THE SUBGROUPS OF PSL(3, q) FOR ODD q[1]

BY
DAVID M. BLOOM

1. **Introduction.** Let SL(n, q) denote the group of n by n matrices of determinant 1 over the field GF(q) of q elements; let PSL(n, q) be equal to SL(n, q) modulo its center. The subgroups of PSL(2, q) were determined by Dickson [12]. Those of PSL(3, q) were determined for odd q by Mitchell [19], using geometric methods. (The results for even q are given by Hartley [18].)

In this paper we show that more modern group-theoretic methods can be used for a new determination of the subgroups of PSL(3, q), at least when q is odd. (For a result relevant to of the case of even q, see Suzuki [28].) Our major result is

THEOREM 1.1. *Let $q=p^\alpha$ be a power of an odd prime p, and let $\mathfrak{G}$ be a subgroup of* PSL(3, q) *of order >1. Assume $\mathfrak{G}$ has no normal elementary-abelian subgroup of order >1. Then $\mathfrak{G}$ is isomorphic to one of the following*:

(1) PSL(3, p^β); $\beta|\alpha$.

(2) PU(3, p^β); $2\beta|\alpha$.

(3) *in the case where* $3 \mid (p^\beta-1)$ *and* $3\beta|\alpha$, *a group containing the subgroup of type* (1) *with index* 3.

(4) *in the case where* $3 \mid (p^\beta+1)$ *and* $6\beta|\alpha$, *a group containing the subgroup of type* (2) *with index* 3.

(5) PSL(2, p^β) *or* PGL(2, p^β), *with* $\beta|\alpha$ *and* $p^\beta \neq 3$.

(6) PSL(2, 5), *with* $q \equiv \pm 1 \pmod{10}$.

(7) PSL(2, 7), *with* $q^3 \equiv 1 \pmod 7$.

(8) A_6, A_7, *or a group containing* A_6 *with index* 2, *with* $p=5$ *and* α *even.*

(9) A_6, *with* $q \equiv 1$ *or* $19 \pmod{30}$.

Moreover, PSL(3, q) *has exactly one subgroup $\mathfrak{G}$ of each type mentioned (for each indicated value of q, β), up to conjugacy in* GL(3, q)/Z(SL(3, q)).

Here GL(n, q) denotes the group of nonsingular matrices of degree n over the field GF(q); $U(n, q)$ is the subgroup of SL(n, q^2), and $U^*(n, q)$ the subgroup of GL(n, q^2), consisting of matrices A such that A^{-1} is the transpose of the matrix obtained from A via the automorphism $c \to c^q$ of GF(q^2). For any group $\mathfrak{G}$, P$\mathfrak{G}$ denotes $\mathfrak{G}/Z(\mathfrak{G})$ where $Z(\mathfrak{G})$ is the center of $\mathfrak{G}$. A_n, S_n denote the alternating and symmetric groups on n letters.

We will give explicit representatives (in matrix form) of all conjugacy classes

Received by the editors November 8, 1965.

(1) This paper is based on research partially completed under a National Science Foundation Graduate Fellowship.

of subgroups satisfying the hypothesis of Theorem 1.1. (Actually, the inverse images in SL(3, q) of these subgroups will be given; see Theorem 5.14 and the lemmas of §6.) In §7 we classify the subgroups of PSL(3, q) not satisfying this hypothesis.

Our treatment uses results of Brauer, et al. by which information about a group $\mathfrak{G}$ of even order may be obtained from information about the centralizer $C(X)$ of an element X of order 2 in $\mathfrak{G}$; see [3], [6], [7], [15] (particularly [3, equation (8)], which gives information about the order of $\mathfrak{G}$ and will be referred to as Brauer's Formula). If $\mathfrak{G} \subseteq \mathrm{PSL}(3, q)$ then $C(X)$ is isomorphic to a subgroup of GL(2, q), or of GL(2, q) modulo a scalar subgroup of order 3. Accordingly, we first determine (§3) the possible types of subgroups of GL(2, q), and then, by considering each of these types in turn, determine (§5) the possible *simple* subgroups of PSL(3, q) up to isomorphism (these are all of even order, by [14]). In §6 we find the conjugacy classes of these subgroups, and also their normalizers. Since any finite group of order > 1 has a nontrivial normal subgroup which is the direct product of isomorphic simple groups, we can then obtain enough information about arbitrary subgroups of PSL(3, q) to prove Theorem 1.1.

The author wishes to express gratitude to Professor R. Brauer for his invaluable guidance, and thanks to Professors M. Suzuki and D. G. Higman for calling attention to items in the literature. In addition, the referee has made some helpful suggestions for improving the paper.

2. **Notations and terminology.** Some of the notation used in this paper is not standard. We here list all of the notations and terminology about which any explanation is needed.

The notations GL(n, k), SL(n, k), $U(n, k)$, $U^*(n, k)$, and $\mathrm{P}\mathfrak{G}$ were defined above. $(\mathrm{GF}(k))^*$ is the multiplicative group of nonzero elements in the field GF(k).

If $\mathfrak{G}$ is any finite group, $|\mathfrak{G}|$ is the order of $\mathfrak{G}$. $|\mathfrak{G} : \mathfrak{H}|$ is the index in $\mathfrak{G}$ of (a subgroup) $\mathfrak{H}$. Aut($\mathfrak{G}$) is the group of automorphisms of $\mathfrak{G}$. For any subset $\mathfrak{S}$ of $\mathfrak{G}$, $\{\mathfrak{S}\}$ is the subgroup generated by $\mathfrak{S}$.

For $X \in \mathfrak{G}$, $|X|$ is the order of X. If $|X| = 2$, X is called an *involution*. A group or element, whose order is relatively prime to the positive integer r, is called *r-regular*. C_r denotes a cyclic group of order r.

"Characters" are always complex characters unless indicated otherwise.

It will be important to distinguish between SL(3, q) and PSL(3, q). The natural homomorphism of SL(3, q) onto PSL(3, q) will be denoted Δ, and the kernel of Δ will be denoted $\mathfrak{Z}$; then $|\mathfrak{Z}| = 1$ or 3 according to whether $q \not\equiv 1$ or $q \equiv 1 \pmod 3$.

A *diagonal* matrix is one having zeroes everywhere except on the main diagonal. A diagonal matrix with diagonal entries $a_1, \ldots, a_n$ will be written $\|a_1, \ldots, a_n\|$. A scalar matrix is one of the form $\|a, a, \ldots, a\| = aI$ (where I denotes the identity matrix). An *anti-diagonal* matrix is an n by n matrix whose entries a_{ij} are zero except when $i+j = n+1$; such a matrix will be written $[a_{1n}, \ldots, a_{n1}]$, displaying

the diagonal entries reading from top right to bottom left. (This type will occur mostly for $n=2$.)

In much of the paper, $\mathfrak{G}$ denotes a (variable) subgroup of some fixed linear group $\boldsymbol{L}$. If $\mathfrak{Q}$ is in turn a subgroup of $\mathfrak{G}$, $N(\mathfrak{Q})$ and $C(\mathfrak{Q})$ will denote the normalizer and centralizer of $\mathfrak{Q}$ in $\mathfrak{G}$, whereas $\boldsymbol{N}(\mathfrak{Q})$, $\boldsymbol{C}(\mathfrak{Q})$ are the normalizer and centralizer of $\mathfrak{Q}$ in the larger group $\boldsymbol{L}$. Similar conventions apply to centralizers of elements of $\mathfrak{G}$.

If $G \in \mathfrak{G}$ is fixed, the inner automorphism $X \to X' = GXG^{-1}$ is called *conjugation by* G, and we say that G maps X into X'; this is also written $G\colon X \to X'$, or $X' = X^G$. G *fixes* X if $G\colon X \to X$; G *inverts* X if $G\colon X \to X^{-1}$. Two elements conjugate in $\mathfrak{G}$ will be called $\mathfrak{G}$-conjugate.

Multiplication in the symmetric group $\boldsymbol{S}_r$ will be taken as *left* composition; e.g., $(123)(234) = (12)(34)$, not $(13)(24)$.

"R.A.A." (reductio ad absurdum) means "contradiction." We fail to understand why this abbreviation is so rarely used in mathematical writing, in contrast to the wide use of "Q.E.D."

A direct product of cyclic groups of orders $r_1, \ldots, r_n$ is called abelian of type $(r_1, \ldots, r_n)$, *elementary-abelian* if all r_i are equal to the same fixed prime. A group $\mathfrak{P}$ generated by two elements A, B is *dihedral*, *semidihedral*, or *generalized quaternion* if it has generating relations of (respectively) the form (a), (b), (c) as follows:

(a) $A^{2k} = B^2 = 1$; $BAB^{-1} = A^{-1}$, $\quad (k \geqq 1)$

(b) $A^{2^{m+1}} = B^2 = 1$; $BAB^{-1} = A^{2^m - 1}$, $\quad (m > 1)$

(c) $A^{2r} = B^4 = 1$; $B^2 = A^r$; $BAB^{-1} = A^{-1}$, $\quad (r > 1)$.

Note that the four-group is included in (a) (case $k=1$). If $r=2$ in (c) we have the (ordinary) quaternion group.

Finally, *the following notation will be fixed throughout this paper*: (p is a fixed odd prime and $q = p^\alpha$ is a fixed power of p). Only if the notation (p, q, α) is kept in mind will statements be comprehensible.

3. **The subgroups of** PSL(2, q), SL(2, q), **and** GL(2, q). In this section we find the subgroups of GL(2, q) (Theorem 3.4). These subgroups are not difficult to obtain once those of PSL(2, q) are known, and the latter are given by Dickson [12]. Dickson's results can be summarized as follows:

THEOREM 3.1. *Let* $\mathfrak{G}$ *be a subgroup of* PSL(2, q). *Then one of the following occurs*:

(a) $\mathfrak{G}$ *is isomorphic to* (i) $\boldsymbol{A}_5$ *with* $p \neq 5$, *or* (ii) $\boldsymbol{S}_4$ *or* $\boldsymbol{A}_4$.

(b) $\mathfrak{G}$ *is cyclic and p-regular.*

(c) $\mathfrak{G}$ *is dihedral and p-regular.*

(d) $\mathfrak{G} = \{\mathfrak{Q}, X\}$ *where* $\mathfrak{Q} \neq \{1\}$ *is a p-group and* $X \in N(\mathfrak{Q})$ *is a p-regular element.*

(e) $\mathfrak{G}$ *is conjugate in* GL(2, q)/$\{-I\}$ *to* PSL(2, p^β), $\beta | \alpha$, $p^\beta > 3$.

(f) $q \equiv 1 \pmod 4$; *up to conjugacy in* GL(2, q)/$\{-I\}$, $\mathfrak{G}$ *contains*

$$\mathfrak{R} = \mathrm{PSL}(2, p^\beta)$$

as a subgroup of index 2 ($2\beta|\alpha$, $p^\beta > 3$), *and is generated by* $\mathfrak{R}$ *and the diagonal matrix* $\|c, c^{-1}\|$ *where* c^2 *generates* $(\mathrm{GF}(p^\beta))^*$.

Parts of the proof of Theorem 3.1 can be simplified by the use of more modern methods, in particular by using the Brauer-Suzuki-Wall characterization of PSL(2, q) [11]; details of such a proof can be found in [1].

THEOREM 3.2. *Let* $\mathfrak{G}$ *be a subgroup of* SL(2, q). *Then one of the following occurs*:

(a) $\mathfrak{G}/\{-I\}$ *is isomorphic to* A_5 *with* $p \neq 5$, *or to* A_4 *or* S_4.

(b) $\mathfrak{G}$ *is cyclic and p-regular.*

(c) $\mathfrak{G}$ *is generalized quaternion and p-regular.*

(d) $\mathfrak{G} = \{\mathfrak{Q}, X\}$ *where* $\mathfrak{Q} \neq \{1\}$ *is a p-group and* $X \in N(\mathfrak{Q})$ *is p-regular.*

(e) $\mathfrak{G}$ *is conjugate in* GL(2, q) *to* SL(2, p^β), $\beta|\alpha$, $p^\beta > 3$.

(f) $q \equiv 1 \pmod 4$; *up to conjugacy in* GL(2, q), $\mathfrak{G}$ *contains* $\mathfrak{H} = \mathrm{SL}(2, p^\beta)$ *as a subgroup of index* 2 ($2\beta|\alpha$, $p^\beta > 3$) *and is generated by* $\mathfrak{H}$ *and the matrix* $\|c, c^{-1}\|$ *where* c^2 *generates* $(\mathrm{GF}(p^\beta))^*$.

Proof. Observing that the scalar matrix $-I$ is the only involution in SL(2, q), it follows easily that, if $|\mathfrak{G}|$ is even, then $\mathfrak{G}$ is the inverse image of a subgroup of PSL(2, q) under the natural homomorphism of SL(2, q) onto PSL(2, q). The theorem then follows easily from Theorem 3.1.

LEMMA 3.3. *Let* $\mathfrak{H}$ *be a subgroup of* GL(2, q) *containing* $-I$. *If* $\mathfrak{H}/\{-I\}$ *is isomorphic to* A_4, *then the* 2*-Sylow group* $\mathfrak{P}$ *of* $\mathfrak{H}$ *is the quaternion group. If* $\mathfrak{H}/\{-I\}$ *is isomorphic to* S_5, *then* $p = 5$.

Proof. Assume $\mathfrak{H}/\{-I\} \cong A_4$. $\mathfrak{P}$ is not elementary-abelian (since $\mathfrak{H} \subseteq \mathrm{GL}(2, q)$) and hence $\mathfrak{P}$ has an element P of order 4. Since A_4 has no element of order 4, $P^2 = -I$. Since all involutions of A_4 are conjugate, all elements of $\mathfrak{P}$ different from $\pm I$ are conjugate to $\pm P$ and hence have order 4, whence $\mathfrak{P}$ is the quaternion group. If instead $\mathfrak{H}/\{-I\} \cong S_5$ then an element of $\mathfrak{H}$ of order 5 is conjugate to four of its powers, which is possible in GL(2, q) only if $p = 5$.

THEOREM 3.4. *Let* $\mathfrak{G}$ *be a subgroup of* GL(2, q). *Then, up to conjugacy in* GL(2, q), *one of the following occurs*:

(1) $\mathfrak{G}$ *is cyclic.*

(2) $\mathfrak{G} = \mathfrak{Q}\mathfrak{M}$ *where* $\mathfrak{Q}$ *is a subgroup of the p-group*

$$\left\{ \left\| \begin{matrix} 1 & 0 \\ \tau & 1 \end{matrix} \right\| : \tau \in \mathrm{GF}(q) \right\} \tag{3.1}$$

and $\mathfrak{M} \subseteq N(\mathfrak{Q})$ *is a subgroup of the group* $\mathfrak{D}$ *of all diagonal matrices.*

(3) $\mathfrak{G} = \{C_u, S\}$ *where* $u|q^2 - 1$, S: $Y \to Y^q$ *for all* $Y \in C_u$, *and* S^2 *is a scalar* 2*-element in* C_u.

(4) $\mathfrak{G} = \{\mathfrak{M}, S\}$ *where* $\mathfrak{M} \subseteq \mathfrak{D}$ *and* S *is an anti-diagonal* 2*-element*; $|\mathfrak{G} : \mathfrak{M}| = 2$.

(5) $\mathfrak{G}=\{\mathrm{SL}(2,p^\beta), V\}$ ("*Case* 1") *or* $\mathfrak{G}=\{\mathrm{SL}(2,p^\beta), V, \|b, \varepsilon b\|\}$ ("*Case* 2") *where* V *is a scalar matrix,* ε *generates* $(\mathrm{GF}(p^\beta))^*$, $p^\beta>3$, $\beta|\alpha$. *In Case* 2,

$$|\mathfrak{G}\colon \{\mathrm{SL}(2,p^\beta), V\}| = 2.$$

(6) $\mathfrak{G}/\{-I\}$ *is isomorphic to* $\boldsymbol{S}_4\times C_u$, $\boldsymbol{A}_4\times C_u$, *or* (*with* $p\neq 5$) $\boldsymbol{A}_5\times C_u$, *where* C_u *is a scalar subgroup of* $\mathrm{GL}(2,q)/\{-I\}$.

(7) $\mathfrak{G}$ *is not of type* (6), *but* $\mathfrak{G}/\{-I\}$ *contains* $\boldsymbol{A}_4\times C_u$ *as a subgroup of index* 2 *and* $\boldsymbol{A}_4$ *as a subgroup with cyclic quotient group;* C_u *is as in type* (6) *with* u *even.*

Proof. Let $\mathfrak{H}=\mathfrak{G}\cap \mathrm{SL}(2,q)$; then $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$ and $\mathfrak{G}/\mathfrak{H}$ is cyclic of order dividing $q-1$. $\mathfrak{H}$ is one of the types (a)–(f) of Theorem 3.2; we consider each type in turn.

(a) If $\mathfrak{H}/\{-I\}\cong \boldsymbol{S}_4$, then $\mathfrak{G}/\{-I\}\cong \boldsymbol{S}_4\times C_u$ by [17, Theorem 6.4.1], where $C_u\cong \mathfrak{G}/\mathfrak{H}$ is cyclic of order u dividing $q-1$. The inverse image of C_u in $\mathfrak{G}$ must be a scalar subgroup, since in $\mathrm{GL}(2,q)$ the centralizer of any nonscalar p-regular element is abelian. Thus $\mathfrak{G}$ is of type (6) above.

Similarly, suppose $\mathfrak{H}/\{-I\}\cong \boldsymbol{A}_r$ with $r=4$ or 5 (and $p\neq 5$ if $r=5$). The inner automorphisms of $\mathfrak{G}^*=\mathfrak{G}/\{-I\}$ yield automorphisms of $\mathfrak{H}^*=\mathfrak{H}/\{-I\}$ and this gives us a homomorphism

$$f\colon \mathfrak{G}^*\to \boldsymbol{S}_r = \mathrm{Aut}(\boldsymbol{A}_r)$$

under which $\mathfrak{H}^*\to \boldsymbol{A}_r$. The inverse image $\mathfrak{L}^*=f^{-1}(\boldsymbol{A}_r)$ is thus a subgroup of $\mathfrak{G}^*$ of index $\leqq 2$. Then f maps $\mathfrak{L}^*$ onto $\boldsymbol{A}_r$ with kernel $\mathfrak{C}^*$, the centralizer of $\mathfrak{H}^*$ in $\mathfrak{L}^*$. Since $\mathfrak{C}^*\cap\mathfrak{H}^*=\{1\}$ and $|\mathfrak{L}^*|=|\mathfrak{H}^*|\cdot|\mathfrak{C}^*|$, we have $\mathfrak{L}^*=\mathfrak{H}^*\times\mathfrak{C}^*$. As before, the elements commuting with $\mathfrak{H}^*$ must be scalar. Now the only groups containing $\boldsymbol{A}_r$ with index 2 are $\boldsymbol{A}_r\times C_2$ and $\boldsymbol{S}_r$; since $\mathfrak{G}^*/\mathfrak{H}^*$ is cyclic, it follows that $\mathfrak{G}$ is of type (6) or (7) of Theorem 3.4. Indeed, in the case $r=5$, the reasoning used in Lemma 3.3 shows that $f(\mathfrak{G}^*)$ cannot be $\boldsymbol{S}_5$, so that $\mathfrak{G}^*=\mathfrak{L}^*$ and we have type (6) rather than type (7). If u were odd in type (7), we would actually have type (6).

(b) If $\mathfrak{H}$ is a scalar subgroup, then $\mathfrak{G}$ is abelian, since $\mathfrak{H}\subseteq \boldsymbol{Z}(\mathfrak{G})$ and $\mathfrak{G}/\mathfrak{H}$ is cyclic. In this case $\mathfrak{G}$ is of type (2) with $\mathfrak{Q}=\{1\}$, or of type (1).

If $\mathfrak{H}$ is cyclic, p-regular, and nonscalar, then $C(\mathfrak{H})$ is a subgroup of C_r ($r=q^2-1$) or of $\mathfrak{D}$ (modulo a conjugation), and

$$|\mathfrak{G}\,:\,C(\mathfrak{H})| = |N(\mathfrak{H})\,:\,C(\mathfrak{H})| \leqq 2.$$

If $\mathfrak{G}=C(\mathfrak{H})$, $\mathfrak{G}$ is of type (1) or type (2) with $\mathfrak{Q}=\{1\}$. Otherwise, choosing $S\in N(\mathfrak{H})$, $S\notin C(\mathfrak{H})$, we may assume (replacing S by an odd power of S if necessary) that S is a 2-element. If $C(\mathfrak{H})\subseteq\mathfrak{D}$, S is anti-diagonal and hence S^2 is scalar; $\mathfrak{G}$ is of type (4). If instead $C(\mathfrak{H})=C_u$, $u\mid q^2-1$, we may assume $u\nmid q-1$; a conjugation over $\mathrm{GF}(q^2)$ maps the generator of C_u into a matrix of the form $\|a, a^q\|$ and hence S into an antidiagonal matrix, so that again S^2 is scalar; $\mathfrak{G}$ is then of type (3).

(c) Let $\mathfrak{H}$ be of type (c) of Theorem 3.2. If $|\mathfrak{H}| > 8$ then $\mathfrak{H}$ has a unique cyclic subgroup $\{A\}$ of index 2. $\{A\}$ is then normal in $\mathfrak{G}$ and the analysis is like that of the preceding paragraphs. Suppose instead that $|\mathfrak{H}| = 8$. Let $\mathfrak{M}$ be the normalizer of $\mathfrak{H}$ in SL(2, q); then $\mathfrak{M}/\{-I\}$ is a group of automorphisms of $\mathfrak{H}$, i.e., a subgroup of S_4. Thus $\mathfrak{M}$ is a 2-group or else $\mathfrak{M}/\{-I\}$ is isomorphic to A_4 or S_4. In the latter case the argument of paragraphs (a) can be applied to $(\mathfrak{G}\mathfrak{M}, \mathfrak{M})$ instead of $(\mathfrak{G}, \mathfrak{H})$, so that $\mathfrak{G}\mathfrak{M}$ is of type (6) or (7). Moreover, in this case $\mathfrak{G} \cap \mathfrak{M} = \mathfrak{H}$ so that

$$|\mathfrak{G}\mathfrak{M} : \mathfrak{G}| = |\mathfrak{M} : \mathfrak{H}| = 3 \text{ or } 6.$$

Hence $\mathfrak{G} = \mathfrak{P}\mathfrak{Z}$ where $\mathfrak{P}$ is a 2-group and $\mathfrak{Z}$ is a scalar subgroup. On the other hand, if $\mathfrak{M}$ is a 2-group, let $\mathfrak{P}$ be a 2-Sylow group of $N(\mathfrak{H})$ containing $\mathfrak{M}$. Since $|N(\mathfrak{H}) : \mathfrak{M}|$ divides $q-1$, a cardinality argument shows that

$$N(\mathfrak{H}) = \mathfrak{P} \cdot Z(\mathrm{GL}(2, q)),$$

and $\mathfrak{G}$ is a subgroup of this. In either case, $\mathfrak{G}$ is of type (3) or (4) depending on whether $q \equiv \pm 1 \pmod 4$.

(d) Suppose $\mathfrak{H} = \{\mathfrak{Q}, \mathrm{X}\}$ as in Theorem 3.2(d). We may assume $\mathfrak{Q}$ is a subgroup of the group $\mathfrak{P}$ of (3.1). Evidently $\mathfrak{Q}$ is characteristic in $\mathfrak{H}$ and hence normal in $\mathfrak{G}$, so that $\mathfrak{G} \subseteq N(\mathfrak{Q}) \subseteq N(\mathfrak{P})$. By Hall's Theorem [17, Theorem 9.3.1], $\mathfrak{G}$ has a subgroup $\mathfrak{M}$ such that $\mathfrak{G} = \mathfrak{Q}\mathfrak{M}$ and $|\mathfrak{M}|$ divides $(q-1)^2$. Applying Hall's Theorem to $N(\mathfrak{P})$ instead of $\mathfrak{G}$, $\mathfrak{M}$ may be assumed to be a diagonal subgroup, so that $\mathfrak{G}$ is of type (2).

(e)(f) Finally, if $\mathfrak{H}$ satisfies Theorem 3.2(e) or (f), then SL(2, p^β) is a normal subgroup of $\mathfrak{G}$. Now every element of SL(2, p^β) of the same order as $S = \|\varepsilon, \varepsilon^{-1}\|$ (where ε generates $(\mathrm{GF}(p^\beta))^*$) is conjugate in SL(2, p^β) to a power of S. On the other hand, any conjugacy in GL(2, q) between powers of S takes place in SL(2, p^β). Hence, if $G \in \mathfrak{G}$, there is an element Y in SL(2, p^β) such that YG fixes S. Evidently YG maps the matrix (3.1) (with $\tau = 1$) into a matrix with coefficients in GF(p^β). Direct computation gives $YG = \|b, cb\|$ for some $b \in \mathrm{GF}(q)$, $c = \varepsilon^n \in \mathrm{GF}(p^\beta)$. If n is even then YG (hence also G) is congruent modulo SL(2, p^β) to a scalar matrix. It easily follows that $\mathfrak{G}$ is of type (5). This completes the proof of Theorem 3.4.

For the sake of completeness, we include the following result, which gives further precision to cases (6) and (7) of Theorem 3.4.

THEOREM 3.5. *In* GL(2, q),

(a) *There exist subgroups* $\mathfrak{G}$ *such that* $\mathfrak{G}/\{-I\} \cong A_4$, *for all values of* q.

(b) *There exist subgroups* $\mathfrak{G}$ *such that* $\mathfrak{G}/\{-I\} \cong S_4$, *if and only if* $q \not\equiv 5 \pmod 8$.

(c) *There exist subgroups* $\mathfrak{G}$ *as in Theorem* 3.4(7) *if and only if* $q \equiv 1 \pmod 4$.

(d) *There exist subgroups* $\mathfrak{G}$ *such that* $\mathfrak{G}/\{-I\} \cong A_5$ (*with* $p \neq 5$), *if and only if* $q \equiv \pm 1 \pmod{10}$.

Since Theorem 3.5 is not needed for our further work, we omit the proof, which consists of computations with matrices.

4. **Preliminary group-theoretical results.** We need two theorems about abstract groups. The first of these is the following theorem of Schur [20]:

LEMMA 4.1. *If a finite group $\mathfrak{G}$ has a faithful representation of degree n (over the complex numbers) whose character is rational-valued, then any prime p divides $|\mathfrak{G}|$ with exponent at most e_p, where*

$$e_p = \sum_{k=0}^{n} [n/(p^{k+1}-p^k)],$$

brackets denoting the greatest-integer function.

Our second theorem is the main result of this section. For convenience in stating it (and also for future reference), we shall say that a 2-group $\boldsymbol{P}$ is of "Type B" if it has generating relations of the following form:

$$\begin{aligned} &\boldsymbol{P} = \{S_1, S_2, T\};\ S_1^{2^n} = S_2^{2^n} = T^2 = 1 \qquad (n \geqq 2), \\ &S_1S_2 = S_2S_1;\ T\colon S_1 \to S_2;\ \{S_1\} \cap \{S_2\} = \{1\}. \end{aligned} \tag{4.1}$$

The 2-Sylow group of GL(2, q), $q \equiv 1 \pmod 4$, is of this type.

THEOREM 4.2. *Let $\boldsymbol{P}$ be of Type* B, *with the generating relations* (4.1). *Let $\mathfrak{P}$ be a nonabelian subgroup of $\boldsymbol{P}$, such that $\mathfrak{P}$ has no cyclic subgroup of index* 2. *Let $\mathfrak{Q} = \mathfrak{P} \cap \{S_1, S_2\}$.*

Then, for suitable elements A, B, S, R, we have

$$\begin{aligned} &\mathfrak{P} = \{\mathfrak{Q}, R\}, \\ &\mathfrak{Q} = \{A, B\};\ \{A\} = \boldsymbol{Z}(\mathfrak{P});\ R \in N(\mathfrak{Q}),\ R^2 \in \mathfrak{Q}, \\ &\{A\} \cap \{B\} = \{S\};\ |B| \geqq |A| > |S|. \end{aligned} \tag{4.2}$$

Moreover, let $\mathfrak{G}$ be a group having $\mathfrak{P}$ as its 2-Sylow subgroup, and assume $\mathfrak{P}$ is not itself of Type B. *Then $S \neq 1$ and the unique involution X in $\{S\}$ is not $\mathfrak{G}$-conjugate to any other element of $\mathfrak{P}$. If, in addition, we assume that*

$$C(X) = C(A) \text{ in } \mathfrak{G}; \tag{4.3}$$

any two elements of $\mathfrak{Q}$ conjugate in $C(X)$ are conjugate in $\mathfrak{P}$, (4.4)

then $\mathfrak{G}$ has a normal subgroup of index 2.

Proof. Clearly $\mathfrak{P} = \{\mathfrak{Q}, R\}$ where $R \notin \{S_1, S_2\}$, $R \in N(\mathfrak{Q})$, $R^2 \in \mathfrak{Q}$. The elements of $\mathfrak{Q}$ which commute with R are precisely those powers of $J = S_1S_2$ which lie in $\mathfrak{P}$, and hence $\boldsymbol{Z}(\mathfrak{P}) = (\mathfrak{P}) \cap \{J\}$ is a cyclic subgroup $\{A\}$. Since $\mathfrak{Q}/\{A\}$ is isomorphic to a subgroup of $\{S_1, S_2\}/\{J\}$ and is thus cyclic, we have $\mathfrak{Q} = \{A, B\}$ for some element B. Replacing B by BA if necessary, we may assume $|B| \geqq |A|$. Let S be a generator of $\{A\} \cap \{B\}$; then $|A| > |S|$ since otherwise $\mathfrak{Q}$ is cyclic, contrary to assumption. Thus the Relations (4.2) are all valid.

We may write $R=ET$ where $E\in\{S_1, S_2\}$ and T is as in (4.1). A computation shows that $BRBR^{-1}$ and R^2 lie in $\{J\}$, and hence in $\{A\}$, so that

$$RBR^{-1} = B^{-1}A^m \quad (\text{some } m); \qquad R^2\in\{A\}. \tag{4.5}$$

We now assume $\mathfrak{P}$ is *not of Type* B. If $|B|=|A|$ and $|S|=1$, then R commutes with no power of B except 1 (since $C(R)\cap\{B\}=\{S\}$), so that m must be odd in (4.5). Hence $R^2=A^{-rm}$ for some r. Since then $|B^rR|=2$, $\{B\}\cap\{B^{-1}A^m\}=\{1\}$, and $\mathfrak{Q}=\{B, B^{-1}A^m\}$, (4.5) implies that $\mathfrak{P}$ is of Type B, R.A.A.

Hence either $|B|>|A|$ or $S\neq 1$; in either case, letting X be the involution in $\{B\}$, X is the unique involution which is a power of an element of $\mathfrak{Q}$ of maximal order. Hence *any automorphism of* $\mathfrak{Q}$ *leaves* X *fixed*; in particular, R fixes X and thus $X\in\{A\}$, showing that $X\in\{S\}$ and hence $S\neq 1$. We now let $\mathfrak{G}$ be a group having $\mathfrak{P}$ as its 2-Sylow subgroup.

Suppose X is $\mathfrak{G}$-conjugate to an involution $W\in\mathfrak{Q}$. Then some $G\in\mathfrak{G}$ maps $X\to W$, $\mathfrak{P}\to\mathfrak{R}$ where $\mathfrak{R}$ is a 2-Sylow group of $C(W)$ containing $\mathfrak{Q}$. If $|B|>2|S|$, then $\mathfrak{Q}$ is the unique abelian subgroup of $\mathfrak{P}$ of index 2; the same must be true of $\mathfrak{Q}$ as a subgroup of $\mathfrak{R}$, so that $G\colon\mathfrak{Q}\to\mathfrak{Q}$ and hence $G\colon X\to X$. If $|B|=2|S|$ then X is the unique involution which is the square of an element of $\mathfrak{P}$; the same must be true for X as an element of $\mathfrak{R}$, and again this implies $G\colon X\to X$. In either case, we see that X is not $\mathfrak{G}$-conjugate to any other element of $\mathfrak{Q}$. If X were conjugate to an element $V\in\mathfrak{P}$ not in $\mathfrak{Q}$, then some $H\in\mathfrak{G}$ maps $X\to V$, $\mathfrak{P}\to\mathfrak{S}$ where $\mathfrak{S}$ is a 2-Sylow group of $C(V)$ containing A. Then X (being a power of A) is a square in $\mathfrak{S}$. However, the pre-image of X in $\mathfrak{P}$ (under the mapping $H\colon\mathfrak{P}\to\mathfrak{S}$) lies outside $\mathfrak{Q}$ (by the result above), and hence is *not* a square in $\mathfrak{P}$, R.A.A. We have thus shown that X *is not* $\mathfrak{G}$*-conjugate to any other element of* $\mathfrak{P}$.

Now assume (4.3) and (4.4). The above result then implies:

(4.6) Any power of A is $\mathfrak{G}$-conjugate to no other element of $\mathfrak{P}$.

It remains to be shown that $\mathfrak{G}$ has a normal subgroup of index 2. Assume the contrary; then it follows from transfer theory that

$$\mathfrak{P} = \{C^{-1}D : C\in\mathfrak{P},\ D\in\mathfrak{P},\ C\sim D\}, \tag{4.7}$$

"$\sim$" denoting $\mathfrak{G}$-conjugacy. We shall show that (4.7) leads to a contradiction.

Any relation of $\mathfrak{G}$-conjugacy between elements of $\mathfrak{P}$ must, of course, be one of the following three types:

$$\begin{aligned} &\text{I.} && B^rA^sR \sim B^uA^v,\\ &\text{II.} && B^rA^s \sim B^uA^v,\\ &\text{III.} && B^rA^sR \sim B^uA^vR. \end{aligned} \tag{4.8}$$

Suppose first that m is odd in (4.5). As before, we obtain $|B^rR|=2$ for some r; hence we may assume $R^2=1$. If $|B|=|A|$, the left and right sides of (4.5) do not have the same order; thus $|B|>|A|$. By (4.7) we must have a relation (4.8) with

$r-u$ odd, and this relation must be of type (I) since conjugate elements must have the same order. Squaring both sides and applying (4.6), we get

$$A^{2s+mr} = B^{2u}A^{2v}$$

so that $B^{2u} = A^{2(s-v)+mr}$; since $r-u$ is odd, this implies either $|B| \leqq |A|$ or $A \in \{B\}$, R.A.A.

Thus m must be even. Let $m=-2k$, $B'=BA^k$. Then (4.5) implies that $R: B' \to (B')^{-1}$. Clearly $\mathfrak{Q}=\{A, B'\}$, and we may replace B by B' in (4.2). (We thereby lose the inequality $|B| \geqq |A|$, but this will not be used again.) We now have

$$RBR^{-1} = B^{-1}. \tag{4.9}$$

The involution in $\{B\}$ is the only power of B (except 1) which is fixed by R (i.e., which lies in $\{A\}$); thus $\{A\} \cap \{B\} = \{X\}$.

By (4.7) there must exist a relation (4.8,I). Squaring both sides and applying (4.6), we obtain $A^{2(s-v)}R^2 = B^{2u}$; since $A \notin \{B\}$, R^2 must be an even power of A. Replacing R by A^nR for suitable n, we may assume $R^2=1$. (4.9) now gives

$$(B^rA^sR)^2 = A^{2s} \qquad (\text{all } r, s).$$

There can be no relation (4.8,III) with $s-v$ odd, since the elements are not of the same order. If a relation (4.8,II) occurs with $s-v$ odd, then X must be a power of at least one of the two elements involved, and hence (4.4) and (4.6) imply that the given relation occurs in $\mathfrak{P}$ itself, R.A.A. Hence, by (4.7), we must have a relation (4.8,I) with $s-v$ odd. Squaring both sides and applying (4.6), we get

$$B^{2u} = A^{2(s-v)} \in \{A\} \cap \{B\} = \{X\}$$

and hence $|A|=4$. Furthermore, since $\mathfrak{P} \neq \{B, AR\}$, (4.7) implies the existence of a relation (4.8,I) for which $s-v$ is even. Squaring this relation gives $B^{2u}=1$, $B^u=1$ or X. The right side of (4.8,I) is then a power of A, contradicting (4.6). Thus we have the desired contradiction, and the proof is complete.

5. **The simple subgroups of** PSL(3, q). In this section we show that any simple subgroup of PSL(3, q) of even order is isomorphic to one of a set of known simple groups. (The actual occurrence of all of these groups as subgroups of PSL(3, q) will be shown in the following section.)

The following notation will be used throughout this section (in addition to that introduced in §2). $\mathfrak{G}$ will be the inverse image in SL(3, q) of a simple nonabelian subgroup of PSL(3, q) of even order. (There can be no such subgroups of odd order, by [14].) Then $\mathfrak{G}$ contains $\mathfrak{Z}$, the center of SL(3, q). If $p \neq 3$, η will be a primitive cube root of unity in GF(q^2) and W is the diagonal matrix $\|1, \eta, \eta^2\|$. X denotes the diagonal matrix $\|1, -1, -1\|$. We assume that X lies in the center of a 2-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$. (We may do this since all involutions of SL(3, q) are conjugate.) The subgroup $C(X)$ of $\mathfrak{G}$ can be naturally identified with a subgroup of

GL(2, q) and thus is one of the types (1)–(7) of Theorem 3.4. (*All references in this section to numbered "types" will refer to these seven types,* although "Type B" refers to (4.1).) Thus any matrix A in GL(2, q) will be identified (without further explanation) with the corresponding matrix

$$\left\| \begin{array}{c|cc} d^{-1} & 0 & 0 \\ \hline 0 & & \\ & & A \\ 0 & & \end{array} \right\|$$

in SL(3, q), where $d=\det A$. We observe, incidentally, that $\Delta C(X)=C(X)/\mathfrak{Z}$ is the centralizer of ΔX in $\Delta\mathfrak{G}=\mathfrak{G}/\mathfrak{Z}$, and that $\mathfrak{G}$ and $\Delta\mathfrak{G}$ have the same 2-Sylow group.

By "blocks" we shall always mean 2-blocks of ordinary characters, unless otherwise indicated.

LEMMA 5.1. $\mathfrak{P}$ *is either dihedral, semidihedral, or of Type* B.

Proof. $\mathfrak{P}$ is contained in the 2-Sylow group $\boldsymbol{P}$ of GL(2, q^2), and the latter is of Type B (to express $\boldsymbol{P}$ as in (4.1), take S_1, S_2 to be diagonal and $T=[1, 1]$ anti-diagonal). Then $\boldsymbol{Z}(\mathfrak{P})$ consists only of scalar matrices $\|a, a\|$ if $\mathfrak{P}$ is nonabelian; it easily follows that (4.3), (4.4) hold for $\mathfrak{P}$ in this case. By Theorem 4.2, it follows that $\mathfrak{P}$ is abelian, or of Type B, or has a cyclic subgroup of index 2.

If $\mathfrak{P}$ is abelian of type $(2^m, 2^m)$ with $m\geqq 2$, then $\Delta\mathfrak{G}$ cannot be simple (Brauer [4]); while if $\mathfrak{P}$ is cyclic or of type $(2^n, 2^m)$ with $n\neq m$, then $\Delta\mathfrak{G}$ cannot be simple by Burnside's Theorem. Hence if $\mathfrak{P}$ is abelian it must be the four-group (i.e., dihedral). If $\mathfrak{P}$ is nonabelian but has a cyclic subgroup of index 2, then by [17, Theorem 12.5.1] $\mathfrak{P}$ is either dihedral, semidihedral, generalized quaternion, or of the form

$$\mathfrak{P} = \{A, B\};\ A^{2^{n-1}} = B^2 = 1,\ BAB^{-1} = A^{1+2^{n-2}}$$

with $n\geqq 4$. In the latter case it is easy to show that (4.7) cannot hold, R.A.A.; and $\mathfrak{P}$ cannot be generalized quaternion by [10].

LEMMA 5.2. *All involutions of* $\mathfrak{P}$ *are* $\mathfrak{G}$*-conjugate. All involutions of* $\mathfrak{P}$ *different from* X *are* $C(X)$*-conjugate unless* $\mathfrak{P}$ *is dihedral.*

These assertions are a consequence of (4.7). For the detailed arguments corresponding to the three cases of Lemma 5.1, see respectively [15], [6], [7].

LEMMA 5.3. *Let* T *be an involution in* $\mathfrak{P}$ *with* $T\neq X$; *let* $\mathfrak{D}=\{X, T\}$ *and let* $\mathfrak{R}$ *be the maximal normal subgroup of* $C(\mathfrak{D})$ *of odd order. Assume* $\mathfrak{P}\neq\mathfrak{D}$. *Then*

(a) $|N(\mathfrak{D}) : C(\mathfrak{D})|=6$, *and there exist elements* $S\in\mathfrak{G}$ *which interchange* T, XT.

(b) *Let S be any element as in* (a); *let i, f be the number of elements of $\mathfrak{R}$ respectively inverted and fixed by S. Then $i=f$ or $3i=f$. If either f or i is divisible by* 3 *then* $q\equiv 1 \pmod 3$.

Proof. After a conjugation in $C(X)=\mathrm{GL}(2,q)$, we may assume that $T=\|-1,\ -1,\ 1\|$. Then $C(\mathfrak{D})$ is a diagonal subgroup. If $\mathfrak{P}$ is dihedral, (a) is proved in [15]. If $\mathfrak{P}$ is not dihedral, then by Lemma 5.2 there exist elements $Z\in\mathfrak{G}$ and $S\in C(X)$ with $Z\colon X\to T$, $S\colon T\to XT$. There is an element $V\in C(T)$ which maps the 2-Sylow subgroup $Z\mathfrak{P}Z^{-1}$ of $C(T)$ onto a 2-Sylow group $\mathfrak{Q}$ of $C(T)$ containing X and T. Then $G=VZ$ maps $X\to T$, $\mathfrak{P}\to\mathfrak{Q}$. By Lemma 5.2, all involutions of $\mathfrak{Q}$ different from T are conjugate in $C(T)$; hence there is an element $H\in C(T)$ which maps $GTG^{-1}\to X$. Letting $M=HG$, we have

$$\begin{aligned} &M\colon X\to T\to X,\ XT\to XT,\\ &S\colon T\to XT\to T,\ X\to X, \end{aligned} \tag{5.1}$$

and hence $N(\mathfrak{D})/C(\mathfrak{D})\cong S_3$, proving (a).

Let M, S now be any elements of $\mathfrak{G}$ satisfying (5.1). The group $C(\mathfrak{D})$ is a diagonal (hence abelian) subgroup, so that any element which commutes with $\mathfrak{D}$ also commutes with $C(\mathfrak{D})$. S must be an anti-diagonal matrix in $\mathrm{GL}(2,q)=C(X)$. M and S induce automorphisms of $C(\mathfrak{D})$ (hence also of $\mathfrak{R}$) of order $\leqq 2$, and hence

$$\mathfrak{R} = \mathfrak{F}(S)\times\mathfrak{I}(S) = \mathfrak{F}(M)\times\mathfrak{I}(M) \tag{5.2}$$

where $\mathfrak{F}(S)$, $\mathfrak{I}(S)$ are the subgroups of $\mathfrak{R}$ respectively fixed and inverted by S, and similarly for M. Now S acts on $C(\mathfrak{D})$ in the same way as $(MS)M(MS)^{-1}$ which is conjugate to M in $N(\mathfrak{D})=N(C(\mathfrak{D}))$. Hence

$$|\mathfrak{F}(S)| = |\mathfrak{F}(M)|. \tag{5.3}$$

The elements of $\mathfrak{F}(S)$ are scalar elements of $\mathrm{GL}(2,q)$, which (except for the elements of $\mathfrak{Z}$) do not commute with M since $M\notin C(X)$. Similarly, the elements $\|a,a^{-1}\|$ in $\mathfrak{I}(S)$ do not commute with $M^{-1}S$ (unless $a=1$) and hence are not inverted by M. Thus

$$\mathfrak{F}(M)\cap\mathfrak{F}(S) = \{1\} \text{ or } \mathfrak{Z};\ \mathfrak{I}(M)\cap\mathfrak{I}(S) = \{1\}.$$

Combined with (5.2) and (5.3), this implies that $i=f$ or $3i=f$. If $3|f$ or $3|i$ then we must have $q\equiv 1 \pmod 3$ since $\mathfrak{F}(S)$ and $\mathfrak{I}(S)$ are diagonal subgroups.

LEMMA 5.4. *$C(X)$ is not of type* (1). *If $C(X)$ is of type* (2), *then* $\Delta\mathfrak{G}\cong A_5$.

Proof. The first assertion follows from Lemma 5.1. Suppose that $C(X)$ is of type (2); then $C(X)=\mathfrak{Q}\mathfrak{M}$ where $\mathfrak{Q}$ and $\mathfrak{M}$ are as in Theorem 3.4(2). $\mathfrak{P}$ is clearly abelian and hence is the four-group. We have

$$C(\mathfrak{P}) = \mathfrak{M} = \mathfrak{P}\mathfrak{E}$$

where $|\mathfrak{E}|$ is odd. Also, since $N(\mathfrak{P}) \neq C(\mathfrak{P})$, $N(\mathfrak{P})$ must have an element of the form

$$Z = \begin{Vmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{Vmatrix} \qquad (abc = \det Z = 1) \tag{5.4}$$

which must then map every element $\|r, s, t\|$ of $\mathfrak{M}$ into $\|s, t, r\|$. We then have $|N(\mathfrak{P}) : C(\mathfrak{P})| = 3$ and $N(\mathfrak{P}) \cap C(X) = C(\mathfrak{P})$. It follows from block theory that there is a one-to-one correspondence between the blocks of $C(X)$ of defect 2 and the characters of $\mathfrak{E}$, and a one-to-one correspondence between the blocks of $\mathfrak{G}$ of defect 2 and the $N(\mathfrak{P})$-associate classes of characters of $\mathfrak{E}$. $C(X)$ has $|\mathfrak{E}|$ blocks of defect 2, each containing four characters (cf. [8]); these must be precisely the $|\mathfrak{M}|$ characters of degree 1 given by

$$\begin{Vmatrix} x & 0 \\ z & y \end{Vmatrix} \to \theta\left(\begin{Vmatrix} x & 0 \\ 0 & y \end{Vmatrix}\right)$$

where θ ranges over the characters of $\mathfrak{M}$.

Suppose first that $\mathfrak{E} \neq \mathfrak{Z}$. Then some character of $\mathfrak{E}$ has three distinct associates in $N(\mathfrak{P})$; the three corresponding blocks of $C(X)$ "induce" the same block $\boldsymbol{B}$ of $\mathfrak{G}$. One can deduce that the matrix of generalized decomposition numbers for $\boldsymbol{B}$ consists entirely of entries ± 1, and that the four characters in $\boldsymbol{B}$ all have the same degree f. Applying Brauer's formula [3], one can then compute

$$|\mathfrak{G}| = f|\mathfrak{M}| \cdot |\mathfrak{Q}|^3.$$

On the other hand, if $1, f_2, f_3, f_4$ are the degrees of the characters in the *principal* block of $\mathfrak{G}$, Brauer's formula gives the well-known result (see [5] or [1])

$$|\mathfrak{G}| = 8\pi|C(X)|^3/|C(\mathfrak{P})|^2 = 8\pi|\mathfrak{M}| \cdot |\mathfrak{Q}|^3 \tag{5.5}$$

where

$$\pi = \frac{f_2 f_3 f_4}{(f_2+1)(f_3+\delta)(f_4-1)}; \quad \delta = \pm 1; \quad f_4 = 1+f_2+\delta f_3.$$

Thus we obtain

$$f = 8f_2 f_3 f_4/(f_2+1)(f_3+\delta)(f_4-1). \tag{5.6}$$

Here f and the f_i are odd and > 1. (Even if $\mathfrak{G} \neq \mathfrak{G}'$, we would then have $\mathfrak{G}/\mathfrak{G}'$ of order 3 whereas there are *four* characters of degree f, so that $f > 1$; and the f_i are $\neq 1$ since these characters, being in the principal 2-block, contain $\mathfrak{Z}$ in their kernel.) The only integral solution of (5.6) consistent with these conditions is $(f_2, f_3, f_4) = (5, 3, 3)$. The character of degree 5 has no conjugates and is hence rational-valued. Thus $|\mathfrak{G}/\mathfrak{Z}|$ divides $2^2 \cdot 3^2 \cdot 5 = 180$ (Lemma 4.1), and hence $\mathfrak{G}/\mathfrak{Z}$ is isomorphic to A_5.

On the other hand, suppose $\mathfrak{E}=\mathfrak{Z}$. (5.5) is still valid, with $|\mathfrak{M}|=4$ or 12; and since the f_i are >1, one easily sees that $\pi\leqq 15/8$. If $|\mathfrak{Q}|=1$ then $|\mathfrak{G}|\leqq 180$; since $|\mathfrak{P}|=4$, $|\mathfrak{G}|\neq 168$ and hence $\Delta\mathfrak{G}\cong A_5$. Assume $|\mathfrak{Q}|>1$. Let $d=ba^{-1}$, $e=bc^{-1}$ in (5.4); then a computation shows that the most general element of the set

$$\mathfrak{Q}^Z\cdot\mathfrak{Q}\cdot\mathfrak{Q}^{Z^2}\cdot\mathfrak{Q}^Z\cdot\mathfrak{Q}$$

has the form

$$\left\|\begin{matrix} 1 & tve & te \\ (r+u)d & 1+rtvde & rtde \\ sud & s+v & 1 \end{matrix}\right\| \tag{5.7}$$

where the elements (3.1) ($\tau=r, s, t, u, v$) lie in $\mathfrak{Q}$. Distinct choices of r, s, t, u, v with $t\neq 0$ give distinct elements (5.7), and hence

$$|\mathfrak{G}| > |\mathfrak{Q}|^4(|\mathfrak{Q}|-1).$$

Comparing this with (5.5), and noting that $|\mathfrak{M}|>4$ only if $q\equiv 1 \pmod 3$, we find that $|\mathfrak{Q}|=p\leqq 13$. Since $\mathfrak{Q}^Z\mathfrak{Q}$ generates a p-subgroup strictly larger than itself, $p^3=|\mathfrak{Q}|^3$ must divide $|\mathfrak{G}|$, and hence 8π is an odd integer. This integer can only be 15, with

$$(f_2, f_3, f_4) = (3, 3, 5).$$

It follows as before that $\Delta\mathfrak{G}\cong A_5$.

REMARK. The results of [16] are applicable to the case treated in Lemma 5.4. Since these results are quite difficult, we have avoided using them. The special case $\mathfrak{E}=\mathfrak{Z}$ is also covered by [15].

LEMMA 5.5. *If $C(X)$ is of type* (3) *or* (4), *then $\Delta\mathfrak{G}$ is isomorphic to A_7 or to* PSL(2, k) *for some odd $k\geqq 5$. If $\Delta\mathfrak{G}\cong A_7$ then $p=5$ and α is even.*

Proof. Any subgroup of GL(2, q) of type (3) is conjugate over the extension field GF(q^2) to a subgroup of GL(2, q^2) of type (4) (cf. proof of Theorem 3.4); hence we may assume $C(X)$ is of type (4). Thus $C(X)=\{\mathfrak{M}, S\}$ where $\mathfrak{M}$ is a diagonal subgroup of GL(2, q) and S is an anti-diagonal 2-element in GL(2, q). If $\mathfrak{Q}=\mathfrak{P}\cap\mathfrak{M}$, then $\mathfrak{Q}$ is an abelian subgroup of $\mathfrak{P}$ of index 2 and is normal in $C(X)$. Using (4.7) and Lemmas 5.1 and 5.2, we can conclude that $\mathfrak{P}$ is dihedral. Since the normal 2-complement $\mathfrak{E}$ of $C(X)$ is abelian, the results of [15] imply that $\Delta\mathfrak{G}$ is isomorphic to A_7 or to PSL(2, k) for some odd $k\geqq 5$. If $\Delta\mathfrak{G}\cong A_7$ then an element of order 5 in $\mathfrak{G}$ is conjugate to four of its powers, and this is possible in SL(3, q) only if $p=5$. From the structure of A_7, the group $C(\mathfrak{D})$ of Lemma 5.3 (which may be assumed to be diagonal, as in the proof of Lemma 5.3) must contain a 3-element, so that $q\equiv 1 \pmod 3$; with $p=5$, this implies that α is even. Thus Lemma 5.5 is proved.

We remark here that Lemma 5.5 can be proved without using the results of [15]. The general idea is as follows: let $\mathfrak{I}$, $\mathfrak{F}$ be the subgroups of $\mathfrak{E}$ respectively inverted

and fixed by S. If $\mathfrak{Q}$ is cyclic, or is the four-group with $|\mathfrak{N}|=1$, one can easily show that $\Delta\mathfrak{G}$ satisfies the assumptions made in [11], and hence is isomorphic to PSL(2, k). (The argument is given in [1] for $q\not\equiv 1 \pmod 3$; only slight modifications are needed if $q\equiv 1 \pmod 3$.) If $\mathfrak{Q}$ is the four-group with $|\mathfrak{N}|>1$, an application of Brauer's formula to the principal block gives $|\mathfrak{G}:\mathfrak{F}|=2520$, $|\mathfrak{N}|=3$, $|\mathfrak{F}:\mathfrak{Z}|=1$ or 3. (Some of the calculations may be found in [1], but not this result since the restriction $q\not\equiv 1 \pmod 3$ is imposed. See also [27].) If $\mathfrak{F}=\mathfrak{Z}$, the results of [26] are applicable to $\Delta\mathfrak{G}$ and we have $\Delta\mathfrak{G}\cong A_7$. If $|\mathfrak{F}:\mathfrak{Z}|=3$, one can apply Brauer's formula to a nonprincipal block of $\Delta\mathfrak{G}$ of defect 3, and show that this block must have a character of degree 1, R.A.A.

LEMMA 5.6. *If* $\Delta\mathfrak{G}\cong\mathrm{PSL}(2,k)$ *as in Lemma* 5.5, *and if* k *is not a power of* p, *then* $k=5$, 7, *or* 9. *The case* $k=9$ *does not occur if* $q\not\equiv 1 \pmod 3$.

Proof. Suppose $r\neq p$ is the prime factor of k. The r-Sylow group $\mathfrak{Q}$ of $\Delta\mathfrak{G}$ is elementary-abelian, and is hence conjugate to one of the following:

(5.8)
(i) a cyclic group of order dividing q^2-1 or q^2+q+1 but not $q-1$;
(ii) a diagonal subgroup of PSL(3, q);
(iii) the group $\Delta(\{W, Y\})$ of order 9, where Y is a permutation matrix of order 3 and $q\equiv 1 \pmod 3$.

In case (iii), clearly $k=|\mathfrak{Q}|=9$. In cases (i) and (ii), consideration of characteristic roots shows that $\mathfrak{Q}$ contains an element $Z\neq 1$ which is $\mathfrak{G}$-conjugate to exactly 1, 2, 3, or 6 elements of $\mathfrak{Q}$. Since this number equals $(k-1)/2$ from the structure of PSL(2, k), we have $k=5$, 7, or 13 (not 3 since PSL(2, 3) is not simple). The case $k=13$ is impossible, for in this case $\mathfrak{Q}$ is cyclic (since $|\mathfrak{Q}|=13$) and $(k-1)/2=6$, whereas no p-regular element of PSL(3, q) is conjugate to six of its powers.

LEMMA 5.7. *If* $C(X)$ *is of type* (5), *then we have "Case* 2" *of Theorem* 3.4(5):

$$C(X) = \{\mathrm{SL}(2,p^\beta),\ V,\ \|b,\varepsilon b\|\}.$$

Moreover, if the 2*-Sylow group* $\mathfrak{Q}$ *of* $\mathrm{SL}(2,p^\beta)$ *has order* 2^{m+1} *and the element* V *has order* $2^n u$ (u *odd*), *then either* $\mathfrak{P}$ *is of Type* B *with* $n=m$, *or* $\mathfrak{P}$ *is semidihedral with* $n=0$.

Proof. Since $\mathfrak{P}$ contains $\mathfrak{Q}$ (which is generalized quaternion), $\mathfrak{P}$ cannot be dihedral, and hence is semidihedral or of Type B.

Suppose $\mathfrak{P}$ is semidihedral. Then $\mathfrak{P}$ has a cyclic subgroup of index 2. This is consistent with the structure of $\mathfrak{P}$ obtained from Theorem 3.4(5) only if $n\leqq 1$; since $X=\|-1,-1\|$ already belongs to $\mathrm{SL}(2,p^\beta)$, we may say $n=0$. Since $\mathfrak{P}\neq\mathfrak{Q}$ it follows that the element $\|b,\varepsilon b\|$ must appear.

On the other hand, if $\mathfrak{P}$ is of Type B, then $|\mathfrak{P}|=2^{2k+1}$ where 2^k is both the order of $\boldsymbol{Z}(\mathfrak{P})$ and the maximum order of any element of $\mathfrak{P}$ which is $\mathfrak{P}$-conjugate to its inverse. Hence $m\leqq k$ and $n\leqq k$. Since $2^{2k+1}=|\mathfrak{P}|$ equals 2^{m+n} or 2^{m+n+1}, we

can only have $m=n=k$, $|\mathfrak{P}|=2^{m+n+1}$ so that the element $\|b, \varepsilon b\|$ appears. This proves Lemma 5.7.

If $C(X)$ is of type (5), we thus have four possible cases:

(5.9)
- CASE I. $p^\beta \equiv 1 \pmod 4$; $\mathfrak{P}$ is of Type B.
- CASE II. $p^\beta \equiv 1 \pmod 4$; $\mathfrak{P}$ is semidihedral.
- CASE III. $p^\beta \equiv -1 \pmod 4$; $\mathfrak{P}$ is of Type B.
- CASE IV. $p^\beta \equiv -1 \pmod 4$; $\mathfrak{P}$ is semidihedral.

LEMMA 5.8. *In Cases* I *and* IV *of* (5.9), *either* (a) *or* (b) (*as follows*) *occurs*:

(a) $C(X)=\mathrm{GL}(2, p^\beta)$.

(b) $q\equiv 1 \pmod 3$; $C(X)=\{\mathrm{GL}(2, p^\beta), V\}$ *where* V *is a scalar element of* $\mathrm{GL}(2, q)$ *of order* $3(p^\beta-1)$.

Proof. In Case I, if ι is an element of order 4 in $(\mathrm{GF}(q))^*$ then $\|\iota, -\iota\|$ is in $\mathrm{SL}(2, p^\beta)$ and $\|\iota, \iota\| \in \{V\}$ (using the notation of Lemma 5.7 and its proof), so that the product

$$T = \|\iota, -\iota\| \cdot \|\iota, \iota\| = \|-1, 1\|$$

lies in $C(X)$. In Case IV, some odd power of $\|b, \varepsilon b\|$ is a 2-element, and hence of the form $\|c, \pm c\|$ since $(p^\beta-1)/2$ is odd (in fact, by the first assertion of Lemma 5.7 we must have $\|c, -c\|$). Then $\|c, -c\|^2$ is a scalar 2-element in $\{\mathrm{SL}(2, p^\beta), V\}$ and hence equal to $\pm I$ (since $n=0$), so that $c=\pm 1$ or $\pm\iota$. If $c=\pm\iota$ then

$$\mathfrak{P} = \{\mathfrak{Q}, \|c, -c\|\}$$

(with $\mathfrak{Q}$ as in Lemma 5.7) is contained in the 2-Sylow group of $\mathrm{SL}(2, p^{2\beta})$ which is generalized quaternion, R.A.A. Hence $c=\pm 1$ so that again $T=\|-1, 1\|$ is in $C(X)$.

In either case, letting f, i be as in Lemma 5.3(b), we have here $f=u$ (cf. Lemma 5.7), while i is the number of odd-order diagonal elements in $\mathrm{SL}(2, p^\beta)$. It follows at once, by Lemma 5.3(b), that $|V|=2^n u$ equals $p^\beta-1$ or $3(p^\beta-1)$ (replace V by $-V$ if necessary in Case IV). In Case IV it follows at once that

$$C(X) = \{\mathrm{SL}(2, p^\beta), V, T\} = \{\mathrm{GL}(2, p^\beta), V\}.$$

In Case I the same conclusion follows by considering the structure of the abelian (diagonal) subgroup of $\mathfrak{P}$ of index 2. Moreover, if $|V|=p^\beta-1$ then $V\in \mathrm{GL}(2, p^\beta)$. Lemma 5.8 follows at once.

We now consider the structure of $C(X)$ in Cases II, III of (5.9). In either case, $q\equiv 1 \pmod 4$ (true in Case III since $\mathfrak{P}$ is of Type B).

Discussion of Case II. Here $|V|$ is odd. We may replace $\|b, \varepsilon b\|$ by an odd power $M=\|c, \delta c\|$ which is a 2-element. Then $C(X)$ has the 2-Sylow group $\mathfrak{P}=\{\mathfrak{Q}, M\}$ where $\mathfrak{Q}$ is the 2-Sylow group of $\mathrm{SL}(2, p^\beta)$. Hence $\mathfrak{P}$ has a diagonal subgroup $\mathfrak{D}$ of index 2, and $\mathfrak{P}=\{\mathfrak{D}, J\}$ where $J=[1, -1]$. If $T=\|-1, 1\|$ lies in $\mathfrak{D}$ then also $\|\iota, \iota\| = T\|-\iota, \iota\|$ is in $\mathfrak{D}$, contradicting $n=0$ (Lemma 5.7). Hence X is the only

involution in $\mathfrak{D}$, and $\mathfrak{D}$ is cyclic. Since $\mathfrak{P}$ is semidihedral of order 2^{m+2} where $p^\beta - 1 = 2^m k$ (k odd), $\mathfrak{D}$ must be generated by an element

$$A = \|w, w^{2^m - 1}\|$$

where $w^{2^m} = \text{Det } A = -1$. In particular, 2^{m+1} divides $q-1$ so that $2\beta|\alpha$. Letting $B = AJ = [w, w^{-1}]$, B is an involution, $\mathfrak{P} = \{A, B\}$, and the element $S = \|\iota, -\iota\|$ of SL$(2, p^\beta)$ maps $B \to XB \to B$. A computation shows that $C(X, B)$ consists of matrices of the form

$$\begin{Vmatrix} e & w^2 d \\ d & e \end{Vmatrix}.$$

Such a matrix is inverted by S if and only if it has determinant 1 as an element of GL$(2, q)$; the number of these matrices in $C(X)$ is $p^\beta + 1$ (see [12]) and the number of them of odd order is $(p^\beta + 1)/2$. It follows from Lemma 5.3 that the order of V as an element in $C(X)$ is $(p^\beta + 1)/2$ or $3(p^\beta + 1)/2$. The latter clearly can occur only if $q \equiv 1 \pmod 3$. Now let

$$G = \begin{Vmatrix} \lambda\mu & \mu \\ -\lambda & 1 \end{Vmatrix} \tag{5.10}$$

where λ, μ have orders $2(p^\beta + 1)$, $2(p^\beta - 1)$ in $(\text{GF}(q))^*$. Then a computation shows that G maps the subgroup of $U^*(2, p^\beta)$ of determinant 1 onto SL$(2, p^\beta)$, $V \to V$, and

$$\|-1, 1\| \to [\mu, \mu^{-1}] = \|\mu w^{-1}, w\mu^{-1}\| \cdot [w, w^{-1}] \in C(X).$$

Thus $C(X)$ is conjugate to $\{U^*(2, p^\beta), V\}$.

Discussion of Case III. Here again $2\beta|\alpha$, since $q \equiv 1$, $p^\beta \equiv -1 \pmod 4$. The same argument as for Case IV (Lemma 5.8) shows that

$$C(X) = \{\text{SL}(2, p^\beta), V, \|c, -c\|\}$$

where $\|c^2, c^2\|$ is a 2-element in $\{V\}$. Let $p^\beta + 1 = 2^m k$ with k odd. If $c^{2^m} = 1$, then we would have $(\det M)^{2^{m-1}} = 1$ for all $M \in \mathfrak{P}$; since $|\mathfrak{P}| = 2^{2m+1}$, $\mathfrak{P}$ would then have a subgroup $\mathfrak{Q}$ of order 2^{m+2} contained in SL$(2, q)$ and thus cyclic or generalized quaternion. This is inconsistent with the structure of $\mathfrak{P}$ as a group of Type B. Thus we must have $|c| = 2^{m+1}$. Writing $\iota = c^{2^{m-1}}$, the element

$$B = \|\iota, \iota\| \cdot [1, -1] = [\iota, -\iota]$$

is an involution in $C(X)$, and the elements B, XB are interchanged by an element of the form

$$S = \begin{Vmatrix} d & e \\ e & -d \end{Vmatrix}$$

in SL$(2, p^\beta)$. $C(X, B)$ consists of matrices of the form

$$\begin{Vmatrix} a & b \\ -b & a \end{Vmatrix}.$$

Just as in the discussion of Case II, the elements of $C(X, B)$ inverted by S are those of determinant 1, while those fixed by S are scalar. It follows in the same way as before that the order of V in $C(X)$ is $(p^\beta+1)/2$ or $3(p^\beta+1)/2$. If G is as in (5.10) then G maps

$$[\mu^{-2}, 1] \to \|\mu^{-1}, -\mu^{-1}\| \in \{V, \|c, -c\|\} \subseteq C(X)$$

and as in Case II we deduce that $C(X)$ is conjugate to $\{U^*(2, p^\beta), V\}$.

Combining the results for Cases II and III with Lemma 5.8, we obtain

LEMMA 5.9. *If $C(X)$ is of type* (5), *then $C(X)$ is conjugate to $\mathfrak{R}$ or $\{\mathfrak{R}, V\}$, where $\mathfrak{R}=\mathrm{GL}(2, p^\beta)$ $(\beta|\alpha)$ or $U^*(2, p^\beta)$ $(2\beta|\alpha)$ and V is a scalar element of* $\mathrm{GL}(2, q)$ *such that $V^3 \in \mathfrak{R}$.*

In connection with Lemma 5.9, note that if $q\equiv 1$ but $p^\beta \not\equiv 1 \pmod 3$ and $\mathfrak{R}=\mathrm{GL}(2, p^\beta)$, then $\mathfrak{Z} \not\subseteq \mathfrak{R}$, and hence $C(X)=\{\mathfrak{R}, V\}$. In this case $\Delta C(X)=\{\mathfrak{R}, V\}/\mathfrak{Z}$ coincides with $\mathfrak{R}$. Similar considerations apply to the case where $p^\beta \not\equiv -1 \pmod 3$ and $\mathfrak{R}=U^*(2, p^\beta)$. Hence Lemma 5.9 gives the following for $\Delta C(X)$:

LEMMA 5.9A. *If $C(X)$ is of type* (5), *then $\Delta C(X)$ is isomorphic to one of the following*:

(a) $\mathrm{GL}(2, p^\beta)$, *with* $\beta|\alpha$, $p^\beta \not\equiv 1 \pmod 3$;

(b) $U^*(2, p^\beta)$, *with* $2\beta|\alpha$, $p^\beta \not\equiv -1 \pmod 3$;

(c) $\mathrm{GL}(2, p^\beta)/\mathfrak{Z}$ *or* $\{\mathrm{GL}(2, p^\beta), V\}/\mathfrak{Z}$, *with* $\beta|\alpha$, $p^\beta \equiv 1 \pmod 3$;

(d) $U^*(2, p^\beta)/\mathfrak{Z}$ *or* $\{U^*(2, p^\beta), V\}/\mathfrak{Z}$, *with* $2\beta|\alpha$, $p^\beta \equiv -1 \pmod 3$.

(*Here V is as in Lemma* 5.9.)

The further treatment of type (5) depends on the following group-theoretic lemma.

LEMMA 5.10. *Let $\mathfrak{H}$ be any group containing an involution X in the center of its 2-Sylow group. Assume that in $\mathfrak{H}$,*

(i) $C(U)=C(X)$ *for all* $U\neq 1$ *in* $\boldsymbol{Z}(C(X))$;

(ii) $C(X)$ *has any one of the structures* (a), (b), (c), (d) *of Lemma* 5.9A;

(iii) $\mathfrak{H}$ *contains an element G which maps $X \to T \to XT$, where $T \in C(X)$ is the matrix* $\|-1, 1\|$ (*or, in cases* (c) *and* (d), *the residue class modulo $\mathfrak{Z}$ of this matrix*).

Then $|\mathfrak{H}|$ is uniquely determined by the structure of $C(X)$, with three exceptions: (1) $C(X)=\mathrm{GL}(2, 3)$, $|\mathfrak{H}|=5616$ *or* 7920; (2) $C(X)=\mathrm{GL}(2, 7)/\mathfrak{Z}$, $|\mathfrak{H}|=1876896$ *or* 2328480; (3) $C(X)=U^*(2, 5)/\mathfrak{Z}$, $|\mathfrak{H}|=68400$, 85680, *or* 126000.

Proof. If $\mathfrak{P}$ is of Type B, the conclusion is stated by Brauer in [7] with much weaker assumptions (in fact, only (4.7) is used, and that is implied here by (iii)). If $\mathfrak{P}$ is semidihedral, the method of proof involves application of Brauer's formula to the principal block of $\mathfrak{H}$, and also to a block of defect 2 of $\mathfrak{H}$ which is induced by three distinct blocks of $C(X)$. (The "exceptions" occur only when no such block exists.) If $C(X)$ has the structure of Lemma 5.9A, case (a), the argument is given

in detail by Brauer [6]. The argument in all the other cases is similar, and we omit it in order to keep the length of this paper within reason. The characters of $\mathfrak{R}$, which are needed in the proof, are found in [25] for $\mathfrak{R}=\mathrm{GL}(2, p^\beta)$ and in [13] for $\mathfrak{R}=U^*(2, p^\beta)$. (Alternatively, the characters of $U^*(2, p^\beta)$ can be computed as follows: those of degrees 1, q, $q+1$ are obtained by considering the characters induced by linear characters of the normalizer of a p-Sylow group, while those of degree $q-1$ may be found by an argument like that used in [25].)

LEMMA 5.11. *If $C(X)$ is of type* (5), *then $\mathfrak{G}$ is conjugate in* GL(3, q) *to*
(a) $\{\mathrm{SL}(3, p^\beta), \mathfrak{Z}\}$, *with* $\beta|\alpha$; *or*
(b) $\{U(3, p^\beta), \mathfrak{Z}\}$, *with* $2\beta|\alpha$.

Proof. $C(X)$ is given by Lemma 5.9. By Lemma 5.3(a), $\mathfrak{G}$ must contain an element Z of the form (5.4). Let us first suppose that $C(X)=\mathrm{GL}(2, p^\beta)$. After conjugation by a suitable element of the form $\|y, z, z\|$, we may assume $a=1$, $b=c^{-1}$. But then, letting $S=[1, 1]\in C(X)$, the element

$$ZSZ = \begin{Vmatrix} c & 0 & 0 \\ 0 & 0 & c^{-2} \\ 0 & -c & 0 \end{Vmatrix}$$

lies in $\mathfrak{G}\cap C(X)=\mathrm{GL}(2, p^\beta)$, so that $c\in \mathrm{GF}(p^\beta)$.

Suppose instead that $C(X)=\{\mathrm{GL}(2, p^\beta), V\}$ as in Lemma 5.8(b). The same reasoning as above gives $c\in \mathrm{GF}(p^\beta)$ or $c\pi\in \mathrm{GF}(p^\beta)$ where π has order $3(p^\beta-1)$ in $(\mathrm{GF}(q))^*$. In the latter case, we may say $V=\|\pi, \pi\|$; if we conjugate by the element $Y=\|\pi, 1, 1\|$ in GL(3, q) and then replace Z by ZV^{-1}, we find that we may still assume the coefficients of Z lie in $\mathrm{GF}(p^\beta)$.

Similar arguments can be used if $\mathfrak{R}=U^*(2, p^\beta)$ in Lemma 5.9; here we find that the coefficients of Z satisfy $a^k=b^k=c^k=1$, $k=p^\beta+1$.

Again assume $C(X)=\mathrm{GL}(2, p^\beta)$. With Z as above, let

$$\mathfrak{G}_1 = \{C(X), Z\}; \quad \mathfrak{G}_2 = \{\mathrm{SL}(3, p^\beta), \mathfrak{Z}\}.$$

Then $\mathfrak{G}_1\subseteq\mathfrak{G}$ and $\mathfrak{G}_1\subseteq\mathfrak{G}_2$. Since the assumptions of Lemma 5.10 are satisfied simultaneously by all three groups $\Delta\mathfrak{G}$, $\Delta\mathfrak{G}_1$, $\Delta\mathfrak{G}_2$ (with the same $C(X)$), it follows that $\mathfrak{G}_1=\mathfrak{G}$ and $\mathfrak{G}_1=\mathfrak{G}_2$, so that $\mathfrak{G}=\{\mathrm{SL}(3, p^\beta), \mathfrak{Z}\}$. If $C(X)=\{\mathrm{GL}(2, p^\beta), V\}$, similar argument gives $\mathfrak{G}=\{\mathrm{SL}(3, p^\beta), V\}$; here if $p^\beta\equiv 1 \pmod 3$ then $\Delta\mathfrak{G}$ is not simple, while if $p^\beta\not\equiv 1 \pmod 3$ then $V\in\{\mathrm{SL}(3, p^\beta), \mathfrak{Z}\}$ and thus $\mathfrak{G}=\{\mathrm{SL}(3, p^\beta), \mathfrak{Z}\}$. Similar arguments apply when $\mathfrak{R}=U^*(2, p^\beta)$.

LEMMA 5.12. *If $C(X)$ is of type* (6), *then $p=3$ and $\mathfrak{G}$ is conjugate to* SL(3, 3).

Proof. Using the notations of Theorem 3.4(6), let $u=2^m v$ where v is odd. By Lemmas 5.1 and 3.3, $\mathfrak{P}$ is semidihedral or of Type B. Suppose the latter. If $|\mathfrak{P}|=2^{2n+1}$, then $Z(\mathfrak{P}/\{X\})$ has the form $C_2\times C_k$, $k=2^{n-1}$, which is consistent with Theorem 3.4(6) only if $n=2$, $m=1$, $S_4\subseteq C(X)/\{X\}$. In this case, if $G\in\mathfrak{P}$

corresponds to the permutation (1234) in S_4, then (by Lemma 3.3) G^2 is an element of order $4=2^n$ conjugate in $\mathfrak{P}$ to its inverse, and this is impossible. Hence $\mathfrak{P}$ must be semidihedral. $\mathfrak{P}/\{X\}$ is then dihedral of order $\geqq 8$, so that u is odd and $S_4 \subseteq C(X)/\{X\}$. Thus

$$C(X)/\{X\} \cong S_4 \times C_w \qquad (w \text{ odd}).$$

Let G, $T \in C(X)$ correspond to the permutations (1234) and (13) in S_4. Then $|G|=8$ and $|T|=2$, since all six elements of $\mathfrak{P}$ of order 4 correspond to even permutations (cf. Lemma 3.3). Since $\mathfrak{P}$ is semidihedral and T is not a power of G, G^2 interchanges T and XT. Lemma 5.3 applies here with $\mathfrak{N}=C_w$ and $S=G^2$. Clearly no element of C_w is inverted by S, and hence Lemma 5.3(b) implies $C_w=\mathfrak{Z}$, $\Delta C(X)/\{X\} \cong S_4$. This, combined with the structure of $\mathfrak{P}$, is enough to determine the structure of $\Delta C(X)$; we find that $\Delta C(X) \cong \mathrm{GL}(2, 3)$. Brauer's results [6] now show that either (a) $\Delta\mathfrak{G} \cong \mathrm{PSL}(3, 3)$, or (b) $\Delta\mathfrak{G}$ is simple of order 7920. In case (b), each element of $\mathfrak{G}$ of order 11 is conjugate to five of its powers (so that $p=11$) and each element of order 5 is conjugate to four of its powers (so that $p=5$), R.A.A. Hence we must have $\Delta\mathfrak{G} \cong \mathrm{PSL}(3, 3)$.

The group $\Delta\mathfrak{G}$ has a faithful (modular) projective representation $\mathscr{R}$ of degree 3 in the obvious way. The tensor product of $\mathscr{R}$ with its contragredient is a faithful representation (*not* projective) of degree 9; let ψ be its character. Since the nonprincipal ordinary irreducible representations of $\Delta\mathfrak{G}$ all have degrees > 9 (cf. [25]), it follows that the characteristic p must divide $|\mathfrak{G}|$. Hence $p=3$ or 13. If $p=3$, it can be shown by a short computation (details given in [1]) that $C(X)$ is *conjugate* to GL(2, 3) in GL(2, q). The proof of Lemma 5.11 now shows that $\mathfrak{G}$ is conjugate to SL(3, 3).

We must still show that the case $p=13$ cannot occur. If $p=13$, the character ψ is a nonnegative linear combination of irreducible modular (with respect to the prime 13) characters ϕ_i of $\Delta\mathfrak{G} \cong \mathrm{PSL}(3, 3)$. The ϕ_i must belong to the 13-blocks which consist of *ordinary* characters χ_j of degrees prime to 13, since all modular characters not in these blocks coincide with the ordinary characters of degrees divisible by 13 whereas $\deg \psi < 13$. By a standard result from block theory, the ϕ_i, restricted to 13-regular elements, are linear combinations of the χ_j with integer coefficients. However, if $G \in \Delta\mathfrak{G}$ is an element of order 8, then $\chi_j(G)=\chi_j(G^2)$ for all such χ_j (cf. [25]), whereas $\psi(G)=3$, $\psi(G^2)=1 \neq \psi(G)$, R.A.A.

LEMMA 5.13. *If $C(X)$ is of type* (7), *then $p=3$, α is even, and $\mathfrak{G}$ is conjugate to the subgroup $U(3, 3)$.*

Proof. $C(X)/\{X\}$ has an elementary-abelian subgroup of order 8. Hence $\mathfrak{P}$ can only be of Type B, and $q \equiv 1 \pmod 4$. Writing $u=2^m v$ (v odd), $|\mathfrak{P}|=2^{m+4}$ and $|Z(\mathfrak{P})|=2^{m+1}$, so that $m=1$, $u=2v$. Up to conjugacy in $C(X)$ we have

$$\mathfrak{P} = \{\|\iota, 1\|, \|1, \iota\|, [1, 1]\} \tag{5.11}$$

where as usual $\iota^2 = -1$. By Lemma 3.3, some element σ of order 2 in A_4 corresponds to an element B of order 4 in the diagonal subgroup of $\mathfrak{P}$, such that B is inverted in $\mathfrak{P}$. Evidently we may take $B = \|\iota, -\iota\|$. Since σ commutes with no element of odd order in A_4, the odd-order diagonal subgroup of $C(X)$ must consist only of scalar matrices $\|a, a\|$, and hence (by Lemma 5.3) is just $\mathfrak{Z}$. Thus $C(X)$ has a subgroup $\mathfrak{H}$ with

$$|C(X) : \mathfrak{H}| = 2; \quad \Delta\mathfrak{H}/\{X\} \cong A_4 \times C_2. \tag{5.12}$$

The results of [7] give

$$|\mathfrak{G} : C(X)| = \mu^2 f^2 (f^2+f+1),$$

$$|\Delta C(X)| = \mu\varepsilon t\gamma f(f^2-1),$$

where μ, t, f are odd, $f \equiv 5 \pmod 8$, and $\varepsilon = f/|f| = \pm 1$. Since here $|\Delta C(X)| = 96$, the only solution is $f = -3$, $\mu = t = 1$, $|\Delta\mathfrak{G}| = 6048$. By a result in [24], the only simple group of this order is $U(3, 3)$. Since $|\mathfrak{G}|$ is divisible by the prime 7 to exactly the first power, the results of Brauer [2] show that $\mathfrak{G}$ cannot have a faithful ordinary representation of degree 3. Hence the characteristic p divides $|\mathfrak{G}|$, i.e., $p = 3$ or 7. In the case $p = 3$, a short computation (done in [1]) shows that, after replacing $C(X)$ by a conjugate subgroup, we have exactly the situation of (5.9), Case III. The former reasoning still applies with $p^\beta = 3$, and we conclude (as in Lemma 5.11) that $\mathfrak{G}$ is *conjugate* to $U(3, 3)$.

Suppose instead that $p = 7$. By (5.11), $\mathfrak{P}$ contains the elements $X = \|-1, -1\|$, $T = \|1, -1\|$, $B = \|\iota, -\iota\|$, $Y = [1, -1]$ (identifying GL(2, q) with a subgroup of SL(3, q) as usual). These matrices also belong to $U(3, 3)$; we may assume (after a conjugation and possible replacement of ι by $-\iota$) that they correspond to themselves under the isomorphism of $\Delta\mathfrak{G} \to U(3, 3)$. (We here regard $\mathfrak{P}$ as contained in $\Delta\mathfrak{G}$ rather than $\mathfrak{G}$.) If E is the element of $\Delta\mathfrak{G}$ which corresponds to the element

$$\begin{Vmatrix} 1 & 1 & 1-\iota \\ -(1+\iota) & (1+\iota) & 0 \\ 1 & 1 & \iota-1 \end{Vmatrix}$$

of $U(3, 3)$, then

$$|E| = 7; \ |EXT| = 3; \ |XE| = 7; \ Y \sim TE; \ E \sim EB \tag{5.13}$$

where these relations are taken in $\Delta\mathfrak{G}$ rather than $\mathfrak{G}$, and "$\sim$" denotes conjugacy. In $\Delta\mathfrak{G} \subseteq \mathrm{PSL}(3, 7^\alpha)$, an element of order 7 has trace 3 (strictly speaking, this means that one of its pre-images in SL(3, 7^α) has trace 3), and the traces of conjugate elements differ by at most a factor 2^m (here $\eta = 2$ is a cube root of unity). Hence from (5.13) we get five equations for the three diagonal coefficients of E. A computation shows that these equations have no solution in GF(7^α). Thus the case $p = 7$ does not occur, and Lemma 5.13 is proved.

REMARK. A similar method can be used to exclude all of the cases where p does not divide $|\mathfrak{G}|$, without the necessity of using the results of [2].

Summarizing the results of this section, we have

THEOREM 5.14. *Let $\mathfrak{G}$ be the inverse image under Δ of a nonabelian simple subgroup of even order of the group* $\mathrm{PSL}(3,q)=\mathrm{PSL}(3,p^\alpha)$. *Then one of the following occurs*:

I. *$\mathfrak{G}$ is conjugate (in* $\mathrm{GL}(3,q)$*) to* $\{\mathrm{SL}(3,p^\beta),\mathfrak{Z}\}$ *with* $\beta|\alpha$, *or to* $\{U(3,p^\beta),\mathfrak{Z}\}$ *with* $2\beta|\alpha$.

II. *$\Delta\mathfrak{G}$ is isomorphic to* $\mathrm{PSL}(2,p^\beta)$ *for some* β.

III. *$\Delta\mathfrak{G}$ is isomorphic to A_5 or* $\mathrm{PSL}(2,7)$.

IV. *$\Delta\mathfrak{G}$ is isomorphic to A_6, with* $q\equiv 1 \pmod 3$.

V. *$\Delta\mathfrak{G}$ is isomorphic to A_7, with $p=5$ and α even.*

(*Note that* $\mathrm{PSL}(2,5)$ *is isomorphic to A_5, and* $\mathrm{PSL}(2,9)$ *to A_6.*)

6. **Proof of Theorem 1.1.** It is clear that subgroups of $\mathrm{SL}(3,q)$ as in Theorem 5.14(I) occur for each value of β. In this section we determine the conditions under which subgroups of the other types mentioned in Theorem 5.14 will occur. We also determine the $\mathrm{GL}(3,q)$-conjugacy classes of these subgroups, and their normalizers in $\mathrm{SL}(3,q)$. Theorem 1.1 will follow easily.

As in §5, $\mathfrak{G}$ will denote the inverse image under Δ of a simple subgroup of $\mathrm{PSL}(3,q)$, and $X=\|1,-1,-1\|$ is an involution in the center of the 2-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$.

LEMMA 6.1. *If $\mathfrak{G}=\{\mathrm{SL}(3,p^\beta),\mathfrak{Z}\}$ with $\beta|\alpha$, then $N(\mathfrak{G})\neq\mathfrak{G}$ if and only if both* $3 \mid (p^\beta-1)$ *and* $3\beta|\alpha$; *in this case, $N(\mathfrak{G})/\mathfrak{G}$ is generated by a matrix $V=\|a^{-2},a,a\|$ such that $V^3\in\mathfrak{G}$.*

Proof. Let $S\in N(\mathfrak{G})$. Since all involutions in $\mathfrak{G}$ are $\mathfrak{G}$-conjugate, there exists an element $G\in\mathfrak{G}$ such that GS commutes with X; i.e., $GS\in C(X)$. Moreover, GS normalizes $\mathfrak{G}$, hence also

$$\mathfrak{G}\cap C(X)=\{\mathrm{GL}(2,p^\beta),\mathfrak{Z}\},$$

hence also $\mathrm{SL}(2,p^\beta)$. The argument used in the last paragraph of the proof of Theorem 3.4 then shows that GS has the form PV where $P\in\mathrm{GL}(2,p^\beta)\subseteq\mathfrak{G}$ and $V=\|a^{-2},a,a\|$, $a\in\mathrm{GF}(q)$. Thus $S\in\mathfrak{G}V$. Similar argument shows that $S\in\mathfrak{G}R$ where $R=\|b,b,b^{-2}\|$, $b\in\mathrm{GF}(q)$. Hence $RV^{-1}\in\mathfrak{G}$, so that $a^3\in\mathrm{GF}(p^\beta)$ and thus $V^3\in\mathfrak{G}$. Conversely, any matrix V of this form (with $a^3\in\mathrm{GF}(p^\beta)$) does in fact normalize $\mathfrak{G}$. The lemma easily follows, if we observe that V is already in $\mathfrak{G}$ unless $p^\beta-1$ and $(q-1)/(p^\beta-1)$ are divisible by 3 (which is equivalent to $3 \mid (p^\beta-1)$, $3\beta|\alpha$).

LEMMA 6.2. *If $\mathfrak{G}=\{U(3,p^\beta),\mathfrak{Z}\}$ with $2\beta|\alpha$, then $N(\mathfrak{G})\neq\mathfrak{G}$ if and only if both* $3 \mid (p^\beta+1)$ *and* $6\beta|\alpha$; *in this case, $N(\mathfrak{G})/\mathfrak{G}$ is generated by a matrix $U=\|b,b,b^{-2}\|$ such that $U^3\in\mathfrak{G}$.*

Proof. Let $S \in N(\mathfrak{G})$. As in the preceding proof, there exists an element $G \in \mathfrak{G}$ such that GS lies in GL(2, q) and normalizes

$$C(X) = \{U^*(2, p^\beta), \mathfrak{Z}\}.$$

Hence there is an element $H \in C(X)$ such that $R = HGS$ commutes with $\|1, \pi, \pi^{k-1}\|$ (where $|\pi| = k = p^\beta + 1$ in $(\mathrm{GF}(q))^*$), and maps the element (5.4) (with $a = b = c = 1$) into an element of $\mathfrak{G}$. This implies (via a short computation) that R has the form $\|a, b, a^{-1}b^{-1}\|$ where $a^{3k} = b^{3k} = 1$. Such a matrix R will in fact normalize $\mathfrak{G}$ if and only if $(ab^{-1})^k = 1$, so that $R \in \mathfrak{G}U$ where $U = \|b, b, b^{-2}\|$. As before, the lemma easily follows.

LEMMA 6.3. *If* $\Delta\mathfrak{G} \cong \mathrm{PSL}(2, p^\beta)$ *for some* β, *then* $\beta | \alpha$ *and* $\mathfrak{G} = \mathfrak{G}_0 \times \mathfrak{Z}$ *where* $\mathfrak{G}_0 \cong \mathrm{PSL}(2, p^\beta)$. *For each value of* β *dividing* α, *such subgroups* $\mathfrak{G}_0$ *exist and are all conjugate in* GL(3, q). *One such subgroup* $\mathfrak{G}_0$ (*for given* β) *is the image of* PSL(2, p^β) *under the isomorphism*

$$\left\|\begin{matrix} a & b \\ c & d \end{matrix}\right\| \to D^{-1} \left\|\begin{matrix} a^2 & 2ab & 2b^2 \\ ac & ad+bc & 2bd \\ c^2/2 & cd & d^2 \end{matrix}\right\| \tag{6.1}$$

where $D = ad - bc$. *The same mapping gives an isomorphism of* PGL(2, p^β) *onto a subgroup* $\mathfrak{G}_1$ *of* SL(3, q), *and* $N(\mathfrak{G}) = \mathfrak{G}_1 \times \mathfrak{Z}$.

Proof. By Schur [21], the representation group of PSL(2, k) is SL(2, k) for $k \neq 9$, which implies that if $|\mathfrak{Z}| = 3$ and $\mathfrak{G}/\mathfrak{Z} \cong \mathrm{PSL}(2, p^\beta)$ then $\mathfrak{G} \neq \mathfrak{G}'$ and hence

$$\mathfrak{G} \cong \mathrm{PSL}(2, p^\beta) \times \mathfrak{Z}.$$

(The latter is still true if $p^\beta = 9$, since here $|\mathfrak{Z}| = 1$.) If such a subgroup $\mathfrak{G}$ exists, then $\mathfrak{G}$ contains elements of orders $(p^\beta - 1)/2$ and $(p^\beta + 1)/2$; each of these elements is conjugate to its inverse, and hence its order divides $q-1$ or $q+1$. Thus $(p^{2\beta} - 1)/4$ divides $(p^{2\alpha} - 1)/2$, so that $\beta | \alpha$. Conversely, for any β dividing α, it is verified directly that the mapping (6.1) is an isomorphism of PSL(2, p^β) onto a subgroup $\mathfrak{G}_0$ of SL(3, q), and of PGL(2, p^β) onto a subgroup $\mathfrak{G}_1 \supseteq \mathfrak{G}_0$; moreover, $\mathfrak{G}_1 \cap \mathfrak{Z} = \{1\}$. It must still be shown that all subgroups isomorphic to $\mathfrak{G}_0$ are conjugate, and that $N(\mathfrak{G}_0)$ is no larger than $\mathfrak{G}_1 \times \mathfrak{Z}$.

The group $\mathfrak{G}_0$ obtained via (6.1) corresponds to a faithful representation $\mathfrak{F}$ of PSL(2, p^β) of degree 3 over GF(q). $\mathfrak{F}$ must be irreducible, since PSL(2, p^β) has no nonprincipal irreducible p-modular representation of degree < 3. (This fact follows either from Theorem 3.4 or from the classification in [9] of the p-modular representations of PSL(2, p^β).) In fact, the results of [9] show that any irreducible p-modular representation $\mathfrak{F}_i$ of degree 3 is obtained from $\mathfrak{F}$ by applying a fixed automorphism θ of GF(p^β) to all matrix coefficients in the representation $\mathfrak{F}$. Under this automorphism, it is clear from (6.1) that the group $\mathfrak{G}_0$ is mapped into

itself. Hence all $\mathfrak{F}_i$ give the same subgroup $\mathfrak{G}_0$ of SL(3, q), and the assertion about conjugacy follows at once.

Let e have order $(p^\beta-1)/2$ in $(\mathrm{GF}(p^\beta))^*$; then $S=\|e, 1, e^{-1}\|$ lies in $\mathfrak{G}_0$. Let $V\in N(\mathfrak{G})$; then by the usual argument there exists $G\in\mathfrak{G}$ such that $Y=VG$ commutes with S. If $p^\beta>5$ (i.e., $|S|\geqq 3$), Y must be a diagonal matrix $\|a, b, c\|$ in SL(3, q). Since $Y\in N(\mathfrak{G})$, and any matrix $\|a_{ij}\|$ in $\mathfrak{G}$ satisfies $2a_{11}a_{13}=a_{12}^2$, it follows easily that, modulo $\mathfrak{Z}$, $b=1$ and $a=c^{-1}$, from which Y is the image of $\|1, c\|\in\mathrm{PGL}(2, p^\beta)$ under (6.1). Thus $N(\mathfrak{G})$ is given correctly by Lemma 6.3. This still holds for $p^\beta=5$, since no element $\notin\mathfrak{Z}$ of SL(3, q) centralizes $\mathfrak{G}$, whereas the automorphism group of PSL(2, 5) is PGL(2, 5).

REMARK. It is possible (although we have not done so here) to avoid representation theory entirely in the proofs of Lemmas 6.3 through 6.6. (This is done in [1] for Lemmas 6.3, 6.4, and 6.5 by use of generating relations and computations with matrices.)

LEMMA 6.4. *Assume $p\neq 5$. If $\Delta\mathfrak{G}\cong\mathrm{PSL}(2, 5)$ (i.e., to A_5), then $\mathfrak{G}=\mathfrak{G}_0\times\mathfrak{Z}$ with $\mathfrak{G}_0\cong A_5$; such subgroups $\mathfrak{G}$ exist if and only if $q\equiv\pm 1$ (mod 10). In this case, $\mathfrak{G}=N(\mathfrak{G})$ and $\mathfrak{G}_0$ is conjugate in* GL(3, q) *to the image of A_5 under the isomorphism defined by* (345) $\to B$, (13)(24) $\to T$ *where*

$$T=\|-1, -1, 1\|; \qquad B=\begin{Vmatrix} -1/2 & 1/2-t & -t \\ t-1/2 & t & -1/2 \\ t & -1/2 & 1/2-t \end{Vmatrix} \tag{6.2}$$

and t satisfies the equation $4t^2-2t-1=0$. Moreover, under this isomorphism we have (234) $\to S$, (12)(34) $\to X$, *where*

$$S=\begin{Vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{Vmatrix}; \qquad X=\|1, -1, -1\|. \tag{6.3}$$

The two choices for t yield conjugate groups $\mathfrak{G}$.

Proof. If T, B are as in (6.2), then $T^2=B^3=(BT)^5=1$, and these are generating relations for A_5 [12, p. 290] which are satisfied by $T=(13)(24)$ and $B=(345)$. One can then obtain (6.3) using the relations $S=TB^{-1}T(BT)^2$, $X=S^{-1}TS$. (Note that the equation $4t^2-2t-1=0$ has a solution in GF(q) if $q\equiv\pm 1$ (mod 10).)

Conversely, if $\Delta\mathfrak{G}\cong A_5$, then $\mathfrak{G}=\mathfrak{G}_0\times\mathfrak{Z}$ with $\mathfrak{G}_0\cong A_5$ by the same argument as in the proof of Lemma 6.3. Here if $p\neq 3$, $\mathfrak{G}_0$ corresponds to an *ordinary* faithful representation of A_5 of degree 3, which must be irreducible as before. The ordinary character-table of A_5 can be found in [21]; the degrees are 1, 3, 3, 4, 5. If χ_1, χ_2 are the characters of degree 3, their values generate the field of $5^{1/2}$. Since a modular irreducible representation can be written in the field of the character, it follows that subgroups $\mathfrak{G}_0\cong A_5$ exist if and only if $5^{1/2}$ exists in GF(q), i.e., $q\equiv\pm 1$ (mod 10).

(In this case, we have already found one such $\mathfrak{G}_0$ explicitly, above.) Moreover, χ_2 is obtained from χ_1 via an outer automorphism of A_5 which permutes the two classes of 5-elements; the same must be true of the representations, and hence the two representations of degree 3 yield the same group $\mathfrak{G}_0$, proving the assertions about conjugacy. As for the case $p=3$, the 3-modular characters of A_5 can easily be found by using the results of [2, I]; they coincide with the ordinary characters of degrees 1, 3, 3, 4, and the same argument as above still works.

Finally, since no element $\notin \mathfrak{Z}$ of SL(3, q) centralizes $\mathfrak{G}$, we must have

$$N(\mathfrak{G})/\mathfrak{Z} \subseteq \mathrm{Aut}\,(\mathfrak{G}) \cong S_5.$$

If $N(\mathfrak{G})/\mathfrak{Z} \cong S_5$, $N(\mathfrak{G})$ contains an element of order 5 conjugate to four of its powers, and this is impossible if $p \neq 5$. Thus $N(\mathfrak{G}) = \mathfrak{G}$, and the proof of Lemma 6.4 is complete.

LEMMA 6.5. *Assume $p \neq 7$. If $\Delta\mathfrak{G} \cong$ PSL(2, 7), then $\mathfrak{G} = \mathfrak{G}_0 \times \mathfrak{Z}$ with $\mathfrak{G}_0 \cong$ PSL(2, 7); such subgroups $\mathfrak{G}$ exist if and only if $q^3 \equiv 1 \pmod 7$. In this case, $\mathfrak{G} = N(\mathfrak{G})$, and $\mathfrak{G}_0$ is conjugate in* GL(3, q) *to the image of* PSL(2, 7) *under the isomorphism defined by* $[1, -1] \to X$,

$$\left\|\begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}\right\| \to E = \left\|\begin{matrix} r & 1/2 & -1/2 \\ r & -1/2 & 1/2 \\ 0 & r+1/2 & r+1/2 \end{matrix}\right\|$$

where $X = \|1, -1, -1\|$ as before, and r satisfies the equation $2r^2 + r + 1 = 0$. The two choices for r yield conjugate groups $\mathfrak{G}$.

Proof. If X, E are as above, then $X^2 = E^7 = (EX)^3 = (XE^3)^4 = 1$ and these relations generate PSL(2, 7) [12, p. 303]. Hence the given mapping is an isomorphism of PSL(2, 7) onto a subgroup $\mathfrak{G}_0$ of SL(3, q), provided that the equation $2r^2 + r + 1 = 0$ has a solution, i.e., $(-7)^{1/2}$ exists in GF(q); this will occur if and only if $q^3 \equiv 1 \pmod 7$. The remainder of the proof is like that of Lemma 6.4; there are two ordinary characters χ_1, χ_2 of PSL(2, 7) of degree 3. Their values generate the field of $(-7)^{1/2}$, and $\chi_1 \to \chi_2$ under the outer automorphism θ of PSL(2, 7) which maps $X \to X$, $E \to E^{-1}$. For $p = 3$, the 3-modular characters of PSL(2, 7) coincide with the ordinary characters of degrees $\neq 8$. The restriction on q and the assertions about conjugacy now follow just as in the preceding proof. So does the assertion about $N(\mathfrak{G})$: if $N(\mathfrak{G}) > \mathfrak{G}$ then $N(\mathfrak{G})/\mathfrak{Z}$ must be isomorphic to PGL(2, 7) = Aut($\mathfrak{G}_0$) and hence contains an element of order 7 conjugate to six of its powers; this is impossible if $p \neq 7$.

LEMMA 6.6. *Assume $p \neq 3$. If $\Delta\mathfrak{G}$ is isomorphic to* PSL(2, 9) (*i.e., to A_6*), *then*

$$\mathfrak{G} = \mathfrak{G}'; \qquad |\mathfrak{Z}| = 3; \qquad \mathfrak{G}/\mathfrak{Z} \cong A_6 \tag{6.4}$$

and (6.4) *determines the structure of $\mathfrak{G}$ uniquely. Such subgroups $\mathfrak{G}$ exist if and only*

if either (a) $q=5^\alpha$, α *even*; *or* (b) $q\equiv 1$ *or* 19 (mod 30). *In either case,* $\mathfrak{G}$ *is* GL(3, q)*-conjugate to the subgroup* $\{\mathfrak{G}_0, \mathfrak{Z}, V\}$, *where* $\mathfrak{G}_0=\{T, B\}$ *as given explicitly by* (6.2) (*without the restriction* $p\neq 5$), *and*

$$V=\begin{Vmatrix} -1 & 0 & 0 \\ 0 & 0 & -\eta \\ 0 & -\eta^2 & 0 \end{Vmatrix} \qquad (\eta^3=1\neq\eta). \tag{6.5}$$

The two groups $\mathfrak{G}$ *determined by the two choices for* η *are conjugate in* GL(3, q). *In case* (b), $N(\mathfrak{G})=\mathfrak{G}$. *In case* (a), $|N(\mathfrak{G}):\mathfrak{G}|=2$ *and* $N(\mathfrak{G})/\mathfrak{G}$ *is generated by the matrix*

$$U=\begin{Vmatrix} \eta & 0 & 0 \\ 0 & \zeta & \zeta\eta \\ 0 & \zeta\eta^2 & -\zeta \end{Vmatrix} \tag{6.6}$$

where $\zeta=\eta^2-1$.

Proof. Assume that q has one of the values (a) or (b). Then $q\equiv 1$ (mod 3) so that the element V of (6.5) exists in SL(3, q). Let $\mathfrak{G}=\{\mathfrak{G}_0, \mathfrak{Z}, V\}$ where $\mathfrak{G}_0$ is as above. Let $A_1=S$, $A_2=X$ (as in Lemma 6.4), $A_3=B^{-1}TBS$, $A_4=V$, and $K=\eta I\in\mathfrak{Z}$; then the A_i and K generate $\mathfrak{G}$, and it is a direct computation that these elements satisfy Schur's generating relations [22, p. 242] for the representation group $\mathfrak{R}$ of A_6. (We write A_i instead of Schur's C_i since we have used C_u to mean something else.) Hence $\mathfrak{G}$ is a factor group of $\mathfrak{R}$. Since $\mathfrak{R}=\mathfrak{R}'$, $|Z(\mathfrak{R})|=6$, $\mathfrak{R}/Z(\mathfrak{R})=A_6$, $|Z(\mathfrak{G})|=|\mathfrak{Z}|=3$ and $\mathfrak{G}\supseteq\mathfrak{G}_0\cong A_5$, it follows that $\mathfrak{G}$ satisfies (6.4). Since by [22] A_6 has just one representation group, (6.4) must determine the structure of $\mathfrak{G}$ uniquely (cf. [21, pp. 96–99]).

Conversely, suppose $\mathfrak{G}\subseteq$SL(3, q) with $\Delta\mathfrak{G}\cong A_6$. Then q must have one of the values (a) or (b), by Theorem 5.14 and Lemma 6.4. Clearly $\mathfrak{G}$ must contain (up to conjugacy) the subgroup $\mathfrak{G}_0\cong A_5$ which is generated by the matrices (6.2), (6.3). Also, $\mathfrak{G}$ contains an element V of order 2 which corresponds (homomorphically) to the element (34)(56) of A_6. Then V maps $X\to X$, $T\to XT$, showing already that V has zeros in the proper positions (cf. (6.5)); in addition, $|V|=2$, $(SV)^2\in\mathfrak{Z}$, and VB is conjugate to B (modulo $\mathfrak{Z}$) and hence has trace zero. It follows that V is given correctly by (6.5); clearly $\mathfrak{G}=\{\mathfrak{G}_0, \mathfrak{Z}, V\}$. Moreover, let V_1, V_2 be the two elements (6.5) corresponding to the two cube roots $\eta=\eta_1$, η_2. Let $\mathfrak{G}_1$, $\mathfrak{G}_2$ be the corresponding subgroups of SL(3, q). Then the matrix

$$\begin{Vmatrix} -(\eta_1^2+2\eta_1 t) & 0 & 0 \\ 0 & 1 & \eta_1 \\ 0 & \eta_1 & -\eta_1^2 \end{Vmatrix}$$

maps $T\to V_2$, $V_1\to T$, $B\to B^{XT}V_2BV_2(\eta_2 I)$ and hence $\mathfrak{G}_1\to\mathfrak{G}_2$. Thus the lemma is proved except for the assertions about $N(\mathfrak{G})$.

$\mathfrak{G}$ is generated by elements Y of order 2, cf. [22, p. 242]. If $\theta \in \mathrm{Aut}(\mathfrak{G})$ and θ induces the identity automorphism of $\mathfrak{G}/\mathfrak{Z} = A_6$, then $\theta(Y)$ lies in $Y\mathfrak{Z}$ and has order 2, so that $\theta(Y) = Y$ and hence $\theta = I$. By [23, §11.4], $\mathrm{Aut}(A_6)$ has index 4 over the inner automorphisms. In view of the assertion already proved about conjugacy, it follows that, if $|N(\mathfrak{G}) : \mathfrak{G}| = k$, $\mathfrak{G}$ has at most $4/k$ distinct faithful representations of degree 3 over GF(q) (such representations must lie in SL(3, q) since $\mathfrak{G} = \mathfrak{G}'$). In case (b) of Lemma 6.6 these coincide with the ordinary representations; by [22, pp. 242–244] there are four such representations of $\mathfrak{G}$, and hence $k = 1$, $N(\mathfrak{G}) = \mathfrak{G}$. (The characters lie in the field generated by $5^{1/2}$ and the cube roots of unity, and these quantities exist in GF(q).) In case (a) with $p = 5$, the methods of [2, *I*] give only two 5-modular representations of degree 3, since here two pairs of ordinary representations coincide over GF(5^α). Hence in this case, $4/k \geqq 2$ and $|N(\mathfrak{G}) : \mathfrak{G}| \leqq 2$. On the other hand, the element (6.6) does produce an outer automorphism of $\mathfrak{G}$, namely

$$X \to X, \qquad V \to T, \qquad T \to V, \qquad B \to B^{XTV}B(\eta^2 I) \tag{6.7}$$

and hence indeed $|N(\mathfrak{G}) : \mathfrak{G}| > 1$. The entire lemma is thus proved. (The mapping (6.7) is not inner since B corresponds to a 3-cycle in A_6 while its image does not.)

REMARKS. (1) The argument of the last paragraph could have been used to obtain $N(\mathfrak{G})$ in Lemmas 6.4 and 6.5 also. (2) It follows from this argument that $\mathfrak{G}$ has as many automorphisms as A_6, and thus $\mathrm{Aut}(\mathfrak{G}) = \mathrm{Aut}(A_6)$, an interesting result in itself.

LEMMA 6.7. *If $q = 5^\alpha$ and α is even, then* SL(3, q) *has subgroups $\mathfrak{G}$ such that $\Delta\mathfrak{G} \cong A_7$. All such subgroups $\mathfrak{G}$ satisfy*

$$\mathfrak{G} = \mathfrak{G}'; \qquad |\mathfrak{Z}| = 3; \qquad \mathfrak{G}/\mathfrak{Z} \cong A_7 \tag{6.8}$$

and are conjugate in GL(3, q) *to the subgroup $\{\mathfrak{G}_0, \mathfrak{Z}, V, W\}$ where $\mathfrak{G}_0$, V are as in Lemma* 6.6 *and $W = \|1, \eta, \eta^2\|$. For such $\mathfrak{G}$, $N(\mathfrak{G}) = \mathfrak{G}$.* (6.8) *determines the structure of $\mathfrak{G}$ uniquely.*

Proof. If the elements A_i, K are as in the proof of Lemma 6.6 (first paragraph) and we let $A_5 = VW$, then by direct computation the elements $A_1, \ldots, A_5, K$ satisfy Schur's generating relations [22, p. 246] for the representation group of A_7. The same argument as in Lemma 6.6 then shows that $\mathfrak{G} = \{\mathfrak{G}_0, \mathfrak{Z}, V, W\}$ satisfies (6.8) and that (6.8) determines the structure of $\mathfrak{G}$. Conversely, if $\Delta\mathfrak{G} \cong A_7$ then by Lemma 6.6 $\mathfrak{G}$ must contain (up to conjugacy) the subgroup $\{\mathfrak{G}_0, \mathfrak{Z}, V\}$ together with an element corresponding to (567) $\in A_7$. This element must commute (modulo $\mathfrak{Z}$) with the elements X, T, and S of Lemma 6.4, and hence is equal (mod $\mathfrak{Z}$) to W or W^{-1}, showing that $\mathfrak{G}$ is given correctly by Lemma 6.7. Finally, since $p \neq 7$, reasoning as in Lemma 6.4 gives $N(\mathfrak{G}) = \mathfrak{G}$.

Combining Lemmas 6.1 through 6.7 with Theorem 5.14 (and, of course, the result of [14]), we see that the simple nonabelian subgroups $\Delta\mathfrak{G}$ of PSL(3, q),

and the normalizers of these subgroups, constitute precisely the list of subgroups given in Theorem 1.1. Now consider an arbitrary subgroup $\mathfrak{H} \neq \{1\}$ of PSL(3, q), and let $\mathfrak{K}$ be a minimal (nontrivial) normal subgroup of $\mathfrak{H}$. Then $\mathfrak{K}$ has no proper characteristic subgroup except $\{1\}$, and is hence the direct product $\mathfrak{K} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_r$ of isomorphic simple groups. If $\mathfrak{H}$ has no normal elementary-abelian subgroup $\neq \{1\}$ then the $\mathfrak{G}_i$ are non-abelian. Thus $\mathfrak{G}_i$ is one of our groups $\Delta\mathfrak{G}$, and

$$|\mathfrak{K} : \mathfrak{G}_1| \leqq |N(\mathfrak{G}_1) : \mathfrak{G}_1| \leqq 3$$

so that $r = 1$, $\mathfrak{K} = \mathfrak{G}_1$, $\mathfrak{H} \subseteq N(\mathfrak{G}_1)$, i.e., $\mathfrak{H}$ is equal to $\mathfrak{G}_1$ or $N(\mathfrak{G}_1)$. The proof of Theorem 1.1 is complete.

7. **Subgroups not satisfying Theorem 1.1.** In this section, changing notation, we use $\mathfrak{G}$ to represent a subgroup of PSL(3, q) and $\#\mathfrak{G}$ for the inverse image of $\mathfrak{G}$ in SL(3, q).

The subgroups $\mathfrak{G}$ of PSL(3, q) not covered by Theorem 1.1 are those having a normal elementary-abelian subgroup $\mathfrak{H}$ different from $\{1\}$. $\mathfrak{H}$ is then either a p-group or one of the three cases (5.8). In case (i) of (5.8), $C(\mathfrak{H})$ is cyclic and

$$|\mathfrak{G} : C(\mathfrak{H})| \leqq |N(\mathfrak{H}) : C(\mathfrak{H})| \leqq 3$$

since a generator of $\mathfrak{H}$ is conjugate to at most three of its powers.

Suppose $\mathfrak{H}$ is instead a diagonal subgroup (case (ii)). If $\mathfrak{H}$ contains an element H with three distinct characteristic roots (it is clear what we mean by this even though H is in PSL(3, q), not SL(3, q)), or if $\mathfrak{H}$ is the four-group, then $\#C(\mathfrak{H})$ is diagonal and $\#N(\mathfrak{H})/\#C(\mathfrak{H})$ is generated by permutation matrices. If every element of $\mathfrak{H}$ has two equal characteristic roots but $|\mathfrak{H}| \neq 4$, then it is not hard to show that the root which only appears once must occur in the same position in each element of $\mathfrak{H}$, and hence $\mathfrak{G} = N(\mathfrak{H}) = C(\mathfrak{H})$ is a subgroup of GL(2, q)/$\mathfrak{Z}$.

Consider case (iii) of (5.8), $\mathfrak{H} = \Delta\{W, Y\}$. Let $\mathfrak{G}^*$ be the full normalizer of $\mathfrak{H}$ in PSL(3, q^3); then $\mathfrak{H} \subseteq \mathfrak{G} \subseteq \mathfrak{G}^*$. It is easy to show that $\mathfrak{H}$ is its own full centralizer in PSL(3, q^3); hence $\mathfrak{G}^*/\mathfrak{H}$ is isomorphic to a subgroup $\mathbf{\Gamma}_*$ of the group $\mathbf{\Gamma} = \mathrm{Aut}(C_3 \times C_3)$. Letting $a = (1-\eta)^{-1}$ and letting ε be a cube root of η in GF(q^3), the matrices

$$A = \|\varepsilon, \varepsilon, \varepsilon^{-2}\|; \quad B = a \cdot \|\eta^{(i-1)(j-1)}\| \qquad (i, j = 1, 2, 3)$$

(which do have determinant 1) act on $\mathfrak{H}$ as automorphisms of order 3 and 4 and hence generate the derived group $\mathbf{\Gamma}'$ of $\mathbf{\Gamma}$ (cf. Theorem 3.2; clearly $\mathbf{\Gamma}$, $\mathbf{\Gamma}'$ are isomorphic to GL(2, 3), SL(2, 3) respectively). On the other hand, $\mathbf{\Gamma}_*$ is not all of $\mathbf{\Gamma}$, since no matrix maps $W \to W$, $Y \to Y^{-1}$ (not even mod $\mathfrak{Z}$). Hence $\mathbf{\Gamma}_* = \mathbf{\Gamma}'$, and $\mathfrak{G}/\mathfrak{H}$ is a subgroup of $\mathbf{\Gamma}'$. (If $q \not\equiv 1 \pmod 9$ then $A \notin \mathrm{SL}(3, q)$, but B and its $\mathbf{\Gamma}_*$-conjugates still lie in SL(3, q) and generate the quaternion subgroup of $\mathbf{\Gamma}_*$.)

Finally, suppose $\mathfrak{H}$ is a p-group. We may assume $\mathfrak{H} \subseteq \Delta\mathfrak{S}$ where

$$\mathfrak{S} = \{\|a_{ij}\| : a_{12} = a_{13} = a_{23} = 0,\ a_{11} = a_{22} = a_{33} = 1\}.$$

For any $A \in \#\mathfrak{H}$ and $B = \|b_{ij}\| \in \#N(\mathfrak{H})$, we have $AB \in B\mathfrak{S}$, which implies (after a computation) that $b_{13} = 0$. This is true for any element B of $\#\mathfrak{G}$ and hence for all products of such elements, from which it follows that either $b_{23} = 0$ (all $B \in \#\mathfrak{G}$) or $b_{12} = 0$ (all $B \in \#\mathfrak{G}$). Thus, up to conjugacy by the matrix $[-1, -1, 1]$ and/or the inverse-transpose isomorphism, $\#\mathfrak{G} \subseteq \mathfrak{M}$ where $\mathfrak{M}$ is the group of all matrices $C = \|c_{ij}\|$ in SL(3, q) for which $c_{12} = c_{13} = 0$. If $\mathfrak{Q}$ is the p-subgroup of $\mathfrak{M}$ for which $c_{23} = c_{32} = 0$, then $\mathfrak{Q}$ is normal in $\mathfrak{M}$ and $\mathfrak{K} = \mathfrak{Q} \cap \#\mathfrak{G}$ is normal in $\#\mathfrak{G}$, with $\#\mathfrak{G}/\mathfrak{K}$ isomorphic to a subgroup of $\mathfrak{M}/\mathfrak{Q}$, which in turn is isomorphic to GL(2, q).

Summarizing our results, we have

THEOREM 7.1. *Let $\mathfrak{G}$ be a subgroup of* PSL(3, q) *not satisfying the hypothesis of Theorem* 1.1. *Then one of the following occurs*:

(1) *$\mathfrak{G}$ has a cyclic p-regular normal subgroup of index $\leqq 3$.*

(2) *$\mathfrak{G}$ has a diagonal normal subgroup $\mathfrak{K}$ such that $\mathfrak{G}/\mathfrak{K}$ is isomorphic to a subgroup of S_3.*

(3) *$\#\mathfrak{G}$ has a normal elementary-abelian p-subgroup $\mathfrak{K}$ such that $\#\mathfrak{G}/\mathfrak{K}$ is isomorphic to a subgroup of* GL(2, q) (cf. *Theorem* 3.4). *We include the case $\mathfrak{K} = \{1\}$.*

(4) $q \equiv 1 \pmod 9$; *$\mathfrak{G}$ has a normal subgroup $\mathfrak{H}$, abelian of type* (3, 3), *with $\mathfrak{G}/\mathfrak{H}$ isomorphic to a subgroup of* SL(2, 3). *All subgroups of* SL(2, 3) *do occur in this context.*

(5) $q \equiv 1 \pmod 3$, $q \not\equiv 1 \pmod 9$; *$\mathfrak{G}$ has a normal subgroup $\mathfrak{H}$, abelian of type* (3, 3), *with $\mathfrak{G}/\mathfrak{H}$ isomorphic to a subgroup of the quaternion group $\mathfrak{Q}$ of order* 8. *All subgroups of $\mathfrak{Q}$ do occur in this context.*

BIBLIOGRAPHY

1. D. M. Bloom, *On the subgroups of* SL(3, q), Ph.D. Thesis, Harvard Univ., Cambridge, Mass. 1963.

2. R. Brauer, *On groups whose order contains a prime number to the first power*. I, II, Amer. J. Math. **64** (1942), 401–420, 421–440.

3. ———, *Investigations on groups of even order*. I, Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 1891–1893.

4. ———, *Some applications of the theory of blocks of characters of finite groups*. II, J. Algebra **1** (1964), 307–334.

5. ———, *Some applications of the theory of blocks of characters of finite groups*. III, J. Algebra **3** (1966), 225–255.

6. ———, *On finite Desarguesian planes*. II, Math. Z. **91** (1966), 124–151.

7. ———, *Investigations on groups of even order*. II, Proc. Nat. Acad. Sci. U.S.A. **55** (1966), 254–259.

8. R. Brauer and W. Feit, *On the number of irreducible characters of finite groups in a given block*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 361–365.

9. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. **42** (1941), 556–590.

10. R. Brauer and M. Suzuki, *On finite groups of even order whose 2-Sylow group is a quaternion group*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 1757–1759.

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

12. L. E. Dickson, *Linear groups, with an exposition of the Galois field theory*, Teubner, Leipzig, 1901.

13. V. Ennola, *On the characters of the finite unitary groups*, Ann. Acad. Sci. Fenn. Ser. A I No. 323 (1963), 35 pp.

14. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 711–1029.

15. D. Gorenstein and J. Walter, *On finite groups with dihedral Sylow 2-subgroups*, Illinois J. Math. **6** (1962), 553–593.

16. ———, *The characterization of finite groups with dihedral Sylow 2-subgroups*. I, J. Algebra **2** (1965), 85–151.

17. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

18. R. W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the* GF(2^n), Ann. of Math. **27** (1925), 140–158.

19. H. H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), 207–242.

20. I. Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen*, Math.-Natur. Kl. (1905), 77–91.

21. ———, *Untersuchen über die Darstellung der endlichen Gruppen durch gebrochenen linearen Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

22. ———, *Über Darstellung der symmetrischen und der alternieren Gruppen durch gebrochenen linearen Substitutionen*, J. Reine Angew. Math. **139** (1911), 155–250.

23. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.

24. Sister E. L. Michaels, *A study of simple groups of even order*, Ph.D. Thesis, Univ. of Notre Dame, Notre Dame, Ind., 1963.

25. R. Steinberg, *The representations of* GL(3, q), GL(4, q), PGL(3, q), *and* PGL(4, q), Canad. J. Math. **3** (1951), 225–235.

26. M. Suzuki, *On finite groups containing an element of order four which commutes only with its powers*, Illinois J. Math. **3** (1959), 255–271.

27. ———, *Applications of group characters*, Proc. Sympos. Pure Math., Vol. 1, pp. 88–99, Amer. Math. Soc., Providence, R. I., 1959.

28. ———, *Finite groups in which the centralizer of any element of order 2 is 2-closed*, Ann. of Math. **82** (1965), 191–212.

BROOKLYN COLLEGE,
BROOKLYN, NEW YORK