



Contents lists available at [ScienceDirect](https://www.sciencedirect.com)

Journal of Algebra

journal homepage: [www.elsevier.com/locate/jalgebra](http://www.elsevier.com/locate/jalgebra)



Research Paper

# On the structure of the character degree graphs having diameter three



Silvio Dolfi <sup>a</sup>, Roghayeh Hafezieh <sup>b</sup>, Pablo Spiga <sup>c,\*</sup>

<sup>a</sup> *Dipartimento di Matematica e Informatica U. Dini, Università degli Studi di Firenze, viale Morgagni 67/a, 50134 Firenze, Italy*

<sup>b</sup> *Department of Mathematics, Gebze Technical University, P.O. Box 41400, Gebze, Turkey*

<sup>c</sup> *Dipartimento di Matematica Pura e Applicata, University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy*

## ARTICLE INFO

### Article history:

Received 3 May 2024

Available online 11 August 2025

Communicated by E.I. Khukhro

### MSC:

primary 20C15

### Keywords:

Character degree graph

Solvable groups

## ABSTRACT

The structure of the character degree graphs  $\Delta(G)$ , i.e. the prime graphs on the set  $\text{cd}(G)$  of the irreducible character degrees of a finite group  $G$ , such that  $G$  is solvable and  $\Delta(G)$  has diameter three, remains an intriguing area of study. However, a comprehensive understanding of these structures remains elusive. In this paper, we prove some properties and provide an infinite series of examples of this class of graphs, building on the ideas of M. Lewis [8].

© 2025 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Consider a finite group  $G$ , and let  $\text{Irr}(G)$  be the collection of all irreducible complex characters of  $G$ . We define  $\text{cd}(G)$  as the set containing the degrees of these characters, denoted by  $\chi(1)$ , where  $\chi$  belongs to  $\text{Irr}(G)$ . Consequently, the *character degree graph*

\* Corresponding author.

*E-mail addresses:* [silvio.dolfi@unifi.it](mailto:silvio.dolfi@unifi.it) (S. Dolfi), [roghayeh@gtu.edu.tr](mailto:roghayeh@gtu.edu.tr) (R. Hafezieh), [pablo.spiga@unimib.it](mailto:pablo.spiga@unimib.it) (P. Spiga).

$\Delta(G)$  is defined as the graph whose vertex set  $V(G)$  is the set of all prime numbers dividing some degree  $\chi(1)$  in  $\text{cd}(G)$ . In this graph, two distinct primes,  $p$  and  $q$ , are adjacent if their product  $pq$  divides any degree within  $\text{cd}(G)$ .

The exploration of the character degree graph  $\Delta(G)$  and the correlations between its properties and the structural characteristics of the group  $G$  constitute a well-explored area with an extensive body of literature. For a comprehensive overview of this subject, we recommend consulting the survey paper [9]. The objective of this paper is to contribute to a specific facet of this research endeavor: the structure of  $\Delta(G)$ , when  $G$  is a solvable group and  $\Delta(G)$  has diameter three.

A pivotal result established by P. P. Pálffy [13] asserts that, if  $G$  is a solvable group then, for any three distinct primes in the set  $V(G)$ , at least two of them form an adjacent pair in the character degree graph  $\Delta(G)$ . Consequently, it easily follows that, for a solvable group  $G$ ,  $\Delta(G)$  has at most two components, which are complete if  $\Delta(G)$  is not connected. Additionally, in [10], it was shown that if  $\Delta(G)$  is connected, then the diameter of  $\Delta(G)$  is at most 3. Moreover, Pálffy proved in [14] that there is a remarkable difference between the sizes of the two connected components of a disconnected character degree graph of a solvable group. Namely, if  $m$  and  $n$  are their sizes, say  $n \geq m$ , then  $n \geq 2^m - 1$ .

For a considerable time, it remained an open question whether solvable groups with character degree graphs of diameter three existed. Eventually, in [8], Mark Lewis resolved the matter, presenting a beautiful solvable group  $G$  with  $\Delta(G)$  comprising 6 vertices and possessing a diameter of 3 (see Fig. 1).

The structure of the solvable groups  $G$  such that the character degree graph  $\Delta(G)$  has diameter three, as well as some properties of the graph  $\Delta(G)$ , have been further studied in [2] and [16]. In particular, it turns out that in this case the group  $G$  has a unique non-abelian Sylow subgroup  $P$  and that  $\Delta(G/\gamma_3(P))$ , where  $\gamma_3(P) = [P', P]$  is the third term of the descending central series of  $P$ , is a disconnected subgraph of  $\Delta(G)$ , with the same vertex set. Let  $\pi_0$  and  $\pi_1$  denote the connected components of  $\Delta(G/\gamma_3(P))$ , with the notation chosen such that the prime divisor  $p$  of  $|P|$  belongs to  $\pi_1$ . In this context, it is established that  $|\pi_1| \geq 2^{|\pi_0|}$  ([2, Remark 4.4] and [16, Theorem 4]). So, the vertex set of  $\Delta(G)$  is covered by two cliques with vertex sets  $\pi_0$  and  $\pi_1$  of rather different sizes.

Let  $\Delta = \Delta(G)$ , for  $G$  solvable, be a graph of diameter three. Proceeding as in [16], we denote by  $\alpha_\Delta \subseteq \pi_0$  the set of vertices of  $\pi_0$  that are not adjacent to any vertex in  $\pi_1$  and by  $\delta_\Delta \subseteq \pi_1$  the set of vertices of  $\pi_1$  that are not adjacent to any vertex in  $\pi_0$ . Since  $\Delta$  has diameter three, every pair of vertices  $s \in \alpha_\Delta$  and  $t \in \delta_\Delta$  has distance three in  $\Delta(G)$ , while all the other pairs of vertices have distance at most two, and the edges linking  $\pi_0$  and  $\pi_1$  have one vertex in  $\beta_\Delta = \pi_0 \setminus \alpha_\Delta$  and the other in  $\gamma_\Delta = \pi_1 \setminus \delta_\Delta$ , (see Fig. 2).

With respect to this notation, in the example  $\Delta = \Delta(G)$  given in [8] we have  $|\alpha_\Delta| = |\beta_\Delta| = |\delta_\Delta| = 1$  and  $|\gamma_\Delta| = 3$ , (see Fig. 1).

To the best of our knowledge, the example in [8] appears to be the only example in the literature of a character degree graph of a solvable group, having diameter three. In

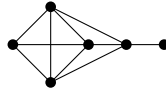


Fig. 1. Lewis’ example.

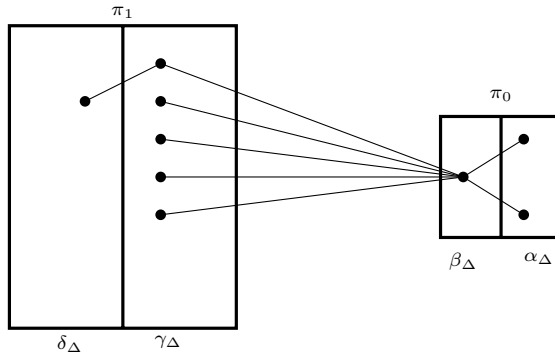


Fig. 2. An auxiliary picture for  $\Delta(G)$  having diameter 3.

Section 3, building on the ideas of [7] and [8], we construct a class of examples of solvable groups that yield the following result.

**Theorem A.** *For every choice of positive integers  $a, b$ , there exists a solvable group  $G$  such that  $\Delta = \Delta(G)$  has diameter three with  $|\alpha_\Delta| = a$  and  $|\delta_\Delta| \geq b$ .*

We also prove

**Theorem B.** *Let  $\Delta = \Delta(G)$  for a solvable group  $G$  and assume that  $\Delta$  has diameter three. Then*

$$|\gamma_\Delta| \geq 2^{|\beta_\Delta|} (2^{|\alpha_\Delta|} - 1) + 1.$$

We believe that  $|\beta_\Delta|$  is related to the nilpotency class of  $P$ .

**Question 1.1.** *Let  $G$  be a solvable group such that  $\Delta(G)$  has diameter three. Is it true that  $|\beta_\Delta|$  is at most the number of primes less than the nilpotency class of the non-abelian normal Sylow subgroup of  $G$ ?*

Actually, we are not aware of any examples with  $|\beta_\Delta| > 1$ . We remark that, for all the character graphs  $\Delta = \Delta(G)$  of the solvable groups in Section 3, and in Theorem A, as well as in Lewis’ example [8], the set  $\beta_\Delta$  consists of a single vertex, namely the prime 3, which is then a *cut-vertex* of  $\Delta$ . This information naturally motivates the following two questions:

**Question 1.2.** *Are there solvable groups  $G$  such that  $\Delta = \Delta(G)$  has diameter three and  $\beta_\Delta$  consists of a single vertex different from the prime 3?*

**Question 1.3.** *Are there solvable groups  $G$  such that  $\Delta = \Delta(G)$  has diameter three and  $|\beta_\Delta| \geq 2$ ?*

The character degree graphs possessing a cut-vertex have been studied in [4] and [11] for solvable groups, and they have been fully described for non-solvable groups in [3]. In particular, when  $G$  is non-solvable,  $\Delta(G)$  has a cut-vertex and diameter three if and only if  $G = J_1 \times A$ , where  $J_1$  is the first Janko group and  $A$  is an abelian group ([3, Theorem A(d)]).

Question 1.3 is quite challenging at present, as our existing methods do not appear sufficiently effective. Furthermore, our current intuition is heavily biased towards the known examples. In light of this, we propose the following alternative, possibly more manageable, question.

**Question 1.4.** *Let  $\Delta = \Delta(G)$  for a solvable group  $G$  with  $\Delta$  having diameter 3. Is  $\lim_{|\pi_0| \rightarrow \infty} \frac{|\alpha_\Delta|}{|\pi_0|} = 1$ ?*

Inspired by our work, we also pose the following.

**Question 1.5.** *Let  $\Delta = \Delta(G)$  for a solvable group  $G$  with  $\Delta$  having diameter 3. Is  $\lim_{|\pi_1| \rightarrow \infty} \frac{|\delta_\Delta|}{|\pi_1|} = 0$ ?*

In Theorem 5.1 we prove that for a character degree graph  $\Delta = \Delta(G)$  of diameter three, where  $G$  is a solvable group, the union of the set  $\beta_\Delta$  with a relatively large portion of the set  $\gamma_\Delta$  induces a complete subgraph of  $\Delta$ . We leave open the following.

**Question 1.6.** *Let  $\Delta = \Delta(G)$  for a solvable group  $G$ . If  $\Delta$  has diameter three, then is the subgraph induced on  $\beta_\Delta \cup \gamma_\Delta$  a complete graph?*

## 2. Preliminaries

This section serves as a compilation of notation and fundamental results employed consistently throughout the paper, often applied without explicit reference.

Given an action of a group  $A$  on a set  $X$ , we say that  $X$  is an  $A$ -set. The action of  $A$  on  $X$  is *semi-regular* if all  $A$ -orbits in  $X$  have cardinality  $|A|$ , i.e. are regular orbits.

If  $A$  acts by automorphisms on a group  $G$  and  $A$  acts semi-regularly on  $G \setminus \{1\}$ , we say that  $A$  acts *fixed-point-freely* on  $G$ .

Two  $A$ -sets  $X$  and  $X_1$  are said to be *isomorphic* if there exists a bijection  $f : X \rightarrow X_1$  that commutes with the action of  $A$ . If this happens when  $A$  acts by automorphisms on the groups  $X$  and  $X_1$ , we say that  $X$  and  $X_1$  are isomorphic  $A$ -groups.

We denote by  $\text{Cl}(G)$  the set of the conjugacy classes of the group  $G$ . For  $g \in G$ , we write  $g^G$  for the  $G$ -conjugacy class of  $g$ . If a group  $A$  acts via automorphisms on a group  $G$ , then  $A$  acts naturally on  $\text{Irr}(G)$  and on  $\text{Cl}(G)$  as follows: for  $a \in A$ ,  $g^G \in \text{Cl}(G)$ ,  $\chi \in \text{Irr}(G)$ ,  $x \in G$ :

$$\chi^a(x) = \chi(x^{a^{-1}}) \quad \text{and} \quad (g^G)^a = (g^a)^G.$$

We denote by  $I_A(\chi) = \{a \in A \mid \chi^a = \chi\}$  the *inertia subgroup* of  $\chi$  in  $A$ , i.e. the stabilizer of  $\chi$  under the action of  $A$  on  $\text{Irr}(G)$ . The following facts will be used repeatedly.

**Lemma 2.1** ([6, Theorem 13.24]). *Let  $A$  be a solvable group acting by automorphisms on a group  $G$ . If  $|A|$  is coprime to  $|G|$ , then  $\text{Irr}(G)$  and  $\text{Cl}(G)$  are isomorphic  $A$ -sets.*

If  $M$  is an abelian group, we denote by  $\widehat{M}$  the *dual group* of  $M$ , which is the set  $\text{Irr}(M)$  with the natural product operation. If  $M$  is an abelian group such that  $A$  acts by automorphisms and such that  $|A|$  is coprime to  $|M|$ , then as a particular case of Lemma 2.1 we have that  $M$  and  $\widehat{M}$  are isomorphic  $A$ -groups.

Given a normal subgroup  $N$  of a group  $G$ ,  $G$  acts naturally by conjugation on  $\text{Irr}(N)$  and  $\text{Cl}(N)$ . For  $\theta \in \text{Irr}(N)$ , we use the following notation:

$$\text{Irr}(G|\theta) = \{\chi \in \text{Irr}(G) \mid [\chi_N, \theta] \neq 0\}$$

and, for a subset  $Y \subseteq \text{Irr}(N)$ ,

$$\text{Irr}(G|Y) = \bigcup_{\theta \in Y} \text{Irr}(G|\theta).$$

Moreover, we write  $\text{Irr}(G|N) = \text{Irr}(G|\text{Irr}(N) \setminus \{1_N\})$ ; so,  $\text{Irr}(G) = \text{Irr}(G/N) \dot{\cup} \text{Irr}(G|N)$ .

**Lemma 2.2.** *Let  $N$  be a normal subgroup of the group  $G$  and  $\theta, \theta_1 \in \text{Irr}(N)$ . Then  $\text{Irr}(G|\theta) = \text{Irr}(G|\theta_1)$  if and only if  $\theta$  and  $\theta_1$  lie in the same  $G$ -orbit in  $\text{Irr}(N)$ .*

*Let  $X$  be a subset of  $\text{Irr}(N)$  and let  $\mathcal{X}$  be a set of representatives for the non-empty intersections of the  $G$ -orbits in  $\text{Irr}(N)$  with  $X$ . Then*

$$\text{Irr}(N|X) = \bigcup_{\theta \in \mathcal{X}} \text{Irr}(N|\theta)$$

*is a disjoint union.*

**Proof.** For  $g \in G$ ,  $\chi \in \text{Irr}(G)$  and  $\theta \in \text{Irr}(N)$ ,

$$[\chi_N, \theta^g] = [\chi_N^g, \theta^g] = [\chi_N, \theta].$$

So, if  $\theta_1 = \theta^g$  for some  $g \in G$ , then  $\text{Irr}(G|\theta) = \text{Irr}(G|\theta_1)$ .

For  $\chi \in \text{Irr}(G)$ , the irreducible constituents of  $\chi_N$  form a  $G$ -orbit in  $\text{Irr}(N)$  by Clifford’s theorem, so  $\text{Irr}(G|\theta) \cap \text{Irr}(G|\theta_1) \neq \emptyset$  implies that  $\theta$  and  $\theta_1$  are  $G$ -conjugate, and the rest of the statement follows.  $\square$

We recall that a character  $\tau \in \text{Irr}(M)$ , where  $M$  is a normal subgroup of a group  $G$ , is *fully ramified with respect to  $G/M$*  if  $\tau$  is  $G$ -invariant and  $|\text{Irr}(G|\tau)| = 1$ . Observe that, given a group  $A$  that acts by automorphisms on  $G$  and an  $A$ -invariant normal subgroup  $N$  of  $G$ , if  $\tau$  is fully ramified with respect to  $G/N$  and  $\text{Irr}(G|\tau) = \{\chi\}$ , then the stabilizers in  $A$  of  $\tau$  and  $\chi$  coincide.

**Lemma 2.3.** *Let  $N$  be a normal subgroup of a group  $G$  and  $\theta \in \text{Irr}(N)$  such that  $\theta$  is  $G$ -invariant. If  $G/N$  is abelian, then there exists a unique subgroup  $U$  such that  $N \leq U \leq G$  and such that every  $\tau \in \text{Irr}(U|\theta)$  is a  $G$ -invariant extension of  $\theta$  and  $\tau$  is fully ramified with respect to  $G/U$ .*

*Moreover, if the group  $A$  acts by automorphisms on  $G$  and both  $N$  and  $\theta$  are  $A$ -invariant, then  $U$  is  $A$ -invariant.*

**Proof.** This is a slight rephrasing of Lemma 2.2 of [17].  $\square$

**3. A construction**

In the following, for a positive integer  $n$ , we denote by  $\pi(n)$  the set of the distinct prime divisors of  $n$  and, for a set of primes  $\sigma$ , we denote by  $n_\sigma$  (or simply by  $n_p$  if  $\sigma = \{p\}$ ) the  $\sigma$ -part of  $n$ , that is, the largest divisor  $k$  of  $n$  such that  $\pi(k) \subseteq \sigma$ .

Let  $p$  be a prime number and let  $n$  be an odd positive integer such that  $n \neq p$ ,  $n_3 = 3$  and

$$\gcd(p^n - 1, n) = 1. \tag{1}$$

Following [7], let  $F$  be a field of cardinality  $p^n$  and let  $F\{X\}$  be the skew polynomial ring with

$$Xa = a^p X,$$

for every  $a \in F$ . Next, let  $R$  be the quotient of  $F\{X\}$  by the ideal generated by  $X^4$  and let  $x$  be the image of  $X$  in  $R$ . Therefore,  $R = \{a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_0, a_1, a_2, a_3 \in F\}$ . Let  $J$  be the Jacobson radical of  $R$ , that is,  $J = \{a_1x + a_2x^2 + a_3x^3 \mid a_1, a_2, a_3 \in F\}$ . Now,

$$P = 1 + J,$$

is a subgroup of the group of units of  $R$ ,  $|P| = p^{3n}$  and each element of  $P$  is of the form  $1 + a_1x + a_2x^2 + a_3x^3$ , for some  $a_1, a_2, a_3 \in F$ .

Let  $C$  be the subgroup of the multiplicative group  $F \setminus \{0\}$  of the field  $F$  having order  $(p^n - 1)/(p - 1)$ . Clearly,  $C$  is cyclic. The group  $C$  acts as a group of automorphisms on  $P$  by letting (see [5])

$$\begin{aligned} (1 + a_1x + a_2x^2 + a_3x^3)^c &= 1 + a_1c^{\frac{p-1}{p-1}}x + a_2c^{\frac{p^2-1}{p-1}}x^2 + a_3c^{\frac{p^3-1}{p-1}}x^3 \\ &= 1 + a_1cx + a_2c^{p+1}x^2 + a_3c^{p^2+p+1}x^3, \end{aligned} \tag{2}$$

for every  $a_1, a_2, a_3 \in F$  and  $c \in C$ . Let  $T = P \rtimes C$ . Therefore,  $T$  is a group of order  $(p^n - 1)p^{3n}/(p - 1)$ .

Let  $H = \text{Gal}(F/F_p)$ , where  $F_p$  is the prime subfield of  $F$ ; thus,  $H$  is a cyclic group of order  $n$ . Now, the group  $H$  acts as a group of automorphisms on  $T$  by letting

$$((1 + a_1x + a_2x^2 + a_3x^3)c)^\sigma = (1 + a_1^\sigma x + a_2^\sigma x^2 + a_3^\sigma x^3)c^\sigma, \tag{3}$$

for every  $a_1, a_2, a_3 \in F$ ,  $c \in C$  and  $\sigma \in H$ .

Let

$$G = T \rtimes H = P \rtimes (C \rtimes H).$$

Therefore,  $G$  is a group of order  $n(p^n - 1)p^{3n}/(p - 1)$  and  $CH$  is a complement of  $P$  in  $G$ .

Recall that  $n_3 = 3$ . Let  $D$  be the subgroup of  $C$  having order  $p^2 + p + 1 = (p^3 - 1)/(p - 1)$ .

**Lemma 3.1.** *The number  $(p^3 - 1)/(p - 1)$  and  $(p^n - 1)/(p^3 - 1)$  are relatively prime.*

*Moreover,  $p - 1$  is relatively prime to  $(p^n - 1)/(p - 1)$ .*

**Proof.** We have  $(p^3 - 1)/(p - 1) = p^2 + p + 1$  and

$$\frac{p^n - 1}{p^3 - 1} = p^{n-3} + p^{n-6} + \dots + p^3 + 1 \equiv \underbrace{1 + 1 + \dots + 1 + 1}_{n/3 \text{ times}} \pmod{p^3 - 1}.$$

This shows that, if  $d$  divides  $p^2 + p + 1$  and  $(p^n - 1)/(p^3 - 1)$ , then  $d$  divides  $n/3$ . Since, by hypothesis,  $\text{gcd}(p^n - 1, n) = 1$ , we deduce  $d = 1$ .

Arguing as above, we have

$$\frac{p^n - 1}{p - 1} = p^{n-1} + p^{n-2} + \dots + p + 1 \equiv \underbrace{1 + 1 + \dots + 1 + 1}_n \pmod{p - 1}.$$

Hence  $\text{gcd}(p - 1, (p^n - 1)/(p - 1)) = \text{gcd}(p - 1, n) = 1$ , since  $\text{gcd}(p^n - 1, n) = 1$  by (1).  $\square$

By Lemma 3.1, we have

$$C = D \times E,$$

where  $|D| = p^2 + p + 1$ ,  $E$  is a Hall  $\pi(p^2 + p + 1)'$ -subgroup of  $C$ , and  $|E| = (p^n - 1)/(p^3 - 1)$ . Moreover,  $F \setminus \{0\} = (F_p \setminus \{0\}) \times D \times E$ .

Following [7], we let  $P_i = 1 + J^i$ . In particular,  $P_1 = P$ ,  $P_4 = 1$  and  $P_i/P_{i+1}$  is isomorphic to the additive group of the field  $F$ , for each  $i \in \{1, 2, 3\}$ . Clearly,  $P_i \trianglelefteq G$ , for each  $i$ .

**Lemma 3.2.**

- (a)  $T/P_3$  is a Frobenius group with Frobenius kernel  $P/P_3$  and with Frobenius complement  $CP_3/P_3 \cong C$ .
- (b)  $E$  acts fixed-point-freely on  $P$  and, for every  $E$ -invariant subgroup  $N$  of  $P$  and a non-principal character  $\theta \in \text{Irr}(N)$ , we have  $I_E(\theta) = 1$ . Moreover,  $D \leq C_G(P_3)$ .

**Proof.** (a) Let  $1 + a_1x + a_2x^2 \in P$  and  $c \in C_C((1 + a_1x + a_2x^2)P_3)$ . By (2), we have

$$1 + a_1cx + a_2c^{p+1}x^2 = (1 + a_1x + a_2x^2)^c \equiv 1 + a_1x + a_2x^2 \pmod{P_3}$$

if and only if  $a_1c = a_1$  and  $a_2c^{p+1} = a_2$ . Assume  $c \neq 1$ . We immediately deduce  $a_1 = 0$ . Moreover, since  $p \equiv -1 \pmod{p + 1}$  and since  $n$  is odd, we have

$$\begin{aligned} \frac{p^n - 1}{p - 1} &= p^{n-1} + p^{n-2} + \dots + p + 1 \equiv (-1)^{n-1} + (-1)^{n-2} + \dots + (-1)^1 + (-1)^0 \pmod{p + 1} \\ &\equiv 1 \pmod{p + 1}. \end{aligned}$$

Therefore,  $\text{gcd}((p^n - 1)/(p - 1), p + 1) = 1$ . In particular,  $c^{p+1} \neq 1$  and hence  $a_2 = 0$ . Therefore,  $1 + a_1x + a_2x^2 = 1$  and part (a) is proved.

(b) Let  $c \in C$ . As  $C = D \times E$ , we may write  $c = de$  for some  $d \in D$  and  $e \in E$ . Let  $t = 1 + bx^3 \in P_3$ . Then

$$t^c = 1 + bc^{p^2+p+1}x^3 = 1 + be^{p^2+p+1}x^3.$$

Then  $D \leq C_G(P_3)$  and, as  $\text{gcd}(p^2 + p + 1, |E|) = 1$ ,  $E$  acts fixed-point-freely on  $P_3$ . Since  $E$  acts fixed-point-freely on  $P/P_3$  by part (a),  $E$  acts fixed-point-freely on  $P$ . Thus, if  $N$  is an  $E$ -invariant subgroup of  $P$ , then  $E$  acts fixed-point-freely on  $N$ , and  $\text{Irr}(N)$  and  $\text{Cl}(N)$  are isomorphic  $E$ -sets by Lemma 2.1. Hence, the rest of part (b) follows by Glauberman’s lemma ([6, Lemma 13.8]).  $\square$

The map  $(x, y) \mapsto [x, y]$  defines a function

$$P/P_2 \times P_2/P_3 \rightarrow P_3.$$

Since  $P/P_2$ ,  $P_2/P_3$  and  $P_3$  are naturally isomorphic to the additive group of the field  $F$ , this commutator mapping defines a function

$$\langle \cdot, \cdot \rangle : F \times F \rightarrow F. \tag{4}$$

This function is computed explicitly in [7]. Indeed, let  $s = 1 + ax + i \in P$  with  $i \in J^2$  and let  $t = 1 + bx^2 + j \in P_2$  with  $j \in J^3$ . From [7, Corollary 4.2], we have

$$[s, t] = 1 + (ab^p - a^{p^2}b)x^3. \tag{5}$$

This shows that the function in (4) is defined by  $\langle a, b \rangle = ab^p - a^{p^2}b$ .

From its definition, we deduce that, for every  $a \in F$ ,  $b \mapsto \langle a, b \rangle$  is a linear  $F_p$ -map, where (as above)  $F_p$  is the finite subfield of  $F$  having cardinality  $p$ . We let

$$\langle a, F \rangle = \{ab^p - a^{p^2}b \mid b \in F\}$$

denote the image of this mapping.

**Lemma 3.3.** *Let  $a \in F$ . If  $a = 0$ , then  $b \mapsto \langle a, b \rangle$  is the zero function. If  $a \neq 0$ , then the kernel of the function  $b \mapsto \langle a, b \rangle$  is  $\{ca^{p+1} \mid c \in F_p\}$  and the image  $\langle a, F \rangle$  is an  $F_p$ -subspace of  $F$  of codimension 1.*

**Proof.** The result is clear when  $a = 0$ . Assume then  $a \neq 0$ . Let  $b \in F$  with  $\langle a, b \rangle = 0$ . Thus  $ab^p = a^{p^2}b$  implies  $(b/a^{p+1})^p = b/a^{p+1}$ , that is,  $b \in \{ca^{p+1} \mid c \in F_p\}$ .  $\square$

We have

$$\langle 1, F \rangle = \{b^p - b \mid b \in F\}. \tag{6}$$

We note that, by the additive form of Hilbert’s Theorem 90,  $\langle 1, F \rangle$  is the kernel of the trace map  $\text{Tr} : F \rightarrow F_p$ , so  $\langle 1, F \rangle$  is an  $H$ -invariant hyperplane of  $F$  (seen as an  $F_p$ -vector space).

Let  $\Pi_0$  be the  $E$ -orbit, with respect to the natural action of  $E$  on the hyperplanes of  $F$ , containing  $\langle 1, F \rangle$ . We denote by  $F_{p^3}$  the subfield of  $F$  of cardinality  $p^3$ .

**Lemma 3.4.** *For  $a \in F$ , we have  $\langle a, F \rangle = \langle 1, F \rangle$  if and only if  $0 \neq a \in F_{p^3}$ , and*

$$\Pi_0 = \{\langle a, F \rangle \mid a \in F \setminus \{0\}\}.$$

**Proof.** Let  $a \in F \setminus \{0\}$ . As  $F \setminus \{0\} = (F_p \setminus \{0\}) \times D \times E$ , we may write  $a = a_f a_d a_e$  for some  $a_f \in F_p \setminus \{0\}$ ,  $a_d \in D$  and  $a_e \in E$ . Next, let  $b \in F \setminus \{0\}$  and let  $b_0 = a_e^{-(p+1)}b$ . We have

$$\begin{aligned} \langle a, b \rangle &= ab^p - a^{p^2}b = a_f a_d a_e b_0^p a_e^{p^2+p} - a_f^{p^2} a_d^{p^2} a_e^{p^2} b_0 a_e^{p+1} \\ &= a_f a_d b_0^p a_e^{p^2+p+1} - a_f a_d^{p^2} b_0 a_e^{p^2+p+1} \end{aligned}$$

$$\begin{aligned}
 &= a_e^{p^2+p+1} \left( a_f a_d b_0^p - a_f a_d^{p^2} b_0 \right) \\
 &= a_e^{p^2+p+1} \underbrace{\left( (-a_f a_d^{p^2} b_0) - (-a_f a_d^{p^2} b_0)^p \right)}_{\in \langle 1, F \rangle} \in a_e^{p^2+p+1} \langle 1, F \rangle.
 \end{aligned}$$

Hence, recalling Lemma 3.3

$$\langle a, F \rangle = a_e^{p^2+p+1} \langle 1, F \rangle$$

and, as  $|E|$  is coprime to  $p^2 + p + 1$  by Lemma 3.1, we conclude that  $\langle a, F \rangle = \langle 1, F \rangle$  if and only if  $a_e = 1$ , which is equivalent to  $a \in (F_p \setminus \{0\}) \times D = F_{p^3} \setminus \{0\}$ .

Finally, by observing that, as  $a_e$  runs through the elements of  $E$ , so does  $a_e^{p^2+p+1}$ , we see that the hyperplanes of the form  $\langle a, F \rangle$  are in one-to-one correspondence with the elements of  $E$  and, in particular, that  $\Pi_0 = \{ \langle a, F \rangle \mid a \in F \setminus \{0\} \}$ .  $\square$

Let

$$H = R \times S,$$

where  $R$  is the Sylow 3-subgroup of  $H$ , so  $|R| = 3$ , and  $S$  is the 3-complement of  $H$ .

As  $P_3 = \{1 + ax^3 \mid a \in F\}$ , the mapping  $\omega : P_3 \rightarrow F$  defined by  $1 + ax^3 \mapsto a$  is a group isomorphism between  $P_3$  and the additive group of  $F$ . We also remark that, via  $\omega$ ,  $P_3$  and  $F$  are isomorphic  $H$ -sets.

**Lemma 3.5.** *Let  $X = \widehat{P_3} \setminus \{1_{P_3}\}$ . Then  $G$  acts on  $X$  and we denote by  $X_0$  the union of the  $H$ -invariant  $C$ -orbits in  $X$ . Then*

- (a) *For every  $\varphi \in X \setminus X_0$ , there exists  $g \in G$  such that  $I_G(\varphi^g) = PDS$ .*
- (b) *If  $\varphi_0 \in X$  is such that  $\omega(\ker(\varphi_0)) = \langle 1, F \rangle$ , then  $\{\varphi_0^i \mid i = 1, \dots, p - 1\}$  is a set of representatives for the  $G$ -orbits in  $X_0$ . Moreover,  $I_G(\varphi_0^i) = PDH$  for every  $i = 1, \dots, p - 1$ .*
- (c) *For every  $\varphi \in X$ ,  $\varphi \in X_0$  if and only if  $\omega(\ker(\varphi)) \in \Pi_0$ .*

**Proof.** Since  $P_3 = Z(P)$  and  $D \leq C_G(P_3)$  by Lemma 3.2 part (b),  $PD \leq C_G(P_3)$ . Therefore, as  $G = PDEH$ , the  $G$ -orbits and the  $EH$ -orbits in  $X$  coincide. Let  $X' = P_3 \setminus \{1\}$ . With reference to Lemma 2.1, it is established that  $X$  and  $X'$  are isomorphic  $EH$ -sets. Consequently, we use the action of  $EH$  on  $X'$  to draw conclusions regarding the action of  $EH$  on  $X$ .

Since the map  $E \rightarrow E$  such that  $e \mapsto e^{p^2+p+1}$  is a bijection, the orbits of  $E$  on  $X'$  are the subsets of the form  $\{1 + eax^3 \mid e \in E\}$ , for  $0 \neq a \in F_{p^3}$ . Thus, they correspond, identifying  $X'$  and  $F^\times = F \setminus \{0\}$  via  $\omega$ , to the non-trivial cosets of  $E$  in  $F^\times$ , i.e. to the non-trivial elements of the group  $F^\times/E \simeq F_{p^3}^\times$ . Let  $\sigma \in H$  be the cube of the Frobenius

automorphism of  $F$ ; thus  $S = \langle \sigma \rangle$ . Since  $a^\sigma = a^{p^3} = a^{p^3-1}a$ , and  $a^{p^3-1} \in E$  (as  $o(a^{p^3-1})$  divides  $(p^n - 1)/(p^3 - 1) = |E|$ ), it follows that  $S$  fixes all  $E$ -orbits on  $X'$ . On the other hand,  $R$  acts on the set of the  $E$ -orbits on  $X'$  as it acts on  $F_{p^3}^\times$ , so  $R$  fixes exactly  $p - 1$   $E$ -orbits on  $X'$ . Therefore, by the isomorphism of the  $EH$ -sets  $X$  and  $X'$ ,  $S$  acts trivially on the set of the  $E$ -orbits in  $X$  and  $R$  fixes exactly  $p - 1$  of them (and permutes the others in orbits of size 3). Hence,  $X_0$  contains exactly  $p - 1$   $G$ -orbits. Moreover, by Glauberman’s lemma every  $E$ -orbit in  $X \setminus X_0$  contains an  $S$ -invariant character. So, recalling that, by Lemma 3.2 part (b),  $I_E(\varphi) = 1$  for every  $\varphi \in X$ , part (a) follows. Hence, this implies that the  $C$ -orbits in  $X$  are in fact  $G$ -orbits.

We observe that for  $\varphi \in X$ , the stabilizer of the group  $\langle \varphi \rangle$  under the action of  $E$  is trivial, because  $C_E(\langle \varphi \rangle) = 1$  and  $|\text{Aut}(\langle \varphi \rangle)| = p - 1$  is coprime to  $|E|$ . It follows that  $\langle \varphi \rangle$  intersects  $p - 1$  distinct  $E$ -orbits in  $X$ .

Now, let  $\varphi_0 \in X$  be such that  $\omega(\ker(\varphi_0)) = \langle 1, F \rangle$ . Then  $\varphi_0$  is  $H$ -invariant. In fact, writing  $H = \langle h \rangle$ , where  $h$  is the Frobenius automorphism of  $F$ , for any  $t = 1 + bx^3 \in P_3$ ,  $\varphi_0^{h^{-1}}(t) = \varphi_0(t^h) = \varphi_0(t)$  as  $t^h t^{-1} = (1 + b^p x^3)(1 - bx^3) = 1 + (b^p - b)x^3 \in \ker(\varphi_0)$ . Thus, by the previous paragraph, we conclude that  $\{\varphi_0^i \mid i = 1, \dots, p - 1\}$  is a set of representatives for the  $G$ -orbits in  $X_0$ . Since the characters  $\varphi_0^i$  generate the same subgroup of  $\widehat{P_3}$  for every  $i = 1, \dots, p - 1$ , recalling again that  $I_E(\varphi_0) = 1$ , we have that  $I_G(\varphi_0^i) = PDH$  for every  $i = 1, \dots, p - 1$ , and part (b) is proved.

Finally, recalling the definition of  $\Pi_0$  and  $X_0$ , we deduce that  $\varphi \in X_0$  if and only if  $\omega(\ker(\varphi)) \in \Pi_0$ , so we have part (c).  $\square$

Let  $B = \{1 + bx^2 \mid b \in F\} \leq P_2$ . Observe that  $B$  is normalized by  $CH$  and

$$P_2 = B \times P_3.$$

Therefore, the characters in  $\text{Irr}(P_2|P_3)$  are of the form  $\nu \times \varphi$ , where  $\nu \in \text{Irr}(B)$  and  $\varphi \in X$ . Recall that, from Lemma 3.5,  $X = \widehat{P_3} \setminus \{1_{P_3}\}$ .

Let

$$Q = \{1 + a_1x + a_2x^2 + a_3x^3 \in P \mid a_1, a_2, a_3 \in F_{p^3}\} = C_P(S).$$

Given  $\varphi \in X$  and  $a \in F$ , we define  $\varphi_a \in \text{Irr}(B)$  by setting

$$\varphi_a(1 + bx^2) = \varphi(1 - \langle a, b \rangle x^3), \tag{7}$$

for every  $b \in F$ .

**Lemma 3.6.** *Let  $\mu \times \varphi \in \text{Irr}(P_2)$ , with  $\mu \in \text{Irr}(B)$  and  $\varphi \in X$ . Then*

(a) *for every  $s = 1 + ax + i \in P$  with  $i \in J^2$ , we have*

$$(\mu \times \varphi)^{s^{-1}} = \mu\varphi_a \times \varphi.$$

(b) If  $\varphi_0$  and  $X_0$  are as in Lemma 3.5, then  $I_P(\mu \times \varphi_0) = P_2Q$ . Moreover, for  $\varphi \in X \setminus X_0$ , we have  $I_P(\mu \times \varphi) = P_2$ .

**Proof.** Let  $t = 1 + bx^2 + cx^3 \in P_2$ . Then, using (5), we obtain

$$\begin{aligned} t^s &= t[t, s] = t[s, t]^{-1} = (1 + bx^2 + cx^3)(1 - \langle a, b \rangle x^3) \\ &= 1 + bx^2 + (c - \langle a, b \rangle)x^3. \end{aligned}$$

Therefore, we have

$$\begin{aligned} (\mu \times \varphi)^{s^{-1}}(t) &= (\mu \times \varphi)(t^s) = (\mu \times \varphi)(1 + bx^2 + (c - \langle a, b \rangle)x^3) \\ &= (\mu \times \varphi)((1 + bx^2)(1 + (c - \langle a, b \rangle)x^3)) = \mu(1 + bx^2)\varphi(1 + (c - \langle a, b \rangle)x^3). \end{aligned} \tag{8}$$

Similarly,

$$\begin{aligned} (\mu\varphi_a \times \varphi)(t) &= \mu\varphi_a(1 + bx^2)\varphi(1 + cx^3) = \mu(1 + bx^2)\varphi(1 - \langle a, b \rangle x^3)\varphi(1 + cx^3) \\ &= \mu(1 + bx^2)\varphi(1 + (c - \langle a, b \rangle)x^3). \end{aligned} \tag{9}$$

Now part (a) follows immediately from (8) and (9).

Moreover, writing  $s = (1 + ax + i)w$  with  $w \in P_2$ , by part (a),  $s \in I_P(\mu \times \varphi)$  if and only if  $\langle a, F \rangle = \omega(\ker(\varphi))$ , so part (b) follows from Lemma 3.4 and part (c) of Lemma 3.5.  $\square$

Since  $\gcd(|S|, |B|) = 1$  and  $Q \cap B = C_Q(S)$ , writing  $B_1 = [B, S]$  we have  $B = (Q \cap B) \times B_1$ . Hence,

$$\widehat{B} = \widehat{Q \cap B} \times \widehat{B_1}. \tag{10}$$

In this way, we see  $\widehat{Q \cap B}$  and  $\widehat{B_1}$  as subgroups of  $\widehat{B}$ .

**Lemma 3.7.** Let  $\varphi_0 \in \widehat{P_3}$  be as in Lemma 3.5. Then PDH acts on  $Y = \text{Irr}(P_2|\varphi_0)$ . Let  $\psi_0 = 1_B \times \varphi_0$  and let  $Y_0$  be the PDH-orbit of  $\psi_0$  in  $Y$ . Then

- (a)  $\{(\varphi_0)_a \mid a \in F\} = \widehat{B_1}$ .
- (b) For every  $\psi \in Y$ , there exists an element  $g \in PD$  such that  $\psi^g$  is  $H$ -invariant.
- (c)  $Y_0$  is a  $P$ -orbit and it is the unique  $D$ -invariant  $P$ -orbit in  $Y$ .
- (d)  $D$  acts semi-regularly on the set of the  $P$ -orbits in  $Y \setminus Y_0$ .
- (e)  $Y \setminus Y_0$  consists of exactly  $p - 1$  PDH-orbits.

**Proof.** Since  $\varphi_0$  is PDH-invariant by Lemma 3.5 part (b), PDH acts on  $Y$ . As  $P_2 = B \times P_3$ , we have  $Y = \{\mu \times \varphi_0 \mid \mu \in \widehat{B}\}$  and, as  $B$  is  $D$ -invariant, the action of  $D$  on  $Y$  is isomorphic to the action of  $D$  on  $\widehat{B}$  and hence, by Lemma 2.1, to the action of  $D$  on  $B$ . Since  $D$  acts fixed-point-freely on  $B$ , we deduce that

$$\psi_0 = 1_B \times \varphi_0$$

is the unique  $D$ -invariant character in  $Y$ . As  $H$  fixes  $D$  and  $Y$ , this uniqueness implies that  $\psi_0$  is  $H$ -invariant as well. So,  $\psi_0$  is  $DH$ -invariant and hence  $Y_0$  is a  $P$ -orbit. Moreover, if  $Y_1$  is a  $D$ -invariant  $P$ -orbit in  $Y$ , then  $Y_1$  contains a  $D$ -invariant character by Glauberman’s lemma, and hence  $Y_1 = Y_0$ , proving (c).

In order to prove (a), we first show that  $Q \cap B \leq \text{Ker}((\varphi_0)_a)$  for every  $a \in F$ . For  $1 \neq 1 + bx^2 \in Q \cap B$ , where  $b \in F_{p^3}^\times$ , we have  $b^{p^3-1} = 1$ . Thus

$$\langle a, b \rangle = ab^p - a^{p^2}b = (ab^p - (ab^p)^p) + (a^pb^{p^2} - (a^pb^{p^2})^p) \in \langle 1, F \rangle = \text{Ker}(\varphi_0).$$

This and (7) show that  $1 + bx^2 \in \text{Ker}((\varphi_0)_a)$ . Therefore,  $\{(\varphi_0)_a \mid a \in F\} \subseteq \widehat{B}_1$ .

On the other hand, the mapping  $F \rightarrow \widehat{B}$  such that  $a \mapsto (\varphi_0)_a$  is a homomorphism of  $F_p$ -vector spaces and its kernel is  $F_{p^3}$  by Lemma 3.4. As  $|\widehat{B}_1| = p^{n-3}$ , part (a) follows.

Now, part (a) of Lemma 3.6, (10) and part (a) of the statement yield that

$$\{\delta \times \varphi_0 \mid \delta \in \widehat{Q \cap B}\} \text{ is a set of representatives for the } P\text{-orbits in } Y. \tag{11}$$

Since  $\varphi_0$  is  $D$ -invariant, by (11) the action of  $D$  on the set of the  $P$ -orbits in  $Y$  is isomorphic to the action of  $D$  on  $\widehat{Q \cap B}$ . Since  $D$  acts transitively on the 1-dimensional subspaces of  $Q \cap B$  (identified, as usual, with  $F_{p^3}$ ), and  $C_{Q \cap B}(H)$  is a 1-dimensional subspace, it follows that every  $D$ -orbit in  $Q \cap B$  contains an  $H$ -invariant element and, by the isomorphism of the actions of  $D$  on  $Q \cap B$  and on  $\widehat{Q \cap B}$ , the same is true for  $\widehat{Q \cap B}$ . Therefore, we conclude that every  $PD$ -orbit in  $Y$  contains an  $H$ -invariant character, proving part (b).

By the same argument, since  $D$  acts fixed-point-freely on  $\widehat{Q \cap B}$ , we deduce that  $D$  acts semi-regularly on the  $P$ -orbits in  $Y$  that do not contain  $\psi_0$ , so we have part (d).

Finally, by Lemma 3.6 part (b),  $I_P(\psi) = P_2Q$  for every  $\psi \in Y$ . By part (b) it follows that the  $PDH$ -orbits in  $Y$  are in fact  $PD$ -orbits and, as  $|Y_0| = p^{n-3}$ , by part (d) of this statement there are  $(|Y| - p^{n-3}) / (p^{n-3}|D|) = p - 1$   $PDH$ -orbits in  $Y \setminus Y_0$ , completing the proof.  $\square$

#### 4. Number theoretic considerations

We start with a result concerning the existence of integers with suitable properties.

**Lemma 4.1.** *For every pair of positive integers  $c$  and  $\ell$ , there exists a prime number  $p$  and a positive integer  $n$  such that*

- (a)  $p^2 + p + 1$  is divisible by at least  $c$  distinct prime numbers.
- (b)  $\text{gcd}(n, p(p^n - 1)) = 1$ .
- (c)  $n$  is odd and the largest power of 3 dividing  $n$  is 3.

(d)  $n$  is divisible by exactly  $\ell$  distinct primes.

**Proof.** Let  $3 = r_1 < r_2 < \dots < r_\ell$  be prime numbers. Moreover, for each  $j \in \{1, \dots, \ell\}$ , let  $b_j \in \mathbb{N}$  be a non-square modulo  $r_j$ , that is,  $b_j + r_j\mathbb{Z}$  is not a square in the ring  $\mathbb{Z}/r_j\mathbb{Z}$ . Furthermore, let  $q_1 < \dots < q_c$  be prime numbers different from the  $r_j$ 's, and each of them congruent to 1 modulo 3. Finally, for each  $i \in \{1, \dots, c\}$ , let  $a_i \in \mathbb{N}$  have order 3 modulo  $q_i$ .

Let  $n = \prod_{j=1}^{\ell} r_j$  and observe that  $n$  is an odd square-free number,  $n$  is divisible by exactly  $\ell$  distinct primes and the largest power of 3 dividing  $n$  is 3.

From the Chinese Remainder Theorem and Dirichlet's theorem on prime numbers in arithmetic progressions, there exists a prime  $p$  such that

$$\begin{aligned} p &\equiv a_i \pmod{q_i}, & \forall i \in \{1, \dots, c\}, \\ p &\equiv b_j \pmod{r_j}, & \forall j \in \{1, \dots, \ell\}. \end{aligned}$$

Then  $p^2 + p + 1 \equiv a_i^2 + a_i + 1 \equiv 0 \pmod{q_i}$ , as  $a_i$  has order 3 modulo  $q_i$ . Therefore,  $p^2 + p + 1$  is divisible by at least  $c$  distinct primes.

Let  $j \in \{1, \dots, \ell\}$ . As  $p \equiv b_j \pmod{r_j}$ , we have  $p \neq r_j$ . Moreover, since  $n$  is odd and since  $b_j$  is a non-square modulo  $r_j$ , we deduce that  $p^n - 1 \not\equiv 0 \pmod{r_j}$ , that is,  $r_j$  does not divide  $p^n - 1$ . Therefore  $r_j$  does not divide  $p(p^n - 1)$  and hence  $\gcd(n, p(p^n - 1)) = 1$ .  $\square$

Lemma 4.1 suffices for our application, namely, the proof of Theorem A. However, before finishing this section, we wish to include a few remarks on the number-theoretic aspects pertaining to the condition in (1).

Let  $n$  be a positive integer. Also, let

$$x^n - 1 = \prod_{d|n} \lambda_d(x), \quad \lambda_d(x) = \prod_{\substack{z \in \mathbb{C} \\ \text{primitive } d^{\text{th}} \\ \text{root of unity}}} x - z$$

be the factorization of  $x^n - 1$  into its irreducible factors in  $\mathbb{Q}[x]$  (i.e. cyclotomic polynomials).

Now, let  $q$  be an integer,  $q \geq 2$ , and let  $d$  be a divisor of  $n$  with  $d \neq 1$ . Observe that, if  $z \in \mathbb{C}$  is a primitive  $d^{\text{th}}$  root of unity, then the Euclidean distance between  $z$  and  $q$  is greater than  $q - 1$ , that is,  $|z - q| > q - 1$ . We deduce

$$|\lambda_d(q)| = \prod_{\substack{z \in \mathbb{C} \\ \text{primitive } d^{\text{th}} \\ \text{root of unity}}} |z - q| > \prod_{\substack{z \in \mathbb{C} \\ \text{primitive } d^{\text{th}} \\ \text{root of unity}}} (q - 1) = (q - 1)^{\varphi(d)} \geq 1.$$

This shows that  $\lambda_d(q) \neq \pm 1$ .

For a positive integer  $k$ , we denote by  $d(k)$  the number of positive divisors of  $k$ .

**Lemma 4.2.** *Let  $n$  and  $q$  be positive integers with  $q \geq 2$  and  $\gcd(n, (q^n - 1)/(q - 1)) = 1$ . Then, for every positive integer  $m$  that divides  $n$ ,*

$$\left| \pi \left( \frac{q^n - 1}{q^m - 1} \right) \right| \geq d(n) - d(m).$$

**Proof.** For each divisor  $d$  of  $n$  different from 1, let  $r_d$  be a prime divisor of  $\lambda_d(q)$ , where  $\lambda_d$  is the  $d$ -th cyclotomic polynomial. Observe that the existence of  $r_d$  follows from the fact that  $\lambda_d(q) > 1$ .

We claim that  $q$  has order exactly  $d$  modulo  $r_d$ , that is, the order of the residue class  $q + r_d\mathbb{Z}$  in  $\mathbb{Z}/r_d\mathbb{Z}$  is  $d$ . From this, it follows that, when  $d$  varies among the divisors  $\geq 2$  of  $n$ , all primes  $r_d$  are distinct and hence the result follows. Let  $o$  be the order of  $q$  modulo  $r_d$ . From the definition of order and from the factorization of  $x^o - 1$ , it follows that  $r_d$  divides  $\lambda_o(q)$ . As  $r_d$  divides  $\lambda_d(q)$  and  $\lambda_d(q)$  divides  $q^d - 1$ , we deduce that  $q^d \equiv 1 \pmod{r_d}$  and hence  $o$  divides  $d$ . Recall

$$x^d - 1 = \prod_{a|d} \lambda_a(x).$$

Now, since  $\gcd(n, (q^n - 1)/(q - 1)) = 1$ ,  $d$  is relatively prime to  $r_d$  and hence the derivative  $(x^d - 1)' = dx^{d-1}$  in the ring  $\mathbb{Z}/r_d\mathbb{Z}[x]$  is relatively prime to  $x^d - 1$ . As  $x^d - 1 \in \mathbb{Z}/r_d\mathbb{Z}[x]$  has no multiple roots, it is not possible that  $q$  is a root of  $\lambda_d(x)$  and  $\lambda_o(x)$  in  $\mathbb{Z}/r_d\mathbb{Z}[x]$ . Since  $r_d$  divides both  $\lambda_o(q)$  and  $\lambda_d(q)$ , this implies  $o = d$ .  $\square$

In view of the proof of Lemma 4.2, the condition  $\gcd(p^n - 1, n) = 1$  in (1) implies that, when  $p \geq 3$ , the number of distinct prime divisors of  $p^n - 1$  is at least  $2^{|\pi(n)|}$ , because for each divisor  $d$  of  $n$  we may select from  $\lambda_d(p)$  at least one prime divisor. However, when  $p = 2$ , since  $\lambda_1(p) = p - 1 = 1$ , we may only infer that the number of distinct prime divisors of  $2^n - 1$  is at least  $2^{|\pi(n)|} - 1$ . Except when  $|\pi(n)| \leq 2$ , we have no examples where  $2^n - 1$  has exactly  $2^{|\pi(n)|} - 1$  distinct prime divisors. We dare to state the following.

**Conjecture 4.3.** *Let  $n$  be divisible by  $\ell$  distinct primes and assume  $\gcd(2^n - 1, n) = 1$ . If  $\ell \geq 3$ , then  $2^n - 1$  is divisible by at least  $2^\ell$  distinct primes.*

The book of Brillhart et al. [1] investigates the factorizations of  $b^n - 1$  when  $b$  is small and  $n$  is a large positive integer. Our conjecture is compatible with the results and the tables presented in that book.

### 5. Main results

We start by proving Theorem A, which we state again.

**Theorem A.** *For every choice of positive integers  $a, b$ , there exists a solvable group  $G$  such that  $\Delta = \Delta(G)$  has diameter three and such that  $|\alpha_\Delta| = a$  and  $|\delta_\Delta| \geq b$ .*

**Proof.** According to Lemma 4.1, we choose a prime number  $p$  and a positive odd integer  $n$  such that  $n$  is divisible by exactly  $a$  distinct primes,  $p^2 + p + 1$  is divisible by at least  $b$  distinct primes,  $\gcd(n, p(p^n - 1)) = 1$ , and the largest power of 3 dividing  $n$  is 3.

We will make consistent use of the notation introduced in Section 3. For the convenience of the reader, we recall here some relevant definitions.

- $F$  is a field of cardinality  $p^n$ ;
- $J$  is the Jacobson radical of the quotient of  $F\{X\}$  by the ideal generated by  $X^4$ , that is,  $J = \{a_1x + a_2x^2 + a_3x^3 \mid a_1, a_2, a_3 \in F\}$ , where  $x$  is the image of  $X$  in the quotient ring;
- $P = 1 + J$ , where  $|P| = p^{3n}$  and each element of  $P$  is of the form  $1 + a_1x + a_2x^2 + a_3x^3$ , for  $a_1, a_2, a_3 \in F$ ;
- $C$  is the subgroup of the multiplicative group of the field  $F$  of order  $(p^n - 1)/(p - 1)$ . Moreover,  $C$  acts as a group of automorphisms on  $P$  as defined in (2);
- $T = P \rtimes C$  is a group of order  $(p^n - 1)p^{3n}/(p - 1)$ ;
- $H = \text{Gal}(F/F_p)$ , where  $F_p$  is the prime subfield of  $F$ . The group  $H$  is cyclic of order  $n$  and acts as a group of automorphisms on  $T$  as defined in (3);
- $R$  is the Sylow 3-subgroup of  $H$  and  $S$  is the 3-complement of  $H$  so that  $H = R \times S$ ;
- $D$  is the subgroup of  $C$  having order  $p^2 + p + 1 = (p^3 - 1)/(p - 1)$ ;
- $E$  is a Hall  $\pi(p^2 + p + 1)'$ -subgroup of  $C$ . Indeed,  $|E| = (p^n - 1)/(p^3 - 1)$ . Moreover,  $F \setminus \{0\} = (F_p \setminus \{0\}) \times D \times E$ ;
- $B = \{1 + bx^2 \mid b \in F\} \leq P_2$ , where  $P_2 = 1 + J^2$  and  $P_2 = B \times P_3$ ;
- $Q = \{1 + a_1x + a_2x^2 + a_3x^3 \in P \mid a_1, a_2, a_3 \in F_{p^3}\} = C_P(S)$ ;

Let  $G = T \rtimes H = P \rtimes (C \rtimes H)$ . Therefore,  $G$  is a group of order  $n(p^n - 1)p^{3n}/(p - 1)$ . We will determine the degrees, along with their multiplicities, of the irreducible characters of  $G$ .

**(I)  $\text{Irr}(G/P)$**

The character degrees of  $G/P \simeq CH$  are determined by McVey in [12]. Indeed, it is shown in [12, Theorem 5] that  $\text{cd}(G/P) = \{d \mid d \text{ divides } n\}$ .

**(II)  $\text{Irr}(G/P_3|P/P_3)$**

The character theory of the group  $P/P_3$  is studied in [5] and [15]. Observe that  $P/P_3$  has nilpotency class 2 and that  $n$  is odd. These two facts, together with  $\gcd(n, p(p^n - 1)) = 1$ , imply that the conditions described in [5, page 340] or in [15, page 190] are satisfied.

We write  $\overline{G} = G/P_3$  and use the bar convention. From [15, Theorem 4.4], we see that  $\overline{P}$  has

- 1 principal character,
- $p^n - 1$  non-principal characters of degree 1,
- $p(p^n - 1)$  characters of degree  $p^{(n-1)/2}$ .

By Lemma 2.1,  $\text{Irr}(\overline{P})$  and  $\text{Cl}(\overline{P})$  are isomorphic  $\overline{C\overline{H}}$ -sets. By [5, Theorem 4.1],

$$\{(1 + a_1x + a_2x^2)^c \mid a_1, a_2 \in F_p, c \in \overline{C}\}$$

is a set of representatives for the conjugacy classes of  $\overline{P}$ . Hence,  $C_{\overline{P}}(\overline{H}) = \{1 + a_1x + a_2x^2 \mid a_1, a_2 \in F_p\}$  has non-trivial intersection with every  $\overline{C}$ -orbit in  $\text{Cl}(\overline{P})$ . Let  $\theta \in \text{Irr}(\overline{P})$  with  $\theta \neq 1_{\overline{P}}$ . By the above-mentioned isomorphism of  $\overline{C\overline{H}}$ -sets, it follows that there exists a  $c \in \overline{C}$  such that  $\theta^c$  is  $\overline{H}$ -invariant. Moreover,  $\overline{C}$  acts semi-regularly on  $\text{Irr}(\overline{P}) \setminus \{1_{\overline{P}}\}$ , hence  $I_{\overline{C}}(\theta^c) = \overline{P\overline{H}}$ . So, by Gallagher’s theorem and Clifford correspondence,  $\text{Irr}(\overline{G}|\theta^c)$  consists of  $n$  irreducible characters of degree  $\theta(1)|C|$ .

Moreover, the  $\overline{G}$ -orbits on  $\text{Irr}(\overline{P})$  coincide with the  $\overline{C}$ -orbits and, by the semi-regular action of  $\overline{C}$ , in  $\text{Irr}(\overline{P})$  there are  $p - 1$   $\overline{G}$ -orbits of linear characters and  $p(p - 1)$   $\overline{G}$ -orbits of characters of degree  $p^{(n-1)/2}$ . Therefore,  $\text{Irr}(G/P_3|P/P_3)$  consists of

- $n(p - 1)$  characters of degree  $(p^n - 1)/(p - 1)$ ,
- $np(p - 1)$  characters of degree  $p^{(n-1)/2}(p^n - 1)/(p - 1)$ .

So far, using (1), we have shown that the character degree graph of  $G/P_3$  has two connected components, which are complete graphs. One connected component consists of prime divisors of  $n$  and the other connected component consists of the prime divisors of  $p(p^n - 1)/(p - 1)$ .

**(III)**  $\text{Irr}(G|P_3)$

Consistently with the notation in Lemma 3.5, we let  $X = \widehat{P_3} \setminus \{1_{P_3}\}$  and let  $X_0$  be the union of the  $H$ -invariant  $C$ -orbits (that is, the  $G$ -orbits) in  $X$ . Recall that the  $H$ -invariant  $C$ -orbits in  $X$  are the  $G$ -orbits in  $X$ . Hence,

$$\text{Irr}(G|P_3) = \text{Irr}(G|X) = \text{Irr}(G|X \setminus X_0) \cup \text{Irr}(G|X_0).$$

**(III.A)**  $\text{Irr}(G|X \setminus X_0)$

Let  $\varphi \in X \setminus X_0$  (i.e.  $\varphi$  does not lie in an  $H$ -invariant  $C$ -orbit). By Lemma 2.2 and part (a) of Lemma 3.5, we can assume that  $I_G(\varphi) = PDS$ . By Lemma 3.6 part (b), for every  $\mu \in \text{Irr}(B)$ ,  $I_P(\mu \times \varphi) = P_2$ . So, the induced character  $\theta = (\mu \times \varphi)^P$  is irreducible and has degree  $p^n$ . Hence, by [6, Problem 6.3],  $\varphi$  is fully ramified with respect to  $P/P_3$  and  $\text{Irr}(P|\varphi) = \{\theta\}$ . It follows that  $I_G(\theta) = I_G(\varphi) = PDS$ . Therefore, since  $\theta$  extends to  $PDS$  by [6, Corollary 6.28] and  $DS$  is abelian, by Gallagher’s theorem,  $\text{Irr}(G|\varphi) = \text{Irr}(G|\theta)$  consists of  $|DS| = n(p^2 + p + 1)/3$  characters of degree  $p^n|ER| = 3 \cdot p^n \cdot (p^n - 1)/(p^3 - 1)$ .

By Lemma 3.5 parts (a) and (b),  $X \setminus X_0$  contains exactly  $(|X| - (p - 1)|E|)/|ER| = (p^3 - p)/3$   $G$ -orbits, so we conclude that  $\text{Irr}(G|X \setminus X_0)$  contains exactly  $\frac{n(p^3 - p)(p^2 + p + 1)}{9}$  characters, all having degree  $3 \cdot p^n \cdot (p^n - 1)/(p^3 - 1)$ .

**(III.B)**  $\text{Irr}(G|X_0)$

Let  $\varphi_0 \in X_0$  be an  $H$ -invariant character. By part (b) of Lemma 3.5,  $\{\varphi_0^i \mid i = 1, \dots, p - 1\}$  is a set of representatives for the  $G$ -orbits in  $X_0$ , so

$$\text{Irr}(G|X_0) = \bigcup_{i=1}^{p-1} \text{Irr}(G|\varphi_0^i). \tag{12}$$

Observe that this is a disjoint union by Lemma 2.2.

We also remark that  $\{\varphi_0^i \mid i = 1, \dots, p - 1\}$  is an orbit under the action of the Galois group  $\text{Gal}(\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q})$ , so for every  $2 \leq i \leq p - 1$  there is a degree-preserving bijection between  $\text{Irr}(G|\varphi_0^i)$  and  $\text{Irr}(G|\varphi_0)$ . Moreover, the sets  $\text{Irr}(G|\varphi_0^i)$  are pairwise disjoint, for  $i = 1, \dots, p - 1$ , since the characters  $\varphi_0^i$  lie in distinct  $G$ -orbits.

Let  $Y = \text{Irr}(P_2|\varphi_0)$  be the set consisting of the  $p^n$  extensions of  $\varphi_0$  to the abelian group  $P_2$ . Since  $PDH = I_G(\varphi_0)$ , we deduce that  $Y$  is a  $PDH$ -set. We observe that, if  $\psi_1 = \psi^g$  for  $\psi, \psi_1 \in Y$  and  $g \in G$ , then  $g \in I_G(\varphi_0) = PDH$ . Therefore,  $\psi, \psi_1 \in Y$  are  $G$ -conjugate if and only if they are  $PDH$ -conjugate. Hence, for every orbit  $Z$  of  $G$  on  $\text{Irr}(P_2)$ , either  $Z \cap Y = \emptyset$  or  $Z \cap Y$  is a  $PDH$ -orbit.

Let  $Y_0$  be the  $PDH$ -orbit of  $\psi_0 = 1_B \times \varphi_0$  in  $Y$  and let  $\mathcal{Y}$  be a set of representatives for the  $PDH$ -orbits in  $Y \setminus Y_0$ . Then  $|\mathcal{Y}| = p - 1$  by part (e) of Lemma 3.7. Moreover, by the previous paragraph and Lemma 2.2,  $\text{Irr}(G|\varphi_0)$  can be expressed as

$$\text{Irr}(G|\varphi_0) = \text{Irr}(G|Y) = \text{Irr}(G|Y \setminus Y_0) \cup \text{Irr}(G|Y_0) = \bigcup_{\psi \in \mathcal{Y}} \text{Irr}(G|\psi) \cup \text{Irr}(G|Y_0),$$

where all unions are disjoint.

**(III.B.1)**  $\text{Irr}(G|Y \setminus Y_0)$

Let  $\psi \in \mathcal{Y}$ . By Lemma 2.2 and part (b) of Lemma 3.7 we can assume that  $\psi$  is  $H$ -invariant.

Since  $\psi = \mu \times \varphi_0 \notin Y_0$ , by part (a) of Lemma 3.6  $\mu \neq (\varphi_0)_a$  for every  $a \in F$  and hence by part (a) of Lemma 3.7  $Q \cap B$  is not contained in  $\ker(\mu)$ .

Let  $I = I_P(\psi)$ ; thus  $I = P_2Q$  by Lemma 3.6. We claim that  $\psi$  does not extend to  $I$ . In fact, if the linear character  $\psi$  extends to  $I$ , then  $I' \cap B \leq \ker(\mu \times \varphi_0) \cap B = \ker(\mu)$ .<sup>1</sup> As  $Q' = Q \cap P_2$  by [7, Corollary 4.4], it follows that  $Q \cap B = Q' \cap B \leq I' \cap B \leq \ker(\mu)$ , a contradiction.

By Lemma 2.3, there exists a subgroup  $U$ , with  $P_2 \leq U \leq I$ , such that all characters  $\tau \in \text{Irr}(U|\psi)$  are extensions of  $\psi$  and are fully ramified with respect to  $I/U$ . Since  $\psi$  does not extend to  $I$ , then  $U < I$  and hence  $|I : U| = p^2$ . As  $\psi$  is  $H$ -invariant and  $\gcd(|H|, |U|) = 1$ , by [6, Corollary 13.30] at least one of the characters in  $\text{Irr}(U|\psi)$  is  $H$ -invariant. But, since  $\gcd(p - 1, |H|) = 1$ ,  $H$  acts trivially on  $U/P_2$ , and hence on its dual group. Therefore, by Gallagher’s theorem all characters in  $\text{Irr}(U|\psi)$  are  $H$ -invariant and,

<sup>1</sup> We denote by  $U'$  the derived subgroup of a finite group  $U$ .

since they are fully ramified with respect to  $I/U$ , the same is true for all the characters in  $\text{Irr}(I|\psi)$ . Hence,  $H \leq I_G(\xi^P)$  for every  $\xi \in \text{Irr}(I|\psi)$ .

We claim that  $I_{CH}(\xi^P) = H$  for all  $\xi \in \text{Irr}(I|\psi)$ . In fact,  $I_E(\xi^P) = 1$  by part (b) of Lemma 3.2, and if  $y \in I_D(\xi^P)$ , then by Clifford’s theorem  $y$  fixes the  $P$ -orbit of  $\psi$ , so  $y = 1$  by part (d) of Lemma 3.7. Thus,  $I_C(\xi^P) = 1$  and the claim follows.

Recall that  $|\text{Irr}(I|\psi)| = |\text{Irr}(U|\psi)| = p$  and hence  $\text{Irr}(I|\psi) = \{\xi_1, \dots, \xi_p\}$ . So, by Clifford’s correspondence,  $\text{Irr}(P|\psi) = \{\xi_1^P, \dots, \xi_p^P\}$ . As for every  $i \in \{1, \dots, p\}$ ,  $\xi_i^P$  extends to  $I_G(\xi_i^P) = PH$ , by Gallagher’s theorem we get that  $\text{Irr}(G|\xi_i^P)$  contains  $n$  characters, all of degree  $\xi_i^P(1)|C| = p^{n-2}(p^n - 1)/(p - 1)$ .

If  $\text{Irr}(G|\xi_i^P) \cap \text{Irr}(G|\xi_j^P) \neq \emptyset$ , then  $\xi_i^P$  and  $\xi_j^P$  are  $G$ -conjugate characters. As  $\varphi_0$  is the only irreducible constituent of the restriction of both  $\xi_i^P$  and  $\xi_j^P$  to  $P_3$ , then  $\xi_i^P$  and  $\xi_j^P$  are in the same orbit under the action of  $I_G(\varphi_0) = PDH$ . But both characters are  $PH$ -invariant, so there exists an element  $y \in D$  such that  $(\xi_i^P)^y = \xi_j^P$ . Since  $(\xi_i^P)^y$  lies over the  $P$ -orbit of  $\psi^y$  in  $Y$ , while  $\xi_j^P$  lies over the  $P$ -orbit of  $\psi$  in  $Y$ , by part (d) of Lemma 3.7 we conclude that  $y = 1$ , and hence  $i = j$ . Therefore, for every  $\psi \in \mathcal{Y}$ ,  $\text{Irr}(G|\psi) = \bigcup_{i=1}^p \text{Irr}(G|\xi_i^P)$  contains  $n \cdot p$  irreducible characters.

As  $|\mathcal{Y}| = p - 1$ ,

$$\text{Irr}(G|Y \setminus Y_0) = \bigcup_{\psi \in \mathcal{Y}} \text{Irr}(G|\psi)$$

consists of  $n \cdot p(p - 1)$  characters of degree  $p^{n-2}(p^n - 1)/(p - 1)$ .

**(III.B.2)  $\text{Irr}(G|Y_0)$**

Recall  $\psi_0 = 1_B \times \varphi_0$ . Let  $I = I_P(\psi_0) = P_2Q$  (by Lemma 3.6 part (b)) and let  $L = I/P_2 \simeq Q/(Q \cap P_2)$ ; as usual, we identify  $L$  and  $F_{p^3}$  by the isomorphism  $\omega_1$  defined by, for  $a \in F_{p^3}$ ,  $(1 + ax) + P_2 \mapsto a$ . Under this identification,  $D$  acts transitively, and hence regularly, on the 1-dimensional subspaces of the 3-dimensional  $F_p$ -space  $L$ . Hence,  $L$  is an irreducible  $D$ -module. Then by Lemma 2.3 and by the fact that  $|L|$  is not a square (so  $\psi_0$  cannot be fully ramified with respect to  $L$ ), it follows that  $\psi_0$  extends to  $I$ . By [6, Theorem 13.28], there is a  $D$ -invariant extension  $\xi_0$  of  $\psi_0$  to  $I$  and, by Gallagher’s theorem  $\text{Irr}(I|\psi_0) = \{\xi_0\tau \mid \tau \in \widehat{L}\}$ . Again,  $\widehat{L}$  and  $L$  are isomorphic  $D$ -sets and, as  $D$  acts fixed-point-freely on  $L$ , we deduce that  $D$  acts fixed-point-freely on  $\widehat{L}$  and hence  $D$  acts semi-regularly on  $\text{Irr}(I|\psi_0) \setminus \{\xi_0\}$ . In particular,  $\xi_0$  is the only  $D$ -invariant character in  $\text{Irr}(I|\psi_0)$ .

Moreover, as  $D$  acts regularly on the 1-dimensional subspaces of  $L$  and  $C_L(R)$  is one of them, it follows that every  $D$ -orbit in  $L$ , and hence in  $\widehat{L}$ , contains an  $R$ -invariant element. Therefore, for every  $\xi = \xi_0\tau \in \text{Irr}(I|\psi_0)$ , there exists an element  $y \in D$  such that  $\xi^y = (\xi_0\tau)^y = \xi_0\tau^y$  is  $R$ -invariant. Since  $\psi_0 = 1_B \times \varphi_0$  is  $S$ -invariant, a similar argument shows that all the characters in  $\text{Irr}(I|\psi_0)$  are  $S$ -invariant. Hence, there exists a set  $\mathcal{Z}$  of representatives of the  $D$ -orbits in  $\text{Irr}(I|\psi_0)$  such that every  $\xi \in \mathcal{Z}$  is  $H$ -invariant. Thus,  $\mathcal{Z}$  is in fact a set of representatives for the  $DH$ -orbits in  $\text{Irr}(I|\psi_0)$ . We observe that

necessarily  $\xi_0 \in \mathcal{Z}$  and that  $|\mathcal{Z} \setminus \{\xi_0\}| = (|L| - 1)/|D| = p - 1$ , as  $D$  acts semi-regularly on  $\text{Irr}(I|\psi_0) \setminus \{\xi_0\}$ .

Let  $W = \text{Irr}(P|Y_0) = \text{Irr}(P|\psi_0)$ . If two characters  $\theta, \theta_1 \in W$  lie in the same  $G$ -orbit, then (being  $P$ -invariant) there exists an element  $g \in CH$  such that  $\theta_1 = \theta^g$ . Since  $\varphi_0$  is the only irreducible constituent of both  $\theta_{P_3}$  and  $(\theta_1)_{P_3}$ , it follows that  $g \in I_{CH}(\varphi_0) = DH$ .

By Clifford correspondence, the mapping  $\xi \mapsto \xi^P$  is a bijection between  $\text{Irr}(I|\psi_0)$  and  $W$ . Therefore,  $\mathcal{Z}^P = \{\xi^P \mid \xi \in \mathcal{Z}\}$  is a set of representatives for the  $DH$ -orbits in  $W$ . By the previous paragraph and Lemma 2.2, we hence have that

$$\text{Irr}(G|Y_0) = \text{Irr}(G|W) = \bigcup_{\xi \in \mathcal{Z}} \text{Irr}(G|\xi^P)$$

is a disjoint union.

We claim that, for every  $\xi \in \mathcal{Z}$  with  $\xi \neq \xi_0$ ,  $I_{CH}(\xi^P) = H$ . In fact, if  $y \in I_D(\xi^P)$ , then (by [6, Theorem 6.11(c)], observing that both  $I$  and  $\psi_0$  are  $D$ -invariant)  $y$  fixes the unique irreducible constituent of  $(\xi^P)_I$  that lies over  $\psi_0$ , that is,  $\xi$  itself. Since  $D$  acts semi-regularly on  $\text{Irr}(I|\psi_0) \setminus \{\xi_0\}$  and  $\xi \neq \xi_0$ , it follows  $y = 1$ . So,  $I_D(\xi^P) = 1$  and, recalling part (b) of Lemma 3.2, we deduce  $I_C(\xi^P) = 1$ . On the other hand, for  $y \in H$ ,  $(\xi^P)^y = (\xi^y)^P = \xi^P$ , so  $\xi^P$  is  $H$ -invariant, and the claim is proved. We also observe that, since  $\xi_0$  is  $D$ -invariant, the same argument proves that  $I_{CH}(\xi_0^P) = DH$ .

Hence, for each  $\theta \in \mathcal{Z}^P$  with  $\theta \neq \xi_0^P$ , by Gallagher’s theorem we have that  $\text{Irr}(G|\theta)$  contains  $n$  characters of degree  $p^{n-3}|C|$ . In fact,  $\theta$  extends to  $I_G(\theta) = PH$ , because  $H$  is cyclic. Therefore,  $\text{Irr}(G|\mathcal{Z}^P \setminus \{\xi_0^P\})$  contains  $n(p - 1)$  characters, each of degree  $p^{n-3}(p^n - 1)/(p - 1)$ .

On the other hand,  $\xi_0^P$  extends to  $I_G(\xi_0^P) = PDH$ , but  $PDH/P \simeq DH = S \times DR$ , where  $DR$  is a Frobenius group with complement  $R$ . Thus,  $DH$  has  $n$  linear characters and  $|S|(|D| - 1)/|R| = \frac{n}{9}(p^2 + p)$  irreducible characters of degree  $|R| = 3$ . Hence, by Gallagher’s theorem,  $\text{Irr}(G|\xi_0^P)$  contains  $n$  irreducible characters of degree  $\xi_0^P(1)|E| = p^{n-3}(p^n - 1)/(p^3 - 1)$  and  $\frac{n}{9}(p^2 + p)$  irreducible characters of degree  $3p^{n-3}(p^n - 1)/(p^3 - 1)$ .

We summarize here the character degrees of  $G$ .

- (I) For each divisor  $d$  of  $n$ ,  $\text{Irr}(G/P)$  has at least one character of degree  $d$ ,
- (II)  $\text{Irr}(G/P_3|P/P_3)$  has  $n(p - 1)$  characters of degree  $(p^n - 1)/(p - 1)$  and  $np(p - 1)$  characters of degree  $p^{\frac{n-1}{2}}(p^n - 1)/(p - 1)$ ,
- (III)  $\text{Irr}(G|P_3)$  has
  - (III.A)  $n(p^3 - p)(p^2 + p + 1)/9$  characters of degree  $3p^n(p^n - 1)/(p^3 - 1)$ ,
  - (III.B) and, recalling (12), we have
    - (III.B.1)  $np(p - 1)^2$  characters of degree  $p^{n-2}(p^n - 1)/(p - 1)$ ,
    - (III.B.2)  $\cdot n(p - 1)^2$  characters of degree  $p^{n-3}(p^n - 1)/(p - 1)$ ,
    - $\cdot n(p - 1)$  characters of degree  $p^{n-3}(p^n - 1)/(p^3 - 1)$ , and
    - $\cdot n(p - 1)(p^2 + p)/9$  characters of degree  $3p^{n-3}(p^n - 1)/(p^3 - 1)$ .

Hence, we see that the character degree graph  $\Delta = \Delta(G)$  is a graph of diameter 3, with  $\alpha_\Delta = \pi(n/3)$ ,  $\beta_\Delta = \{3\}$ ,  $\gamma_\Delta = \pi((p^n - 1)/(p^3 - 1))$  and  $\delta_\Delta = \pi(p^2 + p + 1)$ , concluding the proof.  $\square$

We now shift our focus to proving Theorem B. Before proceeding, we establish some fundamental notation.

Let  $G$  be an arbitrary solvable group. We denote the first two terms of the Fitting series of  $G$  as  $F(G)$  and  $F_2(G)$ , respectively. Additionally,  $Z(G)$  denotes the center of  $G$ .

Consider a prime  $p$  and a positive integer  $n$ . Let  $F = F_{p^n}$  be a field with  $p^n$  elements and let  $F^\times = F \setminus \{0\}$ . Let  $\Gamma(p^n)$  be the group of semilinear transformations of  $F$  and let  $\Gamma_0(p^n)$  be the subgroup  $F^\times$  within  $\Gamma(p^n)$ . By definition, we have:

$$\Gamma(p^n) = \Gamma_0(p^n) \rtimes \text{Gal}(F|F_p) \cong C_{p^n-1} \rtimes C_n.$$

The following result, part of which is Theorem B, utilizes the notation introduced in Section 1 (for  $\pi_0, \pi_1, \alpha_\Delta, \beta_\Delta, \gamma_\Delta, \delta_\Delta$ ). Recall that, for a natural number  $n$  and a set of primes  $\sigma$ , we denote by  $n_\sigma$  the largest divisor  $k$  of  $n$  such that  $\pi(k) \subseteq \sigma$ .

**Theorem 5.1.** *Let  $G$  be a solvable group and assume that  $\Delta = \Delta(G)$  has diameter three. Let  $\pi_0, \pi_1, \alpha = \alpha_\Delta, \beta_\Delta, \gamma_\Delta, \delta_\Delta$  be as in Section 1. Then there exist a prime  $p$  and a positive integer  $n$  such that, setting  $n_0 = n_{\pi_0}$ , we have*

- (a)  $n_0$  is odd,
- (b)  $\{p\} \cup \pi\left(\frac{p^n-1}{p^{n/n_0}-1}\right) \subseteq \pi_1 \subseteq \{p\} \cup \pi(p^n - 1)$ ,
- (c)  $\{p\} \cup \pi\left(\frac{p^n-1}{p^{n/n_\alpha}-1}\right) \subseteq \gamma_\Delta$ ,
- (d) the subgraph of  $\Delta$  induced on  $\beta_\Delta \cup \{p\} \cup \pi\left(\frac{p^n-1}{p^{n/n_\alpha}-1}\right)$  is a clique,
- (e)  $|\gamma_\Delta| \geq 2^{|\beta_\Delta|} (2^{|\alpha|} - 1) + 1$ .

**Proof.** Let  $G$  be a solvable group such that  $\Delta = \Delta(G)$  has diameter three. Then, by [2, Theorem A]  $G = PH$ , where  $P$  is a non-abelian Sylow  $p$ -subgroup of  $G$ ,  $H$  is a  $p$ -complement of  $G$  and  $F(G) = P \times A$ , where  $A = C_H(P) \leq Z(G)$ . Let  $P_1 = [P, G]$  and  $P_i = \gamma_i(P)$  for  $i \in \{2, \dots, c\}$ , where  $c$  is the nilpotency class of  $P$  and  $\gamma_i(P)$  is the  $i^{\text{th}}$  term of the lower central series of  $P$ .

By [2, Theorem A], all factors  $M_i = P_i/P_{i+1}$  for  $i \in \{1, \dots, c\}$  are chief factors of  $G$  of the same order, say  $p^n$ , and each group  $G/C_G(M_i)$  acts irreducibly on the module  $M_i$  as a subgroup of the semilinear group  $\Gamma(p^n)$ .

Moreover, [2, Theorem A] and [2, Remark 4.4] tell us that  $\Delta(G/P_3)$  is a disconnected graph, with the same vertex set as  $\Delta(G)$ , and that the connected components of  $\Delta(G/P_3)$  are

$$\pi_0 = \pi(|G/F_2(G)|) = \pi(|H/F(H)|), \text{ and}$$

$$\pi_1 = \{p\} \cup \pi(|F_2(G)/F(G)|) = \{p\} \cup \pi(|F(H)/A|).$$

By [2, Theorem A(b)], all the Sylow subgroups of  $H/A$  are cyclic and hence, by [6, Corollary 11.22] and [6, Corollary 11.31], each irreducible character of  $F(G)$  extends to its inertia subgroup in  $G$ . Thus,  $\Delta(G) = \Delta(G/A)$  by [2, Lemma 2.4] and hence, by replacing  $G$  with  $G/A$ , we can assume that  $A = 1$  and  $P = F(G)$ .

As  $[P, H] \leq P_1$ , by coprimality  $C_H(M_1)$  acts trivially on  $P/P_2$  and hence (as  $P_2 = P'$ ) on the quotient of  $P$  over its Frattini subgroup. Since  $|H|$  is coprime to  $p$ , it follows that  $C_H(M_1) = C_H(P) = 1$ . In particular,  $H$  acts faithfully by conjugation on  $M_1$ .

Let  $m = |F(H)|$  and  $n_0 = |H/F(H)|$ ; thus  $\pi_0 = \pi(n_0)$ , in particular  $n_0 \neq 1$ , and  $\pi_1 = \{p\} \cup \pi(m)$ . Seeing  $H$ , in its action on  $M_1$ , as a subgroup of  $\Gamma(p^n)$ , let  $H_0 = H \cap \Gamma_0(p^n)$ . So  $H_0$  is a cyclic normal subgroup of  $H$  and hence  $|H_0|$  divides  $m$ . As  $H_0$  acts semi-regularly on  $\text{Irr}(M_1)$ , Clifford theory implies that, for every  $\mu \in \text{Irr}(M_1)$ ,  $I_H(\mu)$  contains a Hall  $\pi(n_0)$ -subgroup of  $H$ . Hence, [2, Lemma 3.5] yields that

$$m_0 = \frac{p^n - 1}{p^{n/n_0} - 1}$$

divides  $|H_0|$  and hence  $m_0$  divides  $m$ , proving the first inclusion in part (b).

We now show that  $n_0$  is odd, which proves part (a). In fact, if  $2 \in \pi(n_0) = \pi_0$ , then  $p \neq 2$ , because  $p$  belongs to  $\pi_1$  which has empty intersection with  $\pi_0$ . Hence,  $p \equiv 1 \pmod{2}$  implies that  $m_0 \equiv n_0 \equiv 0 \pmod{2}$ , so  $m$  is even and hence  $\pi_0 \cap \pi_1 \neq \emptyset$ , a contradiction.

We now observe that there exists a primitive prime divisor of  $p^n - 1$ . Otherwise, since  $n_0$  is an odd divisor of  $n$ , by Zsigmondy’s theorem  $p = 2$  and  $n = 6$ ; thus  $n_0 = 3$  and  $m_0 = 21$ , giving again the contradiction  $\pi_0 \cap \pi_1 \neq \emptyset$ . As a consequence, by [2, Lemma 3.7]  $F(H) = H_0$ , so  $m$  divides  $p^n - 1$  and hence  $\pi_1 \subseteq \{p\} \cup \pi(p^n - 1)$ , finishing the proof of part (b).

Write  $\alpha = \alpha_\Delta$  and  $\beta = \beta_\Delta$ ; thus  $\pi_0 = \alpha \cup \beta$  and  $n_0 = n_\alpha n_\beta$ . Let  $q = p^{n/n_0}$  (so  $m_0 = (q^{n_0} - 1)/(q - 1)$ ) and define

$$m_1 = \frac{q^{n_0} - 1}{q^{n_0/n_\alpha} - 1} = \frac{q^{n_0} - 1}{q^{n_\beta} - 1}.$$

Let now  $t \in \beta$ . We will show that  $t$  is adjacent in  $\Delta(G)$  to every prime in  $\{p\} \cup \pi(m_1)$ . By definition, there exists a prime  $s \in \gamma_\Delta$  and a character  $\chi \in \text{Irr}(G)$  such that  $ts$  divides  $\chi(1)$ . In particular, setting  $K = \ker(\chi) \cap P$ ,  $\chi$  can be considered as a character of  $G/K$ . As  $t$  is adjacent to  $s$  in  $\Delta(G/K)$ , we conclude that  $P_3 \not\leq K$ . Thus  $\Delta(G/K)$  is a connected subgraph of  $\Delta(G)$  with the same set of vertices. So,  $\Delta(G/K)$  has diameter 3. Hence, replacing  $G$  with  $G/K$ , we can assume  $K = 1$ .

Let  $M = P_c$ ; thus  $M \leq Z(P)$  and  $M$  is a faithful irreducible  $\bar{H}$ -module, where  $\bar{H} = H/C_H(M)$ . Seeing  $\bar{H}$  as a subgroup of  $\Gamma(p^n)$ , we set  $\bar{H}_0 = \bar{H} \cap \Gamma_0(p^n)$ . For every  $\mu \in \text{Irr}(M)$  and  $\psi \in \text{Irr}(P|\mu)$ ,  $\psi_M = \psi(1)\mu$  is a homogeneous character, and hence

$I_H(\psi) \leq I_H(\mu)$ . Since  $p$  divides the degree of each character in  $\text{Irr}(G|M)$  and  $p$  is not adjacent in  $\Delta(G)$  to any vertex belonging to  $\alpha$ , Clifford theory implies that, for every  $\psi \in \text{Irr}(P|M)$ ,  $I_H(\psi)$  contains a Hall  $\alpha$ -subgroup of  $H$ . Therefore, for every non-principal  $\mu \in \text{Irr}(M)$ ,  $I_{\bar{H}}(\mu)$  contains a Hall  $\alpha$ -subgroup of  $\bar{H}$  and hence, by [2, Lemma 3.5],  $m_1$  divides  $|\bar{H}_0|$ . Since  $\bar{H}_0$  acts semi-regularly on  $\text{Irr}(M)$ , we deduce that

$$\{t\} \cup \{p\} \cup \pi(m_1) \subseteq \pi(\chi(1)). \tag{13}$$

In particular,  $\{p\} \cup \pi(m_1) \subseteq \gamma_\Delta$ , proving part (c).

Moreover, since (13) holds for every  $t \in \beta$  in  $\Delta(G)$ , we conclude that  $\beta \cup \{p\} \cup \pi(m_1)$  induces a clique in  $\Delta(G)$ , which shows part (d).

Recall that, denoting by  $d(k)$  the number of positive divisors of an integer  $k$ , if  $k = p_1^{e_1} p_2^{e_2} \cdots p_v^{e_v}$ , with  $p_1, p_2, \dots, p_v$  distinct primes and  $e_1, e_2, \dots, e_v$  positive integers, then

$$d(k) = (e_1 + 1)(e_2 + 1) \cdots (e_v + 1).$$

Writing  $n_0 = \prod_{r \in \alpha} r^{e_r} \cdot \prod_{t \in \beta} t^{e_t}$  with  $e_r, e_t \geq 1$  for all  $r \in \alpha, t \in \beta$ , Lemma 4.2 implies that

$$|\pi(m_1)| \geq d(n_0) - d(n_\beta) = \prod_{t \in \beta} (e_t + 1) \left( \prod_{r \in \alpha} (e_r + 1) - 1 \right) \geq 2^{|\beta|} (2^{|\alpha|} - 1).$$

Hence, part (e) now follows from part (c).  $\square$

We finish by mentioning that [4, Question, page 91] asks for the existence of a solvable group  $G$  such that  $\Delta = \Delta(G)$  has diameter three, with  $|\alpha_\Delta| = 2, |\beta_\Delta| = 1$  (so, writing  $\beta = \{q\}$ ,  $q$  is a cut-vertex of  $\Delta$ ) and  $|\text{V}(\Delta)| = 11$ . Notice that 11 is the smallest cardinality for a putative  $\text{V}(\Delta)$ , with the given conditions on  $\alpha$  and  $\beta$ . Indeed, if such a graph  $\Delta$  exists, then Theorem 5.1 shows that  $|\gamma_\Delta| \geq 2^{|\beta_\Delta|} (2^{\alpha_\Delta} - 1) + 1 \geq 2 \cdot 3 + 1 = 7$  and  $q$  is adjacent to all other vertices of  $\Delta$ , except one. Using the notation and the arguments in the proof of Theorem 5.1, one can also show that if  $\Delta = \Delta(G)$  has eleven vertices,  $\beta = \{q\}$  and  $\alpha = \{t_1, t_2\}$ , then  $n = n_0 = qt_1t_2$  is a product of three distinct odd primes. Moreover, by the observation following Lemma 4.2, we deduce that  $p = 2$  and  $\lambda_d(2)$  is a prime power for every divisor  $d > 1$  of  $n$ . Ultimately, our inability to determine the existence of  $\Delta$  leaves us unable to conclusively address Conjecture 4.3. The presence of such a graph would refute it.

Nevertheless, we can prove the existence of a similar graph with twelve vertices. Let  $p = 2$  and  $n = 3 \cdot 5 \cdot 13$ . A computation shows that  $\text{gcd}(2^n - 1, n) = 1$ , so (1) is satisfied and hence we may apply the results from Section 3 and from the proof of Theorem A. We obtain a character degree graph  $\Delta$  having diameter three, where  $\alpha_\Delta = \{5, 13\}, \beta_\Delta = \{3\}, |\gamma_\Delta| = 8$  and  $\delta_\Delta = \{7\}$ . In particular,  $|\text{V}(\Delta)| = 12$ . (We recommend the reader to check the tables in [1] for  $|\gamma_\Delta| = 8$ .)

## Acknowledgments

We extend our heartfelt gratitude to the referee, whose insightful comments significantly enhanced the clarity and readability of this paper. We also wish to thank Ted Dobson and Susan Cook for reviewing an earlier draft and providing valuable feedback.

The first and third authors are funded by the European Union via the Next Generation EU (Mission 4 Component 1 CUP B53D23009410006, PRIN 2022, 2022PSTWLB, Group Theory and Applications). The first and the third authors are members of the GNSAGA INdAM and kindly acknowledge their support.

## Data availability

No data was used for the research described in the article.

## References

- [1] J.D. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, Factorizations of  $b^n \pm 1$ ,  $b = 2, 3, 5, 6, 7, 10, 11, 12$  up to High Powers, Contemporary Mathematics, vol. 22, American Mathematical Society, 1988.
- [2] C. Casolo, S. Dolfi, E. Pacifici, L. Sanus, Groups whose character degree graph has diameter three, *Isr. J. Math.* 215 (2016) 523–558.
- [3] S. Dolfi, E. Pacifici, L. Sanus, V. Sotomayor, Non-solvable groups whose character degree graph has a cut-vertex. I, *Vietnam J. Math.* 51 (2023) 731–753.
- [4] R. Hafezieh, M.A. Hosseinzadeh, S. Hossein-Zadeh, A. Iranmanesh, On cut vertices and eigenvalues of character graphs of solvable groups, *Discrete Appl. Math.* 303 (2021) 86–93.
- [5] A. Hanaki, T. Okuyama, Groups with some combinatorial properties, *Osaka J. Math.* 34 (1997) 337–356.
- [6] I.M. Isaacs, Character Theory of Finite Groups, Pure and Applied Mathematics, Academic Press, New York, 1976.
- [7] I.M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Can. J. Math.* 41 (1989) 68–82.
- [8] M.L. Lewis, A solvable group whose character degree graph has diameter 3, *Proc. Am. Math. Soc.* 130 (2001) 625–630.
- [9] M.L. Lewis, An overview of graphs associated with character degrees and conjugacy class sizes in finite groups, *Rocky Mt. J. Math.* 38 (2008) 175–211.
- [10] M.L. Lewis, D.L. White, Diameters of degree graphs of nonsolvable groups. II, *J. Algebra* 312 (2007) 634–649.
- [11] M.L. Lewis, Q. Meng, Solvable groups whose prime divisor character degree graphs are 1-connected, *Monatshefte Math.* 190 (2019) 541–548.
- [12] J.K. McVey, On a Galois connection between the subfield lattice and the multiplicative subgroup lattice, *Pac. J. Math.* 264 (2013) 213–219.
- [13] P.P. Pálffy, On the character degree graph of solvable groups. I. Three primes, *Period. Math. Hung.* 36 (1998) 61–65.
- [14] P.P. Pálffy, On the character degree graph of solvable groups. II. Disconnected graphs, *Studia Sci. Math. Hung.* 38 (2001) 339–355.
- [15] J.M. Riedl, Character degrees, class sizes, and normal subgroups of a certain class of  $p$ -groups, *J. Algebra* 218 (1999) 190–215.
- [16] C.B. Sass, Character degree graphs of solvable groups with diameter three, *J. Group Theory* 19 (2016) 1097–1127.
- [17] T. Wolf, Character correspondences in solvable groups, III, *J. Math.* 22 (1978) 327–340.