# The trivial intersection problem for characters of principal indecomposable modules

Conchita Martínez-Pérez* and Wolfgang Willems

**Abstract** For a prime $p$ and a finite group $G$ let $\Phi_p(G)$ denote the complex character associated to the projective indecomposable module in characteristc $p$ with trivial head. Let $\mathrm{Irr}(\Phi_p(G))$ denote the set of irreducible characters occuring as constituents in $\Phi_p(G)$. We characterize all finite simple groups which satisfy $\mathrm{Irr}(\Phi_p(G)) \cap \mathrm{Irr}(\Phi_q(G)) = \{1_G\}$ for all primes $p \neq q$.

## 1 Introduction

All groups in this note are assumed to be finite. By $\mathrm{B}_0(G)_p$ we denote the principal $p$-block for a prime $p$ and by $\Phi_p(G)$ the complex character associated to the principal indecomposable module with respect to $p$, i.e., $\Phi_p(G)$ is the complex character afforded by the projective cover of the trivial module in characteristic $p$. Let $\mathrm{Irr}(\mathrm{B}_0(G)_p)$ be the set of all $\chi \in \mathrm{Irr}(G)$ belonging to $\mathrm{B}_0(G)_p$. Recently, Bessenrodt and Zhang proved

**Theorem 1.1** [2] *A group $G$ is nilpotent if and only if*

$$\mathrm{Irr}(\mathrm{B}_0(G)_p) \cap \mathrm{Irr}(\mathrm{B}_0(G)_q) = \{1_G\}$$

*for all primes $p$ and $q$ with $p \neq q$.*

Now, let $\mathrm{Irr}(\Phi_p(G))$ denote the set of all $\chi \in \mathrm{Irr}(G)$ which occur as constituents in $\Phi_p(G)$. Since $\mathrm{Irr}(\Phi_p(G))$ is a subset of $\mathrm{Irr}(\mathrm{B}_0(G)_p)$ we may ask:

*Which properties of $G$ characterize the (weaker) condition*

$$\mathrm{Irr}(\Phi_p(G)) \cap \mathrm{Irr}(\Phi_q(G)) = \{1_G\} \tag{1}$$

*for all primes $p, q$ with $p \neq q$?*

The situation turns out to be more subtle as easy examples already show.

*Supported by Gobierno de Aragon and MTM2007-68010-C03-01

**Lemma 1.2** *The group $G = \mathrm{PSL}(2,r)$, where $r$ is a power of a prime, satisfies*

$$\mathrm{Irr}(\Phi_p(G)) \cap \mathrm{Irr}(\Phi_q(G)) = \{1_G\}$$

*for all primes $p \neq q$ if and only if $r$ is a Mersenne prime.*

Proof: This can be read off from the decomposition matrices for $\mathrm{PSL}(2,r)$ which have been computed in [3].

The main result of this paper is the proof of

**Theorem 1.3** *If $G$ is a finite non-abelian simple group then the following conditions are equivalent.*

*a)* $\mathrm{Irr}(\Phi_p(G)) \cap \mathrm{Irr}(\Phi_q(G)) = \{1_G\}$ *for all primes $p, q$ with $p \neq q$.*

*b)* $G = \mathrm{PSL}(2,r)$ *where $r$ is a Mersenne prime.*

*c) $G$ has a 2-complement.*

The equivalence of b) and c) follows directly from ([9], Theorem 1). Note that the existence of a 2-complement implies the existence of a maximal subgroup whose index is a power of 2. This happens only for $\mathrm{PSL}(d,r)$ with $\frac{r^d-1}{r-1} = 2^a$, as shown by Guralnick in [9]. By Zsigmondy's Lemma (see 3.3), this number theoretical condition is satisfied if and only if $d = 2$ and $r$ is a Mersenne prime. Thus $\mathrm{PSL}(2,r)$ with $r$ a Mersenne prime is the only non-abelian simple group which has a 2-complement.

We would like to mention here that the condition

$$\mathrm{Irr}(\Phi_2(G)) \cap \mathrm{Irr}(\Phi_p(G)) = \{1_G\} \quad \text{for all primes } p \neq 2$$

does not imply that $G$ has a 2-complement, as $\mathrm{PSL}(3,7)$ shows. This is in contrast to a local version of the Bessenrodt-Zhang Theorem which follows by a slight refinement of their proof, and says:

*If $p$ is a fixed prime then*

$$\mathrm{Irr}(\mathrm{B}_0(G)_p) \cap \mathrm{Irr}(\mathrm{B}_0(G)_q) = \{1_G\} \quad \textit{for all primes } q \neq p$$

*implies that $G$ is $p$-nilpotent.*

Finally part c) implies that $\Phi_2(G)$ has degree $|G|_2$ and we may ask the

**Question 1.4** *Are the following two conditions equivalent for a finite non-abelian simple group $G$?*

*a) $G$ has a 2-complement.*

*b) $\Phi_2(G)$ has degree $|G|_2$.*

Note, that for any finite group $G$ the 2-part of the degree of $\Phi_2(G)$ is exactly the 2-part $|G|_2$ of the order of $G$ (see [8]).

If we drop the assumption *simple group* in Theorem 1.3 we do not know a characterization of groups $G$ which satisfy $\mathrm{Irr}(\Phi_p(G)) \cap \mathrm{Irr}(\Phi_q(G)) = \{1_G\}$ for all primes $p, q$ with $p \neq q$.

## 2 General results

Let $(\cdot,\cdot)$ denote the Frobenius product of complex characters, i.e. the usual bilinear form in the ring of characters. To be brief we write $\Phi_p$ for $\Phi_p(G)$ if there is no confusion with the group in question. Since the trivial character $1_G$ appears always with multiplicity one in $\Phi_p$ for all $p$ we have $(\Phi_p, \Phi_q) \geq 1$ for all primes $p, q$. Thus the condition

$$\mathrm{Irr}(\Phi_p) \cap \mathrm{Irr}(\Phi_q) = \{1_G\}$$

is equivalent to

$$(\Phi_p, \Phi_q) = 1.$$

**Definition 2.1** We say that $G$ is a TI-*group for characters* if $(\Phi_p, \Phi_q) = 1$ for all primes $p \neq q$.

**Proposition 2.2** *Let $G$ be a finite group and let $p, q$ be different primes. Suppose that $G = HL$ with $H, L \leq G$ where $p \nmid |H|$ and $q \nmid |L|$. Then*

$$(1_H^G, 1_L^G) = 1.$$

*In particular, $G$ is a* TI-*group for characters.*

Proof: By Frobenius reciprocity and Mackey's Theorem, we have

$$(1_H^G, 1_L^G) = (1_H, (1_L^G)_H) = (1_H, 1_{L\cap H}^H) = (1_{L\cap H}, 1_{L\cap H}) = 1.$$

For the last statement note that $\Phi_p$ is a constituent of $1_H^G$ and $\Phi_q$ is of $1_L^G$ (see for example [20] Theorem 2.27).

□

The following Corollaries are immediate consequences of Proposition 2.2.

**Corollary 2.3** *Let $p$ be a prime. If $G$ has a $p$-complement then*

$$(\Phi_p, \Phi_q) = 1$$

*for all primes $q$ with $q \neq p$.*

**Corollary 2.4** *If for all primes $p$ with possibly one exception the group $G$ has a $p$-complement then $G$ is a* TI-*group for characters. In particular, solvable groups are* TI-*groups for characters.*

**Example 2.5** Let $G = \mathrm{A}_5$ be the alternating group on 5 letters. The irreducible characters of $G$ are $1_G, \chi_3, \chi_{3^*}, \chi_4, \chi_5$ with degrees $1, 3, 3, 4, 5$. One easily sees that

$$\begin{aligned} \Phi_2 &= 1_G + \chi_3 + \chi_{3^*} + \chi_5 \\ \Phi_3 &= 1_G + \chi_5 \\ \Phi_5 &= 1_G + \chi_4. \end{aligned}$$

Hence

$$(\Phi_2, \Phi_3) = 2,\ (\Phi_2.\Phi_5) = 1 \text{ and } (\Phi_3, \Phi_5) = 1.$$

Observe that $G$ has a 5-complement, but neither a 2- nor a 3-complement.

**Proposition 2.6** *Let $q$ be an odd prime and suppose that there exists a character $\chi$ of odd degree with $1_G \neq \chi = \overline{\chi} \in Irr(\Phi_q)$. Then*

$$(\Phi_2, \Phi_q) > 1.$$

Proof: On $2'$-elements we have

$$\chi = \sum_{\beta \in \mathrm{IBr}_2(G)} a_\beta \beta$$

where $\mathrm{IBr}_2(G)$ denotes the set of irreducible 2-Brauer characters. Clearly, the trivial character is the only real-valued linear 2-Brauer character. Since $\chi = \bar{\chi}$ we obtain

$$\chi = a1_G + \sum_{\beta \neq \bar{\beta}} a_\beta(\beta + \overline{\beta}) + \sum_{1_G \neq \beta = \overline{\beta}} a_\beta \beta.$$

Fong's Lemma (see [14], Vol. II, Theorem 8.13) yields $2 \mid \beta(1)$ for all $\beta$ with $1_G \neq \beta = \overline{\beta}$. Since $\chi(1)$ is odd we get $a \geq 1$. This shows that the trivial character is a constituent of the modulo 2 reduction of $\chi$ which means that $\chi$ is a constituent of $\Phi_2$. □

**Corollary 2.7** *Let $G = O^2(G)$ and let $q$ be an odd prime. If $2 \mid \Phi_q(1)$ then $(\Phi_2, \Phi_q) > 1$.*

Proof: The character $\Phi_q$ is real-valued and, by assumption $G = O^2(G)$, the trivial character is the only linear real-valued character. Thus we may write

$$\Phi_q = 1_G + \sum_{\chi \neq \bar{\chi}} a_\chi(\chi + \overline{\chi}) + \sum_{1_G \neq \chi = \overline{\chi}} a_\chi \chi \quad \text{with } a_\chi \in \mathrm{N}_0$$

where $\chi \in \mathrm{Irr}(G)$. Since $\Phi_q(1)$ is assumed to be even there exists an irreducible character $\chi$ of odd degreet with $1_G \neq \chi = \overline{\chi}$ and an application of Proposition 2.6 completes the proof. □

For general groups we do not know much about the degree $\Phi_p(1)$ apart from Dixon's result that $|G|_p$ divides $\Phi_p(1)$. As a warning we would like to mention that even for simple groups it can happen that $\Phi_p(1)$ is even only for the prime $p = 2$. For instance, the Mathieu group $M_{11}$ serves as an example.

**Proposition 2.8** *Let $G$ be a finite group with a transitive permutation action of degree $n > 1$. Suppose that the prime factorization of $n$ contains $t$ different primes. If the complex character of the action contains $k \leq t$ different irreducible characters then*

$$(\Phi_p, \Phi_q) > 1$$

*for suitable primes $p \neq q$ with $pq \mid n$.*

Proof: If $\pi$ denotes the character of the permutation action of $G$ then

$$\pi = 1_G + \sum_{i=1}^{k-1} e_i \chi_i$$

where $e_i \in \mathrm{N}$ and $1_G \neq \chi_i \in \mathrm{Irr}(G)$. Let $p$ be a prime with $p \mid n$. Furthermore, let $M$ be the permutation module over a field $K$ of characteristic $p$ with permutation basis $e_1, \ldots, e_n$. Then $M$ carries a non-degenerate $G$-invariant bilinear form $b$ defined by

$$(e_i, e_j) = \delta_{ij}.$$

Since $p \mid n$ the form $b$ is 0 on the trivial submodule $S = K(e_1 + \ldots + e_n)$. Thus $M$ contains a second trivial module as a composition factor, namely $M/S^{\perp} \cong S^* \cong S$. This means that the modulo $p$ reduction of at least one $\chi_i$ contains the trivial module. The condition $t > k - 1$ implies $(\Phi_p, \Phi_q) > 1$ for some primes $q \neq p$ with $p, q \mid n$. □

**Corollary 2.9** *Let $G$ be a doubly transitive group of degree $n$ where $n$ is not the power of a prime. Then for all primes $p \neq q$ with $pq \mid n$ we have*

$$(\Phi_p, \Phi_q) > 1.$$

Proof: The permutation character $\pi$ of a doubly transitve action satisfies $\pi = 1_G + \chi$ with $1_G \neq \chi \in \mathrm{Irr}(G)$. Thus by the proof of Proposition 2.8 we get the assertion. □

**Corollary 2.10** *If $G$ is a solvable transitive group of degree $n$ and the prime factorization of $n$ contains $t$ different primes then the corresponding complex permutation character contains at least $t + 1$ different irreducible characters.*

Proof: This follows immediately from Proposition 2.8 and Corollary 2.4. □

Recall that a finite group $G$ has a *rank $k$ action of degree $n$* if $G$ acts transitively on a set $\Omega$ with $|\Omega| = n$ and the stabilizer of a point has $k$ orbits on $\Omega$. Let

$$\pi = \sum_{i=1}^{s} e_i \chi_i = 1_G + \sum_{i=2}^{s} e_i \chi_i$$

with $e_i \in \mathrm{N}$ and pairwise different $\chi_i \in \mathrm{Irr}(G)$ denote the complex permutation character of a rank $k$ action. Then, by ([27], 29.2),

$$1 + \sum_{i=1}^{s} e_i^2 = k.$$

In particular, $\pi$ has at most $k$ different irreducible constituents and exactly $k$ if $k \leq 4$.

# 3 Chevalley groups

In this section we prove

**Proposition 3.1** *A (simple) Chevalley group $G$ is a* TI*-group for characters if and only if $G = \mathrm{PSL}(2, r)$ where $r$ is a Mersenne prime.*

The first two results are well-known.

**Lemma 3.2** *Let $p$ and $r$ be primes. If*

$$r^n + 1 = p^m$$

*for $n, m \in \mathrm{N}$ then one of the following cases occur.*

*(i)* $2^3 + 1 = 3^2$.

*(ii)* $m = 1, r = 2$ *and $p$ is a Fermat prime.*

*(iii)* $n = 1, p = 2$ *and $r$ is a Mersenne prime.*

**Lemma 3.3** (Zsigmondy, [14], chap. IX, 8.3) *Let $r$ be a power of a prime and $2 \leq d \in \mathrm{N}$. Then there exists a prime $p$ with*

*(1)* $p \mid r^d - 1$.

*(2)* $p \nmid r^i - 1$ *for $0 < i < d$.*

*unless $d = 6, r = 2$ or $d = 2, r = 2^b - 1$. We call such a prime $p$ a* primitive prime divisor of $r^d - 1$.

In the exceptional case $d = 6$ and $r = 2$ we still can find for any $0 < i < 6$ a prime $p$ dividing $2^6 - 1$ but not dividing $2^i - 1$. Note that in this case the prime $p$ depends on $i$.

**Definition 3.4** We say that a prime power $r$ is *exceptional* if $r = 8$ or $r$ is a Mersenne prime or $r + 1$ is a Fermat prime.

**Proposition 3.5** *Let $G(r)$ be a non-twisted Chevalley group defined over the finite field $\mathbb{F}_r$. If $r$ is not exceptional then*

$$(\Phi_p, \Phi_q) > 1$$

*for all primes $p \neq q$ with $pq \mid r + 1$.*

Proof: This follows immediately from Theorem B of Hiss [11]. □

**Corollary 3.6** *Let $G(r)$ be a non-twisted Chevalley group with $r$ odd. If $G(r)$ is a* TI*-group then $r$ is a Mersenne prime.*

In order to prove Proposition 3.1 we first rule out the cases where the groups have a doubly transitive permutation representation. These groups are determined in [4].

**Lemma 3.7** *The groups* $\mathrm{PSU}(3, r)$, ${}^2B_2(2^{2m+1})$ *and* ${}^2G_2(3^{2m+1})$ *are not* TI*-groups for characters.*

Proof: PSU$(3,r)$ has a doubly transitive action of degree $r^3+1$. By Lemma 3.2, $r^3+1$ is not a prime power since $r \neq 2$ and $r^3+1$ can not be a Fermat prime. Thus the assertion follows by Corollary 2.9.
The Suzuki groups ${}^2B_2(2^{2m+1})$ are doubly transitive of degree $r^2+1$ for $r = 2^{2m+1}$ and the same argument as for unitary groups in dimension 3 works unless $m = 1$. But the smallest Suzuki group ${}^2B_2(8)$ can be checked directly by the GAP library.
The Ree groups ${}^2G_2(3^{2m+1})$ have a doubly transitive action of degree $r^3+1$ where $r = 3^{2m+1}$. Since $r^3+1$ is not a power of a prime we may apply again Corollary 2.9. □

In order to deal with projective special linear groups we need a number theoretical fact.

**Lemma 3.8** *Let $r$ be a power of a prime and $2 < d \in \mathrm{N}$ with $(d,r) \neq (3,8)$. Assume that*

*(i) either $d$ is not a prime,*

*(ii) or $r = 8$,*

*(iii) or $r = 2^{2^t}$ with $t \geq 1$.*

*Then*

$$n = \frac{r^d - 1}{r - 1}$$

*contains at least 2 different primes.*

Proof: If $d$ is not a prime then we can choose an $s \mid d$ with $1 < s < d$. Let $p$ be a primitive prime divisor of $r^d - 1$ and let $q$ be any prime divisor of $\frac{r^s-1}{r-1}$. Then $p \neq q$ and $pq \mid n$.

If $r = 8 = 2^3$ then $d \neq 2, 3$ and

$$\frac{r^d - 1}{r - 1} = \frac{2^{3d} - 1}{2^3 - 1}.$$

As $3d \neq 6$ we may choose a primitive prime divisor $p$ of $2^{3d} - 1$, and as $d > 3$ we may choose a further prime $q \mid 2^d - 1$ with $q \nmid 2^3 - 1$. Obviously, $p \neq q$ and $p, q \mid 2^{3d} - 1$. Moreover, $p, q \nmid 2^3 - 1$. Hence $p, q \mid n$.

In the case $(iii)$ we have $r = 2^{2^t}$ with $t \geq 1$, hence

$$n = \frac{2^{2^t d} - 1}{2^{2^t} - 1}.$$

If $2^t d = 6$ then either $(d,r) = (3,4)$ or $(d,r) = (6,2)$. In the first case $n = 21$ and in the second $n = 63$. So we may assume $6 \neq 2^t d$ and we can choose a primitive prime divisor $p$ of $2^{2^t d} - 1$. Furthermore, as $2^t < 2^{t-1}d$, we may also choose a prime $q$ with $q \mid 2^{2^{t-1}d} - 1$ but $q \nmid 2^{2^t} - 1$. By construction $p, q \mid n$ and $p \neq q$. □

**Lemma 3.9** *For $d \geq 4$ the group $G = \mathrm{PSL}(d,r)$ has a rank 3 permutation representation on the set of 2-dimenional subspaces of the natural vector space $V = V(d,r)$.*

Proof: Clearly, $G$ acts transitively on the set $V^{(2)}$ of 2-dimensional subspaces of $V$. If $H_0 \in V^{(2)}$ then one checks straightforward that the stabilizer $G_{H_0}$ of $H_0$ in $G$ has the following three orbits

$$H, \quad \{H \mid H \in V^{(2)},\ H \cap H_0 = \{0\}\}, \quad \{H \mid H \in V^{(2)},\ \dim H \cap H_0 = 1\}.$$

Thus $G$ has a rank 3 action on $V^{(2)}$. □

**Lemma 3.10** *Let $d \geq 3$. Then $G = \mathrm{PSL}(d, r)$ is a* TI*-group for characters if and only if $G = \mathrm{PSL}(3, 2) \cong \mathrm{PSL}(2, 7)$.*

Proof: Suppose that $(\Phi_p, \Phi_q) = 1$ for all primes $p \neq q$. Note first that, by Proposition 3.5, we may assume that $r$ is exceptional.
a) We claim that $d$ is a prime and either $r = 2$ or is a Mersenne prime.
If $G = \mathrm{PSL}(3, 8)$ then $(\Phi_2, \Phi_7) > 1$, by the GAP library. Thus we may assume that $(d, r) \neq (3, 8)$. The group $\mathrm{PSL}(d, r)$ has a doubly transitive action of degree $n = \frac{r^d - 1}{r - 1}$ on the lines of the natural vector space $V = V(d, r)$ (see [4]). In addition, by Corollary 2.9, we may assume that $n$ is a prime power. Thus, by Lemma 3.8, we get the claim.
b) Let $d = 3$ and note that $\mathrm{PSL}(3, 2) \cong \mathrm{PSL}(2, 7)$ which we considered already in Lemma 1.2. If $r \neq 2$ then, by part a), $G = \mathrm{PSL}(3, r)$ where $r$ is a Mersenne prime and $n = 1 + r + r^2$ is a power of a prime. Thus $r = 2^t - 1$ for a prime $t$. In case $r = 3$ we have $G = \mathrm{PSL}(3, 3)$ which can be checked directly with the GAP library. Thus $t$ is odd and we get $2^t \equiv -1 \bmod 3$, hence $r \equiv 1 \bmod 3$, and therefore

$$n = 1 + r + r^2 \equiv 0 \bmod 3.$$

On the other hand, modulo 9 we obtain three possibilities for $2^t$, namely

$$2^t \equiv 2, -1 \text{ or } 5 \bmod 9,$$

hence $r \equiv 1, -2$ or $4 \bmod 9$, and therefore in each case

$$n = 1 + r + r^2 \equiv 3 \bmod 9.$$

This shows that $3 \mid n$, but $9 \nmid n$. Thus $n = 1 + r + r^2 = 3$, a contradiction to $r > 1$.
c) Finally, let $d \geq 4$, hence by part a) $d \geq 5$ and $d - 1 = 2a$. The space $V(d, r)$ contains exactly

$$m = \Big(\frac{r^d - 1}{r - 1}\Big)\Big(\frac{r^{d-1} - 1}{r^2 - 1}\Big)$$

2-dimensional subspaces on which $G$ allows a rank 3 permutation representation, by Lemma 3.9. Furthermore, by Proposition 2.8, it is enough to show that $m$ contains at least 3 different primes. If $(d, r) = (7, 2)$ then $m = 43 \cdot 7 \cdot 3^2$ and the claim follows. In all the left cases we may choose $p_1$ primitive prime divisor of $r^d - 1$ and $p_2$ primitive prime divisor of $r^{d-1} - 1$. If moreover $a \geq 3$ then take $p_3 \mid r^a - 1$ with $p_3 \nmid r^2 - 1$. Then the three primes $p_1, p_2$ and $p_3$ are different and $p_i \mid m$ for $i = 1, 2, 3$. Assume finally that $a = 2$, hence $d = 5$. In particular

$$m = \frac{r^5 - 1}{r - 1}(r^2 + 1).$$

If $r^2+1$ contains at least two different primes we are done again. In case $r^2+1$ is a prime power we get that $r$ is even. By part a), we obtain $r=2$. But $G=\mathrm{PSL}(5,2)$ is not a TI-group, by the GAP library. □

The classical symplectic, orthogonal and unitary groups allow a rank 3 permutation action on the set of isotropic lines of the underlying vector space (see [18], Theorem 1.1).

**Lemma 3.11** *Let $r$ be a power of a prime and $2<d\in\mathrm{N}$ with $(d,r)\neq(3,2)$. Then $n=\frac{r^{2d}-1}{r-1}$ contains at least 3 different primes.*

Proof: As $(d,r)\neq(3,2)$ we may choose a primitive prime divisor $p$ of $r^{2d}-1$ and a primitive prime divisor $q$ of $r^d-1$. Note that $p,q\nmid r^2-1$. If $t$ is any prime divisor of $r+1$ then $p,q,t$ are pairwise different and $p,q,t\mid n$. □

**Lemma 3.12** *The group $G$ is not a* TI*-group for characters if $G$ is one of the following groups.*

*a)* $\mathrm{PSp}(2d,r)$ *with $d>2$.*

*b)* $\Omega(2d+1,r)$ *with $d>2$.*

Proof: First note that $G=\mathrm{PSp}(6,2)\cong\Omega(7,2)$. For this group we have $(\Phi_2,\Phi_3)>1$, by the GAP library. Thus we may assume that $(d,r)\neq(3,2)$. The rank 3 permutation representation for both groups $\mathrm{PSp}(2d,r)$ and $\Omega(2d+1,r)$ is of degree $n=\frac{r^{2d}-1}{r-1}$. For the symplectic group this is obvious, for the orthogonal group see for instance ([13], Proposition 9.18). By Lemma 3.11, the degree $n$ contains at least 3 different primes and Proposition 2.8 applies. □

Lemma 3.12 does not cover the case $d=2$, hence $G=\mathrm{PSp}(4,r)$. By Proposition 2.8, we may assume that $r^2+1$ and $r+1$ are prime powers. In particular, $r=2^f$. Furthermore $\mathrm{PSp}(4,r)=\Omega(5,r)$ for $r$ even and $\mathrm{PSp}(4,2)\cong\mathrm{S}_6$.

**Lemma 3.13** *For $\mathrm{PSp}(4,r)$ with $r=2^f>2$ we have $(\Phi_2,\Phi_p)>1$ for all primes $p$ with $p\mid r+1$.*

Proof: Let $G=\mathrm{Sp}(4,r)=\mathrm{PSp}(4,r)$ with $r=2^f>2$. By [28], section 2, Table II, the irreducible character $\chi_3$ satisfies $(\Phi_p,\chi_3)=1$ for all primes $p\mid r+1$. On the other hand, $\chi_3$ is denoted by $\psi_2$ in [1], and it is proved in Theorem 3 of [1] that $(\Phi_2,\psi_2)=\frac{r}{2}$. Thus we have $(\Phi_2,\Phi_p)>1$ for all primes $p\mid r+1$. □

**Lemma 3.14** *Let $4\leq d\in\mathrm{N}$ and*

$$n=(r^{d-1}+1)\frac{r^d-1}{r-1}.$$

*Then $n$ contains at least three different primes unless $r=2$, $d=4$ or $r=2$ and $2^{d-1}+1$, $2^d-1$ are primes. In the latter case $d$ is also a prime.*

Proof: First assume that $r^{d-1}+1$ is not a power of a prime. Thus we may choose primes $p_1 \neq p_2$ with $p_1, p_2 \mid r^{d-1}+1$. Observe that

$$\gcd(r^{d-1}+1, r^d-1) \mid r+1 \mid r^2-1.$$

Therefore, if we choose $q \mid r^d-1$ with $q \nmid r^2-1$ (recall that $d>2$) then $q \mid n$ and $p_1, p_2 \neq q$. Thus we have found three different primes dividing $n$.

So we are left with the case when $r^{d-1}+1$ is a power of a prime. Lemma 3.2 (note that $d \geq 4$) implies that either $r=2$, $d=4$ or $p=r^{d-1}+1$ is a Fermat prime. In particular $r=2^{2^t}$. If $t \geq 1$ we may apply Lemma 3.8 and we get two different primes $q_1, q_2 \mid \frac{r^d-1}{r-1}$. Furthermore, if $r=2$ it is also possible to find two different primes $q_1, q_2 \mid 2^d-1$ unless $2^d-1$ is a Mersenne prime. In both cases $q_1, q_2 \neq p$ since $p \nmid r+1$. □

**Lemma 3.15** *$G = \mathrm{P}\Omega^+(2d,r)$ $(d \geq 4)$ is not a* TI*-group for characters.*

Proof: By ([13], Proposition 9.18), there are

$$\frac{r^{2d-1}+r^d-r^{d-1}-1}{r-1} = (r^{d-1}+1)\frac{r^d-1}{r-1}$$

isotropic lines on which $G$ allows a rank 3 permutation representation (see [18]). Thus the result follows by Proposition 2.8 and Lemma 3.14 unless $r=2$, $d=4$ or $r=2$ and both $2^{d-1}+1$ and $2^d-1$ are primes. The group $\mathrm{P}\Omega^+(8,2)$ can be checked directly by the GAP library. Thus we have to deal with the second case. For $d=4$ and $d=5$ the assertion follows again by the GAP library. Therefore we may assume that $d>5$. The group $G = \Omega^+(2d,2) = \mathrm{P}\Omega^+(2d,2)$ acts transitively on the set of anisotropic subspaces of dimension 2 according to Witt's Theorem. By ([6], Lemma 2.1 (ii)), the number of such subspaces is

$$n = \frac{2^{2(d-1)}(2^d-1)(2^{d-1}-1)}{6} = 2^{2d-3}(2^d-1)\frac{2^{d-1}-1}{3}.$$

Furthermore, by ([6], Theorem 6.5 (ii)), the rank of the permutation action is $\frac{2^2+4+2}{2} = 5$. We claim that $n$ contains at least five different primes which completes the proof by Proposition 2.8. Since $2^{d-1}+1$ is a Fermat prime we have $d-1=2^s$ for some $s$. Furthermore $d=2^s+1$ must be a prime. The condition $d>5$ implies $s \geq 4$. Now we choose a primitive prime divisor $p_1$ of $2^{d-1}-1 = 2^{2^s}-1$, a primitive prime divisor $p_2$ of $2^{2^{s-1}}-1$ and a primitive prime divisor $p_3$ of $2^{2^{s-2}}-1$. The choice of these primes implies that $p_1, p_2, p_3$ are pairwise distinct and $p_i \nmid 2^2-1=3$ for $i=1,2,3$. Thus

$$p_1p_2p_3 \mid \frac{2^{d-1}-1}{3}.$$

Finally, if we put $p_4 = 2^d-1$ and $p_5=2$ we have found five different primes dividing $n$. □

**Lemma 3.16** *Let* $4 \leq d \in \mathrm{N}$ *and*

$$n = (r^d + 1)\frac{r^{d-1} - 1}{r - 1}.$$

*Then* $n$ *contains at least three different primes unless* $r = 2$ *and* $2^d + 1$, $2^{d-1} - 1$ *are primes. In the latter case* $d - 1$ *is also a prime.*

Proof: We argue similary as in the proof of Lemma 3.14. □

**Lemma 3.17** $G = \mathrm{P}\Omega^-(2d, r)$ $(d \geq 4)$ *is not a* TI*-group for characters except possibly in case* $r = 2$, $2^d + 1$ *is a Fermat prime and* $2^{d-1} - 1$ *is a Mersenne prime.*

Proof: By ([13], 9.18), the number of isotropc lines is

$$\frac{r^{2d-1} - r^d + r^{d-1} - 1}{r - 1} = (r^d + 1)\frac{r^{d-1} - 1}{r - 1}.$$

Since the action of $G$ on these lines is of rank 3 (see [18]) the result follows by Proposition 2.8 and Lemma 3.16. □

The argument in Lemma 3.17 does not apply for $\mathrm{P}\Omega^-(8, 2)$ and $\mathrm{P}\Omega^-(16, 2)$ since we have the prime factorizations $(2^4 + 1)(2^3 - 1) = 17 \cdot 7$ and $(2^8 + 1)(2^7 - 1) = 257 \cdot 127$.

In order to deal with the cases we left open in Lemma 3.17 we need

**Lemma 3.18** *If* $d \geq 10$ *and* $2^d + 1$ *is a Fermat prime then*

$$f(d) = \frac{(2^{2(d-1)} - 1)(2^d + 1)(2^{d-2} - 1)}{3}$$

*contains at least* 6 *different primes.*

Proof: Let $d = 2a$ with $a = 2^f \geq 5$. We may choose primitive prime divisors $p_1, \ldots, p_4$ of

$$2^{2(d-1)} - 1,\ 2^{d-1} - 1,\ 2^{d-2} - 1,\ 2^{a-1} - 1.$$

Obviously, the primes $p_1 \ldots, p_4$ are pairwise different and $p_i \mid f(d)$ for all $i$. Furthermore, $p_i \neq 3$ for all $i$ as $a \geq 5$. If we put $p_5 = 2^d + 1$ and $p_6 = 3$ then $p_1, \ldots, p_6$ are pairwise distinct and $p_i \mid f(d)$ for $i = 1, \ldots, 5$. For $p_6 = 3$ note that $3 \mid 2^{2(d-1)} - 1$ and $3 \mid 2^{d-2} - 1$ since $d$ is even. Hence $3 \mid f(d)$. □

**Lemma 3.19** (Dempwolff) *Let* $G = \mathrm{PO}^-(2d, 2)$ *and let* $k$ *denote the rank of the action of* $G$ *on the set of 2-dimensional totally isotropic subspaces of the underlying orthogonal vector space. Then*

*a)* $k = 5$ *if* $d = 4$.

*b)* $k = 6$ *if* $d \geq 5$.

Proof: Let $A \neq B$ be two totally isotropic subspaces of dimension 2. By $Q$ we denote the quadratic form and by $b$ the associated symplectic form. We put $W = A + B$ and claim that $W$ has one of the following isometry types.

(i) $\dim W = 3$ and $W$ totally isotropic.

(ii) $\dim W = 3$ and $W = (A \cap B) \perp H$ where $H$ is a hyperbolic plane.

(iii) $\dim W = 4$ and $W$ not degenerate of type $\mathrm{O}^+(4, 2)$.

(iv) $\dim W = 4$ and $W$ totally isotropic.

(v) $\dim W = 4$ and $W = R \perp H$ where $H$ is a hyperbolic plane and $R$ totally isotropic.

Let $R$ denote the radical of $W$ with respect to the symplectic form $b$, hence

$$R = \mathrm{rad}(W) = \{w \in W \mid b(w, x) = 0, \text{ for all } x \in W\}.$$

First we consider the case $\dim A \cap B = 1$, hence $\dim W = 3$.

Suppose that $W$ is not totally isotropic. Thus $Q(w) \neq 0$ for some $w \in W$. If $R = W$ then $W = U \perp \langle w \rangle$ where $U$ is totally isotropic. Thus $U$ is the set of isotropic vectors in $W$ contradicting $A, B \subseteq W$. It follows $R < W$. Thus $\dim R = 1$ and $R = A \cap B$. Moreover, since $W/R$ is a non-degenerate symplectic space via the lift of $b$ we get $W = (A \cap B) \perp H$ where $H$ is a hyperbolic plane. Note that $H$ can not be anisotropic as $W$ contains 2-dimensional totally isotropic subspaces.

Now let $A \cap B = 0$, hence $\dim W = 4$.

If $W$ is non-degenerate then $W$ is of type $\mathrm{O}^+(4, 2)$ since $\mathrm{O}^-(4, 2)$ does not have a totally isotropic 2-dimensional subspace. Suppose that $W$ is degenerate but not totally isotropic. Thus there is a $w \in W$ with $Q(w) \neq 0$ and $\dim R = 2$. The space $W/R$ is non-degenerate and symplectic with respect to the lift of $b$. Thus $W = R \perp U$ where $U$ is non-degenerate. If $R$ is totally isotropic then $U = H$ is a hyperbolic plane.

Finally, we show that $R$ must be totally isotropic. Suppose that $R$ is not totally isotropic. Clearly, $R$ contains isotropic vectors and we may assume that $R_0 = \langle w_0 \rangle$ is the set of isotopic vectors in $R$. Obviously, $R < A + R$ since $A$ is totally isotropic. Furthermore, $A + R < W$ since otherwise $R < \mathrm{rad}(W)$. This shows that $A \cap R \neq 0 \neq B \cap R$. It follows $R_0 \subset A \cap B = 0$, a contradiction.

It is easy to see that the orthogonal group $\mathrm{O}(W)$ acts transitively on the set of pairs of totally isotropic subspaces of dimension 2 which generate $W$. Thus an application of Witt's Theorem completes the proof, observing that for $d = 4$ there are no totally isotropic subspaces of dimension 4. □

**Lemma 3.20** *The group* $G = \mathrm{P}\Omega^-(2d, r)$ $(d \geq 4)$ *is not a* TI*-group for characters except of possibly* $G = \mathrm{P}\Omega^-(16, 2)$.

Proof: By Lemma 3.17, we may assume that $r = 2$ and $2^d + 1$ is a Fermat prime. Thus $d = 2^f$ with $f \geq 2$. For $d = 4$ the assertion follows by the GAP library. Thus we may

suppose that $d \geq 16$. By Lemma 2.1 of [6], the number of isotropic lines in the underlying orthogonal vector space is

$$f(d) = \frac{(2^{2(d-1)} - 1)(2^d + 1)(2^{d-2} - 1)}{3}.$$

The previous Lemma 3.19 shows that the action of $\mathrm{PO}^-(2d, 2)$ on the set of 2-dimensional totally isotropic subspaces is of rank 6, and by Lemma 3.18, $f(d)$ has at least 6 different prime divisors. Thus, by Proposition 2.8, there are primes $p \neq q$ such that $(\Phi_p, \Phi_q) > 1$ for $\mathrm{PO}^-(2d, 2)$. The assertion then also holds for $\mathrm{P\Omega}^-(2d, 2)$ because of the following observation. □

**Lemma 3.21** *Let $G \trianglelefteq H$ with $H/G$ solvable. If $1 < (\Phi_p(H), \Phi_q(H))$ then the same holds true for $G$.*

Proof: Let $\chi \in \mathrm{Irr}\Phi_p(H) \cap \mathrm{Irr}\Phi_q(H)$. Then both the reductions of $\chi$ modulo $p$ and $q$ contain the corresponding trivial Brauer character. Therefore if $G \leq \mathrm{Ker}\chi$ the same happens with respect to the group $H/G$ so we get $1 < (\Phi_p(H/G), \Phi_Q(H/G)))$ which contradicts 2.4. Finally the fact that $\Phi_p(H)_G = e\Phi_p(G)$ for some $e \in \mathrm{N}$ implies that some irreducible $1_G \neq \phi \leq \chi$ is a constituent in both $\Phi_p(G)$, $\Phi_q(G)$. □

The next Lemma finishes the proof for orthogonal groups.

**Lemma 3.22** $G = \mathrm{P\Omega}^-(16, 2)$ *is not a* TI*-group for characters.*

Proof: By ([6], Lemma 2.1), the underlying orthogonal vector space for $G$ contains

$$n = (2^7 - 1)(2^8 + 1) = 127 \cdot 257$$

isotropic lines. The permutation action of $G$ on these lines is of rank 3 (see [18]). If $\pi$ denotes the associated complex permutation character then

$$\pi = 1 + \chi + \psi$$

with irreducible characters $\chi \neq \psi$. By Proposition 2.8, we may assume that w.l.o.g. the reduction of $\chi$ modulo 127 and the reduction of $\psi$ modulo 257 contains the trivial character. Let $M$ denote the permutation module over $\mathbb{F}_2$. Using the computer algebra sytem MAGMA, E. O'Brien proved that $M$ contains the trivial module 7 times as a composition factor. Thus $\chi$ or $\psi$ (maybe both) contain the trivial character if reduced modulo 2. This completes the proof, by Proposition 2.8. □

Next we deal with unitary groups. Note that $\mathrm{PSU}(2, r) \cong \mathrm{PSL}(2, r)$ which we considered already in Lemma 1.2. With the group $\mathrm{PSU}(3, r)$ was dealt earlier in Lemma 3.7.

**Lemma 3.23** $G = \mathrm{PSU}(d, r)$ $(d \geq 4)$ *is not a* TI*-group for characters.*

Proof: According to [18] the action of $G$ on the set of isotropic lines has rank 3. By ([13], 9.17), the number of these lines is

$$n = \frac{r^{2d-1} + (-1)^d(r^d - r^{d-1}) - 1}{r-1}.$$

Thus, for $d$ even,

$$n = (r^{d-1} + 1)\frac{r^d - 1}{r-1}$$

and, for $d$ odd,

$$n = (r^d + 1)\frac{r^{d-1} - 1}{r-1}.$$

Observe that in the first case $d$ and in the second $d-1$ is not a prime. Thus Lemma 3.14 and Lemma 3.16 imply that $n$ contains at least three different primes except the case $r = 2$ and $d = 4$. But for $\mathrm{PSU}(4, 2)$ the statement follows by the GAP library. An application of Proposition 2.8 finishes the proof. □

**Lemma 3.24** *The groups $E_6(r)$, $E_7(r)$, $E_8(r)$, $F_4(r)$, ${}^2E_6(r)$ and ${}^3D_4(r)$ are not* TI*-groups for characters.*

Proof: The listed groups have the following permutation representations of degree $n$ and rank $k$.

| group | degree $n$ | rank $k$ | reference |
|---|---|---|---|
| a) $E_6(r)$ | $\frac{r^9-1}{r-1}(r^8 + r^4 + 1)$ | 3 | [25] |
| b) $E_7(r)$ | $\frac{r^{14}-1}{r-1}(r^9 + 1)(r^5 + 1)$ | 4 | [25] |
| c) $E_8(r)$ | $\frac{r^{30}-1}{r-1}(r^{12} + 1)(r^{10} + 1)(r^6 + 1)$ | 5 | [25] |
| d) $F_4(r)$ | $\frac{r^{12}-1}{r-1}(r^4 + 1)$ | 5 | [24] |
| e) ${}^2E_6(r)$ | $\frac{r^{12}-1}{r^2-1}(r^5 + 1)(r^9 + 1)$ | 5 | [19] |
| f) ${}^3D_4(r)$ | $(r + 1)(r^8 + r^4 + 1)$ | 4 | [26] |

Let $f(r)$ denote one of the expressions in the second column. We replace $r$ by the indeterminate $x$ and factor the corresponding polynomials $f(x)$ over the rationals in irreducible polynomials. Note that all the obtained factors are cyclotomic polynomials $\Phi_d(x)$. By Zsigmondy's Lemma 3.3, a primitive prime divisor of $r^d - 1$ divides $\Phi_d(r)$, but not $\Phi_t(r)$ for $1 \leq t < d$ except of the cases $r = 2$ and $d = 6$ or $d = 2$ and $r$ a Mersenne prime. Moreover, in the second case $\Phi_2(r) = r + 1 = 2^s$, $\Phi_1(r) = r - 1 = 2^s - 2$ and we still may choose 2 different primes dividing $\Phi_2(r)$ and $\Phi_1(r)$.

This implies that the number of different irreducible factors not equal to $\Phi_6(x)$ is a lower bound for the number of different primes occuring in $f(r)$. In case $r \neq 2$ we may also count the factor $\Phi_6(x)$.
The factorizations are as follows

a) $\frac{x^9-1}{x-1}(x^8 + x^4 + 1) = \Phi_{12}(x)\Phi_9(x)\Phi_6(x)\Phi_3(x)^2$.

b) $\frac{x^{14}-1}{x-1}(x^9+1)(x^5+1) = \Phi_{18}(x)\Phi_{14}(x)\Phi_{10}(x)\Phi_7(x)\Phi_6(x)\Phi_2(x)^3$.

c) $\frac{x^{30}-1}{x-1}(x^{12}+1)(x^{10}+1)(x^6+1) =$
$\Phi_{30}(x)\Phi_{24}(x)\Phi_{20}(x)\Phi_{15}(x)\Phi_{12}(x)\Phi_{10}(x)\Phi_8(x)\Phi_6(x)\Phi_5(x)\Phi_4(x)^2\Phi_3(x)\Phi_2(x)$.

d) $\frac{x^{12}-1}{x-1}(x^4+1) = \Phi_{12}(x)\Phi_8(x)\Phi_6(x)\Phi_4(x)\Phi_3(x)\Phi_2(x)$.

e) $\frac{x^{12}-1}{x^2-1}(x^5+1)(x^9+1) = \Phi_{18}(x)\Phi_{12}(x)\Phi_{10}(x)\Phi_6(x)^2\Phi_4(x)\Phi_3(x)\Phi_2(x)^2$.

f) $(x+1)(x^8+x^4+1) = \Phi_{12}(x)\Phi_6(x)\Phi_3(x)\Phi_2(x)$.

Thus in each case we see that the degree $n$ contains at least $k$ different primes except of the case f) with $r = 2$. But $G = {}^3D_4(2)$ satisfies $(\Phi_2, \Phi_3) > 1$, by the GAP library, and the assertion follows again by Proposition 2.8. □

**Lemma 3.25** *Let $r = 2^{2n+1} > 2$. Then ${}^2F_4(r)$ and the Tits simple group ${}^2F_4(2)'$ are not* TI*-groups for characters.*

Proof: By [26], the group ${}^2F_4(r)$ with $r \neq 2$ has a rank 5 permutation representation of degree

$$n = (r+1)(r^6+1)(r^3+1) = (r+1)\frac{r^{12}-1}{r^3-1} = \Phi_{12}(r)\Phi_6(r)\Phi_4(r)(r+1)^2.$$

If $r$ is exceptional then $r = 8$ and $n$ contains 6 different primes. Thus we may assume that $r$ is not exceptional. Therefore $r+1$ must contain two different primes. As $r \neq 2$ we get three more different primes by the same argument as in Lemma 3.24 and we are done. The group ${}^2F_4(2)'$ satisfies $(\Phi_2, \Phi_3) > 1$, by the GAP library. □

**Lemma 3.26** *The groups $G_2(r)$ for $r > 2$ and $G_2(2)'$ are not* TI*-groups for characters.*

Proof: The group $G_2(2)' \cong \mathrm{PSU}(3,9)$ was already considered in Lemma 3.23. Thus let $r > 2$.

Suppose that $(\Phi_p, \Phi_q) = 1$ for all primes $p \neq q$. By Proposition 3.5, we may assume that $r$ is exceptional.

For $r = 8$ we have $p = 19 \mid r^2 - r + 1 = 57$ and by [22], we obtain $(\Phi_{19}, \chi_{16}) = 1$ for $\chi_{16} \in \mathrm{Irr}(G_2(8))$. On the other hand, for $q = 3 \mid r + 1 = 9$, we obtain, by ([10], p. 98), that $(\Phi_3, \chi_{16}) = 2$. Thus $(\Phi_3, \Phi_{19}) > 1$, a contradiction to the assumption.

By [24], there is a transitive permutation representation of $G_2(r)$ of degree $n = \frac{r^6-1}{r-1}$ and rank 4. We claim that $n$ contains at least 4 different primes.

Assume first that $r = 2^{2^s}$ with $s > 0$ and $r + 1$ a Fermat prime, so in this case

$$n = \frac{2^{2^s 6} - 1}{2^{2^s} - 1}.$$

If $r = 4$, then

$$n = 3 \cdot 5 \cdot 7 \cdot 13$$

and the claim follows. Now let $s > 1$. By Lemma 3.3, we may take a primitive prime divisor $p_1$ of $2^{2^s 6} - 1$, a primitive prime divisor $p_2$ of $2^{2^s 2} - 1$, a primitive prime divisor $p_3$ of $2^{2^s 3} - 1$ and a prime $p_4 \mid 2^{2^{s-1} 3} - 1$ with $p_4 \nmid 2^{2^s} - 1$. Then all these primes are distinct and $p_1, p_2, p_3, p_4 \mid n$.

Next we consider the case that $r$ is a Mersenne prime, hence $r = 2^l - 1$ with $l$ a prime. By the GAP library, $r \neq 3$, hence $l$ is odd. Note that this implies that $r \equiv 1 \bmod 3$ and therefore

$$2, 3 \mid (r+1)(r^2 - r + 1)(r^2 + r + 1) = n.$$

Let $p_1$ be a primitive prime divisor of $r^6 - 1$ (note that $r \neq 2$) and let $p_2$ be a primitive prime divisor of $r^3 - 1$. Then $p_1, p_2 \mid n$ and as $2, 3 \mid r^2 - 1$ we get $p_1, p_2 \neq 2, 3$. Thus we have again 4 different prime divisors of $n$.

In both cases an application of Proposition 2.8 finishes the proof. □

# 4 Symmetric and alternating groups

In this section we prove

**Proposition 4.1** *Symmetric or alternating groups on $n \geq 5$ letters are not* TI*-groups for characters.*

Note that we only have to prove Propostion 4.1 for symmetric groups because of Lemma 3.21.

For the rest of this section let $G = \mathrm{S}_n$ with $n \geq 5$. By the GAP library [7], we may even assume $n > 17$. Unfortunately, Corollary 2.9 does not work if $n$ is a power of a prime. Thus we apply a result of James in his book [16] which uses the following notation.

**Definition 4.2** [17] Let $p$ be a prime. We say that an integer $n$ contains $\lambda \bmod p$ if in the $p$-adic representations

$$n = a_s p^s + a_{s-1} p^{s-1} + \ldots + a_1 p + a_0$$
$$\lambda = b_t p^s + b_{t-1} p^{t-1} + \ldots + b_1 p + b_0$$

we either have $b_i = 0$ or $b_i = a_i$. We put

$$f_p(n, \lambda) = \begin{cases} 1, & \text{if } n+1 \text{ contains } \lambda \bmod p \\ 0, & \text{otherwise.} \end{cases}$$

**Theorem 4.3** ([16], Theorem 24.15) *Let $p$ be a prime and let $(n-\lambda, \lambda)$ be a 2-part partition of $n$. Then*

$$[S^{(n-\lambda,\lambda)}, D^{(n)}]_p = f_p(n, \lambda),$$

*which means that modulo $p$ the trivial character occurs in the classical irreducible character $\chi^{(n-\lambda,\lambda)}$ associated to the partition $(n-\lambda, \lambda)$ with multiplicity $f_p(n, \lambda)$. In particular, $(\Phi_p, \chi^{(n-\lambda,\lambda)}) \geq f_p(n, \lambda)$.*

**Lemma 4.4** *Let $p$ be a prime.*

*a) If $p > \lambda$ then $f_p(n, \lambda) = 1$ if and only if $p \mid n - \lambda + 1$.*

*b) If $p^i > \lambda$ for some $i \in \mathrm{N}$ and $p^i \mid n - \lambda + 1$ then $f_p(n, \lambda) = 1$.*

Proof: a) Let $p > \lambda$. Thus $n + 1$ contains $\lambda \bmod p$ if and only if $n + 1 \equiv \lambda \bmod p$.
b) If $p^i \mid n - \lambda + 1$ with $p^i > \lambda$ then $n + 1 = kp^i + \lambda$ contains $\lambda \bmod p$. □

As an immediate consequence we have

**Lemma 4.5** *If there are primes $p \neq q$ with $p, q > \lambda$ and $p, q \mid n - \lambda + 1$ then*

$$f_q(n, \lambda) = 1 = f_p(n, \lambda)$$

*and therefore $(\Phi_p, \Phi_q) > 1$.*

Observe that Lemma 4.5 covers again the case $n \neq p^l$ for $p$ a prime with $\lambda = 1$.

**Lemma 4.6** *Let $n = 2^l$. Then there are primes $p \neq q$ such that $(\Phi_p, \Phi_q) > 1$.*

Proof: If $l = 2s$ then $n - 1 = (2^s - 1)(2^s + 1)$. Since $s \geq 2$ and $gcd(2^s - 1, 2^s + 1) = 1$ there are odd primes $p \neq q$ with $pq \mid n - 1$. Thus the assertion follows by Lemma 4.5 with $\lambda = 2$. In case $l = 2s + 1$ we have $n - 2 = 2(2^s - 1)(2^s + 1)$. If $2^s - 1$ and $2^s + 1$ are not powers of 3 we are done again by Lemma 4.5 with $\lambda = 3$. Thus we may first suppose that $2^s - 1 = 3^t$. By Lemma 3.2, the only solution is $s = 2$ and therefore $n = 32$. But $n + 1 = 33 = 5^2 + 5 + 3 = 4 \cdot 7 + 5$ contains $\lambda = 5$ modulo the primes 5 and 7, which proves that $f_5(32, 5) = 1 = f_7(32, 5)$. Thus the assertion follows by Theorem 4.3. Finally, we are left with the case $2^s + 1 = 3^t$. Since $s \geq 2$ the only solution is $s = 3$ and $t = 2$, by Lemma 3.2. Thus $n = 2^7$ and $2^7 - 2 = 2 \cdot 7 \cdot 9$. By Lemma 4.4 a), we get $f_7(2^7, 3) = 1$, and by part b) of the same Lemma $f_3(2^7, 3) = 1$. □

**Lemma 4.7** *If $n = p^l \equiv 1 \bmod 4$ then there are primes $p \neq q$ such that $(\Phi_p, \Phi_q) > 1$.*

Proof: Since $4 \mid n - 1$ we have $f_2(n, 2) = 1$, by Lemma 4.4 b). If $n - 1$ is not a power of 2 then there is an odd prime $p \mid n - 1$, hence $f_p(n, 2) = 1$, by part a) of Lemma 4.4. Thus we may assume that $p^l - 1 = 2^s$ with $s \geq 4$. By Lemma 3.2, the solutions of this equality are $p = 3, l = 2, s = 3$ a contradiction since $n > 17$, or $l = 1$ and $p = 2^s + 1$ is a Fermat prime. Thus $s$ is a power of 2, in particular $s = 2t$ with $t \geq 3$. We consider now

$$n - 2 = p - 2 = (2^t - 1)(2^t + 1).$$

If both $2^t - 1$ and $2^t + 1$ are not powers of 3 we are done by Lemma 4.4. Since $t \geq 3$ the equation $2^t - 1 = 3^a$ has no solution. The other equation $2^t + 1 = 3^a$ has, by Lemma 3.2, only the solution $t = 3$ and $a = 2$. But then $n - 2 = p - 2 = 7 \cdot 9$, hence $p = 65$, a contradiction. □

According to Lemmata 4.5, 4.6 and 4.7 we are left with the case $n = p^l \equiv 3 \bmod 4$. In particular, $p \equiv 3 \bmod 4$. If $l = 2s$ then $p^l \equiv (3^2)^s \equiv 1 \bmod 4$ and Lemma 4.7 applies. Thus we may assume that $l$ is odd.

**Lemma 4.8** *Let $n = p^l$ with $l$ odd and suppose that one of the following conditions hold.*

(i) $n \equiv 0 \bmod 3$

(ii) $n \equiv 1 \bmod 3$

(iii) $n \equiv 2 \bmod 9$.

*Then there are primes $p \neq q$ such that $(\Phi_p, \Phi_q) > 1$ unless $n = 19$ or $n = 27$.*

Proof: (i) Clearly, $p = 3$ and we may assume $l = 2s+1$ with $s > 1$ since we excluded $n = 27$. If we put $\lambda = 4$ then

$$n - \lambda + 1 = n - 3 = 3^l - 3 = 3(3^s - 1)(3^s + 1).$$

Note that either $4 \mid 3^s + 1$ or $4 \mid 3^s - 1$. Therefore $8 \mid n - 3$ so we have $f_2(n, 4) = 1$ by Lemma 4.4 b). If both $3^s - 1$ and $3^s + 1$ are powers of 2 then $s = 1$ which is a contradiction. Therefore there is a prime $p \geq 5 > \lambda = 4$ such that $p \mid n - 3$. Thus $f_p(n, 4) = 1$, again by Lemma 4.4, and the proof for (i) is complete.
(ii) Since we assume that $n \equiv 3 \bmod 4$ the 2-part of $n - 1$ is exactly 2. Thus we are done with Lemma 4.5 for $\lambda = 2$ if $\frac{n-1}{2}$ is not a power of a prime. In case it is a prime power we get

$$n - 1 = 2 \cdot 3^r$$

since $n \equiv 1 \bmod 3$. If $r = 2s$ we put $\lambda = 4$ and obtain

$$n - 3 = n - \lambda + 1 = 2(3^s - 1)(3^s + 1).$$

Since $4 \mid n - 1$ we have $f_2(n, 2) = 1$. And as before $s > 1$ because if $s = 1$ we get $n = 19$. Therefore there is a prime $p \geq 5 > \lambda = 4$ with $f_p(n, 2) = 1$. Finally, if $r = 2s + 1$ we put $\lambda = 8$. Then

$$n - 7 = n - \lambda + 1 = 6(3^s - 1)(3^s + 1).$$

If $s = 1$ then $n = 55$ and we are done by Lemma 4.5 with $\lambda = 1$, thus $s \geq 2$. Note that $16 \mid n - \lambda + 1$ and therefore $f_2(n, 8) = 1$, by Lemma 4.4 b). By the same lemma we are also done if $5^2$ or $7^2$ or a prime $q > 7$ divides $n - 7$. This shows that we may assume

$$(3^s - 1)(3^s + 1) = 5^a 7^b 2^c$$

with $a, b \leq 1$. Since the 2-part of one of the factors $3^s - 1$ or $3^s + 1$ is exactly 2 we get

$$3^s - 1 \leq 5 \cdot 7 \cdot 2 = 70,$$

hence $s \leq 3$. If $s = 2$ then $n = 487$. For $\lambda = 3$, we have $487 - \lambda + 1 = 487 - 2 = 5 \cdot 97$ and the assertion follows by Lemma 4.4. In the remaining case $s = 3$ we have $n = 4375 = 5^4 \cdot 7$ and Lemma 4.5 with $\lambda = 1$ applies.
(iii) If $9 \mid n-2$ then $9 \mid n-\lambda+1$ for $\lambda = 3$. Thus $f_3(n, 3) = 1$, by Lemma 4.4 b). Since $n-2$ is odd, we may apply again Lemma 4.4 if there exists a prime $q > 5$ with $q \mid n - 2$ which

yields $f_q(n,3) = 1$. Therefore we only have to consider the case $n-2 = 3^t$ with $t \geq 3$. If $t = 2s$ we choose $\lambda = 4$. Then

$$n - \lambda + 1 = n - 3 = 3^{2s} - 1 = (3^s - 1)(3^s + 1).$$

Since $8 \mid n-3$, we get $f_2(n,4) = 1$, by Lemma 4.4 b). Furthermore $(3^s-1)(3^s+1)$ is not a power of 2 since $s > 1$. Thus there is a prime $q > \lambda = 4$ with $q \mid n-3$ and therefore $f_q(n,4) = 1$, by Lemma 4.4. Finally we have to consider $t = 2s+1$. With $\lambda = 6$ we get

$$n - \lambda + 1 = n - 5 = 3^{2s+1} - 3 = 3(3^s - 1)(3^s + 1).$$

If $s = 1$ then $n = 29$. Since $n - 1 = 28 = 4 \cdot 7$ we get by Lemma 4.4 that $f_2(29,2) = 1 = f_7(29,2)$. So we may assume $s \geq 2$. Clearly, $8 \mid n-5$, hence $f_2(n,6) = 1$. Now we are done if there is a prime $q > 5$ with $q \mid n-2$. If $3^s - 1$ is a 2-power then $s = 2$ and therefore $n = 3^5 + 2 = 245$ which is not a prime power. Since $3^s + 1$ is never a 2-power for $s \geq 2$ we get

$$5^2 \mid n - 5,$$

hence $f_5(n,6) = 1$, by Lemma 4.4 b). □

To finish the proof of Proposition 4.1 we consider 3-part partitions. The relevant fact which we need is the following result of To Law.

**Lemma 4.9** (Appendix, [17]) *If* $\Gamma = (n-\lambda-1, \lambda, 1)$ *then*

$$[S^\Gamma, D^{(n)}]_p \geq \left( \sum_{j=0}^{\lambda} m_j f_p(n-1-2j, \lambda - j) \right) - f_p(n,2) - f_p(n,3)$$

*for suitable* $m_j \in \mathrm{N}_0$ *which are given explicitely in* [17].

In the next two lemmas we prove the proposition for $n = 19$ and $n = 27$ which we had to exclude in Lemma 4.9.

**Lemma 4.10** *The statement in* Lemma 4.9 *holds also true for* $n = 19$.

Proof: We prove the assertion for $p = 5$ and $p = 2$ with the 3-part partition $\Gamma = (14, 4, 1)$. First we consider $p = 5$. By Lemma 4.9, we have

$$[S^\Gamma, D^{(19)}]_5 \geq m_0 f_5(18,4) - f_5(19,4) - f_5(19,5).$$

Now, by Lemma 4.4, the equation $19 = 18 + 1 = 3 \cdot 5 + 4$ implies $f_5(18,4) = 1$, and $20 = 19 + 1 = 4 \cdot 5$ implies $f_5(19,4) = 0 = f_5(19,5)$. Furthermore, $m_0 = 1$, by ([17], Appendix, (iv)) which proves that $[S^\Gamma, D^{(19)}]_5 \geq 1$.

For $p = 2$ we have

$$[S^\Gamma, D^{(n)}]_2 \geq m_3 f_2(12,1) - f_2(19,4) - f_2(19,5).$$

The equation $13 = 12 + 1 = 2^3 + 2^2 + 1$ yields $f_2(12,1) = 1$. Since $20 = 19 + 1 = 2^4 + 2^2$ we obtain $f_2(19,4) = 1$ and $f_2(19,5) = 0$. By ([17], Appendix, (iv)), we also have $m_3 = 2$ (since $j = 3 = 2^v - 1$ and $n - j = 16 = 2 \cdot 2^{v+1} + k$ with $v = 2$ and $k = 0$). This shows that $[S^\Gamma, D^{(19)}]_2 \geq 1$ and the proof is complete. □

**Lemma 4.11** *The statement in* Lemma 4.9 *holds also true for* $n = 27$.

Proof: We put $\Gamma = (19, 7, 1)$. For $p = 3$ we have

$$[S^\Gamma, D^{(n)}]_3 \geq m_1 f_3(24, 6) - f_3(27, 7) - f_3(27, 8).$$

The equation $28 = 27 + 1 = 3^3 + 1$ yields $f_3(27, 7) = f_3(27, 8) = 0$. Since $25 = 24 + 1 = 2 \cdot 3^2 + 2 \cdot 3 + 1$ we get $f_3(24, 6) = 1$. By Appendix (iv) of [17], we have $j = 1 \leq p - 2 = 1$ and $n - j = 26 \equiv -1 \bmod 3$, hence $m_1 = 1$. Thus $[S^\Gamma, D^{(n)}]_3 \geq 1$.

In case $p = 2$ we have

$$[S^\Gamma, D^{(n)}]_2 \geq m_3 f_2(20, 4) - f_2(27, 4) - f_2(27, 5).$$

The equation $28 = 27+1 = 2^4+2^3+2^2$ yields $f_2(27, 4) = 1$ and $f_2(27, 5) = 0$. Furthermore, $f_2(20, 4) = 1$ since $21 = 20 + 1 = 2^4 + 2^2 + 1$. By Appendix (iv) of [17], we obtain $m_3 = 2$ as $3 = j = u2^v - 1$ with $u = 1, v = 2$ and $n - j = 24 = 32^{v+1} + k$ with $-1 \leq k = 0 \leq 2^v - 2$. This shows that $[S^\Gamma, D^{(n)}]_2 \geq 1$. □

Now we are ready to finish the proof of Proposition 4.1.

**Lemma 4.12** *Let* $n \equiv 2 \bmod 3$, $n \not\equiv 2 \bmod 9$ *and* $n \equiv 3 \bmod 4$. *Then* $(\Phi_2, \Phi_3) > 1$.

Proof: Let $\Gamma = (n - 3, 2, 1)$. As $n + 1 \equiv 0 \bmod 3$ and $n + 1 \not\equiv 3 \bmod 9$ we have either $n + 1 = 9k + 6$ or $n + 1 = 9k$. In both cases $n + 1$ does not contain neither 2 nor 3 mod 3. Therefore $f_3(n, 2) = f_3(n, 3) = 0$. But $f_3(n - 1, 2) = 1$ as $3 \mid n - 2$. Thus we obtain

$$[S^\Gamma, D^{(n)}]_3 \geq f_3(n - 1, 2) - f_3(n, 2) - f_3(n, 3) = 1.$$

Since $n + 1 \equiv 0 \bmod 4$ we have that $n + 1$ does not contain neither 2 nor 3 mod 2, hence $f_2(n, 2) = f_2(n, 3) = 0$. But $n = 4k - 1 = 4(k - 1) + 2 + 1$ contains 2 mod 2, hence $f_2(n - 1, 2) = 1$. Thus we get

$$[S^\Gamma, D^{(n)}]_2 \geq f_2(n - 1, 2) - f_2(n, 2) - f_2(n, 3) = 1.$$

□

# 5 Sporadic groups

**Proposition 5.1** *A sporadic simple group is not a* TI*-group for characters.*

Proof: If $G$ is not one of the groups $J_4, Th, Fi'_{24}, B, M, Ly$ or $Co_1$ we find decomposition matrices in the GAP library to check the assertion. If $G$ is one of the groups $J_4, Th, M$ decomposition matrices for cyclic blocks are given in [10] and the assertion follows by using Propostion 2.6. Finally, the same approach works for $Fi'_{24}$ and $B$. In both cases the decomposition matrices for cyclic blocks of the cover groups are given in [10]. But the relevant characters are already characters of the simple groups. The assertion for the remaining two

groups $Co_1$ and $Ly$ follows by recent results of Thackrey which was brought to our attention by Lukas Mass from IEM at Essen. More precisely, the Conway group $Co_1$ has an irreducible character $\chi_{10}$ of degree 80730 which is contained in $\Phi_2$ and $\Phi_7$. The Lyons group has a real valued character $\chi_{14}$ of degree 4226695 which contains the trivial character modulo 3. Thus $(\Phi_3, \Phi_2) > 1$, by Proposition 2.6. □

**Acknowledgment** We are gratefully indepted to several people who helped us to solve particular problems. B. Guralnick brought his paper [9] to our attension. O'Brien did the computations we needed in 3.22. To attack the sporadic groups $Ly$ and $Co_1$ we learned unpublished results of Thrackrey from W. Lempken and L. Maas. Finally, the authors thank B. Huppert for fruitful discussions on small rank permutation representations of classical groups.

# References

[1] H. Andikfar. Decomposition numbers and Cartan invariants of $\mathrm{Sp}(4,q)$, $q = 2^n$, *for* $p = 2^*$. Comm. in Algebra 35 (2007), 1715-1745.

[2] C. Bessenrodt and J. Zhang. Block separation and inclusions. To appear Advances Math..

[3] R. Burkhardt. Die Zelegungsmatrizen der Gruppen $\mathrm{PSL}(2, p^f)$. J. Algebra 40 (1976), 75-96.

[4] P.J. Cameron. Finite permutation groups and finite simple groups. Bull. London Math. Soc. 13 (1981), 1-22.

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

[6] T. Fujisaki. The action of finite orthogonal groups in characteristic 2 on the set of anisotropic lines. J. London Math. Soc. 73 (2006), 287-303.

[7] GAP library
`http://www.math.rwth-aachen.de/homes/MOC/decomposition.`

[8] R. Gow and W. Willems. Quadratic geometries, projective modules and idempotents. J. Algebra 160 (1993), 257-272.

[9] R. Guralnick. Subgroups of prime power index in a simple group. J. Algebra 81 (1983), 304-311.

[10] G. Hiss and K. Lux. Brauer trees of sporadic groups. Clarendon Press, Oxford 1989.

[11] G. Hiss. The number of trivial composition factors of the Steinberg module. Arch. Math. 54 (1990), 247-251.

[12] G. Hiss. Zerlegungszahlen endlicher Gruppen vom Lie-Typ in nicht-definierender Charakteristik. Habilitation, Aachen 1990.

[13] B. Huppert. *Geometric algebra.* Lecture Notes, University of Illinois at Chicago Circle, 1970.

[14] B. Huppert and N. Blackburn. *Finite groups II, III.* Springer, Berlin 1982.

[15] I.M. Isaacs. *Character theory if finite groups.* Academic Press, New York 1976.

[16] G. D. James. *The Representation Theory of the Symmetric Groups.* Lecture Notes 682, Springer-Verlag, 1978.

[17] G. D. James and A. Williams. Decomposition Numbers of Symmetric Groups by Induction. J. of Algebra 228 (2000), 119-142.

[18] W.M. Kantor and R.A. Liebler. The rank 3 permutation representations of finite classical groups. Trans. Am. Math. Soc. 271 (1982), .....?

[19] V.V. Korableva. Parabolic permutation representations of the group ${}^2E_6(q^2)$. Mathematical Notes 67 (2000), 758-770.

[20] G. Navarro. *Characters and blocks of finite groups.* London Mathematical Society Lecture Note Series, 250. Cambridge University Press, Cambridge, 1998.

[21] J. Shamash. Blocks and Brauer trees for groups of type $G_2(q)$. Proc. of Symposia in Pure Mathematics 47, part 2 (1986), 283-295.

[22] J. Shamash. Blocks and Brauer trees for the groups $G_2(2^k), G_2(3^k)$. Comm. in Algebra 20 (1992), 1375-1387.

[23] K.W. To Law. Results on Decomposition Matrices for the Symmetric groups. Thesis, University of Cambridge, 1983.

[24] A.V. Vasilyev. Minimal permutation representations of finite simple exceptional groups of types $G_2$ and $F_4$. Algebra and Logic 35 (1996), 371-383.

[25] A.V. Vasilyev. Minimal permutation representations of finite simple exceptional groups of types $E_6, E_7$, and $E_8$. Algebra and Logic 36 (1997), 302-310.

[26] A.V. Vasilyev. Minimal permutation representations of finite simple exceptional twisted groups. Algebra and Logic 37 (1997), 9-20.

[27] H. Wielandt. *Finite permutation groups.* Mathematical works of Helmut Wielandt, Vol. 1, de Gruyter, pp. 119-198.

[28] D. White. Decomposition numbers of $\mathrm{Sp}_4(2^a)$ in odd characteristics. J. Algebra 177 (1995), 264-276.

Conchita Martínez-Pérez
Departamento de Matemáticas
Universidad de Zaragoza,
50009 Zaragoza

Wolfgang Willems
Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg