SOME 5/2 TRANSITIVE PERMUTATION GROUPS

DONALD STEVEN PASSMAN
SOME 5/2 TRANSITIVE PERMUTATION GROUPS

D. S. PASSMAN

In this paper we classify those 5/2-transitive permutation groups \( \mathcal{G} \) such that \( \mathcal{G} \) is not a Zassenhaus group and such that the stabilizer of a point in \( \mathcal{G} \) is solvable. We show in fact that to within a possible finite number of exceptions \( \mathcal{G} \) is a 2-dimensional projective group.

If \( p \) is a prime we let \( \Gamma(p^n) \) denote the set of all functions of the form

\[
x \mapsto \frac{ax^\sigma + b}{cx^t + d}
\]

where \( a, b, c, d \in GF(p^n), ad - bc \neq 0 \) and \( \sigma \) is a field automorphism. These functions permute the set \( GF(p^n) \cup \{\infty\} \) and \( \Gamma(p^n) \) is triply transitive. Moreover \( \Gamma(p^n)_\infty = S(p^n) \), the group of semilinear transformations on \( GF(p^n) \). Let \( \bar{\Gamma}(p^n) \) denote the subgroup of \( \Gamma(p^n) \) consisting of those functions of the form

\[
x \mapsto \frac{ax + b}{cx + d}
\]

with \( ad - bc \) a nonzero square in \( GF(p^n) \). Thus \( \bar{\Gamma}(p^n) \cong PSL(2, p^n) \).

Let \( \mathcal{G} \) be a permutation group on \( GF(p^n) \cup \{\infty\} \) with \( \mathcal{G} > \Gamma(p^n) \). Since \( \bar{\Gamma}(p^n) \) is doubly transitive so is \( \mathcal{G} \). Now \( \Gamma(p^n) / \bar{\Gamma}(p^n) \) is abelian so \( \mathcal{G} \) is normal in \( \Gamma(p^n) \). Hence \( \mathcal{G} \triangleleft \Gamma(p^n) \). Since a nonidentity normal subgroup of a transitive group is half-transitive we see that \( \mathcal{G} \) is half-transitive on \( GF(p^n)^t \) and hence \( \mathcal{G} \) is 5/2-transitive. It is an easy matter to decide which group \( \mathcal{G} \) with \( \Gamma(p^n) \supseteq \mathcal{G} > \bar{\Gamma}(p^n) \) are Zassenhaus groups. If \( p = 2 \), there are none while if \( p > 2 \), we must have \([\mathcal{G} : \bar{\Gamma}(p^n)] = 2\). In this latter case, there is one possibility for \( n \) odd and two for \( n \) even. The main result here is:

**Theorem.** Let \( \mathcal{G} \) be a 5/2-transitive group which is not a Zassenhaus group. Suppose that the stabilizer of a point is solvable. Then modulo a possible finite number of exceptions we have, with suitable identification, \( \Gamma(p^n) \supseteq \mathcal{G} > \bar{\Gamma}(p^n) \) for some \( p^n \).

The question of the possible exceptions will be discussed briefly in \( \S \, 3 \). We use here the notation of [4]. Thus we have certain linear groups \( T(p^n) \) and \( T_6(p^n) \) and certain permutation groups \( S(p^n) \)
and \( S_3(p^n) \). These play a special role in the classification of solvable 3/2-transitive permutation groups.

1. Lemmas. The lemmas here are variants of known results, the first two from [1] and the second two from [9]. We use the following notation and assumptions:

- \( \mathcal{G} \) is a doubly transitive permutation group of degree \( 1 + m \).
- \( \mathcal{G} \) and \( 0 \) are two points.
- \( \mathcal{D} = \mathcal{G}_0, \quad \mathcal{H} = \mathcal{G}_m = \mathcal{D}_0 \)
- \( T \in \mathcal{G} \) is an involution with \( T = (0 \infty) \cdots \).

The above implies that \( T \) normalizes \( \mathcal{H} \) and \( \mathcal{H} = \mathcal{D} \cap \mathcal{D}' \).

In the following we use the usual character theory notation.

**Lemma 1.1.** Let \( \alpha \neq 1_\mathcal{D} \) be a linear character of \( \mathcal{D} \) with \( \alpha(H^T) = \alpha(H) \) for all \( H \in \mathcal{H} \). Then

(i) If \( D \in \mathcal{D} \) then \( \alpha^*(D) = \alpha(D)1_\mathcal{D}(D) \).

(ii) \( \alpha^* = \chi_1 + \chi_2 \) where \( \chi_1 \) and \( \chi_2 \) are distinct irreducible non-principal characters of \( \mathcal{G} \).

**Proof.** We show first that if \( A, B \in \mathcal{D} \) with \( A = B^D \) then \( \alpha(A) = \alpha(B) \). This is clear if \( G \in \mathcal{D} \) so we assume that \( G \in \mathcal{D} \). From \( \mathcal{G} = \mathcal{D} \cup \mathcal{D}T\mathcal{D} \) we have \( G = DTE \) with \( D, E \in \mathcal{D} \). Then

\[
A^D = B^D \in \mathcal{D} \cap \mathcal{D}' = \mathcal{H}
\]

so by assumption \( \alpha(B^D) = \alpha(B^D) \). Thus \( \alpha(A) = \alpha(A^D) = \alpha(A^D) = \alpha(B^D) = \alpha(B) \) and this fact follows.

Let \( D \in \mathcal{D} \). Then by definition and the above we have

\[
\alpha^*(D) = |\mathcal{D}||^{-1} \sum_{g \in \mathcal{G}} \alpha_0(D^g) = \alpha(D) |\mathcal{D}||^{-1} \sum_{g \in \mathcal{G}} 1_\mathcal{D}(D^g) = \alpha(D)1_\mathcal{D}(D)
\]

and (i) follows.

We now compute the norm \(|\alpha^*, \alpha^*|_\mathcal{G} \) using Frobenius reciprocity and the fact that \( \alpha \) is linear so \( \alpha \alpha = 1_\mathcal{D} \). We have

\[
[\alpha^*, \alpha^*]_\mathcal{G} = [\alpha, \alpha^* | \mathcal{D}]_\mathcal{D} = [\alpha, \alpha(1_\mathcal{D}) | \mathcal{D}]_\mathcal{D} = [\alpha, 1_\mathcal{D} | \mathcal{D}]_\mathcal{D} = [1_\mathcal{D}, 1_\mathcal{D}]_\mathcal{D} = 2.
\]

Thus we must have \( \alpha^* = \chi_1 + \chi_2 \) with \( \chi_1 \) and \( \chi_2 \) distinct irreducible characters of \( \mathcal{G} \). Now \( [\alpha^*, 1_\mathcal{G}]_\mathcal{G} = [\alpha, 1_\mathcal{G}]_\mathcal{D} = [\alpha, 1_\mathcal{D}]_\mathcal{D} = 0 \) and hence both \( \chi_1 \) and \( \chi_2 \) are nonprincipal. This proves (ii).
LEMMA 1.2. Let $\mathcal{X} \triangleleft \mathcal{D}$ with $\mathcal{D}/\mathcal{X}$ cyclic. Suppose that $\mathcal{X}$ contains all elements $D \in \mathcal{D}$ satisfying either $D^2 = 1$ or $D^r = D^{-1}$. Suppose further that $m$ is a prime power and $T$ fixes precisely zero or two points. Then there exists $\mathcal{K} \triangleleft \mathcal{G}$ with $\mathcal{K} \cap \mathcal{D} = \mathcal{X}$.

Proof. The result is trivial if $\mathcal{X} = \mathcal{D}$ so we can assume that $\mathcal{X} \neq \mathcal{D}$. Let $\alpha$ be a faithful linear character of $\mathcal{D}/\mathcal{X}$ viewed as one of $\mathcal{K}$. Let $a$ be a faithful linear character of $\mathcal{K}$ and $b$ a character of $\mathcal{D}$ such that $ab \neq 1$. Then $\alpha = \chi_1 + \chi_2$ where $\chi_i$ is an irreducible nonprincipal character. We will prove that either $\chi_1$ or $\chi_2$ is linear. Suppose say $\chi_1$ is linear. Then $1 = [\alpha^*, \chi_1]_0 = [\alpha, \chi_1 | \mathcal{D}]_0$ implies that $\chi_1 | \mathcal{D} = \alpha$. If $\mathcal{K}$ is the kernel of $\chi_1$, then $\mathcal{K} \triangleleft \mathcal{G}$ and $\mathcal{K} \cap \mathcal{D} = \mathcal{X}$, the kernel of $\alpha$. If either $\chi_1$ or $\chi_2$ is $\xi$ then since $\deg 1_\mathcal{D} = \deg \alpha^* = m + 1$ and $\deg \xi = m$ we would have some $\chi_i$ linear and the result would follow. Thus we can assume that $\chi_1, \xi, \chi_1$ and $\chi_2$ are all distinct.

Let $\beta = \alpha - 1_\mathcal{D}$. We show now that $\beta^*$ vanishes on all elements of the form $G = T_1 T_2$ with $T_1$ and $T_2$ conjugate to $T$. We can certainly assume that $G$ is conjugate to an element of $\mathcal{D}$ and hence that $G \in \mathcal{D}$. If $G \in \mathcal{X}$ then by Lemma 2.1 (i), $\alpha^*(G) = \alpha(G)1_\mathcal{D}(G) = 1_\mathcal{D}(G)$ and $\beta^*(G) = 0$. Thus it suffices to show that $G \in \mathcal{X}$. Suppose first that $T_2 \in \mathcal{D}$. Then also $T_1 \in \mathcal{D}$ and since $T_1$ and $T_2$ are involutions, we have by assumption $T_1, T_2 \in \mathcal{X}$ so $G = T_1 T_2 \in \mathcal{X}$. Now we suppose that $T_2 \not\in \mathcal{D}$. From $\mathcal{G} = \mathcal{D} \cup \mathcal{D} T \mathcal{D}$ we see that a suitable $\mathcal{D}$ conjugate of $T_2$ is of the form $T D$ with $D \in \mathcal{D}$. By taking conjugates again we can assume that $G = W T D$ with $G, D \in \mathcal{D}$ and $W$ and $T D$ involutions. Since $(TD)^2 = 1$ we have $D^r = D^{-1}$. Also $E = WT \in \mathcal{D}$ and since $T$ and $W$ are involutions $E^r = E^{-1}$. Hence $E, D \in \mathcal{X}$ so $G = ED \in \mathcal{X}$ and this fact follows.

Let class function $\gamma$ of $\mathcal{G}$ be defined by $\gamma(G)$ is the number of ordered pairs $(T_1, T_2)$ with $T_1$ and $T_2$ conjugate to $T$ and $T_1 T_2 = G$. As is well known, $\gamma(G) = |\mathcal{G}|^{-1} |T^\mathcal{G}| \sum T^\mathcal{G}(T)^2 \chi(G)/\chi(1)$ where the sum runs over all irreducible characters of $\mathcal{G}$. By the remarks of the preceding paragraph $[\beta^*, \gamma]_0 = 0$. Hence since $1_\mathcal{G}, \chi_1, \chi_2$ and $\xi$ are distinct and $\beta^* = \chi_1 + \chi_2 - 1_\mathcal{G} - \xi$ we have

$$\frac{\chi_2(T)^2}{\chi_2(1)} + \frac{\chi_3(T)^2}{\chi_3(1)} = \frac{1_\mathcal{G}(T)^2}{1_\mathcal{G}(1)} + \frac{\xi(T)^2}{\xi(1)}.$$

Note since $T$ is an involution $\chi(T)$ is a rational integer for all such $\chi$. Now $\xi(1) = m$ and $1_\mathcal{D}(T) = r$, the number of fixed points of $T$. Since by assumption $r = 0$ or $2$, $\xi(T)^2 = (r - 1)^2 = 1$. Hence

$$\chi_1(1)\chi_1(T)^2 + \chi_2(1)\chi_2(T)^2 = \chi_1(1)\chi_2(1)(m + 1)/m.$$
Since \( m \) and \( m + 1 \) are relatively prime and the above left hand side is a rational integer, we conclude that \( m | \chi_1(1)\chi_2(1) \).

Now \( m = p^n \) is a prime power. Since \( \chi_1(1) + \chi_2(1) = m + 1 \) we see that \( p \) cannot divide both \( \chi_1(1) \) and \( \chi_2(1) \) so say \( p | \chi_1(1) \). Then \( m | \chi_1(1)\chi_2(1) \) implies that \( m | \chi_2(1) \) so \( \chi_2(1) \leq m \). From \( \chi_1(1) + \chi_2(1) = m + 1 \) we conclude that \( \chi_1(1) = m \) and \( \chi_2(1) = 1 \). Since \( \chi_1 \) is linear the result follows.

The proof of the next lemma is due to G. Glauberman.

**Lemma 1.3.** If \( T \) fixes two points the \( |\mathcal{S}| \geq (m - 1)/2 \). If in addition \( \mathcal{S} \) contains an involution fixing more than two points, then \( |\mathcal{S}| > (m - 1)/2 \).

**Proof.** Let \( \theta = 1^\mathcal{S}_{\mathcal{S}} \) be the permutation character. Then ([3] Th. 3.2) \( \Sigma_{\theta \in \mathcal{S}}\theta(G) = |\mathcal{S}| \) and \( \Sigma_{\theta \in \mathcal{S}}\theta(G^2) = 2 |\mathcal{S}| \). Hence

\[
|\mathcal{S}| = \Sigma_{\theta \in \mathcal{S}}[\theta(G^2) - \theta(G)].
\]

Note that for all \( G \in \mathcal{S} \), \( \theta(G^2) - \theta(G) \geq 0 \) and if \( G \) is conjugate to \( T \) then \( \theta(G^2) - \theta(G) = (m + 1) - 2 = m - 1 \). By considering only conjugates of \( T \) in the above we obtain

\[
|\mathcal{S}| \geq [\mathcal{S} : C_{\mathcal{S}}(T)](m - 1).
\]

Note here that if \( \mathcal{S} \) has an involution \( H \) fixing more than two points, then \( H \) is not conjugate to \( T \) and \( \theta(H^2) - \theta(H) > 0 \). Thus the above inequality is strict.

We have \( |C_{\mathcal{S}}(T)| \geq (m - 1) \) and \( C_{\mathcal{S}}(T) \) permutes the set of points \( \{x, y\} \) fixed by \( T \). Hence since \( [C_{\mathcal{S}}(T) : \mathcal{S}_{xy} \cap C_{\mathcal{S}}(T)] \leq 2 \) we have \( |\mathcal{S}_{xy}| \geq (m - 1)/2 \) with strict inequality if involution \( H \) exists. Since \( \mathcal{S} \) and \( \mathcal{S}_{xy} \) are conjugate, the result follows.

**Lemma 1.4.** Suppose \( \mathcal{D} = \mathcal{S} \mathcal{B} \) where \( \mathcal{B} \) is a regular normal abelian subgroup of \( \mathcal{D} \). We identify the set of points being permuted with \( \mathcal{B} \cup \{\infty\} \) and use additive notation in \( \mathcal{B} \). Then every element of \( \mathcal{D} \) can be written as \( D = \begin{pmatrix} x \\ f(x) \end{pmatrix} \) with \( \begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathcal{S} \) and \( b \in \mathcal{B} \).

Let \( T = \begin{pmatrix} x \\ f(x) \end{pmatrix} \) and assume that \( T \) commutes with the permutation \( \begin{pmatrix} x \\ -x \end{pmatrix} \). Then we have

(i) \( \mathcal{S} = \mathcal{D} \cup \mathcal{D}T\mathcal{B} = \mathcal{D} \cup \mathcal{B}T\mathcal{D} \).

(ii) For each \( a \in \mathcal{B} \), there exists a unique \( \begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathcal{S} \) with

\[
f(f(x) + a) = f(a(x) - a) + f(a).
\]

(iii) Let \( \alpha \) be a subgroup of \( \mathcal{S} \) normalized by \( T \) and containing
all the \( \left( \begin{array}{c} x \\ \alpha(x) \end{array} \right) \) elements which occur above. Then \( \mathfrak{S} = \langle \mathfrak{S}, \mathfrak{B}, T \rangle \) is doubly transitive with \( \mathfrak{S}_\infty = \mathfrak{S} \).

(iv) If \( \left( \begin{array}{c} x \\ -x \end{array} \right) \in \mathfrak{S} \) then \( T \) acts on the orbits of \( \mathfrak{S} \) on \( \mathfrak{B} \).

**Proof.** Now \( \mathfrak{S} = \mathfrak{S} \cup \mathfrak{S} T \mathfrak{B} \) and \( \mathfrak{D} = \mathfrak{S} \mathfrak{B} = \mathfrak{B} \mathfrak{S} \). Since \( T \) normalizes \( \mathfrak{S} \) we have \( T \mathfrak{S} \mathfrak{B} = \mathfrak{S} T \mathfrak{B} \) and \( \mathfrak{D} T = \mathfrak{B} \mathfrak{S} T = \mathfrak{B} \mathfrak{T} \mathfrak{B} \) so (i) clearly follows.

Let \( V \in \mathfrak{B}^* \) be the permutation \( V = \left( \begin{array}{c} x \\ x + a \end{array} \right) \). Then \( TVT \in \mathfrak{S} \) and \( (\infty)TVT = (a)T \neq \infty \). Thus \( TVT \in \mathfrak{D} T \mathfrak{B} \) and hence

\[
\left( \begin{array}{c} x \\ f(x) \end{array} \right) \left( \begin{array}{c} x \\ x + a \end{array} \right) \left( \begin{array}{c} x \\ f(x) \end{array} \right) = \left( \begin{array}{c} x \\ \alpha(x) + b \end{array} \right) \left( \begin{array}{c} x \\ x + c \end{array} \right).
\]

This is equivalent to

\[ f(f(x) + a) = f(\alpha(x) + b) + c. \]

Note that \( \left( \begin{array}{c} x \\ \alpha(x) \end{array} \right) \in \mathfrak{S} \) and \( b, c \in \mathfrak{B} \). With \( x = \infty \) in the above we obtain \( c = f(a) \). Then \( x = 0 \) yields \( f(b) = -f(a) \) and since \( f^2 = 1 \), \( b = f(-f(a)) \). Now by assumption \( T \) commutes with \( \left( \begin{array}{c} x \\ -x \end{array} \right) \) so \( f(-x) = -f(x) \) and \( b = -f^2(a) = -a \). Since \( \left( \begin{array}{c} x \\ \alpha(x) \end{array} \right) \in \mathfrak{S} \) is now clearly unique, we have (ii).

By definition of \( \mathfrak{S} \) we have \( T \mathfrak{B} T = \mathfrak{S} \mathfrak{B} \mathfrak{T} \mathfrak{B} \) and since \( T \) normalizes \( \mathfrak{S}, \mathfrak{G} = \mathfrak{S} \mathfrak{B} \cup \mathfrak{S} \mathfrak{T} \mathfrak{B} \) is a group. Since \( \mathfrak{G} \supseteq \langle \mathfrak{B}, T \rangle, \mathfrak{G} \) is doubly transitive. This clearly yields (iii).

Finally set \( x = -f(a) \) in the formula of part (ii). Since \( f(x) = -a \) we obtain \( \alpha(-f(a)) = a \) or \( -\alpha(f(a)) = a \). Since \( \left( \begin{array}{c} x \\ \alpha(x) \end{array} \right) \in \mathfrak{S}, a \) and \( f(a) \) are in the same orbit of \( \mathfrak{S} \). This completes the proof of this result.

2. 5/2-transitive groups. In this section we consider the transitive extensions of the infinite families of solvable 3/2-transitive permutation groups. We use the following notation and assumptions:

\( \mathfrak{G} \) is a 5/2-transitive permutation group of degree \( 1 + m \)

\( \mathfrak{G} \) is not a Zassenhaus group

\( \infty \) and \( 0 \) are two points

\( \mathfrak{D} = \mathfrak{G}_\infty, \mathfrak{S} = \mathfrak{G}_\infty = \mathfrak{D}_\infty, \mathfrak{D} \) is solvable.

Thus \( \mathfrak{D} \) is a 3/2-transitive permutation group which is not a Frobenius group. By Theorem 10.4 of [8] \( \mathfrak{D} \) is primitive and hence \( \mathfrak{G} \) is doubly primitive. Since \( \mathfrak{D} \) is solvable it has a regular normal elementary abelian \( p \)-group \( \mathfrak{B} \). Thus \( \mathfrak{D} = \mathfrak{B} \mathfrak{G} \) and \( m \) is a power of \( p \).
**Lemma 2.1.** Let $\mathfrak{S} \triangleleft \mathfrak{G}$ with $\mathfrak{S} \neq \langle 1 \rangle$. Then $\mathfrak{S}$ is doubly transitive and has no regular normal subgroup.

**Proof.** We show first that $\mathfrak{G}$ has no regular normal subgroup. Suppose by way of contradiction that $\mathfrak{S}$ is such a group. Since $\mathfrak{G}$ is doubly transitive $\mathfrak{S}$ is an elementary abelian $q$-group for some prime $q$. Then $\mathfrak{S}/\mathfrak{S}$ is sharply 2-transitive so since $\mathfrak{S}$ is an elementary abelian $p$-group it follows that $\mathfrak{S}$ is cyclic of order $p$ and $p + 1 = |L|$. Now $\mathfrak{S}$ acts faithfully on $\mathfrak{S}/\mathfrak{S}$ and hence $\mathfrak{S}$ acts semiregularly on $\mathfrak{S}/\mathfrak{S}$. Thus $\mathfrak{S} = \mathfrak{S}/\mathfrak{S}$ is a Frobenius group, a contradiction.

Now let $\mathfrak{S} \triangleleft \mathfrak{G}$ with $\mathfrak{S} \neq \langle 1 \rangle$. Since $\mathfrak{S}$ cannot be regular and $\mathfrak{G}$ is doubly primitive, it follows that $\mathfrak{S}$ is doubly transitive. If $\mathfrak{S}$ is a regular normal subgroup of $\mathfrak{G}$, then $\mathfrak{S}$ is abelian. This implies easily that $\mathfrak{S}$ is the unique minimal normal subgroup of $\mathfrak{G}$ so $\mathfrak{S} \triangleleft \mathfrak{G}$, a contradiction.

The following is a restatement of Proposition 3.3 of [5].

**Lemma 2.2.** Let $\mathfrak{S} \subseteq T(p^n)$ and suppose $\mathfrak{S}$ acts 1/2-transitively but not semiregularly on $GF(p^n)$. Set $\hat{\mathfrak{S}} = \{H \in \mathfrak{S} | H = ax\}$ so that $\hat{\mathfrak{S}}$ is isomorphic to a multiplicative subgroup of $GF(p^n)$. If $|\hat{\mathfrak{S}}| = k$, then:

(i) Each $\hat{\mathfrak{S}}$ is cyclic of order $k$ and $k | n$.

(ii) $\hat{\mathfrak{S}} \supseteq \{ax | a = b^{i \cdot \sigma}, b \in GF(p^n)\}$ where $\sigma$ is a field automorphism of order $k$.

(iii) $C_\mathfrak{S}(\hat{\mathfrak{S}}) = \hat{\mathfrak{S}}$ except for $p^n = 3^2$, $|\hat{\mathfrak{S}}| = 8$.

(iv) $\hat{\mathfrak{S}}$ is characteristic and self centralizing in $\mathfrak{S}$.

**Lemma 2.3.** Let $p > 2$ and consider $T(p^n)$ as a subgroup of $\text{Sym}(GF(p^n))$. Then $T(p^n) \not\subseteq \text{Alt}(GF(p^n))$. Moreover we have the following:

(i) If $a$ generates the multiplicative group $GF(p^n)^*$, then $(\frac{x}{ax}) \in \text{Alt}(GF(p^n))$.

(ii) If $n$ is even and $\sigma$ is a field automorphism of order $n$, then $(\frac{x}{x^\sigma}) \in \text{Alt}(GF(p^n))$ if and only if $p \equiv 1$ modulo 4.

(iii) If $n$ is even, then $(\frac{x}{-x}) \in \text{Alt}(GF(p^n))$.

**Proof.** The group generated by $(\frac{x}{ax})$ acts regularly on $GF(p^n)^*$ and hence $(\frac{x}{ax})$ is a $(p^n - 1)$-cycle. Since $p > 2$, $p^n - 1$ is even and hence $(\frac{x}{ax})$ is an odd permutation. This also yields the contention that $T(p^n) \not\subseteq \text{Alt}(GF(p^n))$. 
(ii) Let $q$ be an integer and suppose that for some $r \geq 1$, $q^{2r-1} \equiv \pm 1 \mod 2^{r+1}$. Then $q^{2r-1} = 1 + \lambda 2^{r+1}$.

$$q^{2r} = (q^{2r-1})^2 = (1 + \lambda 2^{r+1})^2 = 1 + \lambda 2^{r+2} + \lambda 2^{2r+2}.$$ 

Since $r \geq 1$, $2r + 2 \geq r + 2$ and hence $q^{2r} \equiv 1 \mod 2^{r+2}$. Now if $q$ is an odd integer, then $q \equiv \pm 1 \mod 4$, and thus by the above and induction we obtain for $r > 1$, $q^{2r-1} \equiv 1 \mod 2^{r+1}$.

Let $n = 2^r s$ with $s$ odd. We can write $\sigma = \tau \rho$ where $\tau$ has order $2^r$ and $\rho$ has order $s$. Clearly $\left(\frac{x}{x^s}\right) \in \text{Alt}(GF(p^n))$ if and only if $\left(\frac{x}{x^s}\right) \in \text{Alt}(GF(p^n))$. It is easy to see that if $q = p^s$, then $\left(\frac{x}{x^s}\right)$ has $(q^{2s} - q^{s-1})/2^i$ cycles of length $2^i$ for $i = 1, 2, \cdots, r$. These cycles are all odd permutations so $\left(\frac{x}{x^s}\right)$ has the parity of $\sum (q^{2i} - q^{s-1})/2^i$. Now $q$ is odd and

$$(q^{2i} - q^{s-1})/2^i = q^{2i-1}(q^{s-1} - 1)/2^i.$$ 

By the above, if $i > 1$ then $2^{i+1} | (q^{s-1} - 1)$ and hence $\left(\frac{x}{x^{s'}}\right)$ has the parity of $q(q - 1)/2$. If $q \equiv 1 \mod 4$ then this is even and if $q \equiv -1 \mod 4$ then this term is odd. Finally since $s$ is odd and $q = p^s$ we see that $q = p \mod 4$ and (ii) follows.

(iii) $\left(\frac{x}{x^s}\right)$ is a product of $(p^n - 1)/2$ transpositions. If $n$ is even, then $4 | (p^n - 1)$ and the result follows.

We will consider these transitive extensions in four separate cases.

**Proposition 2.4.** If $\mathcal{D} = S_\xi(p^n)$, then $p^n = 3$ and $\Gamma(3^s) < \mathcal{D} < \Gamma(3^s)$.

**Proof.** Since $\mathcal{D}$ is $3/2$-transitive we have $p \neq 2$. Let $G$ be the central involution of $\mathcal{D} = T_\psi(p^n)$ and let $H$ be another involution. Then $G$ fixes precisely two points and $H$ fixes $p^n + 1 > 2$ points. Since the degree of $\mathcal{D}$ is $1 + p^n$, Lemma 1.3 yields

$$4(p^n - 1) = |T_\psi(p^n)| = |\mathcal{D}| \geq (p^n - 1)/2$$

or $7 > p^n$. Thus $p^n = 3$ or $5$.

Since $\mathcal{D}$ is doubly transitive we can find $T$ conjugate to $G$ with $T = (0 \infty) \cdots$. Then $T$ normalizes $\mathcal{D}$ and centralizes its unique central involution $G = \left(\frac{x}{x^s}\right)$. By Lemma 1.4 (iv), $T$ acts on each orbit of $\mathcal{D}$ on $\mathbb{B}_s$. Now if $v \in \mathbb{B}_s$, then $|\mathcal{D}_v| = 2$. This implies easily that if $H$ is a noncentral involution of $\mathcal{D}$, then $H^r$ is conjugate to $H$ in $\mathcal{D}$. Let $p^n = 5$. Then $\mathcal{D}$ is easily seen to be generated by its noncentral involutions so $\mathcal{D}^r \subseteq \mathcal{D}$. Thus $|\mathcal{D} : C_\mathcal{D}(T)| = |\mathcal{D}^r : C_\mathcal{D}^r(T)| \leq |\mathcal{D}^r| = 2$ and $|C_\mathcal{D}(T)| \geq 8$. On the other hand $C_\mathcal{D}(T)$ acts on the fixed points
of $T$ namely $\{a, b\}$, so $[C_\mathfrak{S}(T) : C_\mathfrak{S}(T) \cap \mathfrak{S}_a] \leq 2$. Since $|\mathfrak{S}_a| = 2$, this is a contradiction.

Finally let $p^* = 3$. Here $T_3(3)$ is a dihedral group of order 8 and $S_3(3) \subseteq S(3^2)$. This case is then included in Proposition 2.7 and we obtain $\Gamma(3^2) \lhd \mathfrak{S} \subseteq \Gamma(3^2)$. By order considerations $\mathfrak{S} \neq \Gamma(3^2)$ so this results follows.

PROPOSITION 2.5. If $D \subseteq S(2^n)$ then $\bar{\Gamma}(2^n) \lhd \mathfrak{S} \subseteq \Gamma(2^n)$.

Proof. Let 1 be a point. Then $\mathfrak{S}_1$ has a regular normal elementary abelian 2-group. Let $T$ be an involution in this subgroup. Then $T$ fixes precisely one point. Say $T = (0 \infty)(1) \cdots$ and use the notation of §1. It is easy to see that we can assume that point 1 corresponds to the unit element of $GF(2^n)$.

Now $T$ normalizes $\mathfrak{S}$. If $H \in C_\mathfrak{S}(T)$, then $1H = (1T)H = (1H)T$ so $T$ fixes $1H$ and hence $H \subseteq \mathfrak{S}_1$. In particular in the notation of Lemma 2.2, $C_{\mathfrak{S}_1}(T) = \langle 1 \rangle$. Then $\mathfrak{S}_1^{-T} = \mathfrak{S}_1$. Since $\mathfrak{S}_1/\mathfrak{S}_1$ is abelian, $(\mathfrak{S}_1/\mathfrak{S}_1)^{-T}$ is a group and hence $\mathfrak{S}_1^{-T}$ is a group containing $\mathfrak{S}$.

If $H \in \mathfrak{S}_1^{-T}$, then $H^T = H^{-1}$ so $\mathfrak{S}_1^{-T}$ is abelian. By Lemma 2.2 (iv), $\mathfrak{S}_1^{-T} = \mathfrak{S}_1$. Now $|\mathfrak{S}_1^{-T}| = |C_{\mathfrak{S}_1}(T)| = |\mathfrak{S}_1|$, $|\mathfrak{S}_1| \leq |\mathfrak{S}|$ and $C_{\mathfrak{S}_1}(T) \subseteq \mathfrak{S}_1$. This yields $C_{\mathfrak{S}_1}(T) = \mathfrak{S}_1$ and $\mathfrak{S} = \mathfrak{S}_1 \mathfrak{S}_1$. The latter shows that each orbit of $\mathfrak{S}$ on $GF(2^n)$ has size $|\mathfrak{S}_1|$, an odd number.

In characteristic 2 the permutation $\left( \begin{array}{c} x \\ \bar{x} \end{array} \right)$ is trivial so by Lemma 1.4 (iv) $T$ acts on each orbit of $\mathfrak{S}$ on $GF(2^n)^4$. These orbits have odd size so $T$ fixes a point in each orbit. Thus there is only one such orbit and $\mathfrak{S}$ is transitive. This yields

$\mathfrak{S}_1^{-T} = \mathfrak{S}_1 = \{ bx \mid b \in GF(2^n)^4 \}$.

If $H = \left( \begin{array}{c} x \\ bx \end{array} \right)$, then $H^T = H^{-1}$ so

$\left( \begin{array}{c} x \\ f(x) \end{array} \right) \left( \begin{array}{c} x \\ b^{-1}x \end{array} \right) = \left( \begin{array}{c} x \\ bx \end{array} \right) \left( \begin{array}{c} x \\ f(x) \end{array} \right)$

and $b^{-1}f(x) = f(bx)$. At $x = 1$ this yields $f(b) = b^{-1}$ and hence we see that $f(x) = 1/x$ for all $x$.

Finally, since $\mathfrak{S} = D \cup DT \mathfrak{S}$, the result follows easily.

The following is an easy special case of a recent result of Bender ([1]).

PROPOSITION 2.6. If $D \subseteq S(p^n)$ with $p \neq 2$ and $|D|$ is odd, then $\bar{\Gamma}(p^n) \lhd \mathfrak{S} \subseteq \Gamma(p^n)$.

Proof. Since $\mathfrak{S}$ is doubly transitive it has even order. Let $T$ be an involution in $\mathfrak{S}$ with $T = (0 \infty) \cdots$. By assumption $T$ fixes
no points. We use the notation of Lemma 2.2. Then $T$ normalizes both $\mathcal{S}$ and $\tilde{\mathcal{S}}$. We show now that $T$ centralizes the quotient $\mathcal{S}/\mathcal{S}$. If not, then the quotient $\mathcal{S}/\mathcal{S}$ is abelian and has odd order, we can find a nonidentity subgroup $\mathfrak{V} \leq \mathcal{S}/\mathcal{S}$ on which $T$ acts in a dihedral manner. Then dihedral group $\langle \mathfrak{W}, T \rangle$ acts on $\mathcal{S}$. Since $\mathcal{S}$ is cyclic, $\text{Aut} \mathcal{S}$ is abelian and hence $\mathfrak{V} = \langle \mathfrak{W}, T \rangle'$ centralizes $\mathcal{S}$. This contradicts the fact that $\mathcal{S}$ is self centralizing in $\mathcal{S}$.

Set $\mathcal{I} = \tilde{\mathcal{S}} \triangle \mathfrak{I}$ so that $\mathcal{D}/\mathcal{I} \cong \mathcal{S}/\mathcal{S}$ is cyclic. Since $\mathcal{D}/\mathcal{I}$ has odd order, we see easily that the hypotheses of Lemma 1.2 are satisfied. Hence there exists $\mathcal{F} \triangle \mathcal{S}$ with $\mathcal{F} \cap \mathcal{D} = \mathcal{I}$. Now $\mathcal{D}$ is maximal in $\mathcal{S}$ and contains no nontrivial normal subgroup of $\mathcal{S}$. Hence $\mathcal{S} = \mathcal{F}\mathcal{D}$ and $\mathcal{S}/\mathcal{S} \cong \mathcal{D}/(\mathcal{F} \cap \mathcal{D})$ has odd order and $T \in \mathcal{F}$.

By Lemma 2.1, $\mathcal{F}$ is doubly transitive and has no regular normal subgroup. Furthermore $\mathcal{F}_0 = \mathcal{I} = \tilde{\mathcal{S}} \mathfrak{B}$ and $\mathfrak{B}$ is abelian. Thus $\mathcal{F}$ is a Zassenhaus group and the result of Feit ([2]) implies that $T$ is a permutation of the form $\left( \begin{array}{c} x \\ \frac{a}{x} \end{array} \right)$ and $|\mathcal{S}| = (p^n - 1)/2$. Since $\mathcal{S} = \mathcal{D} \cup DT\mathfrak{B}$, the result follows easily.

**Proposition 2.7.** If $\mathcal{D} \subseteq S(p^n)$ with $p \neq 2$ and $|\mathcal{D}|$ is even, then $\bar{f}(p^n) < \mathcal{S} \subseteq \Gamma(p^n)$.

**Proof.** We proceed in a series of steps.

Step 1. $\mathcal{F}$ has central element $\left( \begin{array}{c} x \\ -x \end{array} \right)$ of order 2. $\mathcal{F}$ is normalized by involution $T = \left( \begin{array}{c} x \\ f(x) \end{array} \right)$ with $T = (0 \infty)(1)(-1) \cdots$. The fixed points of $T$ are precisely 1 and $-1$ and $T$ centralizes $\left( \begin{array}{c} x \\ -x \end{array} \right)$ so Lemma 1.4 applies. In the notation of Lemma 2.2 we have one of the following two possibilities.

(i) $\tilde{\mathcal{S}} = \mathcal{S} \mathcal{T}^{-1}$ and $[\mathcal{S} : \mathcal{S}\mathcal{T}] = 2$ or

(ii) $[\mathcal{S} : \mathcal{S} \mathcal{T}^{-1}] = 2$ and $\mathcal{S} = \mathcal{S}\mathcal{T}$. In either case $[\mathcal{S} : \mathcal{S}] = 2 |\mathcal{S} \mathcal{T}^{-1}|$.

Now by assumption $2 | |\mathcal{D}|$ so since $p \neq 2$, $2 | |\mathcal{F}|$. If $2 | |\mathcal{S}|$, then certainly $\mathcal{S}$ has a central element of order 2. This is of course the permutation $\left( \begin{array}{c} x \\ -x \end{array} \right)$ which fixes precisely two points. Suppose $2 \nmid |\mathcal{S}|$ and let $H \in \mathcal{S}$ have order 2. Since $H \neq \left( \begin{array}{c} x \\ -x \end{array} \right)$, $H$ must have a fixed point on $\mathfrak{W}$. Hence $2 | |\mathcal{S}|$. If $\rho$ is a field automorphism of order 2, then by Lemma 2.2, $\mathcal{S} \supseteq \{ b^{1-x}x \mid b \in GF(p^n) \}$. Since this latter group has order $(p^n - 1)/(p^{n/2} - 1) = p^{n/2} + 1$ and this is even we have a contradiction.

Since $\mathcal{S}$ is doubly transitive we can choose $T$ conjugate to $\left( \begin{array}{c} x \\ -x \end{array} \right)$.
with $T = (0 \infty) \cdots$. Then $T$ fixes precisely two points and $T$ normalizes $\mathfrak{S}$. We can clearly write the latter group in such a way that $T$ fixes point 1. Clearly $T$ centralizes $\left(\begin{array}{c} x \\ -x \end{array}\right) \in \mathfrak{S}$ so if $T = \left(\begin{array}{c} x \\ f(x) \end{array}\right)$, then $f(-x) = -f(x)$. This shows that $T$ also fixes $-1$ so $T = (0 \infty)(1)(-1) \cdots$.

Let $H \in C_{\mathfrak{S}}(T)$. Then $1H = (1T)H = (1H)T$ so $1H = \pm 1$ and $H \in \left\langle \left(\begin{array}{c} x \\ -x \end{array}\right) \right\rangle \mathfrak{S}$. On the other hand since $\mathfrak{S}_1$ fixes 1 and $-1$ and $T$ is central in $\mathfrak{S}_{1,-1}$, we see that $C_{\mathfrak{S}_1}(T) \supseteq \left\langle \left(\begin{array}{c} x \\ -x \end{array}\right) \right\rangle \mathfrak{S}_1$, so $C_{\mathfrak{S}_1}(T) = \left\langle \left(\begin{array}{c} x \\ -x \end{array}\right) \right\rangle \mathfrak{S}_1$.

Now $T$ acts on $\tilde{\mathfrak{S}}$ and $C_{\tilde{\mathfrak{S}}}(T) = \left\langle \left(\begin{array}{c} x \\ -x \end{array}\right) \right\rangle$. Thus since $\tilde{\mathfrak{S}}$ is abelian, $\tilde{\mathfrak{S}}^\tau$ is a group and $[\tilde{\mathfrak{S}} : \tilde{\mathfrak{S}}^\tau] = 2$. Now $\tilde{\mathfrak{S}}^\tau \triangle \mathfrak{S}$ and $\tilde{\mathfrak{S}}/\tilde{\mathfrak{S}}^\tau$ is abelian since $\mathfrak{S}/\tilde{\mathfrak{S}}^\tau$ is central in this quotient and $\mathfrak{S}/\tilde{\mathfrak{S}}^\tau$ is cyclic. This implies that $\tilde{\mathfrak{S}}^\tau$ is a group so $\tilde{\mathfrak{S}}^\tau$ is abelian and centralizes $\mathfrak{S}^\tau \subseteq \tilde{\mathfrak{S}}^\tau$. By Lemma 2.2 (iii), $\tilde{\mathfrak{S}}^\tau \subseteq \tilde{\mathfrak{S}}$ with the possible exception of $p^n = 3^2$ and $\tilde{\mathfrak{S}}$ dihedral of order 8. However in the latter case $[\tilde{\mathfrak{S}} : \tilde{\mathfrak{S}}^\tau] = 2$ so clearly $\tilde{\mathfrak{S}}^\tau \subseteq \tilde{\mathfrak{S}}$.

We use the fact that $|\tilde{\mathfrak{S}}| = |\tilde{\mathfrak{S}}^\tau| = |C_{\tilde{\mathfrak{S}}}(T)|$ and $C_{\tilde{\mathfrak{S}}}(T) = \left\langle \left(\begin{array}{c} x \\ -x \end{array}\right) \right\rangle \mathfrak{S}_1$. Suppose first that $\tilde{\mathfrak{S}} = \tilde{\mathfrak{S}}^\tau$. Then $[\tilde{\mathfrak{S}} : \tilde{\mathfrak{S}}] = 2$ and we have (i). Now let $[\tilde{\mathfrak{S}} : \tilde{\mathfrak{S}}^\tau] = 2$. Then $[\tilde{\mathfrak{S}} : \tilde{\mathfrak{S}}] = 1$ and we have (ii). This completes the proof of this step.

Step 2. For each $a \in GF(p^n)^\ast$ we have

\[(\ast) \quad f(f(x) + a) = f(a'x^\tau - a) + f(a)\]

where $\left(\begin{array}{c} x \\ a'x^\tau \end{array}\right) \in \tilde{\mathfrak{S}}$ and $a' = -a/f(a)^\tau$. Let $g$ denote the set of all field automorphisms $\sigma$ which occur in the above. If $g = \{1\}$, then

$$\Gamma(p^n) < \mathfrak{S} \subseteq \Gamma(p^n).$$

Equation \((\ast)\) follows from Lemma 1.4 (ii). Set $x = -f(a) = f(-a)$ in \((\ast)\). Then $a'x^\tau - a = 0$ so $a' = -a/f(a)^\tau$. Suppose now that $g = \{1\}$. This implies by Lemma 1.4 (iii) that $\mathfrak{G} = \langle \tilde{\mathfrak{S}}, \mathfrak{S}, T \rangle$ is doubly transitive with $\mathfrak{G}_{m_3} = \tilde{\mathfrak{S}}$. Hence $\mathfrak{G}$ is a Zassenhaus group. Let $\mathfrak{L} = \{H \in \tilde{\mathfrak{S}} | H^r = H^{-1}\}$ so that $\mathfrak{L}$ is a subgroup of $\tilde{\mathfrak{S}}$ containing $\left(\begin{array}{c} x \\ -x \end{array}\right)$. With $\mathfrak{Z} = \mathfrak{G} \triangle \tilde{\mathfrak{S}}\mathfrak{B}$ we see easily that the hypotheses of Lemma 1.2 hold. Hence there exists $\mathfrak{K} \triangle \mathfrak{G}$ with $\mathfrak{K} \cap (\tilde{\mathfrak{S}}\mathfrak{B}) = \mathfrak{G}\mathfrak{B}$. Since $\mathfrak{G}$ is doubly transitive and $\mathfrak{K} \supseteq \mathfrak{B}$ we see that $\mathfrak{K} \subseteq \tilde{\mathfrak{S}}\mathfrak{B}$. Hence $\mathfrak{K}$ is doubly transitive and $\left(\begin{array}{c} x \\ -x \end{array}\right) \in \mathfrak{K}$. By Lemma 1.3, $|\mathfrak{L}| \geq (p^n - 1)/2$. 

166 D. S. PASSMAN
Let \( M = \left\{ b \in GF(p^n) \mid \left( \frac{x}{bx} \right) \in \mathcal{S} \right\} \). Thus \( M \) is a subgroup of \( GF(p^n)^* \) of index 1 or 2 and in particular \( M \) contains all the nonzero squares in \( GF(p^n) \). Note that for all \( b \in M \), \( f(bx) = b^{-1}f(x) \) and at \( x = 1 \) this yields \( f(b) = b^{-1} \).

Let \( a \in M \) in \((*)\) and let \( x = 1 \). Since \( g = \{1\} \), \( a' = -a^2 \) and we obtain

\[
f(1 + a) = f(-a^2 - a) + f(a)
= -a^{-1}f(1 + a) + a^{-1}.
\]

This yields \( f(1 + a) = (1 + a)^{-1} \). If \( b \in M \), then

\[
f(b(1 + a)) = b^{-1}f(1 + a) = b^{-1}(1 + a)^{-1}.
\]

Since \( M \) contains the squares in \( GF(p^n)^* \) and every element of the field is a sum of two squares, the above yields \( f(x) = 1/x \). Since \( \mathcal{S} = \mathcal{D} \cup \mathcal{D}T\mathcal{S} \) and \( |\mathcal{S}| \geq (p^n - 1)/2 \) the result follows here.

Step 3. Let \( \mathcal{R} = \left\{ b \in GF(p^n)^* \mid \left( \frac{x}{bx} \right) \in \mathcal{S}^{1-r} \right\} \). Let \( \sigma \in g - \{1\} \). Then \( \sigma^2 = 1 \) so \( n \) is even. Set \( \mathcal{S} = \{ b \in GF(p^n)^* \mid b^{-1} \in \mathcal{R} \} \). If \( b \in \mathcal{R} \) and \( b + 1 \in \mathcal{S} \), then \( b' = b \). Furthermore, if \( r = |GF(p^n)^* : \mathcal{R}| \) and \( s = |GF(p^n)^* : \mathcal{S}| \) then we have

\[
(i) \quad r = 2, 4 \text{ or } 6.
\]

\[
(ii) \quad s = r/(\text{g.c.d.} \{r, \frac{p^n}{2} - 1\}) \leq r/2.
\]

Define \( \mathcal{I} \triangle \mathcal{D} \) as follows. If \( \mathcal{S}/\mathcal{S} \) has odd order, set \( \mathcal{I} = \tilde{\mathcal{S}}\mathcal{B} \). If \( \mathcal{S}/\mathcal{S} \) has even order and \( \mathcal{S}/\mathcal{S} \) is its subgroup of order 2, set \( \mathcal{I} = \mathcal{S}\mathcal{B} \). By Step 1 it follows that the hypotheses of Lemma 1.2 are satisfied here. Thus there exists \( \mathcal{R} \triangle \mathcal{S} \) with \( \mathcal{R} \cap \mathcal{D} = \mathcal{I} \). Since \( \left( \frac{x}{-x} \right) \in \mathcal{R} \) and \( T \) is conjugate to \( \left( \frac{x}{-x} \right) \) in \( \mathcal{S} \), it follows that \( T \in \mathcal{R} \). Thus \( \mathcal{R} \) is doubly transitive with \( \mathcal{R}_\infty = \mathcal{I} \) and \( \mathcal{R}_\infty = \mathcal{S} \) or \( \mathcal{B} \). Applying the uniqueness part of Lemma 1.4 (ii) to both \( \mathcal{R} \) and \( \mathcal{S} \) we conclude that in equation \((*)\), \( \left( \frac{x}{a^2} \right) \in \tilde{\mathcal{S}} \) or \( \mathcal{B} \). Hence if \( \sigma \neq 1 \) then \( \sigma^2 = 1 \) and \( n \) is even.

We now find \( r \) and \( s \). By Step 1, \( |\mathcal{S}^{1-r}| = |\mathcal{S} : \mathcal{S}_t| \). Since \( \mathcal{S} \) is half-transitive \( |\mathcal{S} : \mathcal{S}_t| = |GF(p^n)^*| \) so \( r \) is even. Set \( \mathcal{L} = \mathcal{R}_\infty \). By Step 1 and the definition of \( \mathcal{R} \) we have one of the following three possibilities:

1. \( \mathcal{L} = \tilde{\mathcal{S}} \), \( \left( \frac{x}{-x} \right) = \tilde{\mathcal{S}} \); 2. \( \mathcal{L} = \tilde{\mathcal{S}} \mathcal{B} \), \( |\mathcal{L}_t| = 2 \); 3. \( \left[ \mathcal{L} : \tilde{\mathcal{S}} \right] = 2 \) so \( \mathcal{L}^{1-r} = 2 \), \( \tilde{\mathcal{S}} = \tilde{\mathcal{S}}^{1-r} \).

We apply Lemma 1.3 to \( \mathcal{R} \) since \( T \in \mathcal{R} \). In cases (1) and (3) above we have \( |\mathcal{S}| \geq (p^n - 1)/2 \) so \( \tilde{\mathcal{S}}^{1-r} \geq (p^n - 1)/4 \). In case (2) since \( |\mathcal{L}_t| = 2 \) we have \( |\mathcal{L}| > (p^n - 1)/2 \) and \( |\mathcal{S}^{1-r}| > (p^n - 1)/8 \). Hence either \( r \leq 4 \) or \( r < 8 \). Since \( r \) is even we have \( r = 2, 4 \) or 6.

Now \( \sigma \) acts on the cyclic quotient \( GF(p^n)^*/\mathcal{R} \) like \( x \rightarrow x^{p^n/2} \) since \( \sigma \) has order 2. Thus \( |\mathcal{S}/\mathcal{R}| = \text{g.c.d.} \{r, \frac{p^n}{2} - 1\} \geq 2 \) since \( r \) is even.
Hence we have (i) and (ii).

Now suppose $\sigma$ occurs in equation (*) and let $b$ satisfy $b \in R$, $b + 1 \in \mathcal{S}$. Set $x = f(ba) = b^{-1}f(a)$ in (*) so that $f(x) = ba$ and

$$f(a) = f(ba + a) + f(af(a)^{-\sigma}b^{-\sigma}f(a)^{\sigma} + a) = f((b + 1)a) + f(b^{-\sigma}(b^\sigma + 1)a).$$

Now $b^{-\sigma} \in R$ and since $b + 1 \in \mathcal{S}$ we have $(b^\sigma + 1)/(b + 1) = (b + 1)^{\sigma - 1} \in R$. Thus

$$f(b^{-\sigma}(b^\sigma + 1)a) = b^\sigma f((b^\sigma + 1)a) = b^\sigma f([(b^\sigma + 1)/(b + 1)](b + 1)a) = [b^\sigma(b + 1)/(b^\sigma + 1)]f((b + 1)a).$$

This yields

$$f(a) = f((b + 1)a) + [b^\sigma(b + 1)/(b^\sigma + 1)]f((b + 1)a)$$

and hence

$$f((b + 1)a) = [(b^\sigma + 1)/(bb^\sigma + 2b^\sigma + 1)]f(a).$$

Now $b^{-1} \in R$ and $b^{-1} + 1 = b^{-1}(b + 1) \in \mathcal{S}$ so applying the above with $b$ replaced by $b^{-1}$ yields

$$f((b^{-1} + 1)a) = [(b^{-\sigma} + 1)/(b^{-1}b^{-\sigma} + 2b^{-\sigma} + 1)]f(a) = b[(b^\sigma + 1)/(bb^\sigma + 2b + 1)]f(a).$$

Finally

$$f((b^{-1} + 1)a) = f(b^{-1}(b + 1)a) = bf((b + 1)a)$$

so the above yields clearly $b = b^\sigma$.

Step 4. Proof of the theorem. Let $N_1$ denote the number of ordered pairs $(x, y)$ with $x, y \in GF(p^n)$ and $y^r - x^r - 1 = 0$. By [7] (page 502) we have $|N_1 - p^n| \leq (r - 1)(x - 1)p^{n/2}$ so that

$$N_1 \geq p^n - (r - 1)(x - 1)p^{n/2}.$$ 

Let $N_1^\dagger$ count the number of solutions with $xy \neq 0$ so that $N_1^\dagger \geq N_1 - r - s$. Finally let $N$ count the number of pairs $(x^r, y^r)$ with $y^r - x^r - 1 = 0$ and $xy \neq 0$. Clearly $N \geq N_1^\dagger/r$s so

$$N \geq [p^n - (r - 1)(x - 1)p^{n/2} - (r + s)]/rs.$$ 

Note that $\mathcal{R} = \{x^r | x \in GF(p^n)^k\}$ and $\mathcal{S} = \{y^r\}$ so that $N$ counts the number of $b \in \mathcal{R}$ with $b + 1 \in \mathcal{S}$.

Suppose we do not have $\Gamma(p^n) < \mathcal{S} \subseteq \Gamma(p^n)$. Then by Step 2, $g \neq \{1\}$. Let $\sigma \in g$ with $\sigma \neq 1$. By [Step 3 we have $n$ even, $\sigma^2 = 1$.
and for all $b \in \mathbb{R}$ with $b + 1 \in \mathcal{S}$, $b$ is in the fixed field of $\sigma$. Thus $p^{\sigma/2} > N$ and

$$p^{\sigma/2} > [p^s - (r - 1)(s - 1)p^{\sigma/2} - (r + s)]/rs$$

or

(**) \[(r + s) > p^{\sigma/2}[p^{\sigma/2} - (r - 1)(s - 1) - rs].\]

Let us consider $n = 2$ first. Clearly $\mathcal{S} = \mathcal{S}_2$, here since $\mathcal{S}$ does not act semiregularly. We have $r = 2, 4$ or $6$. Suppose $r = 6$. Then clearly $[T(p^n) : \mathcal{S}] = 3$ and hence by Lemma 2.3, $\mathcal{S} \subseteq \text{Alt}\,(GF(p^n) \cup \{\infty\})$ but $\left(\begin{array}{c} x \\ -x \end{array}\right)$ is in the alternating group. Apply Lemma 1.3 to doubly transitive $\mathcal{S} \cap \text{Alt}\,(GF(p^n) \cup \{\infty\})$. We obtain

$$|\mathcal{S} \cap \text{Alt}\,(GF(p^n) \cup \{\infty\})| \geq (p^n - 1)/2$$

so $|\mathcal{S}| \geq (p^n - 1)/2$. This contradicts the fact that $|\mathcal{S}| = 2(p^n - 1)/3$. Thus $r \neq 6$.

Let $r = 4$. If $p = 1$ modulo $4$, then by Step 3 (ii), $s = 1$. Then equation (***) yields $p < 5$, a contradiction. Let $p = -1$ modulo $4$. Since $r = 4$ we see that $\mathcal{S} \subseteq \text{Alt}\,(GF(p^n) \cup \{\infty\})$. But by Lemma 2.3 (ii) $\mathcal{S} \subseteq \text{Alt}\,(GF(p^n) \cup \{\infty\})$. Applying Lemma 1.4 (ii) to doubly transitive $\mathcal{S} \cap \text{Alt}\,(GF(p^n) \cup \{\infty\})$ yields $g = \{1\}$, a contradiction. Finally if $r = 2$, then $s = 1$ and (**) yields no exceptions.

Now let $n > 2$ so $n$ is even and $n \geq 4$. Since $r \leq 6$, $s \leq 3$ equation (**) becomes $9 \geq p^{\sigma/2}[p^{\sigma/2} - 28]$ or $p^{\sigma/2} \leq 28$. Hence we have only $p^s = 3^4, 5^4$ and $3^6$. Note that $r \mid (p^n - 1)$ so that if $p = 3$ then $r = 2$ or $4$. This eliminates $p^s = 3^6$ and by (**) we must have $p^s = 3^4$, $r = 4$ or $p^s = 5^4$, $r = 6$. If $p^s = 3^4$, $r = 4$, then Step 3 (ii) yields $s = 1$ and this contradicts (**). Finally let $p^s = 5^4$, $r = 6$. If $a = 41/2$ in $GF(5^4)$ then

$$(2 + a + 4a^3)^8 + 1 = a + 3a^2 + 2a^3 = (2 + 3a^2 + 2a^3)^8.$$  

Hence if $b = 4 + a + 3a^2 + 2a^3$ then $b \in \mathcal{R}$, $b + 1 \in \mathcal{S}$ and $b' \neq b$. This contradicts Step 3 and the result follows.

3. The main result. We now combine the preceding work with the main result of [4] to obtain.

**Theorem 3.1.** Let $\mathcal{S}$ be a $5/2$-transitive permutation group which is not a Zassenhaus group. Suppose that the stabilizer of a point is solvable. Then modulo a possible finite number of exceptions we have $\Gamma(p^n) \supseteq \mathcal{S} > \Gamma(p^n)$ for some prime power $p^n$.

**Proof.** The group $\mathcal{S}_n$ is a solvable $3/2$-transitive group which is
not a Frobenius group. By the main theorem of [4] we have either $\mathcal{G}_\infty \subseteq S(p^n)$, $\mathcal{G}_\infty = S_\infty(p^n)$ with $p \neq 2$, or $\mathcal{G}_\infty$ is one of a finite number of exceptions. The result therefore follows from Propositions 2.4, 2.6 and 2.7.

Presumably we can find the possible exceptions here without knowing all the exceptions in the 3/2-transitive case. This is the case since the existence of a transitive extension greatly restricts the structure of a group. However it appears that we still have to look closer at normal 3-subgroups of half-transitive linear groups. For example, if we can show that for such a linear group $\mathcal{G}$, $O_d(\mathcal{G})$ is cyclic, then we would know (see [4]) that (1) if $p = 2$, then $\mathcal{G}_\infty \subseteq S(2^n)$, (2) if $p \neq 2$ and $|\mathcal{G}_\infty|$ is odd, then $\mathcal{G}_\infty \subseteq S(p^n)$, (3) if $p \neq 2$ and $|\mathcal{G}_\infty|$ is even, then $\mathcal{G} = \mathcal{G}_\infty$ has a central involution. Here $\mathcal{G}_\infty$ has degree $p^n$. Hopefully these normal 3-subgroups will be studied at some later time.

Finally we consider the possible transitive extensions of these 5/2-transitive groups.

**Theorem 3.2.** Let $\mathcal{G}$ be an $(n+1/2)$-transitive permutation group and let $\mathcal{D}$ be the stabilizer of $(n-1)$ points. Suppose that $\mathcal{D}$ is solvable and not a Frobenius group. If $n \geq 3$ then $\mathcal{G} = \text{Sym}_{n+3}$.

*Proof.* We note first that if $\mathcal{G} = \text{Sym}_{n+3}$ then $\mathcal{G}$ is $(n+3)$-transitive and hence $(n+1/2)$-transitive. Also $\mathcal{D} = \text{Sym}_n$ is solvable and not a Frobenius group. Thus these groups do occur.

To prove the result it clearly suffices to assume that $n = 3$ and to show that $\mathcal{G} = \text{Sym}_3$. Let $n = 3$ and let $\infty, 0, 1$ be three points. Set $\mathcal{R} = \mathcal{G}_\infty$, $\mathcal{D} = \mathcal{G}_\infty$, $\mathcal{G} = \mathcal{G}_\infty$. Then $\mathcal{R}$ is 5/2-transitive and by Lemma 2.1, $\mathcal{R}$ has no regular normal subgroup. We know that $\mathcal{D}$ has a regular normal elementary abelian subgroup $\mathcal{B}$ so $\mathcal{D} = \mathcal{B}$. Since $\mathcal{B}$ is abelian and $\mathcal{D}$ is primitive, $\mathcal{B}$ is the unique minimal normal subgroup of $\mathcal{D}$. Hence $\mathcal{B}$ is characteristic in $\mathcal{D}$ and $\mathcal{G}$ acts irreducibly on $\mathcal{B}$. Since $\mathcal{D}$ is not a Frobenius group, we cannot have $|\mathcal{B}| = 3$. Further $\mathcal{B}$ is elementary so we cannot have $|\mathcal{B}| = 8$ with $\mathcal{B}$ having a cyclic subgroup of index 2. By Theorems 1 and 3 of [6] we must therefore have $|\mathcal{B}| = 4$ or 9 and hence $\deg \mathcal{G} = |\mathcal{B}| + 2 = 6$ or 11. Suppose $\deg \mathcal{G} = 6$. Since $\mathcal{G}$ is 7/2-transitive we have $|\mathcal{G}| > 6 \cdot 5 \cdot 4$ so $[\text{Sym}_3 : \mathcal{G}] < 6$. Hence $\mathcal{G} = \text{Alt}_3$ or $\text{Sym}_3$. If $\mathcal{G} = \text{Alt}_3$ then $\mathcal{D} = \text{Alt}_3$, a Frobenius group. Thus we have only $\mathcal{G} = \text{Sym}_3$ here.

We now assume that $|\mathcal{B}| = 9$ and derive a contradiction. Now $\mathcal{B}$ contains an element of order 3 fixing precisely two element. Since $\mathcal{G}$ is triply transitive, $\mathcal{G}$ contains $W$ a conjugate of this element with $W = (a)(b)(0 \infty 1) \cdots$. Hence $W$ normalizes $\mathcal{G}$. If $H \in C_\mathcal{G}(W)$, then
$aH = (aW)H = (aH)W$ so $aH = a$ or $b$ and hence $|C_\delta(W)| \leq 2 |\delta|$. If $W$ acts trivially on $\delta$, then $[\delta : \delta] = 2$ and since $\delta$ is half-transitive, it must be an elementary abelian 2-group. This contradicts the fact that $\delta$ acts irreducibly on $\mathfrak{S}$. We have $\delta \subseteq GL(2, 3)$ and $W$ acts nontrivially on $\delta$. Further $\delta$ acts irreducibly so $O_3(\delta) = \langle 1 \rangle$.

If $3 \nmid |\delta|$, then $\delta$ is a 2-group with a cyclic subgroup of index 2 which admits $W$ nontrivially. Since $\delta$ acts irreducibly we conclude that $\delta$ is the quaternion group of order 8. Then $\mathfrak{S}$ is a Frobenius group, a contradiction. Hence $3 \mid |\delta|$ so since $O_3(\delta) = \langle 1 \rangle$ we have $\delta = SL(2, 3)$ or $GL(2, 3)$. Let $\Delta = O_3(\delta)$. Then $\Delta$ is the quaternion group of order 8. It acts regularly on 8 points and fixes 3. Now $\mathfrak{S}$, a Sylow 3-subgroup of $\langle \delta, W \rangle$ is abelian of type $(3, 3)$ and acts on $\Delta$. Hence there exists $S \in \mathfrak{S}$ with $S$ centralizing $\Delta$. From the way $\Delta$ acts as a permutation group it is clear that $S$ is a 3-cycle, in fact $S = (0 \infty 1)$ or $(0 1 \infty)$. Since $\delta$ is triply transitive it contains all 3-cycles so $\mathfrak{S} \supseteq \text{Alt}_6$. Thus $\mathfrak{S} \supseteq \text{Alt}_9$ and this contradicts the solvability of $\mathfrak{S}$. This completes the proof.

In a later paper, “Exceptional 3/2-transitive Permutation Groups” which will appear in this journal, we completely classify the solvable 3/2-transitive permutation groups. Moreover the exceptional groups, which have degrees $3^2, 5^2, 7^2, 11^2, 17^2$ and $3^4$, are shown to have no transitive extensions. Thus no exceptions occur in our main theorem.

**References**


Received July 26, 1967. This research partially supported by Army Contract SAR/DA-31-124-ARO(D) 336.

YALE UNIVERSITY
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrick Robert Ahern, <em>On the geometry of the unit ball in the space of real annihilating measures</em></td>
<td>1</td>
</tr>
<tr>
<td>Kirby Alan Baker, <em>Equational classes of modular lattices</em></td>
<td>9</td>
</tr>
<tr>
<td>E. F. Beckenbach and Gerald Andrew Hutchison, <em>Meromorphic minimal surfaces</em></td>
<td>17</td>
</tr>
<tr>
<td>Tae Ho Choe, <em>Intrinsic topologies in a topological lattice</em></td>
<td>49</td>
</tr>
<tr>
<td>John Bligh Conway, <em>A theorem on sequential convergence of measures and some applications</em></td>
<td>53</td>
</tr>
<tr>
<td>Roger Cuppens, <em>On the decomposition of infinitely divisible probability laws without normal factor</em></td>
<td>61</td>
</tr>
<tr>
<td>Lynn Harry Erbe, <em>Nonoscillatory solutions of second order nonlinear differential equations</em></td>
<td>77</td>
</tr>
<tr>
<td>Burton I. Fein, <em>The Schur index for projective representations of finite groups</em></td>
<td>87</td>
</tr>
<tr>
<td>Stanley P. Gudder, <em>A note on proposition observables</em></td>
<td>101</td>
</tr>
<tr>
<td>Kenneth Kapp, <em>On Croisot’s theory of decompositions</em></td>
<td>105</td>
</tr>
<tr>
<td>Robert P. Kaufman, <em>Gap series and an example to Malliavin’s theorem</em></td>
<td>117</td>
</tr>
<tr>
<td>E. J. McShane, Robert Breckenridge Warfield, Jr. and V. M. Warfield, <em>Invariant extensions of linear functionals, with applications to measures and stochastic processes</em></td>
<td>121</td>
</tr>
<tr>
<td>Marvin Victor Mielke, <em>Rearrangement of spherical modifications</em></td>
<td>143</td>
</tr>
<tr>
<td>Akio Osada, <em>On unicity of capacity functions</em></td>
<td>151</td>
</tr>
<tr>
<td>Donald Steven Passman, <em>Some 5/2 transitive permutation groups</em></td>
<td>157</td>
</tr>
<tr>
<td>Harold L. Peterson, Jr., <em>Regular and irregular measures on groups and dyadic spaces</em></td>
<td>173</td>
</tr>
<tr>
<td>Habib Salehi, <em>On interpolation of q-variate stationary stochastic processes</em></td>
<td>183</td>
</tr>
<tr>
<td>Michael Samuel Skaff, <em>Vector valued Orlicz spaces generalized N-functions. I</em></td>
<td>193</td>
</tr>
<tr>
<td>Thomas Paul Whaley, <em>Algebras satisfying the descending chain condition for subalgebras</em></td>
<td>217</td>
</tr>
<tr>
<td>G. K. White, <em>On subgroups of fixed index</em></td>
<td>225</td>
</tr>
<tr>
<td>Martin Michael Zuckerman, <em>A unifying condition for implications among the axioms of choice for finite sets</em></td>
<td>233</td>
</tr>
</tbody>
</table>