J. Group Theory **12** (2009), 219–234
DOI 10.1515/JGT.2008.074

Journal of Group Theory

The groups with exactly one class of size a multiple of p

Silvio Dolfi, Alexander Moretó and Gabriel Navarro

(Communicated by R. M. Guralnick)

Abstract. Let p be a prime. The goal of this paper is to classify the finite groups with exactly one conjugacy class of size a multiple of p.

1 Introduction

For reasons that are not fully understood, the conjugacy class sizes of a finite group G share some analogies with the character degrees of G. Sometimes these analogies lead to interesting problems. Fix a prime number p. Recently we have studied in [7] the groups with exactly one irreducible character of degree a multiple of p, trying to find extensions of the Itô–Michler theorem. Here we discover that the corresponding problem on conjugacy class sizes has a similar answer. Our aim in this note is to classify finite groups with one conjugacy class of size a multiple of p.

Theorem A. *Let G be a finite group and p a prime. Then G has exactly one conjugacy class of size divisible by p if and only if one of the following holds*:

(a) *G is a Frobenius group with Frobenius complement of order 2 and Frobenius kernel of order divisible by p*;

(b) *G is a doubly transitive Frobenius group whose Frobenius complement has a non-trivial central Sylow p-subgroup*;

(c) *p is odd, $G = KH$ where $K = \mathrm{F}(G)$ is an ultraspecial q-group, q prime, $H = \mathrm{C}_G(P)$ for a Sylow p-subgroup P of G, $K \cap H = \mathrm{Z}(K)$ and $G/\mathrm{Z}(K)$ is a doubly transitive Frobenius group of Dickson type.*

In particular, if $p = 2$, we obtain that a group has a unique conjugacy class of even size if and only if G is a doubly transitive Frobenius group whose Frobenius complement has a non-trivial central Sylow p-subgroup. The paradigmatic examples of such groups are $\mathrm{GF}(q) \rtimes \mathrm{GF}(q)^\times$, where $\mathrm{GF}(q)$ is the Galois field of q elements for an odd prime power q. But there are some more, all related to the so-called *near fields*.

For instance, the *semi-linear* group $\Gamma(7^3)$ associated to the Galois field $\mathrm{GF}(7^3)$ has a subgroup H of order $7^3 - 1 = 342$ that acts transitively on the non-zero elements of $V = \mathrm{GF}(7^3)$ and such that $|\mathbf{F}(H)| = 114$. The semidirect product $G = V \rtimes H$ has exactly one conjugacy class of even size.

As we will observe in Section 2, there are exactly two non-solvable groups with one conjugacy class of size a multiple of a prime p for some p, one for $p = 7$ and the other for $p = 29$.

We refer the reader to Section 2 for the definition of the concepts that appear in the statement of Theorem A, their basic properties and some known results we will use in the proof. We prove some lemmas that depend on the classification of finite simple groups in Section 3 and we complete the proof of Theorem A in Section 4. We remark that to prove Theorem A for $p = 2$ one can avoid the use of the classification, since solvability follows by Lemma 4.2 and the theorem of Feit and Thompson.

Every group, in the following, is a finite group.

2 Preliminaries

We start by recalling the notions that appear in the statement of Theorem A.

A *Frobenius group* is a semidirect product $G = K \rtimes H$ where H acts *fixed-point freely* on K, i.e. $\mathrm{C}_K(h) = 1$ for all $h \in H - \{1\}$. The subgroup $K \lhd G$ is called the Frobenius kernel and H a Frobenius complement of G. It is known that the Sylow subgroups of H are either cyclic or generalized quaternion groups. Also, if $|H|$ is even, then K is abelian. The Frobenius group G is *doubly transitive* if the Frobenius complement H acts transitively on $K - \{1\}$. In this case, $|H| = |K| - 1$.

Doubly transitive Frobenius groups are in bijective correspondence with finite near fields. A near field is a set F with two binary operations $+$ and $\cdot$ such that:

$F(+)$ is an abelian group with identity 0;

$F^{\#}(\cdot)$ is a group, where $F^{\#} = F - \{0\}$, and $x \cdot 0 = 0 \cdot x = 0$ for every $x \in F$;

a one-sided (right, say) distributive law is satisfied:

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad \text{for every } x, y, z \in F.$$

Observe that a near field is a field precisely when the multiplicative group is abelian and that the additive group of a finite near field F is an elementary abelian q-group for some prime q.

It turns out that a finite group G is a doubly transitive Frobenius group if and only if G is a semidirect product of the additive group and the multiplicative group of a finite near field F.

The finite near fields were classified by Zassenhaus in the 1930s. Most of them are *Dickson near fields*, which arise from fields by 'twisting' the group multiplication by Galois automorphisms. Furthermore, there are just seven *exceptional near fields*, of orders 5^2, 7^2, 11^2 (two of them), 23^2, 29^2 and 59^2.

We will call a doubly transitive Frobenius group of *Dickson type* if the corresponding near field is a Dickson near field. In this case, the Frobenius complement is metacyclic and has a maximal cyclic normal subgroup U with $|U| = (q^n - 1)/v$ where v is

a divisor of n (the near field is a field if and only if $v = 1$). Further, any prime divisor of v divides $q^{n/v} - 1$ and if 4 divides v then 4 divides $q^{n/v} - 1$. See [10, IV.(1.1) and (1.5)] or [6, pp. 31–33].

A check of the structure of the multiplicative group $F^\times$ of the exceptional near fields (see [10, IV (7.1) and (7.3)]) shows that there is no central Sylow subgroup for $|F| = 5^2, 7^2, 11^2$. The three remaining cases give a solvable and two non-solvable instances of groups $G = F^+ \rtimes F^\times$ with exactly one conjugacy class of size divisible by p:

(i) $p = 11$, $|F| = 23^2$, $F^\times \simeq H \times C_{11}$ and H has a subgroup of index 2 isomorphic to $\mathrm{SL}(2, 3)$;

(ii) $p = 7$, $|F| = 29^2$, $F^\times \simeq \mathrm{SL}(2, 5) \times C_7$;

(iii) $p = 29$, $|F| = 59^2$, $F^\times \simeq \mathrm{SL}(2, 5) \times C_{29}$.

Observe that the only non-solvable groups appearing in Theorem A are the groups described in (ii) and (iii) above.

A q-group E is *semi-extraspecial* if for every maximal subgroup Z of $\mathrm{Z}(E)$ the factor group E/Z is extraspecial. In this case the rank $\mathrm{rk}(E)$ of E is even (see [1]) (the rank being the smallest cardinality of a generating set) and $\mathrm{rk}(\mathrm{Z}(E)) \leqslant \mathrm{rk}(E)/2$. When $\mathrm{rk}(\mathrm{Z}(E)) = \mathrm{rk}(E)/2$ the group E is said to be *ultraspecial*.

If E is semi-extraspecial, then one can prove that $\mathrm{Z}(E) = E' = \mathbf{\Phi}(E)$ (i.e. E is a special q-group) and from this it follows that $\mathrm{Z}(E)$ is elementary abelian. Finally, it is easy to see that if E is semi-extraspecial and $Y < \mathrm{Z}(E)$, then $\mathrm{Z}(E/Y) = \mathrm{Z}(E)/Y$ and E/Y is semi-extraspecial, too.

In the proof of Theorem A we will use the Zsigmondy primes. Recall that a prime t is a Zsigmondy prime divisor for $a^n - 1$, where $a > 1$ and n are positive integers, if t divides $a^n - 1$ but t does not divide $a^j - 1$ for $1 \leqslant j < n$. We will use, without further explicit reference, Zsigmondy's prime theorem. (For a proof, see [4, (IX.8.3)].)

Theorem 2.1. *Let $a > 1$ and n be positive integers. Then there exists a Zsigmondy prime divisor for $a^n - 1$ unless $a = 2$ and $n = 6$ or a is a Mersenne prime and $n = 2$.*

We collect in the following lemma some well-known facts that we shall use without explicit reference. We denote by $\mathrm{cl}_G(x)$ the conjugacy class of the element x in the group G.

Lemma 2.2. *Let G be a group.*

(i) *If $x, y \in G$ have coprime orders and commute, or if x and y belong to normal subgroups with trivial intersection, then $\mathrm{C}_G(xy) = \mathrm{C}_G(x) \cap \mathrm{C}_G(y)$. In particular, if a prime p divides $|\mathrm{cl}_G(x)|$ then p also divides $|\mathrm{cl}_G(xy)|$.*

(ii) *If $\varphi : G \to H$ is a surjective homomorphism and K is a conjugacy class of G, then $\varphi(K)$ is a conjugacy class of H and $|\varphi(K)|$ divides $|K|$.*

Next we recall a well-known result concerning module actions of cyclic groups.

Lemma 2.3. *Let C be an abelian group of prime-power order and let M be a faithful $\mathrm{GF}(q)[C]$-module, with q a prime. Write $|M| = q^n$. Then the following are equivalent*:

(i) *M is irreducible*;

(ii) *C is cyclic, $|C|$ divides $q^n - 1$ and $|C|$ does not divide $q^k - 1$ for every $1 \leqslant k < n$.*

Proof. It is shown in [3, Satz II.3.10] that (i) implies (ii).

Conversely, assume (ii). Since $(|M|, |C|) = 1$, M is a completely reducible C-module. As C is cyclic of prime-power order, C has a unique minimal subgroup and that subgroup is not contained in the kernel of all actions of C on the irreducible submodules of M, because M is faithful and completely reducible. So there exists an irreducible and faithful C-submodule V of M. Write $|V| = q^m$, with $1 \leqslant m \leqslant n$. Since we already know that (i) implies (ii), it follows that $|C|$ divides $q^m - 1$, which forces $m = n$ and hence $M = V$ is irreducible. □

The assumption that the order of C is a prime power is necessary for showing that (ii) implies (i) (in the other direction it is not). Consider, namely, a faithful action of a cyclic group of order 21 on the direct sum of vector spaces of dimension 1, 2 and 3, respectively, on $\mathrm{GF}(2)$.

Finally, we state a lemma about cyclic actions on extraspecial groups.

Lemma 2.4. *Let E be an extraspecial group, $|E| = q^{2m+1}$, q prime, and let C be a cyclic subgroup of $\mathrm{Aut}(E)$. Assume that C acts trivially on $\mathrm{Z}(E)$.*

(i) *If C acts fixed-point freely on $E/\mathrm{Z}(E)$, then $|C|$ divides either $q^m + 1$ or $q^m - 1$.*

(ii) *If C acts irreducibly on $E/\mathrm{Z}(E)$, then $|C|$ divides $q^m + 1$.*

Proof. Observe that if C acts fixed-point freely on $E/\mathrm{Z}(E)$ then C is a q'-group and (i) is part of the statement of [3, Satz V.17.13].

If C acts irreducibly on $E/\mathrm{Z}(E)$, then C can be identified with an irreducible cyclic subgroup of $\mathrm{Sp}(2m, q)$ and the assertion follows from [3, Satz II.9.23]. □

3 Simple groups

In this section we prove a couple of lemmas that depend on the classification of finite simple groups.

Lemma 3.1. *Let G be an almost simple group, i.e. $S \leqslant G \leqslant \mathrm{Aut}(S)$ where S is a non-abelian simple group. Let p be a prime divisor of $|G|$ and assume that p does not divide $|S|$. Then there exist $x, y \in S$ such that $o(x) \neq o(y)$ and the sizes of both $\mathrm{cl}_G(x)$ and $\mathrm{cl}_G(y)$ are divisible by p.*

Proof. By the classification, S is a simple group of Lie type and any element of order p in G is conjugate in $\mathrm{Aut}(S)$ to a field automorphism of S. In the proof of [8, Proposition 2.4], it is shown that there exist two elements $x, y \in S$ of distinct prime orders that are not centralized by any non-trivial field automorphism of S. □

If G is a permutation group on a set Ω and $\Gamma \subseteq \Omega$, we denote by G_Γ the setwise stabilizer of Γ in G.

Lemma 3.2. *Let G be a permutation group on a finite set Ω, $|\Omega| \geqslant 2$, and let p be a prime divisor of $|G|$. Then there exist two disjoint non-empty subsets Γ, Δ of Ω such that $|G : G_\Gamma \cap G_\Delta|$ is a multiple of p.*

Proof. We argue by induction on $|\Omega|$.

Assume first that G is imprimitive and let $\Sigma = \{\Theta_1, \Theta_2, \ldots, \Theta_k\}$ be a non-trivial system of blocks, i.e. $2 \leqslant k < |\Omega|$. Let N be the kernel of the action of G on Σ.

If p divides $|G/N|$, then by inductive hypothesis there exist two disjoint non-empty subsets Π, Ξ of Σ such that $|G/N : (G/N)_\Pi \cap (G/N)_\Xi|$ is a multiple of p. Define now $\Gamma = \bigcup_{\Theta \in \Pi} \Theta$ and $\Delta = \bigcup_{\Theta \in \Xi} \Theta$. Then Γ and Δ are non-empty, disjoint subsets of Ω and, observing that $G_\Gamma N/N \leqslant (G/N)_\Pi$ and $G_\Delta N/N \leqslant (G/N)_\Xi$, we see that $|G : G_\Gamma \cap G_\Delta|$ is a multiple of p.

We can assume that $|G : N|$ is not divisible by p. Write $\Theta = \Theta_1$. Let $H = G_\Theta$ and let K be the kernel of the action of H on Θ. If p does not divide $|H/K|$, then $N \cap K$ contains some $P \in \mathrm{Syl}_p(N) = \mathrm{Syl}_p(G)$. Since $N \leqslant H$, we have $N \cap K \lhd N$ and hence $N \cap K$ contains the normal closure $P^N = P^G$. But this gives a contradiction, because the transitivity of G implies that the intersection of the conjugates of K in G is trivial.

Thus, p divides $|H/K|$ and, as $2 \leqslant |\Theta| < |\Omega|$, by induction there exist two non-empty and disjoint subset Γ and Δ of Θ such that $|H/K : (H/K)_\Gamma \cap (H/K)_\Delta|$ is a multiple of p. Since $G_\Gamma \leqslant H$ and $G_\Delta \leqslant H$, it follows that

$$|G : G_\Gamma \cap G_\Delta| = |G : H|\,|H : H_\Gamma \cap H_\Delta|$$

is divisible by p.

We are hence reduced to the case that G is a primitive permutation group on Ω. In [9, Theorem 2], one can find a complete list of the primitive permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ with $\mathrm{Alt}(\Omega) \not\leqslant G$ and such that $G_\Gamma \neq 1$ for all $\Gamma \subseteq \Omega$ (this result uses consequences of the classification). All these exceptional groups are almost simple or of affine type, and their degree, apart from a single exception of degree 32, is at most 24. For all of these groups there is a permutation representation available in the computer algebra system [2]. It is hence easily checked that the assertion holds for all of these exceptional groups, for instance by random choice of two non-empty and disjoint subsets of Ω.

Finally, we are left with the case $G = \mathrm{Alt}(\Omega)$ or $G = \mathrm{Sym}(\Omega)$. Note that then $p \leqslant |\Omega|$. In this case, any choice of disjoint subsets Γ and Δ of Ω with $|\Gamma| = p - 1$ and $|\Delta| = 1$ will do. □

Lemma 3.3. *Let M be the unique minimal normal subgroup of a group G. Let p be a prime divisor of $|G|$ and assume that p does not divide $|M|$. If M is non-solvable, then there exist $x, y \in M$ with $o(x) \neq o(y)$ and such that the sizes of both $\mathrm{cl}_G(x)$ and $\mathrm{cl}_G(y)$ are divisible by p.*

Proof. Write $M = S_1 \times S_2 \times \cdots \times S_k$ with $S_i \simeq S$ a non-abelian simple group. Let $N = \bigcap_{i=1}^{k} \mathrm{N}_G(S_i)$ be the kernel of the transitive action of G on $\Omega = \{S_1, S_2, \ldots, S_k\}$.

Assume first that $|G/N|$ is divisible by p. By Lemma 3.2, there exist two non-empty subsets $\Gamma, \Delta \subseteq \Omega$ with $\Gamma \cap \Delta = \varnothing$ and such that $|G : G_\Gamma \cap G_\Delta|$ is a multiple of p. Choose now three distinct prime divisors p_1, p_2, p_3 of $|S|$ (which exist by Burnside's $p^\alpha q^\beta$ theorem).

Define $x = \prod_{i=1}^{k} a_i$ where $a_i \in S_i$ for $i = 1, \ldots, k$ and $o(a_i) = p_1$ if $S_i \in \Gamma$, $o(a_i) = p_2$ if $S_i \in \Delta$ and $o(a_i) = 1$ otherwise.

Define also $y = \prod_{i=1}^{k} b_i$ where $b_i \in S_i$ for $i = 1, \ldots, k$ and $o(b_i) = p_1$ if $S_i \in \Gamma$, $o(b_i) = p_3$ if $S_i \in \Delta$ and $o(b_i) = 1$ otherwise.

Then $o(x) \neq o(y)$ and both $\mathrm{C}_G(x)$ and $\mathrm{C}_G(y)$ are contained in $G_\Gamma \cap G_\Delta$, which means that p divides both $|\mathrm{cl}_G(x)|$ and $|\mathrm{cl}_G(y)|$.

Assume now that p divides $|N|$. Write $S = S_1$, $K = \mathrm{N}_G(S)$ and $L = \mathrm{C}_G(S)$. Then $SL/L \simeq S$ and $SL/L \leqslant K/L \leqslant \mathrm{Aut}(SL/L)$, so K/L is an almost simple group. As $|K/L|$ and $|N|$ have the same set of prime divisors, p divides $|K/L|$. But p does not divide $|SL/L|$ as p does not divide $|M|$. So we can apply Lemma 3.1 and get $x, y \in S$ with $o(xL) \neq o(yL)$ and such that p divides both $|K/L : \mathrm{C}_{K/L}(xL)|$ and $|K/L : \mathrm{C}_{K/L}(yL)|$. Observe now that $o(x) = o(xL)$ and $o(y) = o(yL)$, since $S \cap L = 1$. Further, considering the action of G on Ω, we have that $\mathrm{C}_G(x)$ and $\mathrm{C}_G(y)$ are contained in $\mathrm{N}_G(S) = K$. This means that $\mathrm{C}_G(x) = \mathrm{C}_K(x)$, $\mathrm{C}_G(y) = \mathrm{C}_K(y)$ and hence p divides both $|\mathrm{cl}_G(x)|$ and $|\mathrm{cl}_G(y)|$. □

4 Proof of Theorem A

We start with three elementary lemmas. We thank M. Isaacs for an argument in the proof of the next lemma.

Lemma 4.1. *Let K be a normal q-subgroup of the group G, q a prime. Let $N = \mathrm{Z}(K)$ and assume that $K - N$ is a conjugacy class of G. Assume also that $|G/K| = |K/N| - 1$. Then K is a semi-extraspecial group and $|\mathrm{cl}_K(x)| = |N|$ for all $x \in K - N$.*

Proof. For $x \in K - N$ we have

$$|G : \mathrm{C}_G(x)| = |K - N| = |N|(|K/N| - 1) = |N|(|G/K|).$$

Since $|G/K| = |G|_{q'}$, the full q'-part of $|G|$, divides $|G : \mathrm{C}_G(x)|$, we have $\mathrm{C}_G(x) \leqslant K$ and hence $|G : \mathrm{C}_G(x)| = |G/K|\,|K : \mathrm{C}_K(x)|$. It follows that $|\mathrm{cl}_K(x)| = |N|$ for all $x \in K - N$.

Now let Z be a maximal subgroup of N. If $z \in K$ is central modulo Z, then $[z, K] \leqslant Z$ and z has at most $|Z| < |N|$ conjugates in K and it follows that $z \in N$. Hence, $\mathrm{Z}(K/Z) = N/Z$ has order q. As $K - N$ is a conjugacy class of G, we see that all non-trivial elements of K/N are conjugate in G/N. It follows that K/N is elementary abelian and hence K/Z is an extraspecial group. Therefore, K is a semi-extraspecial q-group. □

Lemma 4.2. *Let G be a finite group, let p be a prime, and let $P \in \mathrm{Syl}_p(G)$. Suppose that G has a unique conjugacy class of size divisible by p. Then either G has a normal p-complement and P is abelian, or p is odd and G is a Frobenius group with Frobenius complement of order 2.*

Proof. Write $K = \mathrm{cl}_G(z)$ for the unique conjugacy class of G that has size divisible by p and let $P \in \mathrm{Syl}_p(G)$. Let $C = \mathrm{C}_G(P)$.

If $y \in G - \bigcup_{g \in G} C^g$, then p divides $|G : \mathrm{C}_G(y)|$, and therefore $y \in K$. Hence

$$G = \left(\bigcup_{g \in G} C^g \right) \cup K$$

is a disjoint union. We have that

$$|G| - 1 \leqslant |G : \mathrm{N}_G(C)|(|C| - 1) + |G : \mathrm{C}_G(z)|.$$

Assume first that $\mathrm{N}_G(C) < G$. In this case,

$$|G| < \frac{|G|}{|\mathrm{N}_G(C) : C|} + \frac{|G|}{|\mathrm{C}_G(z)|} \leqslant \frac{|G|}{|\mathrm{N}_G(C) : C|} + \frac{|G|}{2}$$

and $\mathrm{N}_G(C) = C$. Since $C \subseteq \mathrm{N}_G(P) \subseteq \mathrm{N}_G(C)$, we conclude that $C = \mathrm{N}_G(P)$. Hence G has a normal p-complement L and P is abelian.

Finally, assume that $C \lhd G$, then $G - C = K$ is a conjugacy class of G. Write $n = |G : C|$. Then $|K| = |G : \mathrm{C}_G(z)| = (n-1)|C|$ divides $|G| = n|C|$. Hence

$$n = 2 = |\mathrm{C}_G(z)| = |\langle z \rangle|$$

and, as $z \notin C$ by hypothesis, it follows that $\langle z \rangle$ complements C and acts fixed-point freely on C. It follows that $|C| = |K|$ is odd, and so is p in this case. □

Lemma 4.3. *Assume that a semi-extraspecial q-group U acts faithfully on an elementary abelian t-group M, where $q \neq t$. If $\mathrm{C}_U(m) \leqslant \mathrm{Z}(U)$ for every $m \in M - \{1\}$, then $q = 2$ and $U \simeq Q_8$, the quaternion group of order 8.*

Proof. By coprimality, M is a completely reducible U-module. Since the action is faithful, there exists an irreducible U-submodule V of M such that $Z = \mathrm{Z}(U)$ does not act trivially on V. Write $Y = \mathrm{C}_U(V)$. Then $Y < Z$ and the semi-extraspecial group U/Y acts faithfully on V. Further, for all $v \in V - \{1\}$ we have $\mathrm{C}_{U/Y}(v) = \mathrm{C}_U(v)/Y$ because Y is the kernel of the action of U on V and hence $\mathrm{C}_{U/Y}(v) \leqslant Z/Y = \mathrm{Z}(U/Y)$.

If $V < M$, working by induction on $|M|$ we get that $q = 2$ and that $U/Y \simeq Q_8$. In particular, $\mathrm{rk}(U/Y) = 2$ and hence $\mathrm{rk}(U) = 2$ and $\mathrm{rk}(Z) = 1$. Thus, $|Z| = 2$ which implies $Y = 1$ and $U \simeq Q_8$.

We can hence assume that M is an irreducible U-module. If X is a subgroup of $Z = \mathrm{Z}(U)$, by Clifford's theorem M_X is a homogeneous X-module and, since the action of U on M is faithful, X does not centralize any non-trivial element in M. It follows that $\mathrm{C}_Z(m) = 1$ for every $m \in M - \{1\}$ and hence, since $\mathrm{C}_U(m) \leqslant Z$ by assumption, U acts fixed-point freely on M. But U is not cyclic and then $q = 2$ and U is a generalized quaternion group. Thus, in particular, $|Z| = 2$. But U is semi-extraspecial, and this forces $U \simeq Q_8$. $\square$

Now we are ready to prove Theorem A. Recall that a prime p does not divide any conjugacy class size of G if and only if G has a central Sylow p-subgroup.

Proof of Theorem A. Assume that G has a unique conjugacy class of size divisible by p and that G is not a Frobenius group with complement of order 2. By Lemma 4.2, G has a normal p-complement and abelian Sylow p-subgroups. Let P be a Sylow p-subgroup of G and $K = [P, G]$. Note that P is abelian and that $|K| \neq 1$ is coprime with p.

Case 1. Assume first that K is abelian.

We will prove that G is one of the groups described in (b). Write $H = \mathrm{N}_G(P) = \mathrm{C}_G(P)$ and observe that, as $(|K|, |P|) = 1$, by well-known results on coprime actions we have $G = KH$ and $K = [K, P] \times (K \cap H)$. Hence H is a complement of $K = [K, P]$ in G and $|\mathrm{cl}_G(x)|$ is divisible by p for all non-trivial $x \in K$. It follows that $K - \{1\} = \mathrm{cl}_G(x)$ and hence K is a minimal normal subgroup of G and H is maximal in G. Let $g_1, g_2, \ldots, g_k$ be a transversal of $H = \mathrm{N}_G(H)$ in G, where $k = |K|$. Now, $G - K = \bigcup_{i=1}^{k} (H^{g_i} - 1)$, because no G-conjugacy class outside K has size divisible by p, and hence we have

$$|G| - |K| \leqslant \sum_{i=1}^{k} (|H^{g_i} - 1|) = |K|(|H| - 1) = |G| - |K|$$

and hence $H^{g_i} \cap H^{g_j} = 1$ for all distinct i, j.

Therefore, G is a Frobenius group with elementary abelian kernel K and complement $H = \mathrm{C}_G(P)$. Since $H \simeq G/K$ acts transitively on $K - \{1\}$, G is a doubly transitive Frobenius group, i.e. one of the groups described in (b).

Case 2. Suppose now that K is non-abelian. We will prove that G is one of the groups described in (c). Let M be a minimal normal subgroup of G contained in K. For the reader's convenience, we split the proof into several steps.

Step 1. M is solvable.

Assume that M is non-solvable and let $N = \mathrm{C}_G(M)$.

If $P \leqslant N$, then there is an $x \in N$ with $|\mathrm{cl}_N(x)|$ divisible by p, as otherwise P would be normal in G and hence $[P, G] \leqslant P \cap K = 1$, a contradiction. Now, if $y, z \in M$ and

$g \in G$ are such that $(xy)^g = xz$, then $x^{-1}x^g = z(y^g)^{-1} \in N \cap M = 1$ and hence $x = x^g$ and $z = y^g$. So, if $o(y) \neq o(z)$ then xy and xz are not conjugate in G. Also, $C_G(xy) = C_G(x) \cap C_G(y)$ and $C_G(xz) = C_G(x) \cap C_G(z)$, and hence p divides both $|cl_G(xy)|$ and $|cl_G(xz)|$, a contradiction.

We can hence assume that p divides the order of the factor group G/N. Observe that the unique minimal normal subgroup of G/N is $MN/N \simeq M$. As $M \leqslant K$, p does not divide $|M|$ and hence we can apply Lemma 3.3 and get $xN, yN \in G/N$ such that $o(xN) \neq o(yN)$ and such that p divides both $|cl_{G/N}(xN)|$ and $|cl_{G/N}(yN)|$. Thus $cl_G(x)$ and $cl_G(y)$ are distinct conjugacy classes of size divisible by p, again a contradiction.

Now, write $\overline{G} = G/M$ and use the bar convention.

Step 2. We claim that $\overline{F} = F(\overline{G})$ is a q-group, q a prime, and either

(B) $\overline{G}$ is a doubly transitive Frobenius group with kernel $\overline{F}$ and complement $C_{\overline{G}}(\overline{P})$; or

(C) $\overline{G} = \overline{F}C_{\overline{G}}(\overline{P})$, with $\overline{F}$ ultraspecial q-group, q prime, and

$$\overline{L} = \overline{F} \cap C_{\overline{G}}(\overline{P}) = Z(\overline{F}) = \overline{F}' = \mathbf{\Phi}(\overline{F})$$

minimal normal in $\overline{G}$; further $\overline{G}/\overline{L}$ is a doubly transitive Frobenius group of Dickson type.

We know that M is solvable and, since we are assuming that K is non-abelian, $M < K$. Thus $\overline{K} = [\overline{G}, \overline{P}]$ is non-trivial and $\overline{G}$ has no central Sylow p-subgroups. Hence, in $\overline{G}$ there is at least a conjugacy class of size divisible by p. Since the conjugacy classes of $\overline{G}$ are images of conjugacy classes of G under the natural projection, we also see that $\overline{G}$ has at most one conjugacy class of size divisible by p. Working by induction on $|G|$, we conclude that $\overline{G}$ is one of the groups described in (a), (b) or (c) of Theorem A. If $\overline{G}$ is as in (a), then $\overline{P} \leqslant \overline{F}$ and then $\overline{P} \triangleleft \overline{G}$. It follows that $\overline{K} = [\overline{G}, \overline{P}] \leqslant \overline{P}$ and $K \leqslant PM$ which implies, as K is a p'-group, that $K = M$, a contradiction. Therefore, $\overline{G}$ is as in (b) or (c).

If $\overline{G}$ is as in (b), i.e. $\overline{G}$ is a doubly transitive Frobenius group, then the Frobenius kernel is $\overline{F}$. Further, since $\overline{P}$ is non-trivial and central in a Frobenius complement of $\overline{G}$, $\overline{P}$ does not centralize any non-trivial element of $\overline{F}$. Hence it follows that $C_{\overline{G}}(\overline{P})$ is a Frobenius complement of $\overline{G}$.

If $\overline{G}$ is of type (c), then (C) clearly follows.

Step 3. $F(G/M) = K/M$.

In both cases $\overline{G}/\overline{F}$ has a central Sylow p-subgroup, and this means that $\overline{F} \geqslant [\overline{G}, \overline{P}] = \overline{K}$.

In case (B) it is clear that $\overline{K} = \overline{F}$, as $\overline{F}$ is minimal normal in $\overline{G}$ and $\overline{K} \neq 1$. In case (C), $\overline{F}/\overline{L}$ is a chief factor of $\overline{G}$ because $\overline{G}/\overline{F}$ is transitive on the non-trivial elements of $\overline{F}/\overline{L}$. As $\overline{K}$ is not contained in $\overline{L}$ because $\overline{G}/\overline{L}$ has no central Sylow p-subgroup, then either $\overline{K} = \overline{F}$ or $\overline{K}$ complements $\overline{L}$ in $\overline{F}$. But the latter is not possible, since $\overline{L} = \mathbf{\Phi}(\overline{F})$. This completes the proof of this step.

Step 4. We now prove that M is a q-group.

Assume by contradiction that $|M| = t^a$, for a prime $t \neq q$.

Observe that by Step 3 we have $\mathrm{F}(G) \leqslant K$. If $\mathrm{F}(G) > M$ then $\mathrm{F}(G) = M \times Q$, with $Q = O_q(G) \neq 1$. Let $N \leqslant Q$ be a minimal normal subgroup of G. Working with N in place of M, by Step 2 and Step 3 we conclude that G/N is of type (b) or (c) in Theorem A and that $\mathrm{F}(G/N) = K/N$ is a group of prime-power order. As $t \neq q$, this implies that $K = M \times N$ and that both G/M and G/N are groups of type (b) in Theorem A. In particular, there are $x \in M$ and $y \in N$ such that $|\mathrm{cl}_{G/M}(xM)|$ and $|\mathrm{cl}_{G/N}(yN)|$ are divisible by p. Then $\mathrm{cl}_G(x)$ and $\mathrm{cl}_G(y)$ are distinct classes of size a multiple of p, a contradiction. Thus, $\mathrm{F}(G) = M$ is minimal normal in G.

It follows also that $\mathbf{\Phi}(G) = 1$, because

$$\mathbf{\Phi}(G) \leqslant M \quad \text{and} \quad \mathrm{F}(G)/\mathbf{\Phi}(G) = \mathrm{F}(G/\mathbf{\Phi}(G)) \neq 1.$$

By [3, (III.4.4)] M has a complement T in G. Note that $T \simeq G/M$. Let $K_0 = K \cap T$ and observe that K_0 acts faithfully on M.

Assume first that $\overline{G}$ is as in (B). Then G has exactly one conjugacy class of q-elements and this is the class of size a multiple of p. It follows that for any $x \in K_0 - \{1\}$ and $m \in M - \{1\}$ we have $xm \neq mx$, as otherwise the size of the class of mx would also be a multiple of p. Therefore, $K_0 \simeq \overline{F}$ is an elementary abelian q-group that acts fixed-point freely on M and hence K_0 is cyclic of prime order q. Since T is a doubly transitive Frobenius group with Frobenius kernel K_0 and Frobenius complement T/K_0, we see that $|T/K_0| = q - 1$. In particular then $q \geqslant 3$, as p divides $|T/K_0|$. We observe that [5, Theorem 15.16] implies that $q - 1$ divides $a = \dim_{\mathrm{GF}(t)}(M)$. Now, as G has only one conjugacy class of size divisible by p, $\mathrm{C}_T(m)$ contains a Sylow p-subgroup of T for all $m \in M - \{1\}$. But $\mathrm{C}_T(m) \cap K_0 = 1$ and then $\mathrm{C}_T(m)$ is isomorphic to a subgroup of T/K_0. Hence $\mathrm{C}_T(m)$ contains exactly one Sylow p-subgroup of T, for every $m \in M - \{1\}$, and it follows that $\{\mathrm{C}_M(P_0) - \{1\} \mid P_0 \in \mathrm{Syl}_p(T)\}$ is a partition of $M - \{1\}$. Since T has $q = |K_0|$ Sylow p-subgroups we obtain the relation $t^a - 1 = q(t^b - 1)$ where $t^b = |\mathrm{C}_M(P_0)|$, $P_0 \in \mathrm{Syl}_p(T)$. Note that $1 \leqslant b < a$ and that b divides a, because $(t^a - 1, t^b - 1) = t^{(a,b)} - 1$. In particular, $b \leqslant (a/2)$ and hence $q \geqslant t^{a/2} + 1 > t^{(q-1)/2}$. Observe now that $t = 2$ implies $q \geqslant 7$, since p divides $q - 1$ and $p \neq t$ because M is a subgroup of the p'-group K. We hence have a contradiction, because $2^{(q-1)/2} \geqslant q$ for all $q \geqslant 7$ and $t^{(q-1)/2} \geqslant 3^{(q-1)/2} \geqslant q$ for all $t, q \geqslant 3$.

Assume now that $\overline{G}$ is as in (C). Write $L_0 = L \cap T$ and observe that p divides $|\mathrm{cl}_G(x)|$ for all $x \in K_0 - L_0$. Arguing as before, we have $C_{K_0}(m) \leqslant L_0 = \mathbf{Z}(K_0)$ for every $m \in M - \{1\}$. Since $K_0 \simeq K/M = \overline{F}$ is semi-extraspecial, by Lemma 4.3 we deduce that K_0 is isomorphic to the quaternion group of order 8. Since T/K_0 acts regularly on K_0/L_0, it follows that $|T/K_0| = 3$. As above we get that $t^a - 1 = 4(t^b - 1)$ and $1 \leqslant b \leqslant a/2$. This implies $t^b + 1 \leqslant 4$, which gives either $t = 2 = q$ or $t = 3 = p$, a contradiction.

Therefore, we have proved that M is a q-group. Hence, K is a q-group and then $\mathrm{F}(G) = K$.

Step 5. $M \leqslant \mathrm{Z}(K)$ and P centralizes M.

Indeed, $M \cap \mathrm{Z}(K)$ is non-trivial and normal in G and hence $M \leqslant \mathrm{Z}(K)$. Further, observe that the conjugacy class of G of size divisible by p is not contained in M and hence p does not divide $|G : \mathrm{C}_G(m)|$ for all $m \in M$. Since $K \leqslant \mathrm{C}_G(m)$ and G/K has just one Sylow p-subgroup, then $\mathrm{C}_G(m)$ contains all Sylow p-subgroups of G, for every $m \in M$. Hence, P centralizes M.

Step 6. The group G/M is as in (B).

Assume, working by contradiction, that G/M is as in (C). Recall now that G/L is a doubly transitive Frobenius group, with kernel K/L and complement of order divisible by p. In particular, all elements in $K - L$ have G-conjugacy classes of size a multiple of p and hence by our assumption $K - L$ is a conjugacy class of G. Observe that $L/M = \mathrm{Z}(K/M)$ is centralized by PM/M. Further, by Step 5, P centralizes M and hence, by coprimality, P centralizes L.

Now let A be any characteristic abelian subgroup of K. We prove that $A \leqslant L$. If $A \cap (K - L) \neq \varnothing$, then $K - L \subseteq A$ because $A \lhd G$ and $K - L$ is a G-conjugacy class. Since $L/M = \mathbf{\Phi}(K/M)$, it follows that $AM/M = K/M$ and $AM = K$. Note that if $A \cap M = 1$ then $K/M \simeq A$, but K/M is non-abelian if G/M is of type (C). So, $M \leqslant A$ and $K = A$ is abelian, again a contradiction. We conclude that every characteristic abelian subgroup of K is contained in L and hence P acts trivially on it. Note also that $K = [K, P]$: if D is the normal p-complement of G, then $K = [DP, P] = [D, P]P' = [D, P]$ and $[K, P] = [D, P, P] = [D, P] = K$.

Hence, by [3, (III.13.6)] it follows that K is a special q-group, i.e. we have $\mathrm{Z}(K) = K' = \mathbf{\Phi}(K)$ and $\mathrm{Z}(K)$ is elementary abelian.

Observe that $L/M = (K/M)' = K'M/M$ and hence $L = K'M = \mathrm{Z}(K)M$. As $M \leqslant \mathrm{Z}(K)$, it follows that $L = \mathrm{Z}(K)$. Hence, by Lemma 4.1 K is a semi-extraspecial q-group and $|\mathrm{cl}_G(x)| = |L|$ for all $x \in K - L$.

Write $|K/L| = q^{2m}$, with m a positive integer. Then $\mathrm{rk}(L) \leqslant m$. Recall now that K/M is ultraspecial and hence the rank of $\mathrm{Z}(K/M) = L/M$ is m. As L is elementary abelian, this implies that $M = 1$, a contradiction.

We have hence proved that G/M must be as in (B), i.e. G/M is a doubly transitive Frobenius group with Frobenius complement $\mathrm{C}_{G/M}(PM/M)$. By Step 5, P centralizes M and hence $M = \mathrm{C}_G(P) \cap K$, because P acts fixed-point freely on K/M.

Step 7. K is semi-extraspecial and $M = \mathrm{Z}(K) = K'$.

As G/M is doubly transitive, K/M is a chief factor of G. It follows that $M = K'$, as $1 \neq K' \leqslant M$ and M is minimal normal in G. Similarly, $1 \neq M \cap \mathrm{Z}(K) \lhd G$ and then $M \leqslant \mathrm{Z}(K) < K$ implies $M = \mathrm{Z}(K)$. Finally, observe that all elements in $K - M$ must be conjugate in G and hence K is semi-extraspecial by Lemma 4.1.

In the following let X be a complement of K in G, with $P \leqslant X$. Then $X \simeq XM/M$ is a Frobenius complement of the doubly transitive Frobenius group G/M and hence it is isomorphic to the multiplicative group of a finite near field. Also, $P \leqslant \mathrm{Z}(X)$ is an abelian Sylow subgroup of a Frobenius complement and hence P is cyclic.

Step 8. p is odd and G/M is of Dickson type.

Let C be a cyclic subgroup of $\mathrm{C}_X(M)$ and Z a maximal subgroup of M. Then C acts on the extraspecial group K/Z, centralizing $\mathrm{Z}(K/Z) = M/Z$ and acting fixed-point freely on K/M. By Lemma 2.4 (i) we have

(∗) $|C|$ divides either $q^m - 1$ or $q^m + 1$, where $q^{2m} = |K/M|$.

Recalling that $P \leqslant \mathrm{C}_X(M)$ is cyclic and that $|P|$ is the p-part of $|X| = q^{2m} - 1$, we see that p must be odd: if $p = 2$, then q is odd and both $q^m - 1$ and $q^m + 1$ are even, so $|P| > \max\{(q^m - 1)_2, (q^m + 1)_2\}$ against (∗).

We now show that X cannot be isomorphic to the multiplicative group of an exceptional near field. Recall that in this case $|K/M| = q^2$ and then K is extraspecial by Step 7.

We have three cases:

Case (i). $p = 11$, $q = 23$, $X \simeq H \times C_{11}$ and H has a subgroup of index 2 isomorphic to $\mathrm{SL}(2, 3)$: in this case $|X/\mathrm{C}_X(M)|$ divides 2, since it divides $q - 1$ and is coprime to p. In particular, $\mathrm{C}_X(M)$ has an element of order $3 \cdot 11 > q + 1$, against (∗).

Case (ii). $p = 7$, $q = 29$, $X \simeq \mathrm{SL}(2, 5) \times C_7$: in this case X centralizes M, but we get a contradiction to (∗) since X has elements of order $35 > q + 1$.

Case (iii). $p = 29$, $q = 59$, $X \simeq \mathrm{SL}(2, 5) \times C_{29}$: here again X centralizes M and has an element of order $5 \cdot p > q + 1$.

It follows that G/M is of Dickson type. Hence X is metacyclic, and in particular G is solvable. Also, there are a divisor v of $2m$ and a cyclic normal subgroup U of X such that $|U| = (q^{2m} - 1)/v$. Any prime divisor of v divides $q^{2m/v} - 1$ and if 4 divides v then 4 divides $q^{2m/v} - 1$, too. Further, U is a maximal abelian normal subgroup of X. (See [10, IV (1.1) and (1.5) (d)]).

Step 9. K is ultraspecial.

Write $|K/M| = q^{2m}$. Let $|M| = q^a$ with $a \leqslant m$. We have to show that $a = m$. We may assume that $m > 1$.

In the case $v = 1$, the near field is in fact a field, $X/\mathrm{C}_X(M)$ is cyclic and acts irreducibly on M. So $|X/\mathrm{C}_X(M)|$ divides $q^a - 1$ by Lemma 2.3. Also, $\mathrm{C}_X(M)$ is cyclic and by (∗) we have $|\mathrm{C}_X(M)| \leqslant q^m + 1$. It follows that

$$q^{2m} - 1 = |X| = |X/\mathrm{C}_X(M)|\,|\mathrm{C}_X(M)| \leqslant (q^a - 1)(q^m + 1)$$

and this forces $a = m$.

We can now assume that $v > 1$.

If $q^{2m} - 1$ has no Zsigmondy prime divisor, recalling that $m > 1$ we conclude that $q = 2$ and $2m = 6$. But then $|X| = 2^6 - 1 = 3^2 \cdot 7$ and $p = 3$ or $p = 7$. But $P \leqslant \mathrm{Z}(X)$ and this implies that X is abelian, contradicting $v > 1$.

Hence we can assume that $q^{2m} - 1$ has Zsigmondy prime divisors. We prove

(∗∗) $|U/\mathrm{C}_U(M)|$ is a multiple of $(q^m - 1)/v$.

To show this, let r be a Zsigmondy prime divisor of $q^{2m}-1$. Then r divides $|C_U(M)|$, as r does not divide $|\mathrm{Aut}(M)|$. By Lemma 2.3 the subgroup $C_U(M)$ acts irreducibly on K/M. If Z is a maximal subgroup of M, then K/Z is extraspecial by Step 7. In this case, $C_U(M) \leqslant \mathrm{Aut}(K/Z)$ acts trivially on $Z(K/Z) = M/Z$ and acts irreducibly on $(K/Z)/(Z(K/Z))$ and then by Lemma 2.4(ii) we have that $|C_U(M)|$ divides q^m+1. Hence $|U/C_U(M)|$ is a multiple of $(q^m-1)/v$ and $(**)$ is proved.

Let us consider first the case that q^m-1 has no Zsigmondy prime divisor. Then we have two cases:

Case (i). q is a Mersenne prime and $m=2$: since $v \mid 2m$ and $v \neq 4$ because $q \not\equiv 1 \pmod 4$, it follows that $v=2$. By $(**)$, $|U/C_U(M)|$ is a multiple of $(q^2-1)/2$. But then M is not cyclic, so $a>1$ and hence $a=2=m$.

Case (ii). $q=2$ and $m=6$: in this case v is odd (as the prime divisors of v divide q^k-1 for some k) and hence $v=3$. By $(**)$, $|U/C_U(M)|$ is a multiple of $(q^6-1)/3=21$. So there exists an irreducible submodule V of M_U such that the subgroup of order 7 of U acts non-trivially on V. It follows that $\dim_{\mathrm{GF}(2)}(V) \geqslant 3$. By Clifford's theorem, $\dim_{\mathrm{GF}(2)}(V)$ divides a and hence $a=3$ or $a=6$. If $a=3$, then M_U is irreducible and by [3, (II.3.10)] it follows that $|U/C_U(M)|$ divides q^3-1, a contradiction. Hence, $a=6=m$.

Assume now that there exists a Zsigmondy prime divisor t of q^m-1. Note that m is the order of q modulo t and hence, in particular, m divides $t-1$.

If $t \mid v$, recalling that $v \mid 2m$ and that m divides $t-1$, we have $t \mid 2m \mid 2(t-1)$ and then $t \mid 2$, a contradiction. Hence, t does not divide v.

It follows that t divides $(q^m-1)/v$ and hence by $(**)$ divides $|U/C_U(M)|$. Hence t divides $|\mathrm{Aut}(M)|$ and this implies that $a=m$.

We have hence proved that G is one of the groups in (c) of Theorem A.

Now assume, conversely, that G is one of the groups described in (a), (b), (c) of Theorem A.

If G is a Frobenius group with complement of order 2, then the Frobenius kernel K is abelian and $G-K$ is the unique conjugacy class of G whose size is divisible by any prime divisor p of $|K|$.

Let G be a doubly transitive Frobenius group with complement $H=C_G(P)$, where P is a Sylow p-subgroup of G. The elements whose conjugacy classes have size divisible by p are precisely the non-trivial elements of the Frobenius kernel and they form a conjugacy class in G, because H acts transitively on them.

Finally, let G be one of the groups in point (c), with $K=F(G)$ semi-extraspecial and $M=Z(K)=K'$. Observe that for every $x \in K-M$ we have $[x,K]=M$, as $Z(K/Z)=M/Z$ for each proper subgroup Z of M. It follows that xM is the conjugacy class of x in K. Since G/K acts regularly on the non-trivial elements of K/M, it follows that $K-M$ is a G-conjugacy class. Further, $G/M=(K/M)(H/M)$ is a doubly transitive Frobenius group, where $H=C_G(P)$, $P \in \mathrm{Syl}_p(G)$. Observe that, in particular, $P \neq 1$. The Frobenius kernel of G/M is the unique minimal normal subgroup of G/M and hence coincides with K/M. So, $G/M-K/M$ is the union of

conjugates of H/M. As $M \leqslant H = \mathrm{C}_G(P)$, we conclude that $K - M$ is precisely the set of all elements of G with conjugacy class size divisible by p. □

5 Examples

In this section we address the question whether the groups described in Theorem A do actually exist.

The construction of the groups in (a) is straightforward: one just takes the semidirect product of any abelian group A of odd order with the inversion automorphism. In this case p can be any prime divisor of $|A|$.

For the discussion of the groups of type (b) and (c), we need some more details concerning the structure of the Dickson near fields.

A finite near field $E(+,\circ)$ is a Dickson near field if and only if there exists a third binary operation $\cdot$ defined on E such that $E(+,\cdot)$ is a field and there exists a group homomorphism $\rho : E^{\#}(\circ) \to \mathrm{Gal}(E(+,\cdot))$, where $E^{\#} = E - \{0\}$, such that

$$a \circ b = a^{\rho(b)} \cdot b$$

for all $a, b \in E$ with $b \neq 0$ (see [6, pp. 31–33]). In particular, the identity elements for the operations $\circ$ and $\cdot$ coincide.

Let $\Gamma = \mathrm{Im}(\rho)$ and let L be the fixed field of Γ. If $m = |\Gamma|$ and $r = |L|$, then $E(+,\circ)$ is said to be a Dickson near field of type $\{r, m\}$. Note that $|E| = r^m$ and that r is a power of the characteristic q of the field $E(+,\cdot)$.

A pair of positive integers $\{r, m\}$ is a *Dickson pair* if the following three conditions hold: (1) r is a prime power; (2) every prime divisor of m divides $r - 1$; (3) $r \equiv 1 \pmod 4$ if $m \equiv 0 \pmod 4$. It can be proved that there exists a Dickson near field of type $\{r, m\}$ if and only if $\{r, m\}$ is a Dickson pair (see [6, Theorems 7.3 and 7.4]).

Now let $U = \mathrm{Ker}(\rho)$. Observe that $|U| = (r^m - 1)/m$ and that $\circ$ and $\cdot$ are the same operation on U and hence U is cyclic.

In the following, we write for short $X = E^{\#}(\circ)$. It is known that the center of the near field $E(+,\circ)$ is $L = \mathrm{Fix}(\Gamma)$. Hence, in particular, $|\mathrm{Z}(X)| = r - 1$. Therefore, $\mathrm{Z}(X)$ contains a non-trivial Sylow p-subgroup P of X if and only if p divides $r - 1$ and p does not divide $(r^m - 1)/(r - 1)$. Thus, $P \leqslant \mathrm{Z}(X)$ if and only if p divides $r - 1$ and p does not divide m.

It follows that the groups in (b) are precisely the semidirect products $E(+) \rtimes X$ where $E(+,\circ)$ is either one of the three exceptional near fields mentioned in (i), (ii) and (iii) in Section 2, or a Dickson near field of type $\{r, m\}$ where p is a prime divisor of $r - 1$ such that p does not divide m.

We now come to groups of type (c), i.e. groups $G = K \rtimes X$ where K is an ultraspecial q-group, $G/\mathrm{Z}(K)$ is a group of type (b) and there is a non-trivial $P \in \mathrm{Syl}_p(X)$ with $p \neq 2$, such that $P \leqslant \mathrm{Z}(X)$ and P centralizes $\mathrm{Z}(K)$. Write $|K/\mathrm{Z}(K)| = q^{2n}$. Since X is the multiplicative group of a Dickson near field of some type $\{r, m\}$, by the previous discussion $P \leqslant \mathrm{Z}(X)$ implies that p divides $r - 1$ and that p does not divide m. Since $r^m = |K/\mathrm{Z}(K)| = q^{2n}$, it follows that $m \mid 2n$ and that $r = q^{2n/m}$. Further,

arguing as in the proof of Step 9, one can see that $P \leqslant C_X(Z(K))$ implies that p divides $q^n + 1$. Hence, p divides $(q^{2n/m} - 1, q^n + 1)$. If m is even, then $2n/m$ divides n and hence $q^{2n/m} - 1$ divides $q^n - 1$, which gives that $(q^{2n/m} - 1, q^n + 1)$ divides $(q^n - 1, q^n + 1)$, against $p \neq 2$. Thus m must be odd. We collect together the arithmetical conditions concerning the relevant invariants of a group of type (c):

(c1) m is odd, $m \mid n$ and $\{q^{2n/m}, m\}$ is a Dickson pair;

(c2) $p \neq 2$, $(p, m) = 1$ and p divides $(q^{2n/m} - 1, q^n + 1)$.

We now show that these groups do actually exist. Let p, q be primes and n, m be positive integers that satisfy (c1) and (c2). To build the ultraspecial group K and a suitable subgroup X of $\mathrm{Aut}(K)$, we use a variation of a construction due to M. Isaacs.

Let $E = E(+, \cdot) = \mathrm{GF}(q^{2n})$ and let $\sigma \in \mathrm{Gal}(E \mid \mathrm{GF}(q))$ be the Galois automorphism of order 2. Let $F = \mathrm{Fix}(\sigma)$; $|F| = q^n$. Choose any element $\gamma \in E$ such that $\gamma^\sigma = -\gamma$ and define $\langle x, y \rangle = \gamma(x \cdot y^\sigma - y \cdot x^\sigma)$ for $x, y \in E$.

Consider $K = \{(x, z) \mid x \in E, z \in F\}$ and define, for $(x, z), (y, w) \in K$,

$$(x, z) * (y, w) = (x + y, z + w + \langle x, y \rangle).$$

Then $K(*)$ turns out to be an ultraspecial q-group, with $|K/Z(K)| = q^{2n}$ and $Z(K) = \{(0, z) \mid z \in F\}$.

Now let $\circ$ be a binary operation on E such that $E(+, \circ)$ is a Dickson near field of type $\{q^{2n/m}, m\}$ and let ρ be the relevant homomorphism from $X = E^{\#}(\circ)$ to $\mathrm{Gal}(E \mid \mathrm{GF}(q))$. Recall that $a \circ b = a^{\rho(b)} \cdot b$ for $a, b \in X$ (also, $0 \circ a = a \circ 0 = 0$ for all $a \in E$) and that $Z(X) = L - \{0\}$, where $L = \mathrm{Fix}(\mathrm{Im}(\rho))$.

We define, for $(x, z) \in K$ and $a \in X$,

$$(x, z)^a = (x^{\rho(a)} \cdot a, y^{\rho(a)} \cdot a \cdot a^\sigma).$$

It is not hard to verify that this defines an embedding of X in $\mathrm{Aut}(K)$, provided that $\langle x, y \rangle^\alpha = \langle x^\alpha, y^\alpha \rangle$ for all $\alpha \in \Gamma$ and $x, y \in E$, which is equivalent to $\gamma \in Z(X)$. To show that there exists a $\gamma \in Z(X)$ such that $\gamma^\sigma = -\gamma$, we consider the endomorphism φ of $C = E^{\#}(\cdot)$ defined by $\varphi(x) = x^{-1} \cdot x^\sigma$ (where x^{-1} is the inverse of x in C). We want to show that there exists $\gamma \in Z(X)$ such that $\varphi(\gamma) = -1$. If $q = 2$, $\gamma = 1$ will do. Assuming that q is odd, it is enough to show that $|Z : Z \cap \mathrm{Ker}(\varphi)|$ is even, where $Z = Z(X)$. Since $\circ$ and $\cdot$ induce the same operation on Z, Z and $\mathrm{Ker}(\varphi)$ are subgroups of the cyclic group C and this implies that $|Z \cap \mathrm{Ker}(\varphi)| = (|Z|, |\mathrm{Ker}(\varphi)|) = (q^{2n/m} - 1, q^n - 1)$. Thus, in particular we see that the 2-part of $|Z \cap \mathrm{Ker}(\varphi)|$ divides the 2-part of $q^n - 1$. As m is odd, the 2-part of $|Z| = q^{2n/m} - 1$ coincides with the 2-part of $q^n - 1$ and hence $|Z : Z \cap \mathrm{Ker}(\varphi)|$ is even.

Let $G = K \rtimes X$ be the semidirect product with respect to the action defined above. Let P be a Sylow p-subgroup of X. By (c1) and (c2), we see that P is non-trivial and that $P \leqslant Z(X)$. Observe also that $P \leqslant U = \mathrm{Ker}(\rho)$, because p does not divide $m = |X : U|$. Further, as $2 \neq p$ divides $q^n + 1$ and $|P|$ is the p-part of $q^{2n} - 1$, we

see that $|P|$ divides $q^n + 1$. Since $N = \{a \in E^{\#} \mid a \cdot a^{\sigma} = 1\}$ and P are both subgroups of the cyclic group $E^{\#}(\cdot)$ and $|N| = q^n + 1$, it follows that $P \leqslant N$. From the definition of the action, we see that $P \leqslant U \cap N$ implies that P centralizes $\mathrm{Z}(K)$.

Finally, observe that $G/\mathrm{Z}(K)$ is isomorphic to $E(+) \rtimes X$, the semidirect product with respect to the action given by right multiplication, and hence it is a doubly transitive Frobenius group of Dickson type. Also, $\mathrm{C}_G(P) = \mathrm{Z}(K)P$ and then G is of type (c).

In conclusion, we have shown that there exists a group of type (c) if and only if the numbers p, q, n, m satisfy the conditions (c1) and (c2). We remark finally that the set of quadruples (p, q, n, m) satisfying the conditions (c1) and (c2) is non-empty: for instance, $p = 3$, $q = 29$, $n = 5$, $m = 5$ or $p = 5$, $q = 2$, $n = 6$, $m = 3$ or $p = 7$, $q = 13$, $n = 3$, $m = 3$.

Acknowledgements. The first author is partially supported by MURST project Teoria dei Gruppi e Applicazioni. The second and third authors are partially supported by the Ministerio de Educación y Ciencia proyecto MTM2004-06067-C02-01 and MTM2004-04665. The second author is also supported by the Programa Ramón y Cajal. The authors thank the referee for his careful reading of the paper.

References

[1] B. Beisiegel. Semi-extraspezielle p-Gruppen. *Math. Z.* **156** (1977), 247–254.
[2] The GAP Group. GAP—Groups, Algorithms, and Programming, Version 4.4.9; 2006. http://www.gap-system.org.
[3] B. Huppert. *Endliche Gruppen*, vol. 1 (Springer-Verlag, 1967).
[4] B. Huppert and N. Blackburn. *Finite groups*, vol. 2 (Springer-Verlag, 1982).
[5] I. M. Isaacs. *Character theory of finite groups* (Dover, 1994).
[6] H. Lüneburg. *Translation planes* (Springer-Verlag, 1980).
[7] A. Moretó, G. Navarro and P. H. Tiep. (In preparation.)
[8] A. Moretó and P. H. Tiep. Prime divisors of character degrees. *J. Group Theory* **11** (2008), 341–356.
[9] A. Seress. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc.* **29** (1997), 697–704.
[10] H. Wähling. *Theorie der Fastkörper* (Thales Verlag, 1987).

Received 10 September, 2007; revised 28 March, 2008

Silvio Dolfi, Dipartimento di Matematica, Università di Firenze, 50134 Firenze, Italy
E-mail: dolfi@math.unifi.it

Alexander Moretó, Departament d'Àlgebra, Facultat de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain
E-mail: alexander.moreto@uv.es

Gabriel Navarro, Departament d'Àlgebra, Facultat de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain
E-mail: gabriel.navarro@uv.es