = \begin{bmatrix} 1 \\ p-2 \\ 1 \end{bmatrix}, \quad [p]' = [p], \quad [k]' = \begin{bmatrix} k \\ p-k-1, p-k+1 \\ k \end{bmatrix} \quad (1 < k < p).$$

There is a very simple projective resolution

$$\cdots \xrightarrow{\partial_3} \Pi_2 \xrightarrow{\partial_2} \Pi_1 \xrightarrow{\partial_1} [1] \to 0,$$

viz.

$$\cdots \to \begin{bmatrix} 3 \\ p-2, p-4 \\ 3 \end{bmatrix} \to \begin{bmatrix} p-2 \\ 1, \;\; 3 \\ p-2 \end{bmatrix} \to \begin{bmatrix} 1 \\ p-2 \\ 1 \end{bmatrix} \to [1] \to 0.$$

https://doi.org/10.1017/S1446788700006182 Published online by Cambridge University Press

The successive kernels $K_i = \ker \partial_i$ are given by

$$\cdots \begin{bmatrix} p-4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ p-2 \end{bmatrix}, \begin{bmatrix} p-2 \\ 1 \end{bmatrix}.$$

Let L, N be modules and $Q \to \Pi \to L$ a projective presentation of L. By definition,

$$\text{Ext}\,(L, N) \cong \text{Hom}\,(Q, N)/J,$$

where J is formed by the elements of $\text{Hom}(Q, N)$ which extend to elements of $\text{Hom}(\Pi, N)$. The cohomology groups $H^i(N) = H^i(\mathscr{G}, N)$ are given by

$$H^i(N) \cong \text{Ext}\,(K_{i-1}, N).$$

In view of the presentations

$$M_k \to [k]' \to [k], K_i \to \Pi_i \to K_{i-1},$$

and since M_k is the unique maximal submodule of $[k]'$, we have

(1) $$\text{Ext}\,([k], [m]) \cong \text{Hom}\,(M_k, [m]),$$

(2) $$H^i([k]) \cong \text{Hom}\,(K_i, [k]).$$

4.3.2. PROPOSITION. *If G is not a split group and $p \neq 5$, then $\bar{G} \cong G$.*

PROOF. We use the same method as in proposition 4.3.1. The proof is by induction on $t (\geqq 1)$. We may assume $G/P_{t-1} \cong \bar{G}/\bar{P}_{t-1}$ (using corollary 4.2.4.). Choose *any* isomorphism $\alpha : G/P_{t-1} \to \bar{G}/\bar{P}_{t-1}$, and form S as before. Then $|Q : Q_1| = |Q_1 : Q'| = p^3$ and $Q/Q' \cong (C_{p^2})^3$ or $(C_p)^6$. Now Q/Q' is a $\mathbf{Z}\Gamma$-module so that the first case is excluded by lemma 4.2.3.

It follows that Q/Q' is an $\mathbf{F}_p\Gamma$-module with composition factors $[3]$, $[3]$. Now the extension S/Q' of Q/Q' by Γ is determined by a certain element of $H^2(Q/Q')$, i.e. (cf. (2)) by a certain homomorphism $K_2 \xrightarrow{\alpha} Q/Q$. Moreover, if $Q/Q' \xrightarrow{\beta} Q/Q_1$ is the canonical epimorphism, the extension S/Q_1 of Q/Q_1 by Γ is determined by the homomorphism $K_2 \xrightarrow{\alpha\beta} Q/Q_1$. By lemma 4.2.4, $\alpha\beta \neq 0$. Since $K_2 \cong \begin{bmatrix} 3 \\ p-2 \end{bmatrix}$ and $p \neq 5$, we have

(3) $$Q/Q' \cong (\text{im}\,\alpha) \oplus (\ker \beta) \text{ (as } \Gamma\text{-modules)},$$

where, of course, $\ker \beta = Q_1/Q'$. Let $\text{im}\,\alpha = R/Q'$. The extension S/R of Q/R by Γ is determined by the homomorphism $K_2 \xrightarrow{\alpha\gamma} Q/R$, where $Q/Q' \xrightarrow{\gamma} Q/R$ is the projection corresponding to (3). Evidently, $\alpha\gamma = 0$ so that Q/R has a complement L/R in S/R. Then L is a common complement of X, Y in S and so $\bar{G} \cong G$ as before.

The remaining case $p = 5$ requires a different argument.

4.3.3. LEMMA. *Let* $G = \Gamma_2(p^{t+1})$ *or* $\Gamma_2^+(p^{t+1})$ $(t \geqq 2)$. *If*[8] $p \neq 3$ *or* 7, *the group of outer automorphism classes of* P *has a single conjugacy class of subgroups* $\cong \Gamma$.

PROOF. Let A be the group of automorphisms of P. Let J, C, B denote the subgroups of inner automorphisms, central automorphisms and automorphisms induced by elements of G. Then $B \cong \Gamma_2(p^t)$ and B is an extension of J by $\Gamma_2(p)$. Choose x_1, x_2, x_3 as in the proof of lemma 4.2.3. An element θ of C has the form

$$x_i^\theta = x_i \prod_1^3 x_j^{\theta_{ij} p^{t-1}} \qquad (i = 1, 2, 3),$$

and we may define C_1, C_2, C_3 as before. An element α of A has the property that

$$(x_i P_1)^\alpha = \prod_1^3 (x_j P_1)^{\alpha_{ij}} \qquad (i = 1, 2, 3),$$

where $(\alpha_{ij})'(\alpha_{ij}) = I$, $|\alpha_{ij}| = 1$. Therefore C is a $\Gamma_2(p)$-module with the C_i as irreducible components. It may be proved that $B \cap C = C_3$, $BC = A$.

It follows that $B/J\,(\cong \Gamma_2(p))$ is a complement of $CJ/J\,(\cong C_1 C_5)$ in the group of outer automorphism classes A/J. The lemma now follows from the fact that

$$H^1([1] \oplus [5]) \cong \mathrm{Hom}\left(\begin{bmatrix} p-2 \\ 1 \end{bmatrix}, [1] \oplus [5]\right) = 0 \qquad (p \neq 3, 7).$$

4.3.4. LEMMA. *Let* $G = \Gamma_2(p^{t+1})$ *or* $\Gamma_2^+(p^{t+1})$ $(t \geqq 2)$. *Let* $\tilde{G}$ *be an extension of* P *by* Γ *such that* $\mathscr{Z}(\tilde{G}) = 1$. *If*[9] $p \neq 3$ *or* 7, $\tilde{G} \cong G$.

PROOF. We may regard $\tilde{G}$, G as groups of pairs $(x, u)(x \in \Gamma, u \in P)$ with multiplications

$$(x, u)(y, v) = (xy, \tilde{c}(x, y)u^{\tilde{\tau}(y)}v) \text{ in } \tilde{G},$$
$$(x, u)(y, v) = (xy, c(x, y)u^{\tau(y)}v) \text{ in } G,$$

where $\tilde{\tau}$, τ are homomorphisms $\Gamma \to A/J$. Since $\tilde{G}$, G have trivial centres, $\tilde{\tau}$, τ are monomorphisms. Hence, by lemma 4.3.3, we may suppose $\tilde{\tau} = \tau$. Then $\tilde{c}(x, y) = c(x, y)d(x, y)$ where $d(x, y) \in \mathscr{Z}(P) = P_{t-1}$.

Now $c(x, y)P_1$, $d(x, y)$ are 2-cocycles for the Γ-modules P/P_1, P_{t-1}. By lemma 4.2.2, the former is not a coboundary. Since

$$H^1([3]) \cong \mathrm{Hom}\left(\begin{bmatrix} 3 \\ p-2 \end{bmatrix}, [3]\right) \cong C_p,$$

[8] The lemma is in fact true for $p = 3$ but false for $p = 7$.

[9] The lemma is in fact true for both $p = 3$ and $p = 7$. The proof in the latter case is somewhat complicated because one has to prove that a certain 3-cocycle is not a coboundary.

https://doi.org/10.1017/S1446788700006182 Published online by Cambridge University Press

we may suppose that $\tilde{d}(x, y) = c(x, y)^{\lambda p^{t-1}}$ for some integer λ. Thus $\tilde{c}(x, y) = c(x, y)^{\omega}$, where ω is the automorphism $u \to u^{1+\lambda p^{t-1}}$ of P. Since $\omega \in \mathscr{Z}(A)$, the mapping $(x, y) \to (x, y^{\omega})$, $G \to \tilde{G}$, is an isomorphism. This proves the lemma.

4.3.5. COROLLARY. *If G is not a split group and $p = 5$, $\bar{G} \cong G$.*

PROOF. Choosing $H < G, \bar{H} < \bar{G}$ so that $H/P \cong \bar{H}/\bar{P} \cong A_4$ and applying lemma 4.3.1 to H, $\bar{H}$, we deduce that $\bar{P} \cong P$. Thus G, $\bar{G}$ are both extensions of P by Γ and so, by the lemma, $\bar{G} \cong G$.

This corollary and Propositions 4.3.1 and 4.3.2 show that $\bar{G} \cong G$ in all cases. Thus, the final step in the proof of Theorem 3 is complete.

References

[1] R. Brauer and C. Nesbitt, 'On the modular characters of groups', *Ann. Math.* 42 (1941), 556—590.

[2] R. Brauer, M. Suzuki and G. E. Wall, 'A characterization of the one-dimensional unimodular projective groups over finite fields,' *Ill. J. Math.* 2 (1958), 718—745.

[3] D. Gorenstein and J. Walter, 'On finite groups with dihedral Sylow 2-subgroups', *Ill. J. Math.* 6 (1962), 553—593.

[4] L. G. Kovács and G. E. Wall, 'Involutory automorphisms of groups of odd order and their fixed-point groups', *Nagoya Math. J.* 27 (1966), 113—119.

[5] J. Schur, 'Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen', *J. für Math.* 132 (1907), 85—137.

[6] M. Suzuki, On characterizations of linear groups, I, *Trans. Amer. Math. Soc.* 92 (1959), 191—204.

[7] J. N. Ward, 'Involutory automorphisms of groups of odd order', *J. Austral. Math. Soc.* 6 (1966), 480—494.

University of Sydney
and
University of Warwick