Pacific Journal of Mathematics

SOME 5/2 TRANSITIVE PERMUTATION GROUPS

DONALD STEVEN PASSMAN

Vol. 28, No. 1 March 1969

PACIFIC JOURNAL OF MATHEMATICS
Vol. 28, No. 1, 1969

SOME 5/2 TRANSITIVE PERMUTATION GROUPS

D. S. PASSMAN

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

$$x \longrightarrow \frac{ax^\sigma + b}{cx^\sigma + d}$$

where $a, b, c, d \in GF(p^n)$, $ad - bc \neq 0$ and σ 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

$$x \longrightarrow \frac{ax + b}{cx + d}$$

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 $\Gamma(p^n) \supseteqq \mathfrak{G} > \bar{\Gamma}(p^n)$. 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 $\mathfrak{G}_{\infty 0} \triangle \Gamma(p^n)_{\infty 0}$. Since a nonidentity normal subgroup of a transitive group is half-transitive we see that $\mathfrak{G}_{\infty 0}$ is half-transitive on $GF(p^n)^\#$ and hence $\mathfrak{G}$ is 5/2-transitive. It is an easy matter to decide which group $\mathfrak{G}$ with $\Gamma(p^n) \supseteqq \mathfrak{G} > \bar{\Gamma}(p^n)$ 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, $\Gamma(p^n) \supseteqq \mathfrak{G} > \bar{\Gamma}(p^n)$ 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 $S_0(p^n)$. 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:

$\mathfrak{G}$ is a doubly transitive permutation group of degree $1 + m$

∞ and 0 are two points

$\mathfrak{D} = \mathfrak{G}_\infty, \qquad \mathfrak{H} = \mathfrak{G}_{\infty 0} = \mathfrak{D}_0$

$T \in \mathfrak{G}$ is an involution with $T = (0\ \infty) \cdots$.

The above implies that T normalizes $\mathfrak{H}$ and $\mathfrak{H} = \mathfrak{D} \cap \mathfrak{D}^T$.

In the following we use the usual character theory notation.

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

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

(ii) *$\alpha^* = \chi_1 + \chi_2$ where χ_1 and χ_2 are distinct irreducible nonprincipal characters of $\mathfrak{G}$.*

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

$$A^{E^{-1}} = B^{DT} \in \mathfrak{D} \cap \mathfrak{D}^T = \mathfrak{H}$$

so by assumption $\alpha(B^{DT}) = \alpha(B^D)$. Thus $\alpha(A) = \alpha(A^{E^{-1}}) = \alpha(B^{DT}) = \alpha(B^D) = \alpha(B)$ and this fact follows.

Let $D \in \mathfrak{D}$. Then by definition and the above we have

$$\begin{aligned}\alpha^*(D) &= |\mathfrak{D}|^{-1}\Sigma_{G \in \mathfrak{G}}\alpha_0(D^G)\\ &= \alpha(D)\,|\mathfrak{D}|^{-1}\Sigma_{G \in \mathfrak{G}}1_{\mathfrak{D}_0}(D^G) = \alpha(D)1_{\mathfrak{D}}^*(D)\end{aligned}$$

and (i) follows.

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

$$\begin{aligned}[\alpha^*, \alpha^*]_{\mathfrak{G}} &= [\alpha, \alpha^* \mid \mathfrak{D}]_{\mathfrak{D}} = [\alpha, \alpha(1_{\mathfrak{D}}^* \mid \mathfrak{D})]_{\mathfrak{D}}\\ &= [\bar{\alpha}\alpha, 1_{\mathfrak{D}}^* \mid \mathfrak{D}]_{\mathfrak{D}} = [1_{\mathfrak{D}}, 1_{\mathfrak{D}}^* \mid \mathfrak{D}]_{\mathfrak{D}}\\ &= [1_{\mathfrak{D}}^*, 1_{\mathfrak{D}}^*]_{\mathfrak{G}} = 2\,.\end{aligned}$$

Thus we must have $\alpha^* = \chi_1 + \chi_2$ with χ_1 and χ_2 distinct irreducible characters of $\mathfrak{G}$. Now $[\alpha^*, 1_{\mathfrak{G}}]_{\mathfrak{G}} = [\alpha, 1_{\mathfrak{G}} \mid \mathfrak{D}]_{\mathfrak{D}} = [\alpha, 1_{\mathfrak{D}}]_{\mathfrak{D}} = 0$ and hence both χ_1 and χ_2 are nonprincipal. This proves (ii).

LEMMA 1.2. *Let* $\mathfrak{T} \triangle \mathfrak{D}$ *with* $\mathfrak{D}/\mathfrak{T}$ *cyclic. Suppose that* $\mathfrak{T}$ *contains all elements* $D \in \mathfrak{D}$ *satisfying either* $D^2 = 1$ *or* $D^T = D^{-1}$. *Suppose further that* m *is a prime power and* T *fixes precisely zero or two points. Then there exists* $\mathfrak{K} \triangle \mathfrak{G}$ *with* $\mathfrak{K} \cap \mathfrak{D} = \mathfrak{T}$.

Proof. The result is trivial if $\mathfrak{T} = \mathfrak{D}$ so we can assume that $\mathfrak{T} \neq \mathfrak{D}$. Let α be a faithful linear character of $\mathfrak{D}/\mathfrak{T}$ viewed as one of of $\mathfrak{D}$. Then $\alpha \neq 1_{\mathfrak{D}}$. If $H \in \mathfrak{H}$ then $D = H^T H^{-1}$ satisfies $D^T = D^{-1}$ so $D \in \mathfrak{T}$. Hence $\alpha(H^T H^{-1}) = 1$ and the hypothesis of Lemma 1.1 holds. Thus we have $\alpha^* = \chi_1 + \chi_2$. Further, as is well known, $1_{\mathfrak{D}}^* = 1_{\mathfrak{G}} + \xi$ where ξ is an irreducible nonprincipal character. We will prove that either χ_1 or χ_2 is linear. Suppose say χ_1 is linear. Then $1 = [\alpha^*, \chi_1]_{\mathfrak{G}} = [\alpha, \chi_1 \mid \mathfrak{D}]_{\mathfrak{D}}$ implies that $\chi_1 \mid \mathfrak{D} = \alpha$. If $\mathfrak{K}$ is the kernel of χ_1, then $\mathfrak{K} \triangle \mathfrak{G}$ and $\mathfrak{K} \cap \mathfrak{D} = \mathfrak{T}$, the kernel of α. If either χ_1 or χ_2 is ξ then since $\deg 1_{\mathfrak{D}}^* = \deg \alpha^* = m + 1$ and $\deg \xi = m$ we would have some χ_i linear and the result would follow. Thus we can assume that $1_{\mathfrak{G}}$, ξ, χ_1 and χ_2 are all distinct.

Let $\beta = \alpha - 1_{\mathfrak{D}}$. We show now that β^* 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 $\mathfrak{D}$ and hence that $G \in \mathfrak{D}$. If $G \in \mathfrak{T}$ then by Lemma 2.1 (i), $\alpha^*(G) = \alpha(G) 1_{\mathfrak{D}}^*(G) = 1_{\mathfrak{D}}^*(G)$ and $\beta^*(G) = 0$. Thus it suffices to show that $G \in \mathfrak{T}$. Suppose first that $T_2 \in \mathfrak{D}$. Then also $T_1 \in \mathfrak{D}$ and since T_1 and T_2 are involutions, we have by assumption $T_1, T_2 \in \mathfrak{T}$ so $G = T_1 T_2 \in \mathfrak{T}$. Now we suppose that $T_2 \notin \mathfrak{D}$. From $\mathfrak{G} = \mathfrak{D} \cup \mathfrak{D} T \mathfrak{D}$ we see that a suitable $\mathfrak{D}$ conjugate of T_2 is of the form TD with $D \in \mathfrak{D}$. By taking conjugates again we can assume that $G = WTD$ with $G, D \in \mathfrak{D}$ and W and TD involutions. Since $(TD)^2 = 1$ we have $D^T = D^{-1}$. Also $E = WT \in \mathfrak{D}$ and since T and W are involutions $E^T = E^{-1}$. Hence $E, D \in \mathfrak{T}$ so $G = ED \in \mathfrak{T}$ and this fact follows.

Let class function γ of $\mathfrak{G}$ 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, $\gamma(G) = |\mathfrak{G}|^{-1} |T^{\mathfrak{G}}|^2 \Sigma \bar{\chi}(T)^2 \chi(G)/\chi(1)$ where the sum runs over all irreducible characters of $\mathfrak{G}$. By the remarks of the preceding paragraph $[\beta^*, \gamma]_{\mathfrak{G}} = 0$. Hence since $1_{\mathfrak{G}}, \chi_1, \chi_2$ and ξ are distinct and $\beta^* = \chi_1 + \chi_2 - 1_{\mathfrak{G}} - \xi$ we have

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

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

$$\chi_2(1)\chi_1(T)^2 + \chi_1(1)\chi_2(T)^2 = \chi_1(1)\chi_2(1)(m + 1)/m .$$

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 $\chi_2(1) \geqq m$. From $\chi_1(1) + \chi_2(1) = m + 1$ we conclude that $\chi_2(1) = m$ and $\chi_1(1) = 1$. Since χ_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 $|\mathfrak{H}| \geqq (m-1)/2$. If in addition $\mathfrak{G}$ contains an involution fixing more than two points, then $|\mathfrak{H}| > (m-1)/2$.*

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

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

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

$$|\mathfrak{G}| \geqq [\mathfrak{G} : C_{\mathfrak{G}}(T)](m-1) .$$

Note here that if $\mathfrak{G}$ 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 $|C_{\mathfrak{G}}(T)| \geqq (m-1)$ and $C_{\mathfrak{G}}(T)$ permutes the set of points $\{x, y\}$ fixed by T. Hence since $[C_{\mathfrak{G}}(T) \colon \mathfrak{G}_{xy} \cap C_{\mathfrak{G}}(T)] \leqq 2$ we have $|\mathfrak{G}_{xy}| \geqq (m-1)/2$ with strict inequality if involution H exists. Since $\mathfrak{H}$ and $\mathfrak{G}_{xy}$ are conjugate, the result follows.

LEMMA 1.4. *Suppose $\mathfrak{D} = \mathfrak{H}\mathfrak{V}$ where $\mathfrak{V}$ is a regular normal abelian subgroup of $\mathfrak{D}$. We identity the set of points being permuted with $\mathfrak{V} \cup \{\infty\}$ and use additive notation in $\mathfrak{V}$. Then every element of $\mathfrak{D}$ can be written as $D = \begin{pmatrix} x \\ \alpha(x) + b \end{pmatrix}$ with $\begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathfrak{H}$ and $b \in \mathfrak{V}$. 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) $\mathfrak{G} = \mathfrak{D} \cup \mathfrak{D}T\mathfrak{V} = \mathfrak{D} \cup \mathfrak{V}T\mathfrak{D}$.

(ii) *For each $a \in \mathfrak{V}^{\#}$, there exists a unique $\begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathfrak{H}$ with*

$$f(f(x) + a) = f(a(x) - a) + f(a) .$$

(iii) *Let α be a subgroup of $\mathfrak{H}$ normalized by T and containing* *all the* $\begin{pmatrix} x \\ \alpha(x) \end{pmatrix}$ *elements which occur above. Then* $\bar{\mathfrak{G}} = \langle \bar{\mathfrak{H}}, \mathfrak{B}, T \rangle$ *is doubly transitive with* $\bar{\mathfrak{G}}_{\infty 0} = \bar{\mathfrak{H}}$.

(iv) *If* $\begin{pmatrix} x \\ -x \end{pmatrix} \in \mathfrak{H}$ *then* T *acts on the orbits of* $\mathfrak{H}$ *on* $\mathfrak{B}$.

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

Let $V \in \mathfrak{B}^{\#}$ be the permutation $V = \begin{pmatrix} x \\ x + a \end{pmatrix}$. Then $TVT \in \mathfrak{G}$ and $(\infty)TVT = (a)T \neq \infty$. Thus $TVT \in \mathfrak{D}T\mathfrak{B}$ and hence

$$\begin{pmatrix} x \\ f(x) \end{pmatrix}\begin{pmatrix} x \\ x + a \end{pmatrix}\begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} x \\ \alpha(x) + b \end{pmatrix}\begin{pmatrix} x \\ f(x) \end{pmatrix}\begin{pmatrix} x \\ x + c \end{pmatrix} .$$

This is equivalent to

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

Note that $\begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathfrak{H}$ 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 $\begin{pmatrix} x \\ -x \end{pmatrix}$ so $f(-x) = -f(x)$ and $b = -f^2(a) = -a$. Since $\begin{pmatrix} x \\ \alpha(x) \end{pmatrix} \in \mathfrak{H}$ is now clearly unique, we have (ii).

By definition of $\bar{\mathfrak{H}}$ we have $T\mathfrak{B}^{\#}T \subseteq \bar{\mathfrak{H}}\mathfrak{B}T\mathfrak{B}$ and since T normalizes $\bar{\mathfrak{H}}$, $\bar{\mathfrak{G}} = \bar{\mathfrak{H}}\mathfrak{B} \cup \bar{\mathfrak{H}}\mathfrak{B}T\mathfrak{B}$ is a group. Since $\bar{\mathfrak{G}} \supseteq \langle \mathfrak{B}, T \rangle$, $\bar{\mathfrak{G}}$ 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 $\begin{pmatrix} x \\ -\alpha(x) \end{pmatrix} \in \mathfrak{H}$, a and $f(a)$ are in the same orbit of $\mathfrak{H}$. 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

∞ and 0 are two points

$\mathfrak{D} = \mathfrak{G}_\infty$, $\mathfrak{H} = \mathfrak{G}_{\infty 0} = \mathfrak{D}_0$, $\mathfrak{D}$ 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 $\mathfrak{D} = \mathfrak{H}\mathfrak{B}$ and m is a power of p.

LEMMA 2.1. *Let $\mathfrak{K} \triangle \mathfrak{G}$ with $\mathfrak{K} \neq \langle 1 \rangle$. Then $\mathfrak{K}$ 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 $\mathfrak{L}$ is such a group. Since $\mathfrak{G}$ is doubly transitive $\mathfrak{L}$ is a elementary abelian q-group for some prime q. Then $\mathfrak{B}\mathfrak{L}$ 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 $\mathfrak{K} \triangle \mathfrak{G}$ with $\mathfrak{K} \neq \langle 1 \rangle$. Since $\mathfrak{K}$ cannot be regular and $\mathfrak{G}$ is doubly primitive, it follows that $\mathfrak{K}$ is doubly transitive. If $\mathfrak{L}$ is a regular normal subgroup of $\mathfrak{K}$, then $\mathfrak{L}$ is abelian. This implies easily that $\mathfrak{L}$ is the unique minimal normal subgroup of $\mathfrak{K}$ so $\mathfrak{L} \triangle \mathfrak{G}$, a contradiction.

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

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

(i) *Each $\mathfrak{H}_v$ is cyclic of order k and $k \mid n$.*

(ii) *$\tilde{\mathfrak{H}} \supseteq \{ax \mid a = b^{1-\sigma},\ b \in GF(p^n)^{\#}\}$ where σ is a field automorphism of order k.*

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

(iv) *$\tilde{\mathfrak{H}}$ is characteristic and self centralizing in $\mathfrak{H}$.*

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

(i) *If a generates the multiplicative group $GF(p^n)^{\#}$, then $\begin{pmatrix} x \\ ax \end{pmatrix} \notin \mathrm{Alt}\,(GF(p^n))$.*

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

(iii) *If n is even, then $\begin{pmatrix} x \\ -x \end{pmatrix} \in \mathrm{Alt}\,(GF(p^n))$.*

Proof. The group generated by $\begin{pmatrix} x \\ ax \end{pmatrix}$ acts regularly on $GF(p^n)^{\#}$ and hence $\begin{pmatrix} x \\ ax \end{pmatrix}$ is a $(p^n - 1)$-cycle. Since $p > 2$, $p^n - 1$ is even and hence $\begin{pmatrix} x \\ ax \end{pmatrix}$ is an odd permutation. This also yields the contention that $T(p^n) \not\subseteq \mathrm{Alt}\,(GF(p^n))$.

(ii) Let q be an integer and suppose that for some $r \geqq 1$, $q^{2^{r-1}} \equiv \pm 1 \bmod 2^{r+1}$. Then $q^{2^{r-1}} = \pm 1 + \lambda 2^{r+1}$

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

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

Let $n = 2^r s$ with s odd. We can write $\sigma = \tau\rho$ where τ has order 2^r and ρ has order s. Clearly $\begin{pmatrix} x \\ x^\sigma \end{pmatrix} \in \mathrm{Alt}\,(GF(p^n))$ if and only if $\begin{pmatrix} x \\ x^\tau \end{pmatrix} \in \mathrm{Alt}\,(GF(p^n))$. It is easy to see that if $q = p^s$, then $\begin{pmatrix} x \\ x^\tau \end{pmatrix}$ has $(q^{2^i} - q^{2^{i-1}})/2^i$ cycles of length 2^i for $i = 1, 2, \cdots, r$. These cycles are all odd permutations so $\begin{pmatrix} x \\ x^\tau \end{pmatrix}$ has the parity of $\Sigma_1^r(q^{2^i} - q^{2^{i-1}})/2^i$. Now q is odd and

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

By the above, if $i > 1$ then $2^{i+1} \mid (q^{2^{i-1}} - 1)$ and hence $\begin{pmatrix} x \\ x^\tau \end{pmatrix}$ has the parity of $q(q-1)/2$. If $q \equiv 1 \bmod 4$ then this is even and if $q \equiv -1 \bmod 4$ then this term is odd. Finally since s is odd and $q = p^s$ we see that $q \equiv p \bmod 4$ and (ii) follows.

(iii) $\begin{pmatrix} x \\ -x \end{pmatrix}$ is a product of $(p^n - 1)/2$ transpositions. If n is even, then $4 \mid (p^n - 1)$ and the result follows.

We will consider these transitive extensions in four separate cases.

PROPOSITION 2.4. If $\mathfrak{D} = S_0(p^n)$, then $p^n = 3$ and $\bar{\Gamma}(3^2) < \mathfrak{G} < \Gamma(3^2)$.

Proof. Since $\mathfrak{D}$ is 3/2-transitive we have $p \neq 2$. Let G be the central involution of $\mathfrak{H} = T_0(p^n)$ and let H be another involution. Then G fixes precisely two points and H fixes $p^n + 1 > 2$ points. Since the degree of $\mathfrak{G}$ is $1 + p^{2n}$, Lemma 1.3 yields

$$4(p^n - 1) = |\, T_0(p^n) \,| = |\, \mathfrak{H} \,| > (p^{2n} - 1)/2$$

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

Since $\mathfrak{G}$ is doubly transitive we can find T conjugate to G with $T = (0\ \infty) \cdots$. Then T normalizes $\mathfrak{H}$ and centralizes its unique central involution $G = \begin{pmatrix} x \\ -x \end{pmatrix}$. By Lemma 1.4 (iv), T acts on each orbit of $\mathfrak{H}$ on $\mathfrak{V}^\#$. Now if $v \in \mathfrak{V}^\#$, then $|\, \mathfrak{H}_v \,| = 2$. This implies easily that if H is a noncentral involution of $\mathfrak{H}$, then H^T is conjugate to H in $\mathfrak{H}$. Let $p^n = 5$. Then $\mathfrak{H}$ is easily seen to be generated by its noncentral involutions so $\mathfrak{H}^{1-T} \subseteqq \mathfrak{H}'$. Thus $[\mathfrak{H} : \boldsymbol{C}_{\mathfrak{H}}(T)] = |\, \mathfrak{H}^{1-T} \,| \leqq |\, \mathfrak{H}' \,| = 2$ and $|\, \boldsymbol{C}_{\mathfrak{H}}(T) \,| \geqq 8$. On the other hand $\boldsymbol{C}_{\mathfrak{H}}(T)$ acts on the fixed points of T namely $\{a, b\}$, so $[C_{\mathfrak{H}}(T) : C_{\mathfrak{H}}(T) \cap \mathfrak{H}_a] \leqq 2$. Since $|\mathfrak{H}_a| = 2$, this is a contradiction.

Finally let $p^n = 3$. Here $T_0(3)$ is a dihedral group of order 8 and $S_0(3) \subseteqq S(3^2)$. This case is then included in Proposition 2.7 and we obtain $\bar{\Gamma}(3^2) < \mathfrak{G} \subseteqq \Gamma(3^2)$. By order considerations $\mathfrak{G} \neq \Gamma(3^2)$ so this results follows.

PROPOSITION 2.5. If $\mathfrak{D} \subseteqq S(2^n)$ then $\bar{\Gamma}(2^n) < \mathfrak{G} \subseteqq \Gamma(2^n)$.

Proof. Let 1 be a point. Then $\mathfrak{G}_1$ 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 $\mathfrak{H}$. If $H \in C_{\mathfrak{H}}(T)$, then $1H = (1T)H = (1H)T$ so T fixes $1H$ and hence $H \subseteqq \mathfrak{H}_1$. In particular in the notation of Lemma 2.2, $C_{\tilde{\mathfrak{H}}}(T) = \langle 1 \rangle$. Then $\tilde{\mathfrak{H}}^{1-T} = \tilde{\mathfrak{H}}$. Since $\mathfrak{H}/\tilde{\mathfrak{H}}$ is abelian, $(\mathfrak{H}/\tilde{\mathfrak{H}})^{1-T}$ is a group and hence $\mathfrak{H}^{1-T}$ is a group containing $\tilde{\mathfrak{H}}$. If $H \in \mathfrak{H}^{1-T}$, then $H^T = H^{-1}$ so $\mathfrak{H}^{1-T}$ is abelian. By Lemma 2.2 (iv), $\mathfrak{H}^{1-T} = \tilde{\mathfrak{H}}$. Now $|\mathfrak{H}^{1-T}|\,|C_{\mathfrak{H}}(T)| = |\mathfrak{H}|$, $|\tilde{\mathfrak{H}}|\,|\mathfrak{H}_1| \leqq |\mathfrak{H}|$ and $C_{\mathfrak{H}}(T) \subseteqq \mathfrak{H}_1$. This yields $C_{\mathfrak{H}}(T) = \mathfrak{H}_1$ and $\mathfrak{H} = \tilde{\mathfrak{H}}\mathfrak{H}_1$. The latter shows that each orbit of $\mathfrak{H}$ on $GF(2)^\#$ has size $|\tilde{\mathfrak{H}}|$, an odd number.

In characteristic 2 the permutation $\begin{pmatrix} x \\ -x \end{pmatrix}$ is trivial so by Lemma 1.4 (iv) T acts on each orbit of $\mathfrak{H}$ 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 $\mathfrak{H}$ is transitive. This yields

$$\mathfrak{H}^{1-T} = \tilde{\mathfrak{H}} = \{bx \mid b \in GF(2^n)^\#\}\ .$$

If $H = \begin{pmatrix} x \\ bx \end{pmatrix}$, then $H^T = H^{-1}$ so

$$\begin{pmatrix} x \\ f(x) \end{pmatrix}\begin{pmatrix} x \\ b^{-1}x \end{pmatrix} = \begin{pmatrix} x \\ bx \end{pmatrix}\begin{pmatrix} x \\ f(x) \end{pmatrix}$$

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 $\mathfrak{G} = \mathfrak{D} \cup \mathfrak{D}T\mathfrak{B}$, the result follows easily.

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

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

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

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

By Lemma 2.1, $\mathfrak{R}$ is doubly transitive and has no regular normal subgroup. Furthermore $\mathfrak{R}_\infty = \mathfrak{T} = \tilde{\mathfrak{H}}\mathfrak{V}$ and $\mathfrak{V}$ is abelian. Thus $\mathfrak{R}$ is a Zassenhaus group and the result of Feit ([2]) implies that T is a permutation of the form $\binom{x}{-a/x}$ and $|\tilde{\mathfrak{H}}| = (p^n - 1)/2$. Since $\mathfrak{G} = \mathfrak{D} \cup \mathfrak{D}T\mathfrak{V}$, the result follows easily.

PROPOSITION 2.7. If $\mathfrak{D} \subseteqq S(p^n)$ with $p \neq 2$ and $|\mathfrak{D}|$ is even, then $\bar{\Gamma}(p^n) < \mathfrak{G} \subseteqq \Gamma(p^n)$.

Proof. We proceed in a series of steps.

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

(i) $\tilde{\mathfrak{H}} = \mathfrak{H}^{1-T}$ and $[\mathfrak{H} : \tilde{\mathfrak{H}}\mathfrak{H}_1] = 2$ or

(ii) $[\tilde{\mathfrak{H}} : \mathfrak{H}^{1-T}] = 2$ and $\mathfrak{H} = \mathfrak{H}\tilde{\mathfrak{H}}_1$.

In either case $[\mathfrak{H} : \mathfrak{H}_1] = 2\,|\mathfrak{H}^{1-T}|$.

Now by assumption $2 \mid |\mathfrak{D}|$ so since $p \neq 2$, $2 \mid |\mathfrak{H}|$. If $2 \mid |\tilde{\mathfrak{H}}|$, then certainly $\mathfrak{H}$ has a central element of order 2. This is of course the permutation $\binom{x}{-x}$ which fixes precisely two points. Suppose $2 \nmid |\tilde{\mathfrak{H}}|$ and let $H \in \mathfrak{H}$ have order 2. Since $H \neq \binom{x}{-x}$, H must have a fixed point on $\mathfrak{V}^\#$. Hence $2 \mid |\mathfrak{H}_v|$. If ρ is a field automorphism of order 2, then by Lemma 2.2, $\tilde{\mathfrak{H}} \supseteqq \{b^{1-\rho}x \mid b \in GF(p^n)^\#\}$. 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 $\mathfrak{G}$ is doubly transitive we can choose T conjugate to $\binom{x}{-x}$

with $T = (0\ \infty)\cdots$. Then T fixes precisely two points and T normalizes $\mathfrak{H}$. We can clearly write the latter group in such a way that T fixes point 1. Clearly T centralizes $\begin{pmatrix} x \\ -x \end{pmatrix} \in \mathfrak{H}$ so if $T = \begin{pmatrix} x \\ f(x) \end{pmatrix}$, then $f(-x) = -f(x)$. This shows that T also fixes -1 so $T = (0\ \infty)(1)(-1)\cdots$.

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

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

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

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

$$(*) \qquad f(f(x) + a) = f(a'x^\sigma - a) + f(a)$$

where $\begin{pmatrix} x \\ a'x^\sigma \end{pmatrix} \in \mathfrak{H}$ and $a' = -a/f(a)^\sigma$. Let $\mathfrak{g}$ denote the set of all field automorphisms σ which occur in the above. If $\mathfrak{g} = \{1\}$, then

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

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

Let $\mathfrak{M} = \left\{b \in GF(p^n)^\# \,\middle|\, \begin{pmatrix} x \\ bx \end{pmatrix} \in \mathfrak{L}\right\}$. Thus $\mathfrak{M}$ is a subgroup of $GF(p^n)^\#$ of index 1 or 2 and in particular $\mathfrak{M}$ contains all the nonzero squares in $GF(p^n)$. Note that for all $b \in \mathfrak{M}$, $f(bx) = b^{-1}f(x)$ and at $x = 1$ this yields $f(b) = b^{-1}$.

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

$$\begin{aligned} f(1 + a) &= f(-a^2 - a) + f(a) \\ &= -a^{-1}f(1 + a) + a^{-1} . \end{aligned}$$

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

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

Since $\mathfrak{M}$ 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 $\mathfrak{G} = \mathfrak{D} \cup \mathfrak{D}T\mathfrak{B}$ and $|\tilde{\mathfrak{H}}| \geqq (p^n - 1)/2$ the result follows here.

Step 3. Let $\mathfrak{N} = \left\{b \in GF(p^n)^\# \,\middle|\, \begin{pmatrix} x \\ bx \end{pmatrix} \in \mathfrak{H}^{1-T}\right\}$. Let $\sigma \in \mathfrak{g} - \{1\}$. Then $\sigma^2 = 1$ so n is even. Set $\mathfrak{S} = \{b \in GF(p^n)^\# \mid b^{\sigma-1} \in \mathfrak{N}\}$. If $b \in \mathfrak{N}$ and $b + 1 \in \mathfrak{S}$, then $b^\sigma = b$. Furthermore, if $r = [GF(p^n)^\# : \mathfrak{N}]$ and $s = [GF(p^n)^\# : \mathfrak{S}]$ then we have

(i) $r = 2, 4$ or 6.

(ii) $s = r/(\text{g. c. d}\{r, p^{n/2} - 1\}) \leqq r/2$.

Define $\mathfrak{T} \triangle \mathfrak{D}$ as follows. If $\mathfrak{H}/\tilde{\mathfrak{H}}$ has odd order, set $\mathfrak{T} = \tilde{\mathfrak{H}}\mathfrak{B}$. If $\mathfrak{H}/\tilde{\mathfrak{H}}$ has even order and $\mathfrak{W}/\tilde{\mathfrak{H}}$ is its subgroup of order 2, set $\mathfrak{T} = \mathfrak{W}\mathfrak{B}$. By Step 1 it follows that the hypotheses of Lemma 1.2 are satisfied here. Thus there exists $\mathfrak{K} \triangle \mathfrak{G}$ with $\mathfrak{K} \cap \mathfrak{D} = \mathfrak{T}$. Since $\begin{pmatrix} x \\ -x \end{pmatrix} \in \mathfrak{K}$ and T is conjugate to $\begin{pmatrix} x \\ -x \end{pmatrix}$ in $\mathfrak{G}$, it follows that $T \in \mathfrak{K}$. Thus $\mathfrak{K}$ is doubly transitive with $\mathfrak{K}_\infty = \mathfrak{T}$ and $\tilde{\mathfrak{K}}_{\infty 0} = \mathfrak{H}$ or $\mathfrak{W}$. Applying the uniqueness part of Lemma 1.4 (ii) to both $\mathfrak{K}$ and $\mathfrak{G}$ we conclude that in equation (*), $\begin{pmatrix} x \\ a'x^\sigma \end{pmatrix} \in \tilde{\mathfrak{H}}$ or $\mathfrak{W}$. Hence if $\sigma \neq 1$ then $\sigma^2 = 1$ and n is even.

We now find r and s. By Step 1, $2\,|\mathfrak{H}^{1-T}| = [\mathfrak{H} : \mathfrak{H}_1]$. Since $\mathfrak{H}$ is half-transitive $[\mathfrak{H} : \mathfrak{H}_1] \mid |GF(p^n)^\#|$ so r is even. Set $\mathfrak{L} = \mathfrak{K}_{\infty 0}$. By Step 1 and the definition of $\mathfrak{K}$ we have one of the following three possibilities: (1) $\mathfrak{L} = \tilde{\mathfrak{H}}$, $[\tilde{\mathfrak{H}} : \mathfrak{H}^{1-T}] = 2$; (2) $\mathfrak{L} = \tilde{\mathfrak{H}}\mathfrak{L}_1$, $|\mathfrak{L}_1| = 2$, $[\tilde{\mathfrak{H}} : \mathfrak{H}^{1-T}] = 2$; (3) $[\mathfrak{L} : \tilde{\mathfrak{H}}] = 2$, $\tilde{\mathfrak{H}} = \mathfrak{H}^{1-T}$. We apply Lemma 1.3 to $\mathfrak{K}$ since $T \in \mathfrak{K}$. In cases (1) and (3) above we have $|\mathfrak{L}| \geqq (p^n - 1)/2$ so $|\mathfrak{H}^{1-T}| \geqq (p^n - 1)/4$. In case (2) since $|\mathfrak{L}_1| = 2$ we have $|\mathfrak{L}| > (p^n - 1)/2$ and $|\mathfrak{H}^{1-T}| > (p^n - 1)/8$. Hence either $r \leqq 4$ or $r < 8$. Since r is even we have $r = 2, 4$ or 6.

Now σ acts on the cyclic quotient $GF(p^n)^\#/\mathfrak{N}$ like $x \to x^{p^{n/2}}$ since σ has order 2. Thus $|\mathfrak{S}/\mathfrak{N}| = \text{g.c.d.}\{r, p^{n/2} - 1\} \geqq 2$ since r is even.

Hence we have (i) and (ii).

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

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

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

$$\begin{aligned} f(b^{-\sigma}(b^{\sigma} + 1)a) &= b^{\sigma}f((b^{\sigma} + 1)a) \\ &= b^{\sigma}f([(b^{\sigma} + 1)/(b + 1)](b + 1)a) \\ &= [b^{\sigma}(b + 1)/(b^{\sigma} + 1)]f((b + 1)a) \,. \end{aligned}$$

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

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

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

$$N_1 \geqq p^n - (r - 1)(s - 1)p^{n/2} \,.$$

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

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

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

Suppose we do not have $\bar{\Gamma}(p^n) < \mathfrak{G} \subseteqq \Gamma(p^n)$. Then by Step 2, $\mathfrak{g} \neq \{1\}$. Let $\sigma \in \mathfrak{g}$ 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 σ. Thus $p^{n/2} > N$ and

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

or

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

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

$$|\, \mathfrak{H} \cap \mathrm{Alt}\,(GF(p^n) \cup \{\infty\}) \,| \geqq (p^n - 1)/2$$

so $|\, \mathfrak{H} \,| \geqq (p^n - 1)$. This contradicts the fact that $|\, \mathfrak{H} \,| = 2(p^n - 1)/3$. 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 $\tilde{\mathfrak{H}} \subseteq \mathrm{Alt}\,(GF(p^n) \cup \{\infty\})$ but by Lemma 2.3 (ii) $\mathfrak{H}_1 \not\subseteq \mathrm{Alt}\,(GF(p^n) \cup \{\infty\})$. Applying Lemma 1.4 (ii) to doubly transitive $\mathfrak{G} \cap \mathrm{Alt}\,(GF(p^n) \cup \{\infty\})$ yields $\mathfrak{g} = \{1\}$, a contradiction. Finally if $r = 2$, then $s = 1$ and $(**)$ yields no exceptions.

Now let $n > 2$ so n is even and $n \geqq 4$. Since $r \leqq 6$, $s \leqq 3$ equation $(**)$ becomes $9 > p^{n/2}[p^{n/2} - 28]$ or $p^{n/2} \leqq 28$. 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

$$(2 + a + 4a^3)^6 + 1 = a + 3a^2 + 2a^3 = (2 + 3a^2 + 2a^3)^3 \, .$$

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

Proof. The group $\mathfrak{G}_\infty$ is a solvable 3/2-transitive group which is not a Frobenius group. By the main theorem of [4] we have either $\mathfrak{G}_\infty \subseteqq S(p^n)$, $\mathfrak{G}_\infty = S_0(p^n)$ with $p \neq 2$, or $\mathfrak{G}_\infty$ 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 $\mathfrak{H}$, $\boldsymbol{O}_3(\mathfrak{H})$ is cyclic, then we would know (see [4]) that (1) if $p = 2$, then $\mathfrak{G}_\infty \subseteqq S(2^n)$, (2) if $p \neq 2$ and $|\mathfrak{G}_\infty|$ is odd, then $\mathfrak{G}_\infty \subseteqq S(p^n)$, (3) if $p \neq 2$ and $|\mathfrak{G}_\infty|$ is even, then $\mathfrak{H} = \mathfrak{G}_{\infty 0}$ has a central involution. Here $\mathfrak{G}_\infty$ 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 $\mathfrak{G}$ be an $(n + 1/2)$-transitive permutation group and let $\mathfrak{D}$ be the stabilizer of $(n - 1)$ points. Suppose that $\mathfrak{D}$ is solvable and not a Frobenius group. If $n \geqq 3$ then $\mathfrak{G} = \mathrm{Sym}_{n+3}$.*

Proof. We note first that if $\mathfrak{G} = \mathrm{Sym}_{n+3}$ then $\mathfrak{G}$ is $(n + 3)$-transitive and hence $(n + 1/2)$-transitive. Also $\mathfrak{D} = \mathrm{Sym}_4$ 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 $\mathfrak{G} = \mathrm{Sym}_6$. Let $n = 3$ and let $\infty, 0, 1$ be three points. Set $\mathfrak{K} = \mathfrak{G}_\infty$, $\mathfrak{D} = \mathfrak{G}_{\infty 0}$, $\mathfrak{H} = \mathfrak{G}_{\infty 01}$. Then $\mathfrak{K}$ is 5/2-transitive and by Lemma 2.1, $\mathfrak{K}$ has no regular normal subgroup. We know that $\mathfrak{D}$ has a regular normal elementary abelian subgroup $\mathfrak{V}$ so $\mathfrak{D} = \mathfrak{H}\mathfrak{V}$. Since $\mathfrak{V}$ is abelian and $\mathfrak{D}$ is primitive, $\mathfrak{V}$ is the unique minimal normal subgroup of $\mathfrak{D}$. Hence $\mathfrak{V}$ is characteristic in $\mathfrak{D}$ and $\mathfrak{H}$ acts irreducibly on $\mathfrak{V}$. Since $\mathfrak{D}$ is not a Frobenius group, we cannot have $|\mathfrak{V}| = 3$. Further $\mathfrak{V}$ is elementary so we cannot have $|\mathfrak{V}| = 8$ with $\mathfrak{V}$ having a cyclic subgroup of index 2. By Theorems 1 and 3 of [6] we must therefore have $|\mathfrak{V}| = 4$ or 9 and hence deg $\mathfrak{G} = |\mathfrak{V}| + 2 = 6$ or 11. Suppose deg $\mathfrak{G} = 6$. Since $\mathfrak{G}$ is 7/2-transitive we have $|\mathfrak{G}| > 6\cdot 5\cdot 4$ so $[\mathrm{Sym}_6 : \mathfrak{G}] < 6$. Hence $\mathfrak{G} = \mathrm{Alt}_6$ or Sym_6. If $\mathfrak{G} = \mathrm{Alt}_6$ then $\mathfrak{D} = \mathrm{Alt}_4$, a Frobenius group. Thus we have only $\mathfrak{G} = \mathrm{Sym}_6$ here.

We now assume that $|\mathfrak{V}| = 9$ and derive a contradiction. Now $\mathfrak{V}$ contains an element of order 3 fixing precisely two element. Since $\mathfrak{G}$ is triply transitive, $\mathfrak{G}$ contains W a conjugate of this element with $W = (a)(b)(0\ \infty\ 1)\cdots$. Hence W normalizes $\mathfrak{H}$. If $H \in \boldsymbol{C}_{\mathfrak{H}}(W)$, then

$aH = (aW)H = (aH)W$ so $aH = a$ or b and hence $|C_{\mathfrak{H}}(W)| \leqq 2|\mathfrak{H}_a|$. If W acts trivially on $\mathfrak{H}$, then $[\mathfrak{H} : \mathfrak{H}_a] = 2$ 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 $\mathfrak{B}$. We have $\mathfrak{H} \subseteqq GL(2, 3)$ 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 $\mathfrak{D}$ 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 $\mathfrak{Q} = O_2(\mathfrak{H})$. Then $\mathfrak{Q}$ is the quaternion group of order 8. It acts regularly on 8 points and fixes 3. Now $\mathfrak{S}$, a Sylow 3-subgroup of $\langle \mathfrak{H}, W \rangle$ is abelian of type (3, 3) and acts on $\mathfrak{Q}$. Hence there exists $S \in \mathfrak{S}^{\#}$ with S centralizing $\mathfrak{Q}$. From the way $\mathfrak{Q}$ 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 $\mathfrak{G}$ is triply transitive it contains all 3-cycles so $\mathfrak{G} \supseteqq \mathrm{Alt}_{11}$. Thus $\mathfrak{D} \supseteqq \mathrm{Alt}_9$ 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

1. H. Bender, *Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine fixpunkte haben*, Math. Zeit. **104** (1968), 175–204.
2. W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math. **4** (1960), 170–186.
3. J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Math. Soc. **47** (1941), 458–467.
4. D. S. Passman, *Solvable 3/2-transitive permutation groups*, J. of Algebra **7** (1967), 192–207.
5. ———, *p-solvable doubly transitive permutation groups*, Pacific J. Math. **26** (1968), 555–577.
6. M. Suzuki, *Transitive extensions of a class of doubly transitive groups*, Nagoya Math. J. **27** (1966), 159–169.
7. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.
8. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.
9. H Zassenhaus, *Kennzeichnung endlichen linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 17–40.

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

YALE UNIVERSITY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 28, No. 1 March, 1969