TORSION SUBGROUPS IN THE UNITS OF THE INTEGRAL GROUP RING OF PSL(2, p^3)

ANDREAS BÄCHLE AND LEO MARGOLIS

Abstract. We show that for every prime \( r \) all \( r \)-subgroups in the normalized units of the integral group ring of \( \text{PSL}(2, p^3) \) are isomorphic to subgroups of \( \text{PSL}(2, p^3) \). This answers a question of M. Hertweck, C.R. Höft and W. Kimmerle for this series of groups.

Let \( G \) be a finite group and \( ZG \) its integral group ring. A natural question is how far the structure of \( G \) is reflected in the structure of the torsion part of \( V(ZG) \), the group of normalized units of the integral group ring of \( G \), and vice versa. One of the first questions studied in this context is, whether a finite subgroup of \( V(ZG) \) is necessarily isomorphic to a subgroup of \( G \), which was already raised in G. Higman’s PhD thesis [Hig40, Section 5] (cf. also the article [San81] outlining this thesis). It was later explicitly stated as a problem in [San85, Problem 5.4].

A first step towards an answer to the above question lies in the consideration of \( p \)-subgroups. It is known that if \( G \) has cyclic Sylow \( p \)-subgroups then all \( p \)-subgroups of \( V(ZG) \) are cyclic; for \( p = 2 \) see [Kim07, Proposition] (the proof involves the Brauer-Suzuki theorem) and cf. [Her08, Corollary 1] for odd primes \( p \). If the Sylow 2-subgroups of \( G \) are elementary abelian, then so are all 2-subgroups of \( V(ZG) \) and in particular they are isomorphic to subgroups of \( G \) (combining [CL65, Corollary 4.1] and [Sak71, Corollary 1.7], cf. also [Seh93, Lemma (37.3)]). But it is not even known in general whether abelian Sylow \( p \)-subgroups of \( G \) cause that the \( p \)-subgroups of \( V(ZG) \) are abelian. However, this assertion holds for solvable \( G \) [DJ96, Proposition 2.11].

In the concluding remarks of [HHK09] the question whether the \( p \)-subgroups of \( V(Z \text{PSL}(2, p^f)) \) are (elementary) abelian is highlighted. For \( p = 2 \) or \( f \leq 2 \) there is an even stronger assertion, recently proved by the second author [Mar14]: for all primes \( r \) the \( r \)-subgroups of \( V(Z \text{PSL}(2, p^f)) \) are conjugate by a unit of the corresponding rational group algebra to a subgroup of the group base \( \text{PSL}(2, p^f) \). It is also known that any subgroup of \( V(Z \text{PSL}(2, p^f)) \) of the same order as \( \text{PSL}(2, p^f) \) is conjugate in the rational group algebra to the group base \( \text{PSL}(2, p^f) \) [Ble95, Propositions 3.2 and 4.1].

In this article we prove that for all primes \( p \) the \( p \)-subgroups of the group \( V(Z \text{PSL}(2, p^3)) \) are abelian. We obtain the following result:

Theorem. Let \( p \) be a prime and set \( G = \text{PSL}(2, p^3) \). Then for all primes \( r \), the \( r \)-subgroups of \( V(ZG) \) are isomorphic to subgroups of \( G \).

The method of choice here is what one could call a “non-cyclic HeLP-method”. For a finite group \( G \) consider a finite subgroup \( U \) of \( V(ZG) \). Every ordinary representation of \( G \) can be linearly extended to a representation of \( ZG \) and then restricted to a representation \( D \) of \( V(ZG) \). Let its character be denoted by \( \chi \). If \( \psi \) is a character of \( U \), then for the inner product we necessarily have

\[
\langle \chi|_U, \psi \rangle_U \in \mathbb{Z}_{\geq 0}.
\]

For cyclic \( U \) this can be expressed in an explicit formula, whose application is known as the HeLP-method, cf. [LP89, Theorem 1] and [Her07, Section 4]. The method for non-cyclic \( U \) was used for the first time in the PhD-thesis of C.R. Höft [Höf08, page 58] and later in [Her08] and [HHK09, page 2].
We will introduce some notation. Let \( u = \sum_{g \in G} z_g g \in \mathbb{Z}G \) be a normalized torsion unit. For \( x^G \), the conjugacy class of the element \( x \in G \) in \( G \), we denote by
\[
\varepsilon_x(u) = \sum_{g \in x^G} z_g
\]
the partial augmentation of \( u \) at \( x \). The partial augmentations will provide us with restrictions on the possible eigenvalues of \( D(u) \) and vice versa. By the so-called Berman-Higman Theorem \( \varepsilon_1(u) = 0 \) if \( u \neq 1 \) [Hig40, Theorem 10], [Ber55, Lemma 2] (cf. also [Seh93, Proposition (1.4)]). Also \( \varepsilon_x(u) = 0 \) if the order of \( x \) does not divide the order of \( u \) [Her07, Proposition 2.2]. Moreover, the order of a finite subgroup of \( V(ZG) \) divides the order of \( G \) [Sak71, Corollary 1.7], cf. also [Seh93, Lemma (37.3)], and its exponent divides the exponent of \( G \) [CL65, Corollary 4.1]. We will use these facts in the sequel without further mention.

Let \( A \) be a complex matrix of finite order. Assume that \( A \) has eigenvalues \( \alpha_1, ..., \alpha_j \) each with multiplicity \( m_1 \), eigenvalues \( \beta_1, ..., \beta_k \) each with multiplicity \( m_2 \) and eigenvalues \( \gamma_1, ..., \gamma_\ell \) each with multiplicity \( m_3 \), then we indicate this by
\[
A \sim \left( m_1 \times \alpha_1, ..., \alpha_j \right) \times \left( m_2 \times \beta_1, ..., \beta_k \right) \times \left( m_3 \times \gamma_1, ..., \gamma_\ell \right).
\]

**Proof of the theorem.**

Set \( G = \text{PSL}(2, p^3) \). By a result of Dickson [Dic58, 260.] (see also [Hup67, 8.27 Hauptsatz]), the Sylow \( r \)-subgroups of the simple groups \( \text{PSL}(2, p^l) \) are elementary abelian for \( r = p \), cyclic for odd \( r \neq p \), and dihedral groups if \( r = 2 \neq p \). By the results cited above we obtain that the \( r \)-subgroups of \( V(ZG) \) are isomorphic to subgroups of \( G \), provided the Sylow \( r \)-subgroups are cyclic. The case of elementary abelian Sylow 2-subgroups is also handled by the remarks in the introduction. If the Sylow 2-subgroups are dihedral, the result is obtained in [HHK09, Theorem 2.1]. It remains the case \( r = p \geq 3 \). Note that in this case the Sylow \( p \)-subgroups of \( G \) are elementary abelian of order \( p^2 \).

Let \( H \) be a finite \( p \)-subgroup of \( V(ZG) \). Hence \( |H| \leq p^3 \) and \( \exp H \mid p \). Assume that \( H \) is not isomorphic to a subgroup of \( G \), then, by the classification of all \( p \)-groups up to order \( p^4 \), it is a so-called Heisenberg group. Thus there are elements \( z, b, c \in H \) such that
\[
H = \langle z, b, c \mid z^p = b^p = c^p = 1, z \in \mathbb{Z}(H), \; c^{-1}bc = zb \rangle \cong (C_p \times C_p) \times C_p. \tag{1}
\]

We will use the non-cyclic HeLP-method to show that \( H \) does not exist. In \( G \) there are exactly two conjugacy classes of elements of order \( p \), let \( g \) and \( h \) be representatives of these classes. In Table 1 we list two irreducible characters [Dor71, Theorem 38.1], one of them we will use in the remainder of the proof. Let \( \epsilon \in \{1, -1\} \) such that \( p \equiv \epsilon \mod 4 \).

| \( \eta \) | \( \eta^p \) | \( \epsilon + \sqrt{\epsilon p^3} \) | \( \epsilon - \sqrt{\epsilon p^3} \) |
| --- | --- | --- | --- |
| \( \eta^p \) | \( \eta^p \) | \( \epsilon - \sqrt{\epsilon p^3} \) | \( \epsilon + \sqrt{\epsilon p^3} \) |

**Table 1.** Part of the character table of \( G = \text{PSL}(2, p^3) \), \( p \geq 3 \), \( \epsilon \in \{1, -1\} \) such that \( p \equiv \epsilon \mod 4 \).

Let \( \zeta = \exp (2\pi i /p) \in \mathbb{C} \), a primitive \( p \)-th root of unity, \( Q \) be a set of integral representatives of the quadratic residues in \((\mathbb{Z}/p\mathbb{Z})^\times\) and \( N \) be a set of integral representatives of the non-quadratic residues in \((\mathbb{Z}/p\mathbb{Z})^\times\). We will also use the Gaussian sums cf. [Gau11] (also [Neu99, Proof of (8.6) in Chapter I])
\[
\sqrt{\epsilon p} = 1 + 2 \sum_{q \in Q} \zeta^q, \tag{2}
\]
\[
-\sqrt{\epsilon p} = 1 + 2 \sum_{n \in N} \zeta^n.
\]
Let $D$ be a representation affording $\eta$. Let $u \in H \setminus \{1\}$ and $\alpha \in \mathbb{Z}_{>0}$ such that $(\varepsilon_g(u), \varepsilon_h(u)) = (\alpha + 1, -\alpha)$ or $(\varepsilon_g(u), \varepsilon_h(u)) = (-\alpha, \alpha + 1)$. By slight abuse of notation we denote from here on by $\eta$ also the restriction $\eta|_H$. For the first possibility of the partial augmentations of $u$ we obtain, using the first equation of (2),

$$\eta(u) = (\alpha + 1) \left( \frac{\epsilon + \sqrt{\epsilon p^3}}{2} \right) + (-\alpha) \left( \frac{\epsilon - \sqrt{\epsilon p^3}}{2} \right)$$

$$= \frac{1}{2} (\epsilon + (2\alpha + 1)p\sqrt{\epsilon})$$

$$= \frac{p + \epsilon}{2} + \alpha p + (2\alpha + 1)p \sum_{q \in Q} \zeta^q. \quad (3)$$

For the second possibility for the partial augmentations of $u$ we get, using the second equation of (2),

$$\eta(u) = \frac{p + \epsilon}{2} + \alpha p + (2\alpha + 1)p \sum_{n \in N} \zeta^n. \quad (4)$$

From the character value we get $\frac{p + \epsilon}{2} + \alpha p + (2\alpha + 1)p$ eigenvalues of $D(u)$. The other eigenvalues have to sum up to 0, hence there are

$$\frac{1}{p} \left( \frac{p^3 + \epsilon}{2} - \left( \frac{p + \epsilon}{2} + \alpha p + \left( \frac{p - 1}{2} \right)(2\alpha + 1)p \right) \right)$$

$$= \frac{1}{2p} \left( p^3 + \epsilon - p - \epsilon - 2\alpha p - (p - 1)(2\alpha + 1)p \right)$$

$$= \frac{p^2 - p}{2} - \alpha p$$

blocks having eigenvalues $1, \zeta, \zeta^2, ..., \zeta^{p - 1}$. Thus in the case of $\varepsilon_g(u) > 0$ we have

$$D(u) \sim \left( \frac{p + \epsilon}{2} + \alpha p \times (2\alpha + 1)p \right) \times \prod_{n \in N} \left( \frac{p^2 - p}{2} - \alpha p \times 1, \zeta, ..., \zeta^{p - 1} \right)$$

where $Q = \{ q_1, ..., q_{p - 1} \}$. In the other case, $\varepsilon_g(u) \leq 0$, we get

$$D(u) \sim \left( \frac{p + \epsilon}{2} + \alpha p \times (2\alpha + 1)p \times \prod_{n \in N} \left( \frac{p^2 - p}{2} - \alpha p \times 1, \zeta, ..., \zeta^{p - 1} \right) \right) \times \prod_{n \in N} \left( \frac{p^2 - p}{2} - \alpha p \times 1, \zeta, ..., \zeta^{p - 1} \right)$$

with $N = \{ n_1, ..., n_{p - 1} \}$.

The group $H$ is an extra-special $p$-group, its character theory is well-known, see e.g. [Dor71, Theorem 31.5]. $H$ has exactly $p - 1$ non-linear irreducible characters which are all of degree $p$. They all vanish on the non-central elements of $H$ and take the values $p\zeta^j$ for $1 \leq j \leq p - 1$ on the non-trivial central elements. Moreover $H$ posses $p^2$ linear characters corresponding to the quotient $H/\mathbb{Z}(H) = H/H' \simeq C_p \times C_p$. In particular, they have value 1 on all central elements of $H$. See table 2. Now we decompose $\eta = \eta|_H$ into the irreducible characters of $H$.

Let $v \in \mathbb{Z}(H) \setminus \{1\}$. To obtain the multiplicity of the eigenvalue 1 of $D(v)$ as calculated above, we must sum up exactly

$$\frac{p + \epsilon}{2} + \alpha p + \frac{p^2 - p}{2} - \alpha p = \frac{p^2 + \epsilon}{2}$$

linear characters of $H$ and hence

$$\frac{1}{p} \left( \frac{p^3 + \epsilon}{2} - \frac{p^2 + \epsilon}{2} \right) = \frac{p^2 - p}{2}$$

irreducible non-linear character of $H$.

Now let $w \in H$ be a non-central element. Since every irreducible non-linear character of $H$ vanishes on $w$, the character value $\eta(w)$ is the sum of exactly $\frac{p^2 + \epsilon}{2}$ roots of unity. Thus from (3)
groups. In every such cyclic subgroup \( p \) direct consequences of the Gaussian sums in (4 and (5) we obtain that \((\varepsilon_{\varphi}(w), \varepsilon_{\psi}(w)) = (1, 0)\) or \((\varepsilon_{\varphi}(w), \varepsilon_{\psi}(w)) = (0, 1)\). Furthermore, from the eigenvalues of \( D(u) \) calculated in these equations, we get

\[
(\varepsilon_{\varphi}(w), \varepsilon_{\psi}(w)) = (1, 0) \iff (\varepsilon_{\varphi}(u^n), \varepsilon_{\psi}(u^n)) = (0, 1) \quad \forall n \in N.
\]

Now we compute the inner product \( \langle \eta, \chi \rangle_H \) of \( \eta \) with a non-trivial linear character \( \chi \) of \( H \). We split up the computation of the contributions of different parts of \( H \) and omit the global factor \( 1/|H| = 1/p^3 \) until adding all contributions. The contribution of the identity element is

\[
\eta(1)\chi(1) = \frac{p^3 + \epsilon}{2}.
\]

There are \( p - 1 \) more elements in the center of \( H \). On \( \eta \) half of them takes the value \( \frac{p+1}{2} + \alpha p + (2 \alpha + 1)p \sum_{\zeta \in Q} \zeta^q \), the other half the value \( \frac{p+1}{2} + \alpha p + (2 \alpha + 1)p \sum_{n \in N} \zeta^n \). Since they all lie in the kernel of \( \chi \) the contribution to the inner product is

\[
\frac{p-1}{2} \left( \frac{p+\epsilon}{2} + \alpha p + (2 \alpha + 1)p \sum_{q \in Q} \zeta^q \right) + \frac{p-1}{2} \left( \frac{p+\epsilon}{2} + \alpha p + (2 \alpha + 1)p \sum_{n \in N} \zeta^n \right)
\]

\[
= \frac{p-1}{2} \left( p + \epsilon + 2 \alpha p - (2 \alpha + 1)p \right)
\]

\[
= \epsilon \cdot \frac{p-1}{2}.
\]

The kernel of \( \chi \) contains another conjugacy class of cyclic subgroups consisting of exactly \( p \) subgroups. In every such cyclic subgroup \( \frac{p-1}{2} \) of the elements take the value \( \frac{p+1}{2} + p \sum_{\zeta \in Q} \zeta^q \) on \( \eta \) and \( \frac{p-1}{2} \) of the elements take the value \( \frac{p+1}{2} + p \sum_{n \in N} \zeta^n \) on \( \eta \). The same computation as above gives the contribution

\[
p \epsilon \cdot \frac{p-1}{2}.
\]

To calculate the contributions of the other elements we need the following formulas which are direct consequences of the Gaussian sums in (2):

\[
\left( \sum_{q \in Q} \zeta^q \right) \left( \sum_{i \in \mathbb{Z}} \zeta^i \right) + \left( \sum_{n \in N} \zeta^n \right) \left( \sum_{j \in \mathbb{Z}} \zeta^j \right) = \frac{\epsilon \cdot p + 1}{2}
\]

and

\[
\left( \sum_{n \in N} \zeta^n \right) \left( \sum_{l \in \mathbb{Z}} \zeta^l \right) + \left( \sum_{q \in Q} \zeta^q \right) \left( \sum_{j \in \mathbb{Z}} \zeta^j \right) = \frac{-\epsilon \cdot p + 1}{2}.
\]
Every conjugacy class of non-central cyclic subgroups contains exactly \( p \) subgroups. Let \( \langle d \rangle \) be such a subgroup. By \( \chi(d) \in Q \) we indicate that \( \chi(d) = \zeta^q \) for some \( q \in Q \). To compute the contribution of the remaining elements we distinguish two cases.

Case 1: \((\varepsilon_g(d), \varepsilon_h(d)) = (1, 0), \chi(d^{-1}) \in N \) or \((\varepsilon_g(d), \varepsilon_h(d)) = (0, 1), \chi(d^{-1}) \in Q \). Then the contribution of the conjugacy class of \( \langle d \rangle \) is

\[
p \sum_{h \in \langle d \rangle \setminus \{1\}} \eta(h)\chi(h^{-1}) = p \left( \sum_{\eta \in Q} \left( \frac{p + \epsilon}{2} + p \sum_{i \in Q} \zeta^i \right) \zeta^q + \sum_{n \in N} \left( \frac{p + \epsilon}{2} + p \sum_{j \in N} \zeta^j \right) \zeta^n \right) = p \left( \frac{p + \epsilon}{2} + p \left( \sum_{\eta \in Q} \left( \sum_{i \in Q} \zeta^i \right) + \left( \sum_{n \in N} \left( \sum_{j \in N} \zeta^j \right) \right) \right) \right) = p \left( \frac{p + \epsilon}{2} + p \left( \frac{\epsilon + p + 1}{2} \right) \right) = \epsilon \cdot \frac{p^3 - p}{2}
\]

Case 2: \((\varepsilon_g(d), \varepsilon_h(d)) = (1, 0), \chi(d^{-1}) \in N \) or \((\varepsilon_g(d), \varepsilon_h(d)) = (0, 1), \chi(d^{-1}) \in Q \). Then the contribution of the conjugacy class of \( \langle d \rangle \) is

\[
p \left( \sum_{n \in N} \left( \frac{p + \epsilon}{2} + p \sum_{i \in Q} \zeta^i \right) \zeta^n + \sum_{\eta \in Q} \left( \frac{p + \epsilon}{2} + p \sum_{j \in N} \zeta^j \right) \zeta^n \right) = p \left( \frac{p + \epsilon}{2} + p \left( \sum_{n \in N} \left( \sum_{i \in Q} \zeta^i \right) + \left( \sum_{j \in N} \zeta^j \right) \right) \right) = p \left( \frac{p + \epsilon}{2} + p \left( -\epsilon \cdot \frac{p + 1}{2} \right) \right) = -\epsilon \cdot \frac{p^3 + p}{2}
\]

From now on let \( I = \{0, 1, ..., p - 1\} \). Let \( \chi \) be a non-trivial linear character of \( H \) and let \( s \in \text{Ker}(\chi) \setminus \mathbb{Z}(H) \). Moreover let \( t \not\in \text{Ker}(\chi) \) such that \( \chi(t^{-1}) \in Q \). Then \( \{(ts^i)^{-1} \mid i \in I \} \) is a set which contains exactly one element from every conjugacy class of cyclic subgroups not lying in \( \text{Ker}(\chi) \) and \( \chi((ts^i)^{-1}) \in Q \) for every \( i \). Set

\[
\gamma = \{ i \mid (\varepsilon_g(ts^i), \varepsilon_h(ts^i)) = (1, 0) \} \quad \text{and} \quad \delta = \{ i \mid (\varepsilon_g(ts^i), \varepsilon_h(ts^i)) = (0, 1) \}.
\]

Then \( \gamma + \delta = p \) and, summing up all the contributions obtained above, we get

\[
\langle \eta, \chi \rangle_H = \frac{1}{p^3} \left( \frac{p^3 + \epsilon}{2} + \epsilon \cdot \frac{p - 1}{2} + \epsilon \gamma \cdot \frac{p^3 - p}{2} - \epsilon \delta \cdot \frac{p^3 + p}{2} \right) = \frac{1}{2p^2} \left( p^3 \left( 1 + \epsilon \gamma - \epsilon \delta \right) + \epsilon p^2 - \epsilon (\gamma + \delta) p \right) = \frac{1 + \epsilon \gamma - \epsilon \delta}{2}
\]

For \( n \in N \) the map \( \chi^n : H \to \mathbb{Z}[\zeta] : x \mapsto \chi(x)^n \) is also a linear character of \( H \) and an analogous computation gives

\[
\langle \eta, \chi^n \rangle_H = \frac{1 - \epsilon \gamma + \epsilon \delta}{2}.
\]

Since both, \( \langle \eta, \chi \rangle_H \) and \( \langle \eta, \chi^n \rangle_H \), are non-negative, necessarily \( |\gamma - \delta| \leq 1 \). Thus \( \gamma = \frac{p+1}{2} \) and \( \delta = \frac{p-1}{2} \).

Recall that by (1), \( H \) is generated by a central element \( z \) and two other elements \( b \) and \( c \). We may assume w.l.o.g. by (5) that \((\varepsilon_g(c), \varepsilon_h(c)) = (1, 0)\). We have that \( \{(c), (bc^i) \mid i \in I \} \) is a set
of representatives of the $p + 1$ conjugacy classes of non-central cyclic subgroups of $H$. Up to the action of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, every linear character is determined by its kernel. Let $n \in N$. Then by (5) there exist $a_0, a_1, ..., a_{p-1} \in \{1, n\}$ such that $c, b^a, b^{a_1}, ..., b^{a_{p-1}}(p-1)a_{p-1}$ all have partial augmentation 1 at $g$ and 0 at $h$.

Let $\chi$ be a non-trivial linear character with $\langle c \rangle \subseteq \text{Ker}(\chi)$ and $\chi(b^{-1}) \in Q$. Then $S = \{bc^i \mid i \in I\}$ is a set which contains exactly one element from every conjugacy class of cyclic subgroups not lying in $\text{Ker}(\chi)$. By the above, $\frac{p+1}{2}$ of the elements of $S$ have partial augmentation 1 at $g$ and the other elements have augmentation 0 at $g$. Since $\varepsilon_g(bc^i) = 1$ if and only if $a_i = 1$ we get

$$|\{i \in I \mid a_i = 1\}| \in \left\{\frac{p+1}{2}\right\}.$$  

(6)

Now let $j \in I$ and $\chi$ be a non-trivial linear character of $H$ such that $\langle bc^j \rangle \subseteq \text{Ker}(\chi)$ and $\chi(c^{-1}) \in Q$. For every $i \in I \setminus \{j\}$ we determine one element of the form $b^{a_i}c^{\ell a_i}$, for some $\ell$, lying in the coset $\text{Ker}(\chi)c = \{z b^{c^{k+1}} \mid 0 \leq k, r \leq p-1\}$. To do so let $\ell, k$ be such that $b^{k}c^{j+1} = b^{a_i}c^{\ell a_i}$.

Thus $k \equiv \ell a_i \pmod{p}$ and $j + k + 1 \equiv \ell a_i \pmod{p}$. This gives $\ell \equiv (\ell a_i - ja_i)^{-1} \pmod{p}$. For the partial augmentations of $b^{a_i}c^{\ell a_i}$ it only matters, by (5), whether $\ell$ is a quadratic residue modulo $p$. Hence $b^{a_i}c^{\ell a_i}$ has the same partial augmentations as $c$ if and only if $\ell \in Q$, i.e. $ja_i - ja_i \in Q$. Hence

$$1 + |\{i \in I \setminus \{j\} \mid ia_i - ja_i \in Q\}| \in \left\{\frac{p+1}{2}\right\},$$  

(7)

where the 1 represents the element $c$.

Denote by $(r \mid p)$ the Legendre symbol of $r$ modulo the prime $p$ and set $\beta_i = (a_i \mid p)$ for $i \in I$. By (6) we have

$$\sum_{i \in I} \beta_i = \sum_{i \in I} \left(\begin{array}{c} a_i \mid p \end{array}\right) \in \{\pm 1\}.\quad (8)$$

From (7) we get for every $j \in I$:

$$1 + \sum_{i \in I} \left(\begin{array}{c} i - j \mid p \end{array}\right) \beta_i = 1 + \sum_{i \in I} \left(\begin{array}{c} i - j \mid a_i \end{array}\right) \in \{\pm 1\}.\quad (9)$$

Set $s_i = (i \mid p)$ for $i \in \{1, ..., p-1\}$. Then the above equations read as follows: there exist $m_0, ..., m_{p-1} \in \{\pm 1\}$ such that

$$\begin{pmatrix} \beta_0 & s_1 & s_2 & \cdots & s_{p-1} \\ s_{p-1} & \beta_1 & s_1 & \cdots & s_{p-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ s_2 & s_3 & \cdots & \beta_{p-2} & s_1 \\ s_1 & s_2 & \cdots & s_{p-1} & \beta_{p-1} \end{pmatrix} \begin{pmatrix} m_0 \\ m_1 \\ \vdots \\ m_{p-2} \\ m_{p-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{p-2} \\ \beta_{p-1} \end{pmatrix}.$$

Summing up all equations and sorting with regard to the $\beta_i$’s we get

$$\beta_0(s_1 + \cdots + s_{p-1}) + \cdots + \beta_{p-1}(s_1 + \cdots + s_{p-1}) + p = m_0 + \cdots + m_{p-1}.$$  

Since $s_1 + \cdots + s_{p-1} = 0$ all the $m_i$’s must be equal to 1. Thus we have to solve the homogeneous system of linear equations given by

$$\begin{pmatrix} 0 & s_1 & s_2 & \cdots & s_{p-1} \\ s_{p-1} & 0 & s_1 & \cdots & s_{p-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ s_2 & s_3 & \cdots & 0 & s_1 \\ s_1 & s_2 & \cdots & s_{p-1} & 0 \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{p-2} \\ \beta_{p-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

The null space of the system has (at most) dimension 1 by the following lemma and contains the vector $(\beta_0, \beta_1, ..., \beta_{p-1})^T = (1, 1, ..., 1)^T$. This is however out of the question by (8).
Lemma. Let \( m \) be odd and \( A \in \mathbb{F}_2^{m \times m} \) where

\[
A = \begin{pmatrix}
0 & 1 & 1 & \ldots & 1 \\
1 & 0 & 1 & \ldots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 1 & \ldots & 0 & 1 \\
1 & 1 & \ldots & 1 & 0
\end{pmatrix}
\]

Then \( \text{rank } A = m - 1 \).

Proof. Summing up all rows of \( A \) gives the zero vector, hence the rank of \( A \) is at most \( m - 1 \). Let \( z_1, \ldots, z_{m-1} \) be the first \( m - 1 \) rows of \( A \) and \( \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{F}_2 \) such that \( \sum_{i=1}^{m-1} \alpha_i z_i = 0 \). Then we get \( \sum_{i=1, i \neq j}^{m-1} \alpha_i = 0 \) for every \( j \in \{1, \ldots, m-1\} \) and \( \sum_{i=1}^{m-1} \alpha_i = 0 \). Hence \( \alpha_j = 0 \) for all \( j \in \{1, \ldots, m-1\} \). \( \square \)

References

[Ber55] S.D. Berman, On the equation \( x^m = 1 \) in an integral group ring, Ukrain. Mat. Ž. 7 (1955), 253–261.

[Bie95] F.M. Bleher, Tensor products and a conjecture of Zassenhaus, Arch. Math. (Basel) 64 (1995), no. 4, 289–298.

[CL65] J.A. Cohn and D. Livingston, On the structure of group algebras I, Canadian Journal of Mathematics 17 (1965), 583–593.

[Dic58] I.E. Dickson, Linear groups: With an exposition of the Galois field theory, with an introduction by W. Magnus, Dover Publications, New York, 1958.

[DJ96] M.A. Dokuchaev and S.O. Juriaans, Finite subgroups in integral group rings, Canad. J. Math. 48 (1996), no. 6, 1170–1179.

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

[Gau11] C.F. Gauß, Summatio quoramdam serierum singularium, Commentationes societ. reg. sc. Gotting. recensiores 1 (1811), Published in German in: Gauss, Untersuchungen über höhere Arithmetik, Chelsea Publishing Co., New York, 1965.

[Her07] M. Hertweck, Partial Augmentations and Brauer character values of torsion units in group rings, arXiv:math.RA/0612429v2 [math.RA] (2007).

[Her08] _____, Unit groups of integral finite group rings with no noncyclic abelian finite \( p \)-subgroups, Comm. Algebra 36 (2008), no. 9, 3224–3229.

[HHK09] M. Hertweck, C.R. Höfert, and W. Kimmerle, Finite groups of units and their composition factors in the integral group rings of the group PSL(2, \( q \)), J. Group Theory 12 (2009), no. 6, 873–882.

[Hig40] G. Higman, Units in group rings, D. phil. thesis, Oxford Univ., 1940.

[Höf08] C.R. Höfert, Bestimmung von Kompositionsfactoren endlicher Gruppen aus Burnsidern und ganzzahligem Gruppenringen, Doktorarbeit, Universität Stuttgart, 2008, http://elib.uni-stuttgart.de/opus/frontdoor.php?source_opus=3551&la=de.

[Hup67] B. Huppert, Endliche Gruppen I, Die Grundlehren der mathematischen Wissenschaften ed., vol. 134, Springer-Verlag, Berlin, 1967.

[Kim07] W. Kimmerle, Torsion units in integral group rings of finite insoluble groups, Oberwolfach Reports 4 (2007), no. 4, 3229–3230. Abstracts from the mini-workshop held November 25–December 1, 2007, Organized by Eric Jespers, Zbigniew Marciniak, Gabriele Nebe, and Wolfgang Kimmerle.

[LP89] I.S. Luthar and I.B.S. Passi, Zassenhaus conjecture for \( A_5 \), Proc. Indian Acad. Sci. Math. Sci. 99 (1989), no. 1, 1–5.

[Mar14] L. Margolis, A Sylow theorem for the integral group ring of \( PSL(2, q) \), arXiv:1408.6075 [math.RA] (2014).

[Neu99] J. Neukirch, Algebraic number theory, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999.

[Sak71] A. I. Saksonov, Group rings of finite groups, I, Publ. Math. Debrecen 18 (1971), 187–209.

[San81] R. Sandling, Graham Higman’s thesis “Units in group rings”, Integral representations and applications (Oberwolfach, 1980), Lecture Notes in Math., vol. 882, Springer, Berlin-New York, 1981, pp. 93–116.

[San85] _____, The isomorphism problem for group rings: a survey, Orders and their applications (Oberwolfach, 1984), Lecture Notes in Math., vol. 1142, Springer, Berlin, 1985, pp. 256–288.

[Sek93] S.K. Sehgal, Units in integral group rings, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 69, Longman Scientific & Technical, Harlow, 1993.