OVERGROUPS OF CYCLIC SYLOW SUBGROUPS OF LINEAR GROUPS

JOHN BAMBERG AND TIM PENTTILA

Abstract. We use a theorem of Guralnick, Penttila, Praeger, and Saxl to classify the subgroups of the general linear group (of a finite dimensional vector space over a finite field) which are overgroups of a cyclic Sylow subgroup. In particular, our results provide the starting point for the classification of transitive m-systems; which include the transitive ovoids and spreads of finite polar spaces. We also use our results to prove a conjecture of Cameron and Liebler on irreducible collineation groups having equally many orbits on points and on lines.

1. Introduction

In 1999, Guralnick et al. [13] produced a classification of subgroups of finite linear groups having non-trivial intersection with a cyclic Sylow subgroup of that linear group. This result has been applied widely, for example, to number theory (Abhyankar [1]), computational group theory (Guralnick and Kantor [14], O'Brien [24]), permutation group theory (Baddeley and Praeger [2]), to maximal overgroups of Singer elements in classical groups (Bereczky [5]), but has as yet seen little application to geometry, a source of some disappointment to the second author, as that was the original motivation of his interest in such a result. While the Guralnick et al result is a powerful tool, it is unwieldy. Since the hypothesis is weak, the conclusion is long. Our purpose here is to produce tools purpose-built for easier application, by refining and delineating consequences of that result.

One target is the application to geometric objects under the hypothesis of transitivity. The cardinality of such objects are generically polynomials in the order of the underlying field, and often this means that the corresponding groups satisfy stronger hypotheses than that of the Guralnick et al. result; not only non-trivial intersection with but also containment of a cyclic Sylow subgroup of the full linear group, and indeed containment of any cyclic Sylow subgroup centralising the first. Our first theorem classifies such subgroups of linear groups – the hypotheses are less convoluted in terms of primitive parts dividing the order of the subgroup. The conclusions that result are much shorter, giving a tool that is far easier to wield. At the end of the paper, we apply this result to prove a conjecture of Cameron and Liebler from 1982, showing that any irreducible subgroup of a projective semilinear group in (algebraic) dimension at least four which has equally many orbits on lines and on points of the associated projective space, is transitive on lines and hence known.

The applications we consider in two sequel papers ([3] and [4]) involve geometric objects with size of the form $p^n + 1$ where p is the characteristic of the underlying field. (These objects are eggs of projective spaces; and ovoids, spreads, and m-systems of polar spaces.) Moreover, in the last three cases, the groups involved are subgroups of symplectic, orthogonal and unitary groups, and the cardinality is the *ovoid number* of the polar space. A further delineation of the possible subgroups in the symplectic and orthogonal cases appears as our second theorem. The hypotheses are again purely numerical: we have a subgroup of the similarity group of a non-degenerate form which has a subgroup of index dividing a particular polynomial in the field order. This weakening of the hypothesis to "dividing" allows the application of the results to projective semisimilarity groups. The third and fourth theorems deal with the unitary case, where the ovoid number is the successor of a power of the characteristic of the underlying field, but not the successor of a power of the field order, so a slightly different tack is taken. These sequel papers lead to a complete classification of transitive eggs, ovoids, m-systems and spreads, provided the group is not metacyclic (i.e., the objects are known or the group is dull, as Kantor put it in another context). Many partial results in these directions are subsumed in this work, most of which required similarly heavy use of group theory.

We would like to thank Michael Giudici for many fruitful and stimulating conversations. This work forms part of an Australian Research Council Discovery Grant, for which the first author was supported.

The authors hope that these examples will inspire others to find further geometric applications of these ideas.

An essential part of our approach is to use strong information concerning the order of a linear group. A prime number r dividing q^e-1 is a *primitive prime divisor* of q^e-1 if r does not divide q^i-1 for i smaller than e, or equivalently, q has order e modulo r. Zsigmondy proved in [28] that if q is an integer greater than 1, and if e is a positive integer such that q^e-1 has no primitive prime divisors, then $q^e=p^e=2^6$ or $e=2$. It turns out that primitive prime divisors play an important role in the behaviour of linear groups, since they tell us something about the irreducibility of the Sylow p-subgroups of linear groups. The result of Guralnick et al. is remarkably strong in that it essentially classifies those subgroups of $\mathrm{GL}_d(q)$ which have an element whose order is a primitive prime divisor of q^e-1 (and $d/2<e\leqslant d$). In many situations, such as when we have a linear group G acting transitively on q^n+1 points, we have stronger information than the existence of primitive prime divisors. A divisor r of q^e-1 that is coprime to each q^i-1 for $i<e$ is said to be a *primitive divisor*, and we call the largest primitive divisor $\Phi_e^*(q)$ of q^e-1 the *primitive part*. One should note that $\Phi_e^*(q)$ is strongly related to cyclotomy in that it is equal to the quotient of the cyclotomic number $\Phi_e(q)$ and $\gcd(e,\Phi_e(q))$ when $e>2$. Now $\Phi_e^*(q)$ is congruent to 1 modulo e, and in many cases, it is either equal to $e+1$ or $2e+1$. In this situation, we can use a result in Hering's 1974 paper [15] to determine the possible values of q and e, and we do so extensively in this paper.

In the next section, we list some definitions and notation that will be used throughout this paper. In particular, we use notation consistent with [13] and [19]. In Section 3, we state the two main theorems of this paper; Theorem 3.1 describes the subgroups of $\mathrm{GL}_d(p^f)$ divisible by the primitive part of $p^{ef}-1$ (where $d/2\leqslant e<d$) and Theorem 3.2 gives more information for subgroups of $\mathrm{GL}_d(p^f)$ which have a subgroup of index dividing $q^{e/2}+1$. In Sections 4 and 5, we give corollaries of our main results for classical groups. Sections 6 and 7 are on the proofs of our two main results, which are finally followed by Section 8 where we give an affirmative proof of Cameron and Liebler's conjecture.

2. Notation

Our notation for classical groups will be consistent with that used in [19] and [13]. Here is a table which gives a summary of the various symbols used for certain classical groups (see also [19, Table 2.1.B]).

Table 1. A summary of the notation used for classical groups.

Type	Semi-similarities	Similarities	Isometries	Isom. det. 1
Linear	$\Gamma\mathrm{L}$	GL	GL	SL
Unitary	$\Gamma\mathrm{U}$		GU	SU
Symplectic	$\Gamma\mathrm{Sp}$	GSp	Sp	Sp
Orthogonal	$\Gamma\mathrm{O}^\epsilon$	GO^ϵ	O^ϵ	SO^ϵ

Here ϵ denotes $+$, $-$, or $\circ$, and the unitary similarity group is precisely the unitary isometry group extended by the full group of scalars. We will also use $\Omega_d^\epsilon(q)$ for the index 2 subgroup of $\mathrm{SO}_d^\epsilon(q)$, and the prefix "P" will denote the associated projective representation.

We will use the notation $V_d(q)$ to denote a d-dimensional vector space over the field of order q. Throughout, if b is a divisor d, we will use $\Gamma\mathrm{L}_{d/b}^{\#}(q^b)$ to denote the stabiliser of the extension field structure of a vector space $V_{d/b}(q^b)$ on the vector space $V_d(q)$. That is $\Gamma\mathrm{L}_{d/b}^{\#}(q^b)=\mathrm{GL}_d(q)\cap\Gamma\mathrm{L}_{d/b}(q^b)$. We will also use the notation "$\overline{H}$" to be the quotient of the linear group H after factoring out by scalar matrices (it will be clear what the ambient dimension and field order is). We will be careful in this paper with our notation for unitary groups. So the projective general unitary group will be denoted $\mathrm{PGU}_d(q^2)$, where the field q^2 has been deliberately written as such to remind the reader that the objects of this group are also elements of $\mathrm{PGL}_d(q^2)$. The standard notation G' will be used for the derived subgroup of G, as well as $G^{(\infty)}$ for the terminating member of the derived series of G.

3. Statements of Main Theorems

The following theorem is a specialisation of [13, Main Theorem]. Note that if $\Phi_{ef}^*(p)$ is nontrivial and divides the order of a subgroup G of $\mathrm{GL}_d(q)$, then by definition, $|G|$ is divisible by a primitive prime

divisor of $p^{ef}-1$, which will in turn also be a primitive prime divisor of q^e-1. Hence we can apply [13, Main Theorem].

Theorem 3.1. *Let $q=p^f$ where p is a prime, let d and e be integers greater than 2 satisfying $d/2<e\leqslant d$. If a subgroup G of $\mathrm{GL}_d(q)$ has order divisible by $\Phi^*_{ef}(p)$, and $\Phi^*_{ef}(p)>1$, then one of the following occurs:*

Classical examples: *We have that G preserves a non-degenerate sesquilinear form on the vector space $V_d(q)$, and one of the following holds:*

(a) $\mathrm{SL}_d(q)\trianglelefteqslant G$;
(b) $\mathrm{Sp}_d(q)\trianglelefteqslant G$;
(c) *q is a square,* $\mathrm{SU}_d(q)\trianglelefteqslant G$, *and e is odd;*
(d) $\Omega^\epsilon_d(q)\trianglelefteqslant G$ *where $\epsilon=\pm$ for d even, and $\epsilon=\circ$ when dq odd.*

Reducible examples:

We have that G fixes a subspace or quotient space U of $V_d(q)$ and $\dim(U)=m\geqslant e$. So $G\leqslant q^{m(d-m)}\cdot(\mathrm{GL}_m(q)\times\mathrm{GL}_{d-m}(q))$ and $\Phi^*_{ef}(p)$ divides $|G^U|$.

Imprimitive examples:

Here $q=p$, $\Phi^*_e(p)=e+1$, and G preserves a direct sum decomposition $V=U_1\bigoplus\cdots\bigoplus U_d$ where each U_i has dimension 1. Moreover, $G\leqslant\mathrm{GL}_1(q)\wr S_d$ in product action, and G induces a primitive group on the factors $\{U_1,\ldots,U_d\}$. The possible values of q, e and d are listed in the table below.

q	e	d	q	e	d
2	4	$5,6,7$	3	4	$5,6,7$
2	10	$11,\ldots,19$	3	6	$7,\ldots,11$
2	12	$13,\ldots,23$	5	6	$7,\ldots,11$
2	18	$19,\ldots,35$			

Extension field examples:

Here we have that there is a divisor b of $\gcd(d,e)$, $b\neq1$, such that G preserves on $V_d(q)$ a field extension structure of a vector space $V_{d/b}(q^b)$. Therefore $G\leqslant\Gamma\mathrm{L}^\#_{d/b}(q^b)$ and we have two subcases according to whether $\Phi^*_{ef}(p)$ is coprime to b or not:

(a) *In this case, we have $q=p$, $\Phi^*_e(p)=b=d=e+1$, $G\leqslant\Gamma\mathrm{L}^\#_1(q^d)$, and $p^e=2^4$, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6.*
(b) *Here, we have that $\Phi^*_{ef}(p)$ is coprime to b. If G preserves a non-degenerate sesquilinear form f on $V_d(q)$, then it either preserves a form of the same type on $V_{d/b}(q^b)$, or $b=2$ and G preserves a form f' on $V_{d/2}(q^2)$ correspondingly:*

f'	f	comments
unitary	symplectic	q odd
unitary	orthogonal, type $(-)^{d/2}$	–
orthogonal, type $\circ$	orthogonal, all types	$qd/2$ odd, $e\leqslant d-2$

Moreover, $\Phi^*_{ef}(p)$ divides $|G\cap\mathrm{GL}_{d/b}(q^b)|$ and $G\cap\mathrm{GL}_{d/b}(q^b)$ satisfies the hypotheses of this theorem if we let d/b, e/b, and q^b play the roles of d, e, and q respectively.

Symplectic type examples:

Here $q=p$, $\Phi^*_e(p)=e+1$, and G normalises an extraspecial 2-group. Specifically, we have one of the following:

(a) *$p=3$, $e=d=4$, and $G\leqslant(2^{1+4}_-\cdot\mathrm{O}^-_4(2))\circ2$.*
(b) *$p=3$, $d=8$, $e=6$ and $G\leqslant(2^{1+6}_+\cdot\mathrm{O}^+_6(2))\circ2$.*
(c) *$p=5$, $d=8$, $e=6$ and either $G\leqslant((4\circ2^{1+6})\cdot\mathrm{Sp}_6(2))\circ4$ or $G\leqslant(2^{1+6}_+\cdot\mathrm{O}^+_6(2))\circ4$.*

Nearly simple case:

In this case, $S\leqslant\overline{G}\leqslant\mathrm{Aut}(S)$ where S is a finite nonabelian simple group. Let Z be the group of non-singular matrices of $\mathrm{GL}_d(q)$. We have four families in this case.

Alternating group case:
(a) Permutation module examples: Here $A_n\leqslant G\leqslant S_n\times Z$ and the vector space $V_d(q)$ can be identified with the fully deleted permutation module for S_n over $\mathrm{GF}(q)$. We have that d is $n-1$ or $n-2$ (according to whether p does not or does divide n respectively), $q=p$, $\Phi^*_e(p)=e+1$, and $p^e=2^4,2^{10},2^{12},2^{18},3^4,3^6,5^6$.

(b) Other examples: These examples do note arise from the action of A_n on its fully deleted permutation module. We have one of the following possibilities for d, e, and q:

n	d	e	q	$\Phi^*_{ef}(p)$	n	d	e	q	$\Phi^*_{ef}(p)$
10	8	6	5	7	7	8	6	5	7
9	8	6	3	7	7	4	4	7	25
9	8	6	5	7	7	4	3	2	7
8	8	6	3	7	7	4	4	2	5
8	8	6	5	7	7	4	3	9	7
8	4	3	2	7	7	4	3	25	7
8	4	4	2	5	7	3	3	25	7

Sporadic simple group case:

Here S is a sporadic simple group and one of the following holds:

G'	d	e	q	$\Phi^*_{ef}(p)$	G'	d	e	q	$\Phi^*_{ef}(p)$
M_{11}	5	4	3	5	$2 \cdot M_{22}$	10	10	2	11
M_{11}	10	10	2	11	M_{23}	11	10	2	11
M_{12}	10	10	2	11	M_{24}	11	10	2	11
$2 \cdot M_{12}$	6	4	3	5	J_1	20	18	2	19
M_{22}	10	10	2	11	$2 \cdot J_2$	6	6	5	7
$3 \cdot M_{22}$	6	5	4	11	$3 \cdot J_3$	9	9	4	19

Cross-characteristic case:

We have one of the following:

S	d	e	q	$\Phi^*_{ef}(p)$	S	d	e	q	$\Phi^*_{ef}(p)$	S	d	e	q	$\Phi^*_{ef}(p)$
$\mathrm{PSL}_2(7)$	6,7	6	3	7	$\mathrm{PSL}_2(13)$	6	6	4	13	$\mathrm{PSL}_3(4)$	8	6	5	7
	6,7,8	6	5	7	$\mathrm{PSL}_2(17)$	8	8	2	17	$\mathrm{PSU}_3(3^2)$	6,7	6	5	7
	3	3	2	7	$\mathrm{PSL}_2(19)$	9	9	4	19	$\mathrm{P}\Omega^+_8(2)$	8	6	3	7
	3,4	3	9	7		20	18	2	19		8	6	5	7
	3,4	3	25	7	$\mathrm{PSL}_2(23)$	11	10	2	11	$\mathrm{Sp}_6(2)$	7	4	3	5
$\mathrm{PSL}_2(8)$	7	6	3	7	$\mathrm{PSL}_2(25)$	12	12	2	13		7,8	6	3	7
	7,8	6	5	7	$\mathrm{PSL}_2(37)$	18	18	2	19		7,8	6	5	7
$\mathrm{PSL}_2(9)$	4	4	2	5	$\mathrm{PSL}_2(41)$	20	20	2	41	$\mathrm{PSp}_4(5)$	12	12	2	13
$\mathrm{PSL}_2(11)$	10	10	2	11	$\mathrm{PSL}_3(3)$	12	12	2	13	$\mathrm{Sz}(8)$	8	6	5	7
	5	5	4	11	$\mathrm{PSL}_3(4)$	4	3	9	7	$G_2(3)$	14	12	2	13
$\mathrm{PSL}_2(13)$	14	12	2	13		6	4	3	5					
	6,7	6	3	7		6	6	3	7					

Natural-characteristic case:

One of the following occurs:

$G^{(\infty)}$	d	e	*Conditions*	$G^{(\infty)}$	d	e	*Conditions*
$\mathrm{SL}_2(q^3)$	8	6	–	$\mathrm{PSU}_3(q^2)$	8	6	$p \neq 3$
$\mathrm{SL}_3(q^2)$	9	6	$q \equiv 1 \pmod 3$		7	6	$p = 3$
$\mathrm{PSL}_3(q^2)$	9	6	$q \neq 1 \pmod 3$	$\mathrm{Sz}(\sqrt{q})$	4	4	$p = 2$, f *even*
$2 \cdot \Omega_7(q)$	8	6	p *odd*	$\mathrm{Sz}(q)$	4	4	$p = 2$
$\mathrm{Sp}_6(q)$	8	6	$p = 2$	${}^2G_2(\sqrt{q})$	7	6	$p = 3$, f *even*
$G_2(q)$	7	6	p *odd*	${}^2G_2(q)$	7	6	$p = 3$
	6	6	$p = 2$				

As mentioned in the introduction, in geometric applications such as in studying transitive m-systems or transitive eggs of finite polar spaces, one is interested in linear groups which have a subgroup whose index divides the successor of a power of the field order. In particular, if G is a group of collineations acting transitively on an m-system or egg, then we have that $G \cap \mathrm{PGL}_d(q)$ has a subgroup, namely $H \cap \mathrm{PGL}_d(q)$ of index $(q^{e/2}+1)/x$ where e is some positive integer and x is coprime to $\Phi^*_e(q)$. It turns out that we can determine the structure of G and H in great detail.

Theorem 3.2. *Let q be a power of a prime p, let d and e be integers greater than 2 satisfying $d-2 \leqslant e \leqslant d$ and suppose e is even. If a subgroup G of $\mathrm{GL}_d(q)$ has a subgroup H of index $(q^{e/2}+1)/x$ where x is coprime to $\Phi^*_e(q)$ and $(q,e) \neq (2,6)$, then one of the following occurs:*

Classical examples: *We have that $d = e = 4$, $x = 1$, and $\Omega^-_4(q) \trianglelefteq G$.*

Reducible examples: *Here, $e = d-2, d-1$. We have that G fixes a subspace or quotient space U of $V_d(q)$ and $\dim(U) = m \geqslant e$. So $G \leqslant q^{m(d-m)} \cdot (\mathrm{GL}_m(q) \times \mathrm{GL}_{d-m}(q))$, $\Phi^*_e(q)$ divides $|G^U|$, and G^U has a subgroup of index $(q^{e/2}+1)/y$, with $\Phi^*_e(q)$ coprime to y. Hence G^U satisfies the hypotheses of this theorem if we substitute m for d in the hypothesis.*

Imprimitive examples: *Here G preserves a direct sum decomposition $V = U_1 \bigoplus \cdots \bigoplus U_d$ where each U_i has dimension 1. Moreover, G is a subgroup of $\mathrm{GL}_1(q) \wr S_d$ in product action, and G induces a primitive group on the factors $\{U_1, \ldots, U_d\}$. Finally, either*

$$(q,e,d) \in \{(3,4,5),(3,4,6),(3,6,7),(3,6,8),(5,6,7),(5,6,8)\}$$

or $q = 2$, $e = 4$, $x = 1$, and G has a unique transitive action on 5 points.

Extension field examples:

Here we have that there is a non-trivial divisor b of $\gcd(d, e)$ such that G preserves on $V_d(q)$ a field extension structure of a vector space $V_{d/b}(q^b)$. Therefore $G \leqslant \Gamma\mathrm{L}^{\#}_{d/b}(q^b)$ and we have two subcases:

(a) *In this case, $b = d = 5$, $e = 4$, $q = p \in \{2, 3\}$, and $G \leqslant \Gamma\mathrm{L}^{\#}_1(q^5)$. Furthermore, if $p = 2$, then $x = 1$, and if $p = 3$, we have $x = 1, 2$.*
(b) *If G preserves a non-degenerate sesquilinear form f on $V_d(q)$, then it either preserves a form of the same type on $V_{d/b}(q^b)$, or $b = 2$ and G preserves a form f' on $V_{d/2}(q^2)$ correspondingly:*

f'	f	*comments*
unitary	*symplectic*	*q odd*
unitary	*orthogonal, type $(-)^{d/2}$*	–
orthogonal, type $\circ$	*orthogonal, all types*	*$qd/2$ odd, $e = d - 2$*

Moreover, $G \cap \mathrm{GL}_{d/b}(q^b)$ has a subgroup of index $(q^{e/2} + 1)/x'$ where x' is coprime to $\Phi^*_{e/b}(q^b)$. So $G \cap \mathrm{GL}_{d/b}(q^b)$ satisfies the hypotheses of this theorem if we let d/b, e/b, and q^b play the roles of d, e, and q respectively.

Symplectic type examples:

Here $q = p$, $\Phi^*_e(p) = e + 1$, and G normalises an extraspecial 2-group. Specifically, we have one of the following:

(a) *$p = 3$, $e = d = 4$, and $G \leqslant (2^{1+4}_- \cdot \mathrm{O}^-_4(2)) \circ 2$. Moreover, G is cyclic of order 10 and H is its trivial subgroup.*
(b) *$p = 3$, $d = 8$, $e = 6$ and $G \leqslant (2^{1+6}_+ \cdot \mathrm{O}^+_6(2)) \circ 2$.*
(c) *$p = 5$, $d = 8$, $e = 6$ and either $G \leqslant ((4 \circ 2^{1+6}) \cdot \mathrm{Sp}_6(2)) \circ 4$ or $G \leqslant (2^{1+6}_+ \cdot \mathrm{O}^+_6(2)) \circ 4$.*

Nearly simple case:

We have in this case, $S \leqslant \overline{G} \leqslant \mathrm{Aut}(S)$ where S is a finite nonabelian simple group.

Alternating group case:

(a) Permutation module examples: Here $A_n \leqslant G \leqslant S_n \times Z$ and the vector space $V_d(q)$ can be identified with the fully deleted permutation module for S_n over $\mathrm{GF}(q)$. We have that d is $n-1$ or $n-2$ (according to whether p does not or does divide n respectively), $q = p$, and $p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$. Moreover, the table below lists all possibilities for $\overline{G}$ and $\overline{H}$ with $n < 9$. The number of times an isomorphism type of a group appears in a row for the $\overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $\overline{H}$ in $\overline{G}$.

p^e	d	n	$\overline{G}$	$\overline{H}$
2^4	4	5	S_5	S_4
			A_5	A_4
3^4	4	5	S_5	D_{12}, A_4, S_4
			A_5	S_3, A_4
		6	S_6	$S_3 \wr S_2$
			A_6	$3^2 : 4$
3^6	6	7	S_7	A_6, S_6
			A_7	A_6
5^6	6	7	S_7	$(5 : 4) \times 2$, S_5, S_5, S_5, $A_5 \times 2$, A_6, $S_5 \times 2$, S_6
			A_7	$5 : 4$, A_5, A_5, S_5, A_6

If $n \geqslant 9$, then one of the following holds:

(i) *$p^e = 5^6$, $d = 8$, $n = 9$, and G has a unique transitive action on 126 points where H is the stabiliser in the action on 5-subsets;*
(ii) *$p^e = 5^6$, $d = 8$, $n = 10$, and G has a unique transitive action on 126 points where H is the stabiliser of a partition of a set of size 10 into 2 sets of size 5;*
(iii) *$p^e = 2^{10}, 2^{12}, 2^{18}$, $n = \Phi^*_e(p) = e + 1$, and G has a unique transitive action on $|G : H|$ elements.*

(b) Other examples: We have that $d = 8$, $e = 6$, $q = p$, $A_n \leqslant \overline{G} \leqslant S_n$ and $(n, p) \in \{(10, 5), (9, 5), (8, 3), (7, 5)\}$. The number of times an isomorphism type of a group appears in a row for the $\overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $\overline{H}$ in $\overline{G}$. We have the following data in each case:

n	x	$\overline{H}$ *for* $\overline{G} = A_n$	$\overline{H}$ *for* $\overline{G} = S_n$
10	1	$(A_5 \times A_5) \cdot 2^2$	$S_5 \wr S_2$
9	1	$(A_5 \times A_4) \cdot 2$	$S_5 \times S_4$
8	1	S_6	$S_6 \times 2$
7	1	$\mathbb{Z}_5 : \mathbb{Z}_4$	$(\mathbb{Z}_5 : \mathbb{Z}_4) \times 2$
	3	$A_5,\ A_5$	$A_5 \times 2,\ S_5,\ S_5,\ S_5$
	6	S_5	$S_5 \times 2$
	9	–	A_6
	18	S_6	S_6

Cross-characteristic case: The table below lists the possibilities for this case. The number of times an isomorphism type of a group appears in a row for the $S \cap \overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $S \cap \overline{H}$ in S.

S	e	q	d	x	$S \cap \overline{H}$	S	e	q	d	x	$S \cap \overline{H}$
$\mathrm{PSL}_2(7)$,$\mathrm{PSL}_3(2)$	6	3	6,7	1	S_3	$\mathrm{PSL}_2(19)$	18	2	20	3	D_{20}
				2	$A_4,\ A_4,\ D_{12},\ D_{12}$					9	A_5, A_5
				4	$S_4,\ S_4$		9	4	9	3	D_{20}
		5	6,7,8	3	$2^2,\ 2^2,\ 4$					9	A_5, A_5
				6	D_8	$\mathrm{PSL}_2(25)$	12	2	12	1	$S_5,\ S_5$
				9	$A_4,\ A_4$	$\mathrm{PSL}_3(3)$	12	2	12	5	$3^2 : 2 \cdot S_4,\ 3^2 : 2 \cdot S_4$
				18	$S_4,\ S_4$	$\mathrm{PSL}_3(4)$	6	5	8	1	$2^4 : D_{10},\ 2^4 : D_{10}$
$\mathrm{PSL}_2(8)$	6	3	7	1	$9 : 2$					6	$2^4 : A_5,\ 2^4 : A_5$
		5	7,8	1	2^2	$\mathrm{PSU}_3(3^2)$	6	5	6,7	1	$4 \cdot A_4,\ 4^2 \cdot A_3$
				2	2^3					2	$4 \cdot S_4,\ 4^2 \cdot S_3$
$\mathrm{PSL}_2(11)$	10	2	10	3	$A_5,\ A_5$	$\mathrm{Sp}_6(2)$	6	5	7,8	1	$2^5 : A_6$
$\mathrm{PSL}_2(13)$	6	3	6,7	1	$13 : 3$					2	$2^5 : S_6$
				2	$13 : 6$			3	7,8	1	$\mathrm{PSU}_4(2^2) : 2$

Natural-characteristic case: Here we have that $x = 1$ and $\overline{G}$ has a unique conjugacy class of subgroups of index $q^{e/2}+1$. We also have that $\overline{G}$ acts 2-transitively of degree $q^{e/2}+1$ and we have one of the following:

S	d	e	q	S	d	e	q
$\mathrm{PSL}_2(q^3)$	8	6	–	$\mathrm{Sz}(q)$	4	4	2^f
$\mathrm{PSU}_3(q^2)$	7	6	3	${}^2G_2(q)$	7	6	$3^f,\ f > 1$
	8	6	$\neq 3$				

4. The Hermitian Case

For most of our geometric applications, we are interested in when a linear group G of $\mathrm{GL}_d(q)$ acts transitively on an object which has size of the form $q^{e/2} + 1$ where e is an even integer. As mentioned in the introduction, we deal with unitary groups separately as the object size we are interested in here is not of the form $q^{e/2} + 1$ where e is an even integer. In the case that G is a subgroup of $\mathrm{GU}_d(q^2)$ and d is even, we are interested in objects of size $q^{d-1} + 1$. If d is odd, this size is then $q^d + 1$. Note that our group G is defined over a field of order p^{2f}, and we have that $\Phi^*_{2ef}(p)$ divides $|G|$, where e is d or $d-1$ according to whether d is odd or even respectively. Hence we can apply Theorem 3.1.

Theorem 4.1 (Odd dimension)**.**
Let p be a prime, let $q = p^f$, and let d be an odd integer greater than 1. If a subgroup G of $\mathrm{GU}_d(q^2)$ has order divisible by $\Phi^*_{2df}(p)$, and $(p, df) \neq (2, 3)$, then we have one of the following:

(a) $\mathrm{SU}_d(q^2) \trianglelefteq G$.
(b) $d = 3$, $q = 5$, *and* $A_7 \leqslant \overline{G} \leqslant S_7$.
(c) $G \leqslant \Gamma\mathrm{U}_1(q^{2d})$.

Proof. Most cases drop out of Theorem 3.1 because of the restriction that d is odd, $d = e$, and our group G is defined over a field of square order. For the Classical examples we have only two cases to deal with. The first is when $\mathrm{SL}_d(q^2) \trianglelefteq G$. This implies that $|\mathrm{SL}_d(q^2)|$ divides $|\mathrm{GU}_d(q^2)|$ and so

$$((q^2)^3 - 1)((q^2)^5 - 1) \cdots ((q^2)^d - 1)$$

divides

$$((q^2)^3 + 1)((q^2)^5 + 1) \cdots ((q^2)^d + 1).$$

This is impossible for all $d \geqslant 3$, and therefore this case does not arise. The second is when d is odd and $\mathrm{SU}_d(q^2) \trianglelefteq G$. This case does arise.

There is one example in the Nearly Simple case to consider. It appears in the Alternating Group case, where $n = 7$, $d = e = 3$, $q^2 = 25$, and $A_7 \leqslant \overline{G} \leqslant S_7$. The only other case remaining is the Extension field case, which gives us the third of the possibilities listed above. □

Theorem 4.2 (Even dimension)**.**
Let p be a prime, let $q = p^f$, and let d be an even integer greater than 2. If a subgroup G of $\mathrm{GU}_d(q^2)$ has order divisible by $\Phi^*_{2(d-1)f}(p)$, and $(p,(d-1)f) \neq (2,3)$, then we have one of the following:

(a) *Here we have $d = 4$ and one of the following*
  (i) *$G' = 4 \cdot \mathrm{PSL}_3(4)$, $q = 3$, and $\mathrm{PSL}_3(4) \leqslant \overline{G} \leqslant \mathrm{Aut}(\mathrm{PSL}_3(4))$;*
  (ii) *$\mathrm{PSL}_2(7) \leqslant G$ and $q = 3$;*
  (iii) *$\mathrm{PSL}_2(7) \leqslant G$ and $q = 5$.*

(b) *G fixes a subspace or quotient space U of $V_d(q^2)$ of dimension $d-1$. So $G \leqslant q^{2(d-1)} \cdot (\mathrm{GU}_{d-1}(q^2) \times \mathrm{GU}_1(q^2))$ and $\Phi^*_{2(d-1)f}(p)$ divides $|G^U|$. Moreover, one of the following occurs:*
  (i) *$\mathrm{SU}_{d-1}(q^2) \trianglelefteq G^U$.*
  (ii) *$d = 4$, $q = 5$, and $A_7 \leqslant \overline{G^U} \leqslant S_7$ (note that $G^U \leqslant \mathrm{GU}_3(25)$).*
  (iii) *$G^U \leqslant \Gamma\mathrm{U}_1(q^{2(d-1)})$.*

Proof. Most cases drop out of Theorem 3.1 because of the restriction that d is even, $d = e + 1$ (in many of the cases, $e+1$ is prime and so $d = 2$; a contradiction), and our linear group G is defined over a square field q^2. By [19, pp. 165] the Classical examples cannot arise.

There are three examples in the Nearly Simple case to consider. They appear in the Cross-characteristic case:

(i) $G' = 4 \cdot \mathrm{PSL}_3(4)$, $d = 4$, and $q^2 = 9$ (we refer to [13] for the extra information present here);
(ii) $\mathrm{PSL}_2(7) \leqslant G$, $d = 4$, $q^2 = 9$;
(iii) $\mathrm{PSL}_2(7) \leqslant G$, $d = 4$, $q^2 = 25$.

All that is left are the Reducible examples. Note that $G^U \leqslant \mathrm{GU}_{d-1}(q^2)$ and G^U is irreducible. Therefore, the remainder follows from Theorem 4.1. □

5. The Non-Hermitian case

Before we analyse symplectic and orthogonal groups which have a subgroup of index dividing $q^{e/2}+1$, we first present a lemma which deals with the two-dimensional semilinear groups, which we will use in the proofs of later results.

Lemma 5.1. *Let d be an even integer greater than 2, and suppose $G \leqslant \Gamma\mathrm{L}_2(q^{d/2})$ and that G is not a one-dimensional semilinear group. If $\Phi^*_d(q)$ divides $|G|$, then G contains $\mathrm{SL}_2(q^{d/2})$, or $\overline{G} \cap \mathrm{PGL}_2(q^{d/2}) \cong A_5$ and $(q,d) \in \{(2,4),(2,6),(3,4)\}$.*

Proof. Let G^* be the image of $G \cap \mathrm{GL}_2(q^{d/2})$ in $\mathrm{PGL}_2(q^2)$ and let Z be the subgroup of scalar matrices in $\mathrm{GL}_2(q^{d/2})$. Note that

$$|G| = |G^*||G \cap Z||G \cdot \mathrm{GL}_2(q^{d/2}) : \mathrm{GL}_2(q^{d/2})|.$$

Since $\Phi^*_d(q)$ is coprime to $q-1$, it is also coprime to $|G \cap Z|$. Also, since $\Phi^*_d(q)$ is coprime to f (by Fermat's Little Theorem), we have that $\Phi^*_d(q)$ is coprime to $|G \cdot \mathrm{GL}_2(q^{d/2}) : \mathrm{GL}_2(q^{d/2})|$. Hence $\Phi^*_d(q)$ divides $|G^*|$. Now we can derive candidates for G^* by using the list of subgroups of $\mathrm{PGL}_2(p^m)$ given in [27]:

Subgroup	order
Elementary abelian	p^f, $f \leqslant m$
Cyclic group	n, where n divides $p^m \pm 1$
Dihedral group	$2n$, where n divides $p^m \pm 1$
(Elem. abelian) $\rtimes$ (Cyclic group)	$p^f \cdot n$, where $f \leqslant m$, and n divides $p^f - 1$ and $p^m - 1$
A_4	12
S_4	24
A_5	60
$\mathrm{PSL}_2(p^f)$, with $f \mid m$	$p^f(p^f-1)/2$
$\mathrm{PGL}_2(p^f)$, with $f \mid m$	$(p^f-1,2)p^f(p^f-1)/2$

Since the primitive part of $q^d - 1$ divides $|G^*|$, and G^* is not one-dimensional semilinear (contained in D_{2n} where $n = q^{d/2}+1$), we are left with the following candidates for G^*:

G^*	order
A_5	60
$\mathrm{PSL}_2(q^{d/2})$	$q^{d/2}(q^{d/2}-1)/2$
$\mathrm{PGL}_2(q^{d/2})$	$(q^{d/2}-1,2)q^{d/2}(q^{d/2}-1)/2$

Now suppose $\Phi_d^*(q)$ divides 60. If r is primitive prime divisor of q^d-1, then r is 2, 3, or 5, and r is congruent to 1 modulo d. Hence $r=5$, and in fact $\Phi_d^*(q)=5$ as no power of 5 divides 60. Since $d\geqslant 4$, we have that $\Phi_d^*(q)<2d+1$ and therefore $\Phi_d^*(q)=1$ or $\Phi_d^*(q)=d+1$. It follows from a result of Hering (see [15, Theorem 3.9] or Lemma 6.1) that $\Phi_d^*(q)$ divides 60 only when $(q,d)\in\{(2,4),(2,6),(3,4)\}$. □

Before we begin to apply Theorem 3.2 to classical groups, we make the following observation which makes our approach valid. Let r be a primitive prime divisor of $p^{ef}-1$ with r dividing f. Then $ef=mr$ for some positive integer m, and so r divides $(p^m)^r-1$. By Fermat's Little Theorem, this implies that r divides p^m-1, which contradicts the fact that r is a primitive prime divisor. So $\Phi_e^*(q)$ is coprime to f. In this section, each of our results have the hypothesis that a group G has a subgroup of index $(q^{e/2}+1)/x$, where x is a divisor of f. Since x is coprime to $\Phi_e^*(q)$, we can apply Theorem 3.2.

Corollary 5.2 (Symplectic case)**.**
Let p be prime, let $q=p^f$, and let d be an even positive integer greater than 2. If a subgroup G of $\mathrm{GSp}_d(q)$ has a subgroup H of index $(q^{d/2}+1)/x$, where x is a divisor of f, and $(q,d)\neq(2,6)$, then one of the following occurs:

Classical examples: *We have that $d=4$, q is even, and $\Omega_4^-(q)\trianglelefteqslant G$.*

Extension field examples: *We have either*

(a) $\mathrm{SL}_2(q^{d/2})\leqslant G\leqslant \Gamma\mathrm{L}_2^{\#}(q^{d/2})$.
(b) $\overline{G}=A_5$, $d=4$, *and* $q\in\{2,3\}$.
(c) *q is even, $G\leqslant \Gamma\mathrm{Sp}_{d/b}(q^b)$, where b is a divisor of d, $b\neq 1$, and one of the following holds:*
  (i) *$d/b=4$, $x=1$, and $\mathrm{Sz}(q^{d/4})\leqslant G\cap\mathrm{GSp}_4(q^{d/4})\leqslant\mathrm{Aut}(\mathrm{Sz}(q^{d/4}))$;*
  (ii) *$d/b=4$ and $\Omega_4^-(q^{d/4})\trianglelefteqslant G\cap\mathrm{GSp}_4(q^{d/4})$;*
(d) *q is odd, $q\neq 5$, $d=6$, $G\leqslant\Gamma\mathrm{U}_3(q^2)$, and $\mathrm{SU}_3(q^2)\trianglelefteqslant G\cap\mathrm{GU}_3(q^2)$.*

Symplectic type examples:
Here $q=3$, $d=4$, G is a cyclic subgroup of $(2_-^{1+4}\cdot\mathrm{O}_4^-(2))\circ 2$ of order 10 and H is its trivial subgroup.

Nearly simple case: *We have that there is a nonabelian simple group S such that $S\leqslant\overline{G}\leqslant\mathrm{Aut}(S)$. In each case below, we have that $x=1$.*

Alternating group case: Here $S=A_5$, $q=2$, $d=4$, and the vector space $V_4(2)$ can be identified with the fully deleted permutation module for S_5 over $\mathrm{GF}(2)$. Moreover, G has the natural transitive action on five points.

Cross-characteristic case: We have that $q=p$ and the table below lists the possibilities for this case. The number of times an isomorphism type of a group appears in a row for the $S\cap\overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $S\cap\overline{H}$ in S.

S	d	q	$S\cap\overline{H}$
$\mathrm{PSU}_3(3^2)$	6	5	$4\cdot A_4$, $4^2\cdot A_3$
$\mathrm{PSL}_2(7)$	6	3	S_3
$\mathrm{PSL}_2(13)$	6	3	$13:3$
$\mathrm{PSL}_2(25)$	12	2	S_5, S_5

Natural-characteristic case: Here $S=\mathrm{Sz}(q)$, $d=4$, $p=2$, and $\overline{G}$ has a unique conjugacy class of subgroups of index q^2+1.

Proof. We apply Theorem 3.2 in the case that G preserves an alternating form on $V_d(q)$. In many cases, it turns out that $x=1$, and so a lot of cases drop out. First note that as $d=e$, we can rule out the Reducible Examples and the Imprimitive Examples. For the Symplectic Type case, we have $d=4$, $p=3$, G is cyclic of order 10, and H is trivial (we used [12] to obtain most of this information).

Since d is even, we have in the Classical Examples case that $d=4$ and G contains $\Omega_4^-(q)$. By [19, pp. 165], q is even. Suppose now we are in the Extension field examples case. So we have that $G\leqslant\Gamma\mathrm{L}_{d/b}(q^b)$ where b is a divisor of d ($b\neq 1$), and G preserves an alternating form on $V_{d/b}(q^b)$, or $b=2$ and G preserves a unitary form on $V_{d/2}(q^2)$. We may assume that b is maximal in that G does not preserve a larger extension field structure. Suppose G preserves an alternating form on $V_{d/b}(q^b)$ and let $G_{Sp}=G\cap\mathrm{GSp}_{d/b}(q^b)$.

Suppose $d/b\geqslant 4$. So we can apply Theorem 3.2 to G_{Sp} where e/b, d/b, and q^b play the roles of e, d, and q respectively. Now since q^b is not prime and $d/b=e/b$, we have only the following two possibilities:

(i) $\Omega^-_{d/b}(q^b) \trianglelefteqslant G_{Sp}$ and $d/b = 4$;
(ii) $G^{(\infty)}_{Sp} = \mathrm{Sz}(q^b)$ and $d/b = 4$.

In the second case above, we have that $|G_{Sp} : H \cap G_{Sp}|$ is at least the minimum degree $(q^{d/4})^2 + 1$ of $\mathrm{Sz}(q^{d/4})$ (see [26]) and so

$$x = \frac{q^{d/2}+1}{|G:H|} \leqslant \frac{(q^{d/4})^2+1}{|G_{Sp} : H \cap G_{Sp}|} \leqslant 1.$$

Now suppose G preserves a unitary form on $V_{d/2}(q^2)$ and let $G_U = G \cap \mathrm{GU}_{d/2}(q^2)$. First suppose that $d/2$ is even. Then by Theorem 3.2, q is odd and G_U has a subgroup of order dividing $q^{d/2}+1$. Since $d \geqslant 6$, we can apply Theorem 3.2 again where $e/2$, $d/2$, and q^2 play the roles of e, d, and q respectively. Now since q^2 is not prime, $d/2 = e/2$, q is odd, and G_U is not of Extension Field type (we chose the extension to be maximal), we find that this case does not arise. So suppose that $d/2$ is odd. Then it follows from Theorem 4.1 that $q \neq 2, 5$, $d = e = 6$, and $\mathrm{SU}_3(q^2) \trianglelefteqslant G_U$. The case $d/b = 2$ follows from Lemma 5.1.

Now consider the Nearly simple examples, and suppose firstly that we are in the Alternating group case. Consider the action of A_n on its fully deleted permutation module M (over a field of order q), and suppose $\perp$ is a polarity on M. Since A_n is absolutely irreducible on M, we have that the centraliser of A_n consists only of scalar matrices (see [19, Lemma 2.10.1]). Therefore, it follows that $\perp$ is a scalar multiple of the natural polarity induced by the dot product on $V_d(q)$, which is of orthogonal type. So q is even and hence $q = 2$, $n = 5$, $x = 1$, and $d = 4$. In the Cross-characteristic case, by inspecting the table in Theorem 3.2, we check that x divides f and $d = e$. From this inspection, we find that $x = 1$ and we arrive at the following possibilities:

S	d	q	$S \cap \overline{H}$
$\mathrm{PSU}_3(3^2)$	6	5	$4 \cdot A_4$, $4^2 \cdot A_3$
$\mathrm{PSL}_2(7)$	6	3	S_3
$\mathrm{PSL}_2(13)$	6	3	$13:3$
$\mathrm{PSL}_2(25)$	12	2	S_5, S_5

Finally, in the Natural-characteristic case, the only case that arises is when $S = \mathrm{Sz}(q)$, $d = 4$, and $p = 2$ (since $d = e$). □

Corollary 5.3 (Orthogonal (elliptic) case)**.**
Let p be prime, let $q = p^f$, and let d be an even positive integer greater than 2. If a subgroup G of $\mathrm{GO}^-_d(q)$ has a subgroup H of index $(q^{d/2}+1)/x$, where x is a divisor of f, and $(q,d) \neq (2,6)$, then one of the following occurs:

Classical examples: *We have $d = 4$ and $\Omega^-_4(q) \leqslant G$.*

Extension field examples: *Here we have that $G \leqslant \Gamma\mathrm{O}^-_{d/b}(q^b)$ where b is a non-trivial divisor of d. We have one of the following:*

(a) $\mathrm{SL}_2(q^{d/2}) \leqslant G \leqslant \Gamma\mathrm{L}^{\#}_2(q^{d/2})$;
(b) $G = A_5$, $d = 4$, *and* $q \in \{2,3\}$;
(c) q *is even,* $d/b = 4$, $G \leqslant \Gamma\mathrm{O}^-_4(q^{d/4})$, *and* $\Omega^-_4(q^{d/4}) \trianglelefteqslant G \cap \mathrm{GO}^-_4(q^{d/4})$;
(d) q *is odd,* $q \neq 5$, $d = 6$, $G \leqslant \Gamma\mathrm{U}_3(q^2)$, *and* $\mathrm{SU}_3(q^2) \trianglelefteqslant G \cap \mathrm{GU}_3(q^2)$.

Nearly simple case: *We have that there is a nonabelian simple group S such that $S \leqslant \overline{G} \leqslant \mathrm{Aut}(S)$. In each case below, we have that $x = 1$.*

Alternating group case: We have $q = p = 3$, $d = 6$, $G = S_7 \times 2$, and $H \cong A_6$. There are two conjugacy classes of subgroups of G isomorphic to A_6.

Cross-characteristic case: Here we have $S = \mathrm{PSL}_2(7)$, $d = 6$, $q = 3$, and $(G,H) \in \{(\mathrm{PGL}_2(7), A_4), (\mathrm{PGL}_2(7), D_{12}), (\mathrm{PSL}_2(7), S_3)\}$.

Proof. As in Corollary 5.2, we apply Theorem 3.2. First note that as $d = e$, we can rule out the Reducible examples and the Imprimitive examples. By [19, pp. 150], the Symplectic type case does not arise.

In the Classical examples case, since d is even, we have that $d = 4$ and $\Omega^-_4(q) \trianglelefteqslant G$. Suppose now we are in the Extension field examples case. So we have that $G \leqslant \Gamma\mathrm{O}^-_{d/b}(q^b)$ where b is a non-trivial divisor of d. By Theorem 3.2, we see that G must either preserve a form on $V_{d/b}(q^b)$ of the same type as that on $V_d(q)$, or $b = 2$ and G preserves a unitary form on $V_{d/2}(q^2)$. Let us assume the former case. We may

assume that b is maximal in that $G \cap \mathrm{GO}^-_{d/b}(q^b)$ does not preserve a larger extension field structure. Let $G_{O^-} = G \cap \mathrm{GO}^-_{d/b}(q^b)$.

Suppose $d/b \geqslant 4$. Then we can apply Theorem 3.2 to G_{O^-} where e/b, d/b, and q^b play the roles of e, d, and q respectively. Now since q^b is not prime and $d/b = e/b$, we have only the following two possibilities:

(i) $\Omega^-_{d/b}(q^b) \trianglelefteqslant G_{O^-}$ and $d/b = 4$;

(ii) $G^{(\infty)}_{O^-} = \mathrm{Sz}(q^b)$ and $d/b = 4$.

However, by [17], $\mathrm{Sz}(q^b)$ does not have a 4-dimensional orthogonal representation in characteristic 2. Hence the second case above does not arise.

Now suppose G preserves a unitary form on $V_{d/2}(q^2)$ and let $G_U = G \cap \mathrm{GU}_{d/2}(q^2)$. First suppose that $d/2$ is even. Then by Theorem 3.2, q is odd and G_U has a subgroup of order dividing $q^{d/2}+1$. Since $d \geqslant 6$, we can apply Theorem 3.2 again where $e/2$, $d/2$, and q^2 play the roles of e, d, and q respectively. Now since q^2 is not prime, $d/2 = e/2$, q is odd, and G_U is not of Extension field type, we find that this case does not arise. For $d/2$ odd, it follows from Theorem 4.1 that $q \neq 2, 5$, $d = e = 6$, and $\mathrm{SU}_3(q^2) \trianglelefteqslant G_U$. The case $d/b = 2$ follows from Lemma 5.1.

Now suppose G is in the Nearly simple case. In the Alternating group case, we do some discriminant calculations as follows: Let V be a vector space of dimension n over a field of order q and let M be the fully deleted permutation module of V of dimension d. Let f be a non-degenerate bilinear form on V (one can take the usual dot product on V) and let f_M be the induced bilinear form on M. For some of the values of n, d, and q given by Theorem 3.2, we can find the possibilities for the signs of f and f_M.

q	d	n	Sign of f	Sign of f_M
2	4	5	$\circ$	$+$
3	4	5	$\circ$	$+$
		6	$-$	$+$
3	6	7	$\circ$	$-$
5	6	7	$\circ$	$+$
	8	9	$\circ$	$+$
		10	$+$	$+$

So we see that $q^e = 3^6$ in this case. Note that $x = 1$ as $q = p$. Now we turn to the case that $q^e \in \{2^{10}, 2^{12}, 2^{18}\}$ and $n = e+1$. First note that again we have $x = 1$ as $q = p$. In the case that $q^e = 2^{10}$, the only maximal subgroups of A_{11} and S_{11} which have index dividing $(q^{e/2}+1)/x = 33$ are A_{10} and S_{10} respectively. Since these groups do not have an index 3 subgroup, this case does not arise. A similar argument shows that the cases $q^e = 2^{12}$ and $q^e = 2^{18}$ do not arise.

In the Cross-characteristic case, by inspecting the table in Theorem 3.2, we arrive at the following possibilities:

S	d	q	$S \cap \overline{H}$
$\mathrm{PSU}_3(3^2)$	6	5	$4 \cdot A_4$, $4^2 \cdot A_3$
$\mathrm{PSL}_2(7)$	6	3	S_3
$\mathrm{PSL}_2(13)$	6	3	$13:3$
$\mathrm{PSL}_2(25)$	12	2	S_5, S_5

By [17], $\mathrm{PSL}_2(13)$ and $\mathrm{PSL}_2(25)$ do not have orthogonal representations of degrees 6 and 12 respectively, of characteristic given in the table above. It is clear from the tables in Kleidman's thesis [23], that $\mathrm{PSU}_3(3^2)$ is not a subgroup of $\mathrm{PSU}_4(5^2)$, and hence not a subgroup of $\Gamma\mathrm{O}^-_6(5)$ (recall that $\mathrm{P}\Omega^-_6(5) \cong \mathrm{PSU}_4(5^2)$). So we are left with the case that $S = \mathrm{PSL}_2(7)$. Indeed, $\mathrm{PSL}_2(7)$ is a subgroup of $\mathrm{PSL}_3(4)$, which is in turn a maximal subgroup of $\mathrm{PSU}_4(3^2)$. Therefore, this case arises.

Finally, since $d = e$, we have in the Natural-Characteristic case that $G^{(\infty)} = \mathrm{Sz}(q)$, $d = 4$, and $p = 2$. However, by [17], $\mathrm{Sz}(q)$ does not have a 4-dimensional orthogonal representation in characteristic 2. Hence this case does not arise. □

Corollary 5.4 (Orthogonal (parabolic) case)**.**
Let p be prime, let $q = p^f$, and let d be an odd positive integer greater than 1. If a subgroup G of $\mathrm{GO}_d(q)$ has a subgroup H of index $(q^{(d-1)/2}+1)/x$, where x is a divisor of f, then one of the following occurs:

REDUCIBLE EXAMPLES: *We have that G fixes a subspace or quotient space U of $V_d(q)$ and $\dim(U) = d-1$. So $G \leqslant q^{d-1} \cdot (\mathrm{GO}^-_{d-1}(q) \times \mathrm{GO}_1(q))$, where $\Phi^*_{d-1}(q)$ divides $|G^U|$, and G^U has a subgroup of index $(q^{(d-1)/2}+1)/y$, with $\Phi^*_{d-1}(q)$ coprime to y. The group G^U satisfies the hypotheses of Corollary 5.3.*

IMPRIMITIVE EXAMPLES: *Here G preserves a direct sum decomposition $V = U_1 \bigoplus \cdots \bigoplus U_d$ where each U_i has dimension 1. Moreover, G is a subgroup of $\mathrm{GL}_1(q) \wr S_d$ in product action, and G induces a primitive group on the factors $\{U_1, \ldots, U_d\}$. Finally, either $q^d = 3^5, 3^7$ or $q = 2$, $d = 5$, $x = 1$.*

EXTENSION FIELD EXAMPLES: *In this case, $q = p \in \{2, 3\}$, $d = 5$, and $G \leqslant \Gamma\mathrm{L}_1^{\#}(q^5)$. Furthermore, if $q = 2$, then $x = 1$, and if $q = 3$, we have $x = 1, 2$.*

NEARLY SIMPLE CASE: *We have in this case, $S \leqslant \overline{G} \leqslant \mathrm{Aut}(S)$ where S is a finite nonabelian simple group.*

Cross-characteristic case: The table below lists the possibilities for this case. The number of times an isomorphism type of a group appears in a row for the $S \cap \overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $S \cap \overline{H}$ in S. We have that $d = 7$ and $x = 1$ in each case.

S	q	$S \cap \overline{H}$	S	q	$S \cap \overline{H}$
$\mathrm{PSL}_2(7)$,$\mathrm{PSL}_3(2)$	3	S_3	$\mathrm{PSU}_3(3^2)$	5	$4 \cdot A_4$, $4^2 \cdot A_3$
$\mathrm{PSL}_2(8)$	3	$9:2$	$\mathrm{Sp}_6(2)$	3	$\mathrm{PSU}_4(2^2):2$
	5	2^2		5	$2^5 : A_6$
$\mathrm{PSL}_2(13)$	3	$13:3$			

Natural-characteristic case: Here we have that $x = 1$, $d = 7$, $p = 3$, and $\overline{G}$ has a unique conjugacy class of subgroups of index $q^3 + 1$. We also have that $\overline{G}$ acts 2-transitively of degree $q^3 + 1$ and we have either $S = \mathrm{PSU}_3(q^2)$ or $S = {}^2G_2(q)$ (and $q \neq 3$).

Proof. We apply Theorem 3.2. First note that as $d = e+1$, we can rule out the Symplectic type examples and the second part of the Extension field examples (note that $\gcd(d, e) = 1$ in these cases). The Classical examples case does not arise by [19, pp. 165]. The Imprimitive examples case is largely unchanged from Theorem 3.2 except that we impose the restriction that $d = e+1$, and the case $(q, d) = (5, 7)$ is missing for the following argument. Let π be the natural projection map from $\mathrm{GL}_1(5) \wr S_7$ to S_7. Since $q^3 + 1 = 126$ and $\ker \pi$ is even, we have that $|\pi(G) : \pi(H)| \in \{63, 126\}$. It follows that $\pi(G) \in \{A_7, S_7\}$ by elementary knowledge of the subgroups of S_7. However, A_7 and S_7 do not have subgroups of index 63 or 126; which is a contradiction. Hence $(q, d) \neq (5, 7)$.

In the Reducible examples case, we have from [19, pp. 83] that $G \leqslant q^{d-1)} \cdot (\mathrm{GO}^{\epsilon}_{d-1}(q) \times \mathrm{GO}_1(q))$ where $\epsilon = \pm$. Now since $\Phi^*_{d-1}(q)$ divides $|G^U|$, and $\Phi^*_{d-1}(q)$ is coprime to the order of $\mathrm{GO}^+_{d-1}(q)$, we have that $\epsilon = -$.

Now suppose G is in the Nearly simple case. In the Cross-characteristic examples subcase, we have from [17], that $\mathrm{PSL}_2(25)$ does not have a 12-dimensional orthogonal representation in characteristic 2, and we are left with the following:

S	q	d	x	$S \cap \overline{H}$	S	q	d	x	$S \cap \overline{H}$
$\mathrm{PSL}_2(7)$,$\mathrm{PSL}_3(2)$	3	7	1	S_3	$\mathrm{PSL}_2(25)$	2	13	1	S_5, S_5
$\mathrm{PSL}_2(8)$	3	7	1	$9:2$	$\mathrm{PSU}_3(3^2)$	5	7	1	$4 \cdot A_4$, $4^2 \cdot A_3$
	5	7	1	2^2	$\mathrm{Sp}_6(2)$	5	7	1	$2^5 : A_6$
$\mathrm{PSL}_2(13)$	3	7	1	$13:3$		3	7	1	$\mathrm{PSU}_4(2^2):2$

For the Natural-characteristic case, we have $d = 7$, $p = 3$, and $S \in \{\mathrm{PSU}_3(q^2), {}^2G_2(q)\}$. □

Corollary 5.5 (Orthogonal (hyperbolic) case)**.**
Let p be prime, let $q = p^f$, and let d be an even positive integer greater than 2. If a subgroup G of $\mathrm{GO}^+_d(q)$ has a subgroup H of index $(q^{d/2-1} + 1)/x$, where x is a divisor of f, and $(q, d) \neq (2, 6)$, then one of the following occurs:

REDUCIBLE EXAMPLES: *We have that G fixes a subspace or quotient space U of $V_d(q)$ of dimension m with $m \in \{d-1, d-2\}$. So $G \leqslant q^{m(d-m)} \cdot (\mathrm{GL}_m(q) \times \mathrm{GL}_{d-m}(q))$, $\Phi^*_{d-2}(q)$ divides $|G^U|$, and G^U has a subgroup of index $(q^{d/2-1} + 1)/y$, with $\Phi^*_{d-2}(q)$ coprime to y. There are two subcases:*

(i) $\dim(U) = d - 1$ *and* $G^U \leqslant \mathrm{GO}_{d-1}(q)$*; or*
(ii) $\dim(U) = d - 2$ *and* $G^U \leqslant \mathrm{GO}^-_{d-2}(q)$.

EXTENSION FIELD EXAMPLES:
Here we have that $d = 14$, $p = 3$, $G \leqslant \Gamma\mathrm{O}_7(q^2)$, and $\mathrm{PSU}_3(q^4) \leqslant G \cap \mathrm{GO}_7(q^2)$.

SYMPLECTIC TYPE EXAMPLES:
Here $q = p \in \{3, 5\}$, $d = 8$, and $G \leqslant (2^{1+6}_+ \cdot \mathrm{O}^+_6(2)) \circ Z$ where Z is the subgroup of scalar matrices of $\mathrm{GL}_8(q)$.

NEARLY SIMPLE CASE: *We have that there is a nonabelian simple group S such that $S \leqslant \overline{G} \leqslant \mathrm{Aut}(S)$. In each case below, we have $x = 1$ and $d = 8$.*

Alternating group case:

In this case $q = p$, $S = A_n$, and G has a unique conjugacy class of subgroups of index q^3+1. We have one of the following:

n	p	*Description of subgroup of index q^3+1*
10	5	*Stabiliser of action on 5-subsets of a 10 element set*
9	5	*Stabiliser of action on 5-subsets of a 10 element set*
8	3	*Stabiliser of action on unordered pairs*
7	5	*Stabiliser of action on Sylow 5-subgroups*

Cross-characteristic case: Firstly, we have that $q = p$. The table below lists the possibilities for this case. The number of times an isomorphism type of a group appears in a row for the $S \cap \overline{H}$ column is equal to the number of conjugacy classes of that isomorphism type for $S \cap \overline{H}$ in S.

S	q	$S \cap \overline{H}$
$\mathrm{PSL}_3(4)$	5	$2^4 : D_{10}$, $2^4 : D_{10}$
$\mathrm{PSL}_2(8)$	5	2^2
$\mathrm{Sp}_6(2)$	3	$\mathrm{PSU}_4(2^2) : 2$
	5	$2^5 : A_6$

Natural-characteristic case: Here we have that $\overline{G}$ has a unique conjugacy class of subgroups of index q^3+1. Either $S = \mathrm{PSL}_2(q^3)$ and q is even, or $S = \mathrm{PSU}_3(q^2)$ and $p \neq 3$.

Proof. We apply Theorem 3.2. First note that as $d = e + 2$, we can rule out the one-dimensional Extension field examples. For the Symplectic type case, we have by [19, pp. 150], that $d = 8$, $p \in \{3, 5\}$, and $G \leqslant (2_+^{1+6} \cdot \mathrm{O}_6^+(2)) \circ Z$. The Classical examples case does not arise by [19, pp. 165].

Suppose now that we have the Reducible examples case. So G fixes a subspace or quotient space U of $V_d(q)$, of dimension m, where $m \in \{d-1, d-2\}$. There are two subcases:

(i) $m = d-1$ and $G^U \leqslant \mathrm{GO}_{d-1}(q)$;
(ii) $m = d-2$ and either $G^U \leqslant \mathrm{GO}^+_{d-2}(q)$ or $G^U \leqslant \mathrm{GO}^-_{d-2}(q)$.

Suppose we have the second case above where $G^U \leqslant \mathrm{GO}^+_{d-2}(q)$. Since $\Phi^*_{d-2}(q)$ divides $|G^U|$, we must have that $\Phi^*_{d-2}(q)$ divides $|\mathrm{GO}^+_{d-2}(q)|$. Now the largest $q^i - 1$ term of $|\mathrm{GO}^+_{d-2}(q)|$ is $q^{d/2-1} - 1$, and hence we have a contradiction. Therefore, we have only $G^U \leqslant \mathrm{GO}^-_{d-2}(q)$ in the situation where $m = d-2$.

In the Imprimitive Examples case, we have from [19, pp. 100] that $qd/2$ is odd and hence $q = 3$ and $d = 6$. Moreover, we have that $G \leqslant \mathrm{GO}_{d/2}(q)^2$. Now the primitive groups of degree 6 are $PSL_2(5)$, $\mathrm{PGL}_2(5)$, A_6, and S_6. Each of these does not have size dividing $\mathrm{GO}_3(3)^2 = 48^2$. Hence this case does not arise.

Suppose now we are in the Extension field case. So we have three subcases:

(i) $d/2$ is even and $G \leqslant \Gamma\mathrm{O}^+_{d/2}(q^2)$ (note that $\gcd(d, d-2) = 2$ and so $b = 2$),
(ii) $d/2$ is odd and $G \leqslant \Gamma\mathrm{O}^\circ_{d/2}(q^2)$, or
(iii) $d/2$ is even and $G \leqslant \Gamma\mathrm{U}_{d/2}(q^2)$.

(i) Let us assume the first case. Note that $\Phi^*_{d-2}(q)$ divides $|G \cap \mathrm{GO}^+_{d/2}(q^2)|$, however, the largest $q^i - 1$ factor of $|\mathrm{GO}^+_{d/2}(q^2)|$ has $i < d-2$; a contradiction.

(ii) Now suppose we are in the second case; that is, $G \leqslant \Gamma\mathrm{O}_{d/2}(q^2)$, and $d/2$ is odd. Let $G_O = G \cap \mathrm{GO}_{d/2}(q^2)$. Since $d/2 \geqslant 3$, we can apply Corollary 5.4 to G_O where $d/2 - 1$, $d/2$, and q^2 play the roles of e, d, and q respectively. Now since q^2 is not prime, and we can assume that G_O is irreducible, we have that $d/2 = 7$, $p = 3$, and $S \leqslant \overline{G_O} \leqslant \mathrm{Aut}(S)$ where $S = \mathrm{PSU}_3(q^4)$.

(iii) Finally, suppose we have the third case; that is, $G \leqslant \Gamma\mathrm{U}_{d/2}(q^2)$, and $d/2$ is even. Let $G_U = G \cap \mathrm{GU}_{d/2}(q^2)$. If $d/2 \geqslant 4$, then we can apply Theorem 3.2 to G_U where $d/2 - 1$, $d/2$, and q^2 play the roles of e, d, and q respectively. Now since q^2 is not prime, we have one of the following:

(a) $d = 8$, $\Omega_4^-(q^2) \trianglelefteq G_U$;
(b) $S \trianglelefteq \overline{G_U} \leqslant \mathrm{Aut}(S)$ where (d, q, S) is $(8, 9, \mathrm{PSL}_2(7))$, $(8, 25, \mathrm{PSL}_2(7))$, or $(20, 4, \mathrm{PSL}_2(19))$.

The first case does not arise by [19, pp. 165]. We can also check the representations of the groups S in case (b). It turns out that $\mathrm{PSL}_2(7)$ does not have the required unitary representation (see [17]), so we are

now left with the case that $S = \mathrm{PSL}_2(19)$. Now in this case, $q^{d/2-1}+1 = 262145$ but $|\mathrm{Aut}(S)| = 6840$. Clearly this case is impossible.

If $d = 4$, so that $G \leqslant \Gamma\mathrm{L}_2^{\#}(q^{d/2})$, we apply Lemma 5.1. If $A_5 \leqslant G$ and $q \in \{2,3\}$, then this implies that 60 divides $\mathrm{GO}_4^+(q)$ – which is impossible. Again, by inspecting orders, the case $\mathrm{SL}_2(q^2) \leqslant G$ does not arise as $\mathrm{SL}_2(q^2)$ is not a subgroup of $\mathrm{GO}_4^+(q)$. Therefore $d > 4$.

Now suppose G is in the Nearly simple case. In the Alternating group case: Permutation module examples, note that in many of the cases, we do not have $e = d-2$. We are left with the following possibilities:

(i) $q^e = 5^6$, $d = 8$, $n = 9$, and G has a unique transitive action on 126 points where H is the stabiliser in the action on 5-subsets;
(ii) $q^e = 5^6$, $d = 8$, $n = 10$, and G has a unique transitive action on 126 points where H is the stabiliser of a partition of a set of size 10 into 2 sets of size 5;

For Alternating group case: Other examples, we have $d = 8$, $q = p$, $S = A_n$, and G has a unique conjugacy class of subgroups of index q^3+1. So we have one of the following:

n	p	Description of subgroup of index q^3+1
10	5	Stabiliser of action on 5-subsets of a 10 element set
9	5	Stabiliser of action on 5-subsets of a 10 element set
8	3	Stabiliser of action on unordered pairs
7	5	Stabiliser of action on Sylow 5-subgroups

By [17], A_9 and A_{10} both have a unique 8-dimensional absolutely irreducible orthogonal representation over GF(5). In the Cross-characteristic case, by inspecting the table in Theorem 3.2, we have that $d = 8$ and one of the following possibilities:

S	q	$S \cap \overline{H}$	S	q	$S \cap \overline{H}$
$\mathrm{PSL}_2(7)$	3	S_3	$\mathrm{PSL}_3(4)$	5	$2^4 : D_{10}$, $2^4 : D_{10}$
$\mathrm{PSL}_2(8)$	3	$9:2$	$\mathrm{Sp}_6(2)$	3	$\mathrm{PSU}_4(2^2) : 2$
	5	2^2		5	$2^5 : A_6$

By [17], $\mathrm{PSL}_2(7)$ and $\mathrm{PSL}_2(8)$ do not have absolutely irreducible 8-dimensional representations in characteristic 3. Finally, since $d = e+2$, we have in the Natural-Characteristic case that $d = 8$ and either $S = \mathrm{PSL}_2(q^3)$ or $S = \mathrm{PSU}_3(q^2)$. If $S = \mathrm{PSL}_2(q^3)$, then by [20], q is even. □

6. Proof of Theorem 3.1

Before we begin proving the first main theorem of this paper, we recast a simple number theoretic result which appears in Hering's 1974 paper [15] which lists the possible values of q and e when $\Phi_e^*(q)$ is small. By definition, the number $\Phi_e^*(q)$ is congruent to 1 modulo e. So if this quantity is nontrivial, the smallest values it can take are $e+1$ and $2e+1$. In these cases, we have specific information on the values of q and e.

Lemma 6.1. *Let q be a power of a prime p and $e \geqslant 3$ an integer.*

(i) *If $\Phi_e^*(q) = e+1$ then $q^e = p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$.*
(ii) *If $\Phi_e^*(q) = 2e+1$ then either $q^e = p^e = 2^3, 2^8, 2^{20}$, or $q^e = p^{2e} = 4^3, 4^6, 9^2$.*
(iii) *If $\Phi_e^*(q) = (e+1)^2$ then $q^e = p^e = 7^4$.*
(iv) *If $\Phi_e^*(q) = (e+1)(2e+1)$ then $q^e = p^e = 3^{18}, 17^6$.*

Note that if $q = p^f$, then $\Phi_{ef}^*(p)$ divides $\Phi_e^*(q)$. In our applications, it will be necessary to investigate the values of this possibly smaller number $\Phi_{ef}^*(p)$. Hence, we will often refer to the following simple observation.

Lemma 6.2. *If $\Phi_{ef}^*(p) = e+1$ and $e > 1$, then $f = 1$.*

Proof. First note that $\Phi_{ef}^*(p) \equiv 1 \pmod{ef}$ as by definition, ef is the order of p modulo $\Phi_{ef}^*(p)$. Since $\Phi_{ef}^*(p) > 1$, we have $\Phi_{ef}^*(p) \geqslant ef+1$ and hence $e+1 \geqslant ef+1$. So it follows that $f = 1$. □

Now we will prove Theorem 3.1. We have that $q = p^f$ where p is a prime, d and e are integers greater than 2 satisfying $d/2 < e \leqslant d$, and G is a subgroup of $\mathrm{GL}_d(q)$ with order divisible by $\Phi_{ef}^*(p)$ (which is nontrivial). By the latter condition, there exists a primitive prime divisor r of $p^{ef}-1$ that divides $|G|$. Since $\Phi_{ef}^*(p)$ divides $\Phi_e^*(q)$, we have that r is a primitive prime divisor of q^e-1. So we can apply the result of Guralnick, Praeger, Penttila, Saxl (see [13, Main Theorem]).

Classical examples: By [13, Main Theorem], we have $G \leqslant \mathrm{GL}_d(q_0) \circ Z$, where $q = q_0^b$ and Z is the group of non-singular scalar matrices in $\mathrm{GL}_d(q)$. So $\Phi^*_{ef}(p)$ divides

$$|\mathrm{GL}_d(q_0) \circ Z| = p^{\frac{df(d-1)}{2b}}(p^f - 1)\left[(p^{2f/b} - 1)(p^{3f/b} - 1)\cdots(p^{df/b} - 1)\right].$$

Now $\Phi^*_{ef}(p)$ is coprime to $p^i - 1$ for $1 \leqslant i < ef$, and hence $\Phi^*_{ef}(p)$ divides

$$\left[(p^{ef/b} - 1)(p^{ef/b+1} - 1)\cdots(p^{df/b} - 1)\right].$$

Therefore $d/b \geqslant e$ (as $\Phi^*_{ef}(p) > 1$). Now $d/2 < e \leqslant d$ and hence if $b \neq 1$, we have $d/b \leqslant d/2 < e$, which is a contradiction. Therefore $b = 1$, $q = q_0$, and the rest follows from [13, Main Theorem].

Reducible examples: By [13, Main Theorem], we have that G fixes a subspace or quotient space U of $V_d(q)$ and $\dim(U) = m \geqslant e$. So $G \leqslant q^{m(d-m)} \cdot (\mathrm{GL}_m(q) \times \mathrm{GL}_{d-m}(q))$. Since $m > d/2$, the point-wise stabiliser $G_{(U)}$ can be identified with a subgroup of $\mathrm{GL}_{d-m}(q)$. Now $|G| = |G^U||G_{(U)}|$ and $|G_{(U)}|$ divides $q^{(d-m)(d-m-1)/2}(q-1)(q^2-1)\cdots(q^{d-m}-1)$. Since $\Phi^*_{ef}(p)$ divides $|G|$, it follows that $\Phi^*_{ef}(p)$ divides $|G^U|$ as $\Phi^*_{ef}(p)$ is coprime to $q^i - 1 = p^{fi} - 1$ for $0 < i < e$ and $d - m < e$.

Imprimitive examples: By [13, Main Theorem], we have $r = e + 1 \leqslant d$, and by [13, Lemma 4.1], every primitive prime divisor of $q^e - 1$ is equal to $e + 1$. Therefore every primitive prime divisor of $p^{ef} - 1$ is equal to $e + 1$, and so $\Phi^*_{ef}(p)$ is a power of $e + 1$. Now G is a subgroup of $\mathrm{GL}_1(q) \wr S_d$ and hence $\Phi^*_{ef}(p)$ divides $|\mathrm{GL}_1(q) \wr S_d| = (q-1)^d d!$. Since $\Phi^*_{ef}(p)$ is coprime to $q - 1$, it follows that $\Phi^*_{ef}(p)$ divides $d!$. If r^2 divides $d!$, then $r \leqslant d/2$, which contradicts the fact that $r = e + 1 > d/2$. So $\Phi^*_{ef}(p) = r = e + 1$. By Lemma 6.2, we have that $f = 1$ and hence $q = p$. We have from Lemma 6.1 the following possibilities for q, e, and d:

q	e	d	q	e	d
2	4	$5, 6, 7$	3	4	$5, 6, 7$
2	10	$11, \ldots, 19$	3	6	$7, \ldots, 11$
2	12	$13, \ldots, 23$	5	6	$7, \ldots, 11$
2	18	$19, \ldots, 35$			

Extension field examples:

(a) Here we have $r = d = e + 1$. By the proof of [13, Lemma 4.2], $\Phi^*_{ef}(p)$ is a power of r. Now G is a subgroup of $\mathrm{GL}_1(q^d) \cdot d$ and hence $\Phi^*_{ef}(p)$ divides $(q^d - 1)d$. Since $\Phi^*_{ef}(p)$ is coprime to $p^{(e+1)f} - 1 = q^d - 1$, it follows that $\Phi^*_{ef}(p)$ divides d and hence $\Phi^*_{ef}(p) = r = e + 1$. So by Lemma 6.2 and Hering's Theorem, we have $q^e = p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$.

(b) As given in the statement of the Theorem, we have that $G \leqslant \mathrm{GL}_{d/b}(q^b) \cdot b$ where b is divisor of $\gcd(d, e)$ and $b \neq 1$. Suppose G preserves a non-degenerate sesquilinear form f on $V_d(q)$. By [19, Table 4.3A], G preserves a form f' on $V_{d/b}(q^b)$ of a type related to f as follows:

type of f	type of f'	conditions
null	null	
unitary	unitary	
symplectic	symplectic	
symplectic	unitary	q odd
orthogonal	orthogonal	$d/b \geqslant 3$, same sign
orthogonal	orthogonal	$b = 2$, $dq/2$ odd
orthogonal	unitary	$b = 2$, sign is $(-)^{d/2}$

Now the largest $q^i - 1$ term of $|\mathrm{GO}_{d/2}(q)|$ is $q^{d/2-1} - 1$, and so since $\Phi^*_{ef}(p)$ is coprime to $q^i - 1$ for $1 \leqslant i < e$, it follows that $d - 2 \geqslant e$. The remaining cases are precisely when f' is unitary or f' is the same type as f.

We show now that $\Phi^*_{ef}(p)$ divides $|G \cap \mathrm{GL}_{d/b}(q^b)|$. Let r' be any primitive prime divisor of $q^e - 1$ which divides $|G|$. By the proof of [13, Lemma 4.2], if r' divides b, then $r' = b = d = e + 1$ and we are in case (a) above. So we can assume that every primitive prime divisor of $q^e - 1$ that divides $|G|$ is not a divisor of b. So in particular, every primitive prime divisor of $p^{ef} - 1$ that divides $|G|$ is not a divisor of b, and hence $\Phi^*_{ef}(p)$ is coprime to b. Therefore $\Phi^*_{ef}(p)$ divides $|G \cap \mathrm{GL}_{d/b}(q^b)|$.

Symplectic type examples:

Here we have two cases, but in all cases we have $d = 2^m$, p is odd, and f is odd.

(a) In this case, $r = d + 1 = e + 1$ and r is a Fermat prime. By the proof of [13, Lemma 4.3], the only primitive prime divisor of $q^e - 1$ is r and so the only primitive prime divisor of $p^{ef} - 1$ is r. Therefore,

$\Phi^*_{ef}(p)$ is a power of r. Now G is a subgroup of $(S \cdot M_0) \circ Z$, where S is a 2-group, and M_0 is given by [13, Table 1]. It follows that $\Phi^*_{ef}(p)$ divides

$$|\mathrm{Sp}_{2m}(2)| = 2^{m^2}(2^2-1)(2^4-1)\cdots(2^{2m}-1).$$

Since r is a primitive prime divisor of $2^{2m}-1$ (see the proof of [13, Lemma 4.3]), we have that $\Phi^*_{ef}(p) = r = e+1$. By Lemma 6.1 and Lemma 6.2, we get $q^e = p^e = 3^4$ (recall that p is odd and $e+1$ is a Fermat prime). Therefore, by [13, Main Theorem], $G \leqslant (2^5_- \cdot \mathrm{O}^-_4(2)) \circ 2$ (note that $\Phi^*_e(q) = 5$ and 5 does not divide $|\mathrm{O}^+_4(2)| = 72$).

(b) In this case, $r = d-1 = e+1$ and r is a Mersenne prime (and hence m is prime). Again, by the proof of [13, Lemma 4.3], the only primitive prime divisor of q^e-1 is r and so $\Phi^*_{ef}(p)$ is a power of r. Now

$$\gcd(r, 2^{2i}-1) = \gcd(2^m-1, 2^{2i}-1) = 2^{\gcd(m,2i)}-1$$

and hence r divides $2^{2i}-1$ if and only if m divides $2i$. It follows that $\Phi^*_{ef}(p) = r = e+1$. By Lemma 6.1 and Lemma 6.2, we have $q^e = p^e = 3^6, 5^6$ (note that p is odd and $e+1$ is a Mersenne prime). If $p = 3$, then by [13, Main Theorem], $G \leqslant (2^7_+ \cdot \mathrm{O}^+_6(2)) \circ 2$ (note that $\Phi^*_e(q) = 7$ and 7 does not divide $|\mathrm{O}^-_6(2)| = 51840$). If $p = 5$, then by [13, Main Theorem], either $G \leqslant ((4 \circ 2^7) \cdot \mathrm{Sp}_6(2)) \circ 4$ or $G \leqslant (2^7_+ \cdot \mathrm{O}^+_6(2)) \circ 4$.

Nearly simple case:

Alternating group case: In all subcases, $S = A_n$ for $n \geqslant 5$, and $S \leqslant G/(G \cap Z) \leqslant \mathrm{Aut}(S)$ where Z is the group of scalar matrices in $\mathrm{GL}_d(q)$. So $|G|$ divides $|Z||\mathrm{Aut}(S)|$ and thus $|\Phi^*_{ef}(p)|$ divides $n!$.

(a) Here d is $n-1$ or $n-2$, and $(d+3)/2 \leqslant r \leqslant n$ with r a primitive prime divisor of $q^{r-1}-1$ (thus $r = e+1$). So $\Phi^*_{ef}(p)$ is a power of r. But if r^2 divides $n!$, then $r \leqslant n/2 \leqslant (d+2)/2$. This is a contradiction as $r \geqslant (d+3)/2$. Therefore $\Phi^*_{ef}(p) = r = e+1$ and we can apply Lemma 6.1 and Lemma 6.2. So in this case $q^e = p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$.

(b) Here we run through Tables 2 and 3 of [13], and apply Lemma 6.1, but first a subtlety will be noted which occurs in Table 2 of [13]. In one of the lines of the table, it has two possibilities for r; it could be $e+1$ or $2e+1$. However, it is not stated explicitly that there cannot be two distinct primitive prime divisors of q^e-1 dividing $|G|$. But the table states that if $r = e+1$, then $r = 5$, and if $r = 2e+1$, then $r = 7$. Since these values of r yield different values of e, we see that every primitive prime divisor of q^e-1 dividing $|G|$ must have the same value; either $e+1$ or $2e+1$. So we can now deduce that $\Phi^*_{ef}(p)$ is a power of r. By knowing that $\Phi^*_{ef}(p)$ divides $n!$, from the tables below we find that $\Phi^*_{ef}(p)$ is r or r^2. The case for Table 2 is shown below:

n	d	p (always odd)	$r = e+1$	$r = 2e+1$	$\Phi^*_{ef}(p)$
10	8	5	7	–	r
9	8	$p \equiv 3, 5 \pmod 7$	7	–	r
8	8	$p \equiv 3, 5 \pmod 7$	7	–	r
7	4	7	5	–	r^2
	4	$p \equiv 3, 5 \pmod 7$	–	7	r
	4	$p \equiv 1, 2, 4 \pmod 7$	5	7	r
6	4	$p \geqslant 7$, $p \equiv \pm 2 \pmod 5$	5	–	r
5	4	$p \geqslant 7$, $p \equiv \pm 2 \pmod 5$	5	–	r
	6	$p \equiv \pm 2 \pmod 5$	5	–	r

Table 2. The remaining possibilities arising from Table 2 of [13].

If $\Phi^*_{ef}(p) = r$, then we can apply Lemma 6.1 as follows:

$\underline{r = e+1 \textbf{ case}}$**:** If $r = e+1$, then $f = 1$ by Lemma 6.2 and hence $\Phi^*_e(p) = e+1$. So $p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$. By looking at Table 2, we find that this case is only valid in the first three rows. We give a summary of the possibilities for p^e in the table below:

n	d	r	p^e
10	8	7	5^6
9	8	7	$3^6, 5^6$
8	8	7	$3^6, 5^6$

Table 3. The remaining possibilities in the case that $r = e+1$.

$\underline{r = 2e+1 \textbf{ case:}}$ If $r = 2e+1$, then by Table 2, we have $e = 3$. Also $2e+1 \equiv 1 \pmod{ef}$ and hence $f = 1, 2$. If $f = 1$, then $\Phi_e^*(p) = 2e+1$ which contradicts Lemma 6.1, as $e \neq 8, 20$. If $f = 2$, then $\Phi_{2e}^*(p) = 2e+1$, and we obtain from Lemma 6.1 that $p^{2e} = 3^6, 5^6$. We give a summary of the possibilities for this case in the table below:

n	d	r	p^e
7	4	7	3^3
7	4	7	5^3

TABLE 4. The remaining possibilities in the case that $r = 2e+1$.

So if $\Phi_{ef}^*(p) = r$, we have the five situations described in Tables 3 and 4. If $\Phi_{ef}^*(p) = r^2$, then we have from Table 2 that $n = 7$, $d = 4$, $p = 7$, $e = 4$, and $r = 25$. So for $f = 1, 2$, we can directly calculate $\Phi_e^*(p)$ and $\Phi_{2e}^*(p)$. These values are respectively 25 and 1201. Only the former value is valid and hence $f = 1$.

We now list the possibilities arising from Table 3 of [13]. Note that $n = 6, 7$ and so r^2 does not divide $n!$ for the values of r given in [13, Table 3], and hence $\Phi_{ef}^*(p) = r$. So we have two cases: either $f = 1$ and $\Phi_e^*(p) = e+1$, or $f = 1, 2$ and $\Phi_{ef}^*(p) = 2e+1$. In both cases we can apply Lemma 6.1. If $\Phi_{ef}^*(p) = 2e+1$, then $p^e = 2^5, 2^6, 2^9, 3^3, 5^3$ (if $f = 2$) or $p^e = 2^8, 2^{20}$ (if $f = 1$). In [13, Table 3], e only takes the values 3, 4, and 6. So we have $p^e = 2^6, 3^3, 5^3$. However, only one of these values correspond to those for which $r = 2e+1$, namely when $p^e = 5^3$ in the first line of Table 5. If $\Phi_e^*(p) = e+1$, then $p^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6, 5^6$. None of these values correspond to those for which $r = e+1$. Here is a summary of the possibilities arising from [13, Table 3].

G'	d	p	$r = e+1$	$r = 2e+1$	Possibilities
$3 \cdot A_7$	3	5	–	7	$f = 2$
	6	$p \equiv 1 \pmod 6$	5,7	–	None
$6 \cdot A_7$	6	$p \equiv 1, 7 \pmod{24}$	5,7	–	None
$3 \cdot A_6$	3	$p \equiv 1, 4 \pmod{15}$	–	5	None
	3	$p \neq 3, p \equiv \pm 2 \pmod 5$	–	5	None
$3 \cdot A_6$	6	$p \equiv 1 \pmod 6$	5	–	None
$6 \cdot A_6$	6	$p \equiv 1, 7 \pmod{24}$	5	–	None

TABLE 5. Possibilities arising from Table 3 of [13].

So in this case, we have that $G' = 3 \cdot A_7$, $d = e = 3$, $p = 5$, and $f = 2$.

(c) By using similar techniques to that above, we list the possibilities arising from Table 4 of [13]. Note that $n \leqslant 8$ and so $\Phi_{ef}^*(p) = r$ in all cases.

n	d	p	$r = e+1$	$r = 2e+1$	Possibilities
8	4	2	5	7	$q^e = p^e = 2^4$, $q^e = p^e = 2^3$
7	4	2	5	7	$q^e = p^e = 2^4$, $q^e = p^e = 2^3$
	8	5	7	–	$q^e = p^e = 5^6$

TABLE 6. Possibilities arising from Table 4 of [13].

We will now give a demonstrative example of how these possibilities arise. Consider the third line of [13, Table 4], where $n = 7$, $d = 8$, $p = 5$, and $r = e+1 = 7$. Now $\Phi_{ef}(p) = e+1$ and so by Lemma 6.2, we have that $f = 1$. Hence only the case $q^e = p^e = 5^6$ arises (which also satisfies Lemma 6.1). In the cases where no possibilities exist, the possible values of q^e were in contradiction to Lemma 6.1.

Sporadic simple group case:

In this case, we run through Table 5 of [13]. For each case, S, $\mathrm{Aut}(S)$, and their orders are known (see the ATLAS [8]). Since $\Phi_{ef}^*(p)$ divides $|G|$, we check to see whether nontrivial powers of r divide $|\mathrm{Aut}(S)|$, and then surmise whether $\Phi_{ef}^*(p) = r$ or not. In all cases, from inspecting the order of $\mathrm{Aut}(S)$, it turns out that $\Phi_{ef}^*(p) \in \{e+1, 2e+1\}$. Thus Lemma 6.1 applies and in some cases, we have no possibilities arising as the value of p and e do not match. Here we recast Table 5 of [13] together with the values of p, q, and e which are possible in each case.

G'	d	$r=e+1$	$r=2e+1$	Possibilities	G'	d	$r=e+1$	$r=2e+1$	Possibilities
M_{11}	5	5	11	$q^e=p^e=3^4$	M_{24}	11	11	23	$q^e=p^e=2^{10}$
	10	11	–	$q^e=p^e=2^{10}$		23	23	–	None
	11	11	–	None	J_1	20	19	–	$q^e=p^e=2^{18}$
M_{12}	10	11	–	$q^e=p^e=2^{10}$	$2\cdot J_2$	6	7	–	$q^e=p^e=5^6$
	11	11	–	None	$3\cdot J_3$	9	–	19	$q^e=p^{2e}=2^{18}$
$2\cdot M_{12}$	6	5	11	$q^e=p^e=3^4$		18	17, 19	–	None
	10	11	–	None	Co_3	23	23	–	None
	12	11	–	None	Co_2	23	23	–	None
M_{22}	10	11	–	$q^e=p^e=2^{10}$	$2\cdot Co_1$	24	23	–	None
$2\cdot M_{22}$	10	11	–	$q^e=p^e=2^{10}$	Ru	28	29	–	None
$3\cdot M_{22}$	6	–	11	$q^e=p^{2e}=2^{10}$	$2\cdot Ru$	28	29	–	None
M_{23}	11	11	23	$q^e=p^e=2^{10}$	$6\cdot Suz$	12	11, 13	–	None
	22	23	–	None					

TABLE 7. Possibilities arising from Table 5 of [13].

Cross-characteristic case:

Here we derive the possibilities arising from Table 7 of [13]. In all cases below, r^2 does not divide $|\mathrm{Aut}(S)|$, and hence $\Phi^*_{ef}(p)=r$.

G'	d	p	r	Possibilities
$2\cdot \mathrm{Sz}(8)$	8	5	$e+1=7$	$q^e=p^e=5^6$
$\mathrm{Sz}(8)$	14	$p\equiv 1 \pmod 4$	$e+1=13$	None
$G_2(3)$	14	–	$e+1=13$	$q^e=p^e=2^{12}$
$2\cdot G_2(3)$	12	$p>2$	$e+1=13$	None
$2\cdot \Omega_8^+(2)$	8	$p>2$	$e+1=7$	$q^e=p^e=3^6,5^6$
$\mathrm{Sp}_6(2)$	7	$p>2$	$e+1=5,7$	$q^e=p^e=3^4,3^6,5^6$
$2\cdot \mathrm{Sp}_6(2)$	8	$p>2$	$e+1=7$	$q^e=p^e=3^6,5^6$
$\mathrm{Sp}_4(4)$	18	$p>2$	$e+1=17$	None
$2\cdot \mathrm{PSU}_4(2^2)\cong \mathrm{Sp}_4(3)$	4	$p\equiv 1 \pmod 6$	$e+1=5$	None
$\mathrm{PSU}_4(2^2)\cong \mathrm{PSp}_4(2)$	5	$p\equiv 1 \pmod 6$	$e+1=5$	None
	6	$p>5$	$e+1=5$	None
$6\cdot \mathrm{PSU}_4(3^2)$	6	$p\equiv 1 \pmod 6$	$e+1=5,7$	None
$4\cdot \mathrm{PSL}_3(4)$	4	3	$2e+1=7$	$q^{2e}=p^e=3^6$
	8	$p=5$, or $p\equiv 1,9 \pmod{20}$	$e+1=7$	$q^e=p^e=5^6$
$2\cdot \mathrm{PSL}_3(4)$	6	3	$e+1=5,7$	$q^e=p^e=3^4,3^6$
$6\cdot \mathrm{PSL}_3(4)$	6	$p\equiv 1 \pmod 6$	$e+1=5,7$	None

TABLE 8. Possibilities arising from Table 7 of [13].

Here we investigate the possibilities arising from Table 8 of [13]. We split this case into 5 parts, but first we make a general observation which we use in each case. We leave the proof to the reader.

Lemma 6.3. *Let r be a primitive prime divisor of s^n-1, let ℓ be a positive integer, and let z be a multiple of r such that $z/r=k(s-1)(s^2-1)\cdots(s^j-1)$ where k is coprime to r and $j<n$. If r^ℓ divides z, then $\ell=1$.*

(a) $S=\mathrm{PSL}_n(s)$, $n\geqslant 3$, $d=\frac{s^n-1}{s-1}-1, \frac{s^n-1}{s-1}$, $r=e+1=\frac{s^n-1}{s-1}$, n is prime.

Since n is an odd prime, Zsigmondy's Theorem implies that there exists a primitive prime divisor r' of s^n-1. Since r' divides $(s^n-1)/(s-1)$, it follows that $r=r'$ as r is prime. Therefore, r is a primitive prime divisor of s^n-1. Also, $|\mathrm{Out}(S)|=2y\gcd(n,s-1)$ where $s=s_0^y$ for some prime s_0 and positive integer y. Since n is prime, we have that $|\mathrm{Out}(S)|=2y$ or $|\mathrm{Out}(S)|=2yn$. Suppose r divides $|\mathrm{Out}(S)|$. Now r is an odd prime, and so r divides $|\mathrm{Out}(S)|/2$. Then $\frac{s^n-1}{s-1}$ divides ny. This implies that $\frac{s^n-1}{s-1}\leqslant ny$ and hence $s_0^{(n-1)y}<ny$. Now it is easy to prove by induction that $ny\leqslant 2^{(n-1)y}$ for all $y\geqslant 1$, and so $s_0^{(n-1)y}<2^{(n-1)y}$, which is a contradiction as $s_0\geqslant 2$. Therefore r does not divide $|\mathrm{Out}(S)|$ and $\Phi^*_{ef}(p)$ divides $|S|$ (as $|\mathrm{Aut}(S)|=|S||\mathrm{Out}(S)|$). Now $\Phi^*_{ef}(p)$ is a power of r, but by Lemma 6.3, we have that $\Phi^*_{ef}(p)=r$ as $|S|/r=s^{n(n-1)/2}(s-1)(s^2-1)\cdots(s^{n-1}-1)$.

By Lemma 6.2 we have $f=1$, and by Lemma 6.1, $e\in\{4,6,10,12,18\}$. Note that $s\frac{s^{n-1}-1}{s-1}=e$. Now s is a proper nontrivial divisor of e, and $s^{n-1}=\frac{e}{s}(s-1)+1$. So $\frac{e}{s}(s-1)+1$ is the power of an integer. We have the following calculations

e	s	$\frac{e}{s}(s-1)+1$	e	s	$\frac{e}{s}(s-1)+1$
4	2	3		4	10
6	2	4		6	11
	3	5	18	2	10
10	2	6		3	13
	5	9		6	16
12	2	7		9	17
	3	9			

So the only possible choices for q, e, s, and n are

$$(q,e,s,n) \in \{(3,6,2,3),(5,6,2,3),(2,12,3,3)\}.$$

(b) $S = \mathrm{PSU}_n(s^2)$, $n \geqslant 3$, $d = \frac{s^n+1}{s+1} - 1, \frac{s^n+1}{s+1}$, $r = e+1 = \frac{s^n+1}{s+1}$, n is prime.

Since n is an odd prime, Zsigmondy's Theorem implies that there exists a primitive prime divisor r' of $s^{2n}-1$. So $r' = r$ as r' divides $(s^n+1)/(s+1) = r$. Therefore r is a primitive prime divisor of $s^{2n}-1$. Also, $|\mathrm{Out}(S)| = 2y\gcd(n, s+1)$ where $s = s_0^y$ for some prime s_0 and positive integer y. Since n is prime, we have that $|\mathrm{Out}(S)| = 2y$ or $|\mathrm{Out}(S)| = 2yn$. Suppose r divides $|\mathrm{Out}(S)|$. Since Now r is an odd prime, r divides $|\mathrm{Out}(S)|/2$. So $\frac{s^n+1}{s+1}$ divides ny and hence $\frac{s^{2n}-1}{s^2-1} \leqslant ny$. Thus $s_0^{2(n-1)y} < ny$. We have $s_0^{2(n-1)y} < 2^{(n-1)y} \leqslant 2^{2(n-1)y}$, which is a contradiction as $s_0 \geqslant 2$. Therefore r does not divide $|\mathrm{Out}(S)|$ and $\Phi^*_{ef}(p)$ divides $|S|$.

Now $\Phi^*_{ef}(p)$ is a power of r, but by Lemma 6.3, we have that $\Phi^*_{ef}(p) = r$ as $|S|/r$ divides $(s^2-1)(s^4-1)\cdots(s^{2n-4}-1)$. (Note that we must apply Lemma 6.3 with s^2 in place of s.) Hence $\Phi^*_{ef}(p) = r$.

By Lemma 6.2 we have $f = 1$, and by Lemma 6.1, $e \in \{4,6,10,12,18\}$. Note that $s\frac{s^{n-1}-1}{s+1} = e$. Now s is a proper nontrivial divisor of e, and $s^{n-1} = \frac{e}{s}(s+1)+1$. So $\frac{e}{s}(s+1)+1$ is the power of an integer. We have the following calculations

e	s	$\frac{e}{s}(s+1)+1$	e	s	$\frac{e}{s}(s+1)+1$
4	2	7	12	4	16
6	2	10		6	15
	3	9	18	2	28
10	2	16		3	25
	5	13		6	22
12	2	19		9	21
	3	17			

Recall that p does not divide s and so $(q,e,s,n) = (5,6,3,3)$.

(c) $S = \mathrm{PSp}_{2n}(s)$, $d = \frac{1}{2}(s^n-1), \frac{1}{2}(s^n+1)$, $r = e+1 = \frac{1}{2}(s^n+1)$, s is odd, $n = 2^b \geqslant 2$.

Since $n > 2$, Zsigmondy's Theorem implies that there exists a primitive prime divisor r' of $s^{2n}-1$. So r' divides s^n+1 and so $r = \frac{1}{2}(s^n+1)$ divides r'. Since r' is prime, we have that $r = r'$ and hence r is a primitive prime divisor of $s^{2n}-1$. Also, $|\mathrm{Out}(S)| = 2y$ where $s = s_0^y$ for some prime s_0 and positive integer y. Suppose r divides $|\mathrm{Out}(S)|$. Now r is an odd prime, and so r divides y. Then $\frac{1}{2}(s^n+1)$ divides y. This implies that $s^n+1 \leqslant 2y$ and hence $s_0^{nf} < 2y$. Now it is easy to prove by induction that $w \leqslant 2^w$ for all $w \geqslant 1$, and so $s_0^{ny} < 2^{y+1} \leqslant 2^{ny}$, which is a contradiction as $s_0 > 2$. Therefore r does not divide $|\mathrm{Out}(S)|$ and $\Phi^*_{ef}(p)$ divides $|S|$.

Now $\Phi^*_{ef}(p)$ is a power of r, but by Lemma 6.3, we have that $\Phi^*_{ef}(p) = r$ as $|S|/r = 2s^{n^2}(s^4-1)(s^6-1)\cdots(s^{2n-2}-1)$. (Note that we have applied Lemma 6.3 with s^2 in place of s). By Lemma 6.2 we have $f = 1$, and by Lemma 6.1, $e \in \{4,6,10,12,18\}$. Note that $\frac{1}{2}(s^n+1)-1 = e$, and thus $s^n = 2e+1$. Therefore $(q,e,s,n) = (2,12,5,2)$.

(d) $S = \mathrm{PSp}_{2n}(3)$, $d = \frac{1}{2}(3^n-1), \frac{1}{2}(3^n+1)$, $r = e+1 = \frac{1}{2}(3^n-1)$, n an odd prime.

By Zsigmondy's Theorem, there exists a primitive prime divisor r' of $3^{2n}-1$. Clearly r does not divide $|\mathrm{Out}(S)|$ as $|\mathrm{Out}(S)| = 2$. Therefore $\Phi^*_{ef}(p)$ divides $|S|$, and by a similar argument as that for $S = \mathrm{PSp}_n(s)$ above, we have $\Phi^*_{ef}(p) = r = e+1$. By Lemma 6.2 we have $f = 1$, and by Lemma 6.1, $e \in \{4,6,10,12,18\}$. Note that $\frac{1}{2}(3^n+1)-1 = e$, and thus $3^n = 2e+1$, where n is an odd prime. There are no solutions for this equation and so this case cannot occur.

(e) $\mathrm{PSL}_2(s)$, $s \geqslant 7$. In this case, we have that $r \in \{s-1, s+1, s, \frac{1}{2}(s-1), \frac{1}{2}(s+1)\}$.

Now $|L_2(s)| = \frac{1}{2}s(s-1)(s+1)$ and so r^2 does not divide $|L_2(s)|$. Therefore $\Phi^*_{ef}(p) = r$. There are five subcases to deal with here.

(i) $d = s-1, s, s+1$, $r = e+1 = s-1$, $s = 2^c$, c is prime: Here $e = 6$ as $e \in \{4,6,10,12,18\}$ and $s = e+2$ is a prime power of 2. So the only possible choices for q, e, and s are $(q,e,s) \in \{(3,6,8),(5,6,8)\}$.

(ii) $d = s, s+1$, $r = e+1 = s+1$, $s = 2^c$, $c = 2^{c'}$: Here $e = s \geqslant 7$ and none of the possible values for e (which are 10, 12, and 18) are powers of 2. Therefore, this case cannot occur.

(iii) $d = s-1, s, s+1$, $r = e+1 = s$, s is prime: By Lemma 6.1, the possible choices for q and $e = s-1$ are $(q, e) \in \{(2, 10), (2, 12), (2, 18), (3, 6), (5, 6)\}$.

(iv) $d = \frac{1}{2}(s-1), \frac{1}{2}(s+1)$, $r = 2e+1 = s$, s is prime: Since $\Phi^*_{ef}(p) = 2e+1$, we have that $f = 1$ or $f = 2$. If $f = 1$, then by Lemma 6.1, we have $q^e = p^e = 2^3, 2^8, 2^{20}$. If $f = 2$, then by Lemma 6.1, we have $q^e = p^{2e} = 2^{10}, 2^{12}, 2^{18}, 3^6, 5^6$. So the possibilities for q and $e = \frac{1}{2}(s-1)$ are $(q, e) \in \{(4, 5), (4, 6), (4, 9), (9, 3), (25, 3), (2, 3), (2, 8), (2, 20)\}$.

(v) $d = \frac{1}{2}(s-1), \frac{1}{2}(s+1)$, s is odd. We have that $r = e+1$ and two subcases; $r = \frac{1}{2}(q-1)$ and when $r = \frac{1}{2}(s+1)$. First note that by Lemma 6.2, we have $f = 1$. If $r = \frac{1}{2}(s-1)$, then by Lemma 6.1, the possible choices for q and $e = \frac{1}{2}(s-1)-1$ are $(q, e) \in \{(2, 4), (3, 4), (2, 10), (2, 12)\}$. If $r = \frac{1}{2}(s+1)$, then by Lemma 6.1, the possible choices for q and $e = \frac{1}{2}(s+1)-1$ are $(q, e) \in \{(2, 4), (2, 12), (2, 18), (3, 6), (5, 6)\}$.

Here is a table which summarises the valid cases obtained from Table 8 of [13].

Case	S	d	e	q	Case	S	d	e	q	Case	S	d	e	q
(a)	$\mathrm{PSL}_3(2)$	6,7	6	3,5	(e)(iv)	$\mathrm{PSL}_2(11)$	5,6	5	4	(e)(v)	$\mathrm{PSL}_2(11)$	5,6	4	2,3
	$\mathrm{PSL}_3(3)$	12,13	12	2		$\mathrm{PSL}_2(13)$	6,7	6	4		$\mathrm{PSL}_2(23)$	11,12	10	2
(b)	$\mathrm{PSU}_3(3^2)$	6,7	6	5		$\mathrm{PSL}_2(19)$	9,10	9	4		$\mathrm{PSL}_2(27)$	13,14	12	2
(c)	$\mathrm{PSp}_4(5)$	12,13	12	2		$\mathrm{PSL}_2(7)$	3,4	3	9		$\mathrm{PSL}_2(9)$	4,5	4	2
(e)(i)	$\mathrm{PSL}_2(8)$	7,8,9	6	3,5		$\mathrm{PSL}_2(7)$	3,4	3	25		$\mathrm{PSL}_2(25)$	12,13	12	2
(e)(iii)	$\mathrm{PSL}_2(11)$	10,11,12	10	2		$\mathrm{PSL}_2(7)$	3,4	3	2		$\mathrm{PSL}_2(37)$	18,19	18	2
	$\mathrm{PSL}_2(13)$	12,13,14	12	2		$\mathrm{PSL}_2(17)$	8,9	8	2		$\mathrm{PSL}_2(13)$	6,7	6	3,5
	$\mathrm{PSL}_2(19)$	18,19,20	18	2		$\mathrm{PSL}_2(41)$	20,21	20	2					
	$\mathrm{PSL}_2(7)$	6,7,8	6	3,5										

TABLE 9. Possibilities arising from Table 8 of [13].

However, not all of the above cases have valid absolutely irreducible representations. For example, $\mathrm{PSL}_2(13)$ (or a cover thereof) does not have an absolutely irreducible 12-dimensional representation over GF(2). We use [17], [8], and [16, Table 2] to eliminate those representations above that do not exist, and so arrive at the following list of possibilities arising from Table 8 of [13].

Case	S	d	e	q	Case	S	d	e	q	Case	S	d	e	q
(a)	$\mathrm{PSL}_3(2)$	6,7	6	3,5	(e)(iv)	$\mathrm{PSL}_2(11)$	5	5	4	(e)(v)	$\mathrm{PSL}_2(23)$	11	10	2
	$\mathrm{PSL}_3(3)$	12	12	2		$\mathrm{PSL}_2(13)$	6	6	4		$\mathrm{PSL}_2(9)$	4	4	2
(b)	$\mathrm{PSU}_3(3^2)$	6,7	6	5		$\mathrm{PSL}_2(19)$	9	9	4		$\mathrm{PSL}_2(25)$	12	12	2
(c)	$\mathrm{PSp}_4(5)$	12	12	2		$\mathrm{PSL}_2(7)$	3,4	3	9		$\mathrm{PSL}_2(37)$	18	18	2
(e)(i)	$\mathrm{PSL}_2(8)$	7	6	3		$\mathrm{PSL}_2(7)$	3,4	3	25		$\mathrm{PSL}_2(13)$	6,7	6	3
		7,8	6	5		$\mathrm{PSL}_2(7)$	3	3	2					
(e)(iii)	$\mathrm{PSL}_2(11)$	10	10	2		$\mathrm{PSL}_2(17)$	8	8	2					
	$\mathrm{PSL}_2(13)$	14	12	2		$\mathrm{PSL}_2(41)$	20	20	2					
	$\mathrm{PSL}_2(19)$	20	18	2										
	$\mathrm{PSL}_2(7)$	6,7	6	3										
		6,7,8	6	5										

Natural-characteristic case:

Here $q = q_0^c$. We will show that c is at most 2 and has the following values in each of the cases below:

$G^{(\infty)}$	d	e	p	c	$G^{(\infty)}$	d	e	p	c
$\mathrm{SL}_2(q_0^3)$	8	6	–	1		6	6	$p = 2$	1
$\mathrm{SL}_3(q_0^2)$	9	6	$q_0 \equiv 1 \pmod 3$	1	$\mathrm{PSU}_3(q_0^2)$	8	6	$p \neq 3$	1
$\mathrm{PSL}_3(q_0^2)$	9	6	$q_0 \neq 1 \pmod 3$	1		7	6	$p = 3$	1
$2 \cdot \Omega_7(q_0)$	8	6	p odd	1	$\mathrm{Sz}(q_0)$	4	4	$p = 2$	1,2
$\mathrm{Sp}_6(q_0)$	8	6	$p = 2$	1	${}^2G_2(q_0)$	7	6	$p = 3$	1,2
$G_2(q_0)$	7	6	p odd	1					

TABLE 10. Possibilities arising from Table 6 of [13].

We know that $\Phi^*_{ef}(p)$ divides $|G|$ and $G/(G \cap Z)$ is a subgroup of $\mathrm{Aut}(S)$. So $\Phi^*_{ef}(p)$ divides $|Z||S||\mathrm{Out}(S)|$. Now $|Z| = q-1$ and thus $\Phi^*_{ef}(p)$ divides $|S||\mathrm{Out}(S)|$. Here is a list of the values of $|\mathrm{Out}(S)|$ corresponding to Table 10:

S	$\lvert\mathrm{Out}(S)\rvert$	e	S	$\lvert\mathrm{Out}(S)\rvert$	e
$\mathrm{PSL}_2(q_0^3)$	$3f/c$ or $6f/c$	6	$G_2(q_0)$	f/c or $2f/c$	6
$\mathrm{PSL}_3(q_0^2)$	$4f/c$	6	$\mathrm{PSU}_3(q_0^2)$	$2f/c$ or $6f/c$	6
$\mathrm{P}\Omega_7(q_0)$	$2f/c$	6	$\mathrm{Sz}(q_0)$	$2f/c+1$	4
$\mathrm{PSp}_6(q_0)$	f/c	6	${}^2G_2(q_0)$	$2f/c+1$	6

TABLE 11. List of values of $|\mathrm{Out}(S)|$ corresponding to Table 10.

Recall that r is a primitive prime divisor of $p^{ef}+1$ and so r is at least $ef+1$. Since $c \geqslant 1$ it follows from the table above that r is coprime to $|\mathrm{Out}(S)|$ for all S in the table above. Thus r divides $|S|$. From this argument, it also follows that $\Phi^*_{ef}(p)$ divides $|S|$. For $S = \mathrm{PSL}_2(q_0^3)$, we see that $|S| = q_0^3(q_0^6-1)/2 = p^{3f/c}(q^{6f/c}-1)/2$. So since $\Phi^*_{6f}(p)$ divides $|S|$, it follows that $c = 1$. Similarly, we have $c = 1$ for for the other cases, except $S = \mathrm{Sz}(q_0)$, ${}^2G_2(q_0)$, where the analogous argument yields $c \leqslant 2$.

7. Proof of Theorem 3.2

In proving Theorem 3.2, we will need to examine the case where the transitive group admitted contains a large classical group.

Lemma 7.1. *Let $q = p^f$ where p is a prime and f is a positive integer, and let d be an integer greater than 4. Let G be a subgroup of $\mathrm{GL}_d(q)$, let S be a normal subgroup of G, and suppose S is one of the following:*

S	*Condition*
$\mathrm{SL}_d(q)$	–
$\mathrm{Sp}_d(q)$	–
$\mathrm{SU}_d(q)$	*q is a square*
$\Omega^{\pm}_d(q) \trianglelefteq G$	*d even*
$\Omega_d(q) \trianglelefteq G$	*dq odd*

If G acts transitively of degree n, and n does not divide $2(q-1)\gcd(2,q-1)$, then

$$n > \frac{(q^{d/2}+1)(q^{d/2-1}-1)}{q-1}.$$

Proof. Let H be a point stabiliser in the action of G. If $S \leqslant H$ and $G \leqslant F \leqslant \mathrm{GL}_d(q)$, then $|F:S| = |F:G| \cdot |G:H| \cdot |H:S|$ and hence n divides $|F:S|$. Now

$$\begin{aligned}
|\mathrm{GL}_d(q) : \mathrm{SL}_d(q)| &= q-1 \\
|\mathrm{GSp}_d(q) : \mathrm{Sp}_d(q)| &= q-1 \\
|\mathrm{GU}_d(q) : \mathrm{SU}_d(q)| &= \sqrt{q}+1 \\
|\mathrm{GO}_d(q) : \Omega_d(q)| &= 2(q-1) \\
|\mathrm{GO}^{\pm}_d(q) : \Omega^{\pm}_d(q)| &= 2(q-1)\gcd(2,q-1)
\end{aligned}$$

and n does not divide these indices. Therefore $S \not\leqslant H$. Note that

$$|G:H| = |G:HS||S:S\cap H| \geqslant |S:S\cap H|.$$

We will use this fact throughout.

Suppose we have the first case, $S = \mathrm{SL}_d(q) \leqslant G \leqslant \mathrm{GL}_d(q)$. Since $d > 4$, we have by [9] that the minimum degree of a nontrivial permutation representation of S is $(q^d-1)/(q-1)$. So in particular, we have that $|S:S\cap H| \geqslant (q^d-1)/(q-1)$, and thus $|G:H| \geqslant (q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$.

Now suppose $S = \mathrm{Sp}_d(q) \trianglelefteq G$. Assume firstly that $q > 2$. Then by [9] the minimum degree of a nontrivial permutation representation of S is $q^{d-1}/(q-1)$. So in particular, we have that $|S:S\cap H| \geqslant q^{d-1}/(q-1)$. So again, we have $|G:H| \geqslant (q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$. Now if $q = 2$, we have from [9] that the minimum degree of $\mathrm{Sp}_d(2)$ is $2^{d/2-1}(2^{d/2}-1)$, which is greater than $|G:H| \geqslant (2^{d/2}+1)(2^{d/2-1}-1)$.

Now consider the case that $S = \mathrm{SU}_d(q) \trianglelefteq G$ where q is a square. Then by [9], we have that the minimum degree of S is $(q^{d/2}-(-1)^d)(q^{d/2-1}-(-1)^{d-1})/(q-1)$. If d is even, then

$$(q^{d/2}-(-1)^d)(q^{d/2-1}-(-1)^{d-1}) = (q^{d/2}-1)(q^{d/2-1}+1)$$

which is clearly larger than $(q^{d/2}+1)(q^{d/2-1}-1)$. If d is odd, then

$$(q^{d/2}-(-1)^d)(q^{d/2-1}-(-1)^{d-1}) = (q^{d/2}+1)(q^{d/2-1}-1)$$

and hence we obtain equality in the bound here. So overall, we have $n \geqslant (q^{d/2}+1)(q^{d/2-1}-1)$.

We turn now to the last case, $S = \Omega_d^\epsilon(q) \trianglelefteq G$. Assume that $d > 6$. By [9], we have the following possible minimum degrees of S:

$\Omega_d(q)$, q odd, $d > 5$	$(q^{d-1}-1)/(q-1)$
$\Omega_d^+(q)$, $q > 2$	$(q^{d/2}-1)(q^{d/2-1}+1)/(q-1)$
$\Omega_d^+(2)$	$2^{d/2-1}(2^{d/2}-1)$
$\Omega_d^-(q)$	$(q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$

Note, $\Omega_5(q)$ (q odd) is isomorphic to $\mathrm{Sp}_4(q)$. In each case, it is clear that the minimum degree of S is at least $(q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$. In fact, $\Omega_d(q)$ has the same minimum degree as $\mathrm{PSU}_d(q)$ when q is square and d is odd, $\Omega_d^+(q)$ has the same minimum degree as $\mathrm{PSU}_d(q)$ when q is square and d is even, $\Omega_d^+(2)$ has the same minimum degree as $\mathrm{Sp}_d(2)$, and the last case, $\Omega_d^-(q)$ attains equality in the bound.

Now suppose $d = 6$ and $S = \Omega_d^\pm(q)$. Note that the minimum degree of $\Omega_d^\pm(q)$ is at least the minimum degree of $\mathrm{P}\Omega_d^\pm(q)$. By [9] we have the following information:

S	Minimum Degree
$\mathrm{P}\Omega_6^+(2)$	8
$\mathrm{P}\Omega_6^+(q)$, $q \neq 2$	q^3+q^2+q+1
$\mathrm{P}\Omega_6^-(q)$	$(q+1)(q^3+1)$

Note that $(q^{d/2}+1)(q^{d/2-1}-1) = (q^3+1)(q^2-1)$, which is greater than each minimum degree in the table above, which concludes the proof. □

Now we proceed to prove Theorem 3.2. First note that as $\Phi_e^*(q)$ divides q^e-1 but does not divide $q^{e/2}-1$, we have that $\Phi_e^*(q)$ divides $q^{e/2}+1$ and hence $\Phi_e^*(q)$ also divides $(q^{e/2}+1)/x$. Since $e > 2$ and $(q,e) \neq (2,6)$, we know by Zsigmondy's Theorem that $\Phi_e^*(q) > 1$ and hence we can apply Theorem 3.1.

Classical examples:

Suppose $S \in \{\mathrm{SL}_d(q), \mathrm{Sp}_d(q), \mathrm{SU}_d(q), \Omega_d^\epsilon(q)\}$ with appropriate conditions on d and q, and suppose $S \trianglelefteq G \leqslant \mathrm{GL}_d(q)$. Assume for the moment that $d > 4$. Since $\Phi_e^*(q)$ divides $(q^{e/2}+1)/x$, we have that $(q^{e/2}+1)/x$ does not divide $2(q-1)\gcd(2,q-1)$. So by Lemma 7.1, we have $(q^{e/2}+1)/x \geqslant (q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$. However, this implies that $q^{d/2}+1 \geqslant (q^{d/2}+1)(q^{d/2-1}-1)/(q-1)$ and hence $q-1 \geqslant q^{d/2-1}-1$. So $1 \geqslant d/2-1$, which is impossible as $d > 4$. Therefore, $d \leqslant 4$.

Suppose we have the first case, $S = \mathrm{SL}_d(q) \leqslant G \leqslant \mathrm{GL}_d(q)$. If $(d,q) = (4,2)$, then by [9], the minimum degree of S is 8. However, $q^{d/2}+1 = 5$ and so we obatin a contradiction. So (d,q) is not $(4,2)$. Then by [9], the minimum degree of a nontrivial permutation representation of S is $(q^d-1)/(q-1)$. So in particular, we have that $|S : S \cap H| \geqslant (q^d-1)/(q-1)$. Thus

$$|G : HS| \leqslant \frac{q^{e/2}+1}{(q^d-1)/(q-1)} = \frac{(q^{e/2}+1)(q-1)}{q^d-1}.$$

Now $q^{e/2-1}-1 \leqslant q^{d-2}+q^{d-3}+\cdots+q+1 = \frac{q^{d-1}-1}{q-1}$ and hence $q^{e/2}-q^{e/2-1}+q+1 = (q-1)(q^{e/2-1}-1) \leqslant q^{d-1}-1$. Therefore $q^{e/2+1}-q^{e/2}+q \leqslant q^d-1$ and thus $(q^{e/2}+1)(q-1) \leqslant q^d-1$. So $G = HS$ and it also follows that $e = 2$ and $d = 3$; a contradiction. Therefore we have ruled out the first case of examples of classical type.

Now suppose $S = \mathrm{Sp}_d(q) \trianglelefteq G$ (so $d = 4$ and $3 \leqslant e \leqslant 4$). Suppose that $q > 3$. Then by [9] the minimum degree of a nontrivial permutation representation of S is $q^3/(q-1)$. So in particular, we have that $|S : S \cap H| \geqslant q^3/(q-1)$. Thus

$$|G : HS| \leqslant \frac{(q^{e/2}+1)(q-1)}{q^3} \leqslant \frac{(q^2+1)(q-1)}{q^3}$$

which is clearly a contradiction. So $q \in \{2,3\}$. By [9], the minimum degree of $\mathrm{Sp}_4(3)$ is 27. So $27 \leqslant q^{e/2}+1 = 3^{e/2}+1$, but $3^{e/2}+1 \leqslant 3^2+1$, which is a contradiction. In the case that $q = 2$, we know that $\mathrm{Sp}_4(2) \cong S_6$, and hence S does not have a subgroup of index dividing $(q^{e/2}+1)/x$. Therefore we have ruled out the second case of examples of classical type.

Now consider the case that $S = \mathrm{SU}_d(q) \trianglelefteq G$ where q is a square. Then by [9], we have the following information for the minimum degrees of S:

$\mathrm{SU}_3(q)$, $q \neq 4, 25$	$q^{3/2}+1$
$\mathrm{SU}_3(2^2)$	2
$\mathrm{SU}_3(5^2)$	50
$\mathrm{SU}_4(q)$	$(q^{1/2}+1)(q^{3/2}+1)$

We begin at the end of the table and work upwards. Now $(q^{1/2}+1)(q^{3/2}+1) > q^2+1$ and hence we have that $S \neq \mathrm{SU}_4(q)$. For the $S = \mathrm{SU}_3(5^2)$ case, we search a little further and we use the Atlas [8] to deduce that the two smallest degrees of the quotient $\mathrm{PSU}_3(5^2)$ are 150 and 1000. Since $\mathrm{SU}_3(5^2)$ is a 3-cover of $\mathrm{PSU}_3(5^2)$, we see that the second largest degree of $\mathrm{SU}_3(5)$ is greater than $126 = q^{3/2}+1$. Since 50 is not a divisor of 126, we see that this case does not arise. Similarly, we can rule out the case $S = \mathrm{SU}_3(2^2)$. We are left with the case that $S = \mathrm{SU}_3(q)$ $(q \neq 2, 5)$ which does arise.

Now we turn to the fourth case, $d = 4$ and $S = \Omega_4^{\pm}(q)$. Now, $\Omega_4^+(q)$ has order $(2, q-1)q^2(q^2-1)^2/4$, which is clearly coprime to $\Phi_e^*(q)$. Therefore, we must have $S = \Omega_4^-(q)$. Moreover, the minimum degree of S is q^2+1 and so $(q^{e/2}+1)/x \geqslant q^2+1$. This implies that $(q^{d/2}+1)/x \geqslant q^2+1$, and hence $x = 1$, as $d = 4$. Note also that $e = 4$ as the greatest common divisor of q^2+1 and q^3-1 is 1 or 2 (depending on whether q is even or odd respectively).

Reducible examples:

Now $|G^U : H^U| = |G : H|/|G_{(U)} : H_{(U)}|$ and $|G_{(U)} : H_{(U)}|$ divides

$$q^{d(d-m)}|\mathrm{GL}_{d-m}(q)| = q^{(d-m)(3d-m-1)/2}(q-1)(q^2-1)\cdots(q^{d-m}-1).$$

So $\Phi_e^*(q)$ is coprime to $|G_{(U)} : H_{(U)}|$ and hence G^U has a subgroup of index $(q^{e/2}+1)/y$, with $\Phi_e^*(q)$ coprime to y.

Imprimitive examples: Firstly, we apply the condition $d-2 \leqslant e \leqslant d$, which rules out many subcases. If $q = 2$, then $\mathrm{GL}_1(q) \wr S_d \cong S_d$ and G can be identified with a primitive subgroup of S_d. By using GAP, and its library of primitive groups of small degree, we know the isomorphism type of G. By knowledge of the maximal subgroups of small degree in A_n and S_n (see [11, Theorem 5.2A]), we can establish that cases can only arise if $e = 4$. Therefore $q^{e/2}+1 = 5$ and hence $x = 1$. Moreover, the only primitive groups of degree 5 and 6 which have a subgroup of index $(q^{e/2}+1)/x$ are $\mathbb{Z}_5$, $\mathbb{Z}_5 : 2$, $\mathbb{Z}_5 : 4$, A_5, and S_5.

Extension field examples:

(a) Now $|\mathrm{GL}_1(q^d) \cdot d| = (q^d-1)d = (q^{e+1}-1)(e+1)$ and so $q^{e/2}+1$ does not divide $(q^d-1)d$ if $(q, e) \in \{(2, 10), (2, 12), (2, 18), (3, 6), (5, 6)\}$, and so $q^{e/2}+1$ does not divide $(q^d-1)d$ for these values of (q, e). Therefore $(q, e) = (2, 4)$ or $(3, 4)$. Now if $q = 2$, then x divides 5 but $\Phi_e^*(q) = 5$, which implies that $x = 1$. If $q = 3$, then x divides 10, and hence $x \in \{1, 2\}$ as again $\Phi_e^*(q) = 5$.

(b) This is mostly unchanged from Theorem 3.1 except we know that

$$|G \cap \mathrm{GL}_{d/b}(q^b) : H \cap \mathrm{GL}_{d/b}(q^b)| = \frac{(q^{e/2}+1)}{xy}$$

where $y = |G \cdot \mathrm{GL}_{d/b}(q^b) : H \cdot \mathrm{GL}_{d/b}(q^b)|$. Now y is a divisor of b and hence $\Phi_{e/b}^*(q^b)$ is coprime to y. So $G \cap \mathrm{GL}_{d/b}(q^b)$ has a subgroup of index $(q^{e/2}+1)/xy$ and xy is coprime to $\Phi_{e/b}^*(q^b)$.

Symplectic type examples:

Unchanged from Theorem 3.1, except that in the first case we find by computer that G is cyclic of order 10 and H is its trivial subgroup.

Nearly simple case:

Alternating group case:

(a) Permutation module examples: Recall from Theorem 3.1 that $A_n \leqslant G \leqslant S_n \times Z$, where Z is the subgroup of scalar matrices in $\mathrm{GL}_d(q)$, and d is $n-1$ or $n-2$ according to whether p does not or does divide n respectively. For $q^e = 2^{10}, 2^{12}, 2^{18}$, we have the following possibilities for d and n:

q^e	d	n	q^e	d	n
2^{10}	10	11		14	15
		12			16
	12	13	2^{18}	18	19
		14			20
2^{12}	12	13		20	21
		14			22

Now for $e \in \{10, 12, 18\}$, the cases we have are $q^e = 2^e$ with $d = e, e+2$ and $n = d+1, d+2$. The two smallest nontrivial degrees of A_n, in this case, are n and $n(n+1)/2$. It turns out that $q^{e/2}+1$ is smaller than $n(n+1)/2$ for all cases $e \in \{10, 12, 18\}$. So $A_n \cap H \leqslant A_{n-1}$ and $n = e+1$, as in every other case, $q^{e/2}+1$ is coprime to n. In fact, since the minimum degree of A_{n-1} is $n-1$, we get that $A_n \cap H = A_{n-1}$. By similar arguments, we can find $J \cap H$ for each $A_n \leqslant J \leqslant S_n \times Z$. We conclude that H is the stabiliser of G in its natural action on n elements (where Z acts trivially).

Now suppose that $q^e = p^e = 2^4, 3^4, 3^6, 5^6$. First note that given the information above, we have the following possible values for p^e, d, and n accordingly:

p^e	d	n	p^e	d	n
2^4	4	5, 6	3^6	7	8, 9
2^4	6	7, 8	5^6	6	7
3^4	4	5, 6	5^6	7	8
3^4	6	7	5^6	8	9, 10
3^6	6	7			

If $A_n \leqslant H$, then $|G : H|$ divides $|G : A_n|$, which in turn divides $|S_n \times Z : A_n|$. But this is a contradiction as $\Phi_e^*(p)$ divides $|G : H|$ and $|S_n \times Z : A_n| = 2(p-1)$. So $A_n \cap H$ is a proper subgroup of A_n with index dividing $p^{e/2}+1$. With this fact in mind, we can eliminate some of the cases from the above table, and we obtain the following remaining possibilities:

p^e	d	n	p^e	d	n
2^4	4	5	5^6	6	7
3^4	4	5, 6	5^6	8	9, 10
3^6	6	7			

TABLE 12. Possiblities arising for the Alternating group examples: Permutation module examples

(b) Other examples: Here we have that $q = p$, as e is even. By checking whether or not G has a subgroup of index dividing $q^{e/2}+1$ (using GAP and the ATLAS [8]), we have that $d = 8$ and $e = 6$. In the cases $n = 10$, $n = 9$, and $n = 8$, it turns out that $x = 1$. The rest follows from using GAP and the ATLAS [8] which we summarise below.

n	x	p	$\overline{H}$ for $\overline{G} = A_n$	$\overline{H}$ for $\overline{G} = S_n$
10	1	5	$(A_5 \times A_5) \cdot 2^2$	$S_5 \wr S_2$
9	1	5	$(A_5 \times A_4) \cdot 2$	$S_5 \times S_4$
8	1	3	S_6	$S_6 \times 2$
7	1	5	$\mathbb{Z}_5 : \mathbb{Z}_4$	$(\mathbb{Z}_5 : \mathbb{Z}_4) \times 2$
	3	5	A_5, A_5	$A_5 \times 2$, S_5, S_5, S_5
	6	5	S_5	$S_5 \times 2$
	9	5	–	A_6
	18	5	S_6	S_6

TABLE 13. Possibilities arising for Alternating group examples: Other examples.

Sporadic simple group case:

By using GAP and the ATLAS, it was found that this case does not arise. That is, there is no example G in this case which has a subgroup of index $(q^{e/2}+1)/x$. To prove this, we will need the following information in the table below:

S	$\lvert\mathrm{Out}(S)\rvert$	Indices of maximal subgroups of S	$q^{e/2}+1$
M_{11}	1	11, 12, 55, 66, 165	10, 33
M_{12}	2	12, 66, 144, 220, 396, 495, 1320	10, 33
M_{22}	2	22, 77, 176, 231, 330, 616, 672	33
M_{23}	1	23, 253, 506, 1288, 1771, 40320	33
M_{24}	1	24, 276, 759, 1288, 1771, 2024, 3795, 40320, 1457280	33
J_1	1	266, 1045, 1463, 1540, 1596, 2926, 4180	513
J_2	2	100, 280, 315, 525, 840, 1008, 1800, 2016, 10080	126

For all S in the table above, except for M_{11}, there are no maximal subgroups of index dividing $(q^{e/2}+1)/x$ in S. Since S is a normal subgroup of $\overline{G}$, we know that $|S : S \cap \overline{H}|$ divides $|\overline{G} : \overline{H}|$. Now $|\overline{G} : \overline{H}|$ divides $|G : H|$, so either $S \leqslant \overline{H}$, or $S = M_{11}$ and $|S : S \cap \overline{H}| \neq 1$. In the latter case, we have that $|S : S \cap \overline{H}|$ is equal to $33|\overline{H} : S \cap \overline{H}|/|\overline{G} : S|$ and divides 11. This is a contradiction as $\mathrm{Out}(S)$ is trivial and so $\overline{G} = S$. Therefore we have that if any of the cases arise here, then $S \leqslant \overline{H}$. Now $|\overline{G} : S|$

divides $|\mathrm{Aut}(S):S| = |\mathrm{Out}(S)|$ and $|\overline{G}:\overline{H}|$ divides $|\overline{G}:S|$. So $|G:H|/|G\cap Z : H\cap Z|$ divides $|\mathrm{Out}(S)|$. However, from the table above, we see that $|\mathrm{Out}(S)| = 1, 2$ and so $|G:H|$ is at most $2|G\cap Z : H\cap Z|$, which in turn divides $2|Z| = 2(q-1)$. However, the only common divisors of $\Phi_e^*(q)$ and $2|Z|$ are 1 or 2; which is a contradiction. Therefore, this case does not arise.

Cross-characteristic case:

First we take the lists from Theorem 3.1 and list the values of $|\mathrm{Out}(S)|$ for each case.

S	e	$\lvert\mathrm{Out}(S)\rvert$	S	e	$\lvert\mathrm{Out}(S)\rvert$	S	e	$\lvert\mathrm{Out}(S)\rvert$
$\mathrm{PSL}_2(7)$	6	2	$\mathrm{PSL}_2(19)$	9,18	2	$\mathrm{PSL}_3(4)$	4,6	12
$\mathrm{PSL}_2(8)$	6	3	$\mathrm{PSL}_2(23)$	10	2	$\mathrm{PSU}_3(3^2)$	6	2
$\mathrm{PSL}_2(9)$	4	4	$\mathrm{PSL}_2(25)$	12	4	$\mathrm{P\Omega}_8^+(2)$	6	6
$\mathrm{PSL}_2(11)$	10	2	$\mathrm{PSL}_2(37)$	18	2	$\mathrm{Sp}_6(2)$	4,6	1
$\mathrm{PSL}_2(13)$	6,12	2	$\mathrm{PSL}_2(41)$	20	2	$\mathrm{PSp}_4(5)$	12	2
$\mathrm{PSL}_2(17)$	8	2	$\mathrm{PSL}_3(3)$	12	2	$\mathrm{Sz}(8)$	6	3
						$G_2(3)$	12	2

TABLE 14. Values of $|\mathrm{Out}(S)|$ for the cases listed in Theorem 3.1.

The general technique for ruling out a case above proceeds as follows. Since G has a subgroup of index $n = (q^{e/2}+1)/x$, we have that $\overline{G}$ has a subgroup (namely $\overline{H}$) of index $n/(ax)$ where a is a divisor of $q-1$. Therefore, S has a subgroup (namely $S\cap\overline{H}$) of index dividing $n/(ax)$ (as S is normal in $\overline{G}$). If $S \leqslant \overline{H}$, then n divides $x(q-1)|\mathrm{Out}(S)|$ as

$$|\mathrm{Out}(S)| = |\mathrm{Aut}(S):S| = |\mathrm{Aut}(S):\overline{G}||\overline{G}:S| = |\mathrm{Aut}(S):\overline{G}||\overline{H}:S||\overline{G}:\overline{H}|.$$

Since $\Phi_e^*(q)$ divides n and is coprime to $x(q-1)$, we have that $e+1 \leqslant |\mathrm{Out}(S)|$. In all the cases above, except $S = \mathrm{PSL}_3(4)$, we see that this inequality fails. So in general, $S \not\leqslant \overline{H}$ if S is not $\mathrm{PSL}_3(4)$. Assume for now that S is not $\mathrm{PSL}_3(4)$. Next we list the indices of the maximal subgroups of each S and check (using the ATLAS [8] and GAP) whether S has a maximal subgroup of index dividing n.

S	d	e	q	Possible values of n	Indices of Max. Subgroups of S
$\mathrm{PSL}_2(7)$, $\mathrm{PSL}_3(2)$	6,7	6	3	7,14,28	7,8
	6,7,8	6	5	7,14,21,42	7,8
$\mathrm{PSL}_2(8)$	7	6	3	28	9,28,36
	7,8	6	5	63,126	9,28,36
$\mathrm{PSL}_2(11)$	10	10	2	11,33	11,12,55
$\mathrm{PSL}_2(13)$	6,7	6	3	14,28	14,78,91
$\mathrm{PSL}_2(19)$	9	9	4	57,171	20,57,171,190
	20	18	2	57,171	20,57,171,190
$\mathrm{PSL}_2(25)$	12	12	2	65	26,65,300,325
$\mathrm{PSL}_3(3)$	12	12	2	13	13,144,234
$\mathrm{PSU}_3(3^2)$	6,7	6	5	63,126	28,36,63
$\mathrm{Sp}_6(2)$	7,8	6	3	28	28,36,63,120,135,315,336,960
	7,8	6	5	63,126	28,36,63,120,135,315,336,960

TABLE 15. Remaining possibilities for $S \neq \mathrm{PSL}_3(4)$.

By using the ATLAS [8] and GAP [12], we can determine the possible values of x and the possible subgroups $S\cap\overline{H}$ of S.

S	e	q	x	$S\cap\overline{H}$	S	e	q	x	$S\cap\overline{H}$
$\mathrm{Sp}_6(2)$	6	3	1	$\mathrm{PSU}_4(2^2):2$	$\mathrm{PSL}_2(13)$	6	3	1	$13:3$
		5	1	$2^5:A_6$				2	$13:6$
			2	$2^5:S_6$	$\mathrm{PSL}_2(19)$	9	4	3	D_{20}
$\mathrm{PSL}_2(7)$,$\mathrm{PSL}_3(2)$	6	3	1	S_3				9	A_5, A_5
			2	A_4, A_4		18	2	3	D_{20}
			4	S_4, S_4				9	A_5, A_5
		5	3	2^2, 2^2, 4	$\mathrm{PSL}_2(25)$	12	2	1	S_5, S_5
		6		D_8	$\mathrm{PSL}_3(3)$	12	2	5	$3^2:2\cdot S_4$, $3^2:2\cdot S_4$
		9		A_4, A_4	$\mathrm{PSL}_3(4)$	6	5	1	$2^4:D_{10}$, $2^4:D_{10}$
		18		S_4, S_4				6	$2^4:A_5$, $2^4:A^5$
$\mathrm{PSL}_2(8)$	6	3	1	$9:2$	$\mathrm{PSU}_3(3^2)$	6	5	1	$4\cdot A_4$, $4^2\cdot A_3$
		5	1	2^2				2	$4\cdot S_4$, $4^2\cdot S_3$
			2	2^3					
$\mathrm{PSL}_2(11)$	10	2	3	A_5, A_5					

Now assume $S = \mathrm{PSL}_3(4)$. So by Theorem 3.1, we have $(q,e) \in \{(3,4),(3,6),(5,6)\}$ and $|\mathrm{Out}(S)| = 12$. Suppose first that $S \leqslant \overline{H}$. We have the following data in each case:

q	x	n	$12x(q-1)$	q	x	n	$12x(q-1)$
3	1	10	24	5	1	126	48
	2	5	48		2	63	96
3	1	28	24		3	42	144
	2	14	48		6	21	288
3	4	7	96		9	14	432
					18	7	864

In all cases above, we have that n does not divide $12x(q-1)$, and hence $\overline{H}$ intersects S in a proper subgroup with index dividing n. Now the indices of maximal subgroups of S are 21, 56, 120, and 280. So in particular, we see readily that $q^e = 5^6$. By using the Atlas [8] and GAP, we can determine the possible values of x, and the possible subgroups $S \cap \overline{H}$ of S.

S	e	q	d	x	$S \cap \overline{H}$
$\mathrm{PSL}_3(4)$	6	5	8	1	$2^4 : D_{10}$, $2^4 : D_{10}$
				6	$2^4 : A_5$, $2^4 : A_5$

Natural-characteristic case:

For a classical simple group L, let $P(L)$ be the smallest number n such that L has a proper subgroup of index n. Kleidman and Liebeck give a table of the values of $P(L)$ for various L in [19, Table 5.2A], and we summarise what we need from this table below:

L	p, q	$P(L)$
$\mathrm{PSL}_2(9)$	$p = 3$	7
$\mathrm{PSL}_2(q^3)$	$q \neq 3$	$q^3 + 1$
$\mathrm{PSL}_3(q^2)$	–	$q^4 + q^2 + 1$
$\Omega_7(q)$	p odd, $q \geqslant 5$	$(q^6 - 1)/(q - 1)$
	$q = 3$	351
$P\mathrm{Sp}_6(q)$	$p = 2$, $q > 2$	$(q^6 - 1)/(q - 1)$
	$q = 2$	28
$\mathrm{PSU}_3(q^2)$	$p = 5$	50
	$p \neq 5$	$q^3 + 1$

Table 16. A list of minimal indices for some of the groups in the Natural-characteristic case.

In most of the cases in Table 16 above, we can rule them out simply by noting that all of their proper subgroups have index larger than $q^{e/2} + 1$. For $G_2(q)$, we must look further afield. It follows by the work of Cooperstein for $p = 2$ (see [10]) and Kleidman for p odd (see [22]), that all proper subgroups of $G_2(q)$ have index greater than $q^3 + 1$. Hence we arrive at the following possibilities:

$G^{(\infty)}$	d	e	p	c
$\mathrm{SL}_2(q_0^3)$	8	6	–	1
$\mathrm{PSU}_3(q_0^2)$	8	6	$p \neq 3$	1
	7	6	$p = 3$	1
$\mathrm{Sz}(q_0)$	4	4	$p = 2$	1,2
${}^2G_2(q_0)$	7	6	$p = 3$	1,2

For the case $S = \mathrm{PSL}_2(q^3)$, we have that the minimum degree of a nontrivial permutation representation of S is $q^3 + 1$ and hence $x = 1$. We know that there is precisely one conjugacy classes of subgroups of S of index $q^3 + 1$; namely the point stabiliser in its natural 2-transitive action. Since $\overline{G} \leqslant \mathrm{Aut}(S)$, we have that $\overline{G}$ also has at most one conjugacy class of subgroups of S of index $q^3 + 1$.

Similarly, if $S = \mathrm{PSU}_3(q^2)$, then $x = 1$ and $\overline{G}$ has a unique conjugacy class of subgroups of S of index $q^3 + 1$.

Suppose $S = \mathrm{Sz}(q_0)$ where $c \in \{1, 2\}$. First note that $q_0^4 + 1$ is coprime to $|S| = q_0^2(q_0^2 + 1)(q_0 - 1)$ and hence we must have $c = 1$. It is well known (see Kleidman's thesis [21, §4.2], or the seminal work of Suzuki [26]) that the index of a maximal subgroup of S is at least $q^2 + 1$ and hence $x = 1$. In fact, $\overline{G}$ has a unique action on $q^2 + 1$ points; namely the natural 2-transitive action of $\overline{G}$ on the Suzuki-Tits ovoid (see [21, Theorem 4.2]).

Suppose $S = {}^2G_2(q_0)$ where $c \in \{1, 2\}$. First note that $q_0^6 + 1$ is coprime to $|S| = q_0^3(q_0^3 + 1)(q_0 - 1)$ and hence we must have $c = 1$. It is well known (see Kleidman's thesis [21, §4.1], or his published work [23]) that the index of a maximal subgroup of S is at least $q^3 + 1$, and hence $x = 1$. In fact, $\overline{G}$ has a unique action on $q^3 + 1$ points; namely the natural 2-transitive action of $\overline{G}$ on the Ree-Tits ovoid (see [21, Theorem 4.1]).

8. An application to a conjecture of Cameron and Liebler

In 1982, Cameron and Liebler [7] studied collineation groups G of finite projective spaces $\mathrm{PG}_{d-1}(q)$ of (projective) dimension at least 3 with equally many orbits on points and on lines. (Thus $d \geqslant 4$.) They

showed that such a group has order divisible by $(q^{d-1}-1)/\gcd(q^{d-1}-1, q^2-1)$ and that any maximal subgroup of $\mathrm{P\Gamma L}_d(q)$ containing G also has equally many orbits on points and on lines. They conjectured that, if irreducible, such a group would be transitive on lines, and so by earlier results of Kantor [18] and Cameron and Kantor [6], the group would either: (i) contain $\mathrm{PSL}_d(q)$, (ii) be $\Gamma\mathrm{L}_1(2^5)$ with $d = 5$ and $q = 2$, or (iii) be A_7 with $d = 4$ and $q = 2$. Here we prove that conjecture. In [25], a more involved proof of this conjecture can be found for the case where $d \geqslant 6$, which also uses primitive prime divisors and the classification of finite simple groups.

Theorem 8.1. *If G is an irreducible collineation group of $\mathrm{PG}_{d-1}(q)$, $d \geqslant 4$, with equally many orbits on points and on lines, then one of the following holds:*

(a) *G contains $\mathrm{PSL}_d(q)$;*
(b) *$d = 5$, $q = 2$, and $G = \Gamma\mathrm{L}_1(2^5)$; or*
(c) *$d = 4$, $q = 2$, and $G = A_7$.*

Proof. By a result of Cameron and Liebler [7], $(q^{d-1}-1)/\gcd(q^{d-1}-1, q^2-1)$ divides the order of G. Hence, if $q = p^f$, p prime, $G \cap \mathrm{PGL}_d(q)$ has order divisible by $\Phi^*_{(d-1)f}(p)$. By Theorem 3.1, the following possibilities for the preimage $\hat{G}$ of $G \cap \mathrm{PGL}_d(q)$ in $\mathrm{GL}_d(q)$ arise: Classical, Imprimitive, Extension field, and Nearly simple examples.

In the Classical examples case, we have that $\Omega_d(q)$ is normalised by $\hat{G}$. However, a maximal subgroup of $\mathrm{P\Gamma L}_d(q)$ normalising $\mathrm{P\Omega}_d(q)$ has 3 orbits on points (namely: totally singular points, those points whose perp with respect to the defining orthogonal polarity intersects the associated parabolic quadric in a hyperbolic quadric, and those points whose perp intersects in an elliptic quadric) and at least 4 on lines (namely: those lines which meet the parabolic quadric in 0, 1, 2, or $q+1$ points respectively). So no Classical examples arise.

In the Imprimitive examples case, we have that q^d is 2^5, 2^{13}, or 3^5. The first two cases give us subgroups of $\Omega_d(2)$, which has 3 orbits on points and 4 on lines (which can be easily verified by computer). In the last case, note that $\mathrm{GL}_1(3) \wr S_5$ has 5 orbits on points and 12 on lines. Hence no Imprimitive example arises.

In the Extension field examples, we have that $G = \Gamma\mathrm{L}_1(2^5)$ with $d = 5$ and $q = 2$, which appears in the statement of the theorem.

Now we look at the subcases of the Nearly simple examples. In the Alternating Group case, we have only A_7, $d = 4$, and $q = 2$; and it appears in the statement of the theorem. In the Sporadic Group case, we have only M_{11}, $d = 5$, and $q = 3$; and it has 2 orbits on points and 4 on lines. In the Cross-characteristic case, we are left with $\mathrm{PSL}_2(13)$, $d = 7$, and $q = 3$; and it has 9 orbits on points and 156 on lines. Finally, in the Natural-characteristic case, we have three families of groups having $e = d-1$; namely $G_2(q)$, $\mathrm{PSU}_3(q^2)$, and ${}^2G_2(q_0)$. These are all subgroups of $\Omega_7(q)$, which has 3 orbits on points and 4 on lines, as noted previously. □

References

[1] Shreeram S. Abhyankar. Again nice equations for nice groups. *Proc. Amer. Math. Soc.*, 124(10):2967–2976, 1996.
[2] Robert W. Baddeley and Cheryl E. Praeger. On primitive overgroups of quasiprimitive permutation groups. *J. Algebra*, 263(2):294–344, 2003.
[3] John Bamberg and Tim Penttila. A classification of transitive ovoids, spreads, and m-systems of polar spaces. *submitted*.
[4] John Bamberg and Tim Penttila. Transitive eggs. *Innov. Incidence Geom.*, 4:1–12, 2007.
[5] Áron Bereczky. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, 234(1):187–206, 2000.
[6] P. J. Cameron and W. M. Kantor. 2-transitive and antiflag transitive collineation groups of finite projective spaces. *J. Algebra*, 60(2):384–422, 1979.
[7] P. J. Cameron and R. A. Liebler. Tactical decompositions and orbits of projective groups. *Linear Algebra Appl.*, 46:91–102, 1982.
[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.
[9] Bruce N. Cooperstein. Minimal degree for a permutation representation of a classical group. *Israel J. Math.*, 30(3):213–235, 1978.
[10] Bruce N. Cooperstein. Maximal subgroups of $G_2(2\mathrm{Sp}n)$. *J. Algebra*, 70(1):23–36, 1981.
[11] John D. Dixon and Brian Mortimer. *Permutation groups*. Springer-Verlag, New York, 1996.
[12] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (`http://www.gap-system.org`).
[13] Robert Guralnick, Tim Penttila, Cheryl E. Praeger, and Jan Saxl. Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc. (3)*, 78(1):167–214, 1999.

[14] Robert M. Guralnick and William M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000. Special issue in honor of Helmut Wielandt.
[15] Christoph Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974.
[16] Gerhard Hiss and Gunter Malle. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.*, 4:22–63 (electronic), 2001.
[17] Christoph Jansen, Klaus Lux, Richard Parker, and Robert Wilson. *An atlas of Brauer characters*, volume 11 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1995. Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications.
[18] William M. Kantor. Line-transitive collineation groups of finite projective spaces. *Israel J. Math.*, 14:229–235, 1973.
[19] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.
[20] Peter B. Kleidman. The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega\mathrm{Sp}_{+8}(q)$ and of their automorphism groups. *J. Algebra*, 110(1):173–242, 1987.
[21] Peter B. Kleidman. *The subgroup structure of some finite simple groups*. PhD Thesis. 1987.
[22] Peter B. Kleidman. The 2-transitive ovoids. *J. Algebra*, 117(1):117–135, 1988.
[23] Peter B. Kleidman. The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups $\mathrm{Sp}2G_2(q)$, and their automorphism groups. *J. Algebra*, 117(1):30–71, 1988.
[24] Eamonn A. O'Brien. Towards effective algorithms for linear groups. *(A. Hulpke, R. Liebler, T. Penttila, A. Seress, eds.) Finite Geometries, Groups and Computation*, 2005 (to appear).
[25] Tim Penttila. *Collineations and configurations in projective spaces.* D. Phil. thesis, University of Oxford, 1985.
[26] Michio Suzuki. On a class of doubly transitive groups. *Ann. of Math. (2)*, 75:105–145, 1962.
[27] Robert C. Valentini and Manohar L. Madan. A hauptsatz of L. E. Dickson and Artin-Schreier extensions. *J. Reine Angew. Math.*, 318:156–177, 1980.
[28] K. Zsigmondy. Zur theorie der potenzreste. *Monatsh. für Math. u. Phys.*, 3:265–284, 1892.

School of Mathematics and Statistics, The University of Western Australia,, 35 Stirling Highway, Crawley, W.A. 6009, Australia.