PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 3, 1968

p-SOLVABLE DOUBLY TRANSITIVE PERMUTATION GROUPS

D. S. PASSMAN

In this paper doubly transitive and 3/2-transitive permutation groups are classified under hypotheses somewhat weaker than solvability. We mention two examples.

Let $\mathscr{S}(p^n)$ denote the group of semilinear transformations over $GF(p^n)$. The following combines a result of Huppert on solvable 2-transitive groups and a result of Zassenhaus on sharply 2-transitive groups.

THEOREM I. Let $\mathfrak{G}$ be a p-solvable doubly transitive permutation group with $O_p(\mathfrak{G}) \neq \langle 1 \rangle$. Then deg $\mathfrak{G} = p^n$ for some n and we have one of the following: (i) $\mathfrak{G} \subseteq \mathscr{S}(p^n)$, (ii) $\mathfrak{G}$ is solvable and $p^n = 3^2, 5^2, 7^2, 11^2, 23^2$ or 3^4, or (iii) $\mathfrak{G}$ is nonsolvable and $p^n = 11^2, 19^2, 29^2$ or 59^2.

The second result reads better as a theorem on linear groups.

THEOREM II. Let group $\mathfrak{G}$ act faithfully on vector space $\mathfrak{V}$ over $GF(p)$ and let $\mathfrak{G}$ act 1/2-transitively but not semiregularly on $\mathfrak{V}^\#$. If $\mathfrak{G}$ is imprimitive as a linear group, then $\mathfrak{G}$ is solvable and we have one of the following: (i) $|\mathfrak{V}| = p^{2n}$ for $p \neq 2$ and $\mathfrak{G}$ is a specific group of order $4(p^n - 1)$, (ii) $|\mathfrak{V}| = 3^4$ and $|\mathfrak{G}| = 32$, or (iii) $|\mathfrak{V}| = 2^6$ and $|\mathfrak{G}| = 18$.

The approach here is first to prove that such groups are solvable, modulo a few exceptions, and then to apply the known results on solvable groups.

1. Number theoretic results.

THEOREM 1.1. *Given integers $a \geqq 2$ and $n \geqq 3$ with*

$$(n, a) \neq (4, 2), (6, 2), (10, 2), (12, 2), (18, 2), (4, 3), (6, 3), (6, 5) .$$

Then there exists a prime q satisfying

(i) $q \mid a^n - 1$ *but* $q \nmid a^m - 1$ *for* $1 \leqq m < n$,

(ii) *either* $q \geqq 2n + 1$ *or* $q = n + 1$ *and* $q^2 \mid a^n - 1$.

Proof. For integer n, let $s = s(n)$ denote the numbers of its distinct prime factors, let $p(n)$ denote its largest prime factor and let $q(n) = n + 1$ or 1 according to whether $n + 1$ is prime or not. Let $Q_n(x)$ denote the cyclotomic polynomial of order n and degree $\varphi(n)$, where φ is the Euler function.

Step 1. We show first that if $s \geqq 2$ and

$$2^{\varphi(n)-2^s-2} \leqq n(n+1)/2$$

then $n = 6, 10, 12, 14, 18, 20, 24$ or 30.

Clearly $\varphi(n) \geqq n(1-1/p_1)(1-1/p_2)\cdots(1-1/p_s)$ where $p_1, p_2, \cdots, p_s$ are the first s primes. Let $s = 2$. Then $\varphi(n) \geqq n(1-1/2)(1-1/3) = n/3$ and hence

$$2^{(n/3)-1} \leqq n(n+1)/2 .$$

This yields easily $n < 33$. Since $s = 2$, an easy check shows that only $n = 6, 10, 12, 14, 18, 20$ and 24 occur.

Now let $s = 3$. Here $\varphi(n) \geqq n(1-1/2)(1-1/3)(1-1/5) = 4n/15$ and hence

$$2^{(4n/15)-2} \leqq n(n+1)/2 .$$

This yields easily $n < 60$ and since $s = 3$ we have $n = 30$ or 42. An easy check shows that only $n = 30$ occurs.

Finally let $s \geqq 4$. If $n = q_1^{a_1}q_2^{a_2}\cdots q_s^{a_s}$, then

$$\begin{aligned}\varphi(n)n^{-1/2} &= \prod q_i^{(a_i-1)/2}(q_i-1)q_i^{-1/2} \\ &\geqq (p_1-1)p_1^{-1/2}(p_2-1)p_2^{-1/2}(p_3-1)p_3^{-1/2}(p_4-1)p_4^{-1/2} \\ &= 48\cdot(210)^{-1/2}\end{aligned}$$

and hence

$$\varphi(n) \geqq 48(n/210)^{1/2} .$$

Clearly

$$\begin{aligned}s-4 &\leqq \log_{p_5}(n/(p_1p_2p_3p_4)) = \log_{11}(n/210) \\ &< \log_8(n/210) = (1/3)\log_2(n/210)\end{aligned}$$

so that

$$2^{s-2} < 4(n/210)^{1/3} .$$

Thus

$$2^{48(n/210)^{1/2}-4(n/210)^{1/3}} \leqq 2^{\varphi(n)-2^s-2} \leqq n(n+1)/2$$

and clearly $n < 210$. Since $s \geqq 4$, this cannot occur. Hence this first result is proved.

Step 2. We show now that if $s \geqq 2$ and

$$2^{\varphi(n)-2^s-2} \leqq p(n)q(n)$$

then $n = 6, 10, 12, 18$ or 30.

Since $n \neq 2$, n and $n+1$ cannot both be prime. Thus $p(n)q(n) \leqq n(n+1)/2$ and the above applies. A check of these few cases shows that only $n = 6, 10, 12, 18$ and 30 occur.

Step 3. If $Q_n(a) \leqq p(n)q(n)$, then $(n, a) = (4, 2)$, $(6, 2)$, $(10, 2)$, $(12, 2)$, $(18, 2)$, $(4, 3)$, $(6, 3)$, $(6, 4)$, $(6, 5)$.

If $s(n) = 1$, then from the known form of $Q_n(x)$ we have

$$2^{n/2} + 1 \leqq a^{n/2} + 1 \leqq Q_n(a) .$$

Since $p(n)q(n) \leqq n(n+1)/2$ we have

$$2^{n/2} + 1 \leqq n(n+1)/2$$

and hence $n < 16$. Since $s = 1$ and $n \geqq 3$ we have $n = 3, 4, 5, 7, 8, 9, 11$ or 13. Let $n \neq 4$ here so that $q(n) = 1$ and

$$2^{n/2} + 1 \leqq n .$$

Thus no values of n occur here. This leaves only $n=4$ so $p(n)q(n)=10$. From $a^2 + 1 \leqq 10$ we have $(n, a) = (4, 2)$ or $(4, 3)$.

Now let $s \geqq 2$. By [4] (bottom of page 88)

$$2^{\varphi(n)-2^{s-2}} \leqq a^{\varphi(n)} \cdot 2^{-2^{s-2}} \leqq Q_n(a)$$

so that Step 2 applies. Thus $n = 6, 10, 12, 18$ or 30. We obtain the following chart quite easily.

n	$Q_n(x)$	$p(n)q(n)$	a
6	$x^2 - x + 1$	21	2, 3, 4, 5
10	$x^4 - x^3 + x^2 - x + 1$	55	2
12	$x^4 - x^2 + 1$	39	2
18	$x^6 - x^3 + 1$	57	2
30	$x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$	155	none .

This completes the proof of this step.

Step 4. We now proceed to prove the theorem. We will follow [4]. Let us suppose first that for all primes q which divide $a^n - 1$ that either $q \mid a^m - 1$ for some $1 \leqq m < n$ or $q = n + 1$ and $q^2 \nmid a^n - 1$. Let $q \mid Q_n(a)$ so that $q \mid a^n - 1$. By [4] since $n > 2$ the first possibility implies that $q = p(n)$ and $q^2 \nmid Q_n(a)$. This yields clearly $Q_n(a) \leqq p(n)q(n)$ and hence by the above $(n, a) = (4, 2)$, $(6, 2)$, $(10, 2)$, $(12, 2)$, $(18, 2)$, $(4, 3)$, $(6, 3)$, $(6, 4)$ or $(6, 5)$. An easy check shows that $(n, a) = (6, 4)$ does not satisfy this assumption on the primes.

Hence if (n, a) is not one of these eight exceptions, then there

exists a prime q with $q \mid a^n - 1$ but $q \nmid a^m - 1$ for $1 \leqq m < n$. Also if $q = n + 1$, then $q^2 \mid a^n - 1$. Now since n is the order of a modulo q we have $n \mid q - 1$ so $q = kn + 1$ for some positive integer k. If $q < 2n + 1$, then $q = n + 1$ and the proof is complete.

As a corollary we obtain the result we generalized.

COROLLARY 1.2. *Given integers $a \geqq 2$ and $n \geqq 3$ with $(n, a) \neq (6, 2)$. Then there exists a prime q satisfying $q \mid a^n - 1$ but $q \nmid a^m - 1$ for $1 \leqq m < n$.*

Proof. We need only consider the exceptions of Theorem 1.1. In all these exceptions other than (6, 2) we see easily that $q = n + 1$ has the required property.

A convenient restatement of the above is

COROLLARY 1.3. *Let $\mathfrak{M}$ denote the multiplicative group of $GF(p^n)$. If σ is a field automorphism, then σ can be viewed as an endomorphism of $\mathfrak{M}$. Let $\sigma_1, \sigma_2, \cdots, \sigma_t$ be field automorphisms. If $n \geqq 3$ and $(n, p) \neq (6, 2)$, then $\prod (1 - \sigma_i) = 0 \in \operatorname{End} \mathfrak{M}$ implies that some $\sigma_i = 1$.*

Proof. $\mathfrak{M}$ is cyclic of order $p^n - 1$. If σ is a nonidentity field automorphism, then σ is of the form $x \to x^{p^m}$ with $1 \leqq m < n$. Say σ_i: $x \to x^{p^{m_i}}$. Then $\prod (1 - \sigma_i) = 0$ as an endomorphism of $\mathfrak{M}$ yields

$$(p^n - 1) \mid \prod (1 - p^{m_i})$$

and this cannot occur by Corollary 1.2 if $1 \leqq m_i < n$ for all i unless $n = 2$ or $(n, p) = (6, 2)$.

In the exceptional cases above we have with the notation of Corollary 1.3.

LEMMA 1.4. (i) *If $n = 2, p \neq 3$ then $\prod_1^3 (1 - \sigma_i) = 0$ implies that some $\sigma_i = 1$.*

(ii) *If $(n, p) = (6, 2)$, then $\prod_1^4 (1 - \sigma_i) = 0$ implies that either some $\sigma_i = 1$ or at least two σ_i's have order 3 and that at least one σ_i has order 2.*

Proof. (i) If $n = 2$ and all $\sigma_i \neq 1$, then all σ_i are equal to say σ and σ has order 2. This yields easily

$$\prod_1^3 (1 - \sigma_i) = 4(1 - \sigma) = 0 .$$

Thus every fourth power in $\mathfrak{M}$ is in the fixed field of σ and

$$(p^2 - 1)/4 = |\mathfrak{M}|/4 \leqq p - 1$$

a contradiction unless $p = 2$ or 3. If $p = 2$, then $4 \nmid |\mathfrak{M}|$ so $\sigma = 1$.

(ii) Here we consider the field automorphisms explicitly. If $o(\sigma)$ denotes the order of σ, we have

$$\begin{aligned} o(\sigma) &= 2 \quad x^{1-\sigma} = x^{-7} \\ o(\sigma) &= 3 \quad x^{1-\sigma} = x^{-3} \quad \text{or} \quad x^{-5\cdot 3} \\ o(\sigma) &= 6 \quad x^{1-\sigma} = x^{-1} \quad \text{or} \quad x^{-31}. \end{aligned}$$

If all $\sigma_i \neq 1$, then a suitable product of these exponents must be divisible by $2^6 - 1 = 3\cdot 3\cdot 7$ so we must have at least two elements of order 3 and at least one of order 2.

2. A solvability theorem.

THEOREM 2.1. *Let p be a prime and $a = p^k$. Suppose that $\mathfrak{G}$ is a p-solvable subgroup of $GL(n, a)$ with $(a^n - 1)/(a^m - 1) \,||\, \mathfrak{G}|$ for some divisor $m \neq n$ of n. Then either $\mathfrak{G}$ is solvable or $(n, a) = (2, 11), (2, 19), (2, 29), (2, 59), (6, 5)$. Moreover if $(n, a) = (6, 5)$, then $\mathfrak{G}$ is solvable unless $m = 3$.*

Proof. Since $\mathfrak{G}$ is p-solvable it has a p-complement $\mathfrak{H}$. Now $(a^n - 1)/(a^m - 1)$ divides $|\mathfrak{G}|$ and this number is prime to p so $(a^n - 1)/(a^m - 1) \,||\, \mathfrak{H}|$. If we show that $\mathfrak{H}$ is solvable, then since $\mathfrak{G}$ is p-solvable it will be solvable. Thus it suffices to assume that $p \nmid |\mathfrak{G}|$. Since $p \nmid |\mathfrak{G}|$, this representation of $\mathfrak{G}$ is realizeable over the complex numbers. Hence theorems on complex linear groups apply here.

Case 1. We consider first the possibility $n \leqq 2$. If $n = 1$, then $\mathfrak{G}$ is certainly solvable. Let $n = 2$. If $\boldsymbol{Z}(\mathfrak{G})$ acts irreducibly, then $\mathfrak{G}$ is abelian by Schur's lemma and the fact that finite division rings are fields. Thus we can assume that $|\boldsymbol{Z}(\mathfrak{G})|$ divides $a - 1$. Now $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G})$ is a 2-dimensional collineation group and hence if $\mathfrak{G}$ is not solvable, then $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq A_5$ by [11] (Chapter X). Thus $|\mathfrak{G}| \,||\, 60(a - 1)$ and by assumption $(a + 1) \,||\, \mathfrak{G}|$. Note that $p \nmid |\mathfrak{G}|$ so $p \neq 2, 3, 5$ and also g.c.d. $\{a - 1, a + 1\} = 2$. This yields $a + 1 \,|\, 120$ and since a is a prime power we get $a = p = 7, 11, 19, 23, 29, 59$. Since $\mathfrak{G} \subseteqq GL(2, p)$ and $5 \,||\, \mathfrak{G}|$ we have $5 \,|\, p^2 - 1$ so that $p \neq 7, 23$. This leaves $a = p = 11, 19, 29, 59$.

We assume now that $n \geqq 3$. Suppose that (n, a) is not one of the exceptions of Theorem 1.1. Then there exists a prime q with $q \,|\, a^n - 1$ but $q \nmid a^j - 1$ for $1 \leqq j < n$. Thus by assumption $q \,||\, \mathfrak{G}|$.

Let $\mathfrak{Q}^*$ be a subgroup of $\mathfrak{G}$ of order q in the center of a Sylow q-subgroup $\mathfrak{Q}$ of $\mathfrak{G}$. Since $q \nmid a^j - 1$ for $1 \leqq j < n$, $\mathfrak{Q}^*$ is irreducible. By Schur's lemma, $C(\mathfrak{Q}^*) \supseteq \mathfrak{Q}$ is cyclic. Since $\operatorname{Aut} \mathfrak{Q}^*$ is abelian, $\mathfrak{G}$ will be solvable if we show that $\mathfrak{Q}^*$ is normal in $\mathfrak{G}$. By Theorem 1.1, q satisfies one of the following two conditions. Either $q^2 \| |\mathfrak{G}|$ and $q \geqq n + 1$ or $q^2 \nmid |\mathfrak{G}|$ and $q \geqq 2n + 1$. We consider these in the following two cases.

Case 2. We assume that $q^2 \| |\mathfrak{G}|$ and $q \geqq n + 1$. Let $\mathscr{R}$ be the associated complex representation of $\mathfrak{G}$. Then there is a homomorphism, $\mathscr{R} \to \mathscr{R}_q$, yielding a representation of $\mathfrak{G}$ of degree n over some finite field $\mathfrak{F}$ of characteristic q. Let $\mathfrak{K}$ be the kernel of the representation $\mathscr{R}_q$. As is well known, $\mathfrak{K}$ is a q-group. Since $q \geqq n + 1$, the Sylow q-subgroup of $GL(n, \mathfrak{F})$ has period q. Thus since $\mathfrak{Q}$ is cyclic and $|\mathfrak{Q}| \geqq q^2$ we see that $\mathfrak{K} \supseteq \mathfrak{Q}^*$. Now $\mathfrak{K}$ is cyclic so $\mathfrak{Q}^* \triangle \mathfrak{G}$ and $\mathfrak{G}$ is solvable.

Case 3. We assume now that $q^2 \nmid |\mathfrak{G}|$ and $q \geqq 2n + 1$. If $q > 2n + 1$, then by Theorem 3 of [1], $\mathfrak{Q} = \mathfrak{Q}^* \triangle \mathfrak{G}$. Moreover if $q = 2n + 1$ and the representation of $\mathfrak{G}$ is not absolutely irreducible, then we can again apply this result. Thus we need only consider the case $q = 2n + 1$ and $\mathfrak{G}$ absolutely irreducible. The latter imples that $\boldsymbol{Z}(\mathfrak{G})$ consists of scalar matrices so $|\boldsymbol{Z}(\mathfrak{G})| \,|\, a - 1$. If $\mathfrak{Q}$ is not normal, then by Theorem 4 of [1] we have $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq PSL(2, q)$. We show now that this cannot occur.

Since $|PSL(2, q)| = q(q - 1)(q + 1)/2$ and $q = 2n + 1$ we obtain

$$(a^n - 1)/(a^m - 1) \,|\, (a - 1)2n(2n + 1)(n + 1) .$$

Note that the order of $PSL(2, q)$ is always divisible by 6 so $p \neq 2, 3$ and hence $a \geqq 5$.

Let us assume first that n is odd. Since a is odd we see that $(a^n - 1)/(a^m - 1)$ is odd and hence

$$(a^n - 1)/(a^m - 1) \,|\, (a - 1)n(2n + 1)(n + 1)/4 .$$

Thus since $a \geqq 5$ and $m \,|\, n$

$$\begin{aligned}(5^n - 1)/(5^{n/3} - 1) &\leqq 4(a^n - 1)/((a - 1)(a^{n/3} - 1)) \\ &\leqq n(n + 1)(2n + 1)\end{aligned}$$

and hence $n < 9$. Now n is odd and $2n + 1$ is prime so we have $n = 3$ or 5. Note that $m \,|\, n$ implies that $m = 1$.

If $n = 3$, then

$$(a^2 + a + 1) \,|\, 3 \cdot 7(a - 1)/2$$

and if $n = 5$, then

$$(a^4 + a^3 + a^2 + a + 1) \mid 3 \cdot 5 \cdot 11(a - 1)/2 .$$

An easy check shows that these have no solution with $a = p^k$ and $p \neq 2, 3$.

Now let n be even. Again since $a \geqq 5$ we have

$$(5^{n/2} + 1)/4 \leqq (a^n - 1)/((a - 1)(a^{n/2} - 1)) \leqq 2n(n + 1)(2n + 1)$$

and hence $n < 14$. Now n is even and $2n + 1$ is prime so we have $n = 6$ or 8. In each case there are three choices for m and we obtain the following six facts.

$$\begin{aligned}
n = 6 \quad m = 3: &\quad (a^3 + 1) \mid (a - 1)2^2 \cdot 3 \cdot 7 \cdot 13 \\
m = 2: &\quad (a^4 + a^2 + 1) \mid (a - 1)2^2 \cdot 3 \cdot 7 \cdot 13 \\
m = 1: &\quad (a^5 + a^4 + a^3 + a^2 + a + 1) \mid (a - 1)2^2 \cdot 3 \cdot 7 \cdot 13 \\
n = 8 \quad m = 4: &\quad (a^4 + 1) \mid (a - 1)2^4 \cdot 3^2 \cdot 17 \\
m = 2: &\quad a^5 < 2^4 \cdot 3^2 \cdot 17 \\
m = 1: &\quad a^6 < 2^4 \cdot 3^2 \cdot 17 .
\end{aligned}$$

An easy check shows that these have no solution for $a \geqq 5$. This completes the study of this case.

We need only consider the exceptional cases of Theorem 1.1 now. Since we do not claim that the subgroup $\mathfrak{G}$ of $GL(6, 5)$ is solvable if $m = 3$, there remains only $(n, a) = (4, 2)$, $(6, 2)$, $(10, 2)$, $(12, 2)$, $(18, 2)$, $(4, 3)$, $(6, 3)$ and $(6, 5)$ with $m \neq 3$. Hence $a = p = 2, 3$ or 5.

Case 4. We now study these exceptions with $p = 2$ or 3. First let $a = p = 2$. Then $\mathfrak{G}$ is a subgroup of odd order of $GL(n, 2)$ with $n \leqq 18$. Here to avoid unpleasant computation we will just apply the theorem of Feit and Thompson ([6]) which guarantees that $\mathfrak{G}$ is solvable.

Now let $a = p = 3$ so that $n = 4$ or 6. If $n = 4$, then since $\mathfrak{G} \subseteqq GL(4, 3)$ and $3 \nmid |\mathfrak{G}|$ we have $|\mathfrak{G}| \mid 2^9 \cdot 5 \cdot 13$. Since $13 > 2n + 1$ we see by Theorem 3 of [1] that $\mathfrak{G}$ has a normal Sylow 13-subgroup. By Burnside's two prime theorem, $\mathfrak{G}$ is solvable.

Now let $n = 6$. Since $\mathfrak{G} \subseteqq GL(6, 3)$ and $3 \nmid |\mathfrak{G}|$ we have $|\mathfrak{G}| \mid 2^{13} \cdot 5 \cdot 7 \cdot 11^2 \cdot 13^2$. Also $(3^6 - 1)/(3^m - 1) \mid |\mathfrak{G}|$ so $7 \mid |\mathfrak{G}|$. We show that if $\mathfrak{G} \subseteqq GL(6, 3)$, $3 \nmid |\mathfrak{G}|$ and $7 \mid |\mathfrak{G}|$, then $\mathfrak{G}$ is solvable. By way of contradiction, let $\mathfrak{G}$ be a counterexample of minimal order.

Let $q = 11$ or 13. If $\mathfrak{G}$ has a normal subgroup of order q^2, then by the minimal nature of $\mathfrak{G}$ a q-complement is solvable. Hence $\mathfrak{G}$ is solvable, a contradiction. If $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}$ of order q, then since $7 \nmid q - 1$ we see that $7 \mid |C(\mathfrak{G})|$. Since $\mathfrak{G}/C(\mathfrak{G})$ is abelian,

we must have $\mathfrak{G} = C(\mathfrak{G})$. By Grün's theorem, $\mathfrak{G}$ has a normal subgroup of index q, again a contradiction. Thus $\mathfrak{G}$ has no normal subgroup of order q or q^2 for $q = 11$ or 13. Now $11, 13 > n + 1$ and hence by [5] we must have

$$|\mathfrak{G}| = 2^s \cdot 5^\delta \cdot 7 \cdot 11^\varepsilon \quad \text{or} \quad 2^s \cdot 5^\delta \cdot 7 \cdot 13$$

where $\varepsilon = 0, 1$ $\delta = 0, 1$ and $s \leqq 13$.

If $|\mathfrak{G}|$ is of the second type above, then since $13 = 2n + 1$, Theorem 4 of [1] implies that $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq PSL(2, 13)$. This is a contradiction since $3 \nmid |\mathfrak{G}|$. Thus $|\mathfrak{G}|$ is of the first type.

We show now that $\delta = 0$. Since $\mathfrak{G} \subseteqq GL(6, 3)$ we see that $\mathfrak{G}$ has no elements of order $7 \cdot 5$ or $7 \cdot 11$. Thus if n_7 denotes the number of Sylow 7-subgroups of $\mathfrak{G}$, then $n_7 = 2^r 5^\delta 11^\varepsilon$ for some integer r. Now $5 \equiv -2 \bmod 7$ and $11 \equiv 2^2 \bmod 7$ so $n_7 \equiv (-)^\delta 2^t \bmod 7$ for some integer t. By Sylow's theorem $n_7 \equiv 1$ and thus $2^t \equiv (-)^\delta \bmod 7$. This equation has no solution if $\delta = 1$ and thus we must have $\delta = 0$ and hence $|\mathfrak{G}| = 2^s \cdot 7 \cdot 11^\varepsilon$. By Burnside's two prime theorem and by the result of [2] we see that $\mathfrak{G}$ is solvable, a contradiction.

Case 5. Finally let $(n, a) = (6, 5)$ with $m \neq 3$. Here

$$(5^6 - 1)/(5^m - 1) \,||\, |\mathfrak{G}|$$

and $m \neq 3$ so $7 \,||\, |\mathfrak{G}|$ and $31 \,||\, |\mathfrak{G}|$. By way of contradiction, let $\mathfrak{G}$ be a nonsolvable subgroup of $GL(6, 5)$ of minimal order with $5 \nmid |\mathfrak{G}|$, $31 \,||\, |\mathfrak{G}|$ and $7 \,||\, |\mathfrak{G}|$. Since $7 \mid 5^6 - 1$ but $7 \nmid 5^j - 1$ for $1 \leqq j < 6$ we see that $\mathfrak{G}$ is irreducible. By [7] since $31 > 2n + 1$, $\mathfrak{G}$ has a normal abelian Sylow 31-subgroup $\mathfrak{A}$. Since $31 \mid 5^3 - 1$ and $31 \mid 5^6 - 1$ but $31 \nmid 5^j - 1$ for any other j with $1 \leqq j \leqq 6$ we see by Clifford's theorem that the representation restricted to $\mathfrak{A}$ breaks up into one or two irreducible constituents. If $\mathfrak{A}$ is irreducible, then $\mathfrak{G}$ is clearly solvable, a contradiction, so there are two irreducible constituents. If these constituents are inequivalent, then the representation is induced from a subgroup $\mathfrak{H}$ of index 2 which is necessarily normal. By the minimal nature of $\mathfrak{G}$, $\mathfrak{H}$ is solvable, a contradiction. Hence the two constituents are equivalent and $\mathfrak{A}$ is cyclic. Since $7 \nmid 31 - 1$ we see that $7, 31 \,||\, \boldsymbol{C}(\mathfrak{A})|$ and so $\mathfrak{G} = \boldsymbol{C}(\mathfrak{A})$. By Lemma 1.1 of [12], $\mathfrak{G}$ is contained isomorphically in $GL(2, 5^3)$. Thus since $\mathfrak{G}$ is not solvable, $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq A_5$ by [11] (Chapter X) and $5 \,||\, |\mathfrak{G}|$, a contradiction. This completes the proof.

EXAMPLES. Let $\mathfrak{G} = SL(2, 5)$, a nonsolvable group of order 120. Then $\mathfrak{G}$ has a faithful character χ of degree 2 with $\boldsymbol{Q}(\chi) = \boldsymbol{Q}(\sqrt{5})$. For $p \neq 2, 3, 5$ this representation is realizable over $GF(p)$ if and only

if $\sqrt{5} \in GF(p)$. By quadratic reciprocity this is true if and only if $p \equiv \pm 1 \bmod 5$. In particular $\mathfrak{G} \subseteqq GL(2, p)$ when $p = 11, 19, 29, 59$. In each of these cases $(p^2 - 1)/(p - 1) = p + 1$ divides $|\mathfrak{G}|$.

Now let $\mathfrak{H} = PSL(2, 7)$, a simple group of order 168. Then $\mathfrak{H}$ has a faithful complex character χ of degree 3 such that $\boldsymbol{Q}(\chi) = \boldsymbol{Q}(\sqrt{7})$. Now $5 \nmid |\mathfrak{H}|$ and obviously $\sqrt{7} \in GF(5^2)$ so $\mathfrak{H} \subseteqq GL(3, 5^2)$. Let $\mathfrak{C}$ be the central subgroup of order 3 of this general linear group and set $\mathfrak{G} = \mathfrak{H}\mathfrak{C}$. Since $\mathfrak{G} \subseteqq GL(3, 5^2)$ we have $\mathfrak{G} \subseteqq GL(6, 5)$. Also

$$(5^6 - 1)/(5^3 - 1) \,||\, |\mathfrak{G}| \,.$$

Thus Theorem 2.1 is best possible.

3. **Solvable groups.** If a is a prime power we let $\mathscr{T}(n, a)$ denote the group of semilinear transformations of $GF(a^n)$ over $GF(a)$. That is, $\mathscr{T}(n, a)$ consists of all functions on $GF(a^n)$ of the form $x \to bx^\sigma$ where $b \in GF(a^n)^\#$ and σ is a field automorphism of $GF(a^n)$ over $GF(a)$. Thus $\mathscr{T}(n, a)$ is a metacyclic group of order $n(a^n - 1)$. It is transitive on $GF(a^n)^\#$.

THEOREM 3.1. *Let p be a prime and $a = p^k$. Suppose $\mathfrak{G}$ is a solvable subgroup of $GL(n, a)$ with $(a^n - 1)/(a^m - 1) \,||\, |\mathfrak{G}|$ for some divisor $m \neq n$ of n. Then either $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ or $(n, a) = (2, 3)$, $(2, 5)$, $(2, 7)$, $(2, 11)$, $(2, 23)$, $(2, 47)$, $(4, 3)$, $(6, 2)$.*

Proof. We proceed in a series of steps.

Step 1. Suppose we can find a prime q with $q \,|\, a^n - 1$ but $q \nmid a^j - 1$ for all $j < n$. Then $\mathfrak{G}$ is irreducible and hence $\boldsymbol{O}_p(\mathfrak{G}) = \langle 1 \rangle$. If further we have one of the following, then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$.

(i) $\boldsymbol{O}_q(\mathfrak{G}) \neq \langle 1 \rangle$

(ii) $q > n + 1$

(iii) $q = n + 1$ and $q^2 \,||\, |\mathfrak{G}|$

(iv) $q = n + 1$ and $\boldsymbol{O}_2(\mathfrak{G}) = \langle 1 \rangle$

(v) $q = n + 1$ and q is not a Fermat prime.

Since $(a^n - 1)/(a^m - 1) \,||\, |\mathfrak{G}|$ we have $q \,||\, |\mathfrak{G}|$. Let $\mathfrak{Q}$ be a subgroup of $\mathfrak{G}$ of order q in the center of a Sylow q-subgroup. Since $q \nmid a^j - 1$ for $j < n$, $\mathfrak{Q}$ is irreducible. By Schur's lemma, $\boldsymbol{C}_{\mathfrak{G}}(\mathfrak{Q})$ is cyclic. If $\mathfrak{Q} \triangle \mathfrak{G}$, then by [8] (Hilfssatz 2) $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$. If $\boldsymbol{O}_q(\mathfrak{G}) \neq \langle 1 \rangle$, then clearly $\mathfrak{Q} \subseteqq \boldsymbol{O}_q(\mathfrak{G})$ and since the latter group is cyclic, $\mathfrak{Q} \triangle \mathfrak{G}$ and (i) follows.

We show now that assumptions (ii)-(v) imply that $\boldsymbol{O}_q(\mathfrak{G}) \neq \langle 1 \rangle$. Suppose by way of contradiction that $\boldsymbol{O}_q(\mathfrak{G}) = \langle 1 \rangle$. By Fitting's theorem there exists a prime r such that $\mathfrak{Q}$ does not centralize $\mathfrak{R} =$

$O_r(\mathfrak{G})$. By the above $r \neq p$ so $\mathfrak{N}\mathfrak{Q}$ is a p'-group. Hence the representation of this group is realizeable over the complex numbers. Certainly $\mathfrak{Q}$ is not normal in $\mathfrak{N}\mathfrak{Q}$. Hence by Ito's theorem ([10]) we cannot have $q > n + 1$. Let $q = n + 1$. Again by Ito's theorem, we must have q a Fermat prime and $|\mathfrak{N}\mathfrak{Q}|$ even so $r = 2$. Thus (ii), (iv) or (v) implies (i).

Now assume $q = n + 1$ and $q^2 \| |\mathfrak{G}|$. Let $\mathfrak{Q}^*$ be a cyclic subgroup of order q^2 containing $\mathfrak{Q}$. Let $\mathfrak{N}$ be as above and consider the group $\mathfrak{N}\mathfrak{Q}^*$. The argument of Case 2 of the proof of Theorem 2.1 shows that $\mathfrak{Q} \triangle \mathfrak{N}\mathfrak{Q}^*$, a contradiction, and we have proved this result.

Step 2. We show now that if $n \geqq 3$, then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ unless $(n, a) = (4, 3)$ or $(6, 2)$.

By Theorem 1.1 we have either (ii) or (iii) of Step 1 in the non-exceptional cases. Thus we need only consider the eight exceptions of that theorem. We apply Corollary 1.2. If $(n, a) = (6, 3)$ or $(6, 5)$, then $\mathfrak{G}$ satisfies (v) of Step 1. If $(n, a) = (4, 2)$, $(10, 2)$, $(12, 2)$ or $(18, 2)$, then, since $a = p = 2$, $\mathfrak{G}$ satisfies (iv) of Step 1. This leaves only $(n, a) = (6, 2)$ or $(4, 3)$.

Step 3. We show now that if $n \leqq 2$, then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ unless $(n, a) = (2, 3)$, $(2, 5)$, $(2, 7)$, $(2, 11)$, $(2, 23)$, $(2, 47)$.

The result is clear for $n = 1$ so we assume $n = 2$. We have $a + 1 \| |\mathfrak{G}|$. If prime $q > 3$ divides $a + 1$ then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ by (ii) of Step 1. If $3^2 | a + 1$, then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ by (iii) of Step 1. Thus we can assume that either $a + 1 = 2^t$ or $a + 1 = 3 \cdot 2^t$.

Now $a = p^k$. We show first that $k = 1$ so a is a prime. If $a + 1 = 2^t$, the result follows from Lemma 4 of [9]. Let $p^k + 1 = a + 1 = 3 \cdot 2^t$. If $p = 2$, then clearly $t = 0$ and $a = 2$. Suppose now that $p \neq 2$. If k is even, then $p^k \equiv 1 \pmod 4$ and hence $3 \cdot 2^t \equiv 2 \pmod 4$. This yields $t = 1$ and $p^k = 5$. If k is odd, then

$$3 \cdot 2^t = (p + 1)(p^{k-1} - p^{k-2} + \cdots + 1) .$$

The second factor on the right is a sum of an odd number of odd terms and is therefore odd. Thus $(p^k + 1)/(p + 1) = 1$ or 3. This has no solution for $k > 1$ and $p \neq 2$ so $k = 1$ and a is a prime.

If $a = 2$, then $\mathfrak{G} \subseteqq GL(2, 2) = \mathscr{T}(2, 2)$. The cases $a = 3, 5, 7$ are allowable exceptions so we assume $a > 7$. We show now that $p \nmid |\mathfrak{G}|$. Now $\mathfrak{G} \subseteqq GL(2, p)$ and hence if $\mathfrak{G}$ has two distinct subgroups of order p then $\mathfrak{G} \supseteqq SL(2, p)$. Since $p \geqq 5$, $SL(2, p)$ is nonsolvable, a contradiction. Thus if $p \| |\mathfrak{G}|$, then the Sylow p-subgroup of $\mathfrak{G}$ is normal. In $GL(2, p)$ the normalizer of a Sylow p-subgroup has order $(p - 1)^2 p$. Since $p + 1 \| |\mathfrak{G}|$ this yields $(p + 1) | (p - 1)^2 p$, a contradiction for $p > 3$. Thus $p \nmid |\mathfrak{G}|$.

If $\mathfrak{G}$ is reducible, then $|\mathfrak{G}| | (p-1)^2$, a contradiction. If $\mathfrak{G}$ is imprimitive, then $|\mathfrak{G}| | 2(p-1)^2$, a contradiction for $p > 7$. Thus $\mathfrak{G}$ is an irreducible, primitive linear group. We can clearly assume that $\mathfrak{G}$ is nonabelian. This implies easily that $\boldsymbol{Z}(\mathfrak{G})$ consists of scalar matrices and $|\boldsymbol{Z}(\mathfrak{G})| | (p-1)$. Also every normal abelian subgroup of $\mathfrak{G}$ is cyclic. Now the representation of $\mathfrak{G}$ is realizeable over the complex numbers and hence the results of [11] (Chapter X) apply. Since $\mathfrak{G}$ is solvable, we cannot have $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq A_5$. If $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G})$ is cyclic, then $\mathfrak{G}$ is abelian, a contradiction. If $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G})$ has a cyclic subgroup of index 2, then $\mathfrak{G}$ has a normal abelian subgroup $\mathfrak{A}$ of index 2. Then $\mathfrak{A}$ is cyclic and since $\mathfrak{G}$ is primitive, $\mathfrak{A}$ is irreducible. Thus by Hilfssatz 2 of [8], $\mathfrak{G} \subseteq \mathscr{T}(2, p)$.

There remains only $|\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G})| = 12$ or 24 and hence $|\mathfrak{G}| | 24(p-1)$ so $(p+1) | 24(p-1)$. This yields $p+1 | 48$ and since $p > 7$ we have $p = 11, 23$ or 47. Note that if we assume in addition that $2(p+1) | |\mathfrak{G}|$ then $p = 47$ does not occur. This completes the proof of this theorem.

EXAMPLES. Let $\mathfrak{G}$ act faithfully on vector space $\mathfrak{V}$ of order p^n. If $\mathfrak{G}$ is transitive on $\mathfrak{V}^\#$, then certainly $(p^n-1) | |\mathfrak{G}|$. Thus we can find examples for the exceptional cases $(n, a) = (2, 3)$, $(2, 5)$, $(2, 7)$, $(2, 11)$, $(2, 23)$ and $(4, 3)$ in [8]. The remaining two exceptions are $(n, a) = (6, 2)$ and $(2, 47)$. Clearly $\mathscr{T}(3, 2) \times \mathscr{T}(3, 2) \subseteq GL(6, 2)$ and $|\mathscr{T}(3, 2) \times \mathscr{T}(3, 2)| = 3^2 \cdot 7^2 = 7(2^6 - 1)$. This group is not a subgroup of $\mathscr{T}(6, 2)$ since $7^2 \nmid |\mathscr{T}(6, 2)|$. Now consider $(n, a) = (2, 47)$. It is easy to see that $GL(2, 47)$ contains an isomorphic copy of $SL(2, 3)$. Let $\mathfrak{D}$ be the Sylow 2-subgroup of the latter group so that $\mathfrak{D}$ is quaternion of order 8. It is easy to see that in $GL(2, 47)$, $C(\mathfrak{D})$ consists of scalar matrices. Now $N(\mathfrak{D})$ picks up a group of order 3 from $SL(2, 3)$ and a factor of 2 from some Sylow 2-subgroup containing $\mathfrak{D}$. Thus $8 \cdot 2 \cdot 3 = 48 | |N(\mathfrak{D})|$. Since $|N(\mathfrak{D})/\mathfrak{D}C(\mathfrak{D})| \leqq 6$ we see that $\mathfrak{G} = N(\mathfrak{D})$ is a solvable subgroup of $GL(2, 47)$ with $48 | |\mathfrak{G}|$ and $\mathfrak{G} \supseteq SL(2, 3)$. Since the Sylow 3-subgroup of $\mathscr{T}(2, 47)$ is normal, we cannot have $\mathfrak{G} \subseteq \mathscr{T}(2, 47)$. Thus Theorem 3.1 is best possible.

It is convenient here to consider some of the above exceptions.

LEMMA 3.2. *Let $\mathfrak{G}$ be a solvable subgroup of $GL(n, a)$. If $(n, a) = (2, 47)$ and $2(a+1) | |\mathfrak{G}|$ or if $(n, a) = (6, 2)$, $(a^n - 1) | |\mathfrak{G}|$ and $\mathfrak{G}$ is irreducible and primitive, then $\mathfrak{G} \subseteq \mathscr{T}(n, a)$.*

Proof. The result on $(n, a) = (2, 47)$ follows from the last sentence of the proof of Theorem 3.1. Now let $(n, a) = (6, 2)$ so $63 = 2^6 - 1$ divides $|\mathfrak{G}|$. Since $\mathfrak{G}$ is irreducible by assumption $\boldsymbol{O}_2(\mathfrak{G}) = \langle 1 \rangle$. Now $\mathfrak{G} \subseteq GL(6, 2)$ so $|\mathfrak{G}| | 2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$. We show first that $\boldsymbol{O}_7(\mathfrak{G}) \neq \langle 1 \rangle$.

If not, then since $7 \mid\mid \mathfrak{G}$ there would exist a subgroup $\mathfrak{Q}$ of order 7 which does not centralize some subgroup $\mathfrak{R} = \boldsymbol{O}_r(\mathfrak{G})$. Since $r \neq 2$ and 7 does not divide $5 - 1$, $31 - 1$ or $3^j - 1$ with $j \leqq 4$, we have a contradiction. Thus $\mathfrak{D} = \boldsymbol{O}_7(\mathfrak{G}) \neq \langle 1 \rangle$. Clearly the representation restricted to $\mathfrak{D}$ breaks up into two 3-dimensional irreducible constituents. If these are inequivalent then $\mathfrak{G}$ is imprimitive, a contradiction. Thus the irreducible constituents of ϑ are equivalent and hence ϑ is cyclic and $|\mathfrak{D}| = 7$.

If $\mathfrak{D}$ is the Fitting subgroup of $\mathfrak{G}$, then $\mathfrak{G}/\mathfrak{D}$ is conta ned in Aut ϑ and $|\mathfrak{G}| \mid 7 \cdot 6$, a contradiction. Thus there exists a normal abelian r-subgroup $\mathfrak{R} \neq \langle 1 \rangle$ of $\mathfrak{G}$ for some prime $r \neq 2, 7$. Set $\mathfrak{A} = \mathfrak{R}\mathfrak{D}$ so that $\mathfrak{A}$ is a normal abelian subgroup of $\mathfrak{G}$. By Clifford's theorem, the irreducible constituents of the representation of $\mathfrak{G}$ restricted to $\mathfrak{A}$ all have equal degree d with $d \mid 6$. Since $\mathfrak{A} \supseteq \mathfrak{D}$ we have $d \geqq 3$ so either $d = 3$ or 6. Now $d = 3$ leads to a contradiction since $\mathfrak{D}$ is self centralizing in each of its 3-dimensional representations and $\mathfrak{R} \neq \langle 1 \rangle$. Thus $d = 6$, $\mathfrak{A}$ is irreducible and $\mathfrak{G} \subseteq \mathscr{T}(n, a)$ by Hilfssatz 2 of [8].

We will need the following result in a later paper. We include it here because its proof follows quickly from the results of § 1.

PROPOSITION 3.3. Let $\mathfrak{G}$ be a subgroup of $\mathscr{T}(n, a)$ and suppose that $\mathfrak{G}$ acts 1/2-transitively but not semiregularly on $GF(p^n)^\sharp$. Let $\tilde{\mathfrak{G}}$ denote the subgroup of $\mathfrak{G}$ consisting of linear transformations (that is, functions of the form $x \to bx$) and let $|\mathfrak{G}_x| = k$ for $x \neq 0$. Then

(i) For all $x \neq 0$, $\mathfrak{G}_x$ is cyclic and $k \mid n$.

(ii) If σ is a field automorphism of order k, then

$$\tilde{\mathfrak{G}} \supseteq \{b^{1-\sigma}x \mid b \in GF(p^n)^\sharp\} .$$

(iii) With the exception of $p^n = 3^2$ and $|\mathfrak{G}| = 8$ we have $\tilde{\mathfrak{G}} = \boldsymbol{C}_{\mathfrak{G}}(\mathfrak{G}')$.

(iv) $\tilde{\mathfrak{G}}$ is characteristic in $\mathfrak{G}$.

Proof. $\mathfrak{T} = \mathscr{T}(n, p)$ is transitive on $\mathfrak{V}^\sharp = GF(p^n)^\sharp$ and hence the groups $\mathfrak{T}_v$ are all conjugate in $\mathfrak{T}$. Let τ be a field automorphism of order n. Then $\mathfrak{T}_1 = \langle x^\tau \rangle$ is cyclic of order n and hence all $\mathfrak{T}_v$ are cyclic of order n.

Now $\mathfrak{T}_v \supseteq \mathfrak{G}_v$ so $\mathfrak{G}_v$ must be the unique subgroup of order k of $\mathfrak{T}_v$. Thus (i) follows. It is easy to see that

$$\mathfrak{T}_v = \{v^{1-\tau^i}x^{\tau^i} \mid i = 1, 2, \cdots, n\}$$

and hence if σ is a field automorphism of order k, then $\mathfrak{G}_v = \{v^{1-\sigma^i}x^{\sigma^i}\}$. Thus for all $b \in GF(p^n)^\sharp$, $\mathfrak{G}$ contains the elements $x^{\sigma-1}$ and $b^{1-\sigma}x^\sigma$ and hence their product $b^{1-\sigma}x$ is in $\mathfrak{G}$. This yields (ii).

Certainly $\mathfrak{G}' \subseteq \tilde{\mathfrak{G}}$ and $\tilde{\mathfrak{G}} \subseteq C_{\mathfrak{G}}(\mathfrak{G}')$. Now if ρ is a field automorphism then $(dx^\rho, cx) = c^{1-\rho}x$. This shows that $\mathfrak{G}' \supseteq \{b^{(1-\sigma)^2}x \mid b \in GF(p^n)^\#\}$ and if dx^ρ centralizes $\mathfrak{G}'$, then for all $b \in \mathfrak{M} = GF(p^n)^\#$ we have $b^{(1-\sigma)^2(1-\rho)} = 1$. Since $\sigma \neq 1$, Corollary 1.3 and Lemma 1.4 show that $\rho = 1$ unless $p^n = 2^6$ or $p^n = 3^2$. Suppose $p^n = 2^6$. If $2 \mid\mid \mathfrak{G}\mid$, then since $p = 2$ some element of $\mathfrak{G}$ of order 2 has a fixed point so we can assume σ has order 2. If $2 \nmid \mid \mathfrak{G}\mid$ then both σ and ρ have odd order. From $(1-\sigma)^2(1-\rho) = 0$, Lemma 1.4 and $\sigma \neq 1$ we obtain $\rho = 1$. Suppose $p^n = 3^2$. Now $|\mathscr{T}(2, 3)| = 16$ and $\mathscr{T}(2, 3)$ is semi-dihedral. Thus (iii) clearly follows.

Certainly (iv) follows from (iii) in all cases except for $p^n = 3^2$, $|\mathfrak{G}| = 8$. Here since $\mathfrak{G}$ acts 1/2-transitively but not semiregularly we have $\mathfrak{G}$ dihedral. Since $\tilde{\mathfrak{G}}$ is cyclic and $[\mathfrak{G}: \tilde{\mathfrak{G}}] = 2$, (iv) follows.

4. Transitive linear groups.

THEOREM 4.1. *Let p be a prime and $a = p^k$. Suppose $\mathfrak{G}$ is a p-solvable subgroup of $GL(n, a)$ which transitively permutes the d-dimensional $GF(a)$-subspaces of the underlying vector space for some d with $1 \leqq d \leqq n-1$. Then we have one of the following.*

(i) $\mathfrak{G} \subseteq \mathscr{T}(n, a)$

(ii) *$\mathfrak{G}$ is solvable and $(n, a) = (2, 3), (2, 5), (2, 7), (2, 11), (2, 23)$ or $(4, 3)$*

(iii) *$\mathfrak{G}$ is nonsolvable and $(n, a) = (2, 11), (2, 19), (2, 29)$ or $(2, 59)$.*

Furthermore with the exception of $(n, a) = (5, 2)$ we have $d = 1$ or $n-1$.

Proof. Let $A(n, d)$ denote the number of d-dimensional subspaces of an n-dimensional vector space over $GF(a)$. Then

$$\begin{aligned} A(n, d) &= \frac{(a^n-1)(a^n-a)\cdots(a^n-a^{d-1})}{(a^d-1)(a^d-a)\cdots(a^d-a^{d-1})} \\ &= \frac{(a^n-1)(a^{n-1}-1)\cdots(a^{n-d+1}-1)}{(a^d-1)(a^{d-1}-1)\cdots(a-1)} \\ &= \frac{(a^n-1)}{(a^d-1)}A(n-1, d-1)\,. \end{aligned}$$

Thus since g.c.d $\{a^n-1, a^d-1\} = a^m-1$ where $m =$ g.c.d. $\{n, d\}$ we have

$$(a^n-1)/(a^m-1) \mid A(n, d)\,.$$

If $\mathfrak{G}$ acts transitively on these d-dimensional subspaces, then $A(n, d) \mid\mid \mathfrak{G}\mid$ so $(a^n-1)/(a^m-1) \mid\mid \mathfrak{G}\mid$.

Let $\mathfrak{G}$ act on vector space $\mathfrak{V}$ and let $\mathfrak{V}_0, \mathfrak{V}_1, \cdots, \mathfrak{V}_t$ be subspaces with $\mathfrak{V} = \mathfrak{V}_0 + \mathfrak{V}_1 + \cdots + \mathfrak{V}_t$. Suppose that $\mathfrak{V}_1 \neq \langle 0 \rangle, \mathfrak{V}$ and that if $g \in \mathfrak{G}$, then $\mathfrak{V}_i g = \mathfrak{V}_{i'}$ where $i \to i'$ is a permutation of $\{1, 2, \cdots, t\}$. If $\dim \mathfrak{V}_1 = w \geqq d$, then the images under $\mathfrak{G}$ of a fixed d-dimensional subspace of $\mathfrak{V}_1$ are each contained in some $\mathfrak{V}_i$. Thus clearly $\mathfrak{G}$ is not transitive on all d-dimensional subspaces of $\mathfrak{V}$. On the other hand if $d \geqq w$, then the images of a fixed d-dimensional subspace of $\mathfrak{V}$ containing $\mathfrak{V}_1$ each contain some $\mathfrak{V}_i$ with $i \neq 0$. Since we can easily construct a linear functional λ of $\mathfrak{V}$ whose kernel does not contain any $\mathfrak{V}_i (i \neq 0)$, it is clear that there is a d-dimensional subspace of $\mathfrak{V}$ which does not contain any $\mathfrak{V}_i (i \neq 0)$. Thus again $\mathfrak{G}$ is not transitive, a contradiction. This shows that $\mathfrak{G}$ is irreducible on $\mathfrak{V}$ and primitive. Hence $O_p(\mathfrak{G}) = \langle 1 \rangle$.

Case 1. We assume now that $\mathfrak{G}$ is solvable.

Since $(a^n - 1)/(a^m - 1) \,|\, |\mathfrak{G}|$, Theorem 3.1 applies. Suppose first that $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$ so that we have (i). We show here that $d = 1$ or $n - 1$ except if $(n, a) = (5, 2)$. If $n = 2$ or 3, then certainly $d = 1$ or $n - 1$. So we can assume $n \geqq 4$. Since $\mathfrak{G}$ is transitive on these subspaces, so is $\mathscr{T}(n, a)$. From

$$A(n, d)/A(n, d - 1) = (a^{n-d+1} - 1)/(a^d - 1)$$

we see easily that if $2 \leqq d \leqq n - 2$, then $A(n, d) \geqq A(n, 2)$. Further, the cyclic subgroup of $\mathscr{T}(n, a)$ of order $a - 1$ consisting of scalar matrices fixes all subspaces so

$$\begin{aligned} n(a^n - 1) = |\mathscr{T}(n, a)| &\geqq (a - 1)A(n, d) \\ &\geqq (a - 1)A(n, 2) = (a^n - 1)(a^{n-1} - 1)/(a^2 - 1) . \end{aligned}$$

Hence $n \geqq (a^{n-1} - 1)/(a^2 - 1) > a^{n-3}$. Since $n \geqq 4$, we see easily that only $(n, a) = (4, 3), (4, 2), (5, 2)$ can occur. Now with $(n, a) = (4, 3), (4, 2)$ we do not have $A(n, d) \,|\, n(a^n - 1)$ so that the only exception here is $(n, a) = (5, 2)$.

We consider the remaining possibilities in the conclusion of Theorem 3.1. Note that if $n = 2$, then $d = 1$. If $(n, a) = (2, 3), (2, 5), (2, 7), (2, 11), (2, 23)$ or $(4, 3)$, then we have (ii). It remains to show the following three facts: (1) if $(n, a) = (2, 47)$, then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$, (2) if $(n, a) = (4, 3)$ then $d = 1$ or 3, (3) if $(n, a) = (6, 2)$ then $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$.

Let $(n, a) = (2, 47)$ and let $\mathfrak{Z}$ denote the group of scalar matrices in $GL(n, a)$. By replacing $\mathfrak{G}$ by $\mathfrak{G}\mathfrak{Z}$ if necessary, we can assume that $\mathfrak{G} \supseteqq \mathfrak{Z}$. Then clearly $\mathfrak{G}$ is transitive on the nonzero vectors and so $(47^2 - 1) \,|\, |\mathfrak{G}|$. By Lemma 3.2, $\mathfrak{G} \subseteqq \mathscr{T}(n, a)$.

Now let $(n, a) = (4, 3)$ and assume that $d \neq 1, n - 1$. Then $d = 2$ and $A(4, 2) = 130$ divides $|\mathfrak{G}|$. Let $\mathfrak{Q}$ be a Sylow 13-subgroup of $\mathfrak{G}$.

Since $13^2 \nmid |GL(4, 3)|$, we have $|\mathfrak{Q}| = 13$. If $\mathfrak{Q} \triangle \mathfrak{G}$, then since $\mathfrak{G}$ is irreducible all constituents of the representation restricted to $\mathfrak{Q}$ have the same degree by Clifford's theorem. Since the nonprincipal irreducible representations of $\mathfrak{Q}$ over $GF(3)$ have degree 3, this is a contradiction. Thus $\mathfrak{Q}$ is not normal and by Fitting's theorem, there exists $\mathfrak{R} = \boldsymbol{O}_r(\mathfrak{G})$ which is not centralized by $\mathfrak{Q}$. Since $\boldsymbol{O}_p(\mathfrak{G}) = \langle 1 \rangle$, $r \neq p$ and we can view $\mathfrak{R}\mathfrak{Q}$ as a complex linear group of degree 4. By [10], $\mathfrak{Q} \triangle \mathfrak{R}\mathfrak{Q}$ and $\mathfrak{Q}$ centralizes $\mathfrak{R}$, a contradiction.

Finally let $(n, a) = (6, 2)$. If $d \neq 1$ or 5 then $31 \mid A(n, d)$. The same argument as above, with 31 the prime of interest, yields a contradiction. Thus $d = 1$ or 5 and $63 \mid\mid |\mathfrak{G}|$. Since $\mathfrak{G}$ is primitive, the result follows from Lemma 3.2.

Case 2. We assume now that $\mathfrak{G}$ is nonsolvable.

Since $(a^n - 1)/(a^m - 1) \mid\mid |\mathfrak{G}|$, Theorem 2.1 applies. If $(n, a) = (2, 11)$, $(2, 19)$, $(2, 29)$ or $(2, 59)$ then we have (iii) and also $d = 1$. We need only show that $(n, a) = (6, 5)$ with $m = 3$ does not occur here. Assume we have this possibility. Since $m = \text{g.c.d.}\{n, d\}$ we must have $d = 3$. Then since $71 \mid A(6, 3)$ we have $71 \mid\mid |\mathfrak{G}|$. Let $\mathfrak{Q}$ be a Sylow 71-subgroup of $\mathfrak{G}$. Since $71^2 \nmid |GL(6, 5)|$ we have $|\mathfrak{Q}| = 71$. If $\mathfrak{Q} \triangle \mathfrak{G}$, then since $\mathfrak{G}$ is irreducible, all constituents of this representation restricted to $\mathfrak{Q}$ have the same degree by Clifford's theorem. Since the nonprincipal representations of $\mathfrak{Q}$ over $GF(5)$ have degree 5, this is a contradiction. Thus $\mathfrak{Q}$ is not normal in $\mathfrak{G}$.

Let $\mathfrak{R} = \boldsymbol{O}_{p'}(\mathfrak{G})$ and consider $\mathfrak{R}\mathfrak{Q}$ as a complex linear group of degree 6. Since $71 > (2 \cdot 6) + 1$, $\mathfrak{Q} \triangle \mathfrak{R}\mathfrak{Q}$ by [7]. If $\mathfrak{Q} \subseteq \mathfrak{R}$, then since $\mathfrak{Q}$ is characteristic in $\mathfrak{R}$ we have $\mathfrak{Q} \triangle \mathfrak{G}$, a contradiction. If $\mathfrak{Q} \not\subseteq \mathfrak{R}$, then $\mathfrak{Q}$ centralizes $\mathfrak{R}$ and this contradicts the fact that $\mathfrak{G}$ is p-solvable, $\boldsymbol{O}_p(\mathfrak{G}) = \langle 1 \rangle$ and $\mathfrak{R} = \boldsymbol{O}_{p'}(\mathfrak{G})$. This completes the proof of the theorem.

EXAMPLE. Consider $\mathfrak{G} = \mathscr{T}(5, 2)$ so that $|\mathfrak{G}| = 5 \cdot 31$. Now the subgroup of $\mathfrak{G}$ of order 31 acts irreducibly and each subgroup of order 5 centralizes a 1-dimensional space and acts irreducibly on a 4-dimensional complement. Thus if $d = 2$ or 3, then $\mathfrak{G}$ acts semiregularly on the d-dimensional subspaces. Since $A(5, 2) = A(5, 3) = 5 \cdot 31 = |\mathfrak{G}|$, we see that $\mathfrak{G}$ is infact transitive. Thus the result on d above is best possible.

We use the notation of [12] and [13] now. Our study of solvable 1/2-transitive linear groups was split into two parts according to whether the linear groups were primitive or imprimitive. We show now that we can drop the solvability assumption in the latter case.

THEOREM 4.2. *Let $\mathfrak{G}$ act faithfully on vector space $\mathfrak{V}$ over $GF(p)$*

and let $\mathfrak{G}$ *act* 1/2*-transitively but not semiregularly on* $\mathfrak{V}^\sharp$. *If* $\mathfrak{G}$ *is imprimitive as a linear group, then* $\mathfrak{G}$ *satisfies one of the following.*

(i) $\mathfrak{G} = \mathscr{T}_0(p^n)$ *with* $p \neq 2$ *and* n *an integer*

(ii) $|\mathfrak{V}| = 3^4$ *and* $\mathfrak{G}$ *is isomorphic to a central product of the dihedral and quaternion groups of order* 8.

(iii) $|\mathfrak{V}| = 2^6$ *and* $\mathfrak{G}$ *is isomorphic to the dihedral group of order* 18 *with cyclic Sylow* 3*-subgroup.*

Proof. By Theorem 1 of [9], $\mathfrak{G}$ acts irreducibly on $\mathfrak{V}$ and by assumption $\mathfrak{G}$ acts imprimitively. If we show that $\mathfrak{G}$ is solvable, then the result follows from Proposition 1.3 of [13]. We proceed to do this now. By Proposition 1.1 of [13] we can assume that the representation of $\mathfrak{G}$ is induced from that of a subgroup $\mathfrak{H}$ with $[\mathfrak{G}: \mathfrak{H}] = 2$ and hence $\mathfrak{H} \triangle \mathfrak{G}$. Moreover if $\mathfrak{V} = \mathfrak{V}_1 + \mathfrak{V}_2$ as $\mathfrak{H}$-modules, then $\mathfrak{V}_1$ and $\mathfrak{V}_2$ are conjugate under $\mathfrak{G}$. Let $\mathfrak{K}_i$ be the kernel of the action of $\mathfrak{H}$ on $\mathfrak{V}_i$. Then $\mathfrak{H}/\mathfrak{K}_i$ acts transitively on $\mathfrak{V}_i^\sharp$ and $|\mathfrak{K}_i| \leqq 2$. Moreover for all $x \in \mathfrak{V}^\sharp$, $\mathfrak{G}_x$ is a 2-group.

Case 1. $p = 2$.

Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{G}$. Since $p = 2$ we see that $\mathfrak{S}$ must fix a point $x \in \mathfrak{V}^\sharp$. Thus since $\mathfrak{G}_x$ is a 2-group, we have $\mathfrak{G}_x = \mathfrak{S}$. Hence since $\mathfrak{G}$ acts 1/2-transitively on $\mathfrak{V}^\sharp$, we see that for all $x \in \mathfrak{V}^\sharp$, $\mathfrak{G}_x$ is a Sylow 2-subgroup of $\mathfrak{G}$. This clearly implies that for all x, $[\mathfrak{G}_x: \mathfrak{H}_x] = 2$. On the other hand if $x \in \mathfrak{V}_1^\sharp$, then clearly $\mathfrak{G}_x \subseteqq \mathfrak{H}$ so $\mathfrak{G}_x = \mathfrak{H}_x$. This is a contradiction and thus $p \neq 2$.

Case 2. $p \neq 2$.

If $p \mid |\mathfrak{G}|$, then a Sylow p-subgroup of $\mathfrak{G}$ would have a fixed point in $\mathfrak{V}^\sharp$ and this contradicts the fact that $\mathfrak{G}_x$ is a 2-group for all $x \in \mathfrak{V}^\sharp$. Thus $p \nmid |\mathfrak{G}|$. Since $\mathfrak{H}/\mathfrak{K}_i$ transitively permutes the 1-dimensional subspaces of $\mathfrak{V}_i$ we see by Theorem 4.1 that either $\mathfrak{H}/\mathfrak{K}_i$ is solvable or $|\mathfrak{V}_i| = 11^2, 19^2, 29^2$ or 59^2. We assume now that $\mathfrak{G}$ is not solvable. Then $\mathfrak{H}/\mathfrak{K}_i$ is not solvable and if $\bar{\mathfrak{H}} = \mathfrak{H}/\mathfrak{K}_1$, then $|\bar{\mathfrak{H}}| = 60\,a$ with $a \mid p - 1$ and $[\bar{\mathfrak{H}}: \bar{\mathfrak{H}}_x] = p^2 - 1$. If $|\bar{\mathfrak{H}}_x| = b$, then $(p^2 - 1)b = 60a$. Using the fact that $a \mid p - 1$ and b is a power of 2 we have

$$\begin{array}{lll} p = 11 & a = 2 & b = 1 \\ p = 19 & a = 6 & b = 1 \\ p = 29 & a = 14 & b = 1 \\ & a = 28 & b = 2 \\ p = 59 & a = 58 & b = 1\,. \end{array}$$

Case 3. $b = 1$.

Since $\mathfrak{G}$ is not semiregular, $b = 1$ yields $|\mathfrak{K}_1| = |\mathfrak{K}_2| = 2$ and $\mathfrak{H}/\mathfrak{K}_i$ acts regularly on $\mathfrak{V}_i^\#$. Further, the third subgroup of order 2 of $\langle \mathfrak{K}_1, \mathfrak{K}_2 \rangle$ is clearly a central subgroup of $\mathfrak{G}$ of order 2. The arguments of the second and third paragraphs of the proof of Proposition 1.3 of [13] show that $\mathfrak{H}$ is solvable, a contradiction.

Case 4. $b = 2$.

We must have $p = 29, a = 28$ here. Suppose first that $|\mathfrak{K}_i| = 2$. Then for all $x \in \mathfrak{V}^\#$, $|\mathfrak{G}_x| = 4$ and hence $|\mathfrak{H}_x| = 2$ or 4. Thus every element of $\mathfrak{V}^\#$ is fixed by some involution of $\mathfrak{H}$. Let $\mathfrak{J}$ denote the set of these involutions. If $g \in \mathfrak{J}$, then g cannot fix all of $\mathfrak{V}_1$ unless $g \in \mathfrak{K}_1^\#$. But $\mathfrak{K}_1^\#$ acts without fixed points on $\mathfrak{V}_2$. Thus no involution of $\mathfrak{H}$ can fix more than a 2-dimensional subspace of $\mathfrak{V}$. This yields easily

$$(p^4 - 1) = |\mathfrak{V}^\#| \leqq |\mathfrak{J}|(p^2 - 1)$$

and $p^2 + 1 \leqq |\mathfrak{J}|$. We have $|\mathfrak{H}| = 4(p^2 - 1)$ and $\mathfrak{H} = \mathfrak{W}\mathfrak{L}$ where $\mathfrak{L}$ is a central subgroup of order 7, since $\mathfrak{L}$ is central in each $\mathfrak{H}/\mathfrak{K}_i$, and $|\mathfrak{W}| = 4(p^2 - 1)/7$. Certainly $\mathfrak{J} \subseteq \mathfrak{W}$ so

$$p^2 + 1 \leqq |\mathfrak{J}| \leqq |\mathfrak{W}| = 4(p^2 - 1)/7 ,$$

a contradiction. Thus we cannot have $|\mathfrak{K}_i| = 2$.

Now let $|\mathfrak{K}_i| = 1$ so that for all $x \in \mathfrak{V}^\#$, $|\mathfrak{G}_x| = 2$. Now $2 | a$ so that $2 | |\boldsymbol{Z}(\mathfrak{H})|$. Also $\boldsymbol{Z}(\mathfrak{H})$ is cyclic, since $\mathfrak{H}$ acts faithfully and irreducibly on $\mathfrak{V}_i$. Thus $\mathfrak{G}$ has a normal and hence central subgroup of order 2. By Lemma 6 of [9], $|\mathfrak{J}| = p^2 + 1$ where $\mathfrak{J}$ denotes the set of noncentral involutions of $\mathfrak{G}$. Now $|\mathfrak{H}| = 2(p^2 - 1)$ and $\mathfrak{H} = \mathfrak{W}\mathfrak{L}$ where $\mathfrak{L}$ is central of order 7 and $|\mathfrak{W}| = 2(p^2 - 1)/7 = 240$. By Lemma 6 of [9] applied to $\mathfrak{H}$ on $\mathfrak{V}_1$ we see that $\mathfrak{H}$ has $p + 1$ noncentral involutions. Thus $|\mathfrak{J} - (\mathfrak{J} \cap \mathfrak{H})| = p^2 - p$.

Let $g \in \mathfrak{J} - (\mathfrak{J} \cap \mathfrak{H})$. Then $kg \in \mathfrak{J}$ with $k \in \mathfrak{H}$ if and only if $k^g = k^{-1}$. Thus g sends precisely $p^2 - p$ elements of $\mathfrak{H}$ to their inverses by conjugation. Since $p^2 - p > |\mathfrak{W}| = 240$ we see that g must act in a dihedral manner on $\mathfrak{L}$. Then g sends precisely $(p^2 - p)/7 = 116$ elements of $\mathfrak{W}$ to their inverses. Now $|\boldsymbol{Z}(\mathfrak{W})| = 4$ and $\mathfrak{W}/\boldsymbol{Z}(\mathfrak{W}) \simeq A_5$ so g acts on A_5 in such a way that at least $116/4 = 29$ elements map to their inverses. Since the automorphism group of A_5 is S_5 we see easily that no such automorphism of A_5 of order 1 or 2 exists with this property. This completes the proof.

We suspect that a result similar to Theorem 4.1 holds for p-solvable 1/2-transitive linear groups. A partial result in this direction is

THEOREM 4.3. *Let $\mathfrak{G}$ be a p-solvable group acting faithfully on*

vector space $\mathfrak{V}$ of order p^n. Suppose $\mathfrak{G}$ acts 1/2-transitively but not semiregularly on $\mathfrak{V}^\sharp$. If all the subgroups $\mathfrak{G}_x$ are conjugate in $\mathfrak{G}$, then $\mathfrak{G}$ satisfies one of the following.

(i) $\mathfrak{G} \subseteq \mathscr{T}(p^n)$

(ii) $\mathfrak{G}$ *is solvable and* $p^n = 3^2, 5^2, 7^2, 11^2$ *or* 3^4

(iii) $\mathfrak{G}$ *is nonsolvable and* $p^n = 11^2, 19^2$ *or* 29^2.

We need first the following lemma.

LEMMA 4.4. *Let $\mathfrak{G}$ be a p-solvable group of automorphisms of elementary abelian p-group $\mathfrak{V}$. Let $\mathfrak{K}$ be a p-complement in $\mathfrak{G}$. If $\mathfrak{G}$ acts 1/2-transitively on $\mathfrak{V}^\sharp$, then so does $\mathfrak{K}$. Moreover if all the groups $\mathfrak{G}_x$ are conjugate in $\mathfrak{G}$, then all the groups $\mathfrak{K}_x$ are conjugate in $\mathfrak{K}$.*

Proof. Let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}$. Since $\mathfrak{V}$ is a p-group, there exists $x \in \mathfrak{V}^\sharp$ with $\mathfrak{P} \subseteq \mathfrak{G}_x$. Since $\mathfrak{G}$ acts 1/2-transitively we see that for all $x \in \mathfrak{V}$, $\mathfrak{G}_x$ contains a Sylow p-subgroup of $\mathfrak{G}$.

Let $x \in \mathfrak{V}^\sharp$ and consider $\mathfrak{K}_x = \mathfrak{K} \cap \mathfrak{G}_x$. By the above $\mathfrak{G}_x$ contains some Sylow p-subgroups $\mathfrak{P}$ of $\mathfrak{G}$. Since $\mathfrak{G} = \mathfrak{P}\mathfrak{K}$ we have $\mathfrak{G} = \mathfrak{G}_x\mathfrak{K}$ and hence

$$|\mathfrak{K}_x| = |\mathfrak{K} \cap \mathfrak{G}_x| = |\mathfrak{G}_x||\mathfrak{K}|/|\mathfrak{G}|$$

is the same for all $x \in \mathfrak{V}^\sharp$. Thus $\mathfrak{K}$ acts 1/2-transitively on $\mathfrak{V}^\sharp$.

Suppose now that the groups $\mathfrak{G}_x$ are all conjugate in $\mathfrak{G}$. Let $x, y \in \mathfrak{V}^\sharp$ and let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}_x$ so that $\mathfrak{P}\mathfrak{K} = \mathfrak{G}$. If $\mathfrak{G}_x^k = \mathfrak{G}_y$ and $h = ak$ with $a \in \mathfrak{P}, k \in \mathfrak{K}$, then clearly $\mathfrak{G}_x^k = \mathfrak{G}_y$. Since $\mathfrak{K}_x = \mathfrak{G}_x \cap \mathfrak{K}$, $\mathfrak{K}_y = \mathfrak{G}_y \cap \mathfrak{K}$ we have $\mathfrak{K}_x^k = \mathfrak{K}_y$ and the result follows.

Proof of Theorem 4.3. We consider a series of cases.

Case 1. $\mathfrak{G}$ solvable.

Let $\mathfrak{N}$ be the Fitting subgroup of $\mathfrak{G}$ so that $\mathfrak{N} \triangle \mathfrak{G}$ and $\mathfrak{N} \neq \langle 1 \rangle$. If $x, y \in \mathfrak{V}^\sharp$, then $\mathfrak{N}_x = \mathfrak{N} \cap \mathfrak{G}_x$, $\mathfrak{N}_y = \mathfrak{N} \cap \mathfrak{G}_y$ so $\mathfrak{N}_x$ and $\mathfrak{N}_y$ are conjugate in $\mathfrak{G}$. Hence $\mathfrak{N}$ acts 1/2-transitively and Theorem II of [12] applies. The type (ii) groups, $\mathscr{T}_0(p)$ of that theorem do not satisfy our conjugacy assumption since the elements $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ are not conjugate in $\mathfrak{G}$. Thus we have (i) and (ii) above.

Case 2. $\mathfrak{G}$ nonsolvable.

Since $|\mathfrak{V}| = p^n$ we have $\mathfrak{G} \subseteq GL(n, p)$ and $\mathfrak{G}$ is p-solvable. For each $x \in \mathfrak{V}^\sharp$ we let $\mathfrak{V}_x = C_{\mathfrak{V}}(\mathfrak{G}_x)$. We see clearly that these groups

form a partition of $\mathfrak{V}$, that is $\mathfrak{V}^\# = \cup \mathfrak{V}_x^\#$ is a disjoint union. Now the groups $\mathfrak{G}_x$ are all conjugate in $\mathfrak{G}$ so that all the subgroups $\mathfrak{V}_x$ have the same order p^m and there are precisely $[\mathfrak{G}: N_{\mathfrak{G}}(\mathfrak{G}_x)]$ of them. Counting elements in the disjoint union then yields

$$(p^n - 1) = [\mathfrak{G}: N_{\mathfrak{G}}(\mathfrak{G}_x)](p^m - 1) .$$

Since $p^m - 1 \mid p^n - 1$ we have $m \mid n$. Furthermore $\mathfrak{G}$ does not act semiregularly so $m \neq n$. Since $(p^n - 1)/(p^m - 1) \mid\mid |\mathfrak{G}|$ and $\mathfrak{G}$ is non-solvable, Theorem 2.1 yields $p^n = 11^2, 19^2, 29^2, 59^2$ or $p^n = 5^6$ with $m = 3$.

Case 3. $p^n = 59^2$.

By Lemma 4.4 we can assume $\mathfrak{G}$ is a p'-group. Since $\mathfrak{G}/\boldsymbol{Z}(\mathfrak{G}) \simeq A_5$ and $(p - 1)/2$ is a prime not equal to 2, 3 or 5 we see that $\mathfrak{G} = \bar{\mathfrak{G}}\mathfrak{L}$ where $\mathfrak{L}$ is central of order 1 or $(p - 1)/2$ and $|\bar{\mathfrak{G}}| = 60$ or 120. Since $\mathfrak{L}$ acts semiregularly we see that $\mathfrak{G}_x = \bar{\mathfrak{G}}_x$ and these groups are all conjugate in $\bar{\mathfrak{G}}$. Clearly $m = 1$ so $[\bar{\mathfrak{G}}: N_{\bar{\mathfrak{G}}}(\bar{\mathfrak{G}}_x)] = p + 1 = 60$ and thus $|N_{\bar{\mathfrak{G}}}(\bar{\mathfrak{G}}_x)| = 2$. This is a contradiction since a subgroup of order 2 has a properly larger normalizer in some Sylow 2-subgroup of $\bar{\mathfrak{G}}$. Thus if $n = 2$ then only $p^n = 11^2, 19^2$ and 29^2 can occur with $\mathfrak{G}$ not semiregular.

Case 4. $p^n = 5^6$ with $m = 3$.

Here we have $(5^6 - 1)/(5^3 - 1) = 2 \cdot 3^2 \cdot 7$ dividing $|\mathfrak{G}|$. If also $31 \mid\mid |\mathfrak{G}|$, then $(5^6 - 1)/(5^2 - 1) = 3 \cdot 7 \cdot 31$ divides $|\mathfrak{G}|$ and $\mathfrak{G}$ is solvable, a contradiction. Hence $31 \nmid |\mathfrak{G}|$. By the previous lemma we can assume that $5 \nmid |\mathfrak{G}|$.

Suppose $x, y \in \mathfrak{V}^\#$ with $\mathfrak{G}_x \neq \mathfrak{G}_y$ and $g \in \mathfrak{G}_x \cap \mathfrak{G}_y$. Then g centralizes $\mathfrak{V}_x$ and $\mathfrak{V}_y$. Now $|\mathfrak{V}_x| = |\mathfrak{V}_y| = 5^3$ and $\mathfrak{V}_x \cap \mathfrak{V}_y = \langle 0 \rangle$ so $\mathfrak{V} = \mathfrak{V}_x + \mathfrak{V}_y$. Hence g centralizes $\mathfrak{V}$ and $g = 1$. Thus $\mathfrak{G}_x \cap \mathfrak{G}_y = \langle 1 \rangle$. Since $5 \nmid |\mathfrak{G}_x|$, $\mathfrak{G}_x$ acts on a 3-dimensional complement of $\mathfrak{V}_x$ and in fact $\mathfrak{G}_x$ acts semiregularly on this subspace since $\mathfrak{G}_x \cap \mathfrak{G}_y = \langle 1 \rangle$. Hence $|\mathfrak{G}_x| \mid (5^3 - 1)$. Now $5^3 - 1 = 4 \cdot 31$ and $31 \nmid |\mathfrak{G}|$ so $\mathfrak{G}_x$ is cyclic of order 2 or 4. From the fact that $\mathfrak{G}$ acts 1/2-transitively on $\mathfrak{V}^\#$ we have $[\mathfrak{G}: \mathfrak{G}_x] \mid (5^6 - 1)$ so $[\mathfrak{G}: \mathfrak{G}_x] \mid 2^3 \cdot 3^2 \cdot 7$. This and the above yields $|\mathfrak{G}| = 2^r \cdot 3^2 \cdot 7$ with $r \leqq 5$.

Set $\bar{\mathfrak{G}} = \mathfrak{G}/(\boldsymbol{O}_2(\mathfrak{G}))$. We show that for all primes q, $\boldsymbol{O}_q(\bar{\mathfrak{G}}) = \langle 1 \rangle$. This is clearly true for $q = 2$ and $q = 7$, the latter by Burnside's two prime theorem. From the fact that $\mathfrak{G}_x$ is a 2-group we see that the Sylow 3-subgroups of $\mathfrak{G}$ are cyclic. If $\boldsymbol{O}_3(\bar{\mathfrak{G}}) \neq \langle 1 \rangle$, then $\bar{\mathfrak{G}}$ has a normal subgroup $\bar{\mathfrak{L}}$ of order 3. By Burnside's transfer theorem $\boldsymbol{C}_{\bar{\mathfrak{G}}}(\bar{\mathfrak{L}})$ has a normal 3-complement and hence $\boldsymbol{C}_{\bar{\mathfrak{G}}}(\bar{\mathfrak{L}})$ is solvable. Since $[\bar{\mathfrak{G}}: \boldsymbol{C}_{\bar{\mathfrak{G}}}(\bar{\mathfrak{L}})] \leqq 2$, $\bar{\mathfrak{G}}$ is solvable, a contradiction. This implies that $\bar{\mathfrak{G}}$ has no nonidentity solvable normal subgroup.

Let $\overline{\mathfrak{W}}$ be a minimal normal subgroup of $\overline{\mathfrak{G}}$ so that $\overline{\mathfrak{W}}$ is a direct product of isomorphic simple groups. By the above $\overline{\mathfrak{W}}$ must be nonabelian. Since the order of a nonabelian simple group must have at least three distinct prime factors and $7^2 \nmid |\mathfrak{G}|$, we see that $\overline{\mathfrak{W}}$ is a nonabelian simple group. Now $C_{\overline{\mathfrak{G}}}(\overline{\mathfrak{W}}) \triangle \overline{\mathfrak{G}}$ and $C_{\overline{\mathfrak{G}}}(\overline{\mathfrak{W}}) \cap \overline{\mathfrak{W}} = \langle 1 \rangle$. Thus $7 \nmid |C_{\overline{\mathfrak{G}}}(\overline{\mathfrak{W}})|$ and so $C_{\overline{\mathfrak{G}}}(\overline{\mathfrak{W}})$ is solvable. This yields $C_{\overline{\mathfrak{G}}}(\overline{\mathfrak{W}}) = \langle 1 \rangle$.

Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{G}$ and let $\mathfrak{L}$ be the subgroup of order 2 of $\mathfrak{G}_x$. Since $\mathfrak{G}_x$ is a T.I. set, $N_{\mathfrak{G}}(\mathfrak{G}_x) = N_{\mathfrak{G}}(\mathfrak{L})$ and $[\mathfrak{G}: N_{\mathfrak{G}}(\mathfrak{L})] = 2 \cdot 3^2 \cdot 7$. In particular $\mathfrak{L}$ cannot be in the center of any Sylow 2-subgroup. This implies that the elements of order 2 in $Z(\mathfrak{S})$ act without fixed points on $\mathfrak{V}$. This shows that $Z(\mathfrak{S})$ is cyclic and the subgroup of $Z(\mathfrak{S})$ of order 2 is central in $\mathfrak{G}$. Thus $|O_2(\mathfrak{G})| \geqq 2$.

We have $|\overline{\mathfrak{W}}| = 2^s \cdot 3^t \cdot 7$ with $s = 2, 3, 4$ and $t = 1$ or 2. Suppose first that $t = 1$. By [2], $\overline{\mathfrak{W}} \simeq PSL(2, 7)$ and by Satz 1 of [14], $|\operatorname{Aut} \overline{\mathfrak{W}}| = 2 \cdot 168$. Since $\overline{\mathfrak{G}} \subseteq \operatorname{Aut} \overline{\mathfrak{W}}$ and $9 \| \mathfrak{G} |$, this is a contradiction. Now let $t = 2$ so that $|\overline{\mathfrak{W}}| = 252, 504$ or 1008. There is certainly no simple group of order 252, since by Sylow's theorem the Sylow 7-subgroup is either normal or in the center of its normalizer. By Theorem 10.7.5 of [15], there is no simple group of order 1008. This leaves only $|\overline{\mathfrak{W}}| = 504$. By [3] (§ III), $\overline{\mathfrak{W}} \simeq SL(2, 8)$.

We will derive a final contradiction by studying a Sylow 2-subgroup $\mathfrak{S}$ of $\mathfrak{G}$. We have already seen that $\mathfrak{S}$ is nonabelian with $Z(\mathfrak{S})$ cyclic. Note that the Sylow 2-subgroup of $\overline{\mathfrak{W}}$ is elementary abelian of order 8. The latter is normalized by a group of order 7 which permutes its involutions transitively. Suppose that $|O_2(\mathfrak{G})| \geqq 4$. Then $|O_2(\mathfrak{G})| = 4$ and $\overline{\mathfrak{W}} = \overline{\mathfrak{G}}$. The group $\overline{\mathfrak{W}}$ acts on $O_2(\mathfrak{G})$ and thus $\overline{\mathfrak{W}}$ centralizes $O_2(\mathfrak{G})$. Hence $O_2(\mathfrak{G})$ is central in $\mathfrak{G}$ and cyclic. Since the nonidentity elements of $\mathfrak{S}/O_2(\mathfrak{G})$ are permuted transitively by a group of order 7, it follows that $Z(\mathfrak{S}) = O_2(\mathfrak{G})$. Then $\mathfrak{S}$ is a class 2 group with a cyclic center and $[\mathfrak{S}: Z(\mathfrak{S})] = 2^3$. This is a contradiction since $\mathfrak{S}/Z(\mathfrak{S})$ has a nondegenerate symplectic geometry.

Now let $|O_2(\mathfrak{G})| = 2$ and let $\mathfrak{S}_0 = \mathfrak{S} \cap \mathfrak{W}$ where $\overline{\mathfrak{W}} = \mathfrak{W}/O_2(\mathfrak{G})$. From the nature of $\mathfrak{S}_0/O_2(\mathfrak{G})$ and the fact that this group admits an automorphism of order 7, we see that $\mathfrak{S}_0$ is elementary abelian of order 16. Since $[\mathfrak{S}: \mathfrak{S}_0] = 1$ or 2 we see that $Z(\mathfrak{S})$ contains a subgroup of type (2, 2), a contradiction. This completes the proof of the theorem.

5. Permutation groups. The results of the previous section translate naturally to theorems about permutation groups with regular normal subgroups. Again we use the notation of [13]. Thus we have groups $\mathscr{S}(p^n)$ and $\mathscr{S}_0(p^n)$ which are solvable and respectively 2- and

3/2-transitive permutation groups.

The following result at once combines the result of Huppert ([8]) on solvable 2-transitive groups and the result of Zassenhaus ([17]) on sharply 2-transitive groups.

THEOREM 5.1. *Let $\mathfrak{G}$ be a doubly transitive permutation group. Suppose that $\mathfrak{G}$ is p-solvable and $O_p(\mathfrak{G}) \neq \langle 1 \rangle$. Then* $\deg \mathfrak{G} = p^n$ *for some integer n and we have one of the following.*

(i) $\mathfrak{G} \subseteq \mathscr{S}(p^n)$

(ii) $\mathfrak{G}$ *is solvable and* $p^n = 3^2, 5^2, 7^2, 11^2, 23^2$ *or* 3^4

(iii) $\mathfrak{G}$ *is nonsolvable and* $p^n = 11^2, 19^2, 29^2$ *or* 59^2.

Proof. Let $\mathfrak{V}$ be a characteristic abelian subgroup of $O_p(\mathfrak{G})$. Then $\mathfrak{V} \neq \langle 1 \rangle$ and $\mathfrak{V} \triangle \mathfrak{G}$. Since $\mathfrak{G}$ is doubly transitive, $\mathfrak{V}$ is transitive and hence regular. If $\mathfrak{H} = \mathfrak{G}_a$, then $\mathfrak{G} = \mathfrak{V}\mathfrak{H}$ and $\mathfrak{H}$ acts transitively on $\mathfrak{V}^\#$. Also $\deg \mathfrak{G} = |\mathfrak{V}| = p^n$ and $\mathfrak{V}$ is a p-solvable subgroup of $GL(n, p)$. The result now follows by Theorem 4.1, since if $\mathfrak{H} \subseteq \mathscr{T}(n, p) = \mathscr{T}(p^n)$, then $\mathfrak{G} \subseteq \mathscr{S}(p^n)$.

EXAMPLES. Nonsolvable sharply 2-transitive groups exist with $p^n = 11^2, 29^2$ or 59^2 by [17]. Let $p^n = 19^2$. Then $GL(2, 19)$ contains $\mathfrak{H} = \bar{\mathfrak{H}}\mathfrak{Q}$ where $\mathfrak{Q}$ is a cyclic central subgroup of order 9 and $\bar{\mathfrak{H}} \simeq SL(2, 5)$. Moreover the elements of $\mathfrak{Q}^\#$ and $\bar{\mathfrak{H}}^\#$ all act fixed point free on $\mathfrak{V}$, a 2-dimensional space over $GF(19)$. Let $x \in \mathfrak{V}^\#$. From the nature of $\mathfrak{H}$ we see easily that $|\mathfrak{H}_x| \leqq 3$ and hence the orbit of x contains at least $|\mathfrak{H}|/3 = 9 \cdot 120/3 = 19^2 - 1$ elements. Thus $\mathfrak{H}$ is transitive on $\mathfrak{V}^\#$ and $\mathfrak{G}$, the semidirect product of $\mathfrak{V}$ by $\mathfrak{H}$, is a 19-solvable 2-transitive group of degree 19^2.

THEOREM 5.2. *Let $\mathfrak{G}$ be a 3/2-transitive permutation group which is not a Frobenius group. Let $\mathfrak{V} \neq \langle 1 \rangle$ be a normal abelian subgroup of $\mathfrak{G}$. Then $\mathfrak{V}$ is an elementary p-group and $\mathfrak{V}$ is a regular normal subgroup of $\mathfrak{G}$. Suppose that as a linear group on $\mathfrak{V}$, $\mathfrak{H} = \mathfrak{G}_a$ is imprimitive. Then $\mathfrak{G}$ satisfies one of the following.*

(i) $\mathfrak{G} = \mathscr{S}_0(p^n)$ *with $p \neq 2$ and n an integer*

(ii) $|\mathfrak{V}| = 3^4$, $\mathfrak{H}$ *is isomorphic to a central product of the dihedral and quaternion groups of order* 8, *and* $|\mathfrak{G}| = 2^5 \cdot 3^4$.

(iii) $|\mathfrak{V}| = 2^6$, $\mathfrak{H}$ *is isomorphic to the dihedral group of order* 18, *and* $|\mathfrak{G}| = 2^7 \cdot 3^2$.

Proof. Since $\mathfrak{G}$ is not a Frobenius group, it is primitive by Theorem 10.4 of [16]. This yields all the remarks concerning $\mathfrak{V}$. Now $\mathfrak{H}$ is a group of automorphisms of $\mathfrak{V}$ which acts 1/2-transitively but

not semiregularly on $\mathfrak{V}^\sharp$. Thus Theorem 4.2 applies to $\mathfrak{H}$ and the result follows.

THEOREM 5.3. *Let $\mathfrak{G}$ be a 3/2-transitive permutation group which is not a Frobenius group. Suppose $\mathfrak{G}$ is p-solvable with $\boldsymbol{O}_p(\mathfrak{G}) \neq \langle 1 \rangle$. If all the subgroups $\mathfrak{G}_{ab}$ are conjugate in $\mathfrak{G}$, then $\deg \mathfrak{G} = p^n$ for some integer n and $\mathfrak{G}$ satisfies one of the following.*

(i) $\mathfrak{G} \subseteq \mathscr{S}(p^n)$

(ii) *$\mathfrak{G}$ is solvable and $p^n = 3^2, 5^2, 7^2, 11^2$ or 3^4*

(iii) *$\mathfrak{G}$ is nonsolvable and $p^n = 11^2, 19^2$ or 29^2.*

Proof. Let $\mathfrak{V}$ be a characteristic elementary abelian subgroup of $\boldsymbol{O}_p(\mathfrak{G})$ with $\mathfrak{V} \neq \langle 1 \rangle$. Then $\mathfrak{V} \triangle \mathfrak{G}$. By Theorem 10.4 of [16], $\mathfrak{G}$ is primitive and hence $\mathfrak{V}$ is transitive. Thus $\mathfrak{V}$ is a regular normal subgroup of $\mathfrak{G}$. If $\mathfrak{H} = \mathfrak{G}_a$, then $\mathfrak{G} = \mathfrak{V}\mathfrak{H}$ and $\mathfrak{H}$ acts 1/2-transitively but not semiregularly on $\mathfrak{V}$.

Let b and c be points distinct from a. We show that $\mathfrak{G}_{ab}$ and $\mathfrak{G}_{ac}$ are conjugate in $\mathfrak{H}$. Since these groups are conjugate in $\mathfrak{G}$ by assumption and $\mathfrak{G} = \mathfrak{H}\mathfrak{V}$ we have $\mathfrak{G}_{ac} = \mathfrak{G}_{ab}^{hv}$ with $h \in \mathfrak{H}$, $v \in \mathfrak{V}$. Now $\mathfrak{V} \triangle \mathfrak{G}$ so $(v, \mathfrak{G}_{ab}^h) \subseteq \mathfrak{H} \cap \mathfrak{V} = \langle 1 \rangle$ and hence v centralizes $\mathfrak{G}_{ab}^h$. Thus $\mathfrak{G}_{ac} = \mathfrak{G}_{ab}^h$. If $x, y \in \mathfrak{V}^\sharp$, then the above implies that $\mathfrak{H}_x$ and $\mathfrak{H}_y$ are conjugate in $\mathfrak{H}$. Hence Theorem 4.3 applies to $\mathfrak{H}$ and the result follows.

The author would like to thank Professor Walter Feit for suggesting the problem studied here and for suggesting the general approach to its solution.

REFERENCES

1. R. Brauer, *On groups whose order contains a prime number to the first power* II, Amer. J. Math. **64** (1942), 421-440.

2. R. Brauer and H. F. Tuan, *On simple groups of finite order* I, Bull. Amer. Math. Soc. **51** (1945), 756-766.

3. F. N. Cole, *Simple groups as far as order* 660, Amer. J. Math. **15** (1893), 303-315.

4. L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly **12** (1905), 86-89.

5. W. Feit, *Groups which have a faithful representation of degree less than p-1*, Trans. Amer. Math. Soc. **112** (1964), 287-303.

6. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775-1029.

7. ———, *On groups which have a faithful representation of degree less than* (p-1)/2, Pacific J. Math. **4** (1961), 1257-1262.

8. B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. **68** (1957), 126-150.

9. I. M. Isaacs and D. S. Passman, *Half-transitive automorphism groups*, Canad. J. Math. **18** (1966), 1243-1250.

10. N. Ito, *On a theorem of H. F. Blichfeldt*, Nagoya Math. J. **5** (1953), 75-77.

11. G. A. Miller, H. F. Blickfeldt, and L. E. Dickson, *Finite Groups*, Dover Publications, New York, 1961.
12. D. S. Passman, *Solvable half transitive automorphism groups*, J. of Algebra **6** (1967), 285-304.
13. ———, *Solvable* 3/2 *transitive permutation groups*, J. of Algebra **7** (1967) 192-207
14. O. Schreier and B. L. van der Waerden, *Die Automorphismen der projectiven Gruppen*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 303-322.
15. W. R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964.
16. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, New York, 1964.
17. H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 187-220.

Received June 27, 1967.

YALE UNIVERSITY