ILLINOIS JOURNAL OF MATHEMATICS
Volume 44, Number 4, Winter 2000

SOME SIMPLE GROUPS WHICH ARE DETERMINED BY THE SET OF THEIR CHARACTER DEGREES I

BERTRAM HUPPERT

In memory of Michio Suzuki

ABSTRACT. The following conjecture is studied. Let G be a simple nonabelian group. If H is any group which has the same *set* of character degrees as G, then $H \cong G \times A$, where A is abelian. In the present paper this is proved if G is a Suzuki group on some $\mathrm{SL}(2, 2^f)$.

1. Introduction

For any group G we denote by $\mathrm{Irr}\, G$ the set of all irreducible complex characters of G. If we know the degreee $\chi(1)$ for all $\chi \in \mathrm{Irr}\, G$, then by

$$|G| = \sum_{\chi \in \mathrm{Irr}\, G} \chi(1)^2$$

the order of G is known. For 2-groups this means very little. A. Caranti informed me that the 2328 groups of order 2^7 have only 30 different degree patterns, and there are 538 of them with the same degrees.

If we turn to simple groups, we expect the situation to be much different, for simple groups have a very high degree of individuality. It is known that the only pairs of simple groups of the same order are

$$\mathrm{A}_8,\ \mathrm{PSL}(3,4) \quad \text{and} \quad \mathrm{PSp}(2n,q),\ P\Omega O(2n+1,q),$$

where $n \geq 3$ and q is odd. It is known that these groups are distinguished by their smallest character degree larger than 1. For instance, the smallest degree of A_8 is 7, while the smallest degree of $\mathrm{PSL}(3,4)$ is 20 (both coming from natural doubly transitive permutation representations of the groups); see V. Landazuri, G. Seitz.

It seems that for simple groups much more is true. For any group G we define the *set* $\mathrm{cd}\, G$ of character degrees of G by

$$\mathrm{cd}\, G = \{\chi(1) \mid \chi \in \mathrm{Irr}\, G\},$$

forgetting multiplicities. We dare to make a conjecture.

Received May 12, 1999; received in revised form November 12, 1999.
1991 Mathematics Subject Classification. Primary 20C15; Secondary 20D05.

CONJECTURE. *Let H be any simple nonabelian group and G a group such that* $\operatorname{cd} G = \operatorname{cd} H$. *Then $G \cong H \times A$, where A is abelian. (All simple groups in the Atlas are indeed distinguished by their sets of character degrees.)*

As some evidence I can prove this conjecture for the following:

(1) $H \cong Sz(q)$ (all q), PSL $(2, 2^f)$ (all f), PSL $(2, q)$ for $q = 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 31, 37, 47, 49, 53$, PSU $(3, q)$ for $q = 3, 4, 5, 7, 8, 9$, PSU $(4, 3)$, PSU $(5, 2)$, A_7, A_8, A_9, A_{10}, M_{11}, M_{12}, J_1, J_2, PSL $(3, q)$ for $q = 3, 4, 5$, PSp $(4, 3)$, PSp $(4, 4)$, PSp $(6, 2)$, $O^+(8, 2)$, $G_2(3)$, ${}^3D_4(2)$.

In this paper I present the proofs for the Suzuki groups $Sz(q)$ and the linear fractional groups PSL $(2, 2^f)$.

The proofs follow, with some deviations, the following pattern:
Step 1. Show $G' = G''$.
Step 2. Identify H as a chief factor G'/M of G.
Step 3. Show that any $\vartheta \in \operatorname{Irr} M$ is stable under G', which implies $[M, G'] = M'$.
Step 4. Show $M = E$(the trivial group).
Step 5. Show $G = G' \times C_G(G')$.

Step 1 is rather uniform; it depends on Lemma 4 below and may generalize to other groups, if their set of character degrees is completely known. Step 2 is the most delicate; it depends in nearly all cases on consequences of the classification of simple groups, in particular on the determination of all simple π-groups, where π is some set of four primes. Step 3 uses information about the maximal subgroups of H; there are complications if indices of some maximal subgroups of G'/M do divide some character degree of G'/M. Step 4 needs the knowledge of the Schur multiplier of H and sometimes information about the degrees of the irreducible projective representations of H. Step 5 finally needs information about the automorphisms of H.

For the groups H listed above all of this information is in the Atlas. I have to thank the authors of the Atlas for the rich mine of information they have provided. It seems possible, to prove the conjecture for Chevalley groups of small rank, like PSL$(2, q)$ or PSU$(3, q)$, provided Step 2 can be overcome by some special argument.

Finally, I want to thank the referee for several helpful suggestions.

We now collect several well known facts, which will be used frequently in our proofs.

LEMMA 1. (N. Ito, G. Michler, W. Willems; see Michler and Willems in bibliography). *Suppose p is a prime and $p \nmid \chi(1)$ for all $\chi \in \operatorname{Irr} G$. Then G has a normal abelian Sylow-p-subgroup. Hence if the character degrees of G are divisible only by the primes p and q, then G has a normal abelian subgroup A such that G/A is a $\{p, q\}$-group. By Burnside's theorem then G is solvable. (For solvable G, see Isaacs, p. 190.)*

We frequently use the following results from Clifford theory.

LEMMA 2. *Suppose* $N \trianglelefteq G$ *and* $\chi \in \operatorname{Irr} G$.

(*a*) *If* $\chi_N = \vartheta_1 + \cdots + \vartheta_k$ *with* $\vartheta_j \in \operatorname{Irr} N$, *then k divides* $|G/N|$. *In particular, if* $\chi(1)$ *is prime to* $|G/N|$ *then* $\chi_N \in \operatorname{Irr} N$.
(*b*) *If* $\chi_N \in \operatorname{Irr} N$, *then* $\chi\theta \in \operatorname{Irr} G$ *for every* $\theta \in \operatorname{Irr} G/N$. (*See Huppert I, pp.* 570–572.)

LEMMA 3. *Suppose* $N \trianglelefteq G$ *and* $\vartheta \in \operatorname{Irr} N$. *By* $I = I_G(\vartheta)$ *we denote the inertia subgroup of* ϑ *in* G.

(*a*) *If* $\vartheta^I = \sum_{i=1}^{k} \varphi_i$ *with* $\varphi_i \in \operatorname{Irr} I$, *then* $\varphi_i^G \in \operatorname{Irr} G$. *In particular* $\varphi_i(1)|G : I| \in \operatorname{cd} G$.
(*b*) *If* ϑ *allows an extension* ϑ_0 *to* I, *then* $(\vartheta_0\tau)^G \in \operatorname{Irr} G$ *for all* $\tau \in \operatorname{Irr} I/N$. *In particular* $\vartheta(1)\tau(1)|G : I| \in \operatorname{cd} G$.
(*c*) *If* $\varrho \in \operatorname{Irr} I$ *such that* $\varrho_N = e\vartheta$, *then* $\varrho = \vartheta_0\tau_0$, *where* ϑ_0 *is a character of an irreducible projective representation of* I *of degree* $\vartheta(1)$ *while* τ_0 *is the character of an irreducible projective representation of* I/N *of degree* e (*Huppert I, pp.* 571–574).

LEMMA 4. *Let* G/N *be a solvable factor group of* G, *minimal with respect to being nonabelian. Then two cases can occur.*

(*a*) G/N *is a p-group for some prime p. Hence there exists* $\psi \in \operatorname{Irr} G/N$ *such that* $\psi(1) = p^b > 1$. *If* $\chi \in \operatorname{Irr} G$ *and* $p \nmid \chi(1)$, *then* $\chi\tau \in \operatorname{Irr} G$ *for all* $\tau \in \operatorname{Irr} G/N$ (*see Lemma* 2).
(*b*) G/N *is a Frobenius group with an elementary abelian Frobenius kernel* F/N. *Then* $|G/F| \in \operatorname{cd} G$ *and* $|F/N| = p^a$ *for some prime p. Then* F/N *is an irreducible module for the cyclic group* G/F, *hence a is the smallest integer such that* $p^a - 1 \equiv 0 (\operatorname{mod} |G/F|)$. *If* $\psi \in \operatorname{Irr} F$, *then either* $|G/F|\psi(1) \in \operatorname{cd} G$ *or* $|F/N|$ *divides* $\psi(1)^2$. *In the latter case p divides* $\psi(1)$.

If no proper multiple of $|G/F|$ *is in* $\operatorname{cd} G$, *then* $\chi(1)$ *divides* $|G/F|$ *for all* $\chi \in \operatorname{Irr} G$ *such that* $p \nmid \chi(1)$.

Proof. All these statements except the last one are in Isaacs, pp. 199–200. Suppose that no proper multiple of $|G/F|$ is in $\operatorname{cd} G$. Then p divides the degree of each nonlinear character of F. Suppose $\chi \in \operatorname{Irr} G$ and $p \nmid \chi(1)$. Then by Lemma 2,

$$\chi_F = \psi_1 + \cdots + \psi_k,\ \psi_j \in \operatorname{Irr} F,$$

where k divides $|G/F|$. As $p \nmid \chi(1)$, so $p \nmid \psi_j(1)$, hence $\psi_j(1) = 1$. But then $\chi(1) = k$ divides $|G/F|$.

In some cases the proof of $G' = G''$ is a consequence of the following lemma.

LEMMA 5. *Let G be a group with the following properties*:

(1) *If $\chi \in \operatorname{Irr} G$ and $\chi(1) > 1$, then no proper multiple of $\chi(1)$ is in $\operatorname{cd} G$.*
(2) *For any $\chi \in \operatorname{Irr} G$, $\chi(1) > 1$, the largest common divisor of*

$$\{\tau(1) \mid \tau \in \operatorname{Irr} G, \tau(1) \neq \chi(1), \tau(1) > 1\}$$

is 1. (This obviously implies $|\operatorname{cd} G| \geq 4$.)

Then $G' = G''$.

Proof. Otherwise there exists a solvable, minimal nonabelian factor group G/N of G.

Suppose at first that G/N is a p-group. Then by assumption (2) there exists $\chi \in \operatorname{Irr} G$ such that $\chi(1) > 1$ and $p \nmid \chi(1)$. By Lemma 4, $\chi\tau \in \operatorname{Irr} G$, where $\tau \in \operatorname{Irr} G/N$ and $\tau(1) = p^b > 1$. But this contradicts assumption (1).

Hence we are in the situation of Lemma 4(b). In particular G/N is a Frobenius group with Frobenius kernel F/N of prime p-power order, and $1 < |G/F| \in \operatorname{cd} G$. Let $\chi \in \operatorname{Irr} G$ with $\chi(1) > 1$ and $\chi(1) \neq |G/F|$. Then $\chi(1)$ does not divide $|G/F|$, by assumption (1). But no proper multiple of $|G/F|$ is in $\operatorname{cd} G$, again by assumption (1). We deduce from Lemma 4 that p divides $\chi(1)$. But this violates assumption (2).

Hence $G' = G''$.

LEMMA 6. *Suppose $M \trianglelefteq G' = G''$. For all $\lambda \in Irr\ M$ such that $\lambda(1) = 1$ and all $g \in G'$ suppose that $\lambda^g = \lambda$. Then $M' = [M, G']$ and $|M/M'|$ divides the order of the Schur multiplier of G'/M.*

Proof. For every $\lambda \in \operatorname{Irr} M$ such that $\lambda(1) = 1$, all $m \in M$, $g \in G'$ we obtain

$$\lambda(m^{-1}m^g) = \lambda(m)^{-1}\lambda^{g^{-1}}(m) = 1.$$

Hence

$$[m, g] \in \bigcap_{\lambda(1)=1} \operatorname{Ker}\lambda = M',$$

which shows $[M, G'] = M'$. As $G' = G''$, so

$$M/[M, G'] \leq Z(G'/[M, G']) \cap (G'/[M, G'])'.$$

Hence $|M/M'| = |M/[M, G'])$ divides the order of the Schur multiplier $H^2(G'/M, \mathbb{C}^\times)$ of G'/M [Huppert I, p. 629].

We first consider the series of the Suzuki groups $\operatorname{Sz}(q)$ ($q = 2^{2n+1} \geq 8$), indeed the only infinite series for which we can prove the conjecture at present.

2. The Suzuki groups $\mathrm{Sz}(q)$

Remarks. Suppose $q = 2^{2n+1} \geq 8$. The Suzuki group $\mathrm{Sz}(q)$ is a simple group of order

$$(q^2+1)q^2(q-1).$$

Its order is not divisible by 3.

Indeed, the Suzuki groups $\mathrm{Sz}(q)$ are the only simple groups whose orders are prime to 3 (see Glauberman, Cor. 7.3). Observe that $5 \mid q^2+1$, but $5 \nmid q-1$.

If we put

$$r = 2^n, \quad a = q+2r+1, \quad b = q-2r+1,$$

then

$$\operatorname{cd}\mathrm{Sz}(q) = \left\{1, q^2, q^2+1, (q-1)a, (q-1)b, (q-1)r\right\}.$$

Observe that $q^2+1 = a\,b$ and

$$(q^2+1, q-1) = (a, b) = 1.$$

Hence no degree $\neq 1$ of $\mathrm{Sz}(q)$ divides another degree, $q^2 = 2^{2(2n+1)}$ is the only prime power among the degrees, and $(q-1)r$ is the only "mixed" degree, which is even, but not a power of 2.

As

$$b < q-1 < a,$$

so

$$(q-1)b < a\,b = q^2+1 < (q-1)a.$$

Therefore $(q-1)\,a$ is the largest degree of $\mathrm{Sz}(q)$. (See Suzuki and Blackburn-Huppert III, p. 182.)

THEOREM 1. *If* $\operatorname{cd} G = \operatorname{cd}\mathrm{Sz}(q)$, *then*

$$G \cong \mathrm{Sz}(q) \times A,$$

where A is abelian.

Proof. Step 1. $G' = G''$.

The assumptions (1) and (2) of Lemma 5 are obviously fulfilled as the greatest common divisor of

$$\left\{q^2+1, (q-1)a, (q-1)b, (q-1)r\right\}$$

is 1 for $(q^2+1, (q-1)r) = 1$. Hence by Lemma 5, $G' = G''$.

Step 2. If G'/M is a chief factor of G, then $G'/M \cong \mathrm{Sz}(q)$.
By Step 1,

$$G'/M = S_1 \times \cdots \times S_k,\ S_i \cong S$$

where S is a simple, nonabelian group. As degrees of S divide some degree of G, so all degrees of S are prime to 3. By Lemma 1, the simple group S is a $3'$-group. Hence by Glauberman, $S \cong \mathrm{Sz}(q_0)$ for some $q_0 = 2^{2m+1} \geq 8$.

Suppose $k > 1$. Then take $\psi_i \in \mathrm{Irr}\, S_i$ $(i = 1, 2)$, where $\psi_1(1) = q_0^2$ and $\psi_2(1) = q_0^2 + 1$. Then $q_0^2(q_0^2+1)$ is a degree of G'/M, hence divides some degree of G. As $q_0^2\ (q_0^2+1)$ is a mixed number, so

$$q_0^2(q_0^2+1) \text{ divides } (q-1)2^n.$$

But $5 \mid q_0^2 + 1$ and $5 \nmid q - 1$, a contradiction. Hence $G'/M \cong \mathrm{Sz}(q_0)$ for some $q_0 = 2^{2m+1}$.

We put $\overline{G} = G/M$. Then

$$\overline{T} = \overline{G}' \times C_{\overline{G}}(\overline{G}') \trianglelefteq \overline{G}.$$

Now $|\overline{G}/\overline{T}|$ divides the order of the outer automorphism group of $\overline{G}' \cong \mathrm{Sz}(q_0)$, which is cyclic of order $2m+1$, hence is odd. Let $\psi \in \mathrm{Irr}\, \overline{G}'$ such that $\psi(1) = q_0^2$ and extend ψ trivially to $\overline{T}$. If $\chi \in \mathrm{Irr}\, \overline{G}$ and

$$(\chi_{\overline{T}}, \psi)_{\overline{T}} > 0$$

then $\chi(1) = e\psi(1) = e\, q_0^2$, where e divides $|\overline{G}/\overline{T}|$, so e is odd. If $e = 1$, then $\chi(1) = q_0^2$ is a power of 2, so $q_0 = q$. If $e > 1$, then $\chi(1)$ is a mixed degree of G, hence

$$\chi(1) = e\, q_0^2 = (q-1)2^n.$$

But then $q_0^2 = 2^n$, hence $n = 4m + 2$ and

$$2^{2n+1} - 1 = q - 1 = e \leq 2m + 1 = \frac{n}{2},$$

a contradiction. Therefore $G'/M \cong \mathrm{Sz}(q)$.

Step 3. If $\vartheta \in \mathrm{Irr}\, M$, then $I_{G'}(\vartheta) = G'$ and therefore $M' = [M, G']$.

Suppose $I_{G'}(\vartheta) = I < G'$ for some $\vartheta \in \mathrm{Irr}\, M$. If

$$\vartheta^I = \sum \varphi_i,\ \varphi_i \in \mathrm{Irr}\, I,$$

then, by Lemma 3,

$$\varphi_i(1)|G' : I|$$

is a degree of G', so divides some degree of G. The maximal subgroups of $\mathrm{Sz}(q)$ are of the orders

$$q^2\,(q-1),\, 4a,\ 4b$$

or are Suzuki groups $\mathrm{Sz}(q_0)$ over subfields $\mathrm{GF}(q_0)$ of $\mathrm{GF}(q)$, where $q = q_0^s$ and s odd (Suzuki, pp. 137–138). The indices are q^2+1 and

$$\frac{(q^2+1)q^2(q-1)}{4a} = b\,\frac{q^2}{4}(q-1),$$

$$\frac{(q^2+1)q^2(q-1)}{4b} = a\,\frac{q^2}{4}(q-1)$$

and

$$\frac{(q^2+1)q^2(q-1)}{(q_0^2+1)q_0^2(q_0-1)}$$

But $a\frac{q^2}{4}(q-1)$ and $b\frac{q^2}{4}(q-1)$ are mixed numbers, whose 2-part $\frac{q^2}{4} = 2^{4n}$ is larger than $r = 2^n$, hence they cannot divide the only mixed degree $(q-1)r$ of G. Also

$$\frac{(q^2+1)q^2(q-1)}{(q_0^2+1)q_0^2(q_0-1)}$$

is a mixed number as $q_0 < q$. If it divides $(q-1)r$, then $q^2+1 = q_0^{2s}+1$ has to divide $(q_0^2+1)(q_0-1)$. But as $s \geq 3$, so

$$q_0^{2s}+1 > q_0^6 > 2q_0^3 > (q_0^2+1)(q_0-1).$$

Hence this index is also impossible. Therefore $|G' : I| = q^2+1$ is the only possibility. But then $\varphi_i(1) = 1$, hence φ_i is an extension of ϑ to I.

Therefore

$$(\varphi_i\,\tau)^{G'} \in \mathrm{Irr}\,G'$$

for all $\tau \in \mathrm{Irr}\,I/M$, so

$$|G' : I|\tau(1) = (q^2+1)\tau(1) \in \mathrm{cd}\,G'.$$

The subgroups I/M of G'/M of index q^2+1 are Frobenius groups, which have characters of degreee $q-1$ (see Suzuki). Hence we obtain the contradiction

$$(q^2+1)(q-1) \in \mathrm{cd}\,G'.$$

Therefore $I_{G'}(\vartheta) = I$ for all $\vartheta \in \mathrm{Irr}\,M$. Hence by Lemma 6,

$$[M, G'] = M'.$$

As Sz(8) has a Schur multiplier of order 4 while $Sz(q)$ for $q > 8$ has trivial Schur multiplier (see Alperin, Gorenstein), we first consider the case $q > 8$.

Step 4. If $q > 8$, then $M = E$.

By Lemma 6, we obtain $M = M'$.

Take $\vartheta \in \operatorname{Irr} M$. By Step 3 then $I_{G'}(\vartheta) = G'$. As G'/M has trivial Schur multiplier, so ϑ allows an extension ϑ_0 to G' (Huppert I, p. 572). Then $\vartheta_0 \tau \in \operatorname{Irr} G'$ for all $\tau \in \operatorname{Irr} G'/M$. As $\operatorname{Irr} G'/M = \operatorname{Irr} G$, this implies

$$1 = \vartheta_0(1) = \vartheta(1).$$

Hence M is abelian, so

$$M = M' = E.$$

Step 5. If $q > 8$, then $G = G' \times C_G(G')$, where $G' \cong Sz(q)$ and $C_G(G')$ is abelian.

If $\chi \in \operatorname{Irr} G'$, $\chi(1) > 1$ and $I_G(\chi) = I$, we obtain a character ψ of G of a degree divisible by $|G : I|\chi(1)$. This forces $I_G(\chi) = G$ for all $\chi \in \operatorname{Irr} G'$. As the irreducible characters of G' separate the conjugacy classes of G', so G fixes all conjugacy classes of G'.

The outer automorphism group of $Sz(q)$ is cyclic of odd order $2n+1$ if $q = 2^{2n+1}$; it is induced by the Galois automorphisms of $GF(q)$. Now $Sz(q)$ contains diagonal matrices

$$\begin{pmatrix} a^{1+2^n} & & & \\ & a^{2^n} & & \\ & & a^{-2^n} & \\ & & & a^{-1-2^n} \end{pmatrix}$$

where $a \in GF(q)^\times$. Let α be an automorphism of $GF(q)$ of odd prime order $p \geq 3$. If $M(a)^\alpha$ and $M(a)$ are conjugate in $Sz(q)$, then

$$\operatorname{trace} M(a)^\alpha = \operatorname{trace} M(a) \in GF(2^m),$$

where $m = \frac{2n+1}{p}$. This implies

$$a^{1+2^n} + a^{2^n} + a^{-2^n} + a^{-1-2^n} = b \in GF(2^m).$$

For every $b \in GF(2^m)$, the equation

$$a^{2+2^{n+1}} + a^{1+2^{n+1}} + b\,a^{1+2^n} + a + 1 = 0$$

has at most $2^{n+1} + 2$ solutions a. Hence if we show that

$$(*) \qquad (2^{n+1} + 2)2^{\frac{2n+1}{p}} < 2^{2n+1} - 1,$$

there exists some a such that $M(a)^\alpha$ and $M(a)$ are not conjugate in $\mathrm{Sz}(q)$. If $n > 1$ and $p \geq 3$, then

$$1 + (2n+1)/p < n + 1 + (2n+1)/p < 2n + 1.$$

Therefore

$$(2^{n+1} + 2)2^{\frac{2n+1}{p}} < 2^{2n} + 2^{2n-1} < 2^{2n+1} - 1.$$

Hence G induces only inner automorphisms on G', which implies $G = G' \times C_G(G')$.

Now we turn to the exceptional case $q = 8$.

Step 4′. If $q = 8$, then $M = M'$.

Again $M/[M, G']$ is bounded by the Schur multiplier of $\mathrm{Sz}(8)$, which is of order 4. The degrees of the projective, not ordinary, representations of $\mathrm{Sz}(8)$ are

$$2^3 \cdot 5 = 40, 2^3 \cdot 7 = 56, 2^6, 2^3 \cdot 13 = 104$$

(see Atlas, p. 28). But the degrees 40, 56, 104 do not divide any degree of G, as

$$\mathrm{cd}\,\mathrm{Sz}(8) = \{1, 14, 35, 64, 65, 91\}.$$

Therefore $|M/[M, G']| = 4$ is impossible. Suppose $|M/[M, G']| = 2$. Then 2^6 is the only admissible degree of a representation of $G'/[M, G']$, not trivial on $M/[M, G']$. But then

$$2|\mathrm{Sz}(8)| = |G'/[M, G']| = |\mathrm{Sz}(8)| + 2^{12}t$$

for some t.

This implies the contradiction $2^{12} \mid |\mathrm{Sz}(8)|$. Hence $M = [M, G'] = M'$.

Step 5′. $M = E$.

Suppose $M = M' > E$. Let M/N be a chief factor of G', so

$$M/N \cong S_1 \times \cdots \times S_k,$$

where the S_i are isomorphic simple $3'$-groups, transitively permuted by G'. If $\vartheta \in \mathrm{Irr}\, S_1$, then by Step 3, ϑ is stable under G'. Hence $M/N \cong \mathrm{Sz}(q_0)$ for some q_0. As the outer automorphism group of $\mathrm{Sz}(q_0)$ is cyclic of order m, where $q_0 = 2^m$, so

$$G'/N = M/N \times C_{G'/N}(M/N) \cong \mathrm{Sz}(q_0) \times \mathrm{Sz}(8).$$

But this produces plenty of forbidden degrees.

Step 6′. $G = G' \times C_G(G')$, where $G' \cong \mathrm{Sz}(8)$ and $C_G(G')$ is abelian.

As $|\mathrm{Aut}\,\mathrm{Sz}(8)| = 3|\mathrm{Sz}(8)|$, so $G' \times C_G(G')$ has in G the index 1 or 3. As no degree of G is divisible by 3, so by Lemma 1, G has a normal Sylow-3-subgroup, which lies in $C_G(G')$. Hence

$$G = G' \times C_G(G').$$

(By Atlas, p. 28 we have $\mathrm{cd}\,\mathrm{Aut}\,\mathrm{Sz}(8) = \{1, 14, 64, 91, 105, 195\}$.)

3. The simple groups SL$(2, 2^f)$

In this section we would like to prove the following theorem.

THEOREM 2. *Suppose that* $f \geq 2$ *and*

$$\operatorname{cd} G = \operatorname{cd} \mathrm{SL}(2, 2^f) = \{1, 2^f - 1, 2^f, 2^f + 1\}.$$

Then $G \cong \mathrm{SL}(2, 2^f) \times A$, *where* A *is abelian.*

To master Step 2 in general, we use an unpublished result by F. Lübeck.

LEMMA 7. *Let* G *be a simple group. Suppose for every* $\chi \in \operatorname{Irr} G$ *that either* $\chi(1)$ *is odd or a power of* 2. *Then* $G \cong PSL\ (2, 2^f)$ *for some* $f \geq 2$.

To give proofs of Theorem 2 for $f = 2$ and $f = 3$, independent of the unpublished lemma 7, we shall use the following result.

LEMMA 8.

(a) *The only simple groups whose orders are divisible by only three primes are*
$\mathrm{PSL}(2, 5) \cong \mathrm{SL}(2, 4) \cong \mathrm{A}_5$, $\mathrm{PSL}(2, 9) \cong \mathrm{A}_6$,
$\mathrm{PSp}(4, 3)$ *for the primes* 2, 3, 5;
$\mathrm{PSL}(2, 7)$, $\mathrm{SL}(2, 8)$, $\mathrm{PSU}(3, 3)$ *for the primes* 2, 3, 7;
$\mathrm{PSL}(3, 3)$ *for the primes* 2, 3, 13;
$\mathrm{PSL}(2, 17)$ *for the primes* 2, 3, 17.
(*See W. Feit.*)

(b) *The only simple groups, all of whose character degrees are powers of primes are* $\mathrm{SL}(2, 4)$ *and* $\mathrm{SL}(2, 8)$. (*See O. Manz.*)

Proof of Theorem 2.
Step 1. $G' = G''$.
As $\operatorname{cd} G = \{1, 2^f - 1, 2^f, 2^f + 1\}$, this follows immediately from Lemma 5.
Step 2. If G'/M is a chief factor of G, then $G'/M \cong \mathrm{SL}(2, 2^f)$.
By Step 1,

$$G'/M = S_1 \times \cdots \times S_k,$$

where $S_i \cong S$ is a simple nonabelian group. If $\psi \in \operatorname{Irr} S$, then $\psi(1)$ is odd or a power of 2, and there are odd and even degrees larger than 1 of the simple group S. As G'/M has no mixed degrees, so $k = 1$. Then by Lemma 7,

$$S \cong \mathrm{SL}(2, 2^d) \text{ for some } d \geq 2.$$

For the cases $f = 2$ and $f = 3$ we can give complete proofs. Suppose at first that

$$\operatorname{cd} G = \operatorname{cd} \mathrm{SL}(2, 4) = \{1, 3, 4, 5\}.$$

Then S is a simple $\{2, 3, 5\}$-group, whose degrees are powers of primes. Then by Lemma 8, $S \cong \mathrm{SL}(2, 4)$. Similarly if

$$\mathrm{cd}\, G = \mathrm{cd}\, \mathrm{SL}(2, 8) = \{1, 7, 8, 9\},$$

then $S \cong \mathrm{SL}(2, 8)$.

Finally we remark that Step 2 can be done for

$$\mathrm{cd}\, G = \{1, 3, 4, 5\}$$

without any reference to the characterization of simple groups.

Take $\chi \in \mathrm{Irr}\, G$ such that $\chi(1) = 3$. As $G' = G''$, so $\chi_{G'} \in \mathrm{Irr}\, G'$. If we put $M = G' \cap \mathrm{Ker}\chi$, then G'/M is a perfect group with an faithful irreducible representation of degree 3. A classical result then shows

$$G'/M \cong \mathrm{A}_5,\ \mathrm{PSL}(2, 7) \text{ or } V,$$

where the Valentiner group V is the non splitting, central extension of a cyclic group of order 3 by the alternating group A_6 (v. d. Waerden, pp. 33–34). But PSL(2, 7) and V have the degree 6 (Atlas, p. 3 and p. 5), which does not divide any degree of G. Hence by this argument we also obtain

$$G/M \cong \mathrm{A}_5 \cong \mathrm{SL}(2, 4).$$

Hence by any of these arguments we have $G'/M \cong \mathrm{SL}(2, 2^d)$ for some $d \geq 2$. If $\psi \in \mathrm{Irr}\, G'/M$ and $\psi(1) = 2^d$, then the degree of any character of G/M above ψ is 2^f. So $d \leq f$.

We claim that $d = f$. Suppose $d < f$. We put $\overline{G} = G/M$. We have

$$\mathrm{cd}\, \overline{G} = \mathrm{cd}\, G = \{1, 2^f - 1, 2^f, 2^f + 1\}.$$

We consider

$$\overline{T} \subseteq \overline{G}' \times C_{\overline{G}}(\overline{G}') \trianglelefteq \overline{G}.$$

Then $|\overline{G}/\overline{T}| = m$ divides the order of the outer automorphism group of $\mathrm{SL}(2, 2^d)$, hence m divides d.

Let ψ be any character in $\mathrm{Irr}\, \overline{G}'$, which we extend trivially to a character ψ_0 of $\overline{T}$. If $\chi \in \mathrm{Irr}\, \overline{G}$ and χ is above ψ_0, then $\chi(1) = e\psi(1)$, where, by Lemma 2, e divides m and d.

First we take $\psi_1 \in \mathrm{Irr}\, \overline{G}'$ such that $\psi_1(1) = 2^d$. If $\chi_1 \in \mathrm{Irr}\, \overline{G}$ is above ψ_1, then

$$2^f = \chi_1(1) = e_1\psi_1(1).$$

Hence $e_1 = 2^{f-d}$ divides d. If $f = sd > d$ is a proper multiple of d, we obtain the contradiction

$$d \geq 2^{f-d} = 2^{(s-1)d} \geq 2^d.$$

Hence d does not divide f. We also can take $\psi_2 \in \operatorname{Irr} \overline{G}'$ such that $\psi_2(1) = 2^d - 1$. If $\chi_2 \in \operatorname{Irr} \overline{G}$ is above ψ_2, we obtain

$$2^f \pm 1 = \chi_2(1) = e_2(2^d - 1).$$

As d does not divide f, so $2^d - 1$ does not divide $2^f - 1$, hence

$$2^f + 1 = e_2(2^d - 1).$$

As $d < f$, this implies

$$1 \equiv -e_2 \pmod{2^d},$$

hence $e_2 \geq 2^d - 1$. But then

$$d \geq e_2 \geq 2^d - 1,$$

a contradiction as $d \geq 2$. Hence

$$G'/M \cong \mathrm{SL}(2, 2^f).$$

Step 3. If $\vartheta \in \operatorname{Irr} M$, then $I_{G'}(\vartheta) = G'$ and hence $[M, G'] = M'$.
We put $I = I_{G'}(\vartheta)$. Then by Lemma 3, if

$$\vartheta^I = \sum_i \varphi_i, \quad \varphi_i \in \operatorname{Irr} I,$$

then

$$|G' : I|\varphi_i(1) \in \operatorname{cd} G'.$$

The maximal subgroups of $\mathrm{SL}(2, 2^f)$ are of index $2^f + 1$ or are dihedral groups of order $2(2^f \pm 1)$ or are groups $\mathrm{SL}(2, 2^d)$ for some divisor d of f (Huppert I, p. 213; observe that $\mathrm{SL}(2, 2^2) \cong A_5$ is in $\mathrm{SL}(2, 2^f)$ for even f and $\mathrm{PGL}(2, 2^f) \cong \mathrm{SL}(2, 2^f)$.) Observe that

$$\frac{|\,\mathrm{SL}(2, 2^f)|}{2(2^f \pm 1)} = 2^{f-1}(2^f \mp 1) \geq 3 \cdot 2^{f-1} > 2^f + 1.$$

If $f = s\,d$ and $s \geq 2$, then

$$\frac{(2^{sd} + 1)2^{sd}(2^{sd} - 1)}{(2^d + 1)2^d(2^d - 1)} > 2^{sd} + 1,$$

for

$$2^{sd}(2^{sd}-1) > \frac{2^{2sd}}{2} \geq 2^{3d} > 2^d(2^{2d}-1)$$

as

$$2sd \geq 4d \geq 3d+1.$$

Hence if $I < G'$, then $|G' : I| = 2^f + 1$. Then $\varphi_i(1) = 1$, so φ_i is an extension of ϑ to I. Then

$$(\varphi_i \tau)^{G'} \in \operatorname{Irr} G'$$

for all $\tau \in \operatorname{Irr} I/M$. The subgroups of PSL $(2, 2^f)$ of index $2^f + 1$ are Frobenius groups with a Frobenius kernel of order 2^f. Hence I/M has a character τ such that $\tau(1) = 2^f - 1$. Then

$$(2^f+1)(2^f-1) \in cd\, G'.$$

a contradiction.

Hence $I_{G'}(\vartheta) = G'$ for all $\vartheta \in \operatorname{Irr} M$. Then by Lemma 6 we obtain $[M, G'] = M'$.

Step 4.If $2^f > 4$, then $M = E$.

By Lemma 6, $|M/[M, G']|$ is bounded by the order of the Schur multiplier of $G'/M \cong \mathrm{SL}(2, 2^f)$. If $f \geq 3$, then

$$M = [M, G'] = M'$$

(see Huppert I, p. 645).

If $\vartheta \in \operatorname{Irr} M$, as G'/M has trivial Schur multiplier, so ϑ allows an extension ϑ_0 to G'. Then $\vartheta_0 \tau \in \operatorname{Irr} G'$ for all $\tau \in \operatorname{Irr} G'/M$. This forces $\vartheta(1) = 1$; therefore

$$E = M' = M.$$

Step 4′. If $2^f = 4$, then $M = E$.

Again, $|M/[M, G']|$ is bounded by the order of the Schur multiplier of $\mathrm{SL}(2, 4) \cong A_5$. Hence $|M/[M, G']| \leq 2$ (see Huppert I, p. 646).

If $|M/[M, G']| = 2$, then $G'/[M, G']$ is the uniquely determined Schur covering group of $G'/M \cong A_5$, so

$$G'/[M, G'] \cong \mathrm{SL}(2, 5)$$

(see Huppert I, p. 646). But SL(2, 5) has the degree 6, which does not divide any degree of G (Atlas, p. 2). Hence

$$M = [M, G'] = M'.$$

As the degrees of G' divide degrees of G, so

$$\operatorname{cd} G' \subseteq \{1, 2, 3, 4, 5\}.$$

If $\chi \in \operatorname{Irr} G'$, $\chi(1) > 1$ and $\chi_M \in \operatorname{Irr} M$, then by Lemma 3, $\chi\psi \in \operatorname{Irr} G'$ for all $\psi \in \operatorname{Irr} G'/M$. But this produces forbidden degrees $\chi(1)\psi(1)$, where $\psi(1) \in \{3, 4, 5\}$.

Hence the characters of G' of degree 3 or 5 split on M into linear characters while characters of degree 4 split on M into characters of degree 1 or 2. Therefore

$$\operatorname{cd} M \subseteq \{1, 2\}$$

and so $M'' = E$ (see Isaacs, p. 202). As $M = M'$, this implies $M = E$.

Step 5. $G = G' \times C_G(G')$, where $G' \cong \mathrm{SL}(2, 2^f)$ and $C_G(G')$ is abelian.

As $\operatorname{cd} G = \operatorname{cd} G'$, so G stabilizes all $\chi \in \operatorname{Irr} G'$, hence G stabilizes all conjugacy classes of G'. If $f = 2$, then the outer automorphisms of $\mathrm{SL}(2, 4) \cong A_5$ are induced by S_5 and interchange the two classes of elements of order 5 of A_5.

Suppose $f > 2$. Let α be an automorphism of $\mathrm{GF}(2^f)$ of prime order p. For $a \in \mathrm{GF}(2^f)^\times$ we put

$$M(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

If $M(a)^\alpha$ and $M(a)$ are conjugate, then

$$trace\, M(a)^\alpha = trace\, M(a) = a + a^{-1} \doteq b \in \mathrm{GF}(2^{f/p}).$$

If $a \neq 1$, then $b \neq 0$. So

$$a^2 + ab + 1 = 0.$$

The number of these a is at most

$$2|\,\mathrm{GF}(2^{f/p})^\times| = 2(2^{f/p} - 1)$$

and

$$2(2^{f/p} - 1) \leq 2(2^{f/2} - 1) < 2^f - 2$$

as $f > 2$. Hence G induces only inner automorphisms on G', which implies

$$G = G' \times C_G(G').$$

References

1. J. L. Alperin and D. Gorenstein, *The multiplicators of certain simple groups*, Proc. Amer. Math. Soc. **17** (1966), 515–519.
2. *Atlas of Finite Groups*. Clarendon Press, Oxford 1985.
3. N. Blackburn and B. Huppert, *Finite groups III*, Springer-Verlag, New York, 1982.
4. W. Feit, *The current situation in the theory of finite simple groups*, Actes du Congres International des Mathematiciens, 1970, pp. 55–93.
5. G. Glauberman, *Factorization of local subgroups of finite groups*, Conf. Board of the Math. Sciences Regional Conference, 1977.
6. B. Huppert, Endliche Gruppen I, Springer-Verlag, New York, 1967.

7. I. M. Isaacs, *Character theory of finite groups*, Academic Press, San Diego, 1976.
8. V. Landazuri and G. Seitz, *On the minimal degrees of projective representations of the finite Chevally groups*, J. Algebra **32** (1974), 418–433.
9. O, Manz, *Endliche nichtauflösbare Gruppen, deren sämtliche Charaktergrade Primzahlpotenzen sind.*, J. Algebra **96** (1985), 114–119.
10. G. Michler, *A finite simple group of Lie-type has p-blocks of different defects*, $p \neq 2$, J. Algebra **104** (1986), 220–230.
11. M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.
12. B. L. v. d. Waerden,*Gruppen von linearen Transformationen*, Springer-Verlag, New York, 1935.
13. W. Willems, *Blocks of defect* 0 *in finite simple groups of Lie-type*, J. Algebra **113** (1988), 511–522.