ZASSENHAUS CONJECTURE ON TORSION UNITS HOLDS FOR $\mathrm{SL}(2,p)$ AND $\mathrm{SL}(2,p^2)$

ÁNGEL DEL RÍO AND MARIANO SERRANO

Abstract. H.J. Zassenhaus conjectured that any unit of finite order and augmentation 1 in the integral group ring $\mathbb{Z}G$ of a finite group G is conjugate in the rational group algebra $\mathbb{Q}G$ to an element of G. We prove the Zassenhaus Conjecture for the groups $\mathrm{SL}(2,p)$ and $\mathrm{SL}(2,p^2)$ with p a prime number. This is the first infinite family of non-solvable groups for which the Zassenhaus Conjecture has been proved. We also prove that if $G = \mathrm{SL}(2,p^f)$, with f arbitrary and u is a torsion unit of $\mathbb{Z}G$ with augmentation 1 and order coprime with p then u is conjugate in $\mathbb{Q}G$ to an element of G. By known results, this reduces the proof of the Zassenhaus Conjecture for this groups to prove that every unit of $\mathbb{Z}G$ of order multiple of p and augmentation 1 has actually order p.

1. Introduction

For a finite group G, let $\mathrm{V}(\mathbb{Z}G)$ denote the group of units of augmentation 1 in $\mathbb{Z}G$. We say that two elements of $\mathbb{Z}G$ are *rationally conjugate* if they are conjugate in the units of $\mathbb{Q}G$. The following conjecture stated by H.J. Zassenhaus [Zas74] (see also [Seh93, Section 37]) has centered the research on torsion units of integral group rings during the last decades:

> **Zassenhaus Conjecture:** If G is a finite group then every torsion element of $\mathrm{V}(\mathbb{Z}G)$ is rationally conjugate to an element of G.

The relevance of the Zassenhaus Conjecture is that it describes the torsion units of the integral group ring of $\mathbb{Z}G$ provided it holds for G. Recently, Eisele and Margolis announced a metabelian counterexample to the Zassenhaus Conjecture [EM18]. Nevertheless, the Zassenhaus Conjecture holds for large classes of solvable groups, e.g. for nilpotent groups [Wei91], groups possessing a normal Sylow subgroup with abelian complement [Her06] or cyclic-by-abelian groups [CMR13]. In contrast with these results, the list of non-solvable groups for which the Zassenhaus Conjecture has been proved is very limited [LP89, DJPM97, Her07, Her08, BH08, BKL08, BM17c, RS17]. For example, the Zassenhaus Conjecture has only been proved for sixty-two simple groups, all of them of the form $\mathrm{PSL}(2,q)$ (see the proof of Theorem C in [BM18] and [MRS18]).

The goal of this paper is proving the following theorem:

Theorem 1.1. *Let $G = SL(2,q)$ with q an odd prime power and let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$ of order coprime with q. Then u is rationally conjugate to an element of G.*

As a consequence of Theorem 1.1 and known results we will obtain the following theorem which provides the first positive result on the Zassenhaus Conjecture for an infinite series of non-solvable groups.

Theorem 1.2. *The Zassenhaus Conjecture holds for $SL(2,p^f)$ with p a prime number and $f \leq 2$.*

In Section 2 we prove a number theoretical result relevant for our arguments. Known results on $\mathrm{V}(\mathbb{Z}G)$ and properties of $\mathrm{V}(\mathbb{Z}\,\mathrm{SL}(2,q))$ are collected in Section 3. A particular case of Theorem 1.1 is proved in Section 4. Finally in Section 5 we prove Theorem 1.1.

Date: March 25, 2019.
2010 *Mathematics Subject Classification.* 16U60, 16S34.
Key words and phrases. Group rings, units, Zassenhaus Conjecture.
Partially supported by Ministerio de Economía y Competitividad projects MTM2012-35240 and MTM2016-77445-P and Fondos FEDER and Fundación Séneca of Murcia 19880/GERM/15.

2. Number theoretical preliminaries

We use the standard notation for the Euler totient function φ and the Möbius function μ. Moreover, $\mathbb{Z}_{\geq 0}$ denotes the set of non-negative integers. Let n be a positive integer. Then $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, ζ_n denotes a complex primitive n-th root of unity, $\Phi_n(X)$ denotes the n-th cyclotomic polynomial, i.e. the minimal polynomial of ζ_n over $\mathbb{Q}$, and for a prime integer p let $v_p(n)$ denote the valuation of n at p, i.e. the maximum non-negative integer m with $p^m \mid n$. If F/K is a finite field extension then $\mathrm{Tr}_{F/K} : F \to K$ denotes the standard trace map. We will frequently use the following formula for d a divisor of n [Mar16, Lemma 2.1]:

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_d) = \mu(d)\frac{\varphi(n)}{\varphi(d)}. \tag{2.1}$$

We reserve the letter p to denote a positive prime integer and for every positive integer n we set

$$n' = \prod_{p \mid n} p \quad \text{and} \quad n_p = p^{v_p(n)}.$$

If moreover $x \in \mathbb{Z}$ then we set

$$\begin{aligned}
(x : n) &= \text{representative of the class of } x \text{ modulo } n \text{ in the interval } \left(-\frac{n}{2}, \frac{n}{2}\right]; \\
|x : n| &= \text{the absolute value of } (x : n); \\
\gamma_n(x) &= \prod_{\substack{p \mid n \\ |x:n_p| < \frac{n_p}{2p}}} p \quad \text{and} \quad \bar{\gamma}_n(x) = \prod_{\substack{p \mid n \\ |x:n_p| \leq \frac{n_p}{2p}}} p = \begin{cases} 2\gamma_n(x), & \text{if } |x : n_2| = \frac{n_2}{4}; \\ \gamma_n(x), & \text{otherwise.} \end{cases}
\end{aligned}$$

The next lemma collects two facts which follow easily from the definitions.

Lemma 2.1. *Let p be a prime dividing n and let $x, y \in \mathbb{Z}$. Then the following conditions hold:*

(1) If $p \mid \bar{\gamma}_n(x)$ then $\left(x : \frac{n_p}{p}\right) \equiv x \bmod n_p$.
(2) Let $d \mid n'$ such that $x \equiv y \bmod \frac{n}{d}$. If d divides both $\bar{\gamma}_n(x)$ and $\bar{\gamma}_n(y)$ then $x \equiv y \bmod n$.

For integers x and y we define the following equivalence relation on $\mathbb{Z}$:

$$x \sim_n y \quad \Leftrightarrow \quad x \equiv \pm y \mod n.$$

We denote by Γ_n the set of these equivalence classes.

If x, y and n are integers with $n > 0$ then let

$$\delta_{x,y}^{(n)} = \begin{cases} 1, & \text{if } x \sim_n y; \\ 0, & \text{otherwise;} \end{cases} \quad \text{and} \quad \kappa_x^{(n)} = \begin{cases} 2, & \text{if } x \equiv 0 \bmod n \text{ or } x \equiv \frac{n}{2} \bmod n; \\ 1, & \text{otherwise.} \end{cases}$$

For an integer x (or $x \in \Gamma_n$) we set

$$\alpha_x^{(n)} = \zeta_n^x + \zeta_n^{-x}.$$

Observe that $\mathbb{Q}(\alpha_1^{(n)})$ is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\alpha_1^{(n)}]$ is the ring of integers of $\mathbb{Q}(\alpha_1^{(n)})$. If $n \neq n_2$ then let p_0 denote the smallest odd prime dividing n. Then let

$$\mathbb{B}_n = \left\{ x \in \mathbb{Z}_n : \text{ for every } p \mid n, \text{ either } \begin{array}{l} |x : n_p| > \frac{n_p}{2p} \text{ or} \\ p = 2, n \neq n_2, |x : n_2| = \frac{n_2}{4}, n_{p_0} \nmid x \text{ and } (x : n_2) \cdot (x : n_{p_0}) > 0 \end{array} \right\}$$

and

$$\mathcal{B}_n = \begin{cases} \{\alpha_b^{(n)} : b \in \mathbb{B}_n\}, & \text{if } n \neq n_2; \\ \{1\} \cup \{\alpha_b^{(n)} : b \in \mathbb{B}_n\}, & \text{otherwise.} \end{cases}$$

For $b \in \mathbb{B}_n$ and $x \in \mathbb{Z}$ let

$$\beta_{b,x}^{(n)} = \begin{cases} -1, & \text{if } n \neq n_2, |x : n_2| = \frac{n_2}{4} \text{ and } (x : n_2) \cdot (b : n_{p_0}) < 0; \\ 1, & \text{otherwise.} \end{cases}$$

The following proposition extends Proposition 3.5 of [MRS18]. The first statement implies that $\mathcal{B}_n$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha_1^{(n)})$. For $x \in \mathbb{Q}(\alpha_1^{(n)})$ and $b \in \mathbb{B}_n$ we use $C_b(x)$ to denote the coefficient of $\alpha_b^{(n)}$ in the expression of x in the basis $\mathcal{B}_n$.

Proposition 2.2. *Let n be a positive integer. Then*

(1) $\mathcal{B}_n$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha_1^{(n)}]$.

(2) If $b \in \mathbb{B}_n$ and $i \in \mathbb{Z}$ then $C_b(\alpha_i^{(n)}) = \kappa_i^{(n)} \cdot \mu(\gamma(i)) \cdot \beta_{b,i}^{(n)} \cdot \delta_{b,i}^{(n/\bar{\gamma}(i))}$.

Proof. We only prove the proposition in the case $n \neq n_2$, as the proof in the case $n = n_2$ is similar (actually simpler). It is easy to see that $|\mathcal{B}_n| \leq \frac{\varphi(n)}{2} = [\mathbb{Q}(\alpha_1^{(n)}) : \mathbb{Q}]$. Thus it is enough to prove the following equality $\alpha_i^{(n)} = \kappa_i^{(n)}\, \mu(\gamma(i)) \sum_{b \in \mathbb{B}_n, b \sim_{n/\bar{\gamma}(i)} i} \beta_{b,i}^{(n)}\, \alpha_b^{(n)}$. Actually we will show

$$\zeta_n^i = \mu(\gamma(i)) \sum_{\substack{b \equiv i \bmod n/\bar{\gamma}(i) \\ b \in \mathbb{B}_n}} \beta_{b,i}^{(n)}\, \zeta_n^b$$

which easily implies the desired expression of $\alpha_i^{(n)}$.

Indeed, for every $p \mid n$ let ζ_{n_p} denote the p-th part of ζ_n, i.e. ζ_{n_p} is a primitive n_p-th root of unity and $\zeta_n = \prod_{p|n} \zeta_{n_p}$. Let J be the set of tuples $(j_p)_{p|\bar{\gamma}(i)}$ satisfying the following conditions:

- If $p \mid \gamma(i)$ then $j_p \in \{1, \ldots, p-1\}$.
- If $p = 2$ and $|i : n_2| = \frac{n_2}{4}$ then $j_2 = \begin{cases} 1, & \text{if } (i : n_2) \cdot \left(i + j_{p_0} \frac{n_{p_0}}{p_0} : n_{p_0}\right) < 0; \\ 0, & \text{otherwise.} \end{cases}$

For every $j \in J$ let $b_j \in \mathbb{Z}_n$ given by

$$b_j \equiv \begin{cases} i + j_p \frac{n_p}{p} \mod n_p, & \text{if } p \mid \bar{\gamma}(i); \\ i \mod n_p, & \text{otherwise.} \end{cases}$$

Then $\{b_j : j \in J\}$ is the set of elements in $\mathbb{B}_n$ satisfying $i \equiv b \bmod \frac{n}{\bar{\gamma}(i)}$. From

$$0 = \zeta_{n_p}^i \left(1 + \zeta_{n_p}^{\frac{n_p}{p}} + \zeta_{n_p}^{\frac{2n_p}{p}} + \ldots + \zeta_{n_p}^{\frac{(p-1)n_p}{p}}\right)$$

we obtain $\zeta_{n_p}^i = -\sum_{j_p=1}^{p-1} \zeta_{n_p}^{i + j_p \frac{n_p}{p}}$. Therefore, if $|i : n_2| \neq \frac{n_2}{4}$ then $\gamma(i) = \bar{\gamma}(i)$, $\beta_{b,i}^{(n)} = 1$ for every $b \in \mathbb{B}_n$ and

$$\zeta_n^i = \prod_{\substack{p|n \\ p \nmid \gamma(i)}} \zeta_{n_p}^i \prod_{\substack{p|n \\ p|\gamma(i)}} \left(-\sum_{j_p=1}^{p-1} \zeta_{n_p}^{i + j_p \frac{n_p}{p}}\right) = \mu(\gamma(i)) \sum_{j \in J} \zeta_n^{b_j} = \mu(\gamma(i)) \sum_{\substack{b \equiv i \bmod n/\bar{\gamma}(i) \\ b \in \mathbb{B}_n}} \zeta_n^b.$$

This gives the desired equality in this case.

Suppose that $|i : n_2| = \frac{n_2}{4}$. Then $\zeta_{n_2}^i = \beta_{b_j,i}^{(n)} \zeta_{n_2}^{b_j}$ for every $j \in J$. Then a small modification of the argument in the previous paragraph gives

$$\zeta_n^i = \zeta_{n_2}^i \prod_{\substack{p|n \\ p \nmid \gamma(i)}} \zeta_{n_p}^i \prod_{\substack{p|n \\ p|\gamma(i)}} \left(-\sum_{j_p=1}^{p-1} \zeta_{n_p}^{i + j_p \frac{n_p}{p}}\right) = \mu(\gamma(i)) \sum_{j \in J} \beta_{b,i}^{(n)}\, \zeta_n^{b_j} = \mu(\gamma(i)) \sum_{\substack{b \equiv i \bmod n/\bar{\gamma}(i) \\ b \in \mathbb{B}_n}} \beta_{b,i}^{(n)}\, \zeta_n^b.$$

□

3. Group theoretical preliminaries

Let G be a finite group. We denote by $Z(G)$ the center of G. If $g \in G$ then $|g|$ denotes the order of g, $\langle g \rangle$ denotes the cyclic group generated by g, and g^G denotes the conjugacy class of g in G. If R is a ring then RG denotes the group ring of G with coefficients in R. If $\alpha = \sum_{g \in G} \alpha_g g$ is an element of a group ring RG, with each $\alpha_g \in R$, then the partial augmentation of α at g is defined as

$$\varepsilon_g(\alpha) = \sum_{h \in g^G} \alpha_h.$$

We collect here some known results on partial augmentations of an element u of order n in $\mathrm{V}(\mathbb{Z}G)$.

(A) [JR16, Proposition 1.5.1] (Berman-Higman Theorem). If $g \in Z(G)$ and $u \neq g$ then $\varepsilon_g(u) = 0$.

(B) [Her07, Theorem 2.3] If $g \in G$ and $\varepsilon_g(u) \neq 0$ then $|g|$ divides n.

(C) [MRSW87, Theorem 2.5] u is rationally conjugate to an element of G if and only if $\varepsilon_g(u^d) \geq 0$ for all $g \in G$ and all divisors d of n.

(D) [LP89, Her07] Let F be a field of characteristic $t \geq 0$ with $t \nmid n$. Let ρ be an F-representation of G. If $t \neq 0$ then let ξ_n be a primitive n-th root of unity in F, so that if $t = 0$ then $\xi_n = \zeta_n$. Let T be a set of representatives of the conjugacy classes of t-regular elements of G (all the conjugacy classes if $t = 0$). Let χ denote the character afforded by ρ if $t = 0$, and the t-Brauer character of G afforded by ρ if $t > 0$ (using a group isomorphism associating ξ_n to ζ_n). Then for every integer ℓ, the multiplicity of ξ_n^ℓ as eigenvalue of $\rho(u)$ is

$$\frac{1}{n} \sum_{x \in T} \sum_{d \mid n} \varepsilon_x(u^d) \mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)\zeta_n^{-\ell d})$$

In the remainder of the paper we fix an odd prime power q and let $G = \mathrm{SL}(2,q)$, $\overline{G} = \mathrm{PSL}(2,q)$ and let $\pi : G \to \overline{G}$ denote the natural projection, which we extend by linearity to a ring homomorphism $\pi : \mathbb{Z}G \to \mathbb{Z}\overline{G}$.

We collect some group theoretical properties of G and $\overline{G}$ (see e.g. [Dor71, Theorem 38.1]).

(E) G has a unique element J of order 2 and $q+4$ conjugacy classes. More precisely, if p is the prime dividing q then 2 of the classes are formed by elements of order p, another 2 are formed by elements of order $2p$ and q classes are formed by elements of order dividing $q+1$ or $q-1$. Furthermore, if g and h are p-regular elements of G and $|h|$ divides $|g|$ then h is conjugate in G to an element of $\langle g \rangle$ and two elements of $\langle g \rangle$ are conjugate in G if and only if they are equal or mutually inverse.

(F) Let C be a conjugacy class of $\overline{G}$ formed by elements of order n. If $n = 2$ then $\pi^{-1}(C)$ is the only conjugacy class of G formed by elements of order 4. Otherwise, $\pi^{-1}(C)$ is the union of two conjugacy classes C_1 and C_2 of G with $C_2 = JC_1$. Furthermore, if n is multiple of 4 then the elements of C_1 and C_2 have order $2n$ while if n is not multiple of 4 then one of the classes C_1 or C_2 is formed by elements of order n.

The following proposition collects some consequences of these facts.

Proposition 3.1. *Let $G = SL(2,q)$ and let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. Set $\overline{G} = PSL(2,q)$ and $n = |u|$. Then the following statements holds:*

(1) J is the unique element of order 2 in $\mathrm{V}(\mathbb{Z}G)$.

(2) $|\pi(u)| = \frac{n}{\gcd(2,n)}$.

(3) If $4 \nmid n$ and $\pi(u)$ is rationally conjugate to an element of $\overline{G}$ then u is rationally conjugate to an element of G.

(4) If $\gcd(n,q) = 1$ and either $n = 4$ or $4 \nmid n$ then u is rationally conjugate to an element of G.

(5) If $\gcd(n,q) = 1$ then G has an element of order n.

(6) Suppose that $q = p^f$ with p prime, $f \leq 2$ and $p \mid n$. Then u is rationally conjugate to an element of G.

(7) *If ρ is a representation of G and ζ is a root of unity of order dividing n then ζ and ζ^{-1} have the same multiplicity as eigenvalues of $\rho(u)$.*

Proof. (1) is a direct consequence of (A) and (E).

(2) By the main result of [Mar17], if $\pi(u) = 1$ then $u^2 = 1$ and hence either $u = 1$ or $u = J$, by (1). Then (2) follows.

(3) Suppose that n is not multiple of 4. If n is even then the order of Ju is odd, by (1). Thus, we may assume without loss of generality that the order of u is odd. If $\varepsilon_g(u) \neq 0$ then $|g|$ is odd, by (B), and hence $\varepsilon_g(u) = \varepsilon_{\pi(g)}(\pi(u)) \geq 0$, by (F). Thus u is rationally conjugate to an element of G.

(4) Let $q = p^f$ where p is an odd prime number and $p \nmid n$. By (E), G has a unique conjugacy class C formed by elements of order 4 and a unique element of order 2. Thus, by (A) and (B), if $n = 4$ then $\varepsilon_g(u) = 0$ for every $g \notin C$, and hence u is rationally conjugate to an element of G, by (C).

If $4 \nmid n$ then $|\pi(u)|$ is coprime with $2q$, by (2), and hence $\pi(u)$ is rationally conjugate to an element of $\overline{G}$, by [MRS18, Theorem 1.1]. Then u is rationally conjugate to an element of G by (3). (5) is a consequence of (2) and [Her07, Proposition 6.7].

(6) In this case $|\pi(u)| = p$ by (2) and [BM17b, Theorem A]. Then n is either p or $2p$, by (2), and $\pi(u)$ is rationally conjugate to an element of $\overline{G}$, by [Her07, Proposition 6.1]. Thus u is rationally conjugate to an element of G, by (3).

(7) is a consequence of (E) and the formula in (D). □

Observe that for q odd, Theorem 1.2 follows at once from Theorem 1.1 and statement (6) of Proposition 3.1. On the other hand $\mathrm{SL}(2,2) \cong S_3$ and $\mathrm{SL}(2,4) \cong A_5$ for which the Zassenhaus Conjecture is well known. So in the remainder of the paper we concentrate on proving Theorem 1.1. For that from now on t denotes the prime dividing q (we want to use freely the letter p to denote an arbitrary prime) and we introduce some t-Brauer characters of G.

Let g be an element of G of order n with $t \nmid n$ and let ξ_n denote a primitive n-th root of unity in a field F of characteristic t. Adapting the proof of [Mar16, Lemma 1.2] we deduce that for every positive integer m there is an F-representation Θ_m of G of degree $1 + m$ such that

$$\Theta_m(g) = \begin{cases} \mathrm{diag}\left(1, \xi_n^2, \xi_n^{-2}, \ldots, \xi_n^m, \xi_n^{-m}\right), & \text{if } 2 \mid m; \\ \mathrm{diag}\left(\xi_n, \xi_n^{-1}, \xi_n^3, \xi_n^{-3}, \ldots, \xi_n^m, \xi_n^{-m}\right), & \text{if } 2 \nmid m. \end{cases} \tag{3.1}$$

In particular, the restriction to $\langle g \rangle$ of the t-Brauer character associated to Θ_m is given by

$$\chi_m(g^i) = \sum_{\substack{j=-m \\ j \equiv m \bmod 2}}^{m} \zeta_n^{ij}.$$

4. Prime power order

In this section we prove the following particular case of Theorem 1.1.

Proposition 4.1. *Let $G = SL(2,q)$ with q an odd prime power and let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. If the order of u is a prime power and it is coprime with q then u is rationally conjugate to an element of G.*

Proof. By Proposition 3.1.(4) we may assume that $|u| = 2^r$ with $r \geq 3$. We argue by induction on r. So we assume that units of order 2^k with $1 \leq k \leq r-1$ are rationally conjugate to an element of G. By Proposition 3.1.(5) and (E), G has an element g_0 of order 2^r such that $\{g_0^k : k = 0, 1, 2, \ldots, 2^{r-1}\}$ is a set of representatives of the conjugacy classes of G with order a divisor of 2^r. By (B), the only possible non-zero partial augmentations of

u are the integers $\varepsilon_k = \varepsilon_{g_0^k}(u)$, with $k = 1, \dots, 2^{r-1} - 1$. By the induction hypothesis, if $1 \le i \le r$ and $g \in G$ then $\varepsilon_g(u^{2^i}) \ge 0$. Hence, by (C), it suffices to prove that $\varepsilon_k = 0$ for all but one $k = 0, 1, \dots, 2^{r-1}$.

By [Mar16, Theorem 2] and Proposition 3.1.(2), $\pi(u)$ is rationally conjugate to an element of order 2^{r-1} in $\overline{G}$ and hence $\varepsilon_{2^{r-2}} = \varepsilon_{\pi(g_0)^{2^{r-2}}}(\pi(u)) = 0$, by (F).

For a t-Brauer character χ of G and an integer ℓ define

$$A(\chi, \ell) = \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \cdot \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\chi(g_0^k) \cdot \zeta_{2^r}^{-\ell}\right) \quad \text{and} \quad B(\chi, \ell) = \sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\chi(g_0^{2^{r-k}}) \cdot \zeta_{2^k}^{-\ell}\right).$$

Then, by (D), we have

$$\frac{1}{2^r}\left(A(\chi, \ell) + B(\chi, \ell)\right) \in \mathbb{Z}_{\ge 0}. \tag{4.1}$$

Observe that $B(\chi, \ell + 2^{r-1}) = B(\chi, \ell)$ and $A(\chi, \ell + 2^{r-1}) = -A(\chi, \ell)$. Therefore, from (4.1) it follows that

$$\text{if } B(\chi, \ell) = 0 \text{ then } A(\chi, \ell) = 0; \tag{4.2}$$

$$\text{if } B(\chi, \ell) = 2^{r-1} \text{ then } A(\chi, \ell) = \pm 2^{r-1}. \tag{4.3}$$

We will calculate $B(\chi, \ell)$ and $A(\chi, \ell)$ for several t-Brauer characters χ and several integers ℓ and for that we will use (2.1) without further mention. We start proving that

$$\text{if } 0 \le h \le r-2 \text{ and } 2^{r-1} \mid \ell \text{ then } B(\chi_{2^h}, \ell) = \begin{cases} 2^{r-1}, & \text{if } h \ge 1; \\ 0, & \text{if } h = 0; \end{cases} \tag{4.4}$$

and

$$\text{if } 0 \le h \le r-3,\ 2^h \mid \ell \text{ and } 2^{r-1} \nmid \ell \text{ then } B(\chi_{2^h}, \ell) = \begin{cases} 2^{r-1}, & \text{if } \ell \equiv \pm 2^h \bmod 2^{r-1}; \\ 0, & \text{otherwise.} \end{cases} \tag{4.5}$$

In both cases we argue by induction on h with the cases $h = 0$ and $h = 1$ being straightforward. Suppose that $1 < h \le r-2$, $2^{r-1} \mid \ell$ and $B(\chi_{2^{h-1}}, \ell) = 2^{r-1}$. If j is even, then straightforward calculations show that $\sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-2^{h-1}-j}\right) = 0$. This implies that $B(\chi_{2^h}, \ell) = B(\chi_{2^{h-1}}, \ell) + \sum_{\substack{j=2 \\ 2 \mid j}}^{2^{h-1}} \sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-2^{h-1}-j}\right) = 2^{r-1}$. This finishes the proof of (4.4).

Suppose that $1 < h \le r-3$, $2^h \mid \ell$ and $2^{r-1} \nmid \ell$. In this case the induction hypothesis implies $B(\chi_{2^{h-1}}, \ell) = 0$. Arguing as in the previous paragraph we get $B(\chi_{2^h}, \ell) = \sum_{j=2, 2 \mid j}^{2^{h-1}} \sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-(2^{h-1}+j)}\right)\zeta_{2^k}^{-\ell}\right)$. However, if j is even and smaller than 2^{h-1} then $\sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-(2^{h-1}+j)}\right)\zeta_{2^k}^{-\ell}\right) = 0$. Therefore, having in mind that $\zeta_{2^{h+2}}^{2^h} + \zeta_{2^{h+2}}^{-2^h} = 0$ we have

$$B(\chi_{2^h}, \ell) = \sum_{k=0}^{h} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right) + \epsilon 2^{h+1} + \sum_{k=h+3}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right),$$

where $\epsilon = 1$ if $2^{h+1} \nmid \ell$ and $\epsilon = -1$ otherwise. Then the claim follows using the following equalities that can be proved by straightforward calculations: $\sum_{k=0}^{h} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right) = 2^{h+1}$ and

$$\sum_{k=h+3}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right) = \begin{cases} 0, & \text{if } 2^{h+1} \mid \ell; \\ 2^{r-1} - 2^{h+2}, & \text{if } 2^{h+1} \nmid \ell \text{ and } \ell \equiv \pm 2^h \bmod 2^{r-1}; \\ -2^{h+2}, & \text{if } 2^{h+1} \nmid \ell \text{ and } \ell \not\equiv \pm 2^h \bmod 2^{r-1}. \end{cases}$$

This finishes the proof of (4.5).

We now prove, by induction on h, that the following two statements hold for any integer $0 \le h \le r-3$:

$$\sum_{k\in X_h} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}) = \pm 1, \text{ where } X_h = \{i \in \{1,\dots,2^{r-2}\} : i \equiv \pm 1 \bmod 2^{r-h}\}; \tag{4.6}$$

$$\text{if } i \equiv \pm j \bmod 2^{r-h-1} \text{ and } i \not\equiv 0, \pm 1 \bmod 2^{r-h-1} \text{ then } \varepsilon_i = \varepsilon_j; \tag{4.7}$$

and that the next one holds for every $0 \le h \le r-2$:

$$\text{if } i \equiv 0 \bmod 2^{r-h-1} \text{ then } \varepsilon_i = 0. \tag{4.8}$$

Observe that $X_0 = \{1\}$. Fix an integer i. Then for every integer k we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\left(\zeta_{2^r}^k + \zeta_{2^r}^{-k}\right)\zeta_{2^r}^{-i}\right) = \begin{cases} 2^{r-1}, & \text{if } k \equiv i \mod 2^r; \\ -2^{r-1}, & \text{if } k \equiv 2^{r-1} - i \mod 2^r; \\ 0, & \text{otherwise.} \end{cases}$$

Thus $A(\chi_1, i) = 2^{r-1}(\varepsilon_i - \varepsilon_{i+2^{r-1}})$ and hence for $h = 0$, (4.6) and (4.7) follows at once from (4.2), (4.3) and (4.5). Moreover, for $h = 0$ (4.8) is clear because $\varepsilon_{2^{r-1}} = 0$.

Suppose $0 < h \le r-3$ and (4.6), (4.7) and (4.8) hold for h replaced by $h-1$. Suppose also that $i \not\equiv 0 \bmod 2^{r-h-1}$. To prove (4.6) and (4.7) we first compute $A(\chi_{2^h}, 2^h i)$ which we split in three summands:

$$\begin{aligned} A(\chi_{2^h}, 2^h i) &= \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(\zeta_{2^r}^{-2^h i}) + \sum_{\substack{j=2\\ 2|j}}^{2^h-2} \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\left(\zeta_{2^r}^{kj} + \zeta_{2^r}^{-kj}\right)\zeta_{2^r}^{-2^h i}\right) \\ &\quad + \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{2^h(k-i)} + \zeta_{2^r}^{-2^h(k+i)}\right). \end{aligned}$$

We now prove that the first two summands are 0. This is clear for the first one because $2^{r-1} \nmid 2^h i$. To prove that the second summand is 0 let $2 \le j \le 2^h - 2$ and $2 \mid j$. Observe that $2^h \nmid j$. Thus, if k is odd then the order of $\zeta_{2^r}^{\pm kj - 2^h i}$ is multiple of 2^{r-h-1} and, as $h \le r-3$, we deduce that $\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{kj-2^h i}\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{-kj-2^h i}\right) = 0$. Thus we only have to consider the summands with k even. Actually we can exclude also the summands with $2^{r-h} \mid k$ because, by the induction hypothesis on (4.8), for such k we have $\varepsilon_k = 0$. For the remaining values of k (i.e. k even and not multiple of 2^{r-h}) we have $\varepsilon_k = \varepsilon_l$ if $k \equiv l \bmod 2^{r-h-1}$, by the induction hypothesis on (4.7). So, we can rewrite $\sum_{k=1}^{2^{r-1}-1} \varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\left(\zeta_{2^r}^{kj} + \zeta_{2^r}^{-kj}\right)\zeta_{2^r}^{-2^h i}\right)$ as

$$\sum_{l\in\mathbb{Z}_{2^{r-h-1}}} \varepsilon_l \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{l-2^h i}\left(\sum_{a=0}^{2^h-1}(\zeta_{2^r}^{2^{r-h-1}j})^a\right) + \zeta_{2^r}^{-l-2^h i}\left(\sum_{a=0}^{2^h-1}(\zeta_{2^r}^{-2^{r-h-1}j})^a\right)\right),$$

which is 0 because $\zeta_{2^r}^{2^{r-h-1}j}$ is a root of unity different from 1 and of order dividing 2^h, as j is even but not multiple of 2^h. This finishes the proof that the first two summands are 0. To finish the calculation of $A(\chi_{2^h}, 2^h i)$ we compute

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{2^h(k-i)} + \zeta_{2^r}^{-2^h(k+i)}\right) = \begin{cases} 2^{r-1}, & \text{if } k \in X_{h,i}; \\ -2^{r-1}, & \text{if } k - 2^{r-h-1} \in X_{h,i}; \\ 0, & \text{otherwise,} \end{cases}$$

where $X_{h,i} = \{k \in \{1,\dots,2^{r-2}\} : k \equiv \pm i \bmod 2^{r-h}\}$. So we have proved the following:

$$A(\chi_{2^h}, 2^h i) = 2^{r-1} \sum_{k\in X_{h,i}} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}).$$

Then (4.6) follows from (4.3), (4.5) and the previous formula. Using (4.2) we also obtain that $\sum_{k\in X_{h,i}}\varepsilon_k = \sum_{k\in X_{h,i}}\varepsilon_{k+2^{r-h-1}}$ if $i\not\equiv \pm 1 \bmod 2^{r-h-1}$. However, in this case the induction hypothesis for (4.7) means that the ε_k with $k\in X_{h,i}$ are all equal and the $\varepsilon_{k+2^{r-h-1}}$ with $k\in X_{h,i}$ are all equal. Hence (4.7) follows.

In order to deal with (4.8), assume that $0<h\le r-2$. By induction hypothesis on (4.8) we have $\varepsilon_k=0$ if $2^{r-h}\mid k$, and by the induction hypothesis on (4.7), we have that ε_k is constant on the set X formed by integers $1\le k\le 2^{r-1}$ such that $k\equiv 2^{r-h-1} \mod 2^{r-h}$. We will use these two facts without specific mention. Arguing as before we have

$$\begin{aligned} A(\chi_{2^h},0) &= \sum_{k=1}^{2^{r-1}-1}\varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(1+\zeta_{2^r}^{2^hk}+\zeta_{2^r}^{-2^hk}\right)+\sum_{k=1}^{2^{r-1}-1}\varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\sum_{j=1}^{2^{h-1}-1}\left(\zeta_{2^r}^{2jk}+\zeta_{2^r}^{-2jk}\right)\right)\\ &= \sum_{k=1,2^{r-h}\nmid k}^{2^{r-1}-1}\varepsilon_k \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(1+\zeta_{2^r}^{2^hk}+\zeta_{2^r}^{-2^hk}\right). \end{aligned}$$

As

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(1+\zeta_{2^r}^{2^hk}+\zeta_{2^r}^{-2^hk}\right)=\begin{cases}2^{r-1}, & \text{if } 2^{r-h-1}\nmid k;\\ -2^{r-1}, & \text{if } 2^{r-h-1}\mid k \text{ and } 2^{r-h}\nmid k;\end{cases}$$

we obtain

$$A(\chi_{2^h},0)=2^{r-1}\left(\sum_{2^{r-h-1}\nmid k}\varepsilon_k-\sum_{2^{r-h-1}\mid k}\varepsilon_k\right)=2^{r-1}\left(1-2\sum_{k\in X}\varepsilon_k\right)=2^{r-1}\left(1-2|X|\varepsilon_k\right).$$

From (4.3) and (4.4) we deduce that if $k\in X$ then $1-2|X|\varepsilon_k=\pm 1$ and hence $\varepsilon_k=0$, since $|X|=2^{r-h-1}\ge 2$, as $h\le r-2$. This finishes the proof of (4.8).

To finish the proof of the proposition it is enough to show that $\varepsilon_i\neq 0$ for exactly one $i\in\{1,\dots,2^{r-1}-1\}$. If i is even then $\varepsilon_i=0$, by (4.8) with $h=r-2$.

We claim that if $\varepsilon_i\neq 0$ then $i\equiv\pm 1 \bmod 2^{r-1}$. Otherwise, there are integers $2\le v\le r-2$ and $2<i<2^{r-1}-1$ satisfying $i\not\equiv\pm 1 \bmod 2^{v+1}$ and $\varepsilon_i\neq 0$. We choose v minimum with this property for some i. Then (1) $\varepsilon_k=0$ for every $k\not\equiv\pm 1 \bmod 2^v$ and (2) $i\equiv\pm(k+2^v) \bmod 2^{v+1}$ for every $k\in X_{r-v-1}$. (1) implies that $\sum_{k\in X_{r-v-1}}(\varepsilon_k+\varepsilon_{k+2^v})=1$. On the other hand $1\le r-v-1\le r-3$ and hence applying (4.6) and (4.7) with $h=r-v-1$ we deduce from (2) that $\varepsilon_i=\varepsilon_{k+2^v}$ for every $k\in X_{r-v-1}$ and $\sum_{k\in X_{r-v-1}}(\varepsilon_k-\varepsilon_{k+2^v})=\pm 1$. Using $|X_{r-v-1}|=2^{r-v-1}$ and $\varepsilon_i\neq 0$ we deduce that $2^{r-v}\varepsilon_i=2\sum_{k\in X_{r-v-1}}\varepsilon_{k+2^{r-v}}=2$, in contradiction with $2\le r-v$. This finishes the proof of the claim.

Then the only possible non-zero partial augmentations of u are ε_1 and $\varepsilon_{2^{r-1}-1}$. Hence $\varepsilon_1+\varepsilon_{2^{r-1}-1}=1$ and, by applying (4.6) with $h=0$ we deduce that $\varepsilon_1-\varepsilon_{2^{r-1}-1}=\pm 1$. Therefore, either $\varepsilon_1=0$ or $\varepsilon_{2^{r-1}-1}=0$, i.e. $\varepsilon_i\neq 0$ for exactly one $i\in\{1,\dots,2^{r-1}-1\}$, as desired. □

5. Proof of Theorem 1.1

In this section we prove Theorem 1.1. Recall that $G=\mathrm{SL}(2,q)$ with $q=t^f$ and t an odd prime number, $\overline{G}=\mathrm{PSL}(2,q)$, $\pi: G\to\overline{G}$ is the natural projection and u is an element of order n in $\mathrm{V}(\mathbb{Z}G)$ with $\gcd(n,q)=1$. We have to show that u is rationally conjugate to an element of G. By Proposition 3.1.(4), we may assume that n is multiple of 4 and by Proposition 4.1 that n is not a prime power. Moreover, we may also assume that $n\neq 12$ because this case follows easily from known results and the HeLP Method. Indeed, if $n=12$ then $\pi(u)$ has order 6, by Proposition 3.1.(2) and hence $\pi(u)$ is rationally conjugate to an element of $\overline{G}$, by [Her07, Proposition 6.6]. Using this and the fact that G has a unique conjugacy class for each of the orders 3, 4 or 6 and two conjugacy classes of elements of order 12, and applying (D) with $\chi=\chi_1$ and $\ell=1,5$ it easily follows that all the partial augmentations of u are non-negative. This can be also obtained using the GAP Package [BM17a].

In the remainder we follow the strategy of the proof of the main result of [MRS18]. The difference with the arguments of that paper is twofold: On the one hand, in our case n is even (actually multiple of 4) and this introduces some difficulties not appearing in [MRS18] where n was odd. On the other hand for $\mathrm{SL}(2,q)$ we have more Brauer characters than for $\mathrm{PSL}(2,q)$ and this will help to reduce some cases.

As the order n of u is fixed throughout, we simplify the notation of the Section 2 by setting

$$\gamma = \gamma_n, \quad \bar{\gamma} = \bar{\gamma}_n, \quad \alpha_x = \alpha_x^{(n)}, \quad \kappa_x = \kappa_x^{(n)}, \quad \beta_{b,x} = \beta_{b,x}^{(n)}, \quad \mathbb{B} = \mathbb{B}_n, \quad \mathcal{B} = \mathcal{B}_n.$$

We argue by induction on n. So we also assume that u^d is rationally conjugate to an element of G for every divisor d of n with $d \neq 1$.

We will use the representations Θ_m and t-Brauer characters χ_m introduced in (3.1). Observe that the kernel of Θ_m is trivial if m is odd, and otherwise it is the center of G. Using this and the induction hypothesis on n it easily follows that the order of $\Theta_m(u)$ is $\frac{n}{2}$ if m is even, while, if m is odd then the order of $\Theta_m(u)$ is n. Combining this with Proposition 3.1.(7) we deduce that $\Theta_1(u)$ is conjugate to $\mathrm{diag}(\zeta, \zeta^{-1})$ for a suitable primitive n-th root of unity ζ. Hence there exists an element $g_0 \in G$ of order n such that $\Theta_1(g_0)$ and $\Theta_1(u)$ are conjugate. The element $g_0 \in G$ and the primitive n-th root of unity ζ will be fixed throughout and from now on we abuse the notation and consider ζ both as a primitive n-th root of unity in a field of characteristic t and as a complex primitive n-th root of unity. Then

$$\Theta_m(g_0) \text{ is conjugate to } \begin{cases} \mathrm{diag}\left(1, \zeta^2, \zeta^{-2}, \ldots, \zeta^m, \zeta^{-m}\right), & \text{if } 2 \mid m; \\ \mathrm{diag}\left(\zeta, \zeta^{-1}, \zeta^3, \zeta^{-3}, \ldots, \zeta^m, \zeta^{-m}\right), & \text{if } 2 \nmid m; \end{cases}$$

and

$$\chi_m(g_0^i) = \sum_{\substack{j=-m \\ j \equiv m \bmod 2}}^{m} \zeta^{ij} = \begin{cases} 1 + \alpha_{2i} + \alpha_{4i} + \cdots + \alpha_{mi}, & \text{if } 2 \mid m; \\ \alpha_i + \alpha_{3i} + \cdots + \alpha_{mi}, & \text{if } 2 \nmid m. \end{cases} \tag{5.1}$$

By the induction hypothesis on n, if c is a divisor of n with $c \neq 1$ then u^c is rationally conjugate to g_0^i for some i and hence $\zeta^c = \zeta^{\pm i}$. Therefore $c \sim_n i$ and hence u^c is conjugate to g_0^c.

By (E), two elements of $\langle g_0 \rangle$ are conjugate in G if and only if they are equal or mutually inverse. Moreover, every element $g \in G$, with $g^n = 1$, is conjugate to an element of $\langle g_0 \rangle$. Therefore $x \mapsto (g_0^x)^G$ induces a bijection from Γ_n to the set of conjugacy classes of G formed by elements of order dividing n. For an integer x (or $x \in \Gamma_n$) we set

$$\varepsilon_x = \varepsilon_{g_0^x}(u) \quad \text{and} \quad \lambda_x = \sum_{i \in \Gamma_n} \varepsilon_i \alpha_{ix}.$$

Our main tool is the following lemma whose proof is exactly the same as the one of Lemma 4.1 in [MRS18]. We also collect Corollary 3.3 of this paper.

Lemma 5.1. *u is rationally conjugate to g_0 if and only if $\lambda_i = \alpha_i$, for any positive integer i.*

For a positive integer n and a subfield F of $\mathbb{Q}(\zeta_n)$, let Γ_F denote a set of representatives of equivalence classes of the following equivalence relation defined on $\mathbb{Z}$:

$$x \sim y \quad \text{if and only if} \quad \zeta_n^x \text{ and } \zeta_n^y \text{ are conjugate in } \mathbb{Q}(\zeta_n) \text{ over } F.$$

Corollary 5.2. *Let n be a positive integer, let F be a subfield of $\mathbb{Q}(\zeta_n)$ and let R be the ring of integers of F. For every $x \in \Gamma_F$ let B_x be an integer and for every integer i define*

$$\omega_i = \sum_{x \in \Gamma_F} B_x \, Tr_{\mathbb{Q}(\zeta_n)/F}(\zeta_n^{ix}).$$

Let d be a divisor of n such that $\omega_{\frac{d}{q}} = 0$ for every prime power q dividing d with $q \neq 1$. Then $\omega_d \in d\,R$.

By Lemma 5.1, in order to achieve our goal it is enough to prove that $\lambda_i = \alpha_i$ for every positive integer i. We argue by contradiction, so we assume that $\lambda_d \neq \alpha_d$ for some positive integer d which we assume to be minimal with this property. Observe that if $\lambda_i = \alpha_i$ and j is an integer such that $\gcd(i,n) = \gcd(j,n)$, then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ such that $\sigma(\alpha_i) = \alpha_j$ and applying σ to the equation $\lambda_i = \alpha_i$ we obtain $\lambda_j = \alpha_j$. This implies that d divides n. Note that $\alpha_1 = \lambda_1$, by our choice of g_0, and hence $d \neq 1$. Moreover, $d \neq n$ because $\lambda_n = 2\sum_{x\in\Gamma_n} \varepsilon_x = 2 = \alpha_n$ as the augmentation of u is 1.

We claim that

$$\lambda_d = \alpha_d + d\tau \text{ for some } \tau \in \mathbb{Z}[\alpha_1]. \tag{5.2}$$

Indeed, for any $x \in \Gamma_n$ let $B_x = \varepsilon_x - 1$ if $x \sim_n 1$ and $B_x = \varepsilon_x$ otherwise. Then for any integer i we have $\lambda_i - \alpha_i = \sum_{x\in\Gamma_n} B_x \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha_1)}\left(\zeta^{ix}\right)$. The claim then follows by applying Corollary 5.2 with $F = \mathbb{Q}(\alpha_1)$, $R = \mathbb{Z}[\alpha_1]$ and $\omega_i = \lambda_i - \alpha_i$. Observe that in the notation of that corollary $\Gamma_n = \Gamma_F$.

By (5.1) we have

$$\chi_d(g_0) = \sum_{\substack{i=0\\ i\equiv d \bmod 2}}^{d} \alpha_i \quad \text{and} \quad \chi_d(u) = \sum_{x\in\Gamma_n} \varepsilon_x \chi_d(g_0^x) = \sum_{x\in\Gamma_n} \varepsilon_x \sum_{\substack{i=0\\ i\equiv d \bmod 2}}^{d} \alpha_{ix} = \sum_{\substack{i=0\\ i\equiv d \bmod 2}}^{d} \lambda_i. \tag{5.3}$$

Combining this with (5.2) and the minimality of d, we deduce that $\chi_d(u) = \chi_d(g_0) + d\tau$. Furthermore, $\tau \neq 0$, as $\lambda_d \neq \alpha_d$. Therefore

$$C_b(\chi_d(u)) \equiv C_b(\chi_d(g_0)) \bmod d \quad \text{for every } b \in \mathbb{B} \tag{5.4}$$

and

$$d \leq |C_{b_0}(\chi_d(u)) - C_{b_0}(\chi_d(g_0))| \quad \text{for some } b_0 \in \mathbb{B}. \tag{5.5}$$

The bulk of our argument relies on an analysis of the eigenvalues of $\Theta_d(u)$ and the induction hypothesis on n and d. More precisely, we will use (5.4) and (5.5) to obtain a contradiction by comparing the eigenvalues of $\Theta_d(g_0)$ and $\Theta_d(u)$. Of course, we do not know the eigenvalues of the latter. However we know the eigenvalues of $\Theta_d(u^c)$ for every $c \mid n$ with $c \neq 1$, because we know the eigenvalues of $\Theta_d(g_0)$ and u^c is conjugate to g_0^c. This provides information on the eigenvalues of $\Theta_d(u)$. For example, recall that if ξ is an eigenvalue of $\Theta_d(u)$ then ξ and ξ^{-1} have the same multiplicity as eigenvalues of $\Theta_d(u)$. Therefore, if $3 \leq h$ then the sum of the multiplicities of the eigenvalues of $\Theta_d(u)$ of order h is even. Moreover, for every t-regular element g of G, the multiplicity of 1 as eigenvalue of $\Theta_d(g)$ is congruent modulo 2 with the degree $d+1$ of χ_d. As n is not a prime power there is an odd prime p dividing n. By the induction hypothesis $\Theta_d(u^p)$ is rationally conjugate to $\Theta_d(g_0^p)$. Thus the multiplicity of -1 as eigenvalue of $\Theta_d(u^p)$ is even. As the latter is the sum of the multiplicities as eigenvalues of $\Theta_d(u)$ of -1 and the elements of order $2p$, we deduce that the multiplicity of -1 as eigenvalue of $\Theta_d(u)$ is even. Using this we can see that $\Theta_d(u)$ is conjugate to $\mathrm{diag}(\zeta^{\nu_{-d}}, \zeta^{\nu_{2-d}}, \ldots, \zeta^{\nu_{d-2}}, \zeta^{\nu_d})$ for integers $\nu_{-d}, \nu_{-d+2}, \ldots, \nu_{d-2}, \nu_d$ such that $\nu_{-i} = -\nu_i$ for every i. Let $X_d = \{i : 1 \leq i \leq d, i \equiv d \bmod 2\}$. Then, by (5.3) and Proposition 2.2, we have for every $b \in \mathbb{B}$ that

$$C_b(\chi_d(u)) - C_b(\chi_d(g_0)) = \sum_{i\in X_d} \left(\kappa_{\nu_i} \cdot \beta_{b,\nu_i} \cdot \mu(\gamma(\nu_i)) \cdot \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} - \kappa_i \cdot \beta_{b,i} \cdot \mu(\gamma(i)) \cdot \delta_{b,i}^{(n/\bar{\gamma}(i))}\right).$$

Moreover, if $c \mid n$ with $c \neq 1$ then the lists $(c\nu_i)_{i\in X_d}$ and $(ci)_{i\in X_d}$ represent the same elements in Γ_n, up to ordering, and hence $(\nu_i)_{i\in X_d}$ and $(i)_{i\in X_d}$ represent the same elements of $\Gamma_{\frac{n}{c}}$, up to ordering. We express this by writing $(\nu(X_d)) \sim_{\frac{n}{c}} (X_d)$. This provides restrictions on d, n and the ν_i.

The following two lemmas are variants of Lemmas 4.2 and 4.3 of [MRS18].

Lemma 5.3. *(1) Let $i \in X_d$. If $\kappa_i \neq 1$ then $n = 2d$ and $i = d$. If $\kappa_{\nu_i} \neq 1$ then $\frac{n}{d}$ is the smallest prime dividing n and $\kappa_{\nu_j} = 1$ for every $j \in X_d \setminus \{i\}$.*

(2) If $d > 2$ then n is not divisible by any prime greater than d. In particular, if d is prime then $\kappa_{\nu_i} = 1$ for every $i \in X_d$.

Proof. Let p denote the smallest prime dividing n.

(1) The first statement is clear. Suppose that $\kappa_{\nu_i} \neq 1$. Then either $p = 2$ and $\nu_i \equiv 0 \bmod \frac{n}{2}$ or $\nu_i \equiv 0 \bmod n$. As $(X_d) \sim_{\frac{n}{p}} (\nu(X_d))$ we deduce that $k \equiv 0 \bmod \frac{n}{p}$ for some $k \in X_d$. Therefore $d = k = \frac{n}{p}$ and for every $j \in X_d \setminus \{i\}$ we have $\nu_j \not\equiv 0 \bmod \frac{n}{p}$. Thus $\kappa_{\nu_j} = 1$.

(2) Suppose that q is a prime divisor of n with $d < q$. Then $\frac{n}{d} \neq p$ and therefore, by (1), $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_d$. Thus, by (5.5) and (5.6), it is enough to show that $\delta_{b,i}^{(n/\bar{\gamma}(i))} \neq 0$ for at most one $i \in X_d$ and $\delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} \neq 0$ for at most one $i \in X_d$. Observe that if $i \in X_d$ then $q \nmid i$ and hence $\frac{n}{\bar{\gamma}(i)}$ is multiple of q. Moreover, if i and j are different elements of X_d then i and j have the same parity and $-q < i - j < i + j < 2q$. Therefore $i \not\sim_q j$. Thus either $\delta_{b,i}^{\frac{n}{\bar{\gamma}(i)}} = 0$ or $\delta_{b,j}^{\frac{n}{\bar{\gamma}(j)}} = 0$. As $(X_d) \sim_q (\nu(X_d))$, this also proves that $\delta_{b,\nu_i}^{\frac{n}{\bar{\gamma}(\nu_i)}} = 0$ or $\delta_{b,\nu_j}^{\frac{n}{\bar{\gamma}(\nu_j)}} = 0$. □

We obtain an upper bound for $|C_b(\chi_d(u)) - C_b(\chi_d(g_0))|$ in terms of the number of prime divisors $P(d)$ of d.

Lemma 5.4. *For every $b \in \mathbb{B}$ we have $|C_b(\chi_d(u)) - C_b(\chi_d(g_0))| \leq 2 + 2^{P(d)+1}$.*

Proof. Using (5.6) it is enough to prove that $\sum_{i \in X_d} \kappa_i \delta_{b,i}^{(n/\bar{\gamma}(i))} \leq 1 + 2^{P(d)}$ and $\sum_{i \in X_d} \kappa_{\nu_i} \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} \leq 1 + 2^{P(d)}$. This is a consequence of Lemma 5.3.(1) and the following inequalities for every e dividing d':

$$\left|\left\{i \in X_d : \gcd(d, \bar{\gamma}(i)) = e, \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1, \quad \left|\left\{i \in X_d : \gcd(d, \bar{\gamma}(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 1.$$

We prove the second inequality, only using that $(\nu(X_d)) \sim_d (X_d)$. This implies the first inequality by applying the second one to $u = g_0$.

Let $Y_e = \left\{i \in X_d : \gcd(d, \bar{\gamma}(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}$. By changing the sign of some ν_i's, we may assume without loss of generality that if $\delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1$ then $b \equiv \nu_i \bmod \frac{n}{\bar{\gamma}(\nu_i)}$. Thus, if $i \in Y_e$ then $b \equiv \nu_i \bmod \frac{n}{\bar{\gamma}(\nu_i)}$. We claim that if $i, j \in Y_e$ then $\nu_i \equiv \nu_j \bmod d$. Indeed, let p be prime divisor of d. If $n_p \neq d_p$ or $p \nmid e$ then clearly $\nu_i \equiv \nu_j \bmod d_p$. Otherwise, i.e. $n_p = d_p$ and $p \mid e$, then p divides both $\bar{\gamma}(\nu_i)$ and $\bar{\gamma}(\nu_j)$ and $\nu_i \equiv \nu_j \bmod \frac{d_p}{p}$. Therefore, by Lemma 2.1.(2), $\nu_i \equiv \nu_j \bmod n_p$, as desired. As $(\nu(X_d)) \sim_d (X_d)$ and the elements of X_d represent different classes in Γ_d we deduce that $|Y_e| \leq 1$. This finishes the proof of the lemma. □

We are ready to finish the proof of Theorem 1.1. Recall that we are arguing by contradiction.

By (5.5) and Lemma 5.4 we have $d \leq 2 + 2^{P(d)+1}$ and, using this, it is easy to show that $d \leq 6$ or $d = 10$. Indeed, if $P(d) \geq 3$ then $2 + 2^{P(d)+1} \geq d \geq 2 \cdot 3 \cdot 5 \cdot 2^{P(d)-3} > 14 + 2^{P(d)+1}$, a contradiction. Thus $P(d) = 2$ and $d \leq 10$ or $P(d) = 1$ and $d \leq 5$. Hence d is either $2, 3, 4, 5, 6$ or 10. We deal with these cases separately.

<u>Suppose that $d = 2$.</u> Then $\nu_2 \sim_{n_p} 2$ for every prime p. By the assumptions on n and Lemma 5.3.(1), this implies that $\kappa_2 = \kappa_{\nu_2} = 1$, $\gamma(2) = \gamma(\nu_2)$ and $\beta_{b_0,2} = \beta_{b_0,\nu_2}$. Therefore $|C_{b_0}(\chi_2(u)) - C_{b_0}(\chi_2(g_0))| = \left|\mu(\gamma(2)) \left(\delta_{b_0,2}^{(n/\bar{\gamma}(2))} - \delta_{b_0,\nu_2}^{(n/\bar{\gamma}(\nu_2))}\right)\right| \leq 1$, contradicting (5.5).

<u>Suppose that $d = 3$.</u> By Lemma 5.3 and the assumptions on n, we have $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_3$ and $n' = 6$. If $2^4 \mid n$ or $3^2 \mid n$ then $\left|\left\{i = 1, 3 : \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1$ and $\left|\left\{i = 1, 3 : \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 1$, which implies $|C_{b_0}(\chi_3(u)) - C_{b_0}(\chi_3(g_0))| \leq 2$, contradicting (5.5). Thus $n = 24$, since n is neither 12 nor a prime power and it is multiple of 4. In this case we have $\bar{\gamma}(1) = \gamma(1) = 2$, $\bar{\gamma}(3) = \gamma(3) = 3$, $\beta_{b,1} = \beta_{b,3} = 1$ and $C_b(\chi_3(g_0)) = -\delta_{b,1}^{(12)} - \delta_{b,3}^{(8)}$ for every $b \in \mathbb{B}$. We may assume that $3 \mid \nu_3$ and $3 \nmid \nu_1$ because $(\nu(X_3)) \sim_3 (X_3)$. Suppose that $\nu_3 \sim_8 3$ and $\nu_1 \sim_8 1$. Then $\bar{\gamma}(\nu_1) = \gamma(\nu_1) = 2$, $\bar{\gamma}(\nu_3) = \gamma(\nu_3) = 3$, $\beta_{b_0,\nu_3} = 1$ and $\delta_{b_0,3}^{(8)} = \delta_{b_0,\nu_3}^{(8)}$, which implies $|C_{b_0}(\chi_3(u)) - C_{b_0}(\chi_3(g_0))| \leq 2$, contradicting (5.5). Suppose now that $\nu_3 \sim_8 1$ and $\nu_1 \sim_8 3$. This implies that $\nu_1 \equiv \pm 3 \bmod 8$ and $\nu_1 \equiv \pm 1 \bmod 3$ (because $3 \mid \nu_3$ but $3 \nmid \nu_1$). Thus either $\nu_1 \equiv \pm 11 \bmod 24$ or

$\nu_1 \equiv \pm 5 \bmod 24$. As $(\nu(X_3)) \sim_{12} (X_3)$, we deduce that the only possibility is $\nu_1 \equiv \pm 11 \bmod 24$. In this case we have $\bar{\gamma}(\nu_1) = \gamma(\nu_1) = 1$ and $\bar{\gamma}(\nu_3) = \gamma(\nu_3) = 6$. Hence $C_{11}(\chi_3(u)) - C_{11}(\chi_3(g_0)) = \delta^{(24)}_{11,\nu_1} + \delta^{(4)}_{11,\nu_3} + \delta^{(12)}_{11,1} + \delta^{(8)}_{11,3} = 4$, contradicting (5.4).

Suppose that $d = 4$. By Lemma 5.3 and the assumptions on n, we have $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_4$ and $n' = 6$. If $3^3 \mid n$ or $2^3 \mid n$ then $\left|\left\{i = 2, 4 : \delta^{(n/\bar{\gamma}(i))}_{b,i} = 1\right\}\right| \leq 1$ which implies $|C_{b_0}(\chi_4(u)) - C_{b_0}(\chi_4(g_0))| \leq 3$, contradicting (5.5). Thus $n = 36$. In this case we have $\gamma(2) = 1 = \beta_{b_0,2} = \beta_{b_0,4}$ and $\gamma(4) = 2$, which implies $|C_{b_0}(\chi_4(g_0))| \leq 1$ and hence $|C_{b_0}(\chi_4(u)) - C_{b_0}(\chi_4(g_0))| \leq 3$, contradicting again (5.5).

Suppose that $d = 5$. Since $(\nu(X_5)) \sim_5 (X_5)$, there is exactly one ν_i which is divisible by 5, say ν_5. In particular, for $i \neq 5$ we have $5 \mid \frac{n}{\bar{\gamma}(\nu_i)}$ and $5 \mid \frac{n}{\bar{\gamma}(i)}$. Moreover, if j is an integer not multiple of 5 then $|\{i = 1, 3 : \nu_i \sim_5 j\}| \leq 1$. This implies that $\left|\left\{i = 1, 3 : \delta^{(n/\bar{\gamma}(i))}_{b,i} = 1\right\}\right| \leq 1$ and $\left|\left\{i = 1, 3 : \delta^{(n/\bar{\gamma}(\nu_i))}_{b,\nu_i} = 1\right\}\right| \leq 1$. On the other hand, as $n \neq 10$, we deduce that $\kappa_i = 1$ for every $i \in X_5$, by Lemma 5.3.(1). Therefore, using (5.5) and (5.6), we deduce that $\kappa_{\nu_5} = 2$, in contradiction with Lemma 5.3.(1).

Suppose that $d = 6$. By Lemma 5.3, we have $n' \mid 30$ and $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_6$ because $n \neq 12$. If $25 \mid n$, or $9 \mid n$ or $8 \mid n$ then we have $\left|\left\{i = 2, 4, 6 : \delta^{(n/\bar{\gamma}(i))}_{b,i} = 1\right\}\right| \leq 2$ and $\left|\left\{i = 2, 4, 6 : \delta^{(n/\bar{\gamma}(\nu_i))}_{b,\nu_i} = 1\right\}\right| \leq 2$. This implies that $|C_{b_0}(\chi_6(u)) - C_{b_0}(\chi_6(g_0))| \leq 4$, yielding a contradiction with (5.5). Therefore $n = 60$ and hence $\beta_{b,2} = \beta_{b,4} = \beta_{b,6} = 1$, $\bar{\gamma}(2) = 1$, $\bar{\gamma}(4) = \gamma(4) = 2$ and $\bar{\gamma}(6) = \gamma(6) = 3$. This implies that $|C_{b_0}(\chi_6(g_0))| \leq 2$ and hence $|C_{b_0}(\chi_6(u)) - C_{b_0}(\chi_6(g_0))| \leq 5$, yielding a contradiction with (5.5).

Suppose that $d = 10$. If $5 \nmid \frac{n}{\bar{\gamma}(i)}$ for some $i \in X_{10}$ then $n_5 = (\bar{\gamma}(i))_5 = 5$ and hence $5 \mid i$. The same also holds for ν_i. Therefore, if $5 \nmid i$ then $5 \mid \frac{n}{\bar{\gamma}(i)}$ and if $5 \nmid \nu_i$ then $5 \mid \frac{n}{\bar{\gamma}(\nu_i)}$. Thus $\left|\left\{i \in X_{10} : 5 \nmid i, \delta^{(n/\bar{\gamma}(i))}_{b,i} = 1\right\}\right| \leq 2$ and $\left|\left\{i \in X_{10} : 5 \nmid \nu_i, \delta^{(n/\bar{\gamma}(\nu_i))}_{b,\nu_i} = 1\right\}\right| \leq 2$. This implies that $|C_{b_0}(\chi_{10}(u)) - C_{b_0}(\chi_{10}(g_0))| \leq 8$, contradicting (5.5).

References

[BH08] V. A. Bovdi and M. Hertweck. Zassenhaus conjecture for central extensions of S_5. *J. Group Theory*, 11(1):63–74, 2008.

[BKL08] V. A. Bovdi, A. B. Konovalov, and S. Linton. Torsion units in integral group ring of the Mathieu simple group M_{22}. *LMS J. Comput. Math.*, 11:28–39, 2008.

[BM17a] A. Bächle and L. Margolis. HeLP – Hertweck-Luthar-Passi method, GAP package, Version 3.3. http://homepages.vub.ac.be/abachle/help/, 2017.

[BM17b] A. Bächle and L. Margolis. On the prime graph question for integral group rings of 4-primary groups I. *Internat. J. Algebra Comput.*, 27(6):731–767, 2017.

[BM17c] A. Bächle and L. Margolis. Rational conjugacy of torsion units in integral group rings of non-solvable groups. *Proc. Edinb. Math. Soc. (2)*, 60(4):813–830, 2017.

[BM18] A. Bächle and L. Margolis. On the Prime Graph Question for Integral Group Rings of 4-Primary Groups II. *L. Algebra Representation Theory*, 2018. https://doi.org/10.1007/s10468-018-9776-6.

[CMR13] M. Caicedo, L. Margolis, and Á. del Río. Zassenhaus conjecture for cyclic-by-abelian groups. *J. Lond. Math. Soc. (2)*, 88(1):65–78, 2013.

[DJPM97] M. Dokuchaev, S. O. Juriaans, and C. Polcino Milies. Integral group rings of Frobenius groups and the conjectures of H. J. Zassenhaus. *Comm. Algebra*, 25(7):2311–2325, 1997.

[Dor71] L. Dornhoff. *Group representation theory. Part A: Ordinary representation theory.* Marcel Dekker, Inc., New York, 1971. Pure and Applied Mathematics, 7.

[EM18] F. Eisele and L. Margolis. A counterexample to the first Zassenhaus conjecture. *Adv. Math.*, 339:599–641, 2018.

[Her06] M. Hertweck. On the torsion units of some integral group rings. *Algebra Colloq.*, 13(2):329–348, 2006.

[Her07] M. Hertweck. Partial augmentations and Brauer character values of torsion units in group rings. 2007. arXiv:math/0612429 [math.RA].

[Her08] M. Hertweck. Zassenhaus conjecture for A_6. *Proc. Indian Acad. Sci. Math. Sci.*, 118(2):189–195, 2008.

[JR16] E. Jespers and Á. del Río. *Group ring groups. Volume 1: Orders and generic constructions of units.* Berlin: De Gruyter, 2016.

[LP89] I. S. Luthar and I. B. S. Passi. Zassenhaus conjecture for A_5. *Proc. Indian Acad. Sci. Math. Sci.*, 99(1):1–5, 1989.

[Mar16] L. Margolis. A Sylow theorem for the integral group ring of $\mathrm{PSL}(2, q)$. *J. Algebra*, 445:295–306, 2016.

[Mar17] L Margolis. A Theorem of Hertweck on p-adic conjugacy. *https://arxiv.org/abs/1706.02117*, 2017.

[MRS18] L. Margolis, Á. del Río, and M. Serrano. Zassenhaus conjecture on torsion units holds for PSL(2,p) with p a Fermat or Mersenne prime. *https://arxiv.org/abs/1608.05797*, 2018.

[MRSW87] Z. Marciniak, J. Ritter, S. K. Sehgal, and A. Weiss. Torsion units in integral group rings of some metabelian groups II. *J. Number Theory*, 25(3):340–352, 1987.

[RS17] Á. del Río and M. Serrano. On the torsion units of the integral group ring of finite projective special linear groups. *Communications in Algebra*, 45(2):5073–5087, 2017.

[Seh93] S. K. Sehgal. *Units in integral group rings*, volume 69 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[Wei91] A. Weiss. Torsion units in integral group rings. *J. Reine Angew. Math.*, 415:175–187, 1991.

[Zas74] H. J. Zassenhaus. On the torsion units of finite group rings. In *Studies in mathematics (in honor of A. Almeida Costa) (Portuguese)*, pages 119–126. Instituto de Alta Cultura, Lisbon, 1974.

Email address: `adelrio@um.es`

Email address: `mariano.serrano@um.es`

Department of Mathematics, University of Murcia.