<table>
<thead>
<tr>
<th>Title</th>
<th>On some doubly transitive permutation groups in which socle(Gα) is nonsolvable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Hiramine, Yutaka</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 1979, 16(3), p. 797-816</td>
</tr>
<tr>
<td>Version Type</td>
<td>VoR</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/8021">https://doi.org/10.18910/8021</a></td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
ON SOME DOUBLY TRANSITIVE PERMUTATION GROUPS IN WHICH SOCLE($G_\alpha$) IS NONSOLVABLE

YUTAKA HIRAMINE

(Received July 3, 1978)

1. Introduction

Let $G$ be a doubly transitive permutation group on a finite set $\Omega$ and $\alpha \in \Omega$. In [8], O’Nan has proved that $\text{socle}(G_\alpha) = A \times N$, where $A$ is an abelian group and $N$ is 1 or a nonabelian simple group. Here $\text{socle}(G_\alpha)$ is the product of all minimal normal subgroups of $G_\alpha$.

In the previous paper [4], we have studied doubly transitive permutation groups in which $N$ is isomorphic to $\text{PSL}(2,q)$, $Sz(q)$ or $\text{PSU}(3,q)$ with $q$ even. In this paper we shall prove the following:

**Theorem.** Let $G$ be a doubly transitive permutation group on a finite set $\Omega$ with $|\Omega|$ even and let $\alpha \in \Omega$. If $G_\alpha$ has a normal simple subgroup $N^*$ isomorphic to $\text{PSL}(2,q)$, where $q$ is odd, then one of the following holds.

(i) $G^\alpha$ has a regular normal subgroup.

(ii) $G^\alpha = A_6$ or $S_6$, $N^* = \text{PSL}(2,5)$ and $|\Omega| = 6$.

(iii) $G^\alpha = M_{11}$, $N^* = \text{PSL}(2,11)$ and $|\Omega| = 12$.

In the case that $G^\alpha$ has a regular normal subgroup, by a result of Hering [3] we have $(|\Omega|, q) = (16, 9)$, $(16, 5)$ or $(8, 7)$.

We introduce some notations:

- $F(X)$: the set of fixed points of a nonempty subset $X$ of $G$
- $X(\Delta)$: the global stabilizer of a subset $\Delta(\subseteq \Omega)$ in $X$
- $X_\Delta$: the pointwise stabilizer of $\Delta$ in $X$
- $X^\alpha$: the restriction of $X$ on $\Delta$
- $m|n$: an integer $m$ divides an integer $n$
- $X^H$: the set of $H$-conjugates of $X$
- $|X|_p$: maximal power of $p$ dividing the order of $X$
- $I(X)$: the set of involutions in $X$
- $D_m$: dihedral group of order $m$

In this paper all sets and groups are finite.
2. Preliminaries

**Lemma 2.1.** Let $G$ be a transitive permutation group on $\Omega$, $\alpha \in \Omega$ and $N^\alpha$ a normal subgroup of $G_\alpha$ such that $F(N^\alpha) = \{\alpha\}$. Let the subgroup $X \leq N^\alpha$ be conjugate in $G_\alpha$ to every group $Y$ which lies in $N^\alpha$ and which is conjugate to $X$ in $G$. Then $N_\alpha(X)$ is transitive on $\Delta = \{\gamma \in \Omega | X \leq N^\gamma\}$.

Proof. Let $\beta \in \Delta$ and let $g \in G$ such that $\beta^g = \alpha$. Then, as $X \leq N^\beta$, $X^\beta \leq N^\beta = N^\alpha$. By assumption, $(X^\beta)^h = X$ for some $h \in G_\alpha$. Hence $gh \in N_\alpha(X)$ and $\alpha^{(gh)^{-1}} = \alpha^g = \beta$. Obviously $N_\alpha(X)$ stabilizes $\Delta$. Thus Lemma 2.1 holds.

**Lemma 2.2.** Let $G$ be a doubly transitive permutation group on $\Omega$ of even degree and $N^\alpha$ a nonabelian simple normal subgroup of $G_\alpha$ with $\alpha \in \Omega$. If $C_G(N^\alpha) \neq 1$, then $N^\alpha = N^\alpha \cap N^\beta$ for $\alpha \neq \beta \in \Omega$ and $C_G(N^\alpha)$ is semiregular on $\Omega - \{\alpha\}$.

Proof. See Lemma 2.1 of [4].

**Lemma 2.3.** Let $G$ be a transitive permutation group on $\Omega$, $H$ a stabilizer of a point of $\Omega$ and $M$ a nonempty subset of $G$. Then

$$|F(M)| = |N_\alpha(M)| \times |M^{\alpha} \cap H| / |H|.$$

Here $M^{\alpha} \cap H = \{g^{-1}Mg | g^{-1}Mg \subseteq H, g \in G\}$.

Proof. See Lemma 2.2 of [4].

**Lemma 2.4.** Let $G$ be a doubly transitive permutation group on $\Omega$ and $N^\alpha$ a normal subgroup of $G_\alpha$ with $\alpha \in \Omega$. Assume that a subgroup $X$ of $N^\alpha$ satisfies $X^{\alpha^X} = X^{\alpha}$. Then the following hold.

(i) $|F(X) \cap \beta^{N^\alpha}| = |F(X) \cap \gamma^{N^\alpha}|$ for $\beta, \gamma \in \Omega - \{\alpha\}$.

(ii) $|F(X)| = 1 + |F(X) \cap \beta^{N}| \times r$, where $r$ is the number of $N^\alpha$-orbits on $\Omega - \{\alpha\}$.

Proof. Let $\Gamma = \{\Delta_1, \Delta_2, \ldots, \Delta_r\}$ be the set of $N^\alpha$-orbits on $\Omega - \{\alpha\}$. Since $G_\alpha$ is transitive on $\Omega - \{\alpha\}$ and $G_\alpha \supseteq N^\alpha$, we have $|\Delta_i| = |\Delta_j|$ for $1 \leq i, j \leq r$. By assumption, $G_\alpha = N_{G_\alpha}(X)N^\alpha$ and so $N_{G_\alpha}(X)$ is transitive on $\Gamma$. Hence for each $i$ with $1 \leq i \leq r$ there exists $g \in N_{G_\alpha}(X)$ such that $(\Delta_i)^g = \Delta_i$. Therefore $|F(X) \cap \Delta_i| = |F(X^g) \cap (\Delta_i)^g| = |F(X) \cap \Delta_i|$. Thus (i) holds and (ii) follows immediately from (i).

**Lemma 2.5** (Huppert [5]). Let $G$ be a doubly transitive permutation group on $\Omega$. Suppose that $\vartheta(G) \neq 1$ and $G_\alpha$ is solvable. Then for any involution $z$ in $G_\alpha$, $|F(z)|^2 = |\Omega|$.

We list now some properties of $PSL(2, q)$ with $q$ odd which will be required
in the proof of our theorem.

**Lemma 2.6** ([2], [6], [10]). Set $N = \text{PSL}(2, q)$ and $G = \text{Aut}(N)$, where $q = p^n$ and $p$ is an odd prime. Let $z$ be an involution in $N$. Then the following hold.

(i) $|N| = (q-1)q(q+1)/2$, $I(N) = z^N$ and $C_N(z) = D_{q-1}$, where $q \equiv \varepsilon \in \{\pm 1\}$ (mod 4).

(ii) If $q \neq 3$, $N$ is a nonabelian simple group and a Sylow $r$-subgroup of $N$ is cyclic when $r \neq 2$, $p$.

(iii) If $X$ and $Y$ are cyclic groups of $N$ and $|X| = |Y| \neq 2$, $p$, then $X$ is conjugate to $Y$ in $\langle X, Y \rangle$ and $N_N(X) = D_{q-1}$.

(iv) If $X \leq N$ and $X = Z_2 \times Z_2$, $N_N(X)$ is isomorphic to $A_4$ or $S_4$.

(v) If $|N|_2 \geq 8$, $N$ has two conjugate classes of four-groups in $N$.

(vi) There exist a field automorphism $f$ of $N$ of order $n$ and a diagonal automorphism $d$ of $N$ of order 2 and if we identify $N$ with its inner automorphism group, $\langle d \rangle N = \text{PGL}(2, q)$, $\langle f \rangle d \, N = G$ and $G/N = Z_2 \times Z_n$.

(vii) $C_N(d) = D_{q+1}$ and $C_{\langle d \rangle N}(z) = D_{q-1}$.

(viii) Suppose $n = mk$ for positive integers $m$, $k$. Then $C_N(f^m) = \text{PSL}(2, p^n)$ if $k$ is odd and $C_N(f^m) = \text{PGL}(2, p^n)$ if $k$ is even.

(ix) Assume $n$ is even and let $u$ be a field automorphism of order 2. Then $I(G) = I(N) \cup d^N \cup u\langle d \rangle N$. If $n$ is odd, $I(G) = I(N) \cup d^N$.

(x) If $H$ is a subgroup of $N$ of odd index, then one of the following holds:

1. $H$ is a subgroup of $C_N(z)$ of odd index for some involution $z \in N$.
2. $H = \text{PGL}(2, p^n)$, where $n = 2mk$ and $k$ is odd.
3. $H = \text{PSL}(2, p^n)$, where $n = mk$ and $k$ is odd.
4. $H = A_4$ and $q \equiv 3, 5$ (mod 8).
5. $H = S_4$ and $q \equiv 7, 9$ (mod 16).
6. $H = A_5$, $q \equiv 3, 5$ (mod 8) and $5|(q-1)q/q+1|.$

**Lemma 2.7.** Let $G$, $N$, $d$ and $f$ be as defined in Lemma 2.6 and $H$ an $\langle f, d \rangle$-invariant subgroup of $N$ isomorphic to $D_{q-1}$. Let $W$ be a cyclic subgroup of $\langle d \rangle H$ of index 2 (cf. (vii) of Lemma 2.6) and set $Y = 0_d(W \cap H)$. Then $C_G(Y) = W \cdot C_{\langle f \rangle N}(Y)$.

Proof. By (viii) of Lemma 2.6, we can take an involution $t$ satisfying $\langle d \rangle H = \langle t \rangle W$ and $[f, t] = 1$. Since $N_G(Y) = \langle f, d \rangle N_N(Y) = \langle f, d \rangle H$, $C_G(Y) = C_{\langle f, d \rangle H}(Y) = W \cdot C_{\langle f \rangle \times \langle t \rangle N}(Y)$. Suppose $ht \in C(Y)$ for some $h \in \langle f \rangle$. Since $t$ inverts $Y$, $h$ also inverts $Y$ and so $h^2$ centralizes $Y$. Hence some nontrivial 2-element $g \in \langle h \rangle$ inverts $Y$, so that $C_Y(g)$ contains no element of order 4, contrary to (viii) of Lemma 2.6.

Throughout the rest of the paper, $G^\Omega$ will always denote a doubly transitive permutation group satisfying the hypothesis of our theorem and we assume $G^\Omega$ has no regular normal subgroup.
Notation. \(C^* = C_G(N^*)\), which is semi-regular on \(\Omega - \{\alpha\}\) by Lemma 2.2. Let \(r\) be the number of \(N^*\)-orbits on \(\Omega - \{\alpha\}\).

Since \(G_\alpha \supseteq N^*\), \(|\beta^N| = |\gamma^N|\) for \(\beta, \gamma \in \Omega - \{\alpha\}\) and so \(|\Omega| = 1 + r \times |\beta^N|\).

Hence \(r\) is odd and \(N^*_\beta\) is a subgroup of \(N^*\) of odd index. Therefore \(N^*_\beta\) is isomorphic to one of the groups listed in (x) of Lemma 2.6. Accordingly the proof of our theorem will be divided in six cases.

**Lemma 2.8.** Let \(Z\) be a cyclic subgroup of \(N^*_\beta\) with \(|Z| \neq 1, p\). Then

(i) \(|Z| = 2, |F(Z)| = 1 + (q-\varepsilon) |I(N^*_\beta)|/|N^*_\beta|\).

(ii) \(|Z| \neq 2, |F(Z)| = 1 + |N^*_\beta(Z)|/|N^*_\beta(Z)|\).

Proof. It follows from Lemma 2.3, 2.4 and 2.6 (i), (iii).

**Lemma 2.9.** Let \(Z\) be a cyclic subgroup of \(N^*_\beta\) with \(|Z| \neq 1, p\) and \(L_\sigma(Z)^{F(Z)}\) is doubly transitive. Then \(C^* = 1\) and one of the following holds.

(i) \(N_\sigma(Z)^{F(Z)} \leq \text{AGL}(1, q_1)\) for some \(q_1\).

(ii) \(C_\sigma(Z)^{F(Z)} \supseteq \text{PSL}(2, p_1), r = 1\) and \(|F(Z)| = 1 = |N^*_\beta(Z)| = N^*_\beta(Z)| = p_1\), where \(p_1 (\geq 5)\) is a prime.

(iii) \(N_\sigma(Z)^{F(Z)} = R(3), the smallest Ree group, |F(Z)| = 28\).

Proof. Set \(N_\sigma(Z) = L\) and \(F(Z) = \Delta\). By Lemma 2.6(iii), \(L \cap N^* = D_{t\pm}\) and \(L \cap N^* = L \cap N^* = N^*_\sigma\).

If \((L \cap N^*) = 1, then \(L \cap N^* = N^*_\beta\) because \(L \cap N^*\) is a maximal subgroup of \(N^*\). Since \(|N^*_\beta| = N^*_\beta\) is odd, \(L \cap N^* = N^*_\beta\) is a proper subgroup of \(N^*\), contrary to the assumption. Hence \((L \cap N^*) = 1\) and as \(L \supseteq L_\sigma \cap N^*\) and \(L \supseteq Y, (L_\sigma)^{\sigma}\) has a nontrivial cyclic normal subgroup. By Theorem 3 of [1], one of the following occurs:

(a) \(L^*\) has a regular normal subgroup

(b) \(L^* \supseteq \text{PSL}(2, p_1), |\Delta| = p_1 + 1, \) where \(p_1 (\geq 5)\) is a prime

(c) \(L^* \supseteq \text{PSL}(3, p_1), p_1 \geq 3, |\Delta| = (p_1) + 1\)

(d) \(L^* = R(3), |\Delta| = 28\).

Suppose \(C^* = 1\). Then there exists a subgroup \(D\) of \(C^*\) of prime order such that \((L_\sigma)^{\sigma} \supseteq D^*\). Since \([L_\sigma, D] \leq D \setminus L_\sigma \cap C^* = D(L_\sigma \cap C^*) = D, D\) is a normal subgroup of \(L_\sigma\). By (i) and (iii) of Lemma 2.6, \(G_\sigma = L_\sigma \cdot N^*\) and so \(D\) is a normal subgroup of \(G_\sigma\). By Theorem 3 of [1], \(G_\sigma\) has a regular normal subgroup, contrary to the hypothesis. Thus \(C^* = 1\).

If (a) occurs, \(L^*\) is solvable because \(L_\sigma/L \cap N^* = L_\sigma L^*/N^* \leq \text{Out}(N^*)\) and \(L \cap N^* = D_{t\pm}\). Hence by [5], (i) holds in this case.

If (b) occurs, we have \(Y^* = 1\), for otherwise \((L \cap N^*)^* = 1\) and so \(N^*_\beta = L \cap N^* = D_{t\pm}\), a contradiction. Hence \(1 = C_\sigma(Z)^{\sigma} \leq D^*\) and so \(C_\sigma(Z)^{\sigma} \supseteq \text{PSL}(2, p_1)\) and \(Y^* \supseteq Z_{p_1}\). Therefore \(|\Delta| = |\beta^N| = p_1\) and \(r = 1\) by Lemma 2.4 (ii). Since \(|\beta^N| = p_1\), we have \(|\beta^{L \cap N^*}| = p_1\), so that \(|L \cap N^*| = L \cap N^* = p_1\). Thus (ii) holds in this case.

The case (c) does not occur, for otherwise, by the structure of \(\text{PSU}(3, p_1)\),
a Sylow $p_1$-subgroup of $(L^\alpha)'$ is not cyclic, while $(L^\alpha)' \leq L \cap N^\alpha = D_{q^2}$, a contradiction.

3. Case (I)

In this section we assume that $N^\alpha_\beta \leq D_{q-r}$, where $\beta \neq \alpha$, $q = p^s$.

(3.1) (i) If $N^\alpha_\beta = \mathbb{Z}_2 \times \mathbb{Z}_2$, $N^\alpha_\beta(N^\alpha_\beta) = N^\alpha_\beta$ and $|F(N^\alpha_\beta)| = r+1$.

(ii) If $N^\alpha_\beta = \mathbb{Z}_2 \times \mathbb{Z}_2$, $N^\alpha_\beta(N^\alpha_\beta) = A_4$ and $|F(N^\alpha_\beta)| = 3r+1$.

Proof. Put $X = N^\alpha_\beta(N^\alpha_\beta)$. Let $S$ be a Sylow 2-subgroup of $N^\alpha_\beta$ and $Y$ a cyclic subgroup of $N^\alpha_\beta$ of index 2. If $N^\alpha_\beta \neq \mathbb{Z}_2 \times \mathbb{Z}_2$, then $|Y| > 2$ and so $Y$ is characteristic in $N^\alpha_\beta$. Hence $X \leq N^\alpha_\beta(Y) = D_{q-r}$. From this $[N^\alpha_\beta(S), S \cap Y] \leq S \cap Y$ and $\mathfrak{g}(N^\alpha_\beta(S))$ stabilizes a normal series $S \unlhd S \cap Y \unlhd 1$, so that $\mathfrak{g}(N^\alpha_\beta(S)) \leq C_{N^\alpha_\beta}(S)$ by Theorem 5.3.2 of [2]. By Lemma 2.6(i), $C_{N^\alpha_\beta}(S) \leq S$ and hence $N^\alpha_\beta(S) = S$. On the other hand by a Frattini argument, $X = N^\alpha_\beta(S)N^\alpha_\beta$ and so $X = N^\alpha_\beta$. By Lemma 2.6(ii), $(N^\alpha_\beta)^{N^\alpha_\beta} = (N^\alpha_\beta)^{N^\alpha_\beta}$ and so by Lemmas 2.3 and 2.4(ii), $|F(N^\alpha_\beta)| = 1 + |F(N^\alpha_\beta) \cap \beta^{N^\alpha_\beta}| \times r = 1 + |N^\alpha_\beta|/r |N^\alpha_\beta| = r+1$. Thus (i) holds.

If $N^\alpha_\beta = \mathbb{Z}_2 \times \mathbb{Z}_2$, $N^\alpha_\beta(N^\alpha_\beta) = A_4$ by Lemma 2.6(iv). Similarly as in the case $N^\alpha_\beta \neq \mathbb{Z}_2 \times \mathbb{Z}_2$, we have $|F(N^\alpha_\beta)| = 3r+1$.

(3.2) $N^\alpha_\beta/N^\alpha \cap N^\beta \leq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. By Lemma 2.2, it suffices to consider the case $C^\alpha = 1$. Suppose $C^\alpha = 1$. Then $N^\alpha_\beta/N^\alpha \cap N^\beta = N^\alpha_\beta/N^\beta \leq \text{Out}(N^\alpha) = \mathbb{Z}_2 \times \mathbb{Z}_2$ by Lemma 2.6(vi) and hence $(N^\alpha_\beta)^{N^\alpha_\beta} = N^\alpha_\beta(N^\alpha_\beta)$ is dihedral, $N^\alpha_\beta(N^\alpha_\beta) = \mathbb{Z}_2 \times \mathbb{Z}_2$, so that $N^\alpha_\beta/N^\alpha \cap N^\beta \leq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(3.3) Suppose $N^\alpha_\beta = N^\alpha \cap N^\beta$ and let $U$ be a subgroup of $N^\alpha_\beta$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then $|F(U)| = 3r+1$ and $N_\alpha(U)^{F(U)}$ is doubly transitive.

Proof. Sex $X = N^\alpha_\beta(N^\alpha_\beta)$, $\Delta = F(N^\alpha_\beta)$ and let $\{\Delta_1, \Delta_2, \ldots, \Delta_r\}$ be the set of $N^\alpha$-orbits on $\Omega - \{\alpha\}$. If $g^{-1}N^\alpha_\beta \leq G_{\alpha\beta}$, then $g^{-1}N^\alpha_\beta \leq N^\alpha \cap N^\beta = N^\alpha \cap N^\beta \leq N^\alpha$, where $\gamma = \alpha^\beta$. By a Witt's theorem, $X^\alpha$ is doubly transitive.

If $U$ is a Sylow 2-subgroup of $N^\alpha_\beta$, by a Witt's theorem, $N_\alpha(U)^{F(U)}$ is doubly transitive. Moreover $N^\alpha_\beta(U) = A_4$ and so by Lemmas 2.3 and 2.4(ii), $|F(U)| = 1 + |A_4| \times |N^\alpha_\beta|/r |N^\alpha_\beta| = 3r+1$.

If $|N^\alpha_\beta| > 4$, by Lemma 2.6(iv) and (v), $N^\alpha_\beta(U) = S_4$ and $N^\alpha_\beta$ has two conjugate classes of four-groups, say $\pi = \{K_1, K_2\}$. Set $X_\alpha = N^\alpha_\beta$. Then $M \geq N^\alpha_\beta$ and $X/M \leq Z_2$. Clearly $F(U) \cap \Delta_i = \emptyset$ for each $i$ and so $|F(U) \cap \Delta_i| = 3$ by Lemma 2.3. Hence $|F(U)| = 3r+1$. Since $N^\alpha_\beta(U) = S_4$, we may assume $r > 1$. Hence by (3.1) (i) $|\Delta| = r+1 \geq 4$, so that $M^\alpha$ is doubly transitive. Since $M = N^\alpha_\beta N_\alpha(U)$, $N_\alpha(U)^{M^\alpha}$ is also doubly transitive and so $N_\alpha(U)$ is transitive on $\Delta$—
\{\alpha\}$. As $|\Delta \cap \Delta_i| = 1$, $\Delta \cap \Delta_i \leq F(\Delta)$ and $N_{\alpha}(\Delta)$ is transitive on $F(\Delta) \cap \Delta_i$ for each $i$, $N_\alpha(U)^{F(U)}$ is doubly transitive.

(3.4) (i) $C^\alpha = 1$.

(ii) Let $U$ be a subgroup of $N_\beta^\alpha$ isomorphic to $Z_2 \times Z_2$. If $N_\beta^\alpha = N_\beta \cap N_\beta^\alpha$, then $N_\alpha(U)^{F(U)}$ has a regular normal 2-subgroup. In particular $|F(U)| = 3r + 1 = 2^b$ for positive integer $b$.

Proof. Since $N_{\alpha}(U)^{F(U)} \geq N_{\beta}(U)^{F(U)} \simeq S_3$ or $Z_2$, by (3.3) and Theorem 3 of [1], $N_\alpha(U)^{F(U)}$ has a regular normal subgroup, $N_\alpha(U)^{F(U)} \geq PSU(3,3)$ or $N_\alpha(U)^{F(U)} = R(3)$.

Suppose $C^\alpha \neq 1$. Let $D$ be a minimal characteristic subgroup of $C^\alpha$. Clearly $G_{\alpha} > D$. If $N_\alpha(U)^{F(U)} = R(3)$, $D$ is cyclic. By Theorem 3 of [1], $G_{\alpha}$ has a regular normal subgroup, contrary to the hypothesis. Hence $N_\alpha(U)^{F(U)} = R(3)$. Therefore $(N_\alpha(U)^{F(U)})'$ contains an element of order 9. Since $N_{\alpha}(U)^{C_\alpha}N_\alpha(U) \simeq N_{\alpha}(U)C_\alpha^\alpha N_\alpha(U)N_\beta \leq Out(N_\alpha(U))$, by (vi) of Lemma 2.6 we have $(N_\alpha(U)^{F(U)})' \leq C^\alpha \times N_\alpha(U)$. From this, $C^\alpha$ contains an element of order 9 and so $C^\alpha \simeq Z_9$ or $M_3(3)$. In both cases, $C^\alpha$ contains a characteristic subgroup of order 3. Since $G_{\alpha} > D$, by Theorem 3 of [1] $G^\alpha$ has a regular normal subgroup, a contradiction. Thus $C^\alpha = 1$.

Let $R$ be a Sylow 3-subgroup of $N_{\alpha}(U)$. Since $N_{\alpha}(U)/N_\alpha(U) = N_{\alpha}(U)N_\alpha(U)/N_\alpha(U) \leq Out(N_\alpha(U)) \simeq Z_2 \times Z_2$, $R/R' \cap N_\alpha(U)$ is cyclic. Clearly $R \cap N_\alpha(U) = Z_3$. Therefore $N_\alpha(U)^{F(U)} \geq PSU(3,3)$, $R(3)$. Thus (3.4) holds.

Since $N_\beta^\alpha$ is dihedral, we set $N_\beta^\alpha = \langle t \rangle W$ and $Y = W \cap N_\alpha^\alpha \cap N_\beta^\alpha$, where $W$ is a cyclic subgroup of $N_\beta^\alpha$ of index 2 and $t$ is an involution in $N_\beta^\alpha$ which inverts $W$.

(3.5) (i) If $|Y| \geq 3$, $N_\alpha(Y)^{F(Y)}$ is doubly transitive.

(ii) If $|Y| < 3$, $N_\beta^\alpha = Z_2 \times Z_2$ or $N_\beta^\alpha = D_2$ and $N_\alpha^\alpha \cap N_\beta \leq Z_2 \times Z_2$.

Proof. Suppose $|Y| \geq 3$. If $Y^\epsilon \leq G_{\alpha^\beta}$, $Y^\epsilon \leq N_\alpha^\alpha \cap G_{\alpha^\beta} \leq N_\alpha^\alpha$, where $\gamma = \alpha^\epsilon$. If $\gamma = \alpha^\epsilon$, obviously $Y^\epsilon \leq N_\alpha^\alpha$. If $\gamma \neq \alpha^\epsilon$, $N_\alpha^\epsilon = N_\beta^\epsilon$. Therefore, as $|Y| \geq 3$, $N_\alpha^\epsilon$ has a unique cyclic subgroup of order $|Y|$. Hence $Y^\epsilon \leq N_\alpha^\epsilon \cap N_\beta = N_\alpha^\epsilon$. Similarly $Y^\epsilon \leq N_\beta^\epsilon$. Thus $Y^\epsilon \leq N_\alpha^\epsilon \cap N_\beta^\epsilon$ and so $Y^\epsilon = Y$. By a Witt’s theorem, $N_\alpha(Y)$ is doubly transitive on $F(Y)$.

Suppose $|Y| < 3$. Since $|N_\alpha^\alpha \cap N_\beta^\alpha| = 2$, we have $N_\alpha^\alpha \cap N_\beta^\alpha \leq Z_2 \times Z_2$. On the other hand, as $N_\beta^\alpha$ is dihedral, $(N_\beta^\alpha)'$ is cyclic. Hence (ii) follows immediately from (3.2).

(3.6) Set $\Delta = F(N_\beta^\alpha)$, $L = G(\Delta)$, $K = G_\Delta$ and suppose $N_\beta^\alpha \neq Z_2 \times Z_2$. Then $L \geq N_\beta^\alpha$, $(L_\alpha)' \leq N_\beta^\alpha$, $K' \leq N_\alpha \cap N_\beta^\alpha$ and $(L_\alpha)^a = Z_r$. If $r \neq 1$, $L^\alpha$ is a doubly transitive Frobenius group of degree $r + 1$.

Proof. By Corollary B1 of [7] and (i) of (3.1), $L^\alpha$ is doubly transitive and
Since $N^a \cap L \succeq N^a \cap K = N^a_{\beta}$, by (i) of (3.1), we have $N^a \cap L = N^a_{\beta}$. Hence $L_a \succeq N^a_{\beta}$. By (i) of (3.4), $L_a/N^a_{\beta} = L_a/N^a_{\beta}/N^a \leq \Out(N^a) = Z_2 \times Z_2$ and so $(L_a)^2 \simeq Z_r$. If $r \neq 1$, then $(L_a)^2 \neq 1$. On the other hand $(L_a)^2 = 1$ as $(L_a)^2$ is abelian. Hence $L^a$ is a Frobenius group.

(3.7) Suppose $|Y| \geq 3$. Then there exists an involution $z$ in $N^a_{\beta} \cap Y$ such that $Z(N^a_{\beta}) = \langle z \rangle$.

Proof. Since $N^a_{\beta} \neq Z_2 \times Z_2$, $|N^a_{\beta}| \geq 2^2$ and $N^a_{\beta}$ is dihedral, we have $\langle I(W) \rangle = Z(N^a_{\beta}) = Z_2$ and $N^a_{\beta}/N^a_{\beta} = Z_2 \times Z_2$. Let $Z(N^a_{\beta}) = \langle z \rangle$ and suppose that $z$ is not contained in $Y$. By (3.2), $(N^a_{\beta})' \leq N^a \cap N^a_{\beta} \cap W = Y$ and so $|N^a_{\beta}'|$ is odd. Hence $|N^a_{\beta}| = 4$ and $q \equiv 3$ or 5 (mod 8), so that $n$ is odd. By (3.2) and (i) of (3.4), $N^a_{\beta}/N^a_{\beta} \simeq N^a_{\beta}/N^a_{\beta} \leq Z_2$. If $N^a_{\beta} = N^a \cap N^a_{\beta}$, then $W = Y$ and so $z \in Y$, contrary to the assumption. Therefore we have $N^a_{\beta} \cap N^a_{\beta} = Z_2$ and $N^a_{\beta} = \langle z \rangle \times (N^a \cap N^a_{\beta})$. Since $n$ is odd and $z \trianglelefteq N^a \cap N^a_{\beta} = Z_2$, by Lemma 2.6 (vi), (vii) and (ix), $N^a_{\beta} = \PGL(2,q)$ and $C_{N^a}(z) = D_{q-1}$. But $N^a_{\beta} \cap N^a \leq C_{N^a}(z)$ and besides it is isomorphic to a subgroup of $D_{q-1}$. Hence $N^a_{\beta} \cap N^a = Z_2$ and $\langle z \rangle \times Z_2$, a contradiction.

(3.8) Suppose $|Y| \geq 3$. Then $N^a_{\beta} = N^a \cap N^a_{\beta}$.

Proof. Suppose $N^a_{\beta} \neq N^a \cap N^a_{\beta}$ and let $\Delta, L, K$ be as defined in (3.6) and $x \in L_a$ such that its order is odd and $\langle x \rangle$ is transitive on $\Delta - \{a\}$. As $|Y| \geq 3$, $W$ is characteristic in $N^a_{\beta}$ and hence by (3.6), $x$ stabilizes a normal series $L_a \succeq N^a_{\beta} \succeq W \succeq (N^a_{\beta})'$. By Theorem 5.3.2 of [2], $[x, 0_{L_a}(N^a_{\beta})'] = 1$. Since $L_a/(N^a_{\beta})'$ has a normal Sylow 2-subgroup and $(N^a_{\beta})' \leq K'$, we have $[x, 0_{L_a}(K')] = 1$, so that $[x, N^a_{\beta}] \leq K' \leq N^a \cap N^a_{\beta}$ by (3.6). If $r \neq 1$, then $\beta^2 + \beta$ and $\beta^2 \in \Delta$, hence $N^a_{\beta} = x^{-1}N^a_{\beta}x = N^a_{\beta}$, where $\gamma = \beta^2$. Since $\gamma \in \Delta$ and $\Delta = F(N^a_{\beta})$, $N^a_{\beta} \leq N^a \cap G_{\gamma} = N^a_{\beta}$ and so $N^a_{\beta} = N^a_{\beta}$. Similarly $N^a_{\beta} = N^a_{\beta}$. Hence $N^a_{\beta} = N^a_{\beta}$, which implies $N^a_{\beta} = N^a \cap N^a_{\beta}$. By the doubly transitivity of $G$, we have $N^a_{\beta} = N^a \cap N^a_{\beta}$, contrary to the assumption. Therefore we obtain $r = 1$.

Let $z$ be as defined in (3.7) and put $k = (q-\varepsilon)/|N^a_{\beta}|$. By Lemma 2.8(i) we have $|F(z)| = 1 + (q-\varepsilon)(|N^a_{\beta}|/2 + 1)/|N^a_{\beta}| = (q-\varepsilon)/2 + k + 1$. Similarly $|F(Y)| = k + 1$. As $N^a_{\beta} = N^a \cap N^a_{\beta}$, there is an involution $t$ in $N^a_{\beta}$ which is not contained in $N^a$. By Lemma 2.6 (i), $t^2 = z$ for some $y \in N^a$. Set $\gamma = \beta^2$. Then $\gamma \in F(z)$ and $z \in N^a_{\beta}$. By Lemma 2.6 (vii), (viii) and (ix), $C_{N^a}(z) = D_{q+1}$ or $\PGL(2,\sqrt{q})$. Assume $C_{N^a}(z) = D_{q+1}$ and let $R$ be a cyclic subgroup of $C_{N^a}(z)$ of index 2. We note that $R$ is semi-regular on $\Omega - \{\alpha\}$. Set $X = C_{\alpha}(z)$. Since $2 \leq k + 1 \leq (q-\varepsilon)/|q-\varepsilon| + 1$, we have $(q+\varepsilon)/2 + k + 1$ and so $|\alpha^x| > k + 1$. By (i) of (3.5) and (3.7), $N_\alpha(Y) \leq C_{\alpha}(z) = X$ and $\alpha^x \leq F(Y)$. It follows from Lemma 2.1 that $\alpha^x = \{z \in N^a \mid \alpha \in N^a \}$;$\gamma$. Hence $|F(z)| \geq |\alpha^x| \geq |F(Y)| \geq (q+\varepsilon)/2 + k + 1 + (q-\varepsilon)/2 + \varepsilon = |F(z)| + \varepsilon$. Therefore $\varepsilon = -1$ and $\gamma^x = \{\gamma\}$, so that $\gamma \in F(Y)$, a contradiction. Thus $C_{N^a}(z) = \PGL(2,\sqrt{q})$, $\varepsilon = 1$, $N^a_{\beta}/N^a \cap N^a_{\beta} = Z_2$ and $|\langle z \rangle \cap G_{\alpha} : N^a_{\beta}| = 2$. Some Doubly Transitive Permutation Groups 803
Set $\Delta_1=\alpha x$ and $\Delta_2=F(z)-\Delta_1$. Let $\delta \in \Delta_2$ and $g$ an element of $G$ satisfying $\delta^g=\gamma$. Then $z \in N_G^* N^3-N^4$ and so $z^G \in N_G N^3-N^4$, where $v=\alpha x$. Since $|\langle v \cap G_\gamma \rangle| = |N^1|=2$ and $x \in G_\gamma \cap N^1$, it follows from Lemma 2.6 (ix) that $(z^g)^x=z$ for some $h \in G_\gamma$. Hence $g \in X$ and $\delta^g=\gamma$. Thus $\Delta_2=\gamma x$. Let $\delta \in \Delta_2$. Then $\delta \in N_G^*$ and $\gamma \in Z(N_G^*)$ by (3.7) and so $X \cap N_G^* = Z_X \times Z_2$, which implies $|\delta^{(c_x)(v)}|=|\alpha x|=|\alpha x|=|(q-1)/4|$. Hence $(|\Delta_1|,|\Delta_2|)=|(q-1)/4+k+1,(q-1)/4)$ or $(k+1,(q-1)/2)$. Let $P$ be a subgroup of $C_N(x)$ of order $\sqrt{q}$. Then $F(P)=\{\gamma\}$ and $P$ is semi-regular on $\Omega-M$. If $|\Delta_2|=(q-1)/4$, then $\sqrt{q} |(q-1)/4-1=(q-5)/4$ and $\sqrt{q} |(q-1)/4+k+1$. From this, $q=5^2$, $k=3$, $|\Delta_1|=10$ and $|\Delta_2|=6$. Since $C_N(x)^z=S_3$, $X^z=S_3$ and so $|X|=3^2$. As $X$ acts on $\Delta_1$ and $|\Delta_1|=1 (mod 3)$, $|G_\alpha| \geq |X_\alpha| \geq 3^2$, contrary to $N_G^* \cong PSL(2,25)$. If $|\Delta_2|=(q-1)/2,\sqrt{q} |(q-1)/2-1=(q-3)/2$, so $q=3^2$, $k=1$, $N^\sigma=D_6$ and $\Delta_1=\{\alpha, \beta\}$. Hence $C_N(x)$ fixes $\alpha$ and $\beta$, so that $\Gamma(2,3) \approx C_N(x) \leq N^\sigma \approx N^\sigma \approx D_6$, a contradiction.

(3.9) Suppose $|Y| \geq 3$. Then $r=1$.

Proof. By (3.6), $r+1=2^c$ for some integer $c \geq 0$. On the other hand $|X| \geq 3$ by (3.8) and (ii) of (3.4). Hence $2r=2^c(2^e-1)$ and so $c=1$ as $r$ is odd. Thus $r=1$.

(3.10) Put $k=(q-\epsilon)/|N_\gamma^z|$. If $N_\beta^z=N^* \cap N^\beta$ and $r=1$, then

$q-\epsilon + 2k + 2((2k+2-\epsilon) (k+1-\epsilon))+1 (2k+2-\epsilon) (k+1-\epsilon)$.

Proof. Set $S=\{(\gamma, u) | \gamma \in F(u), u \in z^G\}$, where $z$ is an involution in $N_G^*$.

We now count the number of elements of $S$ in two ways. Since $N_\beta^z=N^* \cap N^\beta$, $F(z)=\{\gamma \in F^G | z^G \in F^G\}$ and hence $C_G(z)$ is transitive on $F(z)$ by Lemma 2.1. Therefore $|S|=|\Omega| \cdot |z^G|=|z^G| \cdot |F(z)|$. Since $r=1$, $|\Omega|=1+|N^\sigma|: N^*|^z=k(q+\epsilon)/2+1$ and so $|\Omega|^z=|z^G|=(q+\epsilon)/2+k+1$. Since $G_\alpha \leq N^\sigma$, $z^G \alpha$ is contained in $N^\sigma$ and so $|G_\alpha| : C_N^z(x)|=|N^\sigma| : C_N^z(x)|=q(q+\epsilon)/2$. Hence $(q+\epsilon)/2+k+1 | (kq+q+\epsilon+1)/2 | q(q+\epsilon+1)/2$. On the other hand $|F(z)|=|C_G(z)| \leq |G_\alpha| \leq |G_\alpha| \leq |\Omega|^z$ because $|G_\alpha| : C_N^z(x)|=q(q+\epsilon+1)/2$ (mod 2). Hence $|q+\epsilon+2k+2| \leq kq+q+\epsilon+2$. Since $kq+q+\epsilon+2=(kq+q+\epsilon-k-1)$ and $q+q+\epsilon+2=(q+2\epsilon-k+2)$, we have (3.10).

(3.11) Suppose $|Y| \geq 3$. Then one of the following holds.

(i) $N_\beta^z=N^* \cap N^\beta=D_q=-$. 

(ii) $N_\beta^z=N^* \cap N^\beta=D_q=\ast$ and $N_G(Y)^{F(Z)}$ has a regular normal subgroup.

Proof. Suppose false. Then, by (3.5), (3.8) and Lemma 2.9, $N_G(Y)^{F(Z)}=R(3)$ or there exists a prime $p_1 \geq 5$ such that $C_G(Y)^{F(Z)}=PSL(2,p_1)$ and $V/Y \approx Z_2$, where $V=C_N^z(Y)$. By (i) of (3.1) and (3.9), $F(N_\beta^z)=\{\alpha, \beta\}$. On the other hand, $(N_\beta^z)^{F(Z)}=N_\beta^z \cap Y=Z_2$. Hence $N_G(Y)^{F(Z)}=R(3)$ and $C_G(Y)^{F(Z)}=R(3)$.
PSL(2, p)\).

By (i) of (3.4) and Lemma 2.7, we have \( C_{G_e}(Y) = V\langle f_i \rangle \), where \( f_i \) is a field automorphism of \( N^* \). Let \( t \) be the order of \( f_i \), \( n = tm \) and let \( p^m = \pm 1 \) (mod 4). Clearly \( C_{G_e}(Y)^{(n)} \simeq V^{(n)} = Z_{t_i} \) and \( |C_{G_e}(Y)^{(n)}| \mid t \), so that \( (p_i - 1)/2 \mid t \).

First we assume that \( t \) is even and set \( t = 2t_i \). Then \( Y \leq C_{N^*}(f_i) = PGL(2, p^m) \) by Lemma 2.6 (viii). As \( |V/Y| = p_i \) and \( p_i \) is a prime, \( Y \) is a cyclic subgroup of \( C_{N^*}(f_i) \) of order \( p^m - 1 \) and \( (p^m - 1)/2(p^m - 1) = p_i \). Put \( s = \sum_{i=1}^{t_i} (p^m) \). Then \( (p^m + 1)/2 = p_i \), so that we have either (i) \( t_i = 1 \) and \( p_i = (p^m + 1)/2 \) or (ii) \( t_i \geq 2 \), \( p^m = 3 \) and \( p_i = s = 3 \). In the case (i), \( 2 \leq (p_i - 1)/2 = (p^m + 1)/4 \mid 2t_i = 2 \). Hence \( (p_i, q) = (5, 3) \) or \((4, 11)^2\). Let \( s \) be as in (3.7). As mentioned in the proof of (3.10), \( |F(z)| = (q-1)/2 + k + 1 \), \( |\Omega| = qk(q+1)/2 + 1 \) and \( C_G(z) \) is transitive on \( F(z) \). If \( q = 3 \), then \( |F(z)| = 46 \) and \( |\Omega| = 2 \cdot 19 \). Hence \( |C_{G_e}(z)| = |F(z)| / |C_{G_e}(z)N^*/N^*| = 46 \cdot 21/19 = 2 \cdot 11 \cdot 5 \cdot 23 \) with \( 0 \leq i \leq 3 \).

Let \( P \) be a Sylow 23-subgroup of \( C_{G_e}(z) \) and \( Q \) a Sylow 5-subgroup of \( C_{G_e}(z) \). Since \( 11 \nmid |\Omega| \), \( P \) is a subgroup of \( N^* \) for some \( \gamma \in \Omega \) and \( F(P) = \{ \gamma \} \). Hence \( \gamma \in \Lambda(z) \), contrary to \( C_G(z) \mid D_{120} \). In the case (ii), we have \( (p_i - 1)/2 = (k+1)/2 \mid t = 2t_i \). From this, \( 9i+1 \leq 4t_i \), hence \( t_i = 1 \), a contradiction.

Assume \( t \) is odd. Then \( Y \leq C_{N^*}(f_i) = PSL(2, p^m) \) by Lemma 2.6 (viii). As \( |V/Y| = p_i \) and \( p_i = 2 \) is a prime, \( Y \simeq Z_{(p^m - 1)/2} \) (mod \( q-\epsilon \)). Hence \( \sum_{i=1}^{t_i} (p^m) = p_i \) and \( (p_i - 1)/2 = (\sum_{i=1}^{t_i} (p^m) = (p_i - 1)/2 \mid t_i \). In particular \( 2t_i \geq (p^m)^{t_i} - (p^m)^{t_i-2} = (p^m)^{t_i-2} \geq 2(p^m)^{t_i-2} \). From this \( t_i = 3 \), \( m = 1 \), \( p_i = 7 \) and \( q = 3^2 \), so that \( N^* \simeq Z_2 \times Z_2 \), a contradiction.

(3.12) (i) of (3.11) does not occur.

Proof. Let \( G^a \) be a minimal counterexample to (3.12) and \( M \) a minimal normal subgroup of \( G \). By the hypothesis, \( G \) has no regular normal subgroup and hence \( M \neq 1 \). As \( M_a \) is a normal subgroup of \( G_a \), by (i) of (3.4), \( M_a \) contains \( N^* \). By (3.9), \( r \geq 1 \), hence \( M \) is doubly transitive on \( \Omega \). Therefore \( G = M \) and \( G \) is a nonabelian simple group.

Since \( N^* \simeq D_{k-1}, k = 1 \) and so \( q-\epsilon + 4 \leq 2(4-\epsilon)(2-\epsilon) + 1 \), \( 4-\epsilon \) by (3.10). Hence we have \( q = 7, 9, 11, 19, 27 \) or 43.

Let \( x \) be an element of \( N^* \). If \( |x| > 2 \), by Lemma 2.8, \( |F(x)| = 1 + |N^*| \times 1/|N^*| = 2 \) and if \( |x| = 2 \), similarly we have \( |F(x)| = (q-\epsilon)/2 + 2 \). Assume \( q = 9 \) and let \( d \) be an involution in \( G_a - N^* \) such that \( \langle d \rangle N^* \) is isomorphic to \( PGL(2, p) \).
We may assume \( d \in G_{ab} \). Since \( \langle d \rangle \) is transitive on \( \Omega - \{ \alpha \} \), by Lemmas 2.3 and 2.6 (vii), (ix), \( |F(d)| = 2(q-1)(q+1/2)/2(q+1) = 1-(q+1)/2 \), while \( |F(x)| = (q+1)/2+2 \) for \( x \in I(N^\beta) \). Hence \( d \) is an odd permutation, contrary to the simplicity of \( G \). Thus \( G_a = N^\beta \) if \( q \neq 9, 27 \) and \( |G_a/N^\beta| = 1, 3 \) if \( q = 27 \).

If \( q = 9 \), \( |\Omega| = 1 + 9 - 10/2 = 2 \cdot 3 \) and \( |G_a| = 2^3 |PSL(2, 9)| = 2^3 = 3 \cdot 5 \) with \( 0 \leq i \leq 2 \). Let \( P \) be a Sylow 3-subgroup of \( G \). Since \( Aut(Z_{23}) \cong Z_7 \times Z_3 \), \( 3 \not| |N_0(P)| \), for otherwise \( P \) centralizes a nontrivial 3-element and so \( |F(P)| = 3 \), contrary to \( |F(P)| = 2 \). Similarly \( |F(x)| = 1 \), contrary to \( |F(x)| = 2 \).

Hence \( G_a \) contains a Sylow 2-subgroup \( S \) of \( G \). Let \( T \) be a Sylow 2-subgroup of \( N_0 \). Then \( T \) is isomorphic to \( Z_2 \times D_{2^7} \) or \( Z_2 \times D_{2^6} \). Suppose \( \langle t \rangle N_0^\beta = Z_2 \times D_{2^7} \). Then \( \langle t \rangle N_0^\beta \) contains fifteen involutions and so we can take \( u \in I(\langle t \rangle N_0^\beta) \) satisfying \( |F(u)| = 0 \) and \( |F(u^3)| = |\Omega|/2 = 28 \). By Lemma 2.3, \( 28 = |C_0(u)| \times |C_0(u) \cap u^\alpha|/24 \) and hence \( |C_0(u)| = 2 \cdot 3 \cdot 7 \) or \( 2 \cdot 3 \cdot 7 \). Since \( |C_0(u)| = 2 \cdot 3 \cdot 7 \), we have \( |C_0(u) \cap N_0(R)| = 2 \cdot 7 \) or \( 2 \cdot 7 \).

By a Sylow’s theorem, \( |C_0(u)| = 2 \cdot 7 \), so that \( |C_0(u)| = 2 \cdot 7 \). Let \( Q \) be a Sylow 7-subgroup of \( C_0(u) \). Then \( |C_0(u) \cap N_0(Q)| = 2 \cdot 7 \) or \( 2 \cdot 7 \) by a Sylow’s theorem. Hence \( 2 \cdot 3 \cdot 7 \). Since \( Aut(Z_7) \cong Z_2 \times Z_3 \),
5 \not| N_c(Q) \text{ and } 11 \not| N_c(Q) \text{ by the similar argument as in the case } q=9. Therefore \(|G: N_c(Q)| = 2^a \cdot 5 \cdot 11\) for some a with \(0 \leq a \leq 3\). Hence \(|G: N_c(Q)| \equiv 1 \pmod{7}\), a contradiction. Thus \(<t> N_b^{a} = D_{2^a}\).

Let \(U\) be a Sylow 2-subgroup of \(N_b^{a}\) and set \(L = N_G(U)\). It follows from (3.3) and Lemma 2.6 (iv) that \(L \cap N_b^{a} = A_4, L^{(2)} = A_4\) and \(|L| = 2^a 3\). Let \(T, <\alpha>\) be Sylow 2- and 3-subgroup of \(L\), respectively. Obviously \(L \supset T\) and \(|C_T(x)| = 1\).

On the other hand \(T \supset L \supset T' = D_{2^a}\) and so \(T = Z_2 \times Z_2\) because \(C_T(x)\) is a 2-group, so that \(C_T(x) = T\) contrary to the Sylow's theorem.

(3.13) (ii) of (3.11) does not occur.

Proof. Let \(G^a\) be a doubly transitive permutation group satisfying (ii) of (3.11). Let \(x\) be an involution in \(N_b^{a}\) with \(x \not\in \Omega\). Then \(F(x^F(Y)) = F^2(Y) = \{x, \beta\}\) by (i) of (3.1) and (3.9). Since \(|F(Y)| = 1 + (q - \varepsilon)|N_b^{a}| = 1 + k \geq \frac{q - \varepsilon}{2}\), \(x^F(Y)\) is an involution. By Lemma 2.5, \(1 + k = 2^a\) and so \(k = 3\). By (3.11), \(q - \varepsilon + 8|2((q - \varepsilon)(4 - \varepsilon) + 1)\) if \(\varepsilon = 1\) and \(q + 9|2^a 3^i 5^j 7^k\) if \(\varepsilon = -1\). Since \(k = 3\), \(q - \varepsilon + 8|2((q - \varepsilon)(4 - \varepsilon) + 1)\) if \(\varepsilon = 1\) and \(q + 9|2^a 3^i 5^j 7^k\) if \(\varepsilon = -1\). Therefore \(q = 5^2, 7^2, 11^2, 59\) or 71.

Let \(p_1\) be an odd prime such that \(p_1|\Omega\) and \(p_1 \not\mid |G_a|\) and let \(P\) be a Sylow \(p_1\)-subgroup of \(G\). Clearly \(P\) is semi-regular on \(\Omega\) and so any element in \(C_G(P)\) has at least \(p_1\) fixed points. If \(x\) is an element of \(N_b^{a}\) and its order is at least three, \(|x^F(Y)| = |F^2(Y)| = 4\) by Lemma 2.8. Since \(|N_b^{a}| = (q - \varepsilon)/3\), we have \(|\Omega| = 1 + |N_b^{a}| = 1 + 3(q + \varepsilon)/2\).

If \(q = 5^2\), then \(|\Omega| = 2^a 61\) and \(|G_a| = 2^a 3^i 5^j 13\). Let \(P\) be a Sylow 61-subgroup of \(G\). Then \(P \cong Z_{61}\). As mentioned above, \(5, 13 \not\mid |C_G(P)|\) and so \(5^2, 13 \not\mid |N_G(P)|\). Hence \(|G: N_G(P)| = 2^a 3^i 5^j 13\), where \(0 \leq a \leq 10\) and \(0 \leq b, c \leq 1\). But we can easily verify \(|G: N_G(P)| \equiv 1 \pmod{61}\), contrary to a Sylow's theorem.

If \(q = 7^2\), then \(|\Omega| = 2^a 919\) and \(|G_a| = 2^a 3^i 5^j 7^k\). Let \(P\) be a Sylow 919-subgroup of \(G\). By the similar argument as above, we obtain \(5, 7 \not\mid |N_G(P)|\) and so \(|G: N_G(P)| = 2^a 3^i 5^j 7^k \equiv 2^a 306\) or \(-2^a \pmod{919}\), where \(0 \leq a \leq 8\) and \(0 \leq b \leq 5\). Hence \(|G: N_G(P)| \equiv 1 \pmod{7}\), a contradiction.

If \(q = 11^2\), then \(|\Omega| = 2^a 173\) and \(|G_a| = 2^a 3^i 5^j 11^2 61\). Let \(P\) be a Sylow 173-subgroup of \(G\). Similarly we have \(3, 5, 11, 61 \not\mid |N_G(P)|\) and so \(|G: N_G(P)| = 2^a 3^i 5^j 11^2 61 \equiv -5 \cdot 2^a \pmod{173}\), where \(0 \leq a \leq 12\). Hence \(|G: N_G(P)| \equiv 1 \pmod{11}\), a contradiction.

If \(q = 59\), then \(|\Omega| = 2^a 173\) and \(|G_a| = 2^a 3^i 5^j 29 59\). Let \(P\) be a Sylow 173-subgroup of \(G\). Similarly we have \(3, 5, 29, 59 \not\mid |N_G(P)|\) and so \(|G: N_G(P)| = 2^a 3^i 5^j 29 59 \equiv 10 \cdot 2^a \pmod{59}\), where \(0 \leq a \leq 4\) and \(0 \leq b \leq 1\). From this, we have a contradiction.

If \(q = 71\), then \(|\Omega| = 2^a 233\) and \(|G_a| = 2^a 3^i 5^j 7^3 71\). Let \(P\) be
a Sylow $233$–subgroup of $G$. Since $3,5,7,71 \nmid |N_\alpha(P)|$, $|G|: N_\alpha(P)| = 2^a \cdot 3^3 \cdot 5 \cdot 7 \cdot 71 \equiv -3 \cdot 2^a \pmod{233}$, where $0 \leq a \leq 9$. Similarly we get a contradiction.

We now consider the case $|Y|<3$. By (ii) of (3.5), $N_\beta^a \simeq Z_2 \times Z_2$ or $N_\beta^a \simeq D_8$ and $N_\beta^a \cap N_\beta \leq Z_2 \times Z_2$.

(3.14) The case that $N_\beta^a = Z_2 \times Z_2$ does not occur.

Proof. Set $\Delta = F(N_\beta^a)$. Then $|\Delta| = 3r+1$ and $\Delta = F(N_\beta^a, N_\beta^a)$ by (ii) of (3.1) and Corollary B1 of [7]. Since $|N_\beta^a| = 4$, we have $q = p^a \equiv 3,5 \pmod{8}$ and so $n$ is odd. Hence $|G_{ab}/N_\beta^a| \leq 2$ and $N_\beta^a \cap N_\beta = N_\beta^a \cap N_\beta \simeq Z_2 \times Z_2$ by (3.2). Suppose $N_\beta^a \cap N_\beta = Z_2 \times Z_2$. Then $N_\beta^a N_\beta$ is a Sylow $2$–subgroup of $G_{ab}$, hence $N_\beta^a (N_\beta^a N_\beta) \leq N_\beta^a N_\beta \leq D_8$ and $|\Delta|$ is even, $C_8(N_\beta^a N_\beta)\alpha$ is also doubly transitive. Let $g$ be an element of $C_8(N_\beta^a N_\beta)$ such that $(1, \beta, \gamma, \delta)$ and $g' \in G_{ab}$, then $N_\beta^a = gN_\beta g = N_\beta^a$ and hence $N_\beta^a = N_\beta \cap N_\beta$, a contradiction. Thus $N_\beta^a = N_\beta \cap N_\beta \leq Z_2 \times Z_2$.

Let $z$ be an involution in $N_\beta^a$ and $t \in z^G$ an involution such that $\alpha^t = \beta$. Set $\Gamma = \{\{\gamma, \delta\} | \gamma, \delta \in \Omega, \gamma \neq \delta\}$. We consider the action of the element $z$ on $\Gamma$. By the similar argument as in the proof of (3.12), $|F(z)| = |(F(z)(-1)/2+(|\Omega|-|F(z)|)| = |C_8(z)||z^G \cap \langle t \rangle G_{ab}||\langle t \rangle G_{ab}|$. Since $|G_{ab}| = N_\beta^a \cap N_\beta$, by Lemma 2.6 (i), $z^G \cap \langle t \rangle G_{ab}$ and so $|C_8(z)| = |F(z)| \times |C_8(z)|$. Hence $|G_{ab}| = |(F(z)(-1)/2+(|\Omega|-|F(z)|)| = |F(z)||C_8(z)||z^G \cap \langle t \rangle G_{ab}|$, so that $|G_{ab}| \equiv 0 \pmod{|F(z)|}$. Since $|G_{ab}/N_\beta^a| = |G_{ab}N_\beta^a \cap N_\beta^a| \times |2n|$, we have $|G_{ab}| \equiv 8n$. Clearly $|\Omega| = 1+q(q-\varepsilon) (q+\varepsilon)r/4$ and by Lemma 2.8 (i), $|F(z)| = 1+3(q-\varepsilon)r/4$. Hence $1+3(q-\varepsilon)r/4 | 8n(1+q(q-\varepsilon) (q+\varepsilon)r/4)$. Put $n = rs$. Then $3qr - 3er + 4 | (4rs + g(q-\varepsilon) (q+\varepsilon)r) \equiv 3r - 3er (3q + 3er)$ and hence $3qr - 3er + 4 | (484r^2 + 4s(3pq) (3pq-3r) (3qr-3er))$. Since $3qr - 3er + 4 | 864r^2 + 4s(3er - 3er) \equiv 864r^2 - 32s(3er - 3er - 2)$. ($\ast$)

We argue that $r = 1$. Suppose false. Then $32s(3er - 4) (3er - 2) > 0$ and so $3(q-\varepsilon) < 864r^2$. Therefore $288m + \varepsilon > q = p^a \geq 3^a$ and so $288m > 3^a$. Hence $(n, r, p, \varepsilon) = (5, 3, 3, -1)$, $(3, 3, 3, -1)$ or $(3, 3, 5, 1)$, while none of these satisfy (3.14). Thus $r = 1$.

Hence $3q - 3\varepsilon + 4 | 64(5+9\varepsilon)n$ and $|F(z)| = 1+3(q-\varepsilon)r/4$. If $\varepsilon = 1$, then $3(3q-3\varepsilon + 4) \equiv 256m$. Hence $n = 1$ or $(n, p) = (5, 3)$, $(3, 3)$. Since $3q-3\varepsilon + 4 \equiv 256m$ and $3q-3\varepsilon + 4 \equiv 256m$, $n = 1$ and $3q-3\varepsilon + 4 \equiv 256$. From this, $q = 19$ or 83. If $\varepsilon = 1$, then $3(3q-3\varepsilon + 4) = 896n$ and so $n = 1$ or $(n, p) = (5, 3)$. Since $3q-3\varepsilon + 4 \equiv 896 \equiv 1$, we have $n = 1$ and $3q-3\varepsilon + 4 \equiv 896$. From this, $q = 5, 37$ or 149. As $PSL(2, 5) \simeq PSL(2, 4)$, $q = 5$ by [4]. Thus $q = 19, 37, 83$ or 149.

Set $m = z^G \cap \langle t \rangle G_{ab}$. As we mentioned above, $|G_{ab}| = |G(z)| \times |F(z)| = 1+3(q-\varepsilon)r/4$. Since $|G_{ab}/N_\beta^a| = 1$, or $2$, $|C_8(z)| = |G_{ab}| = (q-\varepsilon)/4$. Therefore $m = (2q^2 + (2q+9)q-9q^2)/(3q-3\varepsilon + 4)$. It follows that $(q, m) = (19, 27/2), (37, 28), (83, 449/8)$ or $(149, 411/4)$. Since $m$ is an integer, we have $(q, m) = (37, 28)$. But $m \leq |\langle t \rangle G_{ab}| \leq 16$, a contradiction. Thus (3.14)
The case that $N^a_β=D_8$ and $N^a ∩ N^β ≤ Z_2 × Z_2$ does not occur.

Proof. Let $Δ, L$ and $K$ be as defined in (3.6). By (3.6), there exists an element $x$ in $L_β$ such that its order is odd and $⟨x^γ⟩$ is regular on $Δ−{a}$. Since $(L_β)'≤N^a_β$ by (3.6) and $N^a ∩ N^β=N_β$, $x$ stabilizes a normal series $N^a_βN^a_β ≥ N_β$. Hence $x$ centralizes $N^a_βN^a_β$ by Theorem 5.3.2 of [2] and so $x^−1N^a_βz=xN^a_β$. Put $γ=β^2$. If $r=1$, then $β=γ$, so that $N_β ≅ N^a_β$. From this, $N_β ≅ N^a_β$. By the doubly transitivity of $G$, $N^a_β=N^a_β$, hence $N^a_β=N^a ∩ N^β$, a contradiction. Therefore $r=1$ and $Δ=\{α, β\}$.

Set $⟨x⟩=Z(ΛΓZ_2)$, $Δ=αc∈Γ$ and let \{Δ_1, Δ_2, ..., Δ_j\} be the set of $C_G(α)$-orbits on $F(z)$. Since $L_β ∩ N^a$ and by (3.2), $N^a ∩ N^β=1$, $z$ is contained in $N^a ∩ N^β$. Hence, by Lemma 2.1, $β∈Δ_1$ and $k$ is at least two. By Lemma 2.8, $|F(z)|=1+(q−ε)/8$ or $|N^a_β|=1+(q−ε)/8$. Clearly $|N^a(z)|=N^a_β/(q−ε)/8$ and so $|Δ_1| ≥ 1+(q−ε)/8$. If $γ∈F(z)−Δ_1$, then $C_{N^a_β}(z)≈Z_2 × Z_2$, for otherwise $\langle x⟩=Z(N^a_β)≤ N^a ∩ N^β$ and by Lemma 2.1 $γ∈Δ_1$, a contradiction. Hence one of the following holds.

(i) $k=3$ and $|Δ_1|=1+(q−ε)/8$, $|Δ_2|=|Δ_3|=(q−ε)/4$.
(ii) $k=2$ and $|Δ_1|=1+(q−ε)/8$, $|Δ_2|=(q−ε)/2$.
(iii) $k=2$ and $|Δ_1|=1+(q−ε)/8$, $|Δ_2|=(q−ε)/4$.

Let $γ∈F(z)−Δ_1$. Then, $z∈G_γ−N^β$ and so $C_{N^a_β}(z)≈D_{4+ε}$ or $PGL(2,√q)$ by Lemma 2.6 (vii), (viii), (ix). If $C_{N^a_β}(z)≈D_{4+ε}$, then $(q+ε)/2$ or $|Δ_1|$ and so $q=7$ and (iii) occurs. But $(q+ε)/2=3 |Δ_1|=1−1=1$, a contradiction. If $C_{N^a_β}(z)≈PGL(2,√q)$, then (i) does not occur because $√q ∏ q−ε$. Hence $\sqrt{q} | |Δ_1|$ and $\sqrt{q} | |Δ_2|$—1. From this, $q=25$ and (iii) occurs. In this case, we have $|Δ_1|=10$, so that an element of $C_{N^a}(z)$ of order 3 is contained in $N^a_β$ for some $δ∈Δ_1$, contrary to $N^a_β=N^a_β ≅ D_8$.

4. Case (II)

In this section we assume that $N^a_β=PGL(2, p^n)$, where $n=2mk$ and $k$ is odd. Since $n$ is even, $q=p^n≡1$ (mod 4). We set $p^n ≡ ε \equiv \{±1\}$ (mod 4). In section 7 we shall consider the case that $N^a_β=S_4$. Therefore we assume $(p,m)≠(3,1)$ in this section.

(4.1) The following hold.

(i) $N^a_β/N^a ∩ N^β≡1$ or $Z_2$ and $N^a ∩ N^β≥(N^a_β)'≈PSL(2, p^n)$.
(ii) If $⟨p,m⟩≡(5,1)$, there exists a cyclic subgroup $Y$ of $(N^a_β)'$ such that $N^a(Z(Y)) ≅ D_{4+ε}$ and $N^a_β(Y)^{F(Y)}$ is doubly transitive.

Proof. As $N^a_β/N^a ∩ N^β$, either $N^a_β/N^a ∩ N^β≤ Z_2$ or $N^a ∩ N^β≡1$. If $N^a ∩ N^β≡1$, by Lemma 2.2 and 2.6 (vii), $N^a_β=N^a_β/N^a ∩ N^β=N^a_β/N^β=N^a_β/Z_2 × Z_2$, a
contradiction. Therefore \( N_\alpha^*/N_\alpha \cap N_\beta \simeq 1 \) or \( N_\alpha \cap N_\beta \geq (N_\alpha^*)' \sim PSL(2,p^m) \).

Now we assume that \((p,m) \neq (3,1)\) and set \( z \) be an involution in \((N_\beta^*)'\). Then \( C_{N_\beta}(z) \simeq D_{2p^m-1} \) by Lemma 2.6 (vii). Suppose \( C_{N_\beta}(z) \) is not a 2-subgroup and put \( Y = 0(C_{N_\beta}(z)) \). Then, if \( Y^\alpha \leq G_{ab} \) for some \( g \in G \), we have \( Y^\alpha \leq N_\alpha \) and \( Y^\alpha \leq N_\beta^a \), where \( \gamma = \alpha^\varepsilon \) and \( \delta = \beta^\varepsilon \). By (i) \( Y^\alpha \leq N_\alpha \cap N_\beta^a \) and so \( Y^\alpha = Y^\beta \) for some \( h \in N_\alpha \cap N_\beta^a \). Thus \( N_\alpha(Y)^F(Y) \) is doubly transitive. Assume that \( C_{N_\beta}(z) \) is a 2-subgroup and set \( C_{N_\beta}(z) = \langle u, v | u^2 = u^{-1}, v^2 = 1 \rangle \). We may assume that \( v \in (N_\alpha^*)' \) and \( \langle u^2, v \rangle \) is a Sylow 2-subgroup of \((N_\beta^*)'\). Since \( p^m \neq 3,5 \), the order of \( u^2 \) is at least four. On the other hand there is no element of order \( |u^2| \) in \( \langle u, v | u^2 = u^{-1}, v^2 = 1 \rangle \). Hence any element of order \( |u^2| \) which is contained in \( N_\beta^a \) is necessarily an element of \( N_\alpha \cap N_\beta^a \). By the similar argument as above, \( N_\alpha(Y)^{F(Y)} \) is doubly transitive.

(4.2) Let notations be as in (4.1). Suppose \((p,m) \neq (3,1)\), \((5,1)\) and set \( \Delta = F(Y) \) and \( X = N_\alpha(Y) \). Then \( |\Delta| = rs(p^m+\varepsilon)/2+1 \), where \( s = \sum_{i=0}^{k} p^{2m_i} \), \( C_\alpha(N_\alpha) = 1 \) and one of the following holds.

(i) \( X^\alpha \leq AGL(1,2^c) \) for some integer \( c \).

(ii) \( X^\alpha = PSL(2,p_1) \) or \( PGL(2,p_1) \), \( r = 1 \) and \( 2p_1 = p^m+\varepsilon \).

Proof. By Lemma 2.8 (ii), \( |\Delta| = 1 + |N_\alpha \cap X|/r \) \( |N_\alpha \cap X| = 1 + (p^{2m_k}-1) r/2(p^m-\varepsilon) = rs(p^m+\varepsilon)/2+1 \). By (4.1) and Lemma 2.9, we have (i), (ii) or \( X^\alpha = R(3) \).

Assume that \( X^\alpha = R(3) \). Then \( rs(p^m+\varepsilon)/2+1 = 28 \), hence \( k = 1 \) and \( r(p^m+\varepsilon)/2 = 27 \). Since \( r \) is odd and \( r | 2m = n \), we have \( r = m = 1 \) and \( q = 53^2 \). But a Sylow 3-subgroup of \( X_\alpha \) is cyclic because \( N_\alpha \cap X \simeq D_{q-4} \) and \( X_\alpha/X \cap N_\alpha \simeq X_\alpha N_\alpha/N_\alpha \leq Z_2 \times Z_2 \), a contradiction. Thus (i) or (ii) holds.

(4.3) (i) of (4.2) does not occur.

Proof. Let notations be as in (4.2). Suppose \( X^\alpha \leq AGL(1,2^c) \) and \( W = C_{N_\alpha}(Y) \). Then \( Y \leq W \simeq Z_{p^m-1} \). Since \( C_\alpha(N_\alpha) \) is cyclic, \( W \) is a characteristic subgroup of \( C_\alpha(N_\alpha) \) and so \( W \) is a normal subgroup of \( X_\alpha \). Hence \( W \leq X_\Delta \) and \( (X \cap N_\alpha^a) = 1 \) or \( Z_2 \). By Lemmas 2.4 and 2.6, \( F(X \cap N_\alpha^a) = 1 + |X \cap N_\alpha^a|/|N_\alpha^a : X \cap N_\alpha^a|/r \) \( |N_\alpha^a : X \cap N_\alpha^a| \leq 2 + r \). Since \( 1 + r | |\Delta|, (X \cap N_\alpha^a)^a \leq Z_2 \) and hence \( (1+r)^2 = rs(p^m+\varepsilon)/2+1 \) by Lemma 2.5. From this, \( r = s(p^m+\varepsilon)/2-2 | mk \) and so \( p^{2m(k-1)}+mk \leq 2 \). Hence \( m = k = r = 1 \) and \( q = 7^2 \).

Let \( R \) be a Sylow 3-subgroup of \( N_\alpha^a \). Since \( N_\alpha^a = PGL(2,7) \), we have \( R = Z_3 \). By Lemmas 2.4 and 2.6, \( |F(R)| = 1 + (7^2-1) |N_\alpha^a : N_\alpha^a(R) / |N_\alpha^a : R| = 4 \). Hence \( N_\alpha(R)^F(R) = A_4 \) or \( S_4 \). But is a Sylow 3-subgroup of \( N_\alpha^a(R) \) because \( N_\alpha \simeq PSL(2,7) \), contrary to \( N_\alpha(R)^F(R) \simeq A_3 \) or \( S_3 \).

(4.4) (ii) of (4.2) does not occur.
Proof. Let notations be as in (4.2). Suppose \( X^\Delta \supseteq PSL(2, p_1) \). By the similar argument as in (4.3), \( C_N^\Delta(Y) \leq X_\Delta \) and so \( C_N^\Delta(Y) = Z_{p_1} \), and \( N_N^\Delta(Y)^\Delta = D_{2p_1} \). Hence \( |X^\Delta| = |2p_1 - 2n| \). Since \( X^\Delta \supseteq PSL(2, p_1) \), \( p_1 | p - 2 \) or \( |X^\Delta| = 2p_1 \). Hence \( (p, m, p_1) = (11, 1, 5), (3, 2, 5) \) or \( (3, 3, 13) \).

Let \( R \) be a cyclic subgroup of \( N^\Delta \) such that \( R = Z(p^m + 2) \). By Lemma 2.6, \( N^\Delta(R)^{(R)} \) is doubly transitive and by Lemma 2.8 (ii), \( |F(R)| = 1 + |N_N^\Delta(R)|/|N^\Delta(N^\Delta(R))| = 42 \) and \( N^\Delta(R)^{(R)} = Z_5 \). Since \( |N^\Delta(R) N^\Delta(R^\Delta)| = 6 \), \( N^\Delta(R)^{(R)} = N^\Delta(R)^{(R)} \). Hence \( N_N^\Delta(R) / K = Z_5 \) where \( K = (N_N^\Delta(R))^\Delta \). But \( N_N^\Delta(R) / (N_N^\Delta(R))^\Delta = Z_2 \times Z_2 \), a contradiction.

If \( (p, m, p_1) = (3, 2, 5) \), \( |F(R)| = 5 \) and so by [9], \( |N^\Delta(R)^{(R)}| = 20 \) and \( N^\Delta(R)^{(R)} = Z_4 \). Since \( N^\Delta(R) N^\Delta(R^\Delta) = 4 \), \( N^\Delta(R)^{(R)} = Z_4 \), contrary to \( N^\Delta(R) / (N^\Delta(R))^\Delta = Z_2 \times Z_2 \), a contradiction.

If \( (p, m, p_1) = (3, 3, 13) \), \( |F(R)| = 6 \). By [9], \( N^\Delta(R)^{(R)} \) is not solvable, a contradiction.

(4.5) \( p^m \neq 5 \).

Proof. Assume that \( p^m = 5 \). Then \( n = 2k \) with \( k \) odd and \( N^\Delta = PGL(2, 5) = S_5 \). First we argue that \( N^\Delta = N^\Delta \cap N^\beta \). Suppose false. Then \( C_\sigma(N^\beta) = 1 \) by Lemma 2.2, and \( N^\Delta \setminus N^\Delta \cap N^\beta = Z_2 \) by (4.1). Since \( N^\Delta N^\beta \cap N^\beta \cap N^\beta = Z_2 \) and the outer automorphism group of \( S_5 \) is trivial, we have \( Z(N^\Delta N^\beta) = Z_2 \). Let \( w \) be the involution of \( Z(N^\Delta N^\beta) \) and let \( \omega = I(N^\beta) - I(N^\beta) \). Since \( C_\sigma(N^\omega) \geq N^\beta \), by Lemma 2.6 (viii) and (ix), \( w \) acts on \( N^\alpha \) as a field automorphism of order 2 and \( C_\sigma(w) = PGL(2, 5) \). By Lemma 2.8 \( |F(w)| = 1 + q(\omega - \omega) |I(N^\alpha)| / |N^\alpha| = 1 + 5(5^2 - 1)/24 \). Let \( P \) be a Sylow 5-subgroup of \( C_\sigma(w) \). Then \( |P| = 5^k \) and \( |\sigma^\omega| = 5^k - 1 \) or \( 5^k \) for each \( \sigma \in \Omega - \{\alpha\} \). Since \( \sigma \) acts on \( F(w) \setminus \{\alpha\} \), we have \( 5^k - 1 \) or \( 5^k \) or \( 5^k - 1 \) or \( 5^k \) for each \( \sigma \in \Omega - \{\alpha\} \). Hence \( C_\sigma(w) F(w) = S_5 \) and so \( C_\sigma(w) F(w) = S_6 \). But clearly \( w \in N^\alpha \cap N^\beta \) by Lemma 2.1, a contradiction. Thus \( N^\Delta = N^\alpha \cap N^\beta \).

Let \( V \) be a cyclic subgroup of \( N^\Delta \) of order 4. Since \( N^\Delta = N^\alpha \cap N^\beta = S_5 \), \( N^\Delta(V)^{(V)} \) is doubly transitive and by Lemma 2.8, \( |F(V)| = 1 + |N_N^\Delta(V)|/|N^\Delta(N^\Delta(V))| = 3r^2 + 1 \). By Lemma 2.9, \( C_\sigma(N^\alpha) = 1 \) and (a) \( N^\Delta(V)^{(V)} \leq A_5 \Gamma L(1, 2^r) \) or (b) \( N^\Delta(V)^{(V)} = R(3) \).

Put \( P = N^\Delta(V) \). Then \( P = D_5, |F(P)| = 1 + |N_N^\Delta(P)|/|N_N^\Delta(P)| = 3r^2 + 1 \) and \( P^F \varphi Z_2 \). If (b) occurs, \( k = 1 \) and \( r = 9 \), hence \( |F(P)| = 10 \), a contradiction. Therefore (a) holds.

By Lemma 2.5, \( (r + 1)^2 = 3s + 1 \) and so \( r = 3s - 2 \). Hence \( k = r = 1 \) and \( G_{\alpha} | N^\alpha \leq Z_2 \times Z_2 \). Let \( z \) be an involution in \( N^\beta \). Then \( |F(z)| = 1 + 24 \cdot 25/120 = 6 \).
by Lemma 2.8 and \(|\Omega|=1+|N^\alpha| N^\alpha_{\beta}|=66 \text{ as } r=1. \) By the similar argument as in the proof of (3.12), 
\(|F(z)|(|F(z)| -1)/2+(|\Omega|-|F(z)|)/2=|C_G(z)| |z^G \cap \langle t \rangle G_{\alpha \beta}|/|\langle t \rangle G_{\alpha \beta}|, \) where \(t \) is an involution such that \(\alpha^t=\beta. \) Hence \(|z^G \cap \langle t \rangle G_{\alpha \beta}|=15|G_{\alpha \beta}|/|C_G(z)|. \) Set \(H=\langle t \rangle G_{\alpha \beta} \) and let \(R \) be a Sylow 3-subgroup of \(N^\alpha_{\beta}. \) By Lemma 2.8, 
\(|F(R)|=1+24\cdot10/120=3. \) Set \(F(R)=\{\alpha, \beta, \gamma\}. \) On the other hand, as \(N^\alpha_{\beta}=S_5 \) and Out(\(S_5\))=1, we have \(H=Z(H)N^\alpha_{\beta} \) and \(|Z(H)|=2, 4 \text{ or } 8. \) In the latter case \(G_{\alpha \beta}=Z(G_{\alpha \beta})N^\alpha_{\beta} \) and \(Z(G_{\alpha \beta})=Z_2 \times Z_2, \) contrary to Lemma 2.6 (ix). In the former case, we have \(|Z(H)|=2. \) For otherwise \(Z(H)<G \) and \(Z(H) \) normal in \(G \) and so letting \(u \in Z(H) \) \(Z(H) \) we have \(|R|=3 \) \(|F(u)|=1=5, \) a contradiction. Therefore \(Z(H)=Z_2 \) and so \(|G_{\alpha \beta}|<25+25=50, \) while \(|G_{\alpha \beta}|=15|G_{\alpha \beta}|/|C_G(z)|=15\cdot120/24=75, \) a contradiction.

5. Case (III)

In this section we assume that \(N^\alpha_{\beta}=PSL(2, p^m), \) where \(n=mk \) and \(k \) is odd. Set \(p^m \equiv \varepsilon \equiv 1 (\text{mod } 4). \) Then \(q|\varepsilon \equiv 1 (\text{mod } 4) \) as \(k \) is odd. In section 6 we shall consider the case that \(N^\alpha_{\beta}=A_4, \) so we assume \((p, m) \neq (3, 1) \) in this section. From this \(N^\alpha_{\beta} \) is a nonabelian simple group and so \(N^\alpha_{\beta}=N^\alpha \cap N^\beta \) or \(N^\alpha_{\beta}=N^\alpha \cap N^\beta \). If \(N^\alpha \cap N^\beta=1, \) then \(C_G(N^\alpha)=1 \) by Lemma 2.2 and \(N^\alpha_{\beta}=N^\alpha \cap N^\beta \). In the latter case \(G_{\alpha \beta}=Z(G_{\alpha \beta})N^\alpha_{\beta} \) and so \(|G_{\alpha \beta}|<25+25=50, \) while \(|G_{\alpha \beta}|=15|G_{\alpha \beta}|/|C_G(z)|=15\cdot120/24=75, \) a contradiction.

Let \(z \) be an involution of \(N^\alpha_{\beta}. \) Suppose \(z^G \in G_{\alpha \beta} \) for some \(g \in G \) and set \(\gamma:=\alpha^z, \delta:=\beta^z. \) Then \(z^G \in N^\alpha \cap G_{\alpha \beta} \leq N^\alpha_{\alpha \beta} \leq N^\alpha \cap N^\beta \) and so \(z^G \in N^\beta. \) Hence \(C_G(z)^{F(t)} \) is doubly transitive and by Lemma 2.8 (i), \(|F(z)|=(q-\varepsilon)r/(p^m-\varepsilon)+1. \) In particular \(|F(z)|>3r+1 \) as \((p^m-\varepsilon)/(p^m-\varepsilon) \geq p^{\varepsilon+\varepsilon}+1 \geq 3. \)

By Lemma 2.9, \(C_G(N^\alpha)=1 \) and one of the following holds.

(a) \(C_G(z)^{F(t)}=ATL(1, 2^t). \)

(b) \(C_G(z)^{F(t)} \supseteq PSL(2, p_1) (p_1 \geq 5), r=1 \text{ and } |C_N(z)\cap C_{N^\beta}(z)|=1. \)

(c) \(C_G(z)^{F(t)}=R(3). \)

Let \(Y \) be a cyclic subgroup of \(C_{N^\beta}(z)=D_{p^m-\varepsilon} \) of index 2. Since \(C_{G_{\alpha \beta}}(z) \supseteq Y, \) \(z \in Y \) and \(C_G(z)^{F(t)} \) is doubly transitive, we have \(F(Y)=F(z). \) By the similar argument as in (3.1), \(N^\alpha \cap N(C_{N^\beta}(z))=C_{N^\beta}(z) \) or \(N^\alpha \cap N(C_{N^\beta}(z))=A_4. \) Hence by Lemmas 2.3 and 2.4, \(|F(C_{N^\beta}(z))|=1+|C_{N^\beta}(z)|/|N^\alpha_{\beta}| \text{ or } 1+|A_4|/|N^\alpha_{\beta}| \text{ or } |A_4|/|N^\alpha_{\beta}|. \) Therefore \(|F(C_{N^\beta}(z))|=r \text{ or } 3r+1. \) From this \(C_{N^\beta}(z)^{F(t)}=Z_2. \)

In the case (a), \((r+1)^2=1+(p^m-\varepsilon)r/(p^m-\varepsilon) \) by Lemma 2.5 and hence \(r=(p^m-\varepsilon)/(p^m-\varepsilon)-2 \text{ or } mk. \) Since \((p^m-\varepsilon)/(p^m-\varepsilon) \geq ((p^m)^{k+1}+1)/(p^m+1)=\sum_{i=0}^{k-1}(-p^m)^i \) and \(k \geq 3, \) \(p \geq 3, \) we have \(p^{m-k+1}/(p^m-\varepsilon+1) \leq \text{mk, hence } ((p^m)^{k-1}/k)(p^m-\varepsilon)/(p^m-\varepsilon+1)<1. \) Thus \(k=3, m=1 \text{ and } p=3, \) contrary to \((p, m) \neq (3, 1). \)

In the case (b), \(r=1, p_1=(p^m-\varepsilon)/(p^m-\varepsilon), p_1(p_1-1)/2 \text{ and } s|4mpk_1, \) where \(s \) is the order of \(C_{G_{\alpha \beta}}(z)^{F(t)}. \) Hence \(p_1-1=\varepsilon \) and \(p_1-1=(p^m-\varepsilon)/(p^m-\varepsilon)-1 \)
Some Doubly Transitive Permutation Groups

\[ (p^n + 1)(p^n + 1) - 1 = \left( \sum_{k=0}^{\infty} (-p^m)^k \right) \geq p^{m(k-2)}(p^m - 1), \]
we have \( p^{m(k-2)/2k} \leq 4m/(p^m - 1) \leq 1 \) because \( p^m \neq 3 \). Hence \( k = 3 \) and \( p^m = 5 \), so that \( p_1 - 1 = 30/8 \), a contradiction.

In the case (c), \( r+1 = 4 \) and \( 1 + (p^n - \epsilon)r/(p^n - \epsilon) = 28 \) and so \( r = 3 \) and \( (p^n - \epsilon)/(p^n - \epsilon) = 9 \). Hence \( 9 \geq (p^m + 1)/(p^m + 1) \geq p^m - p^m + 1 \), so that \( p^m = 3 \), a contradiction.

6. Case (IV)

In this section we assume that \( N^e = A_4 \) and \( q = 3, 5 \) (mod 8). If \( N^e \cap N^a = 1 \), by Lemma 2.2, \( C_\alpha(N^e) = 1 \) and so \( N^e/N^a \cap N^a = N^e/N^a \cap N^a = \{ 1 \} \). Hence \( N^e/N^a \cap N^a = 1 \) or \( Z_3 \), so that \( z^6 \cap G_{ab} = z^2 \cap G_{ab} = z^3 \) for an involution \( z \in N^e \). Therefore \( C_\alpha(x)^F(z) \) is doubly transitive. By Lemma 2.9, \( C_\alpha(N^e) = 1 \) and one of the following holds.

(a) \( C_\alpha(z)^F(z) \leq A_T(1, 2) \) for some integer \( c \geq 1 \).
(b) \( C_\alpha(z)^F(z) \cong PSL(2, p_1) \) (\( p_1 \geq 5 \)), \( r = 1 \) and \( |C_\alpha(x) : C_\alpha^\alpha(z)| = p_1 \).
(c) \( C_\alpha(z)^F(z) = R(3) \).

Let \( T \) be a Sylow 2-subgroup of \( N^e \). Then \( z \in T \) and by Lemmas 2.3 and 2.4, \( |F(T)| = 1 + |N_\alpha(T)|/r \) and \( |N_\alpha^e| = r + 1 \). By Lemma 2.8 (i), \( |F(z)| = (q - \epsilon)r/4 + 1 \). Hence \( T^F(z) = Z_2 \) if \( p = 5 \). If \( p = 5 \), as \( PSL(2, 5) = PSL(2, 4) \), (ii) of our theorem holds by [4]. Therefore we may assume \( q = 5 \).

In the case (a), \( (r+1)^2 = 1 + (q - \epsilon)r/4 \) by Lemma 2.5. Hence \( r = (q - \epsilon - 8)/4 \) and \( r = 1 \). Let \( R \) be a Sylow 3-subgroup of \( G_{ab} \). Then \( R \cong Z_3 \) and \( R \leq N^a \) because \( G_{ab}/N^a = G_{ab}/N^a \cap N^a = 1 \) or \( Z_3 \) and \( N^a = A_4 \).

By Lemma 2.8 (ii), \( |F(R)| = 1 + 12/3 = 5 \) and \( N^e(R)^F(R) \) is doubly transitive. Since \( N_{\alpha}(R) = D_4 \) or \( D_4 \) and \( F(R) = 5 \), we have \( N^e(R) = 5 \). Let \( S \) be a Sylow 5-subgroup of \( N^e(R) \). Then \( [S, R] = 1 \) as \( N^e(R) \subset C^\alpha(R) \leq Z_2 \). Since \( 5 \not| [G_{ab}], |F(S)| = 0 \) or 1. If \( |F(S)| = 1 \), \( F(S) \subseteq F(R) \) and so \( 5 \not| |F(R)| = 4 \), a contradiction. Therefore \( S \) is semi-regular on \( \Omega \). But \( |\Omega| = 1 + |N^e : N^e| = 56 \) or \( 92 \). This is a contradiction.

In the case (b), \( p_1(p_1 - 1)/2 \) and \( s \geq 2n(q - \epsilon)/2 = 4np_1 \), where \( s \) is the order of \( C_\alpha(x)^F(z) \). Hence \( p_1 = 1 |8n \). Since \( p_1 = (q - \epsilon)/4 \), \( p_1 = \epsilon - 4 |32n \) and so we have \( q = 11, 13, 19, 27 \) or 37. If \( q = 27 \), by Lemma 2.6, \( C_\alpha(z) \cong D_{27} \) or \( D_{27} \) and so \( C_\alpha(z)^F(z) = Z_2 \). Hence \( (p_1 - 1)/2 = 2 \). From this \( q = 19 \). Let \( R \) be a Sylow 3-subgroup of \( G_{ab} \). By the similar argument as in the case (a), \( N^e(R)^F(R) \) is doubly transitive and \( |F(R)| = 1 + 18/3 = 7 \). Hence \( R \) \( |G| \). On the other hand \( |G| = |\Omega| \cdot |G_\alpha| = (1 + |N^e : N^e|) \cdot |G_\alpha| = (1 + 18 \cdot 19 \cdot 20/2 \cdot 12) \cdot 2^4 \cdot 18 \cdot 19 \cdot 20/2 = 2^2 \cdot 3^4 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \) with \( 0 \leq i \leq 1 \), a contradiction. If \( q = 27 \), then \( |C_\alpha(z)| = |F(z)| \cdot |C_\alpha(z)| = 2 \cdot |G_\alpha| = 12 \cdot |G_\alpha| \). While \( |\Omega| = 1 + |N^e : N^e| = 1 + 26 \cdot 27 \cdot 28/2 \cdot 12 = 820 \), \( 2^2 \cdot 5 \cdot 41 \) and so \( |G_\alpha| = 4 |G_\alpha| \). Therefore \( |C_\alpha(z)| \not| \, |G| \), a contradiction.

In the case (c), \( r+1 = 4 \) and \( 1 + (q - \epsilon)r/4 = 28 \). Hence \( r = 3 \) and \( q = 37 \),
contrary to \( r \mid n \).

7. Case (V)

In this section we assume that \( N^*_\beta = S_4 \) and \( q \equiv 7, 9 \) (mod 16). We note that \( 4 \nmid n \).

First we argue that \( N^*_\beta = N^* \cap N^\beta \). Suppose \( N^*_\beta \neq N^* \cap N^\beta \). Then \( C(G)(N^*) = 1 \) by Lemma 2.2. Since \( N^*_\beta \cap N^\beta = N_\beta^\beta \cap N_\beta \), we have \( N^* \cap N^\beta = A_4 \) and \( N^*_\beta \cap N^\beta = Z_2 \), so that \( N^*_\beta \cap N^\beta = N_\beta^\beta \cap N^\beta = Z_2 \). Hence as \( \text{Out}(S_4) = 1 \), \( Z(N_\beta^\beta N^\beta) = Z_2 \). Set \( t = F(t) \in I(N^*_\beta) - I(N^\beta) \). Since \( C(N_\beta^\beta(t)) \geq N^*_\beta = S_4 \) and \( C(N^\beta(t)) \geq N^*_\beta N^\beta \), by Lemma 2.6, we have \( C(N^*(t)) = \text{PSL}(2, \sqrt{q}) \) and \( |F(t)| = 1 + (q - \varepsilon)r/8 \) by Lemma 2.8.

Let \( P \) be a Sylow \( p \)-subgroup of \( C(N^*(t)) \). Then \( |P| = \sqrt{q} \) if \( p \neq 3 \), and \( |P| = 1 + 3(q - \varepsilon)r/8 \) if \( p = 3 \). If \( p \neq 3 \), \( |P| = 1 + 3(q - \varepsilon)r/8 \) and so \( r \mid n \). If \( p = 3 \), \( |P| = 1 + 273r \). Since \( G \) is doubly transitive, by Lemma 2.9, \( C(G)(N^*) = 1 \) and one of the following holds.

(a) \( N_G(V)^{(N^*)} \leq A_1L(1, 2^\gamma) \).

(b) \( N_G(V)^{(N^*)} \geq \text{PSL}(2, p_1) \), \( p_1 = (q - \varepsilon)/6 \geq 5 \).

(c) \( N_G(V)^{(N^*)} = R(3) \).

In the case (a), \( (r + 1/2) = 1 + (q - \varepsilon)r/8 \) by Lemma 2.5 and \( r \mid n \). From this \( q = 23 \) or \( 25 \), and if \( p \neq 3 \), \( |P| = 1 + 3(q - \varepsilon)r/8 \) and \( r \mid n \). From this \( q = 23 \) or \( 25 \).

In the case (b), if \( (p_1 - 1/2) = 1 + 18n \) and \( s \geq 2n(q - \varepsilon)/4 = 4np_1 \), where \( s \) is the order of \( N_G(V)^{(N^*)} \). Hence \( p_1 = 18n \). From this \( p^* - \varepsilon = 64n \) and so \( q = 23, 41, 71 \) or 73. Since \( p_1 \) is a prime and \( p_1 = (q - \varepsilon)/8 \geq 5 \), \( q = 23, 41, 71, 73 \). Therefore \( q = 41 \) and \( |\Omega| = 1 + N^*: N^*_\beta = 1 + 40 \cdot 41 \cdot 42 \cdot 2 \cdot 24 = 2^2 \cdot 359 \), so that \( |G|_2 = 4 \).
Since $N^*_a = N^a \cap N^b$, $C_\gamma(z)^{F(\gamma)}$ is transitive by Lemma 2.1. On the other hand, $|F(z)| = 1 + 40 \cdot 9/24 = 16$ by Lemma 2.8 (i) and so $|C_\gamma(z)| = 16|C_\gamma(z)| = 16|G_{\gamma}|$, contrary to $|C_\gamma(z)| = |G|$.

In the case (c), $r + 1 = 4$ and $1 + (q - \varepsilon)r/8 = 28$. Hence $r = 3$ and $q = 71$ or 73, contrary to $r | n$.

8. Case (VI)

In this section we assume that $N^*_a = A_5$ and $q \equiv 3, 5$ (mod 8). In particular, $n$ is odd. If $N^*_a \neq N^a \cap N^b$, then $N^a \cap N^b = 1$, $C_\gamma(N^a) = 1$ and so $N^*_a = N^a \cap N^b \leq \text{Out}(N^b) = Z_2 \times Z_2$, a contradiction. Hence $N^*_a = N^a \cap N^b$. Let $z$ be an involution in $N^*_a$ and $T$ a Sylow 2-subgroup of $N_a$ containing $z$. Then, by Lemma 2.8, $|F(z)| = 1 + (q - \varepsilon) 15r/60 = 1 + (q - \varepsilon)r/4$ and by Lemmas 2.3 and 2.4 $|F(T)| = 1 + 12 \cdot 5r/60 = 1 + r$. Since $N^*_a = N^a \cap N^b$, $z^G \cap G_{\gamma} = z^G \cap N^a = z^N_a$ and so $C_\gamma(z)^{F(\gamma)}$ is doubly transitive. By Lemma 2.9, $C_\gamma(N^a) = 1$ and one of the following holds.

(a) $C_\gamma(z)^{F(\gamma)} \leq \text{AGL}(1, 2^5)$.

(b) $C_\gamma(z)^{F(\gamma)} \geq \text{PSL}(2, p_1)$, $p_1 = (q - \varepsilon)/4 \geq 5$.

(c) $C_\gamma(z)^{F(\gamma)} = R(3)$.

In the case (a), by Lemma 2.5, $(q - \varepsilon)/4 = 1$ or $(r + 1)/2 = 1 + (q - \varepsilon)r/4$. Hence $q = 5$ or $r = (q - \varepsilon - 8)/4 | n$. If $q = 5$, then $N^*_a = N^a$, a contradiction. Therefore $p^* - \varepsilon - 8 | 4n$ and so $n = 1$ and $q = 11$ or 13. If $q = 13$, we have $5 \nmid |G_a|$, a contradiction. Hence $q = 11$ and $|\Omega| = 1 + |N^a| = 1 + 10 \cdot 11 \cdot 12/2 \cdot 60 = 12$. By [9], $C_\gamma = M_{11}$, $|\Omega| = 12$ and so (iii) of our theorem holds.

In the case (b), we have $p_1 = (p_1 - 1)/2 | s$ and $s | 2m(q - \varepsilon)/2 = 4np_1$, where $s$ is the order of $C_\gamma(z)^{F(\gamma)}$. Hence $p_1 = 18m$ and so $p^* - \varepsilon - 4 | 32n$. From this $q = 19, 27$ or 37. Since $5 \nmid |G_a|$, $q = 27, 37$. Hence $q = 19$ and $|\Omega| = 1 + |N^a| = 1 + 18 \cdot 19 \cdot 20/2 \cdot 60 = 2.29$. Since $G_a = \text{PSL}(2, 19)$ or $\text{PGL}(2, 19)$, $|G| = |\Omega| \cdot |G_a| = 2.29 \cdot 2^i \cdot 18 \cdot 19 \cdot 20/2 = 2^i \cdot 3^2 \cdot 5 \cdot 19 \cdot 29 \cdot 29$ with $0 \leq i \leq 1$. Let $P$ be a Sylow 29-subgroup of $G$. Then $P$ is semi-regular on $\Omega$ and $3, 5, 19 \nmid |N_\gamma(P)|$ because $N_\gamma(P)/C_\gamma(P) \leq Z_4 \times Z_2$. Hence $|G| = N_\gamma(P) = 2^i \cdot 3^2 \cdot 5 \cdot 19$ with $0 \leq j \leq 4$, while $2^i \cdot 3^2 \cdot 5 \cdot 19 \equiv 1 \pmod{29}$ for any $j$ with $0 \leq j \leq 4$, contrary to a Sylow’s theorem.

If $C_\gamma(z)^{F(\gamma)} = R(3)$, $r + 1 = 4$ and $1 + (q - \varepsilon)r/4 = 28$ and hence $r = 3$, $q = 37$, contrary to $r | n$.

OSAKA KYO IKU UNIVERSITY

References

[3] C. Hering: Transitive linear groups and linear groups which contain irreducible


