Correction to our paper "Finite primitive linear groups of prime degree" (J. London Math. Soc. (2) 57 (1998) 126–134)

J.D. Dixon and A.E. Zalesskii

September 4, 2007

Abstract

In our paper referred to above we claim to enumerate all finite primitive linear groups of prime degree r over $\mathbb{C}$ with a nonabelian socle. However, the case where the socle is imprimitive was overlooked. In the present paper we deal with this case to complete the classification.

2000 Mathematics Subject Classification: 20H20 20C15 20C33

In the paper referred to above, we state a theorem (Theorem 1.2) in which we claim to enumerate all finite primitive subgroups G of $\mathrm{SL}(r,\mathbb{C})$ with r prime for which $G/Z(G)$ has a nonabelian socle $M/Z(G)$. We are indebted to Professor Ziping Zhang (Peking University, Beijing) for pointing out that our classification fails to include the cases where G is primitive but M is imprimitive. In the present note we deal with this latter case.

Theorem 1 *Let r be prime. Suppose that there exists a finite primitive group $G \leq \mathrm{GL}(r,\mathbb{C})$ such that the socle $M/Z(G)$ of $G/Z(G)$ is nonabelian and M is imprimitive. Then the derived group G' is imprimitive and for some n and q we have $G' \cong \mathrm{PSL}(n,q)$ and $r = (q^n - 1)/(q-1) \geq 5$; moreover, if $n = 2$ then q is even, and if $n > 2$ then q is odd except in when $(n,q) = (3,2)$. Conversely, given any integer n and prime power q satisfying these side conditions, if $r = (q^n-1)/(q-1) \geq 5$ then there exists a finite primitive group $G \leq \mathrm{GL}(r,\mathbb{C})$ such that G' is imprimitive and isomorphic to $\mathrm{PSL}(n,q)$. (In the latter case the socle of $G/Z(G)$ contains $\mathrm{PSL}(n,q)$ as a composition factor and so is nonabelian.)*

Futher information, including other arithmetic restrictions on n and q and restrictions on the possible representations of $\mathrm{PSL}(n,q)$, can be deduced from the lemmas below. For example, n must always be a prime and r is a

Fermat prime when $n = 2$. In all cases $G/G'Z(G)$ is cyclic, and has order 2 when $n > 2$.

We first recall from Section 5.1 of [3] a number of properties of $S := \mathrm{PSL}(n, q)$ which hold when $r := (q^n - 1)/(q - 1) \geq 5$ is prime. First $S = \mathrm{SL}(n, q) = \mathrm{PGL}(n, q)$, and S has a single conjugacy class of subgroups of index r if $n = 2$ (the stabilizers of 1-dimensional subspaces) and has two conjugacy classes of subgroups of index r if $n > 2$ (the second class consists of the stabilizers of the $(n-1)$-dimensional subspaces). If $q = p^a$ where p is prime, then the Frobenius automorphism $\xi \mapsto \xi^p$ $(\xi \in \mathbb{F}_q)$ applied to the entries of the matrices in $\mathrm{SL}(n, q)$ induces an outer automorphism γ of S. The group $\Gamma := \langle \gamma \rangle$ has order a and $\Gamma \cong \mathrm{P\Gamma L}(n, q)/\mathrm{PGL}(n, q)$. Similarly, the inverse transpose $\tau : x \mapsto (x^{-1})^\top$ is an outer automorphism of S when $n > 2$. The full outer automorphism group of S is isomorphic to Γ when $n = 2$ and to $\Gamma \times \langle \tau \rangle$ when $n > 2$. If K is a subgroup of index r in S, then K is self-normalizing since r is prime and S is nonabelian simple. The automorphism γ maps K into itself, but (for $n > 2$) τ interchanges the two conjugacy classes of subgroups of index r. Thus for all $n \geq 2$, $\mathrm{Inn}_K(S)\Gamma \cong K \rtimes \Gamma$ is the full set of automorphisms of S which map K into itself where $\mathrm{Inn}_K(S)$ is the group of inner automorphisms of S induced by elements of K.

Assume that G is a finite primitive subgroup of $\mathrm{GL}(r, \mathbb{C})$ with r prime such that the socle $M/Z(G)$ of $G/Z(G)$ is nonabelian and M is imprimitive. Lemma 1.1 of [2] shows that $S := M/Z(G)$ is nonabelian simple and $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(S)$. Let H by the last term in the derived series for M, so $H/Z(H) \cong S$. Since H is nonabelian and r is prime, H must be irreducible and is imprimitive because M is. Recall that imprimitive implies irreducible so, since r is prime, a character of degree r is imprimitive if and only if it is an irreducible monomial character.

Lemma 2 *Under these hypotheses on G and H:*
*(a) $S \cong \mathrm{PSL}(n, q)$ with $r = (q^n - 1)/(q - 1) \geq 5$;*Inn
(b) $Z(H) = 1$ (so $H \cong S$); and
(c) $G/HZ(G)$ is cyclic and so $H = G'$.

Proof. (a) Since H is imprimitive, Proposition 1.1 of [3] shows that one of the following must hold: (i) $S = \mathrm{Alt}(r)$ with $r \geq 7$; (ii) $S = \mathrm{PSL}(n, q)$ and $r = (q^n - 1)/(q - 1) \geq 5$; or (iii) $(r, S) = (11, \mathrm{PSL}(2, 11)), (11, M_{11})$ or $(23, M_{23})$. Lemma 3.2 of [2] (and the remark which follows it) shows that $\mathrm{Alt}(k)$ has no imprimitive projective representation of prime degree when $k \geq 7$, so (i) cannot hold. On the other hand, M_{11} and M_{23} have trivial outer automorphism groups which would contradict $G \neq H$. Furthermore, a central cover of $\mathrm{PSL}(2,11)$ has only one irreducible character of degree 11, and that character has the centre in its kernel (see [1]). Since all subgroups of index 11 in $\mathrm{PSL}(2,11)$ are isomorphic to the simple group $\mathrm{Alt}(5)$, the character of degree 11 is not monomial. Thus it follows that (iii) does not hold and so (ii) must hold as claimed.

(b) The fact that $r = (q^n - 1)/(q-1)$ is prime implies that n is prime and $n \nmid q-1$. However, when $\mathrm{GCD}(n, q-1) = 1$, it is known (see, for example [1, page xvi]) that $PSL(n,q)$ ($= A_{n-1}(q)$) has a trivial Schur multiplier except when $(n,q) = (2,4), (3,2)$, or $(4,2)$. Since r is prime the only cases left to consider are $(n,q) = (2,4)$ and $(3,2)$. In both of these cases [1] shows that the unique irreducible character of degree r for a central cover of $\mathrm{PSL}(n,q)$ contains the centre of the central cover in its kernel. Since H is perfect, this shows that $Z(H) = 1$ in all cases.

(c) As we noted above, the full outer automorphism group $Out(S)$ of S is isomorphic to Γ when $n = 2$ and to $\Gamma \times \langle \tau \rangle$ when $n > 2$. Lemma 3.1 of [2] shows that the cyclic group Γ has order n^k for some k and that n is an odd prime when $n > 2$. Since τ has order 2, this shows that $Out(S)$ is cyclic in all cases. Since $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(S)$ and $S \cong H$ by (b), we conclude that $G/HZ(G)$ is cyclic and so $H = G'$. ∎

This lemma proves the first half of our theorem except for the condition that, if $n > 2$, then q is odd or $(n,q) = (3,2)$. It remains to prove these conditions and to prove existence of a suitable G when the $r = (q^n - 1)/(q-1)$ and the side conditions hold. Thus we consider the following situation:

(*) $S = \mathrm{PSL}(n,q)$ where $r := (q^n - 1)/(q-1) \geq 5$ is prime, K is one of the subgroups of index r in S, and S has an irreducible character $\theta := \lambda^S$ of degree r where λ is a linear character of K.

Note that for the isomorphic pairs $\mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4)$ and $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$ only the second group in each pair satisfies (*). When $S \neq \mathrm{PSL}(3,2)$ Lemma 5.3 of [3] shows that λ^S is irreducible if and only if $\lambda \neq 1_K$; the character table for $\mathrm{PSL}(3,2)$ (see, for example, [1]) shows that this is also true for $S = \mathrm{PSL}(3,2)$. Lemma 5.4 of [3] describes when the images of representations afforded by different monomial characters λ^S are conjugate in $\mathrm{GL}(r, \mathbb{C})$.

We also note that under hypothesis (*) when $n > 2$ we have $\varphi^\tau = \bar{\varphi}$ for every $\varphi \in Irr(S)$. In fact, $\mathrm{PSL}(n,q) = \mathrm{PGL}(n,q)$ because $n \nmid q-1$, and so we have $\mathrm{GL}(n,q) = \mathrm{SL}(n,q)Z$ where Z is the centre of $\mathrm{GL}(n,q)$. On the other hand, for any $x \in \mathrm{GL}(n,q)$, $x^\top$ is conjugate to x in $\mathrm{GL}(n,q)$ because the polynomial matrices $x - X1$ and $x^\top - X1$ have the same invariant factors. Thus $x^\top$ is conjugate to x in S for each $x \in S$ and so $\varphi^\tau(x) = \varphi((x^{-1})^\top) =$

$\varphi(x^{-1}) = \bar{\varphi}(x)$ as asserted.

We shall need the following simple number theoretic lemma.

Lemma 3 *Suppose we have integers $n \geq 2$, $0 \leq e < a$ and a prime p such that $(q^n - 1)/(q - 1)$ is prime for $q = p^a$.*

(a) If $n = 2$, then $p = 2$ and $\mathrm{GCD}(2^a - 1, 2^e + 1) = 2^{2^t} + 1$ *where 2^t is the largest power of 2 dividing e.*

(b) If $n > 2$, then $\mathrm{GCD}(p^a - 1, p^e + 1)$ *equals 1 if $p = 2$ and equals 2 if $p > 2$.*

Proof. As we noted above, n must be prime and $a = n^k$ for some integer $k \geq 1$. If $n = 2$ then $q + 1$ is prime and so $p = 2$. Write $e = 2^t c$ where c is odd, and put $d := \mathrm{GCD}(2^a - 1, 2^e + 1)$. Then there exist integers u, v with v odd such that $2^k u + 2^t cv = 2^t$. Since $2^a \equiv 1 \pmod{d}$ and $2^e \equiv -1 \pmod{d}$, we have $2^{2^t} \equiv 1^u (-1)^v = -1 \pmod{d}$. It is easily seen that $2^{2^t} + 1$ divides d, and so we conclude $d = 2^{2^t} + 1$. On the other hand, if $n > 2$ and $d := \mathrm{GCD}(p^a - 1, p^e + 1)$, then $1^e \equiv p^{ae} \equiv (-1)^a = -1 \pmod{d}$ because $a = n^k$ and n is an odd prime. Thus $d \mid 2$. It is now immediate that $d = 1$ if $p = 2$ and $d = 2$ if p is odd. ■

We now consider the following question: if (*) holds then under what conditions on n, q and λ does there exist a group T and a primitive character χ of T such that S $(= \mathrm{Inn}(S)) < T \leq \mathrm{Aut}(S)$ and $\chi_S = \theta$? We showed earlier that $Out(S)$ is cyclic and so T/S is cyclic. Thus, if such a character χ exists, and G_0 is the image of a representation of T affording χ, then any finite subgroup of $\mathrm{GL}(r, \mathbb{C})$ satisfying $G_0 \leq G < G_0 Z$ where Z is the group of scalar matrices has $G' \cong S$. Conversely, any group G satisfying the conditions of the first half of Theorem 1 can be constructed in this way. The proof of Theorem 1 is now completed by the following lemma.

Lemma 4 *Suppose that (*) holds where $q = p^a$ for a prime p. Then there exists a group T such that $S < T \leq \mathrm{Aut}(S)$ and a primitive character χ on T such that $\chi_S = \theta$ if and only if: (**) $\lambda \neq 1_K$ and the order of λ divides $p^e + 1$ for some integer e with $0 \leq e < a$.*

If $n = 2$ then there is always at least one, and generally several, linear characters λ satisfying (**). If $n > 2$ and $p > 2$ then the linear character λ of order 2 is the only character satisfying (**). Finally, if $n > 2$ and $p = 2$ then the only case in which some character $\lambda \neq 1_K$ satisfies (**) is when $(n, q) = (3, 2)$ (and again λ has order 2).

Proof. Among the groups $\mathrm{PSL}(n, q)$ which satisfy (*) the group $\mathrm{PSL}(3, 2)$ is exceptional in several ways (see Section 5.1 of [3]) and so it is convenient to deal with it separately. We shall deal with $\mathrm{PSL}(3,2)$ in the last paragraph of this proof, and until then assume that $(n,q) \neq (3,2)$.

When $S \neq \mathrm{PSL}(3,2)$ the group $Lin(K)$ of linear characters of K is isomorphic to the multiplicative group of the field $\mathbb{F}_q$ and so is cyclic of order $q-1 = p^a - 1$. Thus the second part of the statement of the lemma follows immediately from the first part and Lemma 3. We therefore consider the first part of the assertion in the lemma.

We now apply Lemma 5.3 of [3] which is valid for any group S satisfying (*) with the exception of $\mathrm{PSL}(3,2)$. This lemma states that if $\mu, \lambda \in Lin(K)$, then $\mu^S = \lambda^S$ if and only if $\mu = \lambda$ or λ^{-1} (for $n=2$) and $\mu = \lambda$ (for $n > 2$). Note that when $n = 2$ we have $\lambda \neq \lambda^{-1}$ because $Lin(K)$ is cyclic of order $q-1$ and (*) implies that $n \nmid q-1$. Frobenius reciprocity now shows that, for $n = 2$, the restriction θ_K has exactly two linear constituents, λ and λ^{-1}, each of multiplicity 1; and that θ_K has exactly one linear constituent λ, of multiplicity 1 for $n > 2$.

First suppose that a pair (T, χ) of the form referred to in the lemma exists and that $n = 2$. Since S has only one conjugacy class of subgroups of index r, the Frattini argument shows that $T = SN$ where $N := N_T(K)$. Since $S \cap N = K$, it follows that N has index r in T and $K \lhd N$. As we observed above, $\theta_K = \chi_K$ has exactly two linear constituents λ and λ^{-1}, each of multiplicity 1. Since $K \lhd N$, Clifford's theorem shows that χ_N either has two linear constituents whose restrictions to K are λ and λ^{-1}, respectively, or χ_N has a constituent η of degree 2 such that $\eta_K = \lambda + \lambda^{-1}$. The former situation cannot hold because it implies that χ is induced from a linear character on N contrary to the hypothesis that χ is primitive. Thus χ_N has a constituent η such that $\eta_K = \lambda + \lambda^{-1}$. Now Clifford's theorem shows that there exists $x \in N \setminus K$ such that $\lambda^x = \lambda^{-1}$. The automorphism of S induced by conjugation by x maps K into itself, and so lies in $\mathrm{Inn}_K(H)\Gamma$ as noted earlier. Since λ is a class function on K, this shows that $\lambda^x = \lambda^\sigma$ for some $\sigma \in \Gamma$. Thus, by the definition of Γ, $\lambda^{-1} = \lambda^x = \lambda^{p^e}$ for some e with $0 \leq e < a$ and so the order of λ divides $p^e + 1$ as asserted.

Next consider the case where such a pair (T, χ) exists and $n > 2$ (excluding $S = \mathrm{PSL}(3,2)$). Then S has two conjugacy classes $\mathcal{C}_1$ and $\mathcal{C}_2$, say, of subgroups of index r which are interchanged under the action of τ. Without loss in generality assume $K \in \mathcal{C}_1$ and so $K^\tau \in \mathcal{C}_2$. First suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ are not fused in T. As in the case $n = 2$, the Frattini argument shows that $T = SN$ where $N := N_T(K)$ has index r in T and $K \lhd N$. However, since $n > 2$, $\theta_K = \chi_K$ has λ as its unique linear constituent, and λ has multiplicity 1. Now Clifford's theorem shows that χ_N has a linear constituent lying over λ which implies that χ is induced from a linear character on N, contrary to the hypothesis that χ is primitive. Thus we conclude that T fuses the two classes and so there exists $x \in T$ which interchanges the two classes $\mathcal{C}_1$ and $\mathcal{C}_2$ by conjugation. Since K^τ and $x^{-1}Kx$ both lie in $\mathcal{C}_2$ we can find $u \in S$ such that $K^\tau = (xu)^{-1}K(xu)$. Thus if α is the automorphism of S induced by conjugation by the element xu from T, then $\alpha\tau \in \mathrm{Aut}(S)$ fixes K. As observed earlier, this means that $\alpha\tau \in \mathrm{Inn}_K(H)\sigma$ for some $\sigma \in \Gamma$. Since $\theta = \chi_S$ is invariant under T, we have $\theta^\alpha = \theta$, and so

$$(\lambda^{-1})^S = (\bar{\lambda})^S = \bar{\theta} = \theta^\tau = \theta^{\alpha\tau} = \theta^\sigma = (\lambda^\sigma)^S.$$

As noted above Lemma 5.3 of [3] now shows that $\lambda^{-1} = \lambda^\sigma$ because $n > 2$, and hence $\lambda^{-1} = \lambda^{p^e}$ for some e with $0 \le e < a$. Thus the order of λ divides p^e+1 in this case as well. In particular, since $Lin(K)$ is cyclic of order p^a-1, and $\lambda \neq 1_K$, Lemma 3 implies that in this case ($n > 2$ and $(n, q) \neq (3, 2)$) p is odd and λ has order 2.

We now assume that λ has order dividing $p^e + 1$ for some e (still excluding the case $(n, q) = (3, 2)$). We shall show that θ can be extended to a primitive character χ on a larger group $T \le \mathrm{Aut}(S)$. Choose $\sigma \in \Gamma$ as the automorphism of S induced by the field automorphism $\xi \mapsto \xi^{p^e}$. Since λ has order dividing $p^e + 1$, and the automorphism σ maps K into itself, $\lambda^\sigma = \lambda^{p^e} = \lambda^{-1}$. Hence $\theta^\sigma = (\lambda^\sigma)^S = (\lambda^{-1})^S = \bar{\theta}$ where $\bar{\theta} = \theta$ if $n = 2$ (by Lemma 5.3 of [3]) and $\bar{\theta} = \theta^\tau$ if $n > 2$. Define $T := S \rtimes \langle\sigma\rangle$ if $n = 2$, and $T := S \rtimes \langle\sigma\tau\rangle$ if $n > 2$. Since T/S is cyclic, the T-invariant character θ can be extended to a character χ on T (see [4, Corollary 11.22]). It remains to show that χ is primitive. Suppose the contrary. Then $\chi = \nu^T$ where ν is a nontrivial linear character of some subgroup L of index r in T. Since $r = (p^{an}-1)/(p^a-1) > 2a$, $\mathrm{GCD}(|T : L|, |T : S|) = 1$ and so $T = LS$. Thus $L \cap S$ has index r in S and $L \cap S \lhd L$. We now show that this leads to a contradiction in both cases: $n = 2$ and $n > 2$.

If $n = 2$ then S has only a single conjugacy class of subgroups of index r and so replacing L by a suitable conjugate we may assume $L \cap S = K \lhd L$. Since K is invariant under σ, a comparison of the orders shows that $L = K\langle\sigma\rangle$. As saw above K has exactly two linear characters λ and λ^{-1}, each of multiplicity 1, and $\lambda^\sigma = \lambda^{-1}$ by the choice of σ. Hence by Clifford's theorem χ_L has an irreducible constituent η, say, such that $\eta_K = \lambda + \lambda^{-1}$ and no linear constituent. This contradicts the choice of L and shows that χ is primitive when $n = 2$. On the other hand, if $n > 2$, then $K^{\sigma\tau} = K^\tau$ and so the two S-conjugacy classes $\mathcal{C}_1$ and $\mathcal{C}_2$ of subgroups of index r in S are fused in T. In particular, $|T : N_T(M)| = |\mathcal{C}_1 \cup \mathcal{C}_2| = 2r$ for each $M \in \mathcal{C}_1 \cup \mathcal{C}_2$. However $L \cap S \in \mathcal{C}_1 \cup \mathcal{C}_2$, and $L \cap S \lhd L$. This contradicts the hypothesis that L has index r in T. Thus in both cases we obtain a contradiction, and so conclude that χ is primitive as claimed. This completes the proof in all cases except when $S = \mathrm{PSL}(3,2)$.

Finally, consider $S = \mathrm{PSL}(3,2)$. Tables in [1] show that S has two conjugacy classes of subgroups of index r, consisting of subgroups isomorphic to Sym(4), and the two classes are fused in $\mathrm{Aut}(S) = S \rtimes \langle\tau\rangle$. Since $Out(S)$ has order 2, the only choice for T is $\mathrm{Aut}(S)$. The unique irreducible character θ of degree 7 for S is induced from the alternating character on K, and the tables in [1] show that θ has two extensions to $T := \mathrm{Aut}(S)$ both of which are primitive (see the argument for $n > 2$ in the preceding paragraph). This completes the proof of the lemma. ■

References

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

[2] J.D. Dixon and A.E. Zalesskii, Finite primitive linear groups of prime degree, J. London Math. Soc. (2) **57** (1998) 126–134.

[3] J.D. Dixon and A.E. Zalesski, Finite imprimitive linear groups of prime degree, J. Algebra **276** (2004) 340–370.

[4] I.M. Isaacs, "Character Theory of Finite Groups", Academic Press, New York, 1976.

John D. Dixon
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada
jdixon@math.carleton.ca

A.E. Zalesski
School of Mathematics
University of East Anglia
Norwich NR4 7TJ
U. K.
a.zalesskii@uea.ac.uk