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 \( G \) such that \( G \) is not a Zassenhaus group and such that the stabilizer of a point in \( G \) is solvable. We show in fact that to within a possible finite number of exceptions \( G \) 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

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

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

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

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

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

**THEOREM.** Let \( \mathfrak{G} \) 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, \( \Gamma(p^n) \supseteq \mathfrak{G} > \bar{\Gamma}(p^n) \) for some \( p^n \).

The question of the possible exceptions will be discussed briefly in § 3. We use here the notation of [4]. Thus we have certain linear groups \( T(p^n) \) and \( T_0(p^n) \) and certain permutation groups \( S(p^n) \).
and \( S_q(p^n) \). 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:

- \( \mathcal{D} \) is a doubly transitive permutation group of degree \( 1 + m \)
- \( \tau \) and 0 are two points
- \( \mathcal{D} = \mathcal{D}_\omega, \quad \mathcal{D} = \mathcal{D}_\omega \cap \mathcal{D}_\tau \)
- \( T \in \mathcal{D} \) is an involution with \( T = (0 \tau) \cdots \).

The above implies that \( T \) normalizes \( \mathcal{D} \) and \( \mathcal{D} = \mathcal{D} \cap \mathcal{D}_\tau \).

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 \( \alpha(H^r) = \alpha(H) \) for all \( H \in \mathcal{D} \). 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 \( \mathcal{D} \).

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

\[
A^{\sigma^{-1}} = B^{\sigma^r} \in \mathcal{D} \cap \mathcal{D}_r = \mathcal{D}
\]

so by assumption \( \alpha(B^{\sigma^r}) = \alpha(B^\sigma) \). Thus \( \alpha(A) = \alpha(A^{\sigma^{-1}}) = \alpha(B^{\sigma^r}) = \alpha(B^\sigma) = \alpha(B) \) and this fact follows.

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

\[
\alpha^*(D) = | D |^{-1} \sum_{\delta \in \mathcal{D}} \alpha_\delta(D^\sigma) = \alpha(D) | \mathcal{D} |^{-1} \sum_{\delta \in \mathcal{D}} 1_{\mathcal{D}\delta}(D^\sigma) = \alpha(D)1_{\mathcal{D}\sigma}(D)
\]

and (i) follows.

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

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

Thus we must have \( \alpha^* = \chi_1 + \chi_2 \) with \( \chi_1 \) and \( \chi_2 \) distinct irreducible characters of \( \mathcal{G} \). Now \([\alpha^*, 1_{\mathcal{D}}]_{\mathcal{D}} = [\alpha, 1_\mathcal{D} | \mathcal{D}] = [\alpha, 1_\mathcal{D}] = 0 \) 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 $\mathcal{R} \triangleleft \mathcal{S}$ with $\mathcal{R} \cap \mathcal{D} = \mathcal{X}$.

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 $\mathcal{D}$. If $H \in \mathcal{D}$ then $D = H^TH^{-1}$ satisfies $D^r = D^{-1}$ so $D \in \mathcal{X}$. Hence $\alpha(H^TH^{-1}) = 1$ and the hypothesis of Lemma 1.1 holds. Thus we have $\alpha^* = \chi_1 + \chi_2$. Further, as is well known, $1_\mathcal{D} = 1_\mathcal{S} + \xi$ where $\xi$ is an irreducible nonprincipal character. We will prove that either $\chi_1$ or $\chi_2$ is linear. Suppose say $\chi_1$ is linear. Then $1 = [\alpha^*, \chi_1]_\mathcal{S} = [\alpha, \chi_1 | \mathcal{D}]_\mathcal{D}$ implies that $\chi_1 | \mathcal{D} = \alpha$. If $\mathcal{S}$ is the kernel of $\chi_1$, then $\mathcal{R} \triangleleft \mathcal{S}$ and $\mathcal{R} \cap \mathcal{D} = \mathcal{X}$, 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 $\chi_1$ linear and the result would follow. Thus we can assume that $1_\mathcal{S}, \xi, \chi_1$ and $\chi_2$ are all distinct.

Let $\beta = \alpha - 1_\mathcal{D}$. We show now that $\beta^*$ vanishes on all elements of the form $G = T_1T_2$ 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), $\alpha^*(G) = \alpha(G)1_\mathcal{D}(G) = 1_\mathcal{S}(G)$ 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 $G = T_1T_2 \in \mathcal{X}$. Now we suppose that $T_2 \in \mathcal{S}$. From $\mathcal{S} = \mathcal{D} \cup \mathcal{D}TD\mathcal{D}$ we see that a suitable $\mathcal{D}$ conjugate of $T_2$ is of the form $TD$ with $D \in \mathcal{D}$. By taking conjugates again we can assume that $G = WT_2D$ with $G, D \in \mathcal{D}$ and $W$ and $TD$ 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 $\mathcal{S}$ 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 $T_1T_2 = G$. As is well known, $\gamma(G) = |\mathcal{S}|^{-1} |\mathcal{S}| \sum \chi(T) \chi(G)/\chi(1)$ where the sum runs over all irreducible characters of $\mathcal{S}$. By the remarks of the preceding paragraph $[\beta^*, \gamma]_{\mathcal{S}} = 0$. Hence since $1_\mathcal{S}, \chi_1, \chi_2$ and $\xi$ are distinct and $\beta^* = \chi_1 + \chi_2 - 1_\mathcal{S} - \xi$ we have

$$\frac{\bar{\chi}_1(T)^2}{\chi_1(1)} + \frac{\bar{\chi}_2(T)^2}{\chi_2(1)} = \frac{\bar{1}_\mathcal{S}(T)^2}{1_\mathcal{S}(1)} + \frac{\bar{\xi}(T)^2}{\xi(1)}.$$ 

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

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

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 $p \nmid \chi_1(1)$. Then $m \mid \chi_1(1)\chi_2(1)$ implies that $m \mid \chi_2(1)$ so $\chi_2(1) \geq m$. From $\chi_1(1) + \chi_2(1) = m + 1$ we conclude that $\chi_2(1) = m$ and $\chi_1(1) = 1$. 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 $\theta = 1_{\mathcal{S}}$ be the permutation character. Then ([3] Th. 3.2) $\sum_{G \in \mathcal{S}} \theta(G) = |\mathcal{S}|$ and $\sum_{G \in \mathcal{S}} \theta(G^2) = 2|\mathcal{S}|$. Hence

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

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 $D = (x, f(x))$ with $(x, \alpha(x)) \in \mathcal{S}$ and $b \in \mathcal{B}$.

Let $T = \left(\begin{array}{c}x \\ f(x)\end{array}\right)$ and assume that $T$ commutes with the permutation $(x, -x)$. 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 $(x, \alpha(x)) \in \mathcal{S}$ 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 \( \binom{x}{\alpha(x)} \) elements which occur above. Then \( \mathcal{G} = \langle \mathcal{S}, \mathcal{B}, T \rangle \) is doubly transitive with \( \mathcal{G}_{\infty_0} = \mathcal{S} \).

(iv) If \( \binom{x}{-x} \in \mathcal{S} \) then \( T \) acts on the orbits of \( \mathcal{G} \) on \( \mathcal{B} \).

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

Let \( V \in \mathcal{B}^* \) be the permutation \( V = \binom{x}{x + a} \). Then \( T V T \in \mathcal{G} \) and \( (\infty) T V T = (a) T \neq \infty \). Thus \( T V T \in \mathcal{D} T \mathcal{S} \) and hence

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

This is equivalent to

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

Note that \( \binom{x}{\alpha(x)} \in \mathcal{S} \) and \( b, c \in \mathcal{B} \). 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 \( \binom{x}{-x} \) so \( f(-x) = -f(x) \) and \( b = -f^2(a) = -a \). Since \( \binom{x}{\alpha(x)} \in \mathcal{S} \) is now clearly unique, we have (ii).

By definition of \( \mathcal{S} \) we have \( T \mathcal{B} T \subseteq \mathcal{S} \mathcal{B} \mathcal{B} \) and since \( T \) normalizes \( \mathcal{S} \), \( \mathcal{G} = \mathcal{S} \mathcal{B} \cup \mathcal{S} \mathcal{B} T \mathcal{B} \) is a group. Since \( \mathcal{G} \supseteq \langle \mathcal{B}, T \rangle \), \( \mathcal{G} \) 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 \( \binom{x}{\alpha(x)} \in \mathcal{S} \), \( a \) and \( f(a) \) are in the same orbit of \( \mathcal{S} \). 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:

\( \mathcal{G} \) is a 5/2-transitive permutation group of degree \( 1 + m \)
\( \mathcal{G} \) is not a Zassenhaus group
\( \infty \) and \( 0 \) are two points
\( \mathcal{D} = \mathcal{G}_{\infty}, \mathcal{S} = \mathcal{G}_{\infty_0} = \mathcal{D}, \mathcal{D} \) is solvable.

Thus \( \mathcal{D} \) is a 3/2-transitive permutation group which is not a Frobenius group. By Theorem 10.4 of [8] \( \mathcal{D} \) is primitive and hence \( \mathcal{G} \) is doubly primitive. Since \( \mathcal{D} \) is solvable it has a regular normal elementary abelian \( p \)-group \( \mathcal{B} \). Thus \( \mathcal{D} = \mathcal{S} \mathcal{B} \) and \( m \) is a power of \( p \).
Lemma 2.1. Let $\mathfrak{A} \triangleleft \mathfrak{G}$ with $\mathfrak{A} \neq \langle 1 \rangle$. Then $\mathfrak{A}$ 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 $\mathfrak{A}$ is such a group. Since $\mathfrak{G}$ is doubly transitive $\mathfrak{A}$ is a elementary abelian $q$-group for some prime $q$. Then $\mathfrak{B}\mathfrak{A}$ is sharply 2-transitive so since $\mathfrak{B}$ is an elementary abelian $p$-group it follows that $\mathfrak{B}$ is cyclic of order $p$ and $p + 1 = |L|$. Now $\mathfrak{H}$ acts faithfully on $\mathfrak{B}$ and hence $\mathfrak{H}$ acts semiregularly on $\mathfrak{B}^*$. Thus $\mathfrak{D} = \mathfrak{H}\mathfrak{B}$ is a Frobenius group, a contradiction.

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

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

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

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

(ii) $\mathfrak{S} \cong \{ax | a = b^{1-\sigma}, b \in GF(p^n)\}$ where $\sigma$ is a field automorphism of order $k$.

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

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

Lemma 2.3. Let $p > 2$ and consider $T(p^n)$ as a subgroup of Sym $(GF(p^n))$. Then $T(p^n) \nsubseteq Alt(GF(p^n))$. Moreover we have the following:

(i) If $a$ generates the multiplicative group $GF(p^n)$, then $\left( x_{ax} \right) \in Alt(GF(p^n))$.

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

(iii) If $n$ is even, then $\left( x_a \right) \in Alt(GF(p^n))$.

Proof. The group generated by $\left( x_{ax} \right)$ acts regularly on $GF(p^n)^*$ and hence $\left( x_{ax} \right)$ is a $(p^n - 1)$-cycle. Since $p > 2$, $p^n - 1$ is even and hence $\left( x_{ax} \right)$ is an odd permutation. This also yields the contention that $T(p^n) \nsubseteq Alt(GF(p^n))$. 
(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 \( q^{2r-1} = \pm 1 + \lambda 2^{r+1} \)

\[
q^{2r} = (q^{2r-1})^2 = (\pm 1 + \lambda 2^{r+1})^2 = 1 \pm \lambda 2^{r+2} + \lambda^2 2^{2r+2}.
\]

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

\[
(q^{2i} - q^{2i-1})/2^i = q^{2i-1}(q^{2i-1} - 1)/2^i.
\]

By the above, if \( i > 1 \) then \( 2^{i+1} | (q^{2i-1} - 1) \) and hence \( \left( \frac{x}{x^\tau} \right) \) 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 \( q \equiv p \mod 4 \) and (ii) follows.

(iii) \( \left( \frac{x}{x^\tau} \right) \) 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 \( S = S_6(p^n) \), then \( p^n = 3 \) and \( \Gamma(3^2) < S < \Gamma(3^2) \).

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

\[
4(p^n - 1) = |T_\sigma(p^n)| = |S| > (p^{2n} - 1)/2
\]

or \( 7 > p^n \). Thus \( p^n = 3 \) or \( 5 \).

Since \( S \) is doubly transitive we can find \( T \) conjugate to \( G \) with \( T = (0 \infty) \cdot \cdots \). Then \( T \) normalizes \( S \) and centralizes its unique central involution \( G = \left( \frac{x}{x^\tau} \right) \). By Lemma 1.4 (iv), \( T \) acts on each orbit of \( S \) on \( \mathcal{S}^p \). Now if \( v \in \mathcal{S}^p \), then \( |S_v| = 2 \). This implies easily that if \( H \) is a noncentral involution of \( S \), then \( H^T \) is conjugate to \( H \) in \( S \). Let \( p^n = 5 \). Then \( S \) is easily seen to be generated by its noncentral involutions so \( S^{1-T} \subseteq S \). Thus \( |S : C_S(T)| = |S^{1-T}| \leq |S_v| = 2 \) and \( |C_S(T)| \geq 8 \). On the other hand \( C_S(T) \) acts on the fixed points
of \(T\) namely \(\{a, b\}\), so \([C_\mathcal{D}(T): C_\mathcal{D}(T) \cap \mathfrak{S}_a] \leq 2\). Since \(|\mathfrak{S}_a| = 2\), this is a contradiction.

Finally let \(p^n = 3\). Here \(T_0(3)\) is a dihedral group of order 8 and \(S_0(3) \subseteq S(3^3)\). This case is then included in Proposition 2.7 and we obtain \(\bar{\Gamma}(3^3) < \mathfrak{S} \subseteq \Gamma(3^3)\). By order considerations \(\mathfrak{S} \neq \Gamma(3^3)\) so this results follows.

**Proposition 2.5.** If \(\mathfrak{D} \subseteq S(2^n)\) then \(\bar{\Gamma}(2^n) < \mathfrak{S} \subseteq \Gamma(2^n)\).

*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 \(\mathfrak{S}_1\). 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, \(C_\mathfrak{S}(T) = \langle 1 \rangle\). Then \(\mathfrak{S}^{1-T} = \mathfrak{S}_1\). Since \(\mathfrak{S}/\mathfrak{S}_1\) is abelian, \((\mathfrak{S}/\mathfrak{S}_1)^{1-T}\) is a group and hence \(\mathfrak{S}^{1-T}\) is a group containing \(\mathfrak{S}_1\). 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 \(|\mathfrak{S}^{1-T}| = |\mathfrak{S}_1|\), |\(\mathfrak{S}_1| \leq |\mathfrak{S}|\) and \(C_\mathfrak{S}(T) \subseteq \mathfrak{S}_1\). This yields \(C_\mathfrak{S}(T) = \mathfrak{S}_1\) and \(\mathfrak{S} = \mathfrak{S}_1\). The latter shows that each orbit of \(\mathfrak{S}_1\) on \(GF(2^n)\) has size \(|\mathfrak{S}_1|\), an odd number.

In characteristic 2 the permutation \(\left(\begin{array}{c} x \\ -x \end{array}\right)\) is trivial so by Lemma 1.4 (iv) \(T\) acts on each orbit of \(\mathfrak{S}_1\) on \(GF(2^n)\). These orbits have odd size so \(T\) fixes a point in each orbit. Thus there is only one such orbit and \(\mathfrak{S}_1\) is transitive. This yields

\[\mathfrak{S}^{1-T} = \mathfrak{S}_1 = \{bx \mid b \in GF(2^n)^d\}\]

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 \(\mathfrak{S} = \mathfrak{D} \cup \mathfrak{D}T\mathfrak{S}\), the result follows easily.

The following is an easy special case of a recent result of Bender ([11]).

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

*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 $\mathcal{D}$ and $\tilde{\mathcal{D}}$. We show now that $T$ centralizes the quotient $\mathcal{D}/\tilde{\mathcal{D}}$. If not, then since $\mathcal{D}/\tilde{\mathcal{D}}$ is abelian and has odd order, we can find a nonidentity subgroup $\mathcal{W} \subseteq \mathcal{D}/\tilde{\mathcal{D}}$ on which $T$ acts in a dihedral manner. Then dihedral group $\langle \mathcal{W}, T \rangle$ acts on $\tilde{\mathcal{D}}$. Since $\tilde{\mathcal{D}}$ is cyclic, $\text{Aut} \tilde{\mathcal{D}}$ is abelian and hence $\mathcal{W} = \langle \mathcal{W}, T \rangle'$ centralizes $\tilde{\mathcal{D}}$. This contradicts the fact that $\tilde{\mathcal{D}}$ is self centralizing in $\mathcal{D}$.

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

By Lemma 2.1, $\mathcal{S}$ is doubly transitive and has no regular normal subgroup. Furthermore $\mathcal{S}_\infty = \mathcal{X} = \tilde{\mathcal{D}} \triangle \mathcal{D}$ and $\mathcal{D}$ is abelian. Thus $\mathcal{K}$ is a Zassenhaus group and the result of Feit ([2]) implies that $T$ is a permutation of the form \( \begin{pmatrix} x \\ -a/x \end{pmatrix} \) and $|\tilde{\mathcal{D}}| = (p^n - 1)/2$. Since $\mathcal{S} = \mathcal{D} \cup \mathcal{D}T\mathcal{W}$, the result follows easily.

**Proposition 2.7.** If $\mathcal{D} \subseteq S(p^n)$ with $p \neq 2$ and $|\mathcal{D}|$ is even, then $I'(p^n) \lesssim \mathcal{S} \lesssim I(p^n)$.

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

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

(i) $\tilde{\mathcal{S}} = \mathcal{S}_{-r}$ and $[\mathcal{S}: \tilde{\mathcal{S}}]$ = 2 or

(ii) $[\tilde{\mathcal{S}} : \mathcal{S}_{-r}] = 2$ and $\mathcal{S} = \tilde{\mathcal{S}} \mathcal{S}_r$.

In either case $[\tilde{\mathcal{S}} : \mathcal{S}_r] = 2 | \mathcal{S}_{-r} |$.

Now by assumption $2 | |\mathcal{D}|$ so since $p \neq 2$, $2 | |\mathcal{S}|$. If $2 | |\tilde{\mathcal{S}}|$, then certainly $\tilde{\mathcal{S}}$ has a central element of order 2. This is of course the permutation $\begin{pmatrix} x \\ -x \end{pmatrix}$ which fixes precisely two points. Suppose $2 \not{|} |\tilde{\mathcal{S}}| \text{ and let } H \in \tilde{\mathcal{S}} \text{ have order 2. Since } H \neq \begin{pmatrix} x \\ -x \end{pmatrix}$, $H$ must have a fixed point on $\mathcal{W}^*$. Hence $2 \not{|} |\mathcal{S}_r|$. If $\rho$ is a field automorphism of order 2, then by Lemma 2.2, $\tilde{\mathcal{S}} \cong \{ b^{-r}x \mid b \in GF(p^n)^* \}$. 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 $\begin{pmatrix} x \\ -x \end{pmatrix}$.
with \( T = (0 \infty) \cdots \). Then \( T \) fixes precisely two points and \( T \) normalizes \( \mathcal{S} \). We can clearly write the latter group in such a way that \( T \) fixes point 1. Clearly \( T \) centralizes \( \left( \begin{array}{c} x \\ -x \end{array} \right) \in \mathcal{S} \) so if \( T = (f(x)) \), then \( f(-x) = -f(x) \). This shows that \( T \) also fixes \(-1\) so \( T = (0 \infty)(1 \cdots) \cdots \).

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

Now \( T \) acts on \( \tilde{\mathcal{S}} \) and \( C_{\tilde{\mathcal{S}}}(T) = \langle \left( \begin{array}{c} x \\ -x \end{array} \right) \rangle \). Thus since \( \tilde{\mathcal{S}} \) is abelian, \( \tilde{\mathcal{S}}^{1-r} \) is a group and \([\tilde{\mathcal{S}} : \tilde{\mathcal{S}}^{1-r}] = 2 \). Now \( \tilde{\mathcal{S}}^{1-r} \triangle \mathcal{S} \) and \( \mathcal{S}/\tilde{\mathcal{S}}^{1-r} \) is abelian since \( \tilde{\mathcal{S}}/\tilde{\mathcal{S}}^{1-r} \) is central in this quotient and \( \mathcal{S}/\tilde{\mathcal{S}} \) is cyclic. This implies that \( \tilde{\mathcal{S}}^{1-r} \) is a group so \( \tilde{\mathcal{S}}^{1-r} \) is abelian and centralizes \( \mathcal{S}' \subseteq \tilde{\mathcal{S}}^{1-r} \). By Lemma 2.2 (iii), \( \tilde{\mathcal{S}}^{1-r} \subseteq \tilde{\mathcal{S}} \) with the possible exception of \( p^n = 3^2 \) and \( \mathcal{S} \) dihedral of order 8. However in the latter case \( |\mathcal{S}/\tilde{\mathcal{S}}| = 2 \) so clearly \( \tilde{\mathcal{S}}^{1-r} \subseteq \tilde{\mathcal{S}} \).

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

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

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

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

\[ \mathcal{F}(p^n) \leq \mathcal{S} \leq \mathcal{F}(p^n) \]

Equation (\ast) follows from Lemma 1.4 (ii). Set \( x = -f(a) = f(-a) \) in (\ast). Then \( a'x^n - a = 0 \) so \( a' = -a/f(a)^r \). Suppose now that \( \mathcal{g} = \{1\} \). This implies by Lemma 1.4 (iii) that \( \mathcal{B} = \langle \tilde{\mathcal{S}}, \mathcal{B}, T \rangle \) is doubly transitive with \( \mathcal{B}_{\infty 2} = \tilde{\mathcal{S}} \). Hence \( \mathcal{B} \) is a Zassenhaus group. Let \( \mathcal{L} = \{H \in \mathcal{S} \mid H^r = H^{-1} \} \) so that \( \mathcal{L} \) is a subgroup of \( \mathcal{S} \) containing \( \left( \begin{array}{c} x \\ -x \end{array} \right) \).

With \( \mathcal{L} = \mathcal{L} \mathcal{B} \triangle \tilde{\mathcal{S}} \mathcal{B} \) we see easily that the hypotheses of Lemma 1.2 hold. Hence there exists \( \mathcal{L} \triangle \tilde{\mathcal{S}} \) with \( \mathcal{L} \cap (\tilde{\mathcal{S}} \mathcal{B}) = \mathcal{L} \mathcal{B} \). Since \( \mathcal{B} \) is doubly transitive and \( \mathcal{L} \geq \mathcal{B} \) we see that \( \mathcal{L} \not\leq \tilde{\mathcal{S}} \mathcal{B} \). Hence \( \mathcal{L} \) is doubly transitive and \( \left( \begin{array}{c} x \\ -x \end{array} \right) \in \mathcal{L} \). By Lemma 1.3, \( |\mathcal{L}| \geq (p^n - 1)/2 \).
Let \( M = \{ b \in GF(p^n) \mid \left( \frac{x}{bx} \right) \in \Omega \} \). 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 \( \mathcal{S} = \mathcal{S} \cup \mathcal{S}T \mathcal{S} \) and \( | \mathcal{S} | \geq (p^n - 1)/2 \) the result follows here.

**Step 3.** Let \( \mathcal{R} = \{ b \in GF(p^n) \mid \left( \frac{x}{bx} \right) \in \mathcal{S}^{-1} \} \). 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 \( b^\sigma = b \). Furthermore, if \( r = [GF(p^n)^* : \mathcal{R}] \) and \( s = [GF(p^n)^* : \mathcal{S}] \) then we have

(i) \( r = 2, 4 \) or 6.
(ii) \( s = r/(g.c.d(r, p^{n/2} - 1)) \leq r/2 \).

Define \( \mathcal{S} \triangle \mathcal{S} \) as follows. If \( \mathcal{S}/\mathcal{S} \) has odd order, set \( \mathcal{S} = \mathcal{S} \mathcal{S} \). If \( \mathcal{S}/\mathcal{S} \) has even order and \( \mathcal{B}/\mathcal{S} \) is its subgroup of order 2, set \( \mathcal{S} = \mathcal{S} \mathcal{B} \).

By Step 1 it follows that the hypotheses of Lemma 1.2 are satisfied here. Thus there exists \( \mathcal{R} \triangle \mathcal{S} \) with \( \mathcal{R} \cap \mathcal{S} = \mathcal{S} \). 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 \( \mathcal{R}_{\infty} = \mathcal{S} \) 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 (*), \( \left( \frac{x}{a'x^e} \right) \in \mathcal{S} \) 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, \( 2 | \mathcal{S}^{-1} | = [\mathcal{S} : \mathcal{S}_1] \). Since \( \mathcal{S} \) is half-transitive \( [\mathcal{S} : \mathcal{S}_1] | [GF(p^n)^*] \) so \( r \) is even. Set \( \mathcal{S} = \mathcal{R}_{\infty} \). By Step 1 and the definition of \( \mathcal{R} \) we have one of the following three possibilities:

1. \( \mathcal{S} = \mathcal{S}_1, | \mathcal{S}_1 : \mathcal{S}^{-1} | = 2 \); 2. \( \mathcal{S} = \mathcal{S}_1 \mathcal{S}_2, | \mathcal{S}_1 | = 2, | \mathcal{S}_1 : \mathcal{S}^{-1} | = 2 \); 3. \( | \mathcal{S} : \mathcal{S}_1 | = 2, \mathcal{S} = \mathcal{S}_1^{-1} \).

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 \( | \mathcal{S}^{-1} | \geq (p^n - 1)/4 \). In case (2) since \( | \mathcal{S}_1 | = 2 \) we have \( | \mathcal{S} | > (p^n - 1)/2 \) and \( | \mathcal{S}^{-1} | > (p^n - 1)/8 \). 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 \( | \mathcal{S}/\mathcal{R} | = g.c.d.(r, p^{n/2} - 1) \geq 2 \) since \( r \) is even.
Hence we have (i) and (ii).
Now suppose $\sigma$ occurs in equation (*) and let $b$ satisfy $b \in \mathbb{R}$, $b + 1 \in \mathbb{S}$. Set $x = f(ba) = b^{-1} f(a)$ in (*) so that $f(x) = ba$ and

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

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

$$f((b^{-1} + 1)a) = f(b^{-1}(b + 1)a) = b f((b + 1)a)$$
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 $y^s - x^r - 1 = 0$. By [7] (page 502) we have $|N_1 - p^n| \leq (r - 1)(s - 1)p^{n/2}$ so that

$$N_1 \geq p^n - (r - 1)(s - 1)p^{n/2}.$$ Let $N_1^f$ count the number of solutions with $xy \neq 0$ so that $N_1^f \geq N_1 - r - s$. Finally let $N$ count the number of pairs $(x^r, y^s)$ with $y^s - x^r - 1 = 0$ and $xy \neq 0$. Clearly $N \geq N_1^f/rs$ so

$$N \geq [p^n - (r - 1)(s - 1)p^{n/2} - (r + s)]/rs.$$ Note that $\mathbb{R} = \{x^r | x \in GF(p^n)^\#\}$ and $\mathbb{S} = \{y^s\}$ so that $N$ counts the number of $b \in \mathbb{R}$ with $b + 1 \in \mathbb{S}$.

Suppose we do not have $\mathbb{F}(p^n) < \mathbb{S} \leq \mathbb{F}(p^n)$. 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 \( b \in \mathfrak{R} \) with \( b + 1 \in \mathfrak{S} \), \( b \) is in the fixed field of \( \sigma \). Thus \( p^{n/2} > N \) and

\[
p^{n/2} > \frac{[p^n - (r - 1)(s - 1)p^{n/2} - (r + s)]}{rs}
\]
or

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

Let us consider \( n = 2 \) first. Clearly \( \mathfrak{S} = \mathfrak{S}_1 \) here since \( \mathfrak{S} \) does not act semiregularly. We have \( r = 2, 4 \) or \( 6 \). Suppose \( r = 6 \). Then clearly \( [T(p^n) : \mathfrak{S}] = 3 \) and hence by Lemma 2.3, \( \mathfrak{S} \not\subseteq \text{Alt}(GF(p^n) \cup \{\infty\}) \) but \( (\frac{x}{x}) \) is in the alternating group. Apply Lemma 1.3 to doubly transitive \( \mathfrak{G} \cap \text{Alt}(GF(p^n) \cup \{\infty\}) \). We obtain

\[
| \mathfrak{G} \cap \text{Alt}(GF(p^n) \cup \{\infty\}) | \geq (p^n - 1)/2
\]
so \( | \mathfrak{G} | \geq (p^n - 1) \). This contradicts the fact that \( | \mathfrak{G} | = 2(p^n - 1)/3 \). Thus \( r \neq 6 \).

Let \( r = 4 \). If \( p \equiv 1 \) modulo 4, then by Step 3 (ii), \( s = 1 \). Then equation (**) yields \( p < 5 \), a contradiction. Let \( p \equiv -1 \) modulo 4. Since \( r = 4 \) we see that \( \mathfrak{S} \subseteq \text{Alt}(GF(p^n) \cup \{\infty\}) \) but by Lemma 2.3 (ii) \( \mathfrak{S} \not\subseteq \text{Alt}(GF(p^n) \cup \{\infty\}) \). Applying Lemma 1.4 (ii) to doubly transitive \( \mathfrak{G} \cap \text{Alt}(GF(p^n) \cup \{\infty\}) \) 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 \( 9 > p^{n/2}[p^{n/2} - 28] \) or \( p^{n/2} \leq 28 \). Hence we have only \( p^n = 3^4, 5^4 \) and \( 3^6 \). Note that \( r \mid (p^n - 1) \) so that if \( p = 3 \) then \( r = 2 \) or \( 4 \). This eliminates \( p^n = 3^6 \) and by (***) we must have \( p^n = 3^4, r = 4 \) or \( p^n = 5^4, r = 6 \). If \( p^n = 3^4, r = 4 \), then Step 3 (ii) yields \( s = 1 \) and this contradicts (***). Finally let \( p^n = 5^4, r = 6 \). If \( a = 4\sqrt{2} \) in \( GF(5^4) \) then

\[
(2 + a + 4a^3) + 1 = a + 3a^2 + 2a^3 = (2 + 3a^2 + 2a^3)^3.
\]

Hence if \( b = 4 + a + 3a^2 + 2a^3 \) then \( b \in \mathfrak{R}, b + 1 \in \mathfrak{S} \) and \( b^c \neq b \). 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 \( \mathfrak{G} \) 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 \( \Gamma(p^n) \supseteq \mathfrak{G} > \Gamma(p^n) \) for some prime power \( p^n \).

**Proof.** The group \( \mathfrak{G}_s \) is a solvable 3/2-transitive group which is
not a Frobenius group. By the main theorem of [4] we have either $\mathcal{G}_\infty \leq S(p^n)$, $\mathcal{G}_\infty = S_r(p^n)$ with $p \neq 2$, or $\mathcal{G}_\infty$ is one of a finite number of exceptions. The result therefore follows from Propositions 2.4, 2.5, 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 $\mathcal{G}$, $O_3(\mathcal{G})$ is cyclic, then we would know (see [4]) that (1) if $p = 2$, then $\mathcal{G}_\infty \leq S(2^n)$, (2) if $p \neq 2$ and $|\mathcal{G}_\infty|$ is odd, then $\mathcal{G}_\infty \leq S(p^n)$, (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 $\mathcal{G} = \text{Sym}_6$. Let $n = 3$ and let $\infty, 0, 1$ be three points. Set $\mathcal{K} = \mathcal{G}_\infty$, $\mathcal{D} = \mathcal{G}_\infty$, $\mathcal{G} = \mathcal{G}_{\infty, 0, 1}$. Then $\mathcal{K}$ is 5/2-transitive and by Lemma 2.1, $\mathcal{K}$ has no regular normal subgroup. We know that $\mathcal{D}$ has a regular normal elementary abelian subgroup $\mathcal{B}$ so $\mathcal{D} = \mathcal{K}\mathcal{B}$. 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 $[\text{Sym}_6 : \mathcal{G}] < 6$. Hence $\mathcal{G} = \text{Alt}_6$ or $\text{Sym}_6$. If $\mathcal{G} = \text{Alt}_6$ then $\mathcal{D} = \text{Alt}_4$, a Frobenius group. Thus we have only $\mathcal{G} = \text{Sym}_6$ 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 \(|C_\mathfrak{H}(W)| \leq 2|\mathfrak{H}|\). If \(W\) acts trivially on \(\mathfrak{H}\), then \([\mathfrak{H}:\mathfrak{H}] = 2\) and since \(\mathfrak{H}\) is half-transitive, it must be an elementary abelian 2-group. This contradicts the fact that \(\mathfrak{H}\) acts irreducibly on \(B\). We have \(\mathfrak{H} \unlhd GL(2, 3)\) and \(W\) acts nontrivially on \(\mathfrak{H}\). Further \(\mathfrak{H}\) acts irreducibly so \(O_3(\mathfrak{H}) = \langle 1 \rangle\).

If \(3 \nmid |\mathfrak{H}|\), then \(\mathfrak{H}\) is a 2-group with a cyclic subgroup of index 2 which admits \(W\) nontrivially. Since \(\mathfrak{H}\) acts irreducibly we conclude that \(\mathfrak{H}\) is the quaternion group of order 8. Then \(\mathfrak{Q}\) is a Frobenius group, a contradiction. Hence \(3 \mid |\mathfrak{H}|\) so since \(O_3(\mathfrak{H}) = \langle 1 \rangle\) we have \(\mathfrak{H} = SL(2, 3)\) or \(GL(2, 3)\). Let \(\mathfrak{O} = O_4(\mathfrak{H})\). Then \(\mathfrak{O}\) is the quaternion group of order 8. It acts regularly on 8 points and fixes 3. Now \(\mathfrak{O}\), a Sylow 3-subgroup of \(\langle \mathfrak{H}, W \rangle\) is abelian of type \((3, 3)\) and acts on \(\mathfrak{O}\). Hence there exists \(S \in \mathfrak{O}\) with \(S\) centralizing \(\mathfrak{O}\). From the way \(\mathfrak{O}\) acts as a permutation group it is clear that \(S\) is a 3-cycle, in fact \(S = (0 \ 1 \ 2)\) or \((0 \ 1 \ 3)\). Since \(\mathfrak{Q}\) is triply transitive it contains all 3-cycles so \(\mathfrak{G} \unlhd Alt_4\). Thus \(\mathfrak{D} \unlhd Alt_3\) and this contradicts the solvability of \(\mathfrak{D}\). 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
Patrick Robert Ahern, On the geometry of the unit ball in the space of real annihilating measures .......................................................... 1
Kirby Alan Baker, Equational classes of modular lattices ......................... 9
E. F. Beckenbach and Gerald Andrew Hutchison, Meromorphic minimal surfaces .......................................................................................... 17
Tae Ho Choe, Intrinsic topologies in a topological lattice .......................... 49
John Bligh Conway, A theorem on sequential convergence of measures and some applications ................................................................. 53
Roger Cuppens, On the decomposition of infinitely divisible probability laws without normal factor ............................................................ 61
Lynn Harry Erbe, Nonoscillatory solutions of second order nonlinear differential equations ............................................................................ 77
Burton I. Fein, The Schur index for projective representations of finite groups ................................................................................................. 87
Stanley P. Gudder, A note on proposition observables ................................ 101
Kenneth Kapp, On Croisot's theory of decompositions ............................... 105
Robert P. Kaufman, Gap series and an example to Malliavin's theorem ....... 117
E. J. McShane, Robert Breckenridge Warfield, Jr. and V. M. Warfield, Invariant extensions of linear functionals, with applications to measures and stochastic processes ........................................... 121
Marvin Victor Mielke, Rearrangement of spherical modifications .............. 143
Akio Osada, On unicity of capacity functions ............................................. 151
Donald Steven Passman, Some 5/2 transitive permutation groups ............... 157
Harold L. Peterson, Jr., Regular and irregular measures on groups and dyadic spaces ..................................................................................... 173
Habib Salehi, On interpolation of q-variate stationary stochastic processes ........................................................................................................ 183
Michael Samuel Skaff, Vector valued Orlicz spaces generalized N-functions. I ................................................................................................. 193
A. J. Ward, On H-equivalence of uniformities. II ........................................ 207
Thomas Paul Whaley, Algebras satisfying the descending chain condition for subalgebras ........................................................................... 217
G. K. White, On subgroups of fixed index .................................................. 225
Martin Michael Zuckerman, A unifying condition for implications among the axioms of choice for finite sets ................................................. 233