PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 10, October 1996

CHARACTERIZATION OF CLASSICAL GROUPS BY ORBIT SIZES ON THE NATURAL MODULE

MARTIN W. LIEBECK

(Communicated by Ronald M. Solomon)

ABSTRACT. We show that if V is a finite vector space, and G is a subgroup of $P\Gamma L(V)$ having the same orbit sizes on 1-spaces as an orthogonal or unitary group on V, then, with a few exceptions, G is itself an orthogonal or unitary group on V.

Let C be a finite orthogonal or unitary group, with associated vector space V, and let G be a subgroup of $P\Gamma L(V)$ having the same orbit sizes as C on the set of 1-dimensional subspaces of V. We shall show that, with a few exceptions, under these hypotheses G must itself be an orthogonal or unitary group on V. The precise result is stated in the Theorem below.

This paper was written in response to a question of Prof. S. Abhyankar, who makes use of the result in [Ab].

Theorem. *Let q be a prime power, $d \geq 3$ an integer, and $V = V_d(q)$ a vector space of dimension d over $\mathbb{F}_q$. Suppose that G is a subgroup of $P\Gamma L_d(q)$ such that the sizes of the orbits of G on the 1-spaces of V are as in one of cases $(1)-(5)$ in Table 1 below. If $d \leq 7$, assume that $q > 2$; and if $d \leq 4$, assume that $q > 3$.*

(a) *If the orbit sizes are as in (4) or (5) of Table 1, then either $G \rhd PSU_d(q^{1/2})$, or $d = 3, q = 4, G \rhd 3^2 = O_3(PSU_3(2))$ (and if also $G \leq PGL_3(4)$, then $G \rhd PSU_3(2)$).*

(b) *If the sizes are as in (2), then either $G \rhd P\Omega_{2m}^+(q)$, or $G \rhd PSU_m(q)$ (m even), or $d = 8$, $G \rhd \Omega_7(q)$ (embedded irreducibly in $PSL_8(q)$), or $d = 4, q = 5, G \rhd A_6$.*

(c) *If the sizes are as in (3), then either $G \rhd P\Omega_{2m}^-(q)$, or $G \rhd PSU_m(q)$ (m odd), or $d = 4$, $G \rhd {}^2B_2(q)$ (q an odd power of 2), or $d = 6, q = 3, G \rhd L_3(4)$, or $d = 4, q = 4, G \leq \Gamma L_1(2^8)$.*

(d) *If the orbit sizes are as in (1) with q odd, then either $G \rhd \Omega_{2m+1}(q)$, or $d = 7, G \rhd G_2(q)$.*

(e) *If the orbit sizes are as in (1) with q even, then $G \rhd Sp_{2a}(q^b)$ ($2ab = 2m$) or $G \rhd G_2(q^b)$ ($6b = 2m$), embedded naturally in $Sp_{2m}(q)$ acting indecomposably on V (fixing a $2m$-dimensional subspace W, with V/W trivial).*

Conversely, all the groups arising in (a)-(e) do have orbit sizes as in Table 1.

Remarks. 1. The classical groups arising in conclusions (a)-(d) all act in the natural way on V.

Received by the editors March 20, 1995.
1991 *Mathematics Subject Classification.* Primary 20G40.

2. If we relax the assumptions in the Theorem made on q for small d, more examples occur, but it would not be hard to list these.

Table 1

Case	d	orbit sizes
(1)	$2m+1$	$\frac{q^{2m}-1}{q-1},\ \frac{1}{2}q^m(q^m+1),\ \frac{1}{2}q^m(q^m-1)$
(2)	$2m$	$\frac{(q^m-1)(q^{m-1}+1)}{q-1},\ q^{m-1}(q^m-1)$ or
		$\frac{(q^m-1)(q^{m-1}+1)}{q-1},\ \frac{1}{2}q^{m-1}(q^m-1),\ \frac{1}{2}q^{m-1}(q^m-1)$ (q odd)
(3)	$2m$	$\frac{(q^m+1)(q^{m-1}-1)}{q-1},\ q^{m-1}(q^m+1)$ or
		$\frac{(q^m+1)(q^{m-1}-1)}{q-1},\ \frac{1}{2}q^{m-1}(q^m+1),\ \frac{1}{2}q^{m-1}(q^m+1)$ (q odd)
(4)	$2m$	$\frac{(q^m-1)(q^{m-\frac{1}{2}}+1)}{q-1},\ \frac{q^{m-\frac{1}{2}}(q^m-1)}{q^{\frac{1}{2}}+1}$ (q square)
(5)	$2m+1$	$\frac{(q^{m+\frac{1}{2}}+1)(q^m-1)}{q-1},\ \frac{q^m(q^{m+\frac{1}{2}}+1)}{q^{\frac{1}{2}}+1}$ (q square)

In the proof we shall use *primitive prime divisors*: if $n \geq 3$ and $(q,n) \neq (2,6)$, then by [Zs] there is a prime which divides q^n-1 but does not divide q^i-1 for $1 \leq i \leq n-1$. Such a prime is called a primitive prime divisor of q^n-1 and is denoted by q_n; note that $q_n \equiv 1 \bmod n$. Write q_n^* for the product of all primitive prime divisors of q^n-1, counting multiplicities.

The proof of the Theorem is a fairly routine application of the results in [Li] and [GPPS]. The paper [Li] determines the irreducible subgroups of $P\Gamma L_d(q)$ having exactly two orbits on 1-spaces, and can be used to handle such cases in the Theorem. And [GPPS] lists subgroups of $P\Gamma L_d(q)$ which have order divisible by q_e for some $e > \frac{1}{2}d$; since our group G is in general divisible by such a prime, this applies to our problem. Despite the routine nature of the proof, we feel that the result may be of some interest, especially in view of the application [Ab].

Proof of the Theorem. Let $G \leq P\Gamma L_d(q)$ be as in the statement of the Theorem. Write $q = p^f$ with p prime. Assume first that $d \geq 5$, and also that $q > 2$ if $d \leq 8$; we shall handle the excluded cases later. Referring to Table 1, we see that $|G|$ is divisible by q_d^*, q_{d-1}^* or q_{d-2}^* in case (1), (2) or (3), and by $(q^{1/2})_{2d}^*$ or $(q^{1/2})_{2d-2}^*$ in case (4) or (5).

Suppose first that G is reducible on V. Then $G \leq P_i$, the stabilizer in $P\Gamma L(V)$ of an i-space, for some i. The orbit sizes of P_i on 1-spaces are $\frac{q^i-1}{q-1}$ and $\frac{q^i(q^{d-i}-1)}{q-1}$, so one of these is an orbit size of G. The only possibility is that $d = 2m+1, i = 2m$ and the orbit sizes of G are as in case (1) of Table 1. Thus $G \leq P_{2m} = QL$, where $Q \cong (\mathbf{F}_q)^{2m}$ is the unipotent radical and $L \triangleright SL_{2m}(q)$ is a Levi subgroup. The orbit sizes of P_{2m} are $\frac{q^{2m}-1}{q-1}, q^{2m}$; G is transitive on the first orbit, and Q is transitive on the second. Therefore $Q \not\leq G$. As G acts irreducibly on Q, it follows that $G \cap Q = 1$, whence G is isomorphic to a subgroup of L which is transitive on the 1-spaces of $V_{2m}(q)$. The list of all transitive linear groups is given in [Li, Appendix 1], and the only possibilities which are divisible by the orbit sizes in (1), hence by $\frac{1}{2}q^m(q^{2m}-1)/(q-1)$, are as follows:

(i) $G \leq \Gamma L_1(p^{2fm})$ (where $q = p^f$);

(ii) $G \rhd S = Sp_{2a}(q^b)$ (where $2ab = 2m$, $a \geq 1$);
(iii) $G \rhd S = SL_a(q^b)$ (where $ab = 2m$, $a \geq 3$);
(iv) $G \rhd S = G_2(q^b)$ (where $6b = 2m$, q even).

In case (i) the divisibility condition forces p^{fm} to divide $4fm$, whence $p = 2$, $fm = 4$; but the subgroup $G \cap GL_1(2^8)$, being of odd order, fixes a 1-space of V, so G has an orbit size dividing $|G : G \cap GL_1(2^8)|$, hence dividing 8, which is not the case.

In case (iii), or in case (ii) with q odd, we have $H^1(S, Q) = 0$ by [JP]. It follows that the subgroup S of G is conjugate to a subgroup of L, hence fixes a 1-space of V. But then G has an orbit of size dividing $|G : S|$, which is not so.

In the remaining cases ((ii) with q even, and (iv)), $H^1(S, Q)$ has dimension 1 by [JP]; by the argument of the previous paragraph, S does not fix a 1-space, so S is not conjugate to a subgroup of L. It follows that conclusion (e) of the Theorem holds. Here S lies in a subgroup $Sp_{2m}(q)$ acting indecomposably on V, with orbit sizes as in (1) of Table 1 and point stabilizers P_1 (a parabolic), $O^+_{2m}(q)$ and $O^-_{2m}(q)$. The group S is transitive on each of the orbits, since $Sp_{2m}(q)$ factorizes as $S.P_1 = S.O^+_{2m}(q) = S.O^-_{2m}(q)$ (see [LPS, Tables 1 and 2]).

Now assume that G is irreducible on V. Write $Z = Z(GL_d(q))$. Choose an integer b, maximal such that $G \leq \Gamma L_a(q^b)/Z$ $(ab = d)$ in its usual embedding in $P\Gamma L_d(q)$. If $a = 1$ then $|G|$ divides $(q^d - 1)df$ (where $q = p^f$), which is impossible since orbit sizes in Table 1 divide $|G|$. Hence $a \geq 2$.

The subgroups of $\Gamma L(V)$ having two orbits on 1-spaces, and their orbit sizes, are listed in [Li, Appendix 2]. A glance at this list shows that the only such groups having orbit sizes as in Table 1 satisfy conclusion (a), (b) or (c) of the Theorem. Thus we may assume that G has three orbits on 1-spaces; the orbit sizes are then as in (1), (2) or (3) of Table 1, with q odd in cases (2), (3). In particular, $|G|$ is divisible by q^*_e, where $e = d$, $d - 1$ or $d - 2$.

Let X be one of the classical groups $SL_a(q^b)$, $Sp_a(q^b)$, $\Omega_a(q^b)$, $U_a(q^{b/2})$, chosen to be minimal such that $G \leq N_{\Gamma L(V)}(X)/Z$. Write $\bar{X} = X/X \cap Z$. If G contains $\bar{X}$ then X must be orthogonal or unitary, and from the orbit sizes of X we see that $b = 1$ in the orthogonal case, $b = 1$ or 2 in the unitary case; hence G is as in (a)-(d) of the Theorem. Consequently we may assume that $\bar{X} \not\leq G$.

At this point we apply the main result of [As] on the subgroups of the classical group $N_{P\Gamma L(V)}(\bar{X})$. According to this result, either G lies in a member of one of the families $\mathcal{C}_1, \ldots, \mathcal{C}_8$ of subgroups of this group, or $G \in \mathcal{S}$, a certain collection of almost simple subgroups. A discussion of this result can be found in [KL, Chapter 1], and detailed descriptions of the members of the families $\mathcal{C}_i$ in [KL, Chapter 4].

Suppose first that $G \in \mathcal{C}_i$ for some i. As G is irreducible, and by choice of b and X, i is not 1, 3 or 8; also subgroups in $\mathcal{C}_i$ for $i = 4, 5, 7$ do not have order divisible by q^*_e. If $G \leq M \in \mathcal{C}_2$, then G stabilizes a decomposition $V = V_1 \oplus \ldots \oplus V_k$, where each V_i has $\mathbb{F}_q$-dimension r, $rk = d$ and $G \cap PGL(V) \leq (GL_r(q) \text{ wr } S_k)/Z$. As q^*_e divides $|G|$ and $e \geq d - 2 > d/2$, we must have $r = 1$, $k = d$ and $q^*_e = d - 1$ or d. But G has at least k orbits on 1-spaces, so this is impossible when $d \geq 5$. Finally, suppose that $G \leq M \in \mathcal{C}_6$. Then $|M \cap PGL(V)|$ divides $r^{2k}|Sp_{2k}(r)|$, where r is prime, $a = r^k$ and $r|q^b - 1$. Since q^*_e divides $|G|$, this means that $r = 2$, $a = d = 2^k$ and $q^*_e = 2^k \pm 1$ with $e = d$ or $d - 2$. A result of Hering [He, 3.9] determines all (q, e) such that $q^*_e = e + 1$, and this implies that $(q, e) = (3, 4), (3, 6)$ or $(5, 6)$. In the first case $d = 4$, contrary to assumption; in the second case $G \leq 2^6.Sp_6(2) < L_8(3)$, and the orbit sizes of $2^6.Sp_6(2)$ on 1-spaces are 720, 2560 by [Li, Appendix 2], neither of which is an orbit size of G; and in the last case the orbit sizes of G do not divide $2^6|Sp_6(2)|$.

It remains to deal with the case where $G \in \mathcal{S}$. Here G is almost simple; write $S = F^*(G)$. In [GPPS, Examples 2.6 - 2.9], all possibilities for subgroups in $\mathcal{S}$ which are divisible by a primitive prime divisor q_{ib}, $i > a/2$, are listed. Clearly $e = ib$ with $i > a/2$, so our group S is in this list.

Suppose first that S is of Lie type in characteristic p. Then S is given by [GPPS, Example 2.8]. The only possibilities with $|S|$ divisible by q_e^* ($e \geq d-2$) are $(S, d, e) = (L_2(q^3), 8, 6)$, $(\Omega_7(q), 8, 6)$, $(G_2(q)$ or ${}^2G_2(q), 7, 6)$ (q odd), $(G_2(q^2), 14, 12)$ (q odd), $(U_3(q), 8-\delta_{3,p}, 6)$ or $(U_3(q^2), 14, 12)$ ($p = 3$). Of these, the only cases where $|\operatorname{Aut} S|$ is divisible by the orbit sizes in Table 1 are $S = \Omega_7(q)$, $G_2(q)$, as in conclusions (b), (d) of the Theorem. In these cases S lies in $\Omega_8^+(q)$, $\Omega_7(q)$ respectively, and is transitive on each orbit of these groups on 1-spaces (see [LPS] again).

Now assume that S is alternating, sporadic, or of Lie type in p'-characteristic. From the lists in [GPPS, Examples 2.6, 2.7 and 2.9], we see that one of the following holds:

(i) there is only *one* primitive prime divisor of $q^e - 1$ dividing $|G|$, and this is equal to $e+1$ or $2e+1$; moreover, this prime divides $|G|$ to the first power only;

(ii) $S = L_2(s)$ with s prime, $d = (s \pm 1)/2$, $e = (s-1)/2$ and $q_e^* = (e+1)(2e+1)$.

Consequently q_e^* must be $e+1$, $2e+1$ or $(e+1)(2e+1)$. Hence the possibilities for (q, e) are given by [He, 3.9]. In case (ii), (q, e) is $(3, 18)$ or $(17, 6)$. But then either $S = L_2(37) < L_d(3)$ ($d = 18$ or 19), or $S = L_2(13) < L_d(17)$ ($d = 6$ or 7), and $|\operatorname{Aut} S|$ is not divisible by the orbit sizes. Therefore (i) holds, and the possibilities for q, e are as follows:

$$\begin{aligned} q = 2: &\quad e = 3, 4, 8, 10, 12, 18 \text{ or } 20 \\ q = 3: &\quad e = 4 \text{ or } 6 \\ q = 4: &\quad e = 3 \text{ or } 6 \\ q = 5: &\quad e = 6. \end{aligned}$$

Suppose that $q = 2$ or 4. Since we are assuming G to have three orbits on 1-spaces, we must have $d = 2m+1$ and $|G|$ divisible by the orbit sizes $\frac{q^{2m}-1}{q-1}$, $\frac{1}{2}q^m(q^m+1)$, $\frac{1}{2}q^m(q^m-1)$. (In particular, $e = 2m = d-1$.) From [GPPS], we see that the only possibilities for $S = F^*(G)$ satisfying these conditions are $S = PSp_4(5)$ or $PSp_6(3)$, with $q = 2, d = 13$. However, $PSp_4(5), PSp_6(3)$ are not subgroups of $L_{13}(2)$ by Lagrange's theorem.

Now let $q = 3$. Here $e = 4$ or 6, so $5 \leq d \leq 8$. If $d = 5$, the orbit sizes 40, 45, 36 divide $|G|$, and [GPPS] shows that $S = M_{11}$; however, $M_{11} < L_5(3)$ has only two orbits on 1-spaces, by [Li]. If $d = 6$ then the orbit sizes of G are 130, 117, 117 or 112, 126, 126, whence $|G|$ is divisible by either $3^2.5.13$ or $2^4.3^2.7$; now [GPPS] implies that S is $L_3(4), A_7$ or J_2. The first case is in conclusion (c) of the Theorem, and $L_3(4) < \Omega_6^-(3)$ is transitive on each $\Omega_6^-(3)$-orbit on 1-spaces (see [At, p. 52]). In the second case, $G = A_7$ or S_7 has orbit sizes 112, 126, 126; but A_7 and S_7 have no transitive actions of degree 112 (see [At, p.10]). Finally, $J_2 \not\leq L_6(3)$ by Lagrange's theorem. When $d = 7$, [GPPS] gives no possibilities for G of order divisible by the orbit sizes $2^2.7.13$, $2.3^3.7$, $3^3.13$. Now suppose $d = 8$. The orbit sizes imply that $|G|$ is divisible by either $2^5.3^3.5.7$ (case (2) of Table 1) or by 13.41 (case (3)). By [GPPS], the former holds, and $S = Sp_6(2), \Omega_8^+(2), A_9$ or $L_3(4)$. In the first three cases the 8-dimensional representation of S is uniquely determined (see the 3-modular character tables of these groups in [At2]), and embeds $S \le \Omega_8^+(2) < \Omega_8^+(3) < L_8(3)$. But in this representation, $\Omega_8^+(2)$ has an orbit of size 120 on 1-spaces (see [Li, p.505, case 3(e,f)]). Finally, if $S = L_3(4)$, one checks using [At, p.23] that the group G with $F^*(G) = S$ has no transitive action of degree $2^3.3^3.5$, which is one of the required orbit sizes.

Now suppose that $q = 5$. Then $e = 6$ and $6 \le d \le 8$. When $d = 6$, $|G|$ is divisible by either 13.31 (case (2) of Table 1) or $2^2.3^3.5^2.7$ (case (3)). By [GPPS], the latter holds, and $S = J_2$. But $J_2 < L_6(5)$ has only two orbits on 1-spaces, by [Li]. Finally, when $d = 7$ or 8, [GPPS] shows that there are no possibilities for S with $|G|$ divisible by the required orbit sizes.

This completes the proof of the Theorem under our initial assumption that $d \ge 5$ and that $q > 2$ if $d \le 8$. By the hypotheses of the Theorem, it remains to handle the cases $d = 3, 4$ with $q \ge 4$, and $d = 8, q = 2$. The argument given at the beginning of the proof of the Theorem (second paragraph) shows that if G is reducible then $d = 3$, q is even and $G \rhd Sp_2(q)$ as in conclusion (e). Thus we suppose that G is irreducible. In the case $d = 8, q = 2$, G has two orbits on 1-spaces, and we check that conclusion (b) or (c) holds using [Li]. Thus we suppose from now on that $d = 3$ or 4 and $q \ge 4$.

As in the proof above, we choose b maximal such that $G \le \Gamma L_a(q^b)/Z$, where $ab = d$. If $a = 1$ then the orbit sizes must divide $(q^d - 1).d \log_p q$, which implies that $d = 4$ and $q = 4, 8$ or 16 (and the orbit sizes are as in (3) of Table 1). The subgroups of $\Gamma L_1(q^d)$ having two orbits on nonzero vectors are given by [FK, §3], from which we see that an example arises if and only if $q = 4$, as in conclusion (c).

Hence we now assume that $a \ge 2$; and $(a, b) = (d, 1)$ or $(2, 2)$. Again choose a classical group X of dimension a over $\mathbf{F}_{q^b}$, minimal such that $G \le N_{\Gamma L(V)}(X)/Z$. If G contains $\bar{X} = X/X \cap Z$, then one of (a)-(d) of the Theorem holds, so assume $\bar{X} \not\le G$. Suppose that G is contained in a member M of one of the families $\mathcal{C}_i$ of subgroups of $N(\bar{X})$. Then $i \ne 1, 3, 4, 7, 8$ by choice of b and X. If $i = 2$ or 5 then the orbit sizes of M are not compatible with those of G. And if $M \in \mathcal{C}_6$, then $|G \cap L_d(q)|$ divides $2^4.3^3$ (if $d = 3$), or $2^8.3^2.5$ (if $d = 4$). The fact that $|G|$ is divisible by orbit sizes in Table 1 forces either $d = 3, q = 4$ or $d = 4, q = 5$. In the first case, $G \le 3^2.2S_4$ (see [At, p.23]) and G has orbit sizes 9,12 as in (5) of Table 1. Then clearly $G \rhd 3^2$, as in (a) of the Theorem; moreover, if also $G \le PGL_3(4)$, then $G \le 3^2.2A_4$, whence from the action on the orbits, G contains $3^2.Q_8 = PSU_3(2)$. Now consider $d = 4, q = 5$. Here $G \le 2^4.Sp_4(2)$ and the orbit sizes of G are 36, 60, 60 or 36, 120. By [Li], the group $2^4.Sp_4(2)$ has orbit sizes 60, 96. The normal subgroup 2^4 has 15 orbits of size 4 and 16 of size 6, both sets permuted transitively by the factor $Sp_4(2)$ (see [Li, 1.2]). Hence G cannot contain this 2^4, and so $G \cap 2^4 = 1$. Thus $G = A_6$ or S_6, as in conclusion (b) of the Theorem.

Thus G lies in the collection $\mathcal{S}$ of almost simple subgroups of $N_{P\Gamma L(V)}(\bar{X})$. Let $S = F^*(G)$. For $d \le 4$, the members of this collection are well known, and are among the following (see [Kl, Chapter 5]):

$$d = 3: \quad S = A_5, A_6 \text{ or } L_2(7)$$
$$d = 4: \quad S = A_5, A_6, A_7, L_2(7), U_4(2), L_3(4) \text{ or } L_2(q).$$

By [Li], the only possibility for G having two orbits is $d = 4, q = 5, S = A_6$, as in (b) of the Theorem. So assume that G has three orbits; these have sizes $q + 1$, $\frac{1}{2}q(q + 1), \frac{1}{2}q(q - 1)$, or $(q + 1)^2, \frac{1}{2}q(q^2 - 1), \frac{1}{2}q(q^2 - 1)$, or $q^2 + 1, \frac{1}{2}q(q^2 + 1)$, $\frac{1}{2}q(q^2 + 1)$. The only possibilities with $|\mathrm{Aut}\ S|$ divisible by orbit sizes are as follows:

$$d=3,\ q=4,\ S=A_5 \text{ or } A_6, \text{ and}$$
$$d=4,\ q=5,\ S=A_6 \text{ or } A_7.$$

In the case $d=3$, A_6 has orbit sizes 6,15 (see [Li]), and there is no irreducible A_5 in $L_3(4)$. And in the case $d=4$, A_6 has two orbits ([Li]) and there is no A_7 in $L_4(5)$.

This completes the proof of the Theorem.

References

[Ab] S. Abhyankar, "Again nice equations for nice groups", Proc. Amer. Math. Soc. **124** (1996), 3567–3576.

[As] M. Aschbacher, "On the maximal subgroups of the finite classical groups", *Invent. Math.* **76** (1984), 469-514. MR **86a:**20054

[At] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985. MR **88g:**20025

[FK] D.A. Foulser and M.J. Kallaher, "Solvable, flag-transitive, rank 3 collineation groups", *Geom. Ded.* **7** (1978), 111-130. MR **57:**12263

[GPPS] R. Guralnick, T. Penttila, C.E. Praeger and J. Saxl, "Linear groups with orders having certain primitive prime divisors", preprint, University of Western Australia, 1994.

[He] C. Hering, "Transitive linear groups and linear groups which contain irreducible subgroups of prime order", *Geom. Ded.* **2** (1974), 425-460. MR **49:**439

[At2] C. Jansen, K. Lux, R.A. Parker and R.A. Wilson, *Atlas of modular characters*, Oxford University Press, 1995.

[JP] W. Jones and B. Parshall, "On the 1–cohomology of finite groups of Lie type", *Proc. Conf. on Finite Groups*, eds. W. Scott and F. Gross, Academic Press, (1976). MR **53:**8272

[Kl] P.B. Kleidman, *The subgroup structure of some finite simple groups*, Ph.D. Thesis, University of Cambridge, 1987.

[KL] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990. MR **91g:**20001

[Li] M.W. Liebeck, "The affine permutation groups of rank three", *Proc. London Math. Soc.* **54** (1987), 477-516. MR **88m:**20004

[LPS] M.W. Liebeck, C.E. Praeger and J. Saxl, "The maximal factorizations of the finite simple groups and their automorphism groups", *Mem. Amer. Math. Soc.* **86**, No. 432 (1990), 1-151. MR **90k:**20048

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

Department of Mathematics, Imperial College, London SW7 2BZ, United Kingdom
E-mail address: m.liebeck@ic.ac.uk