ON PRIMITIVE PERMUTATION GROUPS WHOSE STABILIZER OF A POINT INDUCES $L_2(q)$ ON A SUBORBIT

BY

ULRICH DEMPWOLFF

1. Introduction

In the following we consider primitive permutation groups G acting on a finite set Ω. If $\alpha \in \Omega$ then G_α has a suborbit $\Delta(\alpha)$ such that the group $G_\alpha^{\Delta(\alpha)}$ induced on $\Delta(\alpha)$ is isomorphic to $L_2(q)$ and $|\Delta(\alpha)| = q + 1$, where $q \geq 4$ and $q = p^n$, p a prime. We state:

THEOREM. *Suppose G satisfies the above conditions then either*
(a) $G_\alpha \simeq L_2(q)$ *or*
(b) $p > 2$ *and* $G_\alpha \simeq L_2(q) \times Y$ *where Y is isomorphic to the normalizer of a S_p-subgroup in $L_2(q)$.*

The proof of the theorem will follow to a great extent the pattern of the work of C. C. Sims [9]. In this way we get bounds for $|G_\alpha|$ and structural informations of G_α. Then we use results about irreducible $F_p[L_2(q)]$-modules. In the case $p = 2$ also "2-local arguments" will enter. The notation is standard (see [4] and [14]).

2. Preliminary lemmas

In this section we collect some—mostly known—results, which will be used repeatedly.

PROPOSITION 2.1 (Walter, also see [1]). *Let G be a finite group having abelian S_2-subgroups. Then G possesses a normal subgroup H of odd index, such that*

$$H/O(H) \simeq X_0 \times X_1 \times \cdots \times X_n$$

where X_0 is an abelian 2-group and X_i $(1 \leq i \leq n)$ are finite simple groups isomorphic to $L_2(q)$, q suitable, or of type "Janko-Ree" (for the definition of type "Janko-Ree" see [1]).

PROPOSITION 2.2 (Gilman, Gorenstein [2]). *Let G be a finite simple group and $S \in Syl_2(G)$. Suppose* cl $(S) = 2$. *Then G is isomorphic to one of the following groups:*

$$L_2(q),\ q \equiv 7, 9 \ (\text{mod } 16),\ A_7,\ Sz(2^n),\ U_3(2^n),\ L_3(2^n),\ or\ PSp(4, 2^n).$$

Received January 15, 1975.

PROPOSITION 2.3 (Goldschmidt [3]). *Let G be a finite group and $1 \neq A \subseteq S \in Syl_2(G)$, A abelian. Suppose that for all $a \in A^{\#}$ always $a^g \in S$ implies $a^g \in A$. Then if $\bar{K} = \langle A^G \rangle / O/(\langle A^G \rangle)$ we have:*

(i) *$\bar{K}$ is a central product of an abelian 2-group and quasisimple groups X such that either $X/Z(X)$ has abelian S_2-subgroups or $X/Z(X)$ is isomorphic to $Sz(2^n)$ or $U_3(2^n)$.*

(ii) *$\bar{A} = O_2(\bar{K})\Omega_1(\bar{T})$ for some $A \subseteq T \in Syl_2(K)$.*

LEMMA 2.4 (Thompson [13; 5.38]). *Let G be a finite group and $S \in Syl_2(G)$. Suppose $S^* \subset S$, $|S: S^*| = 2$ and $t \in S - S^*$ is an involution, which is not conjugate to any element in S^*. Then G has a normal subgroup G^* of index 2.*

LEMMA 2.5 (Gilman, Gorenstein [2; (2.66)]). *Let V be a $2n$-dimensional F_2-vectorspace and $SL(2, 2^n) \simeq X \subseteq GL(V)$ such that V is an irreducible X-space. Assume further $[S, V] = C_V(S)$, $\dim C_V(S) = n$ for $S \in Syl_2(X)$. Then V is a standard module of X.* (Here standard module M of $SL(2, q)$ means a 2-dimensional F_q-vectorspace such that $SL(2, q)$ acts on M as $SL(M)$).

LEMMA 2.6. *Let V be a $2n$-dimensional F_p-vectorspace and $X \simeq SL(2, p^n)$ be represented irreducibly on V and $p^n \geq 4$. Suppose $S \in Syl_p(X)$ and $[S, V] = C_V(S)$, $\dim C_V(S) = n$. Then X is faithful on V.*

Proof. Since $SL(2, 2^n) \simeq L_2(2^n)$, we may assume that p is odd.

In X there is an element x of order 4 such that $\langle x, S \rangle = X$ and $x \in N_X(K)$, where K is a p-complement of S in $N_X(S)$.

Set $V_0 = C_V(S)$ and $V_1 = V_0^x$. Suppose that X is not faithful. Then x^2 induces the identity on V and so $V_0 \cap V_1$ is centralized by $X = \langle x, S \rangle$. Hence $V = V_0 \oplus V_1$. According to this decomposition we can find a basis of V such that x corresponds to the matrix

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

and the elements in S to matrices

$$\begin{pmatrix} I & 0 \\ A & I \end{pmatrix}$$

where I is the n-dimensional identity matrix and A is a suitable $(n \times n)$-matrix. There is further $s \in S$ with $|xs| = 3$ (for instance if

$$x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

then $|xs| = 3$ in $SL(2, p^n)$). Since x and s are described by matrices as above the matrix corresponding to $(xs)^3$ has the form

$$\begin{pmatrix} A^3 + 2A & A^2 + I \\ A^2 + I & A \end{pmatrix}.$$

Hence $A = I$ and $A^2 + I = I + I = 2I = 0$ follows, contradicting Char $F_p \neq 2$.

LEMMA 2.7. *Let S be a S_2-subgroup of type $L_3(q)$, q even. Let K be a subgroup of odd order in* Aut (S) *such that the semidirect product $K \cdot S$ contains U the normalizer of a S_2-subgroup in a split extension of the standard module V of order q^2 by $SL(2, q)$. Suppose that t is an involution in* Aut (S) *normalizing K and interchanging the two elementary abelian subgroups of order q^2 in S. Set $T = S\langle t \rangle$ and take an involution $x \in T - S$. We have two cases.*

(i) *$Z(T) = Z(S)$ and $W = [x, S]$ is homocyclic of exponent* 4 *and order q^2. $Z(S) = \Omega_1(W)$ and $C_T(x) = Z(S)\langle x \rangle$.*

(ii) *$Z(T) \neq Z(S)$. Then $|C_S(x)| = |[S, x]| = q\sqrt{q}$. $Z(T) = C_{Z(S)}(x)$ has order $\sqrt{q}$.*

In both cases all involutions in $T - S$ are conjugate under S.

Proof. Consider S/Z as pairs (b, c) with $b, c \in F_q$ and $Z = Z(S)$ we identify with elements $a \in F_q$. The effect of squaring is described by $(b, c)^2 = bc$ and the commutator map by $[(b, c), (e, f)] = bf + ce$. Now $(b, c)^t = (c^{\alpha_1}, b^{\alpha_2})$ and

$$\begin{aligned}(c^{\alpha_1}, b^{\alpha_2}) + (e^{\alpha_1}, f^{\alpha_2}) &= ((b, c) + (f, e))^t\\ &= (b + f, c + e)^t\\ &= ((c + e)^{\alpha_1}, (b + f)^{\alpha_2}).\end{aligned}$$

So α_1, α_2, and α_3 are F_2-homomorphisms, where $a^t = a^{\alpha_3}$. $t^2 = 1$ gives $\alpha_3^2 = 1$ and $\alpha_1\alpha_2 = 1$. Further,

$$\begin{aligned}(be)^{\alpha_3} &= (be)^t\\ &= [(b, 0), (0, e)]^t\\ &= [(0, b^{\alpha_2}), (e^{\alpha_1}, 0)]\\ &= b^{\alpha_2}e^{\alpha_1}.\end{aligned}$$

Suppose first, that t centralizes Z. Then $\alpha_3 = 1$.

Suppose now, that t does not centralize Z. K induces a cyclic group of order $q - 1$ on Z permuting transitively the elements in $Z^{\#}$. If we replace t if necessary by a suitable conjugate in $K\langle t \rangle$ we see by the structure of $GL(n, 2)$, $q = 2^n$, that α_3 acts as an involutory field automorphism on $Z = F_q$. Thus $1^{\alpha_3} = 1$ and so $1^{\alpha_2}(e^{\alpha_1} + g^{\alpha_1}) = e^{\alpha_3} + g^{\alpha_3}$. Since $\alpha_2^{-1} = \alpha_1$ it follows that $a^{\alpha_3} = 1^{\alpha_i - 1}a^{\alpha_i}$ for all $a \in F_q$ and $1 \leq i \leq 2$.

In the case $Z = Z(T)$ we have that $C_K(t)$ induces a cyclic group of order $q - 1$ on Z acting transitively on Z. Since $|[S, t]Z/Z| = q$ it follows immediately that $[t, S]$ is homocyclic of exponent 4 and order q^2 being inverted by t. So every element in $t[S, t]$ is an involution and all involutions in $T - S$ are conjugate in S.

If $Z \neq Z(T)$ and $a \in [t, S]$ then exactly $\sqrt{q}$ elements in taZ are involutions. Hence there are $q\sqrt{q} = |S; C_S(t)|$ involutions in $T - S$ and all of them are conjugate in S.

LEMMA 2.8. *Let p be a prime number and fix $P \in Syl_p(G)$. Consider the set $\mathfrak{X}$ of subgroups X of P that satisfy the following conditions:*

(1) *X is a tame Sylow intersection with P* (for notation see [4]).

(2) $C_P(X) \subseteq X$.

(3) $X \in Syl_p(O_{p',p}(N_G(X)))$.

(4) *$X = P$ or $N_G(X)/X$ is p-isolated.*

Form the set $\mathfrak{T}$ of all pairs (X, N) with $X \in \mathfrak{X}$ and

$$N = N_G(X) \quad \text{if } X = C_P(\Omega_1(Z(X)))$$

and

$$N = N_G(X) \cap C_G(\Omega_1(Z(X))) \quad \text{if } X \subset C_P(\Omega_1(Z(X))).$$

If $x, y \in P$ and $x \sim y$ in G, then there exist $(X_i, N_i) \in \mathfrak{T}$ $(1 \leq i \leq m)$ and elements $x_i \in X_i$, $n_i \in N_i$ such that $x = x_1$, $x_i^{n_i} = x_{i+1}$ for $1 \leq i \leq m - 1$, and $x_m^{n_m} = y$.

For the proof see [11].

3. s-arcs

This section corresponds closely to Section 5 of [9]. Thus we have a graph whose set of points is Ω and α is connected with β if and only if $\beta \in \Delta(\alpha)$.

LEMMA 3.1. (i) $G_\alpha^{\Delta(\alpha)} \simeq G_\alpha^{\Delta'(\alpha)}$.

(ii) *If r is a prime number dividing $q + 1$ then r does not divide $|G_{\alpha,\beta}|$ for $\beta \in \Delta(\alpha)$, except $r = 2$ and $q \equiv 1 \pmod 4$.*

(iii) *If $\beta \in \Delta(\alpha)$ then $|G_{\alpha,\beta}^{\Delta(\alpha)}| = |G_{\alpha,\beta}^{\Delta(\beta)}|$.*

Proof. (i) is true because of [6; 3.2].

(ii) follows by (i) and the proof of [8; Theorem 3].

(iii) $G_{\alpha,\beta}$ is a subgroup of index $q + 1$ in G_α and G_β. We have $G_{\alpha,\Delta(\alpha)} \subseteq G_{\alpha,\beta}$. Suppose $G_{\beta,\Delta(\beta)} \nsubseteq G_{\alpha,\beta}$. Then

$$|G_\beta^{\Delta(\beta)} : G_{\alpha,\beta}^{\Delta(\beta)}| < q + 1$$

and this index divides $q + 1$. Hence by the structure of $L_2(q) \simeq G_\beta^{\Delta(\beta)}$, we have $L_2(q) \simeq G_{\alpha,\beta}^{\Delta(\beta)}$. Take now a prime r such that r divides $q + 1$ but not divides $|G_{\alpha,\beta}|$. Such a prime always exists, because for $q \equiv 1 \pmod 4$ we have $q \not\equiv -1 \pmod 4$ and $q + 1 \geq 5$ together with (ii) then provides us with the existence of such an r. So r divides $|G_{\alpha,\beta}^{\Delta(\beta)}|$ and also $|G_{\alpha,\beta}|$, a contradiction.

DEFINITION. For $\beta \in \Delta(\alpha)$ define $\Gamma(\alpha, \beta)$ as the orbit of length q of $G_{\alpha,\beta}^{\Delta(\beta)}$ and set

$$\Gamma'(\beta, \gamma) = \{\alpha \mid \beta \in \Delta(\alpha), \gamma \in \Gamma(\alpha, \beta)\} \quad \text{for } \gamma \in \Delta(\beta).$$

Set $O = \{(\alpha, \beta, \gamma) \mid \beta \in \Delta(\alpha), \gamma \in \Gamma(\alpha, \beta)\}$.

LEMMA 3.2. *If $\gamma \in \Delta(\beta)$, then $\Gamma'(\beta, \gamma)$ is an orbit of $G_{\beta,\gamma}^{\Delta'(\beta)}$ and $|\Gamma'(\beta, \gamma)| = q$.*

Proof. With 3.1 repeat the proof of [9; 5.6].

DEFINITION. Call a sequence X of points $\alpha_0, \ldots, \alpha_s$ in Ω an s-arc if $(\alpha_i, \alpha_{i+1}, \alpha_{i+2}) \in O$ for $0 \leq i \leq s-2$. An s-arc $\alpha_1, \ldots, \alpha_{s-1}, \alpha_s, \beta$ is called a successor of X and an s-arc $\gamma, \alpha_0, \alpha_1, \ldots, \alpha_{s-1}$ is called a predecessor of X. Suppose X and Y are s-arcs and there is a sequence $X = X_1, X_2, \ldots, X_k = Y$ such that X_i is a predecessor or a successor of X_{i+1} for $1 \leq i \leq k-1$. Then we say that X is equivalent to Y ($X \sim Y$).

LEMMA 3.3. (i) *The number of s-arcs is* $|\Omega|(q+1)q^{s-1}$.
(ii) $X \sim Y$ *for all s-arcs X and Y.*

Proof. It is obvious that the proofs of [9; 5.7–5.10] can be adapted to our situation.

4. The order of an S_p-subgroup of G_α

LEMMA 4.1. *If G is transitive on the s-arcs but not transitive on the* $(s+1)$*-arcs, then* $|G_\alpha|_p = q^{s-1}$.

Proof. Let H be the stabilizer of the s-arc X; $\alpha_0, \ldots, \alpha_s$. Since G is transitive on O we have $s \geq 2$. Clearly, $|G_{\alpha_0}: H| = (q+1)q^{s-1}$ by 3.3. Since $|G_{\alpha_{s-1}, \alpha_s}|_\pi = |H|_\pi$, where $\pi = \pi(G_{\alpha_{s-1}, \alpha_s}) - \{p\}$, it follows that $H^{\Delta(\alpha_s)}$ induces an orbit at least of length $q-1$ (or two orbits of length $(q-1)/2$) on $\Gamma(\alpha_{s-1}, \alpha_s)$. If p divides $H^{\Delta(\alpha_s)}$, then H would act transitively on $\Gamma(\alpha_{s-1}, \alpha_s)$, since nontrivial elements of order p in $H^{\Delta(\alpha_s)}$ would act fixed-point-free. Hence G would be transitive on the $(s+1)$-arcs, a contradiction. So p does not divide $|H^{\Delta(\alpha_s)}|$. If $Q \in Syl_p(H)$, then Q stabilizes all predecessors and all successors of X. 3.3 (ii) implies $Q = 1$.

LEMMA 4.2. $O_{p'}(G_{\alpha,\beta}) = 1$ *for* $\beta \in \Delta(\alpha)$.

Proof. First

$$O_{p'}(G_{\alpha,\beta})G_{\alpha,\Delta(\alpha)}/G_{\alpha,\Delta(\alpha)} \subseteq O_{p'}(G_{\alpha,\beta}^{\Delta(\alpha)}) = 1.$$

Hence $O_{p'}(G_{\alpha,\beta}) \subseteq G_{\alpha,\Delta(\alpha)}$ and similarly $O_{p'}(G_{\alpha,\beta}) \subseteq G_{\beta,\Delta'(\beta)}$, as $\alpha \in \Delta'(\beta)$. Therefore

$$O_{p'}(G_{\alpha,\beta}) = O_{p'}(G_{\alpha,\Delta(\alpha)}) = O_{p'}(G_{\beta,\Delta'(\beta)}) \quad \text{and} \quad O_{p'}(G_{\alpha,\beta}) \lhd \langle G_\alpha, G_\beta \rangle = G.$$

So $O_{p'}(G_{\alpha,\beta}) = 1$.

LEMMA 4.3. *Take* $\beta \in \Delta(\alpha)$. $G_{\alpha,\Delta(\alpha)} \cap G_{\beta,\Delta'(\beta)}$ *is a p-group and* $|G_{\alpha,\beta}|_{p'}$ *divides* $((q-1)/d)^2$ *where* $d = 1$ *if q is even and* $d = 2$ *if q is odd.* $G_{\alpha,\beta}$ *is solvable. If K is a p'-Hall subgroup of* $G_{\alpha,\beta}$ *then*

$$Z_{(q-1)/d} \subseteq K \subseteq Z_{(q-1)/d} \times Z_{(q-1)/d}$$

(Z_r *denotes the cyclic group of order r*).

Proof. $G_{\alpha,\Delta'(\alpha)}G_{\alpha,\Delta(\alpha)}/G_{\alpha,\Delta(\alpha)}$ is a normal subgroup of $G_\alpha^{\Delta(\alpha)}$. So if $G_{\alpha,\Delta'(\alpha)} \nsubseteq G_{\alpha,\Delta(\alpha)}$, then we have a prime r dividing $q+1$ and $|G_{\alpha,\Delta'(\alpha)}|$ and not dividing $|G_{\alpha,\Delta(\alpha)}|$ by 3.1 (ii). This contradicts $|G_{\alpha,\Delta(\alpha)}| = |G_{\alpha,\Delta'(\alpha)}|$ (see 3.1 (i)). So $G_{\alpha,\Delta(\alpha)} = G_{\alpha,\Delta'(\alpha)}$ and by [6; 4.5] and 4.2 we have that $N = G_{\alpha,\Delta(\alpha)} \cap G_{\beta,\Delta'(\beta)}$ is a p-group. Since $G_{\beta,\Delta'(\beta)}/N$ is isomorphic to a subgroup of $G_{\alpha,\beta}^{\Delta(\alpha)}$ we have that $|G_{\alpha,\beta}|_{p'}$ divides $((q-1)/d)^2$.

Suppose $k, h \in K$. Set $t = [k, h]$. Then $t \in N$ and hence $t = 1$. Clearly, $U = K \cap G_{\alpha,\Delta(\alpha)}$ is faithful on $\Delta'(\beta)$ and so $U \subseteq Z_{(q-1)/d}$. Let $x \in K$ be an element inducing a cyclic group of order $(q-1)/d$ on $\Delta(\alpha)$. Then $y = x^{(q-1)/d} \in U$. If $y \neq 1$ then x would induce on $\Delta'(\beta)$ a group of order $>(q-1)/d$, a contradiction.

LEMMA 4.4. *For each s-arc X; $\alpha_0, \ldots, \alpha_s$ there is a successor Y; $\alpha_1, \ldots, \alpha_{s+1}$ such that the group K fixing X is also fixing Y. There is an element $g \in G$ with $Y^g = X$, $\alpha_i^g = \alpha_{i-1}$ $(1 \le i \le s+1)$ and $g \in N_G(K)$.*

Proof. Let K be the stabilizer of X. Then by 3.3, K is a p'-Hall group of G_{α_0,α_1} and $G_{\alpha_{s-1},\alpha_s}$, respectively. So K induces one orbit of length $q-1$ if q is even or two orbits of length $(q-1)/2$ if q is odd on $\Gamma(\alpha_{s-1}, \alpha_s)$ and K fixes exactly one element $\alpha_{s+1} \in \Gamma(\alpha_{s-1}, \alpha_s)$. Since $K = G_{\alpha_0,\ldots,\alpha_s}$, we also have $K = G_{\alpha_1,\ldots,\alpha_{s+1}}$. Choose $g \in G$ with $X = Y^g$, then all assertions follow.

LEMMA 4.5. *Choose $\alpha_0, \ldots, \alpha_{s+1}$, K and $g \in N_G(K)$ as in 4.4. Denote by H the stabilizer of $\alpha_1, \ldots, \alpha_s$ and take $Q \in Syl_p(H)$. Denote further by H_i the stabilizer of $\alpha_0, \ldots, \alpha_{s-i}$ for $1 \le i \le s$. Then*

(i) *Q is elementary abelian of order q.*

(ii) *$|H_{i+1}: H_i| = q$ for $1 \le i < s-1$.*

(iii) *$H_i = \langle K, Q_1, \ldots, Q_i\rangle$ for $1 \le i \le s$, where for each integer r we set $Q_r = g^{-r}Qg^r$.*

(iv) *$P_i = O_p(H_i) = \langle Q_1, \ldots, Q_i\rangle$ for $1 \le i \le s-1$ and $P_{i-1} \lhd P_i$.*

(v) *$G = \langle H, g\rangle$.*

(vi) *$Z_{(q-1)/d} \subseteq K \subseteq Z_{(q-1)/d} \times Z_{(q-1)/d}$ where $d = 1$ if q is even and $d = 2$ if q is odd.*

Proof. Since G is transitive on the s-arcs it follows that H_i is transitive on the s-arcs beginning with $\alpha_0, \ldots, \alpha_{s-i}$. As the number of s-arcs beginning with $\alpha_0, \ldots, \alpha_{s-i}$ is q^i, we have $|H_i| = q^i|K_i|$.

By the structure of $L_2(q)$ we have that Q is elementary abelian of order q. Now $H_i \supseteq \langle K, Q_1, \ldots, Q_i\rangle$ and Q_i acts regularly on $\Gamma(\alpha_{s-i-1}, \alpha_{s-i})$. Hence $Q_i \cap H_{i-1} = 1$, $|H_i| = |Q_i|\,|H_{i-1}|$ and $H_i = \langle K, Q_1, \ldots, Q_i\rangle$ for $1 \le i < s$. H_{s-1} is maximal in H_s and $Q_s \nsubseteq H_{s-1}$, so $H_s = \langle K, Q_1, \ldots, Q_s\rangle$. Since H_s is maximal in G and $Q_{s+1} \nsubseteq H_s$ we have $G = \langle H_s, Q_{s+1}\rangle = \langle H, g\rangle$.

Clearly $N_K(Q)QK_0/K_0$ is represented on $K_0 = K_{\Gamma(\alpha_{s-1},\alpha_s)}$ which is cyclic by 4.3. Hence K_0 centralizes Q and $Q \lhd H$. (vi) follows by 4.3. Since $g \in N_G(K)$

then K normalizes every Q_i. Suppose, we have already shown that $P_i = O_p(H_i)$ for $1 \leq i \leq k < s - 1$. Certainly $N_{Q_{k+1}}(P_k)$ is K-invariant and $\neq 1$. So Q_{k+1} normalizes P_k and $P_k \lhd P_{k+1}$ follows.

DEFINITION. We set $L_i = gH_ig^{-1}$ and $R_i = gP_ig^{-1}$ for all integers i.

LEMMA 4.6. *$R_i = \langle Q_0, \ldots, Q_{i-1}\rangle$ for $1 \leq i \leq s - 1$, $R_{i+1} \cap P_{i+1} = P_i$ for $0 \leq i \leq s - 2$ and $P_i \lhd R_{i+1}$. Also $L_{i+1} \cap H_{i+1} = H_i$.*

Proof. Clearly, $P_i \subseteq R_{i+1} \cap P_{i+1}$. If $P_i \subset R_{i+1} \cap P_{i+1}$, then there is a $1 \neq y \in Q_{i+1} \cap R_{i+1} \cap P_{i+1}$ and $Q_{i+1} = \langle y^K\rangle \subseteq R_{i+1}$. It follows that $R_{i+1} \cap P_{i+1} = P_{i+1}$ and H_{i+1} is g-invariant. So $H_{i+1} \lhd G = \langle H, g\rangle$ by 4.5, a contradiction. Since $1 \neq N_{Q_0}(P_i)$ is K-invariant, we have that Q_0 normalizes P_i and $P_i \lhd R_{i+1}$.

LEMMA 4.7. *Suppose $k \leq j$ and $|k - j| \leq s - 2$. Then*

$$[Q_k, Q_j] \subseteq \langle Q_{k+1}, \ldots, Q_{j-1}\rangle.$$

If $s \geq 3$, then P_2 is abelian.

Proof. By 4.6, $[Q_0, Q_i] \subseteq P_i \cap R_i = P_{i-1}$ for $i \leq s - 2$. Conjugate the above expression with a suitable power of g and the assertion follows.

LEMMA 4.8. *If $2_i \geq s + 2$, then P_i is nonabelian.*

Proof. Choose i as above and assume P_i is abelian. Then $[Q_j, Q_k] = 1$ for $|j - k| \leq i - 1$. So $[Q_i, Q_t] = 1$ for $1 \leq t \leq s + 1$, since

$$|t - i| \leq \operatorname{Max}(i - 1, s - i + 1) = i - 1.$$

Therefore

$$Q_i \lhd G = \langle Q_1, \ldots, Q_{s+1}, K\rangle,$$

a contradiction.

LEMMA 4.9. *If $1 \leq i \leq s - 1$ then an element $x \in P_i$ can be written as $x = y_1y_2\cdots y_i$ where $y_r \in Q_r$ for $1 \leq r \leq i$ is uniquely determined. If P_i is nonabelian, then $i \geq (2s + 1)/3$.*

Proof. The first assertion is obvious since $|P_{i+1}| = |P_i|\,|Q_{i+1}|$.

Without loss we may assume that $s \geq 3$. Choose now $2 < i < s$, such that P_{i-1} is abelian but P_i is not abelian. Hence

$$(+) \qquad [Q_j, Q_k] = 1 \quad \text{whenever } |j - k| \leq i - 2.$$

Since P_i and every Q_j is K-invariant, for every $x_1 \in Q_1^{\#}$ there is a $x_i \in Q_i^{\#}$ with $1 \neq [x_1, x_i]$. By 4.7,

$$(++) \qquad 1 \neq [x_1, x_i] = x_m \cdots x_n$$

where $2 \leq m \leq n \leq i - 1$, $x_m \neq 1 \neq x_n$ and $x_t \in Q_t$ is uniquely determined for $m \leq t \leq n$. We want to show

$$(1) \qquad i + m \geq s + 1$$

$$(2) \qquad 2i - n \geq s.$$

Granted both facts it follows that $s + 1 - i \leq m \leq n \leq 2i - s$ or $i \geq (2s + 1)/3$.

Proof of (1). We copy the proof of [9; 2.6]. Set $k = i + m - 1$ and suppose (1) is false. So $k \leq s - 1$. Since $|k - m| = i - 1$ and $x_m \neq 1$ there is an $x_k \in Q_k^{\#}$ with $[x_m, x_k] \neq 1$. Set $w = [x_1, x_k]$. Then $w \in \langle Q_2, \ldots, Q_{k-1}\rangle$ by Lemma 4.7 since $k \leq s - 1$. By $(+)$, $[w, Q_j] = 1$ for $m \leq j \leq i$. So w commutes with x_i and $[x_1, x_i]$. Finally x_k commutes with Q_j for $m < j \leq i$. We conjugate $(++)$ with x_k. For the left-hand side we get

$$x_k^{-1}[x_1, x_i]x_k = [x_1 w, x_i] = w^{-1}[x_1, x_i]w[w, x_i] = [x_1, x_i] = x_m \cdots x_n.$$

For the right-hand side we get

$$x_k^{-1}(x_m \cdots x_n)x_k = (x_k^{-1}x_m x_k)x_{m-1} \cdots x_n = x_m[x_m, x_k]x_{m-1} \cdots x_n.$$

Thus $[x_m, x_k] = 1$, a contradiction.

Proof of (2). As in the proof of (1) we can adapt our situation to the proof of [9; 2.6].

LEMMA 4.10. *$s \leq 7$ and $s \neq 6$.*

Proof. Take t minimal with $2t \geq s + 2$. Then P_t is not abelian by 4.8. By 4.9, $3t \geq 2s + 1$. Suppose $s \equiv 0 \pmod 2$; then $t = (s + 2)/2$ and $3s + 6 \geq 4s + 2$ or $s \leq 4$. If $s \equiv 1 \pmod 2$, then $t = (s + 3)/2$ and $3s + 9 \geq 4s + 2$ or $s \leq 7$.

5. The structure of G_α

We use the notation of Section 4 and set $\alpha = \alpha_0$.

LEMMA 5.1. (i) *If $s = 2$, then $G_\alpha \simeq L_2(q)$.*
(ii) *If $s = 3$, then $G_\alpha \simeq L_2(q) \times Y$, where Y is isomorphic to a S_p-normalizer in $L_2(q)$.*

Proof. If $s = 2$, then $Syl_p(G_{\alpha, \Delta(\alpha)}) = \{1\}$ and 4.2 implies the assertion.
Suppose now $s = 3$. Then $\langle Q_1, Q_2\rangle$ and $\langle Q_2, Q_3\rangle$ are S_p-subgroups of G_α, whose intersection is Q_2. Hence $O_p(G_\alpha) = Q_2$. Clearly, $C_{G_\alpha}(Q_2)$ covers $G_\alpha^{\Delta(\alpha)}$ and so $G_\alpha = G_{\alpha, \Delta(\alpha)} \cdot C_{G_\alpha}(Q_2)$. Let R be a p'-Hall subgroup of $G_{\alpha, \Delta(\alpha)}$ contained in K. Then R is represented faithful on Q_2 by 4.2 and hence $R \simeq K/C_K(Q_2) \simeq Z_{(q-1)/d}$ where $d = 1$ if q is even and $d = 2$ if q is odd. Also

$[R, C_{G_\alpha}(Q_2)] \subseteq C_{G_\alpha}(Q_2) \cap G_{\alpha,\Delta(\alpha)} = Q_2$. By a theorem of Gaschütz $C_{G_\alpha}(Q_2)$ splits over Q_2 and $C_{G_\alpha}(Q_2) = Q_2 \times X$, where $X \simeq L_2(q)$. Moreover $[X, R] \subseteq Q_2 \cap X = 1$. Hence $G_\alpha \simeq L_2(q) \times Y$.

LEMMA 5.2. *If $s = 4$ then $p = 2$. If $P = O_2(G_\alpha)$, then P is elementary abelian of order q^2 and $C_G(P) = P$. G_α/P is isomorphic to a subgroup of $GL(2, q)$ containing $SL(2, q)$ and acting on P as on the standard module. G_α splits over P.*

Proof. Since the two S_p-subgroups $\langle Q_1, Q_2, Q_3\rangle$ and $\langle Q_2, Q_3, Q_4\rangle$ contain $\langle Q_2, Q_3\rangle$ and $|G_{\alpha,\Delta(\alpha)}|_p = q^2$, we have $P = O_p(G) = \langle Q_2, Q_3\rangle$. By a theorem of Gaschütz G_α splits over P. Further by 4.8, P_3 is nonabelian. Since P_3 is K-invariant we have $[Q_1, Q_3] = Q_2$. Since $O_{p'}(G_\alpha) = 1$, and $C_{G_\alpha}(P) \subseteq G_{\alpha,\Delta(\alpha)}$ we have $C_G(P) = P$. Let X/P denote the smallest member of the derived series of G_α/P. By 4.5, $G_{\alpha,\Delta(\alpha)}/P \subseteq Z(G_\alpha/P)$ and so X/P is either isomorphic to $L_2(q)$ or $SL(2, q)$. Assume q is odd and $X/P \simeq SL(2, q)$, then $KP/P \cap X/P$ contains a four-group by 4.5 in contradiction to the structure of $SL(2, q)$. Hence $X/P \simeq L_2(q)$ and $KP/P \cap X/P$ is cyclic of order $(q - 1)/d$ (where $d = 1$ if q is even and $d = 2$ if q is odd) acting on the subgroups of order p of Q_2 or Q_3 transitively. So P is an irreducible X/P-module in contradiction to 2.6 if q is odd. So q is even and $G_\alpha/P \simeq SL(2, q) \times Z$, $Z \subseteq Z_{q-1}$. Since $X/P \simeq SL(2, q)$ we have by 2.5 that P may be regarded as the standard $SL(2, q) = X/P$-module.

Let L/P denote $Z(G_\alpha/P)$, then L/P permutes all subgroups of order q in P which represent one-dimensional subspaces in respect to the action of X/P on P. Since there are $q + 1$ of them and $|L/P|$ divides $q - 1$ it follows that L/P leaves invariant all these one-dimensional subspaces. Now it is easy to see that G_α/P is isomorphic to a subgroup of $GL(2, q)$ containing $SL(2, q)$ and P may be regarded as the standard module of G_α/P.

LEMMA 5.3. *If $s = 5$, then $p = 2$. $P = O_2(G_\alpha)$ is elementary abelian of order q^3. $K \simeq Z_{q-1} \times Z_{q-1}$ and $G_\alpha/P \simeq GL(2, q)$. $Q_3 \lhd G_\alpha$ and $C_G(Q_3)/P \simeq SL(2, q)$. P/Q_3 may be regarded as the standard module for $GL(2, q) \simeq G_\alpha/P$ and G_α splits over P. P is an indecomposable G_α/P-module* (i.e., *there is no $T \subset P$, $T \lhd G_\alpha$ with $T \times Q_3 = P$*).

Proof. As usual $P = O_p(G_\alpha) = \langle Q_2, Q_3, Q_4\rangle$. Suppose P_3 is not abelian. Then $[Q_2, Q_4] = Q_3$ and $Q_3 \lhd G_\alpha$. But $[Q_1, Q_3] = Q_2$, a contradiction.

So P_3 is abelian and $Q_3 \lhd G_\alpha$, since $Q_3 \subseteq \langle Q_1, Q_2, Q_3\rangle \cap \langle Q_3, Q_4, Q_5\rangle$. Also $C_G(Q_3)$ covers $G_\alpha^{\Delta(\alpha)}$ as $C_G(Q_3)$ contains a S_p-subgroup of G_α. By 4.8, P_4 is not abelian and as $O_{p'}(G_\alpha) = 1$, it follows that $C_G(P) = P$. Since K induces on Q_3 a cyclic group of order $(q - 1)/d$, we have

$$|G_\alpha : C_G(Q_3)| = (q - 1)/d \quad \text{and} \quad K = Z_{(q-1)/d} \times Z_{(q-1)/d},$$

where $d = 1$ if q is even and $d = 2$ if q is odd (see 4.5).

Hence $C_G(Q_3)/P \simeq L_2(q)$. Clearly, $[Q_1, Q_4] \subseteq \langle Q_2, Q_3\rangle$. We have neither $[Q_1, Q_4] = Q_3$ nor $[Q_1, Q_4] = Q_2$ (which implies $[Q_2, Q_5] = Q_3$), since $C_{G_\alpha}(P/Q_3) \subseteq G_{\alpha, \Delta(\alpha)}$. Since Q_1 and Q_4 are K-invariant, we have for $x_i \in Q_i^\#$ ($i = 1, 4$), $[x_1, x_4] = x_2 x_3$ always, with $x_j \in Q_j^\#$ (for $j = 2, 3$). We have

$$C_{P/Q_3}(Q_1) = Q_2 Q_3/Q_3 = [Q_1, P]Q_3/Q_3$$

and as in the proof of 5.2, P/Q_3 is an irreducible $C_{G_\alpha}(Q_3)/P \simeq L_2(q)$-module. As before q is even and P/Q_3 is the standard module for $C_{G_\alpha}(Q_3)/P \simeq SL(2, q)$ by 2.5 and 2.6.

Set $L = C_K(P/Q_3) \cap G_{\alpha, \Delta(\alpha)}$ and assume $L \neq 1$. Clearly, $L \subseteq C_K(Q_2, Q_4)$ and so with $g \in G$ chosen as in 4.4 and 4.5, $L^g \subseteq C_K(Q_3, Q_5)$. Since $C_K(Q_3)$ acts fixed-pointfree on $Q_5 P/Q_3$ (as P/Q_3 is the standard module for $SL(2, q) \simeq C_{G_\alpha}(Q_3)/P$), we have $L^g = 1$ and so $L = 1$. Now the assertion follows as in the proof of 5.2.

LEMMA 5.4. *The case $s = 7$ does not occur.*

Proof. As usual $P = O_p(G) = \langle Q_2, \ldots, Q_6\rangle$. By 4.9, $[Q_i, Q_j] = 1$ whenever $|i - j| \leq 3$. Also the proof of 4.9 shows us that $[Q_1, Q_5] \subseteq Q_3$. Since P_5 is not abelian by 4.8, we have $[Q_1, Q_5] = Q_3$, $[Q_2, Q_6] = Q_4$ and $[Q_3, Q_7] = Q_5$. Hence Q_4 and $T = \langle Q_3, Q_4, Q_5\rangle$ are normal subgroups of G_α. So $C_{G_\alpha}(Q_4)$ covers $G_\alpha^{\Delta(\alpha)}$ and as in the proof of 5.3 we have

$$K = Z_{(q-1)/d} \times Z_{(q-1)/d},$$

where $d = 1$ if q is even and $d = 2$ if q is odd. Also $C_{G_\alpha}(T/Q_4) \cap C_{G_\alpha}(Q_4) = P$ and so $C_{G_\alpha}(Q_4)/P \simeq L_2(q)$ acts faithfully on T/Q_4. Since

$$Q_1 P/P \in Syl_p(C_{G_\alpha}(Q_4)/P) \quad \text{and} \quad C_{T/Q_4}(Q_1 P/P) = Q_3 Q_4/Q_4$$

we have by 2.5 and 2.6 that q is even and T/Q_4 is the standard module for $C_G(Q_4)/P$.

Further $[Q_1, Q_6] \subseteq \langle Q_2, \ldots, Q_5\rangle$ and $[Q_2, Q_7] \subseteq \langle Q_3, \ldots, Q_6\rangle$. Take $x_1 \in Q_1^\#$, $x_6 \in Q_6^\#$. Then there are $x_i \in Q_i$ ($2 \leq i \leq 5$) with $[x_1, x_6] = x_2 \ldots x_5$ and

$$1 = x_1 x_6^2 x_1 = (x_1 x_6 x_1)^2 = (x_2 x_3 x_4 x_5 x_6)^2 = (x_2 x_6)^2.$$

Since T/Q_4 is the standard module for $C_G(Q_4)/P$, we have for $y_1 \in Q_1^\#$ that $C_{Q_5}(y_1) = 1$. Hence $x_2 = 1$. So $[Q_1, Q_6] \subseteq \langle Q_3, Q_4, Q_5\rangle$ and similarly $[Q_1, Q_6] \subseteq \langle Q_2, Q_3, Q_4\rangle$. So finally $[Q_1, Q_6] \subseteq \langle Q_3, Q_4\rangle$ and $[Q_2, Q_7] \subseteq \langle Q_4, Q_5\rangle$.

Now we claim that $\Delta(\alpha_0)$ *is self-paired* (notation as in Section 4 and $\alpha = \alpha_0$). $N = G_{\alpha_0, \alpha_1} = N_{G_{\alpha_0}}(P_6) = N_{G_{\alpha_1}}(P_6)$. Since N^g is also a S_2-normalizer in G_{α_0} there is a $h \in G_{\alpha_0}$ with $N^k = N$ and $k = gh \in N_G(P_6) - N_{G_{\alpha_0}}(P_6)$. Now $N_G(Q_4) = G_{\alpha_0}$ and $P_6' = \langle Q_3, Q_4\rangle$. Since $N = P_6 K$ we can use a Frattini-argument and find a $k \in N_G(K) \cap N_G(P_6) - N_{G_{\alpha_0}}(P_6)$. So $Q_4^k \neq Q_4$. Since

Q_3 and Q_4 are the only K-invariant subgroups in P_6' of order q we have $Q_4^k = Q_3$ and $Q_3^k = Q_4$. Hence $k^2 \in N_G(P_6) \cap G_{\alpha_0} = N$. So $|\langle k\rangle N| = 2|N|$ and we may assume that $\Delta(\alpha_0)$ is self-paired (see [9; 5.16]).

Set $\alpha_{-1} = \alpha_0^g$. Then $\alpha_1, \alpha_{-1} \in \Delta(\alpha_0)$, since $\Delta(\alpha_0)$ is self-paired. Q_1 does not fix $\beta \in \Delta(\alpha_0) - \{\alpha_1\}$ as otherwise Q_1 would fix the 7-arc $\beta, \alpha_0, \ldots, \alpha_6$. Hence Q_1 acts regularly on $\Delta(\alpha_0) - \{\alpha_1\}$. By definition Q_7 does not fix α_1 but does fix α_{-1}. So we can find $x_1 \in Q_1$ and $x_7 \in Q_7$ with $\alpha_{-1}^{x_1} = \beta$ and $\beta^{x_7} = \alpha_1$. Set $h = gx_1x_7$ and $\alpha_0^h = \alpha_1$ and $\alpha_1^h = \alpha_0$ follows. So $h^2 \in N$.

Now

$$h^{-1}y_1h = x_7x_1g^{-1}y_1gx_1x_7 = x_7x_1y_2x_1x_7 = y_2[x_7, y_2] \in \langle Q_2, Q_4, Q_5\rangle$$

where $y_i \in Q_i$ for $1 \leq i \leq 2$. In the same way

$$h^{-1}y_2h \in \langle Q_3, Q_4, Q_5\rangle,\ h^{-1}y_4h \in \langle Q_3, Q_5\rangle, \text{ and } h^{-1}y_5h \in \langle Q_3, Q_4, Q_5, Q_6\rangle$$

where $y_i \in Q_i$ for $i = 2, 4, 5$. Hence $h^{-2}y_1h^2 \in \langle Q_2, Q_3, Q_4, Q_6\rangle = P$. But $h^2 \in P_6K$ and so $h^{-2}y_1h^2 \in P_6 - P$ for $y_1 \in Q_1^{\#}$, a contradiction.

6. The case $p = 2$

In this section we will show that in the case $p = 2$ we have $G_{\alpha, \Delta(\alpha)} = 1$, or equivalently $s \leq 2$. Always we will use the notation of Section 4 and 5.

LEMMA 6.1. $s \neq 3$.

Proof. By 5.1 (ii) we have $G_\alpha = X \times Y$ where $X \simeq SL(2, q)$ and $Y = N_{SL(2,q)}(F)$ with $F \in Syl_2(SL(2, q))$. Now $G_{\alpha_0, \alpha_1} = (E \times F)K$ where $F \in Syl_2(Y)$ and $E \in Syl_2(X)$. Set $S = EF$. Take $x \in G$ with $\alpha_0^x = \alpha_1$. Then $(SK)^x \subseteq G_{\alpha_1}$ and there is an $h \in G_{\alpha_1}$ with $(SK)^{xh} = SK$. Set $y = xh$, then $\alpha_0^y = \alpha_1$ and $y \in N_G(SK) - G_{\alpha_0}$. Since E and F are the only minimal normal subgroups of SK and $G_{\alpha_0} = N_G(F)$, we have $E^y = F$ and $F^y = E$. Since $y^2 \in N_G(F) \cap N_G(SK) = SK$, we may choose—by using a Frattini argument—y as an involution in $N_G(K)$. Now $S^{\#}$ splits in the two $\langle y\rangle K$-orbits $F^{\#} \cup E^{\#}$ and $(F^{\#})(E^{\#})$.

Assume first that $S^* = \langle y\rangle S \in Syl_2(N_G(S))$. Since S char S^* it follows that $S^* \in Syl_2(G)$. Let X be a minimal normal subgroup of G. If $X \cap G_\alpha = 1$, then $|X|$ is odd as $|X|_2 \leq 2$. But then $G_\alpha X = G$ and $|G|_2 < |S^*|$, a contradiction. Hence $X \cap G_\alpha \neq 1$ and so $S \subseteq X$. Even $S^* \subseteq X$ as G_α and so G can not contain a subgroup of index 2. Hence X is simple, in contradiction to 2.2. So if $T \in Syl_2(N_G(S))$, then $S^* \subseteq T$ implies $S^* \subset T$. Then T does not normalize $E^{\#} \cup F^{\#}$ and all elements in $S^{\#}$ are conjugate under $N_G(S)$. Let $E = E_1 \supset E_2 \supset \cdots \supset E_n \supset 1$ be an arbitrary sequence of hyperplanes.

Suppose we have already shown by induction that $S \in Syl_2(N_G(E_{i-1}))$. Certainly, $N_G(E_{i-1}) \cap N_G(E_i)$ is the preimage of $C_{N_G(E_i)/E_i}(E_{i-1}/E_i)$.

Assume first that $S/E_i \notin Syl_2(N_G(E_i)/E_i)$. Since

$$S/E_i \in Syl_2((N_G(E_{i-1}) \cap N_G(E_i))/E_i)$$

for all subgroups $E_i \subset E_{i-1} \subseteq E$ with $|E_{i-1}: E_i| = 2$, it follows that E/E_i contains only noncentral involutions of $N_G(E_i)/E_i$. Take

$$t \in (N_G(E_i) \cap N_G(S)) - S \quad \text{with } t^2 \in S.$$

Then $(E/E_i)^t \cap E/E_i = 1$. If $(E/E_i)^t \cap FE_i/E_i \neq 1$ then the involutions in FE_i/E_i are conjugate under $N_{N_G(S)}(E_i)/E_i$ to involutions in E/E_i. Hence

$$FE_i/E_i \cap (FE_i/E_i)^t = 1$$

which is not true since $|FE_i/E_i| = q > \sqrt{|S/E_i|}$. Therefore the involutions in FE_i/E_i are central and the map

$$(E/E_i)^\# \ni eE_i \to e^t FE_i$$

is a bijection of $(E/E_i)^\#$ onto $(S/FE_i)^\#$. So all involutions in $S/E_i - FE_i/E_i$ are conjugate to an involution in E/E_i. Also t normalizes FE_i/E_i and thus fixes every coset eFE_i/E_i where $e \in E$. Denote by T a S_2-subgroup in

$$N_G(S) \cap C_G(S/FE_i) \cap N_G(E_i)$$

and set $K_0 = C_K(E)$. Then TK_0 induces a Frobenius group of order $q(q-1)$ on the coset eFE_i/E_i for $e \in E - E_i$ (see also [12; lemma 2]). The map $T \ni t \to [e, t] \in E_i$ for $e \in E_i$ is a K_0-homomorphism of T/S into $[T, E_i]/[E_i, T, T]$. So $E_i \subseteq Z(T)$. Set $T_0 = [T, K_0]E_i$; then $T_0/E_i \cap E/E_i = 1$ and $T_0E = T$. Also T_0/E_i is abelian since T_0/FE_i and FE_i/E_i are K_0-isomorphic. If

$$[FE_i, T_0] = 1,$$

then $|N_G(F)|_2 > q^2$, a contradiction.

So we can find a hyperplane $E^* \subset E_i$ such that T_0/E^* is not abelian. If $K_0 = \langle k \rangle$, then k has on FE_i/E_i and T_0/FE_i the eigenvalues $\{\lambda, \lambda^2, \ldots, \lambda^{2^{n-1}}\}$ where λ is a primitive $(q-1)$th root of unit. Since the commutator map is a nontrivial, bilinear, and K_0-admissible map from T_0/E_i onto the trivial K_0-module E_i/E^* we have

$$\{\lambda, \lambda^2, \ldots, \lambda^{2^{n-1}}\} = \{\lambda^{-1}, \lambda^{-2}, \ldots, \lambda^{-2^{n-1}}\}.$$

Therefore $q - 1 = 2^n - 1$ must divide $2^k + 2^l$ for some $0 \leq k, l \leq n - 1$. It follows that $n = 2$, $k = 1$, and $l = 0$. (For these arguments also compare with [5].)

So if $n > 2$, we have by induction that $S \in Syl_2(C_G(e))$ where $e \in E^\#$, contradicting the fact that all elements in $S^\#$ are conjugate and that $S \notin Syl_2(G)$.

So we are in the case $n = 2$ with $E_2 = E_i$, and $2^2 \cdot 3^2 \cdot 5$ divides $|N_G(S)/S|$. Suppose first $2^2 \cdot 3^2 \cdot 5 \neq |N_G(S)/S|$. Then

$$|N_G(S)/S| \geq 2^3 \cdot 3^2 \cdot 5$$

and as S possesses exactly 35 subgroups of order 4 we have a contradiction to

$$|N_G(S): (N_G(S) \cap N_G(E))| \geq 2^3 \cdot 5 = 40.$$

So $|N_G(S)/S| = 2^2 \cdot 3^2 \cdot 5$. Suppose every minimal normal subgroup of $N_G(S)/S$ is nonsolvable, then $N_G(S)/S$ is isomorphic to A_5 extended by an automorphism of order 3 which is impossible. The structure of A_8 implies that $N_G(S)/S \simeq A_5 \times Z_3 \simeq GL(2, 4)$ where S is the standard module for $N_G(S)/S$.

Now K normalizes a $T \in Syl_2(N_G(S))$ by the structure of $GL(2, 4)$. But then either F or E is KT-invariant, a contradiction.

LEMMA 6.2. $s \neq 4$.

Proof. Suppose $s = 4$. $N = G_{\alpha_0, \alpha_1}$ is the normalizer of a S_2-subgroup in G_{α_0} and G_{α_1}. Set $S = O_2(N) \in Syl_2(N)$ and S contains exactly two elementary abelian subgroups—say E and F—of order q^2. One of them—say E—is equal to $O_2(G_{\alpha_0})$. If $\alpha_0^g = \alpha_1$ then there is a $h \in G_{\alpha_1}$ with $z = gh \in N_G(N)$. So $z \in N_G(S)$ and since $z \notin N_G(E) = G_{\alpha_0}$ we have $E^z = F$ and $F^z = E$. As $N_G(E) \subseteq G_{\alpha_0}$ we have $N_G(S) = \langle t \rangle N$ where t interchanges E and F. We can even choose $t \in N_G(K)$ and it follows $|t| = 2$. Since all involutions in S lie in $E \cup F$ and as $C_{(E \cup F)}(x) \subseteq Z = Z(S)$ for $x \in T - S$, $|x| = 2$ it follows that S char T where $T = S\langle t \rangle$. We conclude $T \in Syl_2(G)$.

Set $W = T'$, then W is of exponent 4 and $\Omega_1(W) = Z$. Every element in $T - W$ induces a nontrivial automorphism on W. So $|C_G(W)W : W|$ is odd. Further $C_G(W)W \subseteq M \subseteq N_G(W)$ where $M = C_G(W/Z)$ and M contains T. We apply 2.7. Thus we have either $M_1 = C_M(Z)$ has S as a S_2-subgroup, or W is homocyclic of exponent 4 and t inverts W. In the second case $[C_K(t), T] = S$ and the cosets tW and fW with $f \in F$ are never conjugate in G. Let R be a 2-complement of the preimage of $O(M_1/W)$. In any case R stabilizes the chain $1 \subset Z \subset W$ and so $R \subseteq C_G(W)$. By 2.1 we have

$$O^{2,2'}(M_1/WR) \quad \text{or} \quad O^{2'}(M_1/WR) = V_0 \times V_1 \times \cdots \times V_m,$$

where V_0 is an elementary abelian 2-group and $V_1, \ldots, V_m$ are nonabelian simple. Since $(T \cap M_1)/W$ induces nontrivial automorphisms on W but centralizes W/Z and Z we have SR/WR char M_1/WR. The Frattini argument gives us

$$N_G(W) = O(C_G(W))(N_G(S) \cap N_G(W)).$$

Set $U = Z \cdot O(C_G(Z))$. Clearly, $S \subseteq C_G(Z)$. Let X/U be a minimal normal subgroup of $N_G(Z)/U$ lying in $C_G(Z)/U$.

Suppose first that X/U is semisimple and not abelian. Since WU/U and SU/U are the only $K\langle t \rangle$-invariant, nontrivial subgroups of SU/U we have to distinguish the three cases $W \in Syl_2(X)$, $S \in Syl_2(X)$, and $T \in Syl_2(X)$.

Assume first $W \in Syl_2(X)$, then $X/U \simeq SL(2, q)$ by 2.1 and $N_G(W) \cap C_G(Z)$ contains a group L inducing a cyclic group of order $q - 1$ on W/Z and acting transitively on $(W/Z)^{\#}$, a contradiction.

Suppose now $S \in Syl_2(X)$. Then $X/U \simeq SL(2, q) \times SL(2, q)$ by 2.1. This implies $N_G(E) \supset G_{\alpha_0}$ since $N_X(E) \nsubseteq G_{\alpha_0}$, a contradiction.

If, finally, $T \in Syl_2(X)$, then X/U is simple and by 2.2 we reach a contradiction. So in any case X/U is an elementary abelian 2-group and by the above $N_G(Z) = O(C_G(Z))N_G(S)$ follows.

Let Z_i be any subgroup of Z such that either $Z(T) \subseteq Z_i$ or $Z_i \subseteq Z(T)$, and $|Z_i| = 2^i$. We want to show by induction that $N_G(Z_i) = O(C_G(Z_i))(N_G(S) \cap N_G(Z_i))$. Take $z \in Z - Z_i$, if $Z_i \subset Z(T)$ then choose $z \in Z(T) - Z_i$. Set $Z_{i+1} = \langle Z_i, z \rangle$; then $N_G(Z_i) \cap N_G(Z_{i+1})$ is the preimage of $C_{N_G(Z_i)/Z_i}(zZ_i)$. In particular if x is an involution in $T - Z_i$ we have by induction, that

$$C_{T/Z_i}(xZ_i, zZ_i) \in Syl_2(C_{N_G(Z_i)/Z_i}(xZ_i, zZ_i)).$$

Case 1. Suppose first that $Z(T) = Z(S)$. If $x \in S - Z$ and if $T_{x,z}$ is the preimage of $C_{T/Z_i}(xZ_i, zZ_i)$ then $Z = T'_{x,z}$ and $x \not\sim z$ in $N_G(Z_i)$ if x is an involution. If $x \in T - S$ is an involution then $T'_{x,z} \cap Z(T_{x,z}) = Z$ by 2.7 and again $x \not\sim z$ in $N_G(Z_i)$. Therefore Z/Z_i is strongly closed in T/Z_i with respect to $N_G(Z_i)/Z_i$. 2.3 implies that $R = \langle Z^{N_G(Z_i)} \rangle \subseteq C_G(Z_i)$ and $R/O(R)$ is known. If $R \neq O(R)Z$, it follows that

$$|(C_G(Z_i) \cap N_G(Z)): C_G(Z)| > 1$$

in contradiction to the structure of $N_G(Z)$. The induction goes through in this case.

Case 2. Assume now $Z \neq Z(T)$ and use the information of 2.7. Again if $x \in S - Z$ is an involution we have $z \not\sim x$ in $N_G(Z_i)$ as in Case 1. Suppose now that $x \in T - S$ is an involution; then $x \not\sim z$ in $N_G(Z_i)$ for $i > n/2$ as $C_{Z_i}(x) \neq Z_i$. If $i \leq n/2$ then $Z(T/Z_i)$ has a preimage which is a group $Z^* = Z_{i+(n/2)}$, and $z \in Z^*$. If $x \in T - S$ is an involution and $T_{x,z}$ is the preimage of $C_{T/Z_i}(xZ_i, zZ_i)$, then the preimage of $Z(T_{x,z}/Z_i)$ is $\langle Z^*, x \rangle$ but $x \notin Z(\langle Z^*, x \rangle)$. So $x \not\sim z$ in $N_G(Z_i)$. The weak closure of $\langle zZ_i \rangle$ in

$$(N_G(Z_{i+1}) \cap N_G(Z_i))/Z_i$$

lies in Z/Z_i. Hence by a theorem of Shult (see [3; corollary 3]) we have as before

$$N_G(Z_i) = O(C_G(Z_i))(N_G(S) \cap N_G(Z_i)).$$

Every involution in $S - Z$ is conjugate in G to $z \in Z^\#$. We claim $z \sim t \in T - S$. Assume the contrary.

Case 1. $Z(T) = Z$. Then $Y = C_T(z, t) = \langle Z, t \rangle \in Syl_2(C_G(z, t))$ by the above. Also $C_K(t)$ acts transitively on $Z^\#$ and $t(Z^\#)$. As $t \sim tz$ in W we have that the elements in $Z^\#$ as well as in tZ are all conjugate in $X = N_G(Y)$. Now t has at least q conjugates under $C_X(z)$. Since for z there is $K^* \sim C_K(t)$ in X with $K^* \subseteq C_X(z)$ and $Y = \langle z \rangle \times Y_1$ where $Y_1^\#$ and $zY_1 - \{z\}$ are K^*-orbits. It follows that all involutions in $Y - \langle z \rangle$ are conjugate under $C_X(z)$. Hence 2 divides $|C_X(z): C_X(z, z_1)|$ where $z_1 \in Z - \langle z \rangle$. Take $R \in Syl_2(C_X(z))$ with $[t, T] \subseteq R$ and $Q \in Syl_2(G)$ with $R \subseteq G$. Then

$$Z(Q) \subseteq Y \subseteq \langle t \rangle [t, T] \quad \text{and} \quad Z(Q) \subseteq Z([t, T]\langle t \rangle) = Z.$$

Hence $Z(Q) = Z$, contradicting the fact that 2 divides $|C_X(z): C_X(z, z_1)|$.

Case 2. Assume $Z(T) \neq Z$. Then $z \in C_T(x, t)'$ but $t \notin C_T(x, z)'$ and so $t \nsim z$ in G.

By 2.4, G contains a subgroup of index 2. Since the maximal subgroup G_α does not contain a subgroup of index 2, we reach the final contradiction

$$|G: G_\alpha| = |\Omega| = 2 \geq |\Delta(\alpha)| = q + 1 \geq 5.$$

LEMMA 6.3. $s \neq 5$.

Proof. $P = O_2(G_\alpha) = \langle Q_2, Q_3, Q_4\rangle$ and $G_\alpha = N_G(Q_3)$ and $C_G(Q_3)$ covers $G_\alpha^{\Delta(\alpha)}$. Since $[Q_1, Q_4] \neq 1$ we have that $C_G(Q_3)/P$ is faithfully represented on P/Q_3. The map $x_4 \to [x_1, x_4]$ where $x_1 \in Q_1^\#$ and $x_4 \in Q_4$ is faithful from Q_4 into $\langle Q_2, Q_3\rangle$ and a $C_K(Q_1)$-homomorphism.

Take $k \in G$ with $\alpha_0^k = \alpha_1$ then there is a $x \in G_{\alpha_1}$ such that for $N_{G_\alpha}(P_4) = KP_4 = G_{\alpha_0, \alpha_1}$ we have $(KP_4)^h = KP_4$ where $h = kx$. Since P_4 contains exactly two elementary abelian groups of order q^3 where one of them is P, we have $h^2 \in KP_4$. As in the proof of 6.2, $T = \langle t\rangle P_4 \in Syl_2(G)$, where t is an involution in $N_G(K) \cap N_G(P_4)$ interchanging P and Q the elementary abelian subgroups of order q^3 in P_4. Since

$$K = C_K(Q_2) \times C_K(Q_3) = C_K(Q_1) \times C_K(Q_4)$$

and as t interchanges Q_2 and Q_3 we have that $Q_1^t = Q_4$ and $K_0 = C_K(t)$ is a cyclic group of order $q - 1$. One computes that $|C_{P_4}(t)| = q^2$. Moreover there are at most q cosets $tw\langle Q_2, Q_3\rangle$ with $w \in P_4$ which contain involutions and each of these cosets contains at most q involutions. Hence there are q^2 involutions in $T - P_4$ and all of them are conjugate under P_4.

$P_4 \in Syl_2(C_G(\langle Q_2, Q_3\rangle))$ and by the structure of $N_G(P_4)$ we know—using Burnside's theorem—that

$$N_G(\langle Q_2, Q_3\rangle) = O(C_G(\langle Q_2, Q_3\rangle))N_G(P_4).$$

Set $Z = Z(T) \subseteq \langle Q_2, Q_3\rangle$. Denote by Z_i any subgroup of $\langle Q_2, Q_3\rangle$ with $Z \subseteq Z_i$ and $|Z_i| = 2^i q$. We want to show by induction that

$$N_G(Z_i) = O(C_G(Z_i))(N_G(P_4) \cap N_G(Z_i)).$$

$P_4 \in Syl_2(C_G(Z_i))$ and $T \in Syl_2(N_G(Z_i))$ if $i > 0$. On the other hand if x is an involution in $P_4 - \langle Q_2, Q_3\rangle$ and $z \in \langle Q_2, Q_3\rangle - Z_i$ then by the hypothesis of the induction

$$C_{P_4/Z_i}(xZ_i, zZ_i) \in Syl_2(C_{C_G(Z_i)/Z_i}(xZ_i, zZ_i)).$$

If $T_{x,z}$ is the preimage of this group we have $\langle Q_2, Q_3\rangle = T'_{x,z} \cdot Z_i$ and so $x \nsim z$ in $N_G(z_i)$. Hence $\langle Q_2, Q_3\rangle$ is strongly closed in P_4 with respect to $C_G(Z_i)$. The structure of $N_G(\langle Q_2, Q_3\rangle)$ and 2.3 now implies

$$\langle Q_2, Q_3\rangle O(C_G(Z_i)) \trianglelefteq N_G(Z_i)$$

and the assertion follows.

Finally consider the case $Z_0 = Z$. $z \in \langle Q_2, Q_3 \rangle - Z$ is not conjugate to the involution $x \in T - P_4$ since the preimage $T_{x,z}$ of $C_{T/Z}(xZ, zZ)$ has $\langle Q_2, Q_3 \rangle$ as the only elementary abelian subgroup of index 2. If $z \in \langle Q_2, Q_3 \rangle - Z$ would be conjugate in $N_G(Z)$ to $x \in P_4 - \langle Q_2, Q_3 \rangle$ then all involutions in P_4/Z would be conjugate in $N_G(Z)/Z$. Hence $N_G(Z)/Z$ and so $C_G(Z)/Z$ has a subgroup of index 2 with S_2-subgroup P_4/Z as the proof of 2.4 shows. This group has class 2 and is of type $L_3(q)$. So if $X/O(C_G(Z))Z$ is a minimal normal subgroup of $N_G(Z)/O(C_G(Z))Z$ contained in $C_G(Z)/O(C_G(Z))Z$ and is non-solvable then $X/O(C_G(Z))Z \simeq L_3(q)$ by 2.2 and we get a contradiction to the structure of $N_G(P_4)$. So as usual

$$N_G(Z) = O(C_G(Z))(N_G(P_4) \cap N_G(Z))$$

follows.

Assume an involution $t \in T - P_4$ is conjugate in G to $x \in P_4$. By 2.8 there is a subgroup $X \subseteq T$, t, $x \in X$ satisfying conditions (1)–(4) of 2.8 (here T corresponds to P in 2.8) such that $x \sim t$ in N where

$$N = N_G(X) \quad \text{if } X = C_T(\Omega_1(Z(X)))$$

or

$$N = N_G(X) \cap C_G(\Omega_1(Z(X))) \quad \text{if } X \subset C_T(\Omega_1(Z(X))).$$

Clearly, $Z\langle t \rangle \subseteq X$ by 2.8 (2). Moreover $Z = Z(X)$ or $\Omega_1(Z(X)) = \langle t \rangle Z$, because $C_T(t) = \langle t \rangle U$, where U is homocyclic of order q^2 and $\Omega_1(U) = Z$. If $X = C_T(\Omega_1(Z(X)))$ then in any case Z char X and $x \sim t$ in $N_G(Z)$ which is impossible. If $X \subset C_T(\Omega_1(Z(X)))$ then $N \subseteq N_G(X)$ and we get the same contradiction.

2.4 implies that G has a subgroup of index 2 and we get the usual contradiction.

Remark. The permutation groups with a suborbit of length 3 have been determined by Sims [9] and Wong [15]. The permutation groups with a suborbit of length 4 have been determined by Sims [10] and Quirin [7].

References

1. H. Bender, *On groups with abelian Sylow 2-subgroups*, Math. Zeitschrift, vol., 117 (1970), pp. 164–176.
2. R. Gilman and D. Gorenstein, *Finite groups with Sylow 2-subgroups of class 2*, to appear.
3. D. Goldschmidt, *2-fusion in finite groups*, Ann. Math., vol. 99 (1974), pp. 70–117.
4. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
5. G. Higman, *Suzuki 2-groups*, Illinois J. Math., vol. 7 (1963), pp. 79–96.
6. W. Knapp, *On the point stabilizer of a primitive permutation group*, Math. Zeitschrift, vol. 133 (1973), pp. 137–168.
7. W. L. Quirin, *Primitive permutation groups with small orbits*, Math. Zeitschrift, vol. 122 (1971), pp. 267–274.
8. H. L. Rietz, *On primitive groups of odd order*, Amer. J. Math., vol. 26 (1904), pp. 1–30.
9. C. C. Sims, *Graphs and finite permutation groups*, Math. Zeitschrift, vol. 95 (1967), pp. 76–86.

10. ———, *Graphs and finite permutation groups II*, Math. Zeitschrift, vol. 103 (1968), pp. 276–281.
11. R. Solomon, *Finite groups with a Sylow 2-subgroup of type A_{12}*, J. Algebra, vol. 28 (1974), pp. 346–378.
12. F. L. Smith, *A general characterization of the Janko simple group J_2*, Arch. Math., vol. 25 (1974), pp. 17–22.
13. J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc., vol. 74 (1968), pp. 383–437.
14. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.
15. W. J. Wong, *Determination of a class of permutation groups*, Math. Zeitschrift, vol. 99 (1967), pp. 235–246.

Universität Heidelberg
Heidelberg, Germany