TRANSITIVE LINEAR GROUPS AND LINEAR GROUPS WHICH CONTAIN IRREDUCIBLE SUBGROUPS OF PRIME ORDER*

§1. Introduction

Let $G$ be a group of linear transformations of a vector space $V$ of finite dimension $n$ over a field of finite order $q$. Furthermore, let $\Phi_n(q)$ be the $n$th cyclotomic polynomial evaluated at $q$ and

$$\Phi_n^*(q) = \frac{1}{f^2} \Phi_n(q),$$

where $f = (n, \Phi_n(q))$ and $f^2$ is the largest power of $f$ dividing $\Phi_n(q)$. In an earlier paper (Hering, 1968) the author proved that the structure of $G$ is very restricted if $(|G|, \Phi_n^*(q)) \neq 1$. Also, in all cases known to the author, $G$ has the property

(*) if $(|G|, \Phi_n^*(q)) \neq 1, n+1, 2n+1$ and $(n+1)(2n+1)$, then $G$ is solvable or essentially a Chevalley group (of ordinary or twisted type) operating on $V$ in the natural way.

In this paper we prove, that $G$ must have property (*) provided that $G$ has certain (unfortunately quite special) additional properties, as for example the property that some non-solvable composition factor of $G$ is isomorphic to one of the groups $PSL(n, \bar{q})$, $Sp(n, \bar{q})$ or $A_m$.

Suppose that $G$ operates transitively on the set of non-zero vectors of the underlying vector space $V$. Then $q^n - 1 \mid |G|$ and hence $\Phi_n^*(q) \mid |G|$. Furthermore, we can prove that $\Phi_n^*(q) \neq 1, n+1, 2n+1$ and $(n+1)(2n+1)$ unless either $n \leq 2$ or $n > 2$ and $|V|$ is equal to one of a certain finite number of exceptional degrees (see §3, Theorem 3.9). So, in general, we can assume that $(|G|, \Phi_n^*(q)) \neq 1, n+1, 2n+1$ and $(n+1)(2n+1)$. This fact enables us to use all results mentioned above to obtain information about finite transitive linear groups, i.e., linear groups which operate transitively on the non-trivial vectors of the underlying vector space (see §5). Finally, in §6 we summarize some corollaries concerning doubly transitive permutation groups.

A prime $p$ divides $(\Phi_n^*(q), |G|)$ if and only if $G$ contains an irreducible subgroup of order $p$. This establishes the relationship between our paper and the second part of the title.

* This research was supported by a National Science Foundation grant.
§2. Definitions and preliminary results

We shall in general use standard notation. If $G$ is a group, then $\mathcal{Z}G$ is the center of $G$, $F(G)$ the Fitting subgroup of $G$, $\Phi(G)$ the Frattini subgroup of $G$ and $G^*$ the set consisting of all elements in $G$ which are different from the identity. If $H$ is a subgroup of $G$, then $\mathcal{N}_G H$ is the normalizer of $H$ in $G$ and $\mathcal{C}_G H$ the centralizer of $H$ in $G$. Also, every factor group of $H$ will be called a factor of $G$. For each $p$-group $P$ we define $\Omega(P)$ to be the subgroup generated by all elements of order $p$ in $P$. The alternating group of degree $i$ will be denoted by $A_i$. If $V$ is a vector space over a field $K$, then $GL(V, K)$ is the group consisting of all non-singular $K$-linear transformations of $V$. Both ordinary and generalized quaternion groups will simply be called quaternion groups. A quaternion group of order $2^n$ will be denoted by $Q_{2^n}$.

Let $m$ and $n$ be integers and $p$ a prime. Then $(m, n)$ is the greatest common divisor of $m$ and $n$, while $\varphi(m)$ is the Euler number of $m$. Also, we write $m \mid n$ if $m$ divides $n$ and $p^m \mid n$ if $p^m$ divides $n$ but $p^{m+1}$ does not divide $n$.

This paper is a continuation of work started by the author in an article on doubly transitive groups published in 1968. As we shall frequently refer to this article, we shall denote it here by [TL]. Also, we shall often use some results on projective representations contained in a joint paper with M. E. Harris of 1971. This paper will be denoted by [PR].

**Lemma 2.1.** Let $G$ be a $p$-group such that every proper characteristic subgroup of $G$ is cyclic and contained in $\mathcal{Z}G$. Then one of the following statements holds:

(a) $G$ is cyclic.

(b) $G$ is elementary abelian.

(c) $G$ is extraspecial.

(d) $p=2$ and $G\cong T \cdot \mathcal{Z}G$, where $T$ is an extraspecial 2-group of order $> 8$, $\mathcal{Z}G$ a cyclic group of order 4, and $T \cap \mathcal{Z}G = \mathcal{Z}T$.

**Proof.** If $G$ is abelian but not elementary abelian, then $\Omega(G)$ is cyclic and hence $G$ is cyclic. Assume now that $G$ is not abelian. Clearly $G' \leq \Phi(G) \leq \mathcal{Z}G$, and $\mathcal{Z}G$ is cyclic. Hence $[a, b]^p = [a, b'^p] = 1$ for all $a, b \in G$. So $G'$ is elementary abelian. In fact $|G'| = p$, as $\mathcal{Z}G$ is cyclic. Suppose now that $G' < \Phi(G)$. Then the preimage of $\Omega(G/G')$ in $G$ is a proper characteristic subgroup and hence cyclic. Thus $G/G'$ and therefore $G$ itself is cyclic. Thus $\Phi(G) = G'$. Furthermore, $G' \leq \mathcal{Z}G$ implies that $(xy)^i = x^iy^{i}((y^{-1}x^{-1}y^{-1}x)^{i(t-1)/2}$ for $x, y \in G$ and $i \geq 0$ (see Huppert, 1967, p. 253, Hilfssatz 1.3). Let $B$ be the set of elements in $G$ of order at most $p$, if $p>2$, and of order at most 4, if $p=2$. Then by the above formula $B$ is a characteristic subgroup of $G$. If $B < G$, then $B$ is cyclic and hence $G$ is cyclic. Thus $B = G$, which implies that either $\mathcal{Z}G = G'$ or...
The first possibility leads to extraspecial groups. Assume that $|3G|=4$, and let $T/G'$ be a complement of $3G/G'$ in the elementary abelian group $G/G'$. Then clearly $G=T \cdot 3G$, $[T, 3G]=1$ and $T \cap 3G=G'$. Also $3T \leq 3G$, as $G=T \cdot 3G$. Thus $3T=G'$, and $T$ is extraspecial. Suppose now that $|T|=8$. As $B=G$, there exist elements $t_1$ and $t_2$ of order $4$ in $G$ such that $G=\langle t_1 \rangle \langle t_2 \rangle 3G$. Here the group $\langle t_1 \rangle \langle t_2 \rangle |G'$ is a complement of $3G/G'$ and hence by the above argument extra special. So $\langle t_1 \rangle \langle t_2 \rangle$ is a quaternion group. But this group is characteristic in $G$, as all elements of order $4$ of $G$ lie in $\langle t_1 \rangle \langle t_2 \rangle \cup 3G$. So $|T|=8$ is impossible.

LEMMA 2.2. Let $q$ be a power of a prime $p$, $s$ a prime different from $p$, and let $G$ be a subgroup of $GL(n, q)$. Suppose that $G$ contains a normal $s$-group $N$ such that $N=E \cdot 3N$, where $3N$ is cyclic and $E$ an extra special group of order $s^{2a+1}$. Then $n \geq s^a$. If $n=s^a$, then

(a) $E=3G$ and
(b) $G/E \cdot 3G$ is faithfully represented on $N/3N$.

Proof. As the center $3E$ of $E$ has order $s$, it is contained in every non-trivial normal subgroup of $E$. This implies that each completely reducible faithful representation of $E$ has an irreducible constituent $V_1$ which is faithful. Let $n_1$ be the degree of $V_1$. As $s \neq p$ we have $n \geq n_1 \geq s^a$ by Huppert (1968, p. 562, Satz 16.14).

Assume now that $n=s^a$. Then $n=n_1$, i.e., $E$ is irreducible. Hence by Schur's Lemma the centralizer of $E$ in $\text{Hom}(V, V)$ is a field $L$. This field contains the ground field and hence has order $q^b$ for a suitable number $b$, which divides $n$. As $E$ is linear over $L$, we obtain a representation of $E$ of degree $n/b$. But now by the above argument $n/b \geq s^a=n$, i.e., $b=1$. Thus $E=3G$.

Denote $Z=3N$ and consider the normal subgroup $X$ of $G$ consisting of all elements which fix elementwise the factor group $N/Z$. Clearly $3E=3N$, which implies that $N/Z \cong E/E \cap Z$ is abelian and therefore $E \cdot 3G \leq N \cdot 3G \leq X$. On the other hand we can find subgroups $B_1, \ldots, B_{2a}$ of $N$ each containing $Z$ as a subgroup of index $s$, such that $N=B_1 \ldots B_{2a}$. By (a) $Z \leq 3G$ so that $X$ induces on each $B_i$ a group of automorphisms of order at most $s$. Hence $[X: 3G]=[X: E] \leq [X: E \cap N] \leq s^{2a}$, which implies that $X=E \cdot 3G$.

LEMMA 2.3. Assume that $i \geq 9$ and that the alternating group $A_i$ of degree $i$ has a faithful representation $\varphi$ of degree $n$ over $GF(q)$, where $q$ is a power of $2$. Then one of the following holds:

(a) $A_{i-4}$ has a faithful representation of degree $n-3$ over $GF(q)$.
(b) $A_i^\varphi$ contains a group of order $4$ consisting of transvections with common center and common axis.
Proof. $A_i$ contains a subgroup $B \cong C \times D$, where $C \cong A_4$ and $D \cong A_{i-4}$. Let $E = \langle \sigma, \tau \rangle$ be the elementary abelian subgroup of order 4 in $C$. If $V = V(n, q)$ is the underlying vector space, then we have the series $V > V_\sigma > V(\sigma - 1) > 0$, where $V_\sigma$ is the kernel of $\sigma^{-1}$ and hence $\dim V/V_\sigma = \dim V(\sigma - 1) \leq n/2$. Suppose now that (a) is false. Then any faithful representation of $D$ over $GF(q)$ has at least degree $n - 2$. As $D$ centralizes $E$, it leaves invariant $V_\sigma$ and $V(\sigma - 1)$. Suppose that $D$ acts non-trivially on $V/V_\sigma$ or $V(\sigma - 1)$. Then the simple group $D$ actually is faithful on one of these spaces, so that $n - 2 \leq n/2$, i.e., $n \leq 4$. As $i \geq 9$, we conclude that $A_9$ has a faithful representation of degree at most 4 over $GF(q)$. But $A_9$ contains a subgroup isomorphic to $S_7$, and $S_7$ contains a Frobenius group of order 7.6. However, this leads to a contradiction (see [PR, Lemma 1.3]). So $D$ is trivial on $V/V_\sigma$ and $V(\sigma - 1)$. As $D$ is no 2-group, $D$ must operate non-trivially and hence actually faithfully on $V_\sigma/V(\sigma - 1)$. So $\dim V_\sigma/V(\sigma - 1) \geq n - 2$ and hence $\dim V/V_\sigma = \dim V(\sigma - 1) = 1$, i.e., $\sigma$ is a transvection. Also $\dim V_\sigma/V(\sigma - 1) = n - 2$, and hence $D$ operates irreducibly on $V_\sigma/V(\sigma - 1)$. Now $\tau$ fixes $V_\sigma$ because $\tau \in \Sigma$. As $\dim V/V_\sigma = 1$, $\tau$ centralizes $V/V_\sigma$, and $V(\tau - 1) \leq V_\sigma$. As $D$ leaves invariant $\{V(\tau - 1) + V(\sigma - 1)\}/V(\sigma - 1)$, we have $V(\tau - 1) = V(\sigma - 1)$. Furthermore $V_\tau \supseteq V(\tau - 1) = V(\sigma - 1)$, and $D$ leaves invariant $V_\tau/V(\tau - 1) \cap V_\sigma/V(\sigma - 1)$. Again using the irreducibility of $D$ we see that $V_\tau = V_\sigma$. So $C$ lies in the group consisting of all transvections with center $V(\sigma - 1)$ and axis $V_\sigma$.

LEMMA 2.4. Let $m \geq 2$ be an integer, $q$ a power of a prime $p$ and $K$ a field whose characteristic is different from $p$. Then the degree of any non-trivial representation of $PSp(2m, q)$ is at least $(1/d)(q^m - 1)$, where $d = (2, q - 1)$.

Proof. This follows from [PR, Theorem 4.2], as the group $PSp(2m, q)$ contains a subgroup isomorphic to $PSp(2, q^m) \cong PSL(2, q^m)$ (see Huppert, 1967, p. 228, Satz 9.24). Only for $m = 2$ and $q = 2$ or $q = 3$ we might possibly have exceptions. However, it is easy to check that $PSp(4, 2)$ does not have any non-trivial projective representation of degree $< 3$ and $PSp(4, 3)$ does not have any non-trivial projective representation of degree $< 4$.

§3. SOME ELEMENTARY NUMBER THEORY

Throughout this paragraph we shall use the following notation: If $n$ is a positive integer, then $p(n)$ is the set of prime divisors of $n$, $e(n)$ the set of subsets of $p(n)$ of even cardinality and $o(n)$ the set of subsets of $p(n)$ of odd cardinality. If $\mathfrak{X}$ is a finite set of primes, then $n(\mathfrak{X}) = \prod_{p \in \mathfrak{X} \cup \{1\}} p$. For any two integers $a \geq 2$ and $n \geq 2$ we define
Furthermore, \( \Phi_1(a) = a - 1 \). Finally, if \( M \) is any finite set, then \( D(M) = s - t \), where \( s \) is the number of subsets of \( M \) of even cardinality and \( t \) is the number of subsets of \( M \) of odd cardinality. We have

**Lemma 3.1.** If \( M \) is a finite set, then \( D(M) = 0 \) if \( M \neq \emptyset \) and \( D(M) = 1 \) if \( M = \emptyset \).

**Proof.** Let \( M \neq \emptyset \) and \( P \in M \). For \( X \subseteq M \) define \( X^P = X - \{ P \} \) if \( P \in X \) and \( X^P = X \cup \{ P \} \) if \( P \notin X \). Then \( \phi \) induces a \( 1 \) \( - \) \( 1 \) map of the subsets of \( M \) of even cardinality onto the subsets of \( M \) of odd cardinality.

The main goal of this paragraph is the investigation of \( \Phi_n(a) \). Before we proceed we indicate a second lemma:

**Lemma 3.2.** Let \( a \) be a positive integer, \( r \) a prime divisor of \( a - 1 \) and \( r^a \parallel a - 1 \). Then

(i) if \( k \) is a positive integer and \( r \nmid k \), then \( r^a \parallel a^k - 1 \);

(ii) if \( r^a \neq 2 \), then \( r^{a+1} \parallel a^r - 1 \).

**Proof.** Let \( a - 1 = r^a t \), where \( r \nmid t \). Then \( a = 1 + r^a t \) and

\[
d_k = 1 + \binom{k}{1} r^a t + \binom{k}{2} r^{2a} t^2 + \cdots + r^{ka} t^k.
\]

Hence \( r^a \parallel a^k - 1 \) and \( r^{a+1} \parallel a^r - 1 \), as \( a \geq 1 \). If

\[
r^{a+1} \parallel a^k - 1, \quad \text{then} \quad r \mid \binom{k}{1} t,
\]

and hence \( r \mid x \). So (i) is proved. If \( r^{a+2} \parallel a^r - 1 \), then

\[
r^{a+2} \parallel r^{a+1} t + \binom{r}{2} r^{2a} t^2
\]

and therefore

\[
r^{a+2} \nmid \binom{r}{2} r^{2a} t^2,
\]

which implies \( r = 2 \) and \( a = 1 \).

Let \( n \geq 2 \) and let \( r \) be any prime divisor of

\[
\prod_{X \in \pi(n)} (a^{n/n}(X) - 1) \quad \text{or} \quad \prod_{X \in \alpha(n)} (a^{n/n}(X) - 1).
\]
Furthermore, let
\[ r^a \parallel \prod_{x \in \mathcal{X}(n)} (a^{n/x} - 1), \quad r^b \parallel \prod_{x \in \mathcal{X}(n)} (a^{n/x} - 1) \]
and \( n=r^e n_1 \), where \( r \nmid n_1 \). Obviously \( r \nmid a \). Denote by \( m \) the multiplicative order of \( a \) modulo \( r \). Finally, let \( r^a \parallel a^{mr^e} - 1 \).

For each \( \mathcal{X} \subseteq p(n) \) the conditions \( r \mid a^{n/x} - 1, \ m \mid (n/n(\mathcal{X})) \) and \( \mathcal{X} \subseteq p(n/m) \) are equivalent. (Clearly, \( m \) is a divisor of \( n \).) Furthermore, if \( r \mid a^{n/x} - 1 \) and \( r \notin \mathcal{X} \), then \( mr^e \mid (n/n(\mathcal{X})) \) as \( (m, r)=1 \), and hence \( r^a \parallel a^{n/x} - 1 \) by Lemma 3.2. So we get

\((*) \) if \( q=0 \), then \( \alpha = \beta = \sigma D \{ p(n/m) \} \).

Assume now that \( q>0 \), and let \( r^e \parallel a^{mr^e} - 1 \). Then, again by Lemma 3.2, \( r^a \parallel a^{n/x} - 1 \) if \( \mathcal{X} \subseteq p(n/m) \) and \( r \notin \mathcal{X} \), while \( r^a \parallel a^{n/x} - 1 \) if \( \mathcal{X} \subseteq p(n/m) \) and \( r \in \mathcal{X} \). Hence

\((** \) \) if \( q \neq 0 \), then \( \alpha = \beta = (\sigma - \tau) D \{ p(n/m) - \{ r \} \} \).

As always \( \alpha = \beta \geq 0 \), \( \Phi_n(a) \) is an integer. Furthermore, if \( q=0 \) and \( \alpha = \beta > 0 \), then \( m=n=n_1 \) and \( \alpha - \beta = \sigma \) by Lemma 3.1. If \( q>0 \) and \( \alpha - \beta > 0 \), then \( p(n/m) = \{ r \} \) and again \( m=n_1 \), as \( (m, r)=1 \). Thus \( n_1 \) is the multiplicative order of a modulo \( r \), whenever \( r \mid \Phi_n(a) \). Suppose now that \( q>0 \) and \( \alpha - \beta \geq 2 \). Then \( \sigma - \tau > 1 \) by Lemma 3.1, and hence \( r^e = 2 \) by Lemma 3.2. As \( n_1 = m \mid r - 1 \), we get \( n=2^e \). Furthermore, \( 2^e = 2 \parallel a^{2^{e-1}} - 1 \) implies that \( q=1 \) and \( a \equiv 3(\text{mod } 4) \).

We always have \( r^a - \beta \mid a^n - 1 \). This is clear as \( \alpha = \beta \leq \sigma \) and \( r^a \parallel a^{mr^e} - 1 \mid a^{mr^e} - 1 = a^n - 1 \). So \( \Phi_n(a) \mid a^n - 1 \).

Combining our results we get

THEOREM 3.3. (Zsigmondy, 1892). Let \( a \geq 2 \) and \( n \geq 1 \) be integers.

(a) \( \Phi_n(a) \) is an integer and \( \Phi_n(a) \mid a^n - 1 \).

(b) Let \( r \) be a prime divisor of \( \Phi_n(a) \) and let \( n=r^e n_1 \), where \( r \nmid n_1 \).

Then \( n_1 \) is the multiplicative order of a modulo \( r \).

If \( q>0 \), then \( r^e \nmid \Phi_n(a) \), unless \( r=n=2 \) and \( a \equiv 3(\text{mod } 4) \).

Denote \( f = (n, \Phi_n(a)) \) and suppose that \( f \neq 1 \). Let \( r \) be a prime divisor of \( f \) and let \( n=r^e n_1 \), where \( r \nmid n_1 \). Then by Theorem 3.3 \( n_1 \) is the multiplicative order of a modulo \( r \). In particular, \( n_1 \mid r-1 \) so that \( r \) is the largest prime divisor of \( n \) and hence uniquely defined. Therefore \( f \) is a power of \( r \). If \( r^2 \mid \Phi_n(a) \), then \( n=2 \) by Theorem 3.3. Hence never \( r^2 \mid f \) so that actually \( f=r \). We have proved

THEOREM 3.4. Let \( a \geq 2 \) and \( n \geq 2 \) be integers. Let \( r \) be the largest prime divisor of \( n \) and \( n=r^e n_1 \) such that \( r \nmid n_1 \). If \( (n, \Phi_n(a)) \neq 1 \), then \( (n, \Phi_n(a))=r \) and \( n_1 \) is the multiplicative order of a modulo \( r \).
For \( a \geq 2 \) and \( n \geq 1 \) we define

\[
\Phi^*_n(a) = \frac{1}{f^*} \Phi_n(a),
\]

where \( f = (n, \Phi_n(a)) \) and \( f^* \) is the largest power of \( f \) dividing \( \Phi_n(a) \) if \( f \neq 1 \), and \( \alpha = 1 \) otherwise. Note that \( \alpha = 1 \) unless \( f = n = 2 \) and \( a \equiv 3 \pmod{4} \).

With this definition we have

**THEOREM 3.5.** Let \( q \geq 2 \) be a prime power and \( n \geq 1 \) an integer. Then for any prime \( r \) the following conditions are equivalent:

(i) \( r \mid \Phi^*_n(q) \).

(ii) \( r \nmid q \) and the multiplicative order of \( q \) modulo \( r \) is \( n \).

(iii) \( r \nmid q^n - 1 \) but \( r \nmid q^k - 1 \) for \( 0 < k < n \).

(iv) \( GL(n, q) \) contains non-trivial \( r \)-groups, and every non-trivial \( r \)-group in \( GL(n, q) \) is irreducible.

(v) \( GF(q^n) \) contains an element of multiplicative order \( r \) which does not lie in any proper subfield containing \( GF(q) \).

(vi) \( r \nmid q^n - 1 \) but \( r \nmid q^k - 1 \) for \( 0 < k < n \) and \( k \nmid n \).

*Proof.* Let \( r \mid \Phi^*_n(q) \). If \( r \mid n \), then \( r \mid (n, \Phi_n(q)) \) and \( r = (n, \Phi_n(q)) \) by Theorem 3.4. But this is impossible by the definition of \( \Phi^*_n(q) \). So \( r \nmid n \), and we have (ii) by 3.3.

Obviously (ii) implies (iii).

Assume (iii), and let \( G = GL(n, q) \). Then \( r \mid q^n - 1 \mid |G| \), so that \( G \) contains non-trivial \( r \)-groups. Let, on the other hand, \( R \neq 1 \) be an \( r \)-subgroup of \( G \), and let \( U \) be the centralizer of \( R \) in the underlying vector space \( V = V(n, q) \). Then \( r \mid |V| - |U| \), which implies \( U = 0 \). Thus \( R \) is regular on \( V - \{0\} \), and by (iii), the only \( R \)-invariant subspaces of \( V \) are \( 0 \) and \( V \).

Assume (iv) and let \( R \) be a group of order \( r \) in \( GL(n, q) \). Then by Schur's lemma the \( GF(q) \)-algebra generated by \( R \) is a field \( L \) of order at most \( q^n \). Suppose that \( R \) lies in a subfield \( L \) of \( L \) containing \( GF(q) \) such that \( |L| < q^n \). Then for any \( v \in V(n, q) - \{0\} \), \( vL \) is a proper \( R \)-invariant subspace, a contradiction. Thus (v) holds.

The implication (v) \( \rightarrow \) (vi) follows from the fact that the multiplicative group of the field \( GF(q^n) \) is cyclic.

Assume (vi). Then \( r \mid \Phi_n(q) \) by definition. Let \( m \) be the multiplicative order of \( q \) modulo \( r \). Then \( m \mid n \) and hence actually \( m = n \). So \( n \mid r - 1 \) and clearly \( r \nmid (n, \Phi_n(q)) \). Thus \( r \mid \Phi^*_n(q) \).

**THEOREM 3.6.** Let \( a \geq 2 \) and \( n \geq 2 \) be integers. Let \( n = p_1^{e_1} \cdots p_s^{e_s} \) and \( b = a^{n(p_1 \cdots p_s)} \); where \( p_i \) is a prime and \( e_i \geq 1 \) for \( 1 \leq i \leq s \). Then

\[
(1 - b^{-1}) a^{\phi(n)} < \Phi_n(a) < a^{\phi(n)}
\]
if $s$ is even and

$$a^\varphi(n) < \Phi_n(a) < (1 - b^{-1})^{-1} a^\varphi(n)$$

if $s$ is odd.

Proof. Denote $\tilde{n} = p_1 \ldots p_s$ and

$$u = \prod_{x \in \mathcal{E}(n)} \frac{(1 - a^{-n/n(x)})}{(1 - a^{-n/n(x)})} = \prod_{x \in \mathcal{E}(n)} \frac{(1 - b^{-\tilde{n}/n(x)})}{(1 - b^{-\tilde{n}/n(x)})}. $$

Then

$$\Phi_n(a) = u \prod_{x \in \mathcal{E}(n)} a^{n/n(x)} \prod_{x \in \mathcal{E}(n)} a^{-n/n(x)} =$$

$$= u a^{\sum_{x \in \mathcal{E}(n)} (-1)^{\lfloor x/n \rfloor} n(x)^{-1}} = u a^n [1 - (1/p_1)] \ldots [1 - (1/p_s)] =$$

$$= u a^\varphi(n).$$

For $s \equiv 1 \pmod{2}$ we have

$$u \geq \frac{\prod_{x \in \mathcal{E}(n)}(1 - b^{-\tilde{n}/n(x)})}{1 - b^{-1}} \geq \prod_{i=2}^{n} (1 - b^{-i}) = \prod_{i=1}^{n} (1 - b^{-i}) \geq \frac{nb}{(1 - b^{-1})^2} \geq \frac{nb}{nb - 1}.$$ 

Here we are using the inequality

$$\prod_{i=1}^{n} (1 - b^{-i}) \geq (1 - b^{-1})^2 \frac{nb}{nb - 1}$$

which can be proved by induction. (Alternatively, one can apply the Euler-Legendre theorem on pentagonal numbers (see, e.g., Knopp, 1959, p. 85). One then actually obtains a slightly better bound.) Suppose now that $s$ is even. Then in our representation of $u$ the numerator contains the factor $1 - b^{-1}$, while of course all remaining factors are of the form $1 - b^{-\tilde{n}/n(x)}$, where $x \in \mathcal{E}(n)$ and $p_j \notin \mathcal{X}$, i.e., $x \in \mathcal{E}(\tilde{n}/p_j)$, for a suitable $j$. So certainly

$$u \geq (1 - b^{-1}) u_1 \ldots u_s,$$

where

$$u_j = \prod_{x \in \mathcal{E}(n), p_j \notin \mathcal{X}} (1 - b^{-\tilde{n}/n(x)})$$

$$= (1 - b_j^{-1})^{-1} \prod_{x \in \mathcal{E}(n_j)} (1 - b_j^{-n_j/n(x)}) \geq$$

$$\geq (1 - b_j^{-1})^{-1} \prod_{i=2}^{n_j} (1 - b_j^{-i}) =$$

$$= (1 - b_j^{-1})^{-2} \prod_{i=1}^{n_j} (1 - b_j^{-i}) \geq \frac{n_j b_j}{n_j b_j - 1}.$$
for \( 1 \leq j \leq s \), \( b_j = b_{p_j} \) and \( n_j = \frac{n}{p_j} \). Hence \( u > 1 - b^{-1} \). The remaining inequalities can be proved in the same way.

Theorem 3.6 tells us that \( \Phi_n(a) \) and hence also \( \Phi_n^*(a) \) increase rapidly with increasing \( a \). This fact seems to be rather important, and it can be exploited to study for example linear groups of degree \( n \) over finite fields of order \( q \), whose order is divisible by \( \Phi_n(q) \). For several applications it is useful to determine all cases in which \( \Phi_n^*(q) \) has a particularly small value, namely, one of the numbers \( 1 \), \( (n+1) \), \( (2n+1) \), or \( (n+1) (2n+1) \).

**Lemma 3.7.** If \( n = p_1^{e_1} \cdots p_s^{e_s} \), where \( s \geq 4 \) and \( e_i \geq 1 \) for \( 1 \leq i \leq s \), then \( 2^{\Theta(n)} > n^3 \).

**Proof.** Assume at first that \( s = 4 \). Then clearly \( \varphi(n) \gg n^3 \). Also \( n \geq 210 = 2 \cdot 3 \cdot 5 \cdot 7 \), which implies \( 2^{\Theta(n)/3} \geq 2^{8^{n/105}} > n \). So the statement holds for \( s = 4 \). The general case can be proved by induction: Let \( p \geq 7 \) be a prime not dividing \( n \) and \( e \) a positive integer and assume that \( 2^{\Theta(n)/3} > n \), where \( n \geq 210 \). Then

\[
2^{\Theta(p^e n)/3} = 2^{\Theta(n) p^e (1 - 1/p^e)/3} > n^{6 p^e /7} = nn^{(6 p^e /7)}^{-1} \geq n \cdot 210^{5 p^e /7} > np^e.
\]

Assume now that \( \Phi_n^*(a) \leq (n+1) (2n+1) \), where \( a \geq 2 \) and \( n > 2 \). Let \( n = p_1^{e_1} \cdots p_s^{e_s} \) be the standard representation of \( n \), such that \( p_1 < p_2 < \cdots < p_s \). If \( s \geq 4 \), then \( n \geq 2 \cdot 3 \cdot 5 \cdot 7 \) and \( f \leq p_3 < n/p_1^2 p_2^2 p_3^3 < n/30 \). Thus by Theorem 3.6

\[
2^{\Theta(n)} \leq a^{\Theta(n)} \leq 2^{\Theta(n)} = 2 f \Phi_n^*(a) \leq 2 f (n + 1) (2n + 1) \leq \frac{1}{2} n^3.
\]

However, this is impossible by Lemma 3.7. So \( s \leq 3 \). Assume that \( s = 3 \). Then \( n \geq 30 \), \( f \leq n/6 \) and by Theorem 3.6

\[
a^{\Theta(n)} < \Phi_n(a) = f \Phi_n^*(a) \leq f (n + 1) (2n + 1) < 3 f n^2 \leq \frac{1}{2} n^3.
\]

Suppose that \( p_3 \geq 7 \). Then

\[
2^{n/7} \leq a^{n/7} < f (n + 1) (2n + 1) \leq \frac{1}{2} n^3.
\]

This implies that \( n < 63 \), \( p_3 = 7 \), \( n = 42 \) and \( a^{12} < 7 \cdot 43 \cdot 85 \). Hence \( a = 2 \) and \( f = 1 \) by Theorem 3.4. But from that we obtain \( 2^{12} < 43 \cdot 85 \), a contradiction. So \( p_3 = 5 \), \( f \leq 5 \) and

\[
2^{4 n/15} \leq a^{4 n/15} = a^{\Theta(n)} < 15 n^2.
\]

Therefore \( n < 60 \) and hence \( n = 30 \) and \( a = 3 \). Here \( a = 3 \) implies \( f = 1 \) and \( 3^8 < 31 \cdot 61 \), as \( 3 \) has order 2 modulo 5. Hence there only remains the case \( a^n = 2^{30} \).

Consider now the case \( s = 2 \). Suppose at first that \( n > 30 \). Then \( f \leq n/p_1 \)
and hence
\[ 2^a \leq a^\phi(n) \leq \frac{a^{n/p_1p_2}}{a^{n/p_1p_2} - 1} f^{\frac{3}{2}} n^2 \leq \frac{3}{2} n^3. \]

This implies that \(a = 2\), as otherwise \(3^{n/3} < \frac{3}{2} n^3\), which is impossible for \(n \geq 30\). Also \(p_1 = 2\) as otherwise \(\phi(n) \geq \frac{8}{3} n\), \(f \leq n/3\) and hence \(2^{n/3} \leq \frac{8}{3} n^3\).

Suppose that \(p_2 = 3\). Then \(f \leq 3\), \(a^{n/p_1p_2} \geq 2^5\) and \(2^{n/3} \leq (32/31.5)n^2\), which implies that \(n < 45\) and therefore \(n = 36\). But \(p_1^s \mid f - 1\) by Theorem 3.4.

So in this case \(f = 1\), which leads to a contradiction. Hence \(p_2 \geq 5\), \(\phi(n) \geq \frac{3}{2} n\) and \(f \neq 1\), as otherwise \(2^{n/5} < \frac{8}{5} n^2\). Thus \(p_2 \mid 2^{n/5} - 1\) and \(e_1 \geq 2\). If \(e_1 = 2\), then \(p_2 = 5\) and \(100 \mid n\). In any case \(f \leq n/8\) and \(2^{n/5} < \frac{8}{5} n^3\). Thus \(n < 40\), which is impossible as \(n\) is divisible by 8 or 100. So \(n < 30\), and one easily checks that actually \(n \leq 24\).

Finally assume that \(s = 1\), and suppose that \(n > 16\). Then \(a^{n(1 - 1/p_1)} < \frac{9}{8} fn^2 < \frac{3}{2} n^3\). This implies that \(p_1 > 2\) and \(a = 2\). So \(f = 1\) and \(2^{n/3} < \frac{3}{2} n^2\), which is impossible. Hence we have proved:

**Theorem 3.8.** Let \(a \geq 2\) and \(n \geq 1\) be integers and suppose that \(\Phi_n(a) \leq \leq (n + 1)(2n + 1)\). Then one of the following holds:

(a) \(n = 30\) and \(a = 2\).
(b) \(n \leq 24\) and \(n\) has 2 different prime divisors.
(c) \(n \leq 16\).

**Theorem 3.9.** Let \(q\) be a power of a prime \(p\) and \(n \geq 2\) an integer.

(a) (Zsigmondy, 1892) If \(\Phi_n(q) = 1\), then \(q^n = p^n = 26\) or \(p^2\).
(b) If \(\Phi_n(q) = n + 1\), then \(q^n = p^n = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6\) or \(p^2\).
(c) If \(\Phi_n(q) = 2n + 1\), then \(q = p = q = p^2\). In the first case \(q^n = p^n = 2^3, 2^8, 2^{20}\) or \(p^2\) while in the second case \(q^n = p^n = 4^2, 4^3, 4^6\) or \(9^2\).
(d) If \(\Phi_n(q) = (n + 1)^2\), then \(q^n = p^n = 7^4\) or \(q^3 = p^3 = 8^2\).
(e) If \(\Phi_n(q) = (n + 1)(2n + 1)\), then \(q^n = p^n = 3^{18}, 17^2\) or \(p^2\).

**Proof.** In each of the cases (a)–(d) we have \(n \leq 30\) by Theorem 3.8. Clearly, for every particular value of \(n\), which is different from 2, there are only finitely many possibilities for \(a\). Actually \(n \neq 2\) implies \(a^{n/2} \leq a^{\phi(n)} \leq 2\Phi_n(a) = 2f \Phi_n(a) \leq 12 \cdot 10^4\) and \(a^n \leq 2 \cdot 10^{10}\) by Theorem 3.6. Suppose that \(n = 2\) and \(q = p^n\), where \(m > 1\). Then \(\Phi_n(q) \mid \Phi_n(q) \mid 3 \cdot 5\). Hence again we have only finitely many possibilities. Inspecting the different possibilities for \(n\) one obtains the above list. We present here an independent proof for the statement (a), which is of special interest:

Suppose that \(\Phi_n(a) = 1\) and that \(n > 2\). Again, let \(n = p_1^{s_1} \ldots p_s^{s_s}\) be the standard representation of \(n\). As in the beginning of the proof of Theorem 3.8 we show that \(s \leq 3\). Thus \(2^{n/3} < 2n\), hence \(n < 30\) and \(s \leq 2\). If \(s = 1\), then
$f \mid a - 1$ and $(a^n - 1)/(a^{n/p} - 1) \leq f \mid a - 1$, a contradiction. So $s = 2$, $f \leq n/2$ and $2^{n/3} < n$. This implies that $n < 10$, hence $f = 3$, $p_1 \cdot p_2 = 6 \mid n$ and $n = 6$. Also $a^2 < 6$ and therefore $a = 2$.

The following lemma will be useful in § 4.

**Lemma 3.10.** $d(a - 1) \mid a^n - 1$ and $\Phi_n^*(a) \mid (a^n - 1/d(a - 1))$, whenever $a \geq 2$, $n \geq 2$ and $d = (n, a - 1)$.

**Proof.** By Theorem 3.3, $\Phi_n^*(a) \mid a^n - 1$. Furthermore, $(\Phi_n^*(a), a - 1) = 1$, as $n > 1$ and $(\Phi_n^*(a), d) = 1$, as every prime dividing $\Phi_n^*(a)$ is larger than $n$ by Theorem 3.5. Also $(a^n - 1)/(a - 1) = a^{n-1} + a^{n-2} + \cdots + a + 1 \equiv n \equiv 0 \pmod{d}$. Thus $(a^n - 1)/d(a - 1)$ is an integer divisible by $\Phi_n^*(a)$.

§4. **Linear groups containing an irreducible group of prime order**

Let $K$ be a finite field of order $q$ and characteristic $p$, $V$ a vector space of finite dimension $n$ over $K$ and $G$ a subgroup of $GL(V, K)$. Define $\Phi_n^*(q)$ as in the preceding paragraph and assume that $(\Phi_n^*(q), |G|) \neq 1$. By 3.5 this is equivalent to saying that $G$ contains an irreducible subgroup of prime order. Let $r$ be a prime dividing $(\Phi_n^*(q), |G|)$, $R$ a Sylow $r$-subgroup of $G$ and $S$ the normal closure of $R$ in $G$. Also, in this paragraph, denote by $L$ the centralizer of $S$ in $\text{Hom}(V, V)$ and by $F$ the Fitting subgroup of $G$. Clearly, $S$ is irreducible and therefore $L$ is a field of order $q^m$ for a suitable $m$. Also $V$ is a vector space over $L$ of dimension $n^* = n/m$. We have

**Lemma 4.1.** Every abelian normal subgroup of $G$ is contained in $C_{G} S$.

**Proof.** Let $A$ be an abelian normal subgroup of $G$. Then $A R$ is irreducible by 3.5. Therefore $A$ has only one Wedderburn component in $V$. Hence $[\mathfrak{C}_{G} A : C_{G} A] \mid n$ (see [TL Hilfssatz 5]). But $r \equiv 1 \pmod{n}$ by 3.5. So $R \subseteq \mathfrak{C}_{G} A$ and $S \subseteq \mathfrak{C}_{G} A$.

**Theorem A.** If $F$ is not contained in $C_{G} S$, then the following statements hold:

(a) $(\Phi_n^*(q), |G|) = |R| = r = n + 1 = 2^a + 1$ for a suitable $a \geq 1$.

(b) $|L| = q$ and $q \equiv 1 \pmod{2}$.

(c) $G$ contains a normal subgroup $N$ such that $N = T \mathfrak{Z} N$, where $T$ is an extraspecial group of order $2^{2a+1}$, $\mathfrak{Z} N$ is a cyclic group of order 2 or 4 and $T \cap \mathfrak{Z} N = = \mathfrak{Z} T$. Also $N \subseteq S$, $\mathfrak{Z} N \subseteq \mathfrak{C}_{G} T = \mathfrak{Z} G$, $F = N \mathfrak{Z} G$ and $G/F$ is faithfully represented on $N/\mathfrak{Z} N$.

(d) $C_{G/F}(RF/F) = RF/F$ and $C_{F} R = \mathfrak{Z} G$.

(e) $F(G/F) \leq RF/F$.

**Proof.** Assume that $[F, S] \neq 1$. Then there exists a prime $s$ such that the
Sylow $s$-subgroup $F_s$ of $F$ is not centralized by $S$. Let $N$ be of smallest possible order among the subgroups with the properties $N \leq F_s$, $N \unlhd G$ and $[N, S] \neq 1$. As $S$ is the normal closure of $R$ in $G$ we have $[N, R] \neq 1$. Therefore $r \neq s$, as the Sylow $r$-subgroups of $G$ are cyclic.

Let $X$ be a subgroup maximal with respect to the properties $X \leq N$ and $X \leq G$. Then $[X, R] \leq [X, S] = 1$, and $X$ is cyclic. Thus $X \leq C_N X \leq G$, which implies that either $C_N X = X$ or $C_N X = N$. Assume that $C_N X = X$. Then $C_{NR} X = XR \cong X \times R$, as $s \neq r$. But this implies that $R \leq NR$ and $[N, R] = 1$, a contradiction. So $C_N X = N$, i.e., $X \leq \mathfrak{3}N$. We conclude that every proper characteristic subgroup of $N$ is cyclic and contained in $\mathfrak{3}N$. This allows us to apply Lemma 2.1.

$N$ certainly is not abelian by Lemma 4.1. So $N$ is either extraspecial or of the form described in Lemma 2.1d). In any case $|N : \mathfrak{3}N| = s^{2^a}$ for a suitable $a \geq 1$, and $N = T \cdot \mathfrak{3}N$, where $T$ is an extraspecial group of order $s^{2a+1}$. Here $s \neq p$, because $N \unlhd G$, and $G$ is irreducible. As the center $\mathfrak{3}T$ of $T$ has order $s$, it is contained in every non-trivial normal subgroup of $T$. This implies that each faithful representation of $T$ over a field of characteristic $p$ has an irreducible constituent which is faithful. So $n* \geq s^a$ by Huppert (1968, p. 562, Satz 16.14).

Consider an arbitrary prime divisor $r_1$ of $(\Phi^*_n(q), |G|)$ and a Sylow $r_1$-subgroup $R_1$ of $G$. Let $X'N'$ be a complement of $(C_N (C_N R_1))/N'$, which is invariant under $R_1$. As $C_N R_1$ is cyclic, and as $N$ has exponent $s$ or $s^2$, we have $|C_N R_1| \leq s^2$ and hence $|X'| \leq s^2$. Thus $X \leq C_N R_1 \leq C_N (C_N R_1)$ and hence $C_N R_1 \leq \mathfrak{3}N$. So $C_N R_1 = \mathfrak{3}N$, and $R_1$ is fixed point free on $(N/\mathfrak{3}N)^*$. Thus $|R_1| = s^{2^a-1}$, and we get

$$n+1 \leq r_1 \leq |R_1| \leq s^a + 1 \leq n^* + 1 \leq n + 1.$$ 

Hence $n^* = n$ and $|L| = |K|$. Also $s^a = r_1 - 1$ and $a \geq 1$ imply $s = 2$. Clearly this implies (a). Since, as we have seen above, $p \neq s = 2$ we also have (b). Suppose that $N \leq S$. Then $N \cap S \leq \mathfrak{3}S$ by minimality of $N$. Also $[N, S] \leq \mathfrak{3} \cap S$ so that $S$ centralizes $N/\mathfrak{3}N \cap S$. But this implies that $R$ centralizes $N$, which is impossible. By Lemma 2.2, $C_G T = 3G$. To finish the proof of (c) we consider the group $Y = N \cdot 3G = T \cdot 3G$ and the factor group $G/Y$, which by Lemma 2.2 is faithfully represented on the elementary abelian group $N/\mathfrak{3}N$. So $G/Y$ is isomorphic to a subgroup of $GL(2a, 2)$. As obviously $r \mid \Phi^*_n(2)$, we can apply Korollar 1 of [TL] to this situation: $\mathfrak{C}_{G/Y} / RY / Y$ is cyclic and fixed point free on $(N/\mathfrak{3}N)^*$. As $G/Y$ always leaves invariant a symmetric form on the vector space $N/\mathfrak{3}N$ this implies that $|\mathfrak{C}_{G/Y} (RY/Y)| \leq 2^a + 1$ by Huppert (1967, p. 228, Satz. 9.28). So in fact $|\mathfrak{C}_{G/Y} (RY/Y)| = 2^a + 1$ and $\mathfrak{C}_{G/Y} (RY/Y) = RY/Y$. Applying Theorem A, (b) to this situation, we see that $F (G/Y) \leq \mathfrak{C}_{G/Y} SY/Y \leq \mathfrak{C}_{G/Y} R/Y = RY/Y$. 


Clearly $Y$ is nilpotent and therefore contained in $F$. Also $F/Y \leq F(G/Y) \leq \leq RY/Y$. But this implies $F=Y$, as $r \not| |F|$. Now (c), (d), and (e) are obvious.

**Lemma 4.2.** Suppose that $G=MR$, where $M$ is a proper normal subgroup of $G$. Then $M$ is nilpotent.

**Proof.** By [TL, Satz 2] $G$ is solvable. To prove that $M$ actually is nilpotent, we distinguish the two cases $[F, S]=1$ and $[F, S] \neq 1$. Assume at first that $[F, S]=1$. Then $S \leq F$, as $G$ is solvable. In particular $R \leq F$. This implies that $R \leq G$. Let $M_r$ be a Hall $r'$-subgroup of $M$. Then $R=\mathbb{C}_R M_r \times [R, M_r]$. But $R$ is cyclic and hence either $R=\mathbb{C}_R M_r$, or $R=[R, M_r]$. Here $R=\mathbb{C}_R M_r$ implies $R \leq [R, M] \leq M$ and $M=G$, which contradicts our assumptions. So $R=\mathbb{C}_R M_r$, and $M \leq \mathbb{C} R$. But now $M$ is cyclic by [TL, Korollar 1].

Assume now that $[F, R] \neq 1$. Then by Theorem A and Lemma 4.1 the order of $\exists F$ divides $q-1$, and $q-1 < q^n-1$. Thus every prime divisor of $|F|$ divides $q-1$ and certainly $r \not| |F|$. Hence $F \leq M$ and $M/F \cap RF/F=1$. On the other hand $RF/F=F(G/F)$ by Theorem A (e). This implies $[M/F, RF/F]=1$ and hence $M/F \leq \mathbb{C}_{G/P} RF/F=RF/F$. So $M=F$.

**Theorem B.** (a) $\exists F/F$ is simple.

(b) $G/S$ is isomorphic to a factor of the metacyclic group $\Gamma L(1, q^n)$.

(c) $\mathbb{C}_G S=\exists F$ is a subgroup of the multiplicative group of the field $L$.

(d) If $|L|< q^n$, then $|R| \mid (\Phi^*_s(q), |G|) \mid |SF/F|$.

(e) One of the following statements holds:

(i) $|L|=q^n$.

(ii) $|SF/F|=r$ and $\mathbb{C}_{G/F} SF/F=SF/F$.

(iii) $\mathbb{C}_{G/F} SF/F=1$.

(f) $F \cap S=F(S)$ is the unique maximal normal subgroup of $S$.

(g) If $G$ is not solvable, then $S=G(\infty)$, $G/\exists F$ is isomorphic to a subgroup of the outer automorphism group of $SF/F$.

(h) If $G$ is not solvable and $F \leq \mathbb{C}_G S$, then $F \cap S$ is isomorphic to a subgroup of the Schur multiplier of $SF/F$.

**Proof.** Let $X/F$ be a normal subgroup of $SF/F$. If $X<\exists F$, then $R \leq X$, and $X$ is nilpotent and hence contained in $F$ by Lemma 4.2. This implies (a). Furthermore, (b) follows from [TL, Hilfssatz 5], as $G/S=S \cdot N_G R/S \cong \cong N_G R/S \cap N_G R$ by the Frattini argument.

As $R \leq S$, the centralizer $\mathbb{C}_G S$ is cyclic by [TL, Korollar 1]. Hence always $\mathbb{C}_G S \leq F$. If $F \leq \mathbb{C}_G S$, then $\mathbb{C}_G S=F=\exists F$. In the remaining case we can apply Theorem A. It follows that $\mathbb{C}_G S \leq F \cap \mathbb{C}_G S \leq F \cap \mathbb{C}_G R=F \cap R \cdot 3G=3G=3F$. So in both cases $\mathbb{C}_G S=3F$, and together with Lemma 4.1 we get (c).

Let $r_1$ be any prime divisor of $(\Phi^*_s(q), |G|)$ and $R_1$ a Sylow $r_1$-subgroup of
If \( R_1 \leq S \), then \( S \) is nilpotent by Lemma 4.2, hence \( R = S \) and \( |L| = q^n \). On the other hand, if \( R_1 \cap F \neq 1 \), then \( G \) has a non-trivial normal \( r_1 \)-subgroup and therefore is isomorphic to a subgroup of \( \Gamma L(1, q^n) \). This again implies \( R \leq F \) and \( L = F \). So we have (d).

Finally, let \( X/F = \mathbb{C}_{G/F} R/F \), and suppose that \( X > F \). Then \( X \leq G \) and \( X \) is not nilpotent. Thus \( S \leq X \) by Lemma 4.2. Hence \( SF/F \) is abelian and \( SF/F = RF/F \). If \( F \not\leq \mathbb{C}_G S \), then \( \mathbb{C}_{G/F} RF/F = RF/F \) by Theorem A. If \( F \leq \mathbb{C}_G S \), then \( R \leq F \) and \( |L| = q^n \).

(f) follows immediately from Lemma 4.2. Assume now that \( G \) is not solvable. Then \( S \) is not solvable by (b). Hence \( S \) is perfect by (f). As \( G \) is semilinear over \( L \), we have \( |L| < q^n \) and therefore the property (iii), which implies (g). If, in addition, \( F \leq \mathbb{C}_G S \), then certainly \( S \cap F \leq S' \cap F \).

**THEOREM 4.3.** If \( SF/F \cong A_i \), where \( A_i \) is the alternating group of degree \( i \) and \( i \geq 5 \), then

(a) \( (\Phi^*_n(q), |G|) = n+1, 2n+1 \) or \( (n+1)(2n+1) \) and

(b) if \( r_1 \) is a prime dividing \( (\Phi^*_n(q), |G|) \), then \( r_1 \leq 2r_1 \) and \( |G/F| \) | \((2r_1 - 1)!\).

**Proof.** Let \( r_1 \) be a prime dividing \( (\Phi^*_n(q), |G|) \). Then \( r_1 \nmid |A_i| \) by Theorem B, and hence \( i \geq r_1 \). On the other hand \( A_i \) must have cyclic Sylow \( r_1 \)-subgroups by [TL, Korollar 1]. So \( r_1 \leq i < 2r_1 \). In particular \( r_1^2 \not| |A_i| \) and \( r_1^2 \not| (\Phi^*_n(q), |G|) \). If \( R_1 \) is a Sylow \( r_1 \)-subgroup of \( A_i \), then the normalizer of \( R_1 \) contains a Frobenius group of order \( r_1(r_1-1)/2 \). Thus a group of automorphisms of order \( (r_1-1)/2 \) is induced in \( R_1 \). By [TL, Korollar 1] this implies that \( n \leq r_1 - 1 \mid 2n \). Hence \( r_1 = n+1 \) or \( r_1 = 2n+1 \), and \( (\Phi^*_n(q), |G|) \mid (n+1)(2n+1) \).

As we have seen above, \( r_1 \leq i < 2r_1 \). By Theorem B the factor group \( G/F \) is isomorphic to a subgroup of the automorphism group of \( A_i \), i.e., to a subgroup of \( S_i \) or \( \text{Aut}(A_6) \) if \( i = 6 \). Thus \( |G/F| \mid (2r_1 - 1)! \).

**COROLLARY 4.4.** Assume that \( \Phi^*_n(q) \mid |G| \) and \( SF/F \cong A_i \), where \( A_i \) is the alternating group of degree \( i \geq 5 \). Then \( q = p \) or \( q = p^2 \), and in the first case \( q^n = p^n = 2^4, 2^6, 2^{10}, 2^{12}, 2^{16}, 3^4, 3^6, 5^6 \) or \( p^2 \) while in the second case \( q^n = p^{2n} = 4^2 \) or \( 9^2 \).

If in addition \( i \geq n+3 \) and \( q = p \), then \( q^n \) takes one of the values \( 2^4, 2^{18} \) or \( p^2 \).

**Proof.** Clearly \( \Phi^*_n(q) = n+1, 2n+1 \) or \( (n+1)(2n+1) \) because of Theorem 4.3. Thus we are restricted to the cases listed in Theorem 3.8. If \( r_1 \) is a prime dividing \( \Phi^*_n(q) \), then \( r_1 \mid |A_i| \) and hence \( i \geq r_1 \), which implies \( \frac{1}{r_1} \mid |GL(n, q)| \). This excludes the cases \( q^n = 2^3, 2^8, 2^{20}, 3^{18} \) and \( 17^6 \). Suppose now that \( q = 4 \) and \( n = 3 \). Then \( \Phi^*_n(q) = 7 \mid |A_i| \), which implies that \( SF/F \) contains a subgroup isomorphic to \( S_3 \) and therefore a Frobenius group \( X \) of order 5.4. Also...
\( F \leq G \leq L \) by Theorem A, and obviously \(|L|=4\). So \(|F| \mid 3\), and by the Zassenhaus Theorem \(SF\) itself contains a subgroup isomorphic to the Frobenius group \(X\). But this is impossible by [PR, Lemma 1.3]. Consider the case \(q=4\) and \(n=6\). Here \(\phi_n^*(q)=13\) and therefore \(i \geq 13\). Thus \(SF/F\) contains a Frobenius group \(Y\) of order \(11 \cdot 10\). Also \(|L|=4\), as \(11 \mid |S|\) \(|GL(V, L)|\). So again \(|F| \mid 3\), and we obtain a linear representation of \(Y\), which leads to a contradiction.

Assume now that \(i \geq n+3\) and \(q=p\). We consider at first the cases \(q^n=2^6\) and \(q^n=2^{12}\). By Theorem A the Fitting subgroup \(F\) is contained in \(G\) and therefore in the multiplicative group of the field \(L\). In particular, \(F \cap S\) has odd order. On the other hand \(F \cap S\) is isomorphic to a subgroup of the Schur multiplier of \(FS/F\) by Theorem B. This implies \(F \cap S=1\), as \(i \geq 9\) (see Schur, 1911). Hence we obtain a faithful representation of \(A_i\) over \(GF(2)\). By Lemma 2.3 this leads to a faithful representation of \(A_{i-4}\) of degree \(n-3\) (the possibility (b) in Lemma 2.3 does not arise here as our ground field has order 2).

However, in both cases \(|A_{i-4}| \not| GL(n-3, 2)|\).

If \(q^n=2^10\) or \(3^4\), then \(|A_{i+1}| \not| GL(n, q)|\). So there only remain the cases \(q^n=3^6\) or \(5^6\). Here \(SF/F\) contains a subgroup isomorphic to \(SL(2, 8)\). On the other hand \(n\) is no power of 2 so that \(F \leq G \leq L\). This means that we obtain a projective representation of \(SF/F\) of degree \(n^*\) over \(L\). By [PR, Theorem 4.2] this is impossible.

**Lemma 4.5.** Let \(n \geq 2\) be an integer, \(q\) a power of a prime \(p\), \(d=(n, q-1)\) and \(t\) a prime dividing \(|\Gamma L(n, q)|\).

(a) If \(t \geq (1/d)(q^n-1)/d\), then \(t=(q^n-1)/d(q-1)\) unless \(n=2\) and either \(t=q=p\) or \(t+1=q=3\).

(b) In any case \(t \leq (2/d)(q^n-1)/d+1\). If \(t=(2/d)(q^n-1)/d+1\), then \(n=2\) and \(t=p=q\) or \(q=2\) and \(t=2^n-1\).

**Proof.** (a) Suppose that \(t \mid n\). Then

\[
\begin{align*}
n \geq t & \geq (q^n-1)/d + 1 \geq (q^n-1)/(q-1) + 1 = \\
& = (q^{n-2} + q^{n-3} + \cdots + q + 1) + 1 \geq 2(n-1).
\end{align*}
\]

Hence \(n=2\) and \(2 \geq t \geq (q-1)/d+1\), which implies \(q=t=2\) if \(d=1\) and \(t=2\), \(q=3\) if \(d=2\). Thus we may assume that \(t \not| n\). Then in particular \((t, d)=1\). This implies that \((t, q-1)=1\), because \(t \geq (q^n-1)/d+1 > (q-1)/d\). Suppose now that \(t \mid q^k-1\), where \(1 \leq k < n\). Then

\[
\frac{t}{q^k-1} < \frac{q^n-1}{q-1} \leq \frac{q^n-1}{d} < \frac{q^n-1}{d} + 1,
\]

a contradiction.
As $|\Gamma(n, q)|=nq^{n(q-1)}(q^n-1)<(q-1)$, there remain only two cases, namely $t \mid \Phi_n^*(q)$ or $t=p$. Consider the case $t \mid \Phi_n^*(q)$. Then $t \mid (q^n-1)/d(q-1)$ by Lemma 3.10. If $t<(q^n-1)/d(q-1)$, then $(q^n-1)/d+1<t<(q^n-1)/2d(q-1)$ and hence

$$0 \geq q^n-2q^{n-1}-2q+2d(q-1)+3 \geq q^{n-1}(q-2)-2q+2(q-1)+3 = q^{n-1}(q-2)+1 \geq 1,$$

a contradiction. Therefore actually $t=(q^n-1)/d(q-1)$.

Finally, let $t=p$. Then $p \geq (q^n-1)/d+1 \geq (q^n-1)/(q-1)+1>q^{n-2}\geq p^n-2$. Thus $n=2$ and $p>(q-1)/d+1>(q+1)/2$, which implies that $q=p$.

(b) Assume that $t \geq 2(q^n-1)/d+1$. Then we have one of the cases listed in (a). If $t=p=q$ and $n=2$, then $d \leq 2(2(q^n-1)-1)/d+1=2(q-1)/d+1>q=t$. Clearly the case $t=n=2$ and $p=3$ is impossible. Assume $t=(q^n-1)/d(q-1)$. Then $(q^n-1)/(q-1)=t \geq 2(q^{n-1}-1)/d+1$, which implies

$$0 \geq q^n-2q^{n-1}-2q+d(q-1)+3 \geq q^{n-1}(q-3)+q^{n-1}-2q+(q-1)+3.$$

Thus $q=2$ and $t=(q^n-1)/d(q-1)=2^n-1=2(q^{n-1}-1)/d+1$.

**Theorem 4.6.** Assume that $SF/F \cong PSL(n, \bar{q})$, where $\bar{q}$ is a power of a prime $\bar{p}$ and $n \geq 2$. If $\bar{p} \neq p$, then $(\Phi_n^*(q), |G|) \mid (n+1)(2n+1)$.

**Proof.** Assume that $\bar{p} \neq p$. As $SF/F$ is simple, we have $n \geq 3$ or $\bar{q} \geq 4$. So $G$ is not solvable, which implies that $n^* \geq 2$, $r \geq 3$ and $(\Phi_n^*(q), |G|) \mid |SF/F|$.

1. If $F \leq \mathbb{C}_G$, then $n^* \geq (1/d)(\bar{q}^{n-1}-1)$, unless we have one of the cases

   - $\bar{n}=2$ and $\bar{q}=4$ or 9;
   - $\bar{n}=3$ and $\bar{q}=2$ or 4.

   **Proof.** If $F \leq \mathbb{C}_G$, then $F$ is contained in the multiplicative group of the field $L$. In particular $F$ is abelian so that we have a linear representation of $SF$ and a projective representation of $SF/F$ over $L$. Hence the above statement follows immediately from [PR, Theorem 4.2].

2. If $r=\bar{p}$, then $\bar{p} \geq 5$, $|R|=r$, $r=n+1$ or $r=2n+1$, and $SF/F \cong PSL(2, \bar{p})$.

   **Proof.** Assume that $r=\bar{p}$. Then $PSL(n, \bar{q})$ has cyclic Sylow $\bar{p}$-subgroups (see TL, Korollar 1). But this is only possible, if $\bar{n}=2$ and $\bar{q}=\bar{p}$. So actually $|R|=r=\bar{p}$, as $|R| \mid |SF/F|$ by Theorem B. Clearly $\bar{p} \geq 5$, as $G$ is not solvable. If $F \leq \mathbb{C}_G$, then $(\Phi_n^*(q), |G|)=r=n+1$ by Theorem A. If $F \leq \mathbb{C}_G$, then (1) implies that $n \geq \frac{1}{2}(\bar{p}-1)=\frac{1}{2}(r-1)$, i.e., $r-1 \leq 2n$. Hence in this case $r=n+1$ or $r=2n+1$, as $r \equiv 1 \pmod{n}$.
(3) If \( r=(\bar{q}^n-1)/d \bar{q} \), where \( d=(\bar{n}, \bar{q}-1) \), then \( |R|=r=n+1 \) or \( |R|=r=2n+1 \). In the second case either \( \bar{q}=2 \) or \( \bar{q}^n=2^{2\bar{n}}=4^2 \).

Proof. Assume that \( r=(\bar{q}^n-1)/d \bar{q} \). Then \( r=\Phi^*_{\bar{n}}(\bar{q}) \) by Lemma 3.10. Hence \( r^2 \not| |GL(\bar{n}, \bar{q})| \), and \( |R|=r \) by Theorem B. Suppose that \( r \neq n+1 \). Then \( r \geq 2n+1 \) as \( r=1 \mod n \). If \( n \geq (q^{n-1}-1)/d \), then \( r \geq 2n+1 \geq 2(q^{n-1}-1)/d+1 \) and therefore \( r=2n+1 \) and \( \bar{q}=2 \) by Lemma 4.5. If \( n<(q^{n-1}-1)/d \), then \( F \not\subseteq \mathbb{C}_G S \) or we have one of the exceptional cases of Theorem 4.2 in [PR]. The first case is impossible by Theorem A. If \( \bar{n}=2 \) and \( \bar{q}=4 \), then \( r=5 \) and \( n<3 \), so that \( n=2 \) and \( r=2n+1 \). For the case \( \bar{n}=2 \) and \( \bar{q}=9 \) we obtain \( r=5 \) and \( n<4 \). Also \( n \nmid r-1 \) so that \( n=2 \). But this implies that \( p=3=\bar{p} \) contradicting our assumptions. Suppose now that \( \bar{n}=3 \) and \( \bar{q}=2 \). Then \( r=7 \), \( n<3 \) and therefore \( p=7 \). However, this is impossible if \( 7 \nmid \Phi^*_{\bar{n}}(q) \). Finally, we might have \( \bar{n}=3 \) and \( \bar{q}=4 \), which implies \( r=7 \) and \( n<5 \). On the other hand \( n \nmid r-1 \). Hence actually \( n\leq 3 \), which again is impossible by [PR, Theorem 4.3].

(4) If \( r \) is different from \( \bar{p} \) and \( (q^n-1)/d(q-1) \), then \( |R|=r=n+1 \), and one of the following statements holds:

(a) \( F \not\subseteq \mathbb{C}_G S \).

(b) \( \bar{q}=4 \) and \( \bar{n}=2 \) or 3.

Proof. By Lemma 4.5 our assumption implies that \( r \leq (q^{n-1}-1)/d \). Hence \( n \leq r-1 < (q^{n-1}-1)/d \). If \( F \not\subseteq \mathbb{C}_G S \), then \( |R|=r=n+1 \) by Theorem A. So we can assume that \( F \subseteq \mathbb{C}_G S \), which allows us to apply (1). If \( \bar{n}=2 \) and \( \bar{q}=4 \), then \( r \mid 60 \), and \( r \) is different from 2 and 5. So \( |R|=r=3=n+1 \). For \( \bar{n}=2 \) and \( \bar{q}=9 \) we again obtain \( r=3 \) which leads to a contradiction, as the Sylow 3-subgroups of \( PSL(2, 9) \) are not cyclic. Suppose that \( \bar{n}=3 \) and \( \bar{q}=2 \). Then again \( r=3 \) and therefore \( n=2 \). But this implies that \( p=7 \) and hence \( r \mid q-1 \), a contradiction. Finally, assume that \( \bar{n}=3 \) and \( \bar{q}=4 \). Then \( |R|=r=5 \) and clearly \( n=4 \), as \( n \nmid r-1 \).

We have seen that never \( r^2 \nmid |G| \). Also either \( r=n+1 \) or \( r=2n+1 \). As this holds for every prime dividing \( (\Phi^*_{\bar{n}}(q), |G|) \), our theorem is proved. We also have a corresponding statement about symplectic groups, whose proof is considerably shorter:

**Theorem 4.7.** If \( SF/F \cong PSp(2m, \bar{q}) \), where \( \bar{q} \) is a power of a prime \( \bar{p} \neq p \) and \( m \geq 2 \), then \( (\Phi^*_{\bar{n}}(q), |G|)=r=n+1=(1/d)(q^m+1) \), where \( d=(2, \bar{q}-1) \).

Proof. We know that

\[
r \mid |SF/F| \mid \bar{q}^{m^2} \prod_{i=1}^{m} (\bar{q}^{2i}-1)
\]

Here certainly \( r \neq \bar{p} \), as the Sylow \( r \)-subgroups of \( G \) are cyclic. So \( r \mid \bar{q}^i-1 \) or \( r \mid \bar{q}^i+1 \) for some \( i \leq m \). Let \( r=an+1 \) and \( d=(2, \bar{q}-1) \), and assume at first
that $F \leq \mathbb{C}_G S$. Then by Lemma 2.4
\[
\frac{a}{d}(q^m - 1) < an + 1 = r \leq \frac{1}{d}(q^l + 1) \leq \frac{1}{d}(q^m + 1).
\]
Hence $a < (q^m + 1)/(q^m - 1) \leq 1 + 2/3$, so that $a = 1$. If $d = 1$, then, again by
Lemma 2.4, $q^m \leq r \leq q^l + 1$, which implies that $l = m, r = q^{2m} + 1, r = q^m + 1$ and
$r^2 \nmid |SF/F|$. If $d = 2$, then $(q^m - 1)/2 + 1 \leq r \leq (q^l + 1)/2 \leq (q^m + 1)/2$ and therefore
$r = \frac{1}{2}(q^m + 1)$. Again, $r$ is the greatest prime dividing the order of $SF/F$, and
$r^2 \nmid |SF/F|$. Assume now that $F \leq \mathbb{C}_G S$: By Theorem A the symplectic group $SF/F$ is
faithfully represented on a vector space of dimension $2b$ over $GF(2)$, where
$r = 2^b + 1$. Obviously here $r = \Phi_{2b}^*(2)$. Suppose that $p \neq 2$. Then by the part of
the Theorem proved above, $r = 2b + 1 = \frac{1}{2}(q^m + 1)$. Hence $b = 2$ and $q^m = 9$.
However, this is impossible, as $|PSp(4, 3)| \nmid |Sp(4, 2)|$. So $p = 2$ and hence
$m = b$ as $\Phi_{2m}^*(2) \mid |GL(2b, 2)|$ and $\Phi_{2b}^*(2) \mid |GL(2, 2)|$. This completes our
proof.

**THEOREM 4.8.** If $SF/F \cong J_1$, the Janko group of order $175560$, then $n = n^*$,
$S \cong J_1$, $G = S \times F$ and $(\Phi_n^*(q), |G|) = n + 1$, where $n = 10$ or $18$. If furthermore
$\Phi_n^*(q) \mid |G|$, then $q = 2, n = 18$ and $G \cong J_1$.

**Proof.** By Theorem B we have $(\Phi_n^*(q), |G|) \mid |FS/F| = |J_1| = 23 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot
19$. If $F \leq \mathbb{C}_G S$, then $r$ is of the form $r = 2^a + 1$ by Theorem A. Hence in this
case we only have the possibilities $r = 3$ and $r = 5$. So $a \leq 2$, and by Theorem A
the factor group $SF/F$ can be faithfully represented on a vector space of
dimension $2a$ over $GF(2)$. But this is impossible, as $|J_1| \nmid |GL(2, 2)|$ and
$|J_1| \nmid |GL(4, 2)|$. So $F \leq \mathbb{C}_G S$ and $F(S) = F \cap S \leq J \cap S$ is isomorphic to
a subgroup of the Schur multiplier of $J_1$. Hence $F(S) = 1$ by Janko (1965, Lemma
11.1). Therefore $S \cong J_1$ and $G/F$ is isomorphic to a subgroup of the
automorphism group of $S$. Thus, actually $G = S \times F$ as Janko (1965, Lemma
9.1) showed that the outer automorphism group of $J_1$ is trivial.

By Janko (1965, Lemma 13.1) the smallest possible degree of a faithful
representation of $J_1$ over any field is $7$. So $n \geq n^* \geq 7$. On the other hand
$n \mid r - 1$, where $r = 3, 5, 7, 11$ or $19$. This leaves only the possibilities $r = 11
and r = 19$. If $(\Phi_n^*(q), |G|) = 11 \cdot 19$, then $n \mid (11 - 1, 19 - 1) = 2$, which
certainly is impossible. So $(\Phi_n^*(q), |G|) = 11$ or $19$. In the first case we clearly
have $n = n^* = 10$. Suppose that $(\Phi_n^*(q), |G|) = 19$. Then a priori it might be
possible that $n^* = (r - 1)/2 = 9$. However, $n^* = 9$ implies that the automizer of
$R$ is a cyclic group whose order divides $9$ (see [TL, Korollar 1]), which is
impossible by Janko (1965, Lemma 6.1). Hence in this case again we have
only the possibility $n = n^* = r - 1 = 18$.

If $\Phi_n^*(q) \mid |G|$, then $q = 2$ and $n = 10$ or $18$ by Theorem 3.5. But here
certainly \( n \neq 10 \), as \( |J_1| \nmid |GL(10, 2)| \). Also we have \( n^* = n \), i.e., \( |L| = 2 \), and hence \( F = 1 \). So in this case \( G \cong J_1 \).

**Theorem 4.9.** Assume that \( G \) is not solvable. If \( SF/F \) is an epimorphic image of a finite subgroup of \( GL(n, \mathbb{C}) \), where \( \mathbb{C} \) is the field of complex numbers, then \( \left( \Phi^*_n(q), |G| \right) = n + 1, \ 2n + 1 \) or \( (n + 1)(2n + 1) \). In fact, the case \( \left( \Phi^*_n(q), |G| \right) = (2n + 1) or (n + 1)(2n + 1) \) is only possible if \( SF/F \cong PSL(2, r) \), where \( r = 2n + 1 \).

**Proof.** We assume that \( SF/F \cong X/N \), where \( X \) is a subgroup of \( GL(n, \mathbb{C}) \) and \( N \) is a normal subgroup of \( X \). Let \( r_1 \) be an arbitrary prime divisor of \( \left( \Phi^*_n(q), |G| \right) \). Then the Sylow \( r_1 \)-subgroups of \( X/O_{r_1}(X) \) have exponent \( r_1 \). Clearly \( O_{r_1}(X) \leq N \), as \( SF/F \) is non-abelian simple. Hence the Sylow \( r_1 \)-subgroups of \( SF/F \) are of exponent \( r_1 \) and therefore of order at most \( r_1 \) because of [TL, Korollar 1]. In view of Theorem B(d) we get that \( r_1 \mid |SF/F| \) and \( r_1^2 \nmid |G| \).

By Feit and Thompson (1961, Theorem 1) \( r_1 \leq 2n + 1 \). So \( r_1 \) is either \( n + 1 \) or \( 2n + 1 \) and \( \left( \Phi^*_n(q), |G| \right) = (n + 1)(2n + 1) \). If \( r_1 = 2n + 1 \), then \( SF/F \cong PSL(2, r_1) \) by a result of Winter (1964). (Note that both these statements can be deduced from earlier results of Brauer (1942, Theorem 3 and Theorem 4), if \( r_1 \nmid |N| \).

### §5. Transitive Linear Groups

Let \( p \) be a prime, \( K \) a field of order \( p \), \( V \) a vector space of finite dimension \( n > 0 \) over \( K \), and \( G \) a subgroup of \( GL(V, K) \), which acts transitively on the set consisting of all non-zero vectors of \( V \). As in the preceding paragraph we define \( F \) to be the Fitting subgroup of \( G \). However, we denote \( S = G^{(\infty)} \), the last term of the commutator series of \( G \). Furthermore, let \( L \) be a subset of \( \text{Hom}(V, V) \) maximal with respect to the conditions that \( L \) is normalized by \( G \), \( L \) contains the identity and \( L \) is a field with respect to the addition and multiplication in \( \text{Hom}(V, V) \). Then there exist integers \( m \) and \( n^* \) such that \( n = mn^* \), \( |L| = p^m \) and \( n^* \) is the dimension of the vector space \( (V, L) \). Also \( G \leq \Gamma L(V, L) \), and \( G \) is transitive on the points of the projective space \( PG(V, L) \).

We define \( \Phi_n(p) \) and \( \Phi^*_n(p) \) as in §3. The transitivity of \( G \) implies that \( (p^{n*} - 1) \mid |G| \) and hence \( \Phi^*_n(p) \mid |G| \). Let \( S \) be the subgroup of \( G \) generated by all Sylow \( r \)-subgroups of \( G \) which have the property \( r \mid \Phi^*_n(p) \).

We have examples of the following types:

I. \( SL(V, L) \leq G \leq \Gamma L(V, L) \).

II. There exists a non-degenerate skew-symmetric scalar product on \( (V, L) \), and \( G \) contains as a normal subgroup the group consisting of all isometries of the corresponding symplectic space.
III. $n^* = 6$, $p = 2$ and $G$ contains a normal subgroup isomorphic to $G_2(2^m)$.

IV. $G$ contains a normal subgroup $E$ isomorphic to an extraspecial group of order $2^{n^*+1}$. Furthermore, $G/E \cong \mathbb{Z}_3$ and $G/E: \mathbb{Z}_3G$ is faithfully represented on $E/\mathbb{Z}_3E$. If $n = 2$, then $n^* = n = 2$ and $|L| = 3, 5, 7, 11$ or $23$. If $n > 2$, then $n^* = n = 4$ and $|L| = 3$.

E1. $G(\infty) \cong SL(2, 5)$, $n^* = 2$ and $|L| = 9, 11, 19, 29$ or $59$.
E2. $G \cong A_6$, $n^* = 4$ and $|L| = 2$.
E5. $G \cong PSU(3, 3)$, $n^* = 6$ and $|L| = 2$.

The classical examples are groups of type I or II. All transitive linear groups of type IV have been described by Huppert (1957) and André (1955, § 6). Up to isomorphism there are only finitely many elements in this class. Note that the four examples of characteristic 3 are at the same time of type I or II. Examples for the exceptional type E1 occur as stabilizers on one point in sharply doubly transitive groups, as described by Zassenhaus (1936). The symplectic group $Sp(4, 2)$ contains as a normal subgroup a group $H \cong A_6$. Also, it acts transitively on the fifteen non-zero vectors in the underlying vector space $W$. Thus the stabilizer on any non-zero vector contains a Sylow 2-subgroup and therefore contains properly the stabilizer of $H$ on this vector. Hence $H$ again must be transitive. The general linear group $GL(W)$, which is isomorphic to $A_8$, contains a subgroup $J$ isomorphic to $A_7$. As in $A_8$ all subgroups isomorphic to $A_6$ are conjugate, we can assume that $H \leq J$ so that $J$ is transitive too. The type E4 has been described by Hering (1970).

If $q = 2^m$, then $PSp(6, q)$ contains a subgroup isomorphic to $G_2(q)$ (see Dickson, 1915). One easily checks that this group is transitive on the corresponding projective space. The group $G_2(2)$ is not simple but contains a subgroup of index 2 isomorphic to $PSU(3, 3)$. This subgroup must be transitive by the argument which we used above for $A_6$.

**Lemma 5.1.** Each reducible normal subgroup of $G$ is cyclic of order dividing $p^a - 1$ for a suitable integer $a$ such that $a \mid n$ and $a < n$.

**Proof.** Let $N$ be a reducible normal subgroup of $G$. Denote by $\mathfrak{B}$ the set consisting of all irreducible $N$-subspaces and by $M$ the set consisting of all endomorphisms of $V$ which leave invariant every element of $\mathfrak{B}$. Then each vector $v$ in $V$ lies in at least one element of $\mathfrak{B}$, as $G$ is transitive on $V - \{0\}$. On the other hand $N \leq M$ so that any two different elements of $\mathfrak{B}$ intersect trivially. So $\mathfrak{B}$ is a partition of $V$, which implies that $M$ is a field. To prove this we only have to show that 0 is the only singular element in $M$. Let $\sigma \in M$ and suppose that there exists a vector $u \in V - \{0\}$ such that $u^\sigma = 0$. Let
$I_u$ be the element of $\Psi$ containing $u$, and let $w$ be an arbitrary element in $V - I_u$. Then there exist subspaces $I_w$ and $I_{u+w}$ in $\Psi$ such that $w \in I_w$ and $u + we \in I_{u+w}$. Here $I_w \neq I_{u+w}$, as otherwise $u \in I_w \cap I_u$ and hence $w \in I_u$. Therefore $w' = (u + w)^p \in I_w \cap I_{u+w} = 0$ and $w' = 0$. Now by the same argument $\sigma$ must be trivial on $V - I_u$ and in particular on $I_u$. So $\sigma = 0$. (For the last argument compare Artin, 1940. Lemma 5.1 also has been proved by H. Lünneburg.)

**Lemma 5.2.** $L$ is unique unless $n = 2$, $n^* = 1$, $p = 3$ and $G$ is isomorphic to a quaternion group of order 8.

**Proof.** Let $L_1$ and $L_2$ be two different subfields of $\text{Hom}(V, V)$ which are normalized by $G$, contain the identity, and are maximal with respect to this property. If $|L_i| = p^{m_i}$ for $i = 1, 2$, then clearly $m_1 | n$, $|G: \mathbb{C}_G L_i| | m_i$ and $|G: \mathbb{C}_G L_1 \cap \mathbb{C}_G L_2| | m_1 m_2$. If $\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2$ is irreducible, then the centralizer in $\text{Hom}(V, V)$ of this group is a field $L_3$ which contains $L_1$ and $L_2$. This field is normalized by $G$, as $\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2 \subseteq G$. Also, it obviously contains the identity. But now $L_1 = L_2 = L_3$ by maximality of $L_1$ and $L_2$. As this contradicts our assumptions, $\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2$ must be reducible. Clearly this group is normal in $G$. Thus by Lemma 5.1 it is cyclic and its order divides $p^a - 1$, where $a | n$ and $a < n$. Therefore

$$p^n - 1 | |G| \leq (p^{n/2} - 1) m_1 m_2 \leq (p^{n/2} - 1) n^2$$

and hence $p^{n/2} + 1 \leq n^2$. Clearly this leaves only finitely many possibilities. However, we don't need that here, because a much stronger statement follows immediately from Theorem 3.9: As $|G: \mathbb{C}_G L_1 \cap \mathbb{C}_G L_2| | n^2$, $\Phi^*_u(p) | | \mathbb{C}_G L_1 \cap \mathbb{C}_G L_2|$ and therefore $\Phi^*_u(p) = 1$, because $\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2$ is reducible. Thus either $n \leq 2$, or $n = 6$ and $p = 2$. Assume that $n = 6$ and $p = 2$. Then $7 | |\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2|$, as $m_1 \leq 6$ and hence $|\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2| = 7$ by Lemma 5.1. Hence a Sylow 3-subgroup $X$ of $G$ has order 9 and is regular on $V - \{0\}$. Thus $X$ is cyclic by Burnside. But this implies that $\mathbb{C}_G L_1$ and $\mathbb{C}_G L_2$ both contain the subgroup of order 3 of $X$. This is impossible as $|\mathbb{C}_G L_1 \cap \mathbb{C}_G L_2| = 7$. The case $n = 1$ is trivial. Assume now that $n = 2$. Then by the above inequality $p \leq 3$. If $p = 2$, then $\text{Hom}(V, V)$ contains only one field containing the identity of order 2 and one of order 4, and certainly $L$ is unique. So $p = 3$ and $|L_i| = 9$. In this case, the normalizer of $L_i$ in $GL(V)$ is one of the Sylow 2-subgroups of $GL(V)$. Any two different of these Sylow 2-subgroups intersect in the normal quaternion group $D$ of $GL(V)$. As $G$ is transitive on $V - \{0\}$, we have $8 | |G|$ and hence $G = D$.

**Lemma 5.3.** If we exclude the case $n = 2$, $n^* = 1$, $p = 3$ and $G \cong Q_8$, then every abelian subgroup of $GL(V)$ which is normalized by $G$ is contained in $L$.

**Proof.** Let $X$ be an abelian subgroup of $GL(V)$ which is normalized by $G$. 


As $G$ is transitive, $X$ has only one homogeneous component. By [TL, Hilfssatz 5] the $GF(p)$-algebra generated by $X$ is a field $L_1$. Clearly $L_1$ contains $X$ and therefore the identity. Also $L_1$ is normalized by $G$. Thus $L_1 \leq L$ by Lemma 5.2.

**Lemma 5.4.** If $S \neq 1$, then $L$ is the centralizer of $S$ in $\text{Hom}(V, V)$.

**Proof.** Assume that $S \neq 1$. Then $S$ is irreducible, and therefore the centralizer $X$ of $S$ in $\text{Hom}(V, V)$ is a field. Also $[G: \text{C}_G L] = m | n$ so that $(\Phi_n^*(p), [G: \text{C}_G L]) = 1$. Hence $S$ centralizes $L$, i.e., $L \leq X$. But this implies $L = X$ because of the maximality of $L$.

**Theorem 5.5.** If $F \nsubseteq L$, then $G$ is of type IV or $G$ is of type I, $n^* = 1$, $n = 2$ and $p + 1 = 2^a$ for a suitable $a$.

**Proof.** Assume that $F \nsubseteq L$ and consider at first the case $n = n^* = 2$. Then $L$ is the prime field, and $G$ centralizes $L$. As $F \nsubseteq L$, there exists a prime $s$ such that the Sylow $s$-subgroup $F_s$ of $F$ is not contained in $L$. Let $E$ be a subgroup of $G$ which is minimal with respect to the properties $E \leq G$, $E \nsubseteq F_s$ and $E \nsubseteq L$. Then every proper characteristic subgroup of $E$ is contained in $E \cap L$ and hence is cyclic and central. Thus by Lemma 5.3 we can assume that $E$ is not abelian. Hence $E$ is of type (c) or (d) in Lemma 2.1, and therefore contains an extraspecial group of index $\leq 2$ and of order $s^{2a+1}$ for a suitable $a$. Here $s \mid |3F_s| = |L| - 1$. Hence $s \neq p$ and $n = 2 > s^a$ by Lemma 2.2. Therefore $s = 2, a = 1$ and $p \neq 2$. Thus $E$ cannot be of type (d); actually it is a quaternion group of order 8. Now $\text{C}_G E = \text{Z}G$ by Lemma 2.2. Also $G/\text{Z}G$ is faithfully represented on $E/\text{Z}E$. Clearly $\text{Z}G \leq L$ and hence $|G| \mid (p - 1) 24$. So $p + 1 \mid 24$, which implies that $p = 3, 5, 7, 11$ or 23.

Suppose now that $\Phi_n^*(p) \neq 1$. Then $F$ is not contained in $\text{C}_G S$ by Lemma 5.4. Therefore there exists a prime $r$ dividing $\Phi_n^*(p)$ and a Sylow $r$-subgroup $R$ such that the normal closure $\overline{R}$ of $R$ in $G$ does not centralize $F$. Applying Theorem A to this situation we see that $\Phi_n^*(p) = n + 1$ and $n$ is a power of 2. Also $p \neq 2, |L| = p$ and $n \geq 2$. Thus by § 3 we have either $n = 2$ and $|L| = p$ or $n = 4$ and $|L| = p = 3$. The first possibility implies $n = n^* = 2$ and was considered above. If $|L| = 3$, then $|\text{Z}G| \leq 2$. Hence in this case $F$ is an extraspecial group, and $G$ is of type IV.

Finally, suppose that $\Phi_n^*(p) = 1$. By Zsigmondy's theorem (see § 3) either $n = 2$ and $p + 1 = 2^a$ for a suitable $a$ or $n = 6$ and $p = 2$. Consider the case $n = 6$ and $p = 2$. Again, let $s$ be a prime such that the Sylow $s$-subgroup $F_s$ of $F$ is not contained in $L$. We always have $3F_s \leq L$ because of Lemma 5.3. Thus $F_s$ is not abelian and furthermore, $s = 3$ or $s = 7$ as $|L| = 2, 4, 8$ or 64. But $s = 7$ is impossible as $GL(6, 2)$ has abelian Sylow 7-subgroups. Thus $F_s$ is a 3-group. Let $X$ be a Sylow 7-subgroup of $G$. Then $X$ centralizes $F_s$, and
since the order of $F_s$ divides the order of $GL(6, 2)$ and hence is not larger than $3^4$. But $C_G F_s$ is a field, as $F_s$ is irreducible by Lemma 5.1. So $X < C_G F_s < L$ and hence $3 \cdot 7 \mid |L| - 1$, i.e., $|L| = 2^6$. This implies that $X \cup \{0\}$ is a subfield of order 8 and therefore $|C_G X : (C_G X \cap L)| = 2$. Hence $C_G X$ has cyclic Sylow 3-subgroups. But this is impossible as $F_s < C_G X$.

Thus $n = 2$ and $p + 1 = 2^a$. If in addition $n^* = 2$, then $G$ is of type IV, as we have seen above. So there only remains the case $n^* = 1$.

COROLLARY 5.6. (Huppert). If $G$ is solvable, then either $n^* = 1$ and $G$ is of type I, or $G$ is of type IV.

Proof. If $G$ is solvable, then $C_G F < F$. In the case $F < L$ this implies that $G \cap L \geq F \geq C_G F \geq C_G L$ and $|G|/|G \cap L| \leq |G/C_G L| \leq |\text{Aut}(L)|$, where $\text{Aut}(L)$ is the group of automorphisms of the field $L$. Thus $|G| \leq m(p^m - 1)$ and $(p^n - 1)/(p^m - 1) \leq m$, which is only possible if $m = n$, i.e., $n^* = 1$. Obviously now $G$ is of type I.

In the exceptional case $F \leq L^*$ we can apply Theorem 5.5.

LEMMA 5.7. If $n^* = 3$, then $G$ is of type I.

Proof. We have $S \neq 1$, because in the solvable case $n^* = 1, 2$ or 4 by Corollary 5.6. So $S/F(S)$ has even order by the theorem of Feit and Thompson (1963). (Of course this fact can easily be established without the help of the Feit-Thompson theorem.) Also $F(S) < F < L$ by Theorem 5.5. Hence $F(S) = S \cap L$, and $S/F(S)$ is isomorphic to the subgroup $S^*$ of $PGL(V, L)$ induced by $S$. Clearly $S^* \leq PSL(V, L)$, as $S^*$ is perfect. So every involution in $S$ is a central involution, and by Wagner (1959) $S^*$ contains $PSL(V, L)$. This implies that $S = SL(V, L)$.

THEOREM 5.8. If $S \neq 1$, then the following statements hold:

(a) $SF/F$ is simple.
(b) $G/S$ is isomorphic to a factor of the metacyclic group $\Gamma L(1, p^n)$.
(c) $C_G S = \mathbb{Z} F \leq L$.
(d) $\Phi^*(p) \mid |SF/F|$.
(e) $C_{G/F} SF/F = 1$.
(f) Assume that $\Phi^*(p) \neq 1$. Let $r$ be a prime dividing $\Phi^*(p)$, $R$ a Sylow $r$-subgroup of $G$ and $\bar{S}$ the normal closure of $R$ in $G$. Then $S = \bar{S} = \bar{S}$.
(g) $L$ is the centralizer of $S$ in $\text{Hom}(V, V)$.

Proof. (g) By Lemma 5.1 $S$ is irreducible. Thus by Schur's lemma the centralizer $L$ of $S$ in $\text{Hom}(V, V)$ is a field, and clearly this field contains the identity and is left invariant by $G$, as $S \leq G$. On the other hand $S \leq \Gamma L(V, L)$ implies $S \leq GL(V, L)$, as $S$ is perfect. Hence $L \leq L$ and therefore $L = L$ because of the maximality of $L$. 


(f) Assume that $Φ^*_n(p) \neq 1$, and let $r$ be a prime divisor of $Φ^*_n(p)$. Obviously $r \mid Φ^*_n(p) \mid p^n - 1 \mid |G|$, and we can apply the results of § 4. Let $R$ be a Sylow $r$-subgroup of $G$ and $\bar{S}$ the normal closure of $R$ in $G$. Then $\bar{S} = G^{(∞)}$, by Theorem B(b) and $\bar{S} = S$ by Theorem B(d).

(d) Clearly $|L| < p^n$, as $G$ is not solvable. So (d) follows from Theorem B.

In the case $Φ^*_n(p) = 1$, all remaining properties follow from Theorem B in § 4. So we can assume that $Φ^*_n(p) = 1$. Then $F \leq L$ by Theorem 5.5 (note that $G$ is not solvable). Thus clearly $F = F \cap G$, and this together with (g) implies (c).

Assume that $n = 2$ and $p + 1 = 2^a$ for a suitable $a$, and let $X$ be a Sylow 2-subgroup of $G$. Then $X$ is a subgroup of order at least $2^{a+1}$ of a Sylow 2-subgroup of $GL(2, p)$, which is a semidihedral group of order $2^{a+2}$. Thus $X$ is cyclic, a quaternion group, a dihedral group or a semidihedral group. On the other hand $X$ contains the normal subgroup $X \cap S$, and this normal subgroup is a quaternion group, as $S$ is perfect and therefore contained in $SL(2, p)$. Hence $X$ is a quaternion group or a semidihedral group, and $|X \cap S| \geq 2^a$, as $X \cap S \leq X$. If $S^*$ is the image of $S$ in $PGL(2, p)$, then by Dickson (1901) either $S^* \cong PSL(2, p)$ or $S^* \cong A_5$. But by the above $2^{a-1} \mid |S^*|$, So $S^* \cong A_5$ implies $a \leq 3$ and hence $p = 3$ or 7. In both these cases $5 \nmid |GL(2, p)|$, which leads to a contradiction. Therefore $S^* \cong SF/F \cong PSL(2, p)$ and $S \cong SL(2, p)$. So we have (a) and also (b), since $GL(2, p)/SL(2, p)$ is a cyclic group of order $p - 1$. Also, one easily derives (e): Let $Y/F = \mathbb{C}_{G/F}SF/F$, and let $Y^*$ be the image of $Y$ in $PGL(2, p)$. Then $Y^* \cap S^* = 1$ and hence $|Y^*| \leq 2$. If $Y^* \neq 1$, then $Y^*S^* = Y^* \times S^*$ contains elementary abelian groups of order 8, which is impossible.

By Theorem 3.9 there only remains the case $n = 6$ and $p = 2$. To finish the proof of Theorem 5.8 we show the following:

**Lemma 5.9.** If $n = 6$ and $p = 2$, then $G$ is of type I, II, III or E5.

**Proof.** It is easy to verify this by inspection.

We should point out some implications of Theorem 5.8 about transitive linear groups $G$ with the properties $F \leq L$ and $S \neq 1$. Note that in view of Theorem 5.5 and Corollary 5.6 such groups can be considered to be the general type of transitive linear groups.

Clearly $L \cap G \leq F$, so actually $F = G \cap L$. The group

$$GL^*/L^* \cong G/G \cap L^* = G/F,$$

where $L^*$ is the multiplicative group of $L$, is a subgroup of $PFL(V, L)$ which acts transitively on the points of the projective space $PG(V, L)$. This group contains the simple normal subgroup

$$SL^*/L^* \cong S/S \cap L^* = S/S \cap F = SF/F.$$
which, being perfect, must lie in $\text{PSL}(V, L)$. Also because of Theorem 5.8(e) $G/F$ is isomorphic to a subgroup of $\text{Aut}(SF/F)$. So we obtain

\[(*) \quad \frac{p^{mn*} - 1}{p^m - 1} \mid |G/F| \mid |\text{Aut}(SF/F)|.
\]

Also $S$ has a faithful linear representation of degree $n^*$ over $L$ and $SF/F \cong S/F \cap S = S/F(S)$ has a faithful projective representation of degree $n^*$ over $L$.

**Lemma 5.10.** If $n^* = 1$, then $G$ is of type I. If $n^* = 2$, then $G$ has one of the types I, IV or E1.

**Proof.** If $n^* = 1$, then $\text{SL}(V, L) = 1$, and trivially $G$ is of type I. Consider the case $n^* = 2$. Because of Theorem 5.5 and Corollary 5.6 we can assume that $F \leq L$ and that $G$ is not solvable. Hence $\text{SL}^*/L^*$ is a simple normal subgroup of $\text{GL}^*/L^*$ contained in the two-dimensional group $\text{PSL}(V, L)$. By the result of Dickson (1901) $\text{SL}^*/L^*$ is isomorphic to $\text{PSL}(2, p^s)$, where $s \mid m$, or $\text{SL}^*/L^* \cong A_5$ and $p^m \equiv \pm 1 \pmod{10}$. If $\text{SL}^*/L^* \cong \text{PSL}(2, p^s)$, then the number of Sylow $p$-subgroups of $\text{SL}^*/L^*$ is $p^s + 1$. Each of these Sylow $p$-subgroups leaves invariant exactly one point of the projective line $\text{PG}(V, L)$.

On the other hand, $\text{GL}^*/L^*$ is transitive on $\text{PG}(V, L)$. This implies $p^s = p^m = |L|$ and $S/F(S) \cong \text{SL}^*/L^* \cong \text{PSL}(V, L)$. Obviously $S \leq \text{SL}(V, L)$ and hence $S = \text{SL}(V, L)$, which implies that $G$ is of type I.

Assume now that $\text{SL}^*/L^* \cong A_5$. Then by (*) $p^m + 1 \mid |\text{Aut}(A_5)| = |S_5| = 120$, and furthermore $p^m \equiv \pm 1 \pmod{10}$. So $G$ is of the exceptional type E1.

**Lemma 5.11.** If $n^* > 2$ and $n \equiv 0 \pmod{2}$, then $\Phi_{n/2}(p) \mid |G/F|$. 

**Proof.** Clearly $\Phi_{n/2}(p) \mid p^{n/2} - 1 \mid |G|$. Suppose that there exists a prime $r$ dividing $\Phi_{n/2}(p)$, $|F|$. Then $r \mid |3F|$. But by Lemma 5.3 always $3F \leq L$. Thus $r \mid L$ and hence $m \equiv n/2$ so that $n^* \equiv 2$, which contradicts our hypothesis.

**Theorem 5.12.** If $SF/F \cong A_i$, where $A_i$ is the alternating group of degree $i \geq 5$, then $n^* = 2$, $p^x = 2^4$, or $p^x = 3^4$.

**Proof.** Certainly $\Phi_n(p) \mid p^n - 1 \mid |G|$ because of the transitivity of $G$. If $\Phi_n(p) > 1$, then by Theorem 5.8 (f) and Corollary 4.4 we are immediately limited to finitely many cases.

Clearly we can assume that $n^* > 3$, and therefore $\Phi_{n/2}(p) \mid |G/F|$ whenever $n \equiv 0 \pmod{2}$ (see Lemma 5.11). As $G/F$ is isomorphic to a subgroup of the automorphism group of $A_i$, which contains the group of inner automorphisms as a subgroup of index 2 or 4, we actually have $\Phi_{n/2}(p) \mid |A_i|$. Thus no prime
divisor of $\Phi_m^*(p)$ is larger than $i$. On the other hand $i < 2r$ for any prime $r$ dividing $\Phi_m^*(p)$, as we have seen in the proof of Theorem 4.3. This excludes the orders $2^{10}, 2^{18}$ and $5^6$. Suppose now that $n = 6$ and $p = 3$. Then $13 = \Phi_3^*(3) \mid |A_4|$ and hence $\frac{1}{2}13! \mid |GL(6, 3)|$, which again is impossible. So we are left with the cases $2^4, 2^6, 2^{12}$ and $3^4$.

If $p^n = 2^6$, then $i = 7$ or $i = 8$ by Corollary 4.4. Also, by Lemma 5.9 we have five possibilities for $SF/F$. But none of these is isomorphic to either $A_7$ or $A_8$. Consider the case $p^n = 2^{12}$. Here $i = 13$ or $i = 14$, again because of Corollary 4.4. By Theorem 5.5 the Fitting group $F$ is contained in $L$. Hence by Theorem 5.8 $F = \mathfrak{Z}F = \mathfrak{C}_6S$. So $F \cap S$ is isomorphic to a subgroup of the Schur multiplier of $S/F \cong A_4$. On the other hand $F \cap S$ has odd order, as $F \cap S \leq L$. Therefore $F \cap S = 1$ by Schur (1911). So $S \cong A_4$ and $G \cong S_4$ or $G \cong A_4$ by Theorem 5.8(e). However, in the case considered here $p^n - 1$ is odd. So the fact that $G$ is transitive on $V - \{0\}$ implies that $S$ itself is transitive on $V - \{0\}$. But this is impossible, as neither $A_{13}$ nor $A_{14}$ has a subgroup of index $2^{12} - 1$ (see Lemma 2.5).

**THEOREM 5.13.** If $SF/F \cong PSL(\tilde{n}, \tilde{q})$, where $\tilde{q}$ is a power of a prime $\tilde{p}$, $\tilde{q} = p^n$ and $\tilde{n} \geq 2$, then $G$ is of type I, unless we have done one of the following cases:

(a) $n^* = 2$, $G$ is of type $E_1$.
(b) $n^* = n = 4$, $p = 2$, $S \cong PSL(2, 9) \cong A_6$, $G$ is of type II or $E_2$.
(c) $n^* = n = 4$, $p = 3$, $SF/F \cong PSL(2, 5)$, $G$ is of type $IV$.
(d) $G$ is of type $E_4$.
(e) $q^* = p^n$ but $|L| \neq \tilde{q}$, $\tilde{n} > 2$.

**Proof.** If $n^* \leq 3$, then $G$ must be of type I or $E_1$ by Lemma 5.7 and Lemma 5.10 (note that $S \neq 1$, i.e., $G$ is not solvable by assumption, and therefore not of type IV if $n^* = 2$). So we can assume that $n^* > 3$.

In the following we have to distinguish the two cases $p = \tilde{p}$ and $p \neq \tilde{p}$, as they are totally different. Assume at first that $p \neq \tilde{p}$. If $\Phi_m^*(\tilde{p}) = 1$, then $n = 6$ and $p = 2$, as certainly $n \geq n^* > 2$. Using Lemma 5.11 we find that $7 = \Phi_3^*(2) \mid |G/F|$. As $SF/F$ is isomorphic to a factor of $GL(6, 2)$, we have $\tilde{m}(\tilde{n} - 1)/2 \leq 4$ and hence $7 \nmid |G/F:SF/F|$ by Theorem 5.8(e). So actually $7 \nmid |SF/F|$. This together with the condition $|SF/F| \mid |GL(6, 2)|$ leaves only the possibility $q^* = 7$. Here $n^* = 6$ as $n^* > 3$, hence $|L| = 2$ and $F = 1$. So $|G| \leq |\text{Aut}(PSL(2, 7))| = 6 \cdot 7 \cdot 8$. But this number is not divisible by $2^6 - 1$. Hence $\Phi_m^*(p) \neq 1$, and we can apply the results of § 4. In particular, we have only finitely many possibilities by Theorems 5.8(f), 4.6 and 3.9.

If $\tilde{n} = 2$ and $\tilde{q} = 4$, then $\Phi_m^*(p) \mid |PSL(2, 4)| = 60$, and $\Phi_m^*(p) = 5$. Note that every prime divisor of $\Phi_m^*(p)$ is greater than 3, because $n^* > 2$. Thus $n = 4$ and $p = 2$ or 3. As we assume that $p \neq \tilde{p}$, there remains only the case $n = 4$ and
$p = 3$. Since $n^* > 3$, we have $n^* = 4$ and $|L| = 3$. Suppose now that $F \leq L$. Then $|F| = 2$ and $|G/F| = |\text{Aut}(\text{PSL}(2, 4))| = 120$ so that $|G| = 2^4 \cdot 3 \cdot 5$. Therefore the Sylow 2-subgroups are semi-regular on $V - \{0\}$. Hence they are quaternion groups, as otherwise $SF/F$ would have cyclic Sylow 2-subgroups. Let $X$ be a Sylow 5-subgroup of $S$. As the number of Sylow 5-subgroups of $S$ is 6, $\mathcal{R}_G X$ contains a quaternion group $Q$ of order 8. Also $Q \cap \mathbb{C}_G X$ is a cyclic group of order 4. However, the subalgebra of $\text{Hom}(V, V)$ generated by $X$ is a field of order $3^4$, and $\mathbb{C}_G X$ is the multiplicative group $M^*$ of $M$. So $Q \cap \mathbb{C}_G X$ is the unique cyclic subgroup of order 4 in $M^*$. Also, all elements of $Q$ induce automorphisms of order 1 or 2 of $M$ and hence centralize a subfield of order 9 of $M$. But this implies that $Q$ is abelian, a contradiction. So $F \nsubseteq L$, and $G$ is of type IV by Theorem 5.4.

If $\bar{n} = 2$ and $\bar{q} = 9$, then $SF/F \cong \text{PSL}(2, 9) \cong A_6$. Again $\Phi_n^*(p) = 5$ and hence $n = 4$ and $p = 2$ or 3. Because of the assumption $p \neq \bar{p}$, there only remains the case $n = 4$ and $p = 2$. Again, $n^* = 4$ so that $|L| = 2, F = 1$ and $S \cong \text{PSL}(2, 9) \cong A_6$. Now $\text{GL}(4, 2) \cong A_8$, and all subgroups isomorphic to $A_6$ of $A_8$ are conjugate. Therefore $S$ is the commutator subgroup of the stabilizer $\text{Sp}(f)$ of a suitable symplectic form $f$. Let $X$ be the normalizer of $S$ in $\text{GL}(4, 2)$. Then $X/S$ is isomorphic to a factor of $\Gamma L(1, 2^4)$ and at the same time isomorphic to a subgroup of the outer automorphism group of $S$ (see Theorem 5.8 (b) and (e)). The first group has cyclic Sylow 2-subgroups, while the second is an elementary abelian group of order 4. So $|X/S| = 2$ and $X = \text{Sp}(f)$, which implies that $G$ is of type II or E2.

If $\bar{n} = 3$ and $q = 2$ or 4, then $\Phi_n^*(p) = 7$. Hence $n | 6$, and actually $n = 6$, as $n \geq n^* > 3$. Also $p = 3$ or 5 by Theorem 3.9. On the other hand $\Phi_3^*(p) | \text{PGL}(n, \bar{q})$ as $n^* > 2$ (see Lemma 5.11). This leads to a contradiction.

In the following we assume that $\bar{q} \neq 4, 9$ if $\bar{n} = 2$ and $\bar{q} \neq 2, 4$ if $\bar{n} = 3$. If $F \nsubseteq L$, then $SF/F$ is isomorphic to a factor of the automorphism group of an extraspecial group of order $2^5$ by Theorem 5.5. This means that $SF/F \cong \cong \text{PSL}(2, 4) \cong \text{PSL}(2, 5)$, and we have (c). So we can assume in addition that $F \subseteq L$. Then by [PR, Theorem 4.2] $n \geq n^* \geq (q^8 - 1)/d$, where $d = (n, \bar{q} - 1)$. Together with Lemma 4.5 this implies that no prime divisor of the order of $|G/F|$ is larger than $2n + 1$. This excludes the cases $p^* = 17^6, 3^4 8, 5^6, 2^1 8$, and $2^{10}$, as $\Phi_n^*(p) | |G/F|$, whenever $2 | n$. So $\Phi_n^*(p)$ is equal to a prime $r$, and by Lemma 4.5 we have $r = \bar{p}$ or $r = (\bar{q}^8 - 1)/d (\bar{q} - 1)$, as

$$r \geq n + 1 \geq (q^8 - 1)/d + 1.$$ 

Furthermore, if $r = 2n + 1$, then $r = \bar{p}$ or $\bar{q} = 2$ and $r + 1 = 2^8$. This excludes $p^* = 2^8$ and $p^* = 2^{10}$. Furthermore, $p^* = 2^3$ is excluded because of our condition $n^* > 3$. 

By Theorem 4.6 we have $\Phi_k^*(p) = (n+1)(2n+1)$ or $(n+1)(2n+1)$. Hence because of Theorem 3.9 and the above we are only left with the cases $p^* = 2^4, 2^{12}, 3^4$ and $3^6$. In particular $r = 5, 7$ or 13.

To finish our proof, we have to determine, in how many ways $r$ can be represented as a generalized Mersenne prime, i.e., in the form $r = (\bar{q}^n - 1)/d(\bar{q} - 1)$, where $\bar{q}$ is a power of a prime and $d = (\bar{n}, \bar{q} - 1)$. We see that $r \leq 13$ implies that $\bar{n} \leq 3$: Suppose that $\bar{n} \geq 4$. Then $13 \geq r \geq (\bar{q}^4 - 1)/d(\bar{q} - 1) = \bar{q}^2 + 1$ so that $\bar{q} \leq 3$. However $\bar{q} = 2$ implies $d = 1$ and $\bar{q} = 3$ implies $d \leq 2$. Hence we obtain a contradiction in both cases. Using this it is easy to determine all possibilities: $r = 5, \bar{n} = 2, \bar{q} = 4$ or 9; $r = 7, \bar{n} = 2, \bar{q} = 13$; $r = 7, \bar{n} = 3, \bar{q} = 2$ or 4; $r = 13, \bar{n} = 2, \bar{q} = 25$; $r = 13, \bar{n} = 3$. Most of these cases are not allowed by the above assumption. Consider the case $r = 7, \bar{n} = 2, \bar{q} = 13$: Here $n = 6$ and $p = 3$. Also $n^* \mid 6$ and hence $n^* = 6$, as we are assuming that $n^* > 3$. Suppose that $S \cong PSL(2, 13)$. Then $S$ contains a dihedral group of order $2 \cdot 7$. If $\alpha$ is an involution in this group, then $|C_{\alpha} \alpha| = 3^2$ by [TL, Hilfssatz 5]. Also, the number of involutions in $S$ is $7 \cdot 13$, and all involutions in $S$ are conjugate to $\alpha$. Counting the pairs consisting of a non-zero vector and an involution in $S$ fixing this vector we obtain the equality $(3^6 - 1)b_1 = 7 \cdot 13 \cdot 26$, where $b_1$ is the number of involutions in $S$, for $v \in V - \{0\}$. Note that $b_1$ is independent of the choice of $v$, as $G$ is transitive on $V - \{0\}$. Clearly the above equality is impossible, which proves that $S \not\cong PSL(2, 13)$, i.e., $S \cap F \neq 1$. On the other hand $F \leq L$ by Theorem 5.5. So actually $F = S \cap F = L - \{0\}$. Now it follows from Theorem 5.8 (g) and the work of Schur (1907) that $S \cong SL(2, 13)$. Also, by Theorem 5.8 (e) the factor group $G/F$ is isomorphic to a subgroup of the automorphism group of $PSL(2, 13)$, which is $PGL(2, 13)$. Suppose that $G > S$. Then $G/F \cong PGL(2, 13)$, and $G$ contains an involution $\beta$ which fixes a non-zero vector. The unique involution in $S$ lies in $L$ and hence acts as the $-1$ on $V$. Therefore the Sylow 2-subgroups of $S$, which are quaternion groups, are fixed-point-free on $V - \{0\}$. In particular $\beta \notin S$ and hence $\beta F$ does not belong to the commutator subgroup of $G/F$. This implies that $C_{G/F}(\beta F)$ is a dihedral group of order $4 \cdot 7$ and therefore $7 \mid |C_{G}\beta|$. Clearly this is impossible, so that $G = S \cong SL(2, 13)$, i.e., $G$ is of type E4. Suppose that $r = 13, \bar{n} = 2$ and $\bar{q} = 25$. Then $n \geq n^* \geq 12$, hence $n = 12, |L| = 2, |F| = 1$ and $2^{12} - 1 \mid |G|$ $|PGL(2, 25))$, which is impossible. If $r = 13, \bar{n} = 3$ and $\bar{q} = 3$, then $n^* \geq 8$ so that again $n = 12, |L| = 2$ and $|F| = 1$. But this is impossible as $5 \mid PGL(3, 3)$. Therefore the Sylow 2-subgroups of $S$, which are quaternion groups, are fixed-point-free on $V - \{0\}$. In particular $\beta \notin S$ and hence $\beta F$ does not belong to the commutator subgroup of $G/F$. This implies that $C_{G/F}(\beta F)$ is a dihedral group of order $4 \cdot 7$ and therefore $7 \mid |C_{G}\beta|$. Clearly this is impossible, so that $G = S \cong SL(2, 13)$, i.e., $G$ is of type E4. Suppose that $r = 13, \bar{n} = 2$ and $\bar{q} = 25$. Then $n \geq n^* \geq 12$, hence $n = 12, |L| = 2, |F| = 1$ and $2^{12} - 1 \mid |G|$ $|PGL(2, 25))$, which is impossible. If $r = 13, \bar{n} = 3$ and $\bar{q} = 3$, then $n^* \geq 8$ so that again $n = 12, |L| = 2$ and $|F| = 1$. But this is impossible as $5 \mid PGL(3, 3)$. Therefore the Sylow 2-subgroups of $S$, which are quaternion groups, are fixed-point-free on $V - \{0\}$. In particular $\beta \notin S$ and hence $\beta F$ does not belong to the commutator subgroup of $G/F$. This implies that $C_{G/F}(\beta F)$ is a dihedral group of order $4 \cdot 7$ and therefore $7 \mid |C_{G}\beta|$. Clearly this is impossible, so that $G = S \cong SL(2, 13)$, i.e., $G$ is of type E4. Suppose that $r = 13, \bar{n} = 2$ and $\bar{q} = 25$. Then $n \geq n^* \geq 12$, hence $n = 12, |L| = 2, |F| = 1$ and $2^{12} - 1 \mid |G|$ $|PGL(2, 25))$, which is impossible. If $r = 13, \bar{n} = 3$ and $\bar{q} = 3$, then $n^* \geq 8$ so that again $n = 12, |L| = 2$ and $|F| = 1$. But this is impossible as $5 \mid PGL(3, 3)$. Therefore the Sylow 2-subgroups of $S$, which are quaternion groups, are fixed-point-free on $V - \{0\}$. In particular $\beta \notin S$ and hence $\beta F$ does not belong to the commutator subgroup of $G/F$. This implies that $C_{G/F}(\beta F)$ is a dihedral group of order $4 \cdot 7$ and therefore $7 \mid |C_{G}\beta|$. Clearly this is impossible, so that $G = S \cong SL(2, 13)$, i.e., $G$ is of type E4. Suppose that $r = 13, \bar{n} = 2$ and $\bar{q} = 25$. Then $n \geq n^* \geq 12$, hence $n = 12, |L| = 2, |F| = 1$ and $2^{12} - 1 \mid |G|$ $|PGL(2, 25))$, which is impossible. If $r = 13, \bar{n} = 3$ and $\bar{q} = 3$, then $n^* \geq 8$ so that again $n = 12, |L| = 2$ and $|F| = 1$. But this is impossible as $5 \mid PGL(3, 3)$.
Let $p = 2$ and $n^* \geq 6$ so that $5 \nmid |F|$ and hence $5 \mid |G/F| \mid PGL(2, 13)$. So again we do not obtain any transitive linear groups.

Assume now that $p = p$. As a consequence of the results of § 3 we obtain

\[(**) \quad \text{If } p = p, \text{ then } \bar{m}n = n.\]

This holds for any dimension $n^*$, as we can see in the following way: By Theorem 5.8 (d) we have $\Phi_n^*(p) \mid |SF/F| \mid GL(n, p^m)$. Hence every prime dividing $\Phi_n^*(p)$ must divide a number of the form $p^{nk} - 1$, where $k \leq n$. Thus $\bar{m}n \geq n$, whenever $\Phi_n^*(p) \neq 1$. On the other hand $\Phi_n^*(p) \mid |PSL(n, p^m)|$, which implies that every prime divisor of $\Phi_n^*(p)$ divides a number of the form $p^k - 1$, where $k \leq n$. Hence $\bar{m}n \leq n$, whenever $\Phi_n^*(p) \neq 1$. Thus (**) is true, if both $\Phi_n^*(p)$ and $\Phi_n^*(p)$ are different from 1.

Consider the case $\Phi_n^*(p) = 1$: If $n = 2$, then the perfect group $SL^*/L^* \cong \cong PSL(\bar{n}, p^m)$ is contained in $PSL(2, p)$, and hence obviously $\bar{n} = 2$ and $\bar{m} = 1$. Because of Theorem 3.9, the only possibility of dimension $\geq 2$ is $n = 6$ and $p = 2$. In this case clearly $\bar{m}n \leq 6$, as $\Phi_n^*(2) \mid |GL(6, 2)|$. Suppose that $\bar{m}n \leq 5$, and let $X$ be a Sylow 3-subgroup of $G$. If $3 \nmid |F|$, then $X$ is isomorphic to a subgroup of $PGL(n, p^m)$ by Theorem 5.8. Here $\bar{m}n \leq 2$ as $\bar{n} \geq 2$. Thus $X$ actually is isomorphic to a subgroup of $PGL(2, 2^m)$. Hence $X$ is elementary abelian and of order at most 9. But this implies that $X$ acts regularly on $V^*$ and leads to a contradiction to a theorem of Burnside (see Huppert, 1967, p. 499, 8.7b). So $3 \mid |F|$, which implies that $3 \mid |S| \mid |3F|$ and hence $|L| = 4$ and $n^* = 3$. Thus $G$ is of type I by Lemma 5.7 and $PSL(\bar{n}, 2^m) \cong SF/F \cong PSL(3, 4)$. Comparing the orders of the Sylow 2-subgroups, we see that $\bar{n} = 4$ and $\bar{m} = 1$. But the center of the Sylow 2-subgroup of $PSL(4, 2)$ has order 2, while the center of a Sylow 2-subgroup of $PSL(3, 4)$ has order 4, a contradiction.

Next we prove:

\[\text{If } \bar{n} = 2 \text{ and } \bar{p} = p, \text{ then } n^* = \bar{n} \text{ and } |L| = \bar{q}.\]

\[\text{Proof.} \]Clearly $F \leq L$ by Theorem 5.5. Hence $S \cap F \leq 3S$, and therefore the number of Sylow $p$-subgroups of $S$ is equal to the number of Sylow...
$p$-subgroups of $F/S$, namely, $\bar{q} + 1$. Let $\mathcal{J}_1, \ldots, \mathcal{J}_{\bar{q}+1}$ be the fixed-point-spaces of these groups. Obviously these spaces are non-trivial, and because of the transitivity of $G$ we have that

$$\bigcup_{1 \leq i \leq \bar{q} + 1} \mathcal{J}_i = V.$$ 

Furthermore, any two Sylow $p$-subgroups of $S$ generate $S$. Hence $\mathcal{J}_i \cap \mathcal{J}_j = 0$ for $i \neq j$. As $|V| = p^n = \bar{q}^{\bar{q}} = \bar{q}^2$, the set $\{\mathcal{J}_1, \mathcal{J}_2, \ldots, \mathcal{J}_{\bar{q}+1}\}$ is a congruence. This congruence determines a translation plane $\mathcal{A}$, and all $p$-elements of $S$ are shears of $\mathcal{A}$. It follows that $S \cong SL(2, \bar{q})$ and that $\text{Hom}(V, V)$ contains a field of order $\bar{q}$ centralizing $S$ (see Hering, 1972, Theorems 2 and 3 and Lemma 7). So $L = \bar{q}$.

**Theorem 5.14.** $SF/F$ cannot be isomorphic to Janko's group of order 175560.

*Proof.* Suppose that $SF/F \cong J_1$, where $J_1$ is the simple group of order 175560 described by Janko (1966). Then $p = 2$, $n = 18$ and $G \cong J_1$ by Theorem 4.8. But this is impossible, as it implies that $2^{18} - 1 \mid |J_1|$.

**Theorem 5.15.** If the Sylow 2-subgroups of $G$ are cyclic, then $n^* = 1$, and $G$ is of type I.

If the Sylow 2-subgroups of $S$ are ordinary or generalized quaternion groups, then $n^* \leq 2$ and $G$ is of type I, IV, E1 or E4.

*Proof.* Assume that the Sylow 2-subgroups of $G$ are cyclic or the Sylow 2-subgroups of $S$ are (generalized) quaternion groups. If $G$ is solvable, then by Corollary 5.6 either $n^* = 1$ and $G$ is of type I, or $G$ is of type IV. Suppose that $G$ is of type IV. Then clearly the Sylow 2-subgroups of $S$ are generalized quaternion groups. Also the case $n^* = 4$, $|L| = 3$ is not possible, as in this case $F$ contains more than one involution. Hence we can assume that $G$ is not solvable. As a Sylow 2-subgroup $Y$ of $SF/F$ is isomorphic to a factor of a Sylow 2-subgroup of $S$, $Y$ is cyclic, a (generalized) quaternion group or a dihedral group. By Theorem 5.8 the factor $SF/F$ is a non-abelian simple group. If $Y$ is cyclic, then $Y = 1$ and $SF/F$ is solvable by the theorem of Feit and Thompson, a contradiction. Also $Y$ cannot be a quaternion group by the theorem of Brauer and Suzuki (see Brauer, 1959). Thus $Y$ is a dihedral group. By a result of Gorenstein and Walter (1962) this implies that $SF/F$ is isomorphic to some $PSL(2, q)$ or to $A_7$.

The fact that $Y$ is a dihedral group implies that $2 \mid F$, hence $2 \mid |3F| \mid |L| - 1$, and therefore $p \neq 2$. The theorem now follows from Theorems 5.12 and 5.13.
§6. ON COMPOSITION FACTORS OF FINITE DOUBLY TRANSITIVE GROUPS

Let $G$ be a finite doubly transitive permutation group. Denote by $A$ the maximal solvable normal subgroup of $G$ and by $E(G)$ the group generated by all minimal normal subgroups of $G/A$. Then $E(G)$ is a simple group. This follows from a result of Burnside (1911), if $G$ does not contain a sharply transitive normal subgroup. If $G$ does contain a sharply transitive normal subgroup, then actually $G$ has at most one non-solvable composition factor (see [TL, pp. 159-161]). The structure of solvable doubly transitive groups is known completely by Huppert (1957). Therefore, we can assume that $E(G) \neq 1$. It is easy to see that in this case the degree of $G$ is not larger than the square of the order of the automorphism group of $E(G)$. So for each non-abelian finite simple group $E$ there exist only finitely many doubly transitive permutation groups $G$ with the property $E(G) \cong E$.

In this paragraph we report on the problem to determine all finite doubly transitive groups belonging to a given simple group $E$. We find that the cases $E(G) \cong \text{PSL}(2, q)$ and $E(G) \cong A_i$, the alternating group of degree $i$, can be handled completely. Also we prove, that $E(G)$ is never isomorphic to $J_1$, Janko's group of order 175560. Hence the map $G \mapsto E(G)$, which maps each finite doubly transitive permutation group into the collection of isomorphism types of finite simple groups, is not onto. This strengthens a result of Parker (1954) to the effect that not every non-abelian simple group has a doubly transitive permutation representation. Finally, as a consequence of our results, we obtain a classification of all finite doubly transitive groups which have a sharply transitive normal subgroup and the property that the stabilizer on two points has odd order.

We present here only those cases, in which a complete answer is known. Therefore, it should be mentioned, that for many other cases, partial results exist (see, e.g., Bannai (to appear), Seitz (to appear) and § 5 of this paper).

We shall use the following notation:

DEFINITION. Let $G$ be any group and $A$ the maximal solvable normal subgroup of $G$. Then $E(G)$ is the smallest subgroup of $G/A$ containing all minimal normal subgroups of $G/A$.

As mentioned above, we have

THEOREM 6.1. If $G$ is a finite doubly transitive permutation group, then $E(G)$ is simple.

Let $G$ be a finite doubly transitive permutation group and let $A$ be the maximal solvable normal subgroup of $G$. By Burnside (1911, §§ 151-154),
G contains exactly one minimal normal subgroup H. Furthermore, \( A = 1 \) if and only if \( H \) is a non-abelian simple group, and \( A \neq 1 \) if and only if \( H \) is elementary abelian and sharply transitive. If \( A = 1 \), then \( \mathbb{C}_G H = 1 \). Suppose that \( A \neq 1 \), and let \( V \) be the set of permuted symbols. Choose an arbitrary element \( \sigma \in V \) and define a binary operation on \( V \) by

\[
O^x + O^y = O^{xy}
\]

for \( x, y \in H \). Then \( V \) together with this operation is a group isomorphic to the minimal normal subgroup \( H \), hence an elementary abelian \( p \)-group. Also, the stabilizer \( G_0 \) of \( G \) on \( \sigma \) is a group of automorphisms of \( V \) operating transitively on the set of elements different from the identity. Let \( L \) be a subring of \( \text{Hom}(V, V) \) maximal with respect to the property that it is a field containing the identity and that it is normalized by \( G_0 \). Then actually \( G_0 \) is a group of semilinear transformations of the \( L \)-vector space \((V, L)\) determined by \( V \) and \( L \) in the natural way. Clearly \( G \) is the set of all maps of the form

\[
x \mapsto x^g + \sigma
\]

for \( x \in V \), where \( \sigma \in V \) and \( g \) belongs to the semilinear group \( G_0 \). In our proofs we shall frequently use the notation introduced in this paragraph.

**THEOREM 6.2.** Let \( G \) be a finite doubly transitive permutation group of degree \( n \), and let \( \text{Aut}(E(G)) \) be the automorphism group of \( E(G) \). If \( E(G) \neq 1 \), then \( n < |\text{Aut}(E(G))|^2 \).

**Proof.** Assume that \( E(G) \neq 1 \). If \( A = 1 \), then \( E(G) \cong H \) and \( n \mid |E(G)| \), as \( H \) is transitive. Suppose that \( A \neq 1 \). If the Fitting subgroup of \( G_0 \) is not contained in \( L \), then by Theorem 5.5

\[
n = 3^4 < 120^2 \leq |\text{Aut}(E(G))|^2.
\]

If the Fitting subgroup of \( G_0 \) is contained in \( L \), then by Theorem 5.8,

\[
q^{n^* - 1} + q^{n^* - 2} + \cdots + q + 1 = \frac{q^{n^* - 1}}{q - 1} \leq |G/F| \leq |\text{Aut}(E(G))|,
\]

where \( q = |L| \) and \( n^* \) is the dimension of the vector space \((V, L)\). But this implies that

\[
n = q^{n^*} \leq q^{2n^* - 2} < (q^{n^* - 1} + \cdots + q + 1)^2 \leq |\text{Aut}(E(G))|^2.
\]

**COROLLARY 6.3.** If \( E \) is a finite simple group, then there exist only finitely many finite doubly transitive groups \( G \) with the property \( E(G) \cong E \).
THEOREM 6.4. Let $G$ be a finite doubly transitive permutation group of degree $n$ and assume that $E(G) \cong PSL(2, q)$, where $q \geq 4$.

If $q = 4$ or $5$, then $n = 5, 6, 5^2, 11^2, 19^2, 29^2, 59^2, 2^4$ or $3^4$.

If $q = 7$, then $n = 7, 8$ or $49$.

If $q = 8$, then $n = 9, 28$ or $8^2$.

If $q = 9$, then $n = 6, 10, 16$ or $9^2$.

If $q = 11$, then $n = 11, 12$ or $11^2$.

If $q = 13$, then $n = 14, 13^2$ or $3^6$.

If $q > 13$, then $n = q + 1$ or $q^2$.

Proof. Assume at first that $A = 1$. Then $G$ is isomorphic to a subgroup $\bar{H}$ of $PGL(2, q)$, as $PGL(2, q)$ is isomorphic to the automorphism group of $PSL(2, q)$. The group $\bar{H}$ contains a normal subgroup $\bar{E}$ which is isomorphic to $PSL(2, q)$. In particular $\bar{E}$ is simple and hence contained in the largest perfect normal subgroup of $PGL(2, q)$, which is $PSL(2, q)$. So actually $PSL(2, q) = \bar{E} \leq \bar{H}$. By Lüneburg (1964, Satz 1), we have one of the cases mentioned in the theorem.

Assume now that $A \neq 1$. Then we can apply Theorem 5.13. If the associated transitive linear group $G_0$ is of 'type I', then $n = q^2$, unless we have $E(G) \cong PSL(2, 4), PSL(2, 5)$ or $PSL(2, 7)$, in which case there are the additional possibilities $n = 5^2, 4^2$ or $7^2$, respectively. This follows from the proof of Theorem 5.13. Alternatively, it can be deduced from the classification of the exceptional automorphisms between the projective special linear groups over finite fields (see Artin, 1955).

THEOREM 6.5. Let $G$ be a finite doubly transitive permutation group of degree $n$ and assume that $E(G) \cong A_i$, where $i \geq 5$.

If $i = 5$, then $n = 5, 6, 5^2, 11^2, 19^2, 29^2, 59^2, 2^4$ or $3^4$.

If $i = 6$, then $n = 6, 10, 16$ or $8^2$.

If $i = 7$, then $n = 7, 15$ or $16$.

If $i = 8$, then $n = 8, 15$ or $16$.

If $i > 8$, then $n = i$.

Proof. As $A_5 \cong PSL(2, 4)$ and $A_6 \cong PSL(2, 9)$, we have settled the cases $i = 5$ and $i = 6$ already in Theorem 6.4. So we can assume in the following that $i \geq 7$. Let us consider at first the case $A \neq 1$. By Theorem 5.12, we have either $n^* = 2$, where $n^*$ is the dimension of $V$ over $L$, or $n \in \{2^4, 3^4\}$. If $n^* = 2$, then $E$ is involved in $PSL(2, q)$, where again $q = |L|$. Hence by Dickson (1901, Chapter XII) $E(G)$ is isomorphic to a two-dimensional linear fractional group $PSL(2, \bar{q})$ for a suitable prime power $\bar{q}$. But by Artin (1955) this implies that $i = 5$ or $6$, which contradicts our assumptions. So $n = 2^4$ or $3^4$.

If $n = 3^4$, then $V$ is a vector space of dimension $4$ over $GF(3)$ and hence $E(G)$ a factor of $GL(4, 3)$. This again implies $i \leq 6$, as $7 \not| |GL(4, 3)|$. So there
only remains the possibility \( n = 2^4 \). In this case \( E(G) \) is a factor of \( GL(4, 2) \) and hence \( i = 7 \) or 8.

Assume now that \( A = 1 \). As \( i \geq 7 \), \( \text{Aut}(E) \cong S_i \) (see Passman, 1968, Theorem 5.7). So either \( G \cong A_i \) or \( G \cong S_i \). The doubly transitive permutation representations of \( A_i \) and \( S_i \) have been determined by Maillet (1895).

**THEOREM 6.6.** Let \( G \) be a finite doubly transitive permutation group. Then \( E(G) \) cannot be isomorphic to Janko's group of order 175560.

**Proof.** In the case \( A = 1 \), this follows from Theorem 5.14. If \( A = 1 \), then \( G \cong J_1 \), as the outer automorphism group of \( J_1 \) is trivial by Janko (1966, Lemma 9.1). But, again by Janko (1966), \( J_1 \) does not have any doubly transitive permutation representation.

**THEOREM 6.7.** Let \( G \) be a doubly transitive group of permutations of a finite set \( V \). Suppose that \( G \) contains a sharply transitive normal subgroup and that no involution in \( G \) fixes more than one point. Then there exists a field \( L \) such that \( (V, L) \) together with suitable binary operations is a vector space over \( L \), and \( G \) is a subgroup of the group of permutations of \( V \) of the form

\[
x \mapsto x^h + v,
\]

where \( v \in V \) and \( h \) is a semilinear transformation of \( (V, L) \). Furthermore, we can choose \( L \) in such a way that one of the following statements holds:

(a) \((V, L)\) has dimension 1.

(b) \((V, L)\) has dimension 2 and \( G \) contains all permutations of \( V \) of the form

\[
x \mapsto x^h + v,
\]

where \( v \in V \) and \( h \) is a linear transformation of \( (V, L) \) with determinant 1.

(c) \((V, L)\) has dimension 2, \( |L| = 9, 11, 19, 29 \text{ or } 59 \), and \( G_0^o = SL(2, 5) \), where \( G_0 \) is the stabilizer of \( G \) on some element of \( V \).

(d) \((V, L)\) has dimension 2, \( |L| = 5, 7, 11 \text{ or } 23 \), and \( G_0 \) contains a normal quaternion group of order 8.

(e) \((V, L)\) has dimension 6, \( |L| = 3 \), and \( G_0 \cong SL(2, 13) \).

**Proof.** We define \( O, G_0 \) and \( L \) as before. Suppose there exists an involution \( i \) in \( G_0 \). Then \(|V| \equiv 0 \pmod{2}\), and \( i \) is an automorphism of the abelian group \( V \) which leaves invariant no element different from \( O \). Hence \( x^i = -x \) for all elements \( x \) in \( V \) (see Zassenhaus, 1936, p. 189). In particular, \( i \) is uniquely determined. This implies that the Sylow 2-subgroups of \( G_0 \) always are cyclic or generalized quaternion groups. If \( G_0 \) has cyclic Sylow 2-subgroups, then (a) holds by Theorem 5.15. If the Sylow 2-subgroups of \( G_0 \) are quaternion, then again by Theorem 5.15, we have one of the cases (a)–(e).

Finally, we note that there exists examples of doubly transitive groups
fulfilling the hypotheses of our theorem for each of the types (1)–(e) (see Zassenhaus, 1936; Huppert, 1957; Hering, 1970).

**BIBLIOGRAPHY**


Bannai, E., 'Doubly Transitive Permutation Representations of the Finite Projective Special Linear Groups $PSL(n, q)$', to appear.


Feit, W. and Thompson, J. G., 'Groups Which have a Faithful Representation of Degree less than $(p - 1)/2$', *Pacific J. Math.* 11 (1961), 1257–1262.


Author's address:

Christoph Hering,
Math. Institut der Universität,
D-74 Tübingen,
Auf der Morgenstelle 10,
Bundesrepublik Deutschland

(Received May 2, 1973).