On subgroups of prime power index

Barbara Baumeister

June 25, 1997

Abstract

We determine all finite groups G which admit a subgroup K of index p^a, p a prime, under the assumption that G has an irreducible and faithful $GF(p)$-module of dimension at most a. As an application to the theory of permutation groups we determine the maximal transitive subgroups of the primitive affine permutation groups.

1 Introduction.

In [Gu] Guralnick classified all the finite simple groups which possess a subgroup of prime power index. In this paper we determine all the finite groups G which admit a subgroup K of index p^a, p a prime, under the assumption that G has an irreducible and faithful $GF(p)$-module of dimension at most a.

Our main theorem is as follows.

Theorem 1 *Suppose that G is a finite group which contains a subgroup K of index p^a such that a is at least the dimension d of an irreducible and faithful $GF(p)$-modul V of G. Then the following holds.*

(i) $F(G) = 1$;

(ii) $p = 2$ *and* $d = 3r$, *for an* $r \in \mathbb{N}$;

(iii) $E(G) = T_1 \times \ldots \times T_r$, *where* $T_i \cong L_3(2)$, *for* $i = 1, \ldots, r$;

(iv) $G \cong T_1 \wr X$, *where X is a transitive subgroup of* S_r;

(v) $E(G) \not\leq K$ *and either* $T_i \leq K$ *or* $K \cap T_i \cong \mathrm{Frob}(7:3)$, *for* $i = 1, \ldots, r$;

(vi) $V = [V, T_1] \oplus \ldots \oplus [V, T_r]$, *where $[V, T_i]$ is the natural module for* T_i.

Theorem 1 generalizes the following more specialized version proved in [Ba1].

Theorem 2 *[Ba1, Proposition (2.7.1)] Suppose that G is as in Theorem 1 and that $F(G) = 1$. Then (ii) – (vi) of Theorem 1 hold.*

We consider the following hypothesis (A)

(A) The group G has a subgroup K of index p^a, p a prime, and G has an irreducible and faithful $GF(p)$-module V of dimension d, where d is at most a.

Remark 1. In fact it can happen that $T_i \leq K$, for some $i \in \{1, \dots, r\}$. The following group provides us with such an example.

Let $T_1, \dots, T_8$ be copies of $L_3(2)$, take $S \cong L_2(7)$ in its action of degree 8 and let G be the wreath product

$$G = (T_1 \times \cdots \times T_8) : S = T_1 \wr S.$$

As described in Theorem 1(vi), G has an irreducible and faithful $GF(2)$–module of dimension 24. Let K_2 be a subgroup of T_2 with $K_2 \cong \mathrm{Frob}(7:3)$ and let S_1 be the stabilizer of T_1 in S. Then $S_1 \cong \mathrm{Frob}(7:3)$ and $\langle K_2^{S_1} \rangle \cong \mathrm{Frob}(7:3)^7$. Set $K = T_1 \times \langle K_2, S_1 \rangle$. Then K has index $|G:K| = 2^{24}$. Thus G fulfils property (A), but T_1 is contained in K.

Let (G, Ω) be a primitive group of affine type, that is $G = O_p(G)G_w$ with G_w the stabilisator of $w \in \Omega$ and $O_p(G)$ an irreducible and faithful $GF(p)G_w$-module. The initial motivation for Theorem 1 was the wish to prove the following theorem.

Theorem 3 *Let (G, Ω) be a primitive permutation group of affine type. Suppose that B is a maximal subgroup of G which acts transitively on Ω. Then one of the following hold.*

(i) $O_p(G) \leq B$;

(ii) $O_p(G)$ *is elementary abelian of order* 2^{3r} *for some positive integer* r, $G \cong (E_8 : L_3(2)) \wr X$ *for some transitive subgroup* X *of* S_r *and* $B \cong L_3(2) \wr X$.

This theorem generalizes for the affine case the classification given in [Ba2]. There all the finite primitive permutation groups (G, Ω) which admit a factorization $G = G_\omega G_\omega^\alpha$ with $\alpha \in Aut(G)$ are determined.

The paper is organized as follows: In the next section we prove two lemmas on the order of the outer automorphism group of a simple group and in the third section we recall the theorem of Clifford and give simple estimations of the dimension of some special $GF(p)G$-modules. We will need the results of the two sections in the proof of Theorem 1. In the fourth section we prove, if a group G, which has a normal p-complement, but no normal p-subgroup, has a faithful $GF(p)$-module V of dimension d, then any Sylow p-subgroup of G has less then p^d elements. In Section 5 we prove Theorem 1 and in Section 6 Theorem 3.

The idea of the proof of Theorem 1 is as follows: Using the results of sections 2 through 4 we give bounds for a and d. These estimates imply that there is a component T of G satisfying the following property:

(B) The group T has a subgroup U of index p^u and an irreducible and faithful $GF(p)$-module of dimension n such that $n \leq u + b$, where $|Out(T)|_p = p^b$.

We then determine the quasisimple groups T satisfying property (B) (for the result see Proposition 5.6). Here the main idea is to reduce the problem to the classification of subgroups of prime power index in almost simple groups and to apply the classification of Guralnick [Gu]. There he used the classification of finite simple groups. Therefore also our result is based on this classification.

Using again $a \geq d$ and the estimates for a and d, we are then able to finish the proof of Theorem 1.

2 On the order of the outer automorphism group of a simple group.

If t is a natural number and $t = xp^i$ with $(x, p) = 1$, then we denote the p–part p^i of t by t_p.

Let q be a power of p, say $q = p^r$. Suppose $s \geq 3$ and $(s, q) \neq (6, 2), (3, 4)$.

It was proved by Zsigmondy [Zsig] that there exists a prime which divides $p^s - 1$, but does not divide $p^i - 1$, for $i = 1, \dots s - 1$. More precisely he did show the following.

Lemma 2.1 *[Zsig] Let p be a prime and $s \in \mathbb{N}$. Then one of the following holds:*

(i) There exists a prime r which divides $p^s - 1$, but does not divide $p^i - 1$, for $i = 1, \dots s - 1$;

(ii) $s = 2$ and p is a Mersenne prime;

(iii) $s = 6$ and $p = 2$.

Moreover we need:

Lemma 2.2 *Let p and r be two different primes. Then $p^{r^m} > r^{m^2}$ for any natural number $m \geq 1$.*

Proof. We show the assertion by induction on m.

Since $p^r > r$, the assertion clearly holds for $m = 1$.

Now let $m = 2$. If $r = 2$, then $p > 2$ and therefore $p^4 > 2^4$. Therefore we may assume $r \geq 3$. Clearly, the assertion also holds for $r = 3$. By induction on r we have

$$p^{(r+1)^2} = p^{r^2+2r+1} \geq p^{r^2} 2^{2r+1} > r^4 2^{2r+1} > 5r^4 \geq (r + 1)^4,$$

which proves the statement for $m = 2$.

Now let $m \geq 3$. Then $m^2 \geq 2m + 1$. We obtain by induction

$$p^{r^{m+1}} = p^{r^m r} = (p^{r^m})^r > (r^{m^2})^r \geq (r^{m^2})^2 \geq r^{m^2} r^{2m+1} = r^{(m+1)^2}.$$

$\square$

Lemma 2.3 *Let $T = \mathcal{L}(q)$ be a group of Lie type with $q = p^r$ for a prime p. Then there exists a number $b \in \mathbb{N}$ such that q^b divides $|T|$ and such that $|Out(T)| \leq 2br$.*

Proof. If $|Out(T)| \leq 2r$, then obviously the assertion holds. Hence according to [CCNPW] the lemma holds for $T \cong L_2(q),\ PSp_{2n}(q),\ Sz(q),\ P\Omega_{2n+1}(q),\ G_2(q),\ {}^2G_2(q),\ F_4(q),\ {}^2F_4(q),\ E_7(q)$ and $E_8(q)$.

If $n \geq 3$ and $T \cong L_n(q)$ or $T \cong U_n(q)$, then $|Out(T)| \leq 2nr$. Choose $b = n$. Since $q^{n(n-1)/2}$ divides $|T|$, see [CCNPW], the assertion follows in these cases, as well.

If $T \cong P\Omega_{2n}^{+}(q)$, $\mathrm{P}\Omega_{2n}^{-}(q)$ or ${}^3D_4(q)$, then $|Out(T)| \leq 24 \cdot r$ and on the other hand q^{12} divides $|T|$.

If $T \cong E_6(q)$ or ${}^2E_6(q)$, then $|Out(T)| \leq 6r$ and q^{36} divides $|T|$. Since $|\mathrm{Out}(T)| \leq 2br$ for $b = 3$, also for these two groups the assertion holds, which proves the lemma. $\square$

In order to prove Proposition 4.1 and to prove the main theorem, we also need the following result, which relies on the classification of the finite simple groups.

Lemma 2.4 *Let T be a quasisimple group and let n be the minimal dimension of an irreducible and faithful $GF(p)$-module. Then $|Out(T)|_p < p^n$.*

Proof. Assume $|Out(T)|_p \geq p^n$. For $\overline{T} = T/Z(T)$ either a sporadic or an alternating group, $Out(\overline{T})$ is of order at most 2. Hence $\overline{T}$ is neither isomorphic to a sporadic nor to an alternating group, but to a group of Lie type, $\overline{T} = \mathcal{L}(q),\ q = t^u,\ t$ prime. By assumption $T \leq GL_n(p)$ and therefore $\overline{T} \leq L_n(q)$. In particular, p does not divide the order of $Z(T)$.

Suppose $p = t$. According to [CCNPW] we have $|Out(\overline{T})|_p \leq u \cdot p$. Thus $p^n \leq u \cdot p$, which yields $p^{n-1} \leq u$. Since $\overline{T} \leq L_n(p)$, we have $u \leq n(n-1)/2$, so $p^{n-1} \leq n(n-1)/2$. This is not possible, as $n \geq 2$. Hence $p \neq t$.

Now the strategy is to use a result of Artin [Art, Theorem 1]. He determines the groups of Lie type X which are not twisted and which have the property that there is a prime c different from the characteristic p of X, so that $|X|_c > |X|_p$.

For this propose we show that $|T|_t > p^{n(n-1)/2}$. In order to prove this we use the following inequality which is easily checked by induction:

If $n \geq 2$, then $2^{p^{n-1}} > p^{n(n-1)/2}$.

By Lemma 2.3 there exists $b > 0$ such that q^b divides $|T|$ and such that $|Out(T)| \leq 2bu$. Therefore $p^n \leq 2bu$. This implies $|T|_t \geq q^b = t^{ub} \geq t^{p^n/2} \geq t^{p^{n-1}} \geq 2^{p^{n-1}} > p^{n(n-1)/2}$, as claimed.

Thus $|L_n(p)|_t > |L_n(p)|_p$ and we may apply the Theorem of Artin to $X = L_n(p)$. It follows $n = 2$ and $p = 2^s - 1$ a Mersenne prime [Art, Theorem 1]. As $\overline{T}$ is a simple non–abelian subgroup of $L_2(p)$, we obtain $\overline{T} \cong A_5$ (cf. [HuI, II. (8.27)]). Then $Out(T) \cong \mathbb{Z}_2$ in contradiction with $|Out(T)|_p \geq p^2$. This shows the assertion. $\square$

3 On Representations.

Notation. Let k be a finite field, G a group and V a kG–module. If there is no confusion we also simply speak of the G–module V.

In the following we will often use the Theorem of Clifford , cf. [Asch, (12.13)], which we include for the convenience of the reader.

Theorem 4 *(Clifford) Let V be a finite dimensional irreducible kG–module and $X \trianglelefteq G$. Then*

(i) *V is a semisimple kX–module.*

(ii) *G acts transitively on the kX–homogeneous components of V.*

(iii) *Let U be a kX–homogeneous component of V. Then $N_G(U)$ is irreducible on U and $XC_G(X) \leq N_G(U)$.*

If V is an irreducible module for the group $T_1 \times \cdots \times T_r$, then Theorem 4 applies as follows. For each $i = 1, \ldots, r$ the module V splits in a direct sum of irreducible T_i-modules. Further by (iii) the kT_i irreducible submodules of V are kT_i–isomorphic. In particular, if V is a faithful $T_1 \times \cdots \times T_r$–module, then $C_V(T_i) = 1$, for $i = 1, \ldots, r$.

Lemma 3.1 *Let V be an irreducible and faithful $k(T_1 * \cdots * T_r)$–module, where $T_1, \ldots, T_r$ are quasisimple groups. Let n_i be the dimension of an irreducible and faithful kT_i–submodule of V, for $i = 1, \ldots, r$. Then we have dim $V \geq \sum_{i=1}^r n_i$.*

Proof. Obviously the claim holds for $r = 1$. Let $r \geq 2$. Let the numbering $T_1, \ldots, T_r$ be chosen such that $n_1 \leq n_2 \leq \ldots \leq n_r$. According to the Theorem of Clifford $V = V_1 \oplus V_2 \oplus \ldots \oplus V_s$, where $V_1, \ldots, V_s$ are irreducible and faithful $T_2 * \cdots * T_r$–modules.

Assume $s = 1$. Then V is also an irreducible $T_2 * \cdots * T_r$–module. As k is a finite field, application of the Lemma of Schur yields that T_1 is a cyclic group, in contradiction to our assumption.

Thus $s \geq 2$ and we obtain by induction dim $V \geq s$ dim $V_1 = s(\sum_{i=2}^r n_i) \geq 2(\sum_{i=2}^r n_i) \geq \sum_{i=1}^r n_i$, as claimed. $\square$

Lemma 3.2 *Let $G = A \times B$ and let V be a faithful and irreducible kG–module. Further let k be a splitting field for A. Then $V \cong U \bigotimes_k W$, with U an irreducible kA–module and W an irreducible kB–module. If k is a splitting field for both A and B, then k is a splitting field for G.*

Proof. Let k be a splitting field for A. Then by the same proof as in [Go, Chapter 3, (7.1)] we obtain $V \cong U \bigotimes_k W$ for an irreducible kA–module U and an irreducible kB–module W.

Now assume that k is a splitting field for B, as well. Let $K \geq k$ be a splitting field for G and let $\{V_1, \ldots, V_n\}$ be the set of the irreducible KG–modules. Then k is a splitting field for G, if kG has also n irreducible kG–modules. By [Go, Chapter 3, (7.1)] there is a bijection between the irreducible kG–modules and the tensor products $U \bigotimes_k W$ of irreducible kA–modules U and irreducible kB–modules W. This implies, as k is a splitting field for A and B, that kG has n irreducible modules. This proves the last assertion. $\square$

Let p be a prime and let T be a group. Suppose that U is a subgroup of T such that $|T:U| = p^u$ and such that $A \leq T$ with $|T:A| = p^i$ yields $i \leq u$. Further let $|Out(T)|_p = p^b$. We will often use the following simple fact.

Lemma 3.3 *Let G be a group and $1 = M_0 \leq M_1 \leq \ldots \leq M_s = G$ a chain of subgroups of G such that M_{i-1} is normal in M_i, for $i = 1, \ldots, s$. Let K be a subgroup of G. Then there exist subgroups U_i in $B_i = M_i/M_{i-1}$, such that $|G:K| = \prod_{i=1}^{s} |B_i : U_i|$.*
In particular, if $G \leq Aut(T) \wr S_r$ and $|G:K| = p^a$, then $p^a \leq p^{r(u+b+1)-1}$, where u and b are as introduced just before the lemma.

Proof. Set $U_i = M_{i-1}(K \cap M_i)/M_{i-1}$. Then because of Lagrange's Theorem the first assertion follows.

Now let $G \leq Aut(T) \wr S_r$. Denote by L the kernel of the action of G on the components of G. Then $1 \leq E(G) \leq L \leq G$ is a chain of normal subgroups of G with $L/E(G)$ isomorphic to a subgroup of $Out(T)^r$ and G/L isomorphic to a subgroup of S_r. Since the p–part of $|S_r|$ is at most p^{r-1}, (see for instance [HuI, III (15.3)]), and since $|E(G) : E(G) \cap K| \leq |T:U|^r$, the assertion holds. $\square$

4 Coprime action.

Let G be a group with $O_p(G) = 1$ and let V be an faithful $GF(p)G$-module of dimension d. Let $P \in Syl_p(G)$ and suppose $|P| \geq p^d$. In this section we prove that G has no normal p-complement.

Proposition 4.1 *Let G be a group, $G = O_{p'}(G)P$, $P \in Syl_p(G)$, $|P| = p^a$, with $C_P(O_{p'}(G)) = 1$. Let V be an faithful $GF(p)G$-module of dimension d. Then $d > a$.*

Proof. Let K be the algebraic closure of $GF(p)$. Then G acts faithfully on $W = V \otimes_{GF(p)} K$ and $\dim_K(W) = \dim_{GF(p)}(V)$. Therefore we have to show $d = \dim_K(W) > a$. Let (W, G) be a counterexample with d minimal.

Set $Q = O_{p'}(G)$.
(1) G acts irreducibly on W:
Let $U \leq [W, Q]$ be an irreducible G-module. Then Q acts faithfully on U. As

$C_P(Q) = 1$, U is a faithful G-module. Now, the fact that (W, G) is a minimal counterexample implies $U = W$.

(2) G acts primitively on W:
Assume that G acts imprimitively on W, that is $W = \bigoplus_{i=1}^k W_i$ and G acts on $\Omega = \{W_1, \ldots, W_k\}$.

Let L be the kernel of the action of G on Ω. Then G/L is isomorphic to a subgroup of the symmetric group S_k. Let M_i be the group induced by L on W_i, for $i = 1, \ldots, k$. Let $R \in Syl_p(L)$, $P_i \in Syl_p(M_i/O_p(M_i))$ and let N_i be the preimage of $O_p(M_i)$ in L. If $x \in R \cap \bigcap_{i=1}^k N_i$, then, as $O_{p'}(L) \cap N_i = C_{O_{p'}(L)}(W_i)$, we obtain $[O_{p'}(L), x] \leq O_{p'}(L) \cap \bigcap_{i=1}^k N_i = \bigcap_{i=1}^k C_{O_{p'}(L)}(W_i) = C_{O_{p'}(L)}(W) = 1$, so $x = 1$. This implies $|R| \leq \prod_{i=1}^k |P_i|$.

Let $\tilde{P} \in Syl_p(M_i)$. Then $C_{\tilde{P}}(O_{p'}(M_i)) \leq O_p(M_i)$. Therefore $C_{P_i}(O_{p'}(M_i)/O_p(M_i)) = 1$.

Assume $O_{p'}(M_i) = 1$ for some $i \in \{1, \ldots, k\}$. Then

$$O_{p'}(M_i/O_p(M_i)) = O_{p'}(M_i)O_p(M_i)/O_p(M_i)$$

implies $P_i = 1$ and therefore $M_i = 1$. Since W is an irreducible G-module, G acts transitively on Ω. Hence $M_i = 1$ for all $i \in \{1, \ldots, k\}$. So $L = 1$, $G \leq S_k$ and $|P| \leq p^{k-1}$ in contradiction with $d \geq k \cdot \dim W_1 \geq k$.

Thus $O_{p'}(M_i) \neq 1$ for any $i \in \{1, \ldots, k\}$. Since $\dim W_i < \dim W$ we obtain by induction $|P_i| \leq p^{\dim W_i - 1}$ (for $i = 1, \ldots, k$) and therefore $|R| \leq \prod_{i=1}^k (p^{\dim W_i - 1}) = p^{\dim W - k}$. As $|S_k|_p \leq p^{k-1}$, it follows $|P| \leq |R||S_k|_p = p^{\dim W - 1}$ in contradiction to our assumption. Hence G acts primitively on W.

Let $M \leq O_{p'}(G)$ be a normal subgroup of G minimal with respect to $[M, G] \neq 1$.
(3) M acts irreducibly on W:
According to the theorem of Clifford W is a semisimple KM-module. Since G acts primitively on W, the module splits into isomorphic irreducible KM-modules: $W = \bigoplus_{i=1}^s W_i$ with W_i isomorphic irreducible KM-modules. By a theorem of Clifford [HuI, V. (17.5)] W is as an KG-module isomorphic to $X \otimes_K Y$, where X and Y are modules of a central extension $\hat{G}$ of G and where Y is an faithful $K\hat{G}$-module. Further $Y_{|M}$ is isomorphic to W_1 as an KM-module. As $\dim Y \leq \dim W$, we have by induction $Y = W$. Therefore W is an irreducible KM-module.

(4) $C_G(M) = Z(G)$ and $Z(G)$ is cyclic:
Since W is an irreducible KM-module, according to the Lemma of Schur $C_G(M) \leq Z(G)$ and therefore $C_G(M) = Z(G)$. As $Z(G)$ is finite, it is a cyclic group.

(5) M is solvable:
Let $N < M$ be a normal subgroup of G. Then the minimality of M implies $[G, N] = 1$, so $N \leq Z(M)$. In particular, $M/Z(M)$ has no G-invariant subgroup.

Assume that M is not solvable. Then, as $M/Z(M)$ is a minimal normal subgroup of $G/Z(M)$, it is a direct product of isomorphic simple non-abelian groups. Thus $M = T_1 * \ldots * T_k$ is a central product of isomorphic quasisimple groups. By Lemma 3.1 and as G acts transitively on $\{T_1, \ldots, T_k\}$, it follows $k \cdot n \leq d$ with n the minimal dimension of an irreducible and faithful $GF(p)T_1$-module. Since $C_Q(P) = 1$, the prime p does not divide $|Z(G)|$. Therefore

$$|P| \leq |G/Z(G)|_p = |G/C_G(M)|_p \leq |Aut(M)|_p = (|Aut(T_1)|_p)^k |S_k|_p$$

and as T_1 is a p'-group

$$(|Aut(T_1)|_p)^k |S_k|_p = (|Out(T_1)|_p)^k |S_k|_p.$$

Application of Lemma 2.4 to T_1 implies

$$(|Out(T_1)|_p)^k |S_k|_p \leq p^{(n-1)\cdot k} \cdot p^{k-1} = p^{k \cdot n - 1},$$

so $a \leq k \cdot n - 1 < d$ in contradiction with our assumption. Therefore M is solvable.

(6) M is a r-group for some prime r, $M = [M, G]$, $G/Z(G)$ acts faithfully and irreducibly on $M/C_M(G)$. Moreover, M is an extraspecial group of order r^{1+2m} or $r = 2$ and M a central extension of $\mathbb{Z}_4$ by an extraspecial group of order 2^{1+2m}. Moreover, $d = r^m$:
Since $C_G(M) = Z(G)$, we have $M/Z(M) \neq 1$ and since $M/Z(M)$ is solvable, $O_r(M/Z(M)) \neq 1$ for some prime r. Let $X = O_r(M)$. Now $Z(M) \subseteq Z(G)$ yields $[G, X] \neq 1$. By the minimal choice of M we obtain $M = X$. Since, moreover, $M/Z(M)$ has no G-invariant subgroup, $M/Z(M)$ is an elementary abelian r-group.

Since $Z(M)$ is cyclic, it follows $M' \cong \mathbb{Z}_r$ and $\Phi(M) = M'$.

Let $\overline{E}$ be a complement in $\overline{M} = M/M'$ to $\overline{Z(M)}$ and let E be the preimage of $\overline{E}$ in M. Clearly, $M = Z(M)E$. Further $Z(E) = Z(M) \cap E = M'$ and therefore we have $Z(E) = \Phi(E) = E' \cong \mathbb{Z}_r$ which proves that E is an extraspecial group, $E \cong r^{1+2m}$ for some natural number m. As $Z(M)$ is cyclic, the index of E in M is at most r. If $r \neq 2$, then M is of exponent r and $Z(M) = M' \leq E$. If $r = 2$, then M is of exponent 4 and either $Z(M) \cong \mathbb{Z}_4$ or $Z(M) \cong \mathbb{Z}_2$.

It remains to show $d = r^m$. Clearly, W is an irreducible E-module. According to [Asch, (34.9)] $d = r^m$.

(7) The final contradiction:
As $C_G(M) = Z(G) \leq Q$, the Sylow p-subgroup P of G acts faithfully on $M/Z(M)$. Therefore P is isomorphic to a p-subgroup of $Aut(M/Z(M)) \cong Sp_{2m}(r)$. Since p and r are different primes, according to a result of Artin [Art, Theorem 1] either

(i) $|P| \leq |Sp_{2m}(r)|_r$ or

(ii) $m = 1$ and $r = 2^s - 1$ is a Mersenne prime.

In the second case $|P| = 2^s$ and $d = r = 2^s - 1$, which yields the inequality $s = a \geq d = 2^s - 1$. So $s = 1$ and P acts trivially on W in contradiction to our assumption. Therefore $|P| \leq |Sp_{2m}(r)|_r = r^{m^2}$. Now the fact that $d = r^m$ and that $|P| = p^a \geq p^d$ yields $p^d = p^{r^m} \leq r^{m^2}$. But this contradicts with Lemma 2.2.

Hence our assumption $a \geq d$ was false and the assertion holds. □

5 Proof of Theorem 1.

In this section we prove the theorem and therefore we suppose hypothesis

(A) G has an irreducible and faithful $GF(p)$–module V of dimension d and G contains a subgroup K with $|G : K| = p^a$ for an $a \geq d$.

Let $E(G) = N_1 * \cdots * N_s$, where $N_1, \ldots, N_s$ are normal subgroups of G, where $N_i = T_{i1} * \cdots * T_{ir_i}$, $T_{i1}, \ldots, T_{ir_i}$ isomorphic quasisimple groups, and where G acts transitively on $\{T_{i1}, \ldots, T_{ir_i}\}$. Let n_i be the minimal dimension of an irreducible and faithful T_{i1}–submodule of V, for $i = 1, \ldots, s$.

As V is an faithful $GF(p)G$-module, p does not divide $|F(G)|$.

Lemma 5.1 *The prime p divides the order of $E(G)$.*

Proof. Assume p does not divide $|E(G)|$. Then p does not divide $|F^*(G)|$. Let $P \in Syl_p(G)$. By hypothesis (A) $|P| \geq p^a \geq p^d$. Since $C_P(F^*(G)) \leq P \cap Z(F^*(G)) = 1$ and since V is a faithful $GF(p)(F^*(G)P)$-module of dimension d, we obtain a contradiction with Proposition 4.1. □

In particular, Lemma 5.1 implies $E(G) \neq 1$. Thus G is not a solvable group.

Let $V = \bigoplus_{l=1}^m V_l$, where V_l are the homogeneous components for $E(G)$. Let $j_i \in \mathbb{N}$ such that

$$C_{N_i}(V_1) \cong (T_{i1})^{r_i - j_i}, \text{ for } i = 1, \ldots, s.$$

Then V_1 is an faithful $GF(p)$–module for $N_i/C_{N_i}(V_1) \cong (T_{i1})^{j_i}$. Let m_i be natural numbers, such that

$$m_i \geq r_i/j_i > m_i - 1, \text{ for } i = 1, \ldots, s.$$

Since V is a faithful G–module, V contains at least m_i non-isomorphic N_i–modules, $1 \leq i \leq s$. As all irreducible N_i–submodules of an irreducible $E(G)$–submodule of V are isomorphic, $E(G)$ has at least $max\{m_i,\ 1 \leq i \leq s\}$ non–isomorphic irreducible submodules in V, so

- $$m \geq max\{m_i \mid i = 1, \ldots, s\}.$$

The homogeneous component V_1 splits into isomorphic irreducible $E(G)$-modules:

$$V_1 = V_{11} \oplus \ldots \oplus V_{1t}.$$

By Lemma 3.1 we have $dimV_{11} \geq \sum_{i=1}^{s} j_i n_i$ which implies $dimV_1 \geq t \cdot \sum_{i=1}^{s} j_i n_i$. Together with $\bullet$ we obtain:

Lemma 5.2 $d \geq t \cdot \sum_{i=1}^{s} r_i n_i$. □

Lemma 5.3 $|C_G(E(G))|_p \leq p^{d/2}$.

Proof. Let $P \in Syl_p(C_G(E(G)))$. Since p does not divide $|F(G)|$, we have $C_P(F(G)) \leq P \cap Z(F(G)) = 1$.

Let $R \in Syl_p(E(G))$ and $W_i = C_{V_i}(R)$. Clearly, $W_i \neq 1$.

Assume $W_i = V_i$. Then, as p does not divide $|Z(E(G))|$, for some j, $1 \leq j \leq s$, we have $[N_j, V_i] = 1$. Since G acts transitively on $\{V_1, \ldots, V_m\}$, it follows $[N_j, V] = 1$, which is false by hypothesis (A). Therefore $W_i < V_i$ for $i = 1, \ldots, m$.

Let $g \in F(G)^{\#}$. If $[W_i, g] = 1$, then by the $A \times B$-Lemma of Thompson [Asch, (24.2)] $[V_i, g] = 1$. We claim that $[V_i, g] \leq W_i$ implies as well $[V_i, g] = 1$. Thus assume $[V_i, g] \leq W_i$, but $[V_i, g] \neq 1$. Then $V_i = C_{V_i}(g) + W_i$. Since $[E(G), g] = 1$, the group $E(G)$ acts on $C_{V_i}(g)$. The fact that $[W_i, R] = 1$ yields $[V_i/C_{V_i}(g), N_j] = 1$ for some j, $1 \leq j \leq s$. Since V_i is the direct sum of isomorphic $E(G)$-modules and since $V_i/C_{V_i}(g) \neq 1$ by assumption, it follows $[V_i, N_j] = 1$ which is not possible, as seen above. Thus $[V_i, g] \leq W_i$ implies $[V_i, g] = 1$.

Set $X_i = W_i$ if $dimW_i \leq \frac{1}{2} dimV_i$ and else $X_i = V_i/W_i$ for $i = 1, \ldots, m$. Then, as shown above, $X = X_1 \oplus \cdots \oplus X_m$ is a faithful $GF(p)F(G)$-module. Since $C_P(F(G)) = 1$, also P acts faithfully on X and by Proposition 4.1 $|P| < p^{dimX}$. So $dimX \leq d/2$ yields the assertion. □

Suppose that U_i is a subgroup of T_{i1} such that $|T_{i1} : U_i| = p^{u_i}$ and such that $A_i \leq T_{i1}$ with $|T_{i1} : A_i| = p^x$ yields $x \leq u_i$. Further let $|Out(T_{i1})|_p = p^{b_i}$.

Lemma 5.4 *Either*

(i) $|C_G(E(G))|_p = 1$ *and* $a \leq \sum_{i=1}^{s}(r_i(u_i + b_i + 1) - 1)$
or

(ii) $|C_G(E(G))|_p \neq 1$, $t \geq 2$ *and* $a \leq \sum_{i=1}^{s}(r_i(u_i + b_i + 1) - 1) + d/2$.

Proof. We have $|G : K| = |G : C_G(E(G))K||C_G(E(G))K : K|$. Notice,

$$|G : C_G(E(G))K| = |G/C_G(E(G)) : C_G(E(G))K/C_G(E(G))|.$$

Since $G/C_G(E(G)) \leq Aut(G/Z(E(G)))$ Lemma 3.3 implies

$$|G : C_G(E(G))K| \leq p^{\sum_{i=1}^{s}(r_i(u_i+b_i+1)-1)}.$$

Moreover $|C_G(E(G))K : K| = |C_G(E(G)) : (K \cap C_G(E(G)))| \leq |C_G(E(G))|_p$. If $|C_G(E(G))|_p = 1$, then (i) follows.

Now let $|C_G(E(G))|_p \neq 1$. Then $a \leq \sum_{i=1}^{s}(r_i(u_i + b_i + 1) - 1) + d/2$ by Lemma 5.3. It remains to show $t \geq 2$. By the theorem of Clifford $C_G(E(G))$ acts on the homogeneous component V_1. Let L be the stabilizer of V_{11} in $C_G(E(G))$. Since V_{11} is an irreducible $E(G)$-module, according to the Lemma of Schur, L is a cyclic group which is not divisible by p. Therefore $t \geq |C_G(E(G))|_p \geq 2$, as asserted. □

Corollary 5.5 *$n_i \leq u_i + b_i$ for some $i \in \{1, \cdots, s\}$.*

Proof. Hypothesis (A) yields $t \cdot \sum_{i=1}^{s} r_i n_i \leq d \leq a$. First suppose $|C_G(E(G))|_p = 1$. Then $\sum_{i=1}^{s} r_i n_i \leq \sum_{i=1}^{s} r_i(u_i + b_i + 1) - 1$, which implies the assertion.

If $|C_G(E(G))|_p \neq 1$, then by Lemma 5.4 $d \leq (\sum_{i=1}^{s} r_i(u_i + b_i + 1) - 1) + d/2$, so $d/2 \leq \sum_{i=1}^{s} r_i(u_i + b_i + 1) - 1$. Since $t \geq 2$ and since $t \cdot \sum_{i=1}^{s} r_i n_i \leq d$ we obtain again $\sum_{i=1}^{s} r_i n_i \leq \sum_{i=1}^{s} r_i(u_i + b_i + 1) - 1$ so the assertion of the lemma. □

In order to determine T_{i1} and n_i we prove the following special case:

Proposition 5.6 *Let T be a quasisimple group, p a prime which divides $|T|$, but not $|Z(T)|$. Let n the dimension of an irreducible and faithful $GF(p)T$-module. Suppose that there is a subgroup U of T with $|T : U| = p^u$ and suppose $n \leq u + b$, where $|Out(T)|_p = p^b$. Then $p = 2$ and either*

(i) $n = 4$, $T \cong L_4(2) \cong A_8$ and $U \cong A_7$
or

(ii) $n = 3$, $T \cong L_3(2)$ and $U \cong Frob(7:3)$.

Proof. Set $\overline{T} = T/Z(T)$.

(1) $\overline{T} \cong A_m,\ m = p^u$ or $\overline{T} \cong L_m(q),\ p^u = (q^m - 1)/(q - 1)$:
According to Lemma 2.4 $b < n$, so $u > 1$. Since p does not divide $|Z(T)|$, we have $|\overline{T} : \overline{U}\ | = p^u$. Guralnik classified the simple groups which possess a subgroup of primepower index [Gu, Theorem 1]. According to [Gu, Theorem 1]

$$\overline{T} \cong A_m, L_n(q), L_2(11), M_{23}, M_{11}, U_4(2) \text{ and}$$

$$p^u = m,\ \frac{q^n - 1}{q - 1},\ 11,\ 23,\ 11,\ 27, \text{ respectively.}$$

Assume $\overline{T} \cong L_2(11), M_{23}, M_{11}$ or $U_4(2)$. Then $\overline{U} \cong A_5, M_{22}, M_{10}$ or $E_{2^4}A_5$ and $p^u = |\overline{T} : \overline{U}| = 11, 23, 11, 3^3$, respectively [Gu]. Since these cases $|Out(\overline{T})|_p = 1$, by assumption $n \leq u$. This gives $n \leq 1, 1, 1, 3$, respectively. Since $L_2(11)$, M_{23} or M_{11} are not solvable groups, they are not contained in $\Gamma L_1(p)$ for any prime p. Therefore $\overline{T} \cong U_4(2)$ and $\overline{T} \leq GL_3(3)$. This is also not possible, as 5 divides $|\overline{T}|$ but not $|GL_3(3)|$.

Thus (1) holds.

Since T has an n-dimensional irreducible and faithful $GF(p)T$-module, $\overline{T}$ is isomorphic to a subgroup of $L_n(p)$. Let $S \in Syl_p(L_n(p))$.

(2) Suppose $\overline{T} \cong A_m$. Then $p = 2$ and (i) holds:
Then, cf. [HuI, III. (16.5a)]

$$exp(S) \leq \begin{cases} p^{\frac{n+1}{2}} & n \text{ odd} \\ p^{\frac{n}{2}} & n \text{ even} \end{cases}.$$

In order to prove (2) we will use the fact that on the one hand either $n \leq u$ or $n \leq u+1$ for p odd or even, respectively, and on the other hand $\overline{T} \leq L_n(p)$.

Assume $p \neq 2$. As $m = p^u$ by (1), there is an $x \in \overline{T}$ with $o(x) = p^u$. Thus $p^u \leq exp(S) \leq p^{(n+1)/2}$ contrary to $n \leq u$. Thus $p = 2$.

As $p = 2$, there is an element $x \in \overline{T}$ with $o(x) = 2^{u-1}$. Hence $2^{u-1} \leq exp(S) \leq 2^{(n+1)/2}$. Since $n \leq u+1$, we obtain $n-2 \leq (n+1)/2$, which yields $n \leq 5$ and $u \leq 4$. As $\overline{T}$ is not a solvable group, $u \geq 3$ and as $\overline{T} \leq L_n(2)$ we obtain $u = 3$, $n = 4$ and $\overline{T} \cong A_8$. The Schur-multiplier of A_8 is isomorphic to $\mathbb{Z}_2$. Since by assumption T has a faithful embedding in $GL_4(2)$, it follows $T = \overline{T} \cong A_8$ and $U \cong A_7$, as asserted in (2).

(3) Suppose $\overline{T} \cong L_m(q)$. Then $p = 2$ and (ii) holds:
By (1) $(q^m-1)/(q-1) = p^u$. Let $q = t^y$, t prime.

Assume that p is a Zsigmondy prime for $q^m - 1$, this means p divides $t^{ym}-1$, but not $t^i - 1$ for $i < y \cdot m$. Then $p \neq 2$ and $p \equiv 1 (y \cdot m)$, which yields in particular $(p, y \cdot m) = 1$, Lemma 2.1. Hence $(p,m) = 1$ and there exists an element $x \in \overline{T}$, the Singer cycle, with $o(x) = (q^m-1)/(q-1) = p^u$, [HuI, II. (7.3)]. By [HuI, III. (16.5a)] $exp(S) \leq p^{(n+1)/2}$, which implies $u \leq (n+1)/2$. But as $|Out(T)|$ divides $2 \cdot (q-1) \cdot y$, the prime p does not divide $|Out(T)|$. Therefore $n \leq u$ in contradiction with $u \leq (n+1)/2$. Hence p is not a Zsigmondy prime for $q^m - 1$.

Thus $q^m = 64$ or q is a Mersenne prime and $m = 2$, Lemma 2.1. Since $(q^m-1)/(q-1)$ is the power of a prime, $q^m = 64$ yields $q = 8$ and $m = 2$. Assume $q = 8$ and $m = 2$. Then $\overline{T} \cong L_2(8)$, $Out(T) \cong \mathbb{Z}_3$ and $(q^m-1)/(q-1) = 3^2$. Hence $p = 3$ and $n \leq 3$. Thus T is isomorphic to a subgroup of $GL_3(3)$, which is false: For instance 7 divides $|L_2(8)|$, but not $|GL_3(3)|$.

Hence q is a Mersenne prime, $m = 2$ and $p = 2$. So $q = 2^u - 1$ and $|Out(T)|_2 = 2$, which yields $n \leq u+1$. Due to the existence of the Singer cycle, [HuI, II. (7.3)], there exists $y \in \overline{T}$ with $o(y) = 2^{u-1}$. It follows $2^{u-1} \leq exp(S) \leq 2^{(n+1)/2}$. This results in $n-2 \leq u-1 \leq (n+1)/2$, showing $n \leq 5$ and $u \leq 4$. Since $\overline{T}$ is simple and $q = 2^u - 1$ is a prime, we obtain $u = 3$. Thus $q = 7$ and $n = 3$. The Schur-multiplier of $L_2(7)$ is isomorphic to $\mathbb{Z}_2$. Thus, as in (2) we obtain $T = \overline{T}$. So $T \cong L_2(7)$ and $U \cong Frob(7:3)$ which proves (3). $\square$

Corollary 5.7 *Suppose that G is a group satisfying (A). Then $p = 2$ and for some $i \in \{1, \cdots, s\}$ either*

(i) $n_i = 4$, $T_{i1} \cong L_4(2) \cong A_8$
or

(ii) $n_i = 3$, $T_{i1} \cong L_3(2)$.

Proof. By Corollary 5.5 the T_{i1} fulfiles the assumptions of Proposition 5.6. Thus the assertion follows with Proposition 5.6. □

Let $k \in \{1, \ldots, s\}$ and let the numbering be such that for $i \leq k$, either $(n_i, T_{i1}) = (3, L_3(2))$ or $(n_i, T_{i1}) = (4, L_4(2))$ and such that for $i \geq k+1$, $(n_i, T_{i1}) \neq (3, L_3(2))$, $(4, L_4(2))$.

Lemma 5.8 *We have either*

(i) $|C_G(E(G))|_p = 1$ *and* $a \leq 5 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i - s$
or

(ii) $|C_G(E(G))|_p \neq 1$, $t \geq 2$ *and* $a \leq 5 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i - s + d/2$

Proof. Notice that $u_i = 3$ and $b_i = 1$ for $i \leq k$ and that $n_i \geq (u_i + b_i + 1)$ for $i > k$. Therefore

$$\sum_{i=1}^{s} (r_i(u_i + b_i + 1) - 1) \leq 5 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i - s.$$

Thus Lemma 5.4 implies the assertion. □

Remark. If $N_G(T_{i1})/C_G(T_{i1}) \cong T_{i1}$ for $i \in M$, $M \subseteq \{1, \ldots, k\} = P$, then we obtain the following better estimation.

In case (i) $a \leq 4 \sum_{i \in M} r_i + 5 \sum_{i \in P \setminus M} r_i + \sum_{i=k+1}^{s} r_i n_i - s$

and

in case (ii) $a \leq 4 \sum_{i \in M} r_i + 5 \sum_{i \in P \setminus M} r_i + \sum_{i=k+1}^{s} r_i n_i - s + d/2$.

Lemma 5.9 *We have*

$$m \cdot t \cdot (\prod_{i=1}^{k} d_i^{j_i}) \sum_{i=k+1}^{s} j_i n_i \leq d,$$

where $d_i = 3$ for $T_{i1} \cong L_3(2)$, and $d_i = 4$ for $T_{i1} \cong L_4(2)$.

Proof. Since in both cases, $T \cong L_3(2)$ and $T \cong L_4(2)$ the field $k = GF(2)$ is a splitting field for T, repeated application of Lemma 3.2 yields that $GF(2)$ is a splitting field for $N_1, \ldots, N_k$ and $N_1 \times \cdots \times N_k$ as well. Hence by Lemmas 3.1 and 3.2

$$(d_1^{j_1} \cdot \ldots \cdot d_k^{j_k})(\sum_{i=k+1}^{s} j_i n_i) \leq \dim V_{11}.$$

Thus $t \cdot (\prod_{i=1}^{k} d_i^{j_i}) \sum_{i=k+1}^{s} j_i n_i \leq dim V_1$ and therefore $V = \bigoplus_{i=1}^{m} V_i$ implies the assertion.
$\square$

Now Lemmas 5.8 and 5.9 imply:

Corollary 5.10 $m \cdot (\prod_{i=1}^{k} d_i^{j_i}) \sum_{i=k+1}^{s} j_i n_i \leq 5 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i - s.$ $\square$

Lemma 5.11 *The group G has exactly one minimal normal subgroup in $E(G)$. Moreover, we have $T_{11} \cong N_G(T_{11})/C_G(T_{11}) \cong L_3(2)$ and $j_1 = 1$.*

Proof. Set $T = T_{11}$ and let the numbering be chosen such that $T_{11}, \ldots, T_{l1} \cong L_3(2)$ and $T_{l+1,1}, \ldots, T_{k,1} \cong L_4(2)$. Set $J_1 = j_1 + \cdots + j_l$ and $J_2 = j_{l+1} + \cdots j_k$ (clearly, if $T_{i1} \not\cong L_3(2)$ (resp. $T_{i1} \not\cong L_4(2)$) for all $i \leq k$, then $J_1 = 0$ (resp. $J_2 = 0$)).

By Corollary 5.10

$$m 3^{J_1} 4^{J_2} \sum_{i=k+1}^{s} j_i n_i \leq 5 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i - s. \tag{1}$$

In the following we will repeatedly use the fact that $m_i j_i \geq r_i$ and that $m \geq m_i$, for $i = 1, \ldots, s$.

First we show $s = k$. Assume $s > k$. Notice that $n_i \geq 4$ for $i \geq k+1$ and that therefore

$$m(3^{J_1} 4^{J_2} \sum_{i=k+1}^{s} j_i n_i) \geq m(8(J_1 + J_2) + \sum_{i=k+1}^{s} j_i n_i) \geq 8 \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{s} r_i n_i$$

in contradiction to (1). Thus $s = k$.

Therefore we have

$$3^{J_1} 4^{J_2} m \leq 5 \sum_{i=1}^{s} r_i - s. \tag{2}$$

Assume $J_2 \neq 0$. Then (2) implies $J_1 = 0$ and $J_2 = 1$. Hence $s = 1$, $T = T_{11} \cong L_4(2)$, $j_1 = 1$ and $m_1 = r_1$. Further since $d \leq a$, in fact $N_G(T)/C_G(T) \cong Aut(T)$. Let U be an irreducible 4–dimensional kT–submodule of V and let $\alpha \in N_G(T) \setminus C_G(T)T$. Then α maps U on the dual $GF(2)T$-module. Since each irreducible $E(G)$–module splits into isomorphic N_1–modules, it follows $m \geq 2m_1 = 2r_1$. We obtain the contradiction $8r_1 \leq d \leq a \leq 5r_1 - 1$. Thus $J_2 = 0$.

Hence $T_{i1} \cong L_3(2)$, for $i = 1, \ldots, s$ and (2) yields that $J_1 \leq 2$.

Assume $s = 2$. Then $j_1 = j_2 = 1$, $m_1 = r_1$ and $m_2 = r_2$. Again $d \leq a$ yields $N_G(T_{i1})/C_G(T_{i1}) \cong Aut(T_{i1})$, for some $i \in \{1, 2\}$. Assume $i = 1$. Then by the same argument as before $m \geq 2r_1$ and therefore

$$9m \leq 5(r_1 + r_2) - 2 \leq 5(m/2 + m) < 8m.$$

This proves $s = 1$.

Assume $N_G(T)/C_G(T) \cong \mathrm{Aut}(T)$. Then $m \geq 2m_1$ and therefore

$$6r_1 \leq 3J_1 m \leq 3^{J_1} m$$

in contradiction with (2).

Hence it follows, according to Lemma 3.3 and property (A),

$$3^{J_1} m \leq d \leq a \leq 4r_1 - 1,$$

which yields $J_1 = 1$. This proves the lemma. $\square$

Set $r = r_1$ and $T_i = T_{1i}$ for $i = 1, \ldots, r_1$.

Corollary 5.12 *$C_G(E(G)) = 1$ and V decomposes as a $GF(2)E(G)$–module into $V = [V, T_1] \oplus \ldots \oplus [V, T_r]$, where $[V, T_i]$ are natural $GF(2)T_i$–modules, for $i = 1, \ldots r$. Moreover, $d = 3r$ and $t = 1$.*

Proof. Since $j_1 = 1$, any irreducible $E(G)$–submodule of V is 3–dimensional. This implies $[V, T_i, T_j] = 1$, for $i \neq j$. Thus

$$V = [V, T_1] \oplus \ldots \oplus [V, T_r]$$

and $m = r$. So $d = 3r \cdot t$.

Since $Z(GL_3(2)) = 1$, $C_G(E(G))$ acts semiregularly on the irreducible $E(G)$-submodules of V_1. So the order of $C_G(E(G))$ divides $2^t - 1$. Therefore $|C_G(E(G))|_2 = 1$. Then by Lemma 5.8 $5r - 1 \geq 3r \cdot t$ which implies $t = 1$ and $C_G(E(G)) = 1$. Therefore we also obtain $d = 3r$ and $\dim[V, T_i] = 3$. This proves the Corollary. $\square$

Proof of Theorem 1.
From $C_G(E(G)) = 1$ follows $F(G) = 1$, so (i) holds. Corollary 5.7 and Corollary 5.12 yield (ii). By Lemma 5.11, (iii) holds. Lemma 2.4 and Proposition 5.6 imply (v) and Corollary 5.12 proves (vi).

It remains to show (iv). Consider the semi-direct product $V : G$. It follows from the fact that no nontrivial element of G centralizes $[V, T_1]T_1 \times \cdots \times [V, T_r]T_r$ that $G \leq \mathrm{Aut}([V, T_1]T_1 \times \cdots \times [V, T_r]T_r)$. Since G normalizes $E(G) = T_1 \times \cdots \times T_r$, we obtain that G acts on $\{T_1, \ldots, T_r\}$ as well as on $\{[V, T_1]T_1, \ldots, [V, T_r]T_r\}$. Since in $Aut([V, T_1]T_1)$ the subgroup T_1 is selfnormalising, it follows $V : G \leq ([V, T_1]T_1) \wr S_r$ and $G = N_{VG}(G) \leq T_1 \wr S_r$. Therefore (iv) holds, which proves Theorem 1. $\square$

6 Proof of Theorem 3.

Proof of Theorem 3.
Suppose $O_p(G) \not\leq B$. Set $V = O_p(G)$ and $A = G_0$. Since B is maximal in G, it follows $G = VB$. Therefore, $A \cong G/V = VB/V \cong B/B \cap V$. Thus B induces on V the full group A. As V is an irreducible $GF(p)A$-module and as $V \not\leq B$, it follows $B \cap V = 1$. Thus $|B| = |A|$ and $|VA| = |G| = |BA|$ implies $|A : A \cap B| = |V|$. Now, Theorem 1 yields the assertion. $\square$

References

[Art] E. Artin, The orders of the linear groups, *Comm. Pure and Appl. Math.* **8** (1955), 355–366.

[Asch] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, Cambridge, London 1986.

[Ba1] B. Baumeister, Dual extended grids or a characterization of the third group of Janko, Phd-thesis, FU-Berlin, 1996.

[Ba2] B. Baumeister, Factorizations of primitive permutation groups, to appear in *J. Algebra*.

[CCNPW] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford 1985.

[Go] D. Gorenstein, *Finite Groups*, Harper & Row, New York 1968.

[Gu] R.M. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* **81** (1983), 304–311.

[HuI] B. Huppert, *Endliche Gruppen I*, Springer–Verlag, Berlin, Heidelberg 1979.

[Zsig] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892) 265–284.