Proceedings of the Edinburgh Mathematical Society (2023) **66**, 940–959
doi:10.1017/S0013091523000500

THE REIDEMEISTER SPECTRUM OF FINITE ABELIAN GROUPS

PIETER SENDEN

Department of Mathematics, KU Leuven Kulak Kortrijk Campus, Kortrijk, Belgium
(pieter.senden@kuleuven.be)

(Received 3 June 2022)

Abstract For a finite abelian group A, the Reidemeister number of an endomorphism φ is the same as the number of fixed points of φ, and the Reidemeister spectrum of A is completely determined by the Reidemeister spectra of its Sylow p-subgroups. To compute the Reidemeister spectrum of a finite abelian p-group P, we introduce a new number associated to an automorphism ψ of P that captures the number of fixed points of ψ and its (additive) multiples, we provide upper and lower bounds for that number, and we prove that every power of p between those bounds occurs as such a number.

Keywords: finite abelian groups; twisted conjugacy; Reidemeister number; Reidemeister spectrum; fixed points

2020 Mathematics subject classification: Primary 20K30; 20E45

1. Introduction

Given a group G and an endomorphism φ, we define the φ-twisted conjugacy relation on G by stating that $x, y \in G$ are φ-conjugate if there exists a $z \in G$ such that $x = zy\varphi(z)^{-1}$. If x and y are φ-conjugate, we write this as $x \sim_\varphi y$. The number of φ-conjugacy classes is called the Reidemeister number of φ, and it is denoted by $R(\varphi)$. If G is a finite abelian group, the Reidemeister number of φ coincides with the size of $\mathrm{Fix}(\varphi)$, the fixed-point subgroup of φ (see Proposition 2.1). Furthermore, we define the Reidemeister spectrum of G as $\mathrm{Spec}_{\mathrm{R}}(G) := \{R(\psi) \mid \psi \in \mathrm{Aut}(G)\}$.

One of the general objectives is to determine the complete Reidemeister spectrum of a group. There are two extreme cases that can occur: (1) G has the R_∞-property, which means that $\mathrm{Spec}_{\mathrm{R}}(G) = \{\infty\}$, and (2) G has full Reidemeister spectrum, which means that $\mathrm{Spec}_{\mathrm{R}}(G) = \mathbb{N}_0 \cup \{\infty\}$. The first case in particular has been extensively studied. Non-abelian Baumslag-Solitar groups [6] and their generalizations [18], certain extensions of linear groups by a countable abelian group [13] and Thompson's group F [1] all have the R_∞-property; it has been proven that the free nilpotent group $N_{r,c}$ of rank $r \geq 2$ and class $c \geq 1$ has the R_∞-property if and only if $c \geq 2r$, see, for example [2, 14]. We refer the reader to [8] for a more exhaustive list of examples.

For the second extreme case, fewer examples of groups have been found. One family of such groups are the groups $N_{r,2}$, where $r \geq 4$ [5]. Finally, groups whose Reidemeister spectrum has been fully determined but have neither the R_∞-property nor full Reidemeister spectrum include the semidirect products $\mathbb{Z}^n \rtimes \mathbb{Z}/2\mathbb{Z}$, where $n \geq 2$ and $\mathbb{Z}/2\mathbb{Z}$ acts by inversion [4].

For finite groups, however, neither extreme case can occur. As far as the author knows, there is only little literature concerning twisted conjugacy and Reidemeister numbers on finite groups. A. Fel'shtyn and R. Hill have proven that the Reidemeister number of an endomorphism φ of a finite group equals the number of (ordinary) conjugacy classes that are fixed by φ [7, Theorem 5], and they have also discussed Reidemeister zeta functions on finite groups. Still, information about Reidemeister numbers of finite groups can aid in determining the Reidemeister spectrum of infinite groups, since finitely generated residually finite groups can be studied by looking at their finite characteristic quotients.

Given a finite group G, it is theoretically possible to compute its Reidemeister spectrum using a computer; for instance, Tertooy has developed a GAP-package [19] that has these functionalities. However, for an arbitrary finite group, the only feasible way to do so is to use either the definition or the result by Fel'shtyn and Hill relating Reidemeister numbers to fixed conjugacy classes. Either method requires a substantial amount of computation time if the order of G increases, since one has to determine $\mathrm{Aut}(G)$, possibly the set of all conjugacy classes, and the Reidemeister number $R(\varphi)$ for each $\varphi \in \mathrm{Aut}(G)$. To reduce this time, one can try and find explicit expressions for the Reidemeister spectrum of certain (families of) finite groups or even just methods that do not require to fully compute $\mathrm{Aut}(G)$ in order to determine $\mathrm{Spec}_{\mathrm{R}}(G)$. The former has been done by the author for split metacyclic groups of the form $C_n \rtimes C_p$, where p is a prime number in [16].

The aim of this paper is to completely determine the Reidemeister spectrum of finite abelian groups. We would like to mention that Reidemeister spectra of infinite abelian groups, on the other hand, have already been studied, see [14, § 3],[3, 9]. To determine complete and explicit expressions for the Reidemeister spectrum of finite abelian groups, we start in § 2 with recalling the necessary results regarding Reidemeister numbers and reducing the problem to counting fixed points on finite abelian groups of prime power order. In § 3, we determine the Reidemeister spectrum of finite abelian p-groups with p an odd prime. In § 4, finally, we determine the Reidemeister spectrum of finite abelian 2-groups by solving a more general problem: we introduce a new number that counts the number of fixed points of an automorphism and its (additive) multiples on a finite abelian p-group and provide sharp upper and lower bounds for that number.

Unless otherwise stated, p denotes a prime number.

2. Preliminaries

Proposition 2.1. *Let A be a finite abelian group and $\varphi \in \mathrm{End}(A)$. Then $R(\varphi) = |\mathrm{Fix}(\varphi)|$.*

Proof. Note that, for all $x, y \in A$, we have

$$x \sim_\varphi y \iff \exists z \in A : x = z + y - \varphi(z) \iff x - y \in \mathrm{Im}(\mathrm{Id} - \varphi).$$

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Therefore, $R(\varphi) = [A : \mathrm{Im}(\mathrm{Id} - \varphi)]$. Since A is finite, we moreover have that

$$[A : \mathrm{Im}(\mathrm{Id} - \varphi)] = \frac{|A|}{|\mathrm{Im}(\mathrm{Id} - \varphi)|} = |\ker(\mathrm{Id} - \varphi)| = |\mathrm{Fix}(\varphi)|$$

by the first isomorphism theorem for groups. □

Corollary 2.2. *Let A be a finite abelian group. Then* $\mathrm{Spec}_{\mathrm{R}}(A) \subseteq \{d \in \mathbb{N} \mid d$ *divides* $|A|\}$.

By this corollary, determining the complete Reidemeister spectrum of a finite abelian group A reduces to determining which divisors of $|A|$ occur. We argue that we can even restrict ourselves to solving that problem for finite abelian p-groups.

Definition 2.3. *Let $A_1, \dots, A_n$ be sets of natural numbers. We define*

$$\prod_{i=1}^{n} A_i := \{a_1 \cdots a_n \mid \forall i \in \{1, \dots, n\} : a_i \in A_i\}.$$

If $A_1 = \cdots = A_n =: A$, we also write $A^{(n)}$.

The following can be found in, for example, [17, Corollary 2.6]:

Proposition 2.4. *Let $G_1, \dots, G_n$ be groups and put $G := \bigtimes_{i=1}^{n} G_i$. Then*

$$\prod_{i=1}^{n} \mathrm{Spec}_{\mathrm{R}}(G_i) \subseteq \mathrm{Spec}_{\mathrm{R}}(G).$$

Equality holds if $\mathrm{Aut}(G) = \bigtimes_{i=1}^{n} \mathrm{Aut}(G_i)$ (i.e., if the natural embedding of $\bigtimes_{i=1}^{n} \mathrm{Aut}(G_i)$ in $\mathrm{Aut}(G)$ is onto).

Corollary 2.5. *Let $G = G_1 \times \cdots \times G_n$ be a direct product of finite groups such that $\gcd(|G_i|, |G_j|) = 1$ for $i \neq j$. Then*

$$\mathrm{Spec}_{\mathrm{R}}(G) = \prod_{i=1}^{n} \mathrm{Spec}_{\mathrm{R}}(G_i).$$

Proof. It is well known that under the conditions in the statement, the equality

$$\mathrm{Aut}(G) = \bigtimes_{i=1}^{n} \mathrm{Aut}(G_i)$$

holds. The result now follows from the previous proposition. □

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Since each finite abelian group A admits a unique decomposition of the form

$$A = \bigoplus_{p \in \mathcal{P}} A(p),$$

where $\mathcal{P}$ is the set of all primes and $A(p)$ is the Sylow p-subgroup of A, it is consequently sufficient to determine the Reidemeister spectrum of finite abelian p-groups to completely determine the Reidemeister spectrum of finite abelian groups. For odd prime numbers, this is straightforward. For $p = 2$, on the other hand, the situation is much more complicated, both the Reidemeister spectrum itself and the proof.

We write the cyclic group of order n as $\mathbb{Z}/n\mathbb{Z}$ and write abelian groups additively. The following two lemmata are tools to compute and bound Reidemeister numbers:

Lemma 2.6. *Let $n \geq 2$ and let $\varphi \in \mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ be given by $\varphi(1) = k$. Then $R(\varphi) = \gcd(k-1, n)$.*

Proof. Since $R(\varphi) = |\mathrm{Fix}(\varphi)|$, we determine the fixed points of φ. We have that $\varphi(i) = i$ if and only if $i \cdot (k-1) \equiv 0 \bmod n$. Writing $d = \gcd(k-1, n)$, we see that $\frac{k-1}{d}$ is invertible modulo n. Hence, $i \cdot (k-1) \equiv 0 \bmod n$ if and only if $i \cdot d \equiv 0 \bmod n$. Thus, for $i \cdot d \equiv 0 \bmod n$ to hold, i must be a multiple of $\frac{n}{d}$. Since i has to lie between 0 and $n-1$ and there are d multiples of $\frac{n}{d}$ lying between 0 and $n-1$, φ has d fixed points. □

Lemma 2.7. *Let G be a group, $\varphi \in \mathrm{End}(G)$ and N a φ-invariant normal subgroup of G (i.e., $\varphi(N) \leq N$). Let $\bar{\varphi}$ denote the induced endomorphism on G/N and φ' the induced endomorphism on N. Then $R(\varphi) \geq R(\bar{\varphi})$.*

If, moreover, G is finite abelian, then $R(\varphi') \leq R(\varphi)$.

Proof. The first inequality is well known, see, for example, [10, Lemma 1.1]. For the second, if G is finite abelian, we know that $R(\varphi) = |\mathrm{Fix}(\varphi)|$ and $R(\varphi') = |\mathrm{Fix}(\varphi')|$. As $\mathrm{Fix}(\varphi') \leq \mathrm{Fix}(\varphi)$, the inequality $R(\varphi') \leq R(\varphi)$ follows. □

We end with introducing some notation and terminology.

Definition 2.8. *Let n be a positive integer. We define $E(n)$ to be*

$$E(n) := \{(e_1, \ldots, e_n) \in \mathbb{Z}^n \mid \forall i \in \{1, \ldots, n-1\} : 1 \leq e_i \leq e_{i+1}\}.$$

Given a prime p and $e \in E(n)$, we define the abelian p-group of type e to be the group

$$P_{p,e} := \bigoplus_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}.$$

By the fundamental theorem of finite abelian groups, we know that, for each non-trivial finite abelian p-group P, there exists a unique $n \geq 1$ and a unique $e \in E(n)$ such that $P \cong P_{p,e}$. We say that P is *of type e*. For the trivial group, we take $n = 0$ and e the 'empty' tuple.

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

3. Reidemeister spectrum of finite abelian p-groups with p odd prime

For p an odd prime, the computation of the Reidemeister spectrum of a finite abelian p-group of type e is a straightforward application of Lemma 2.6 and Proposition 2.4.

Lemma 3.1. *Let p be an odd prime and $n \geq 1$ a natural number. Then*

$$\mathrm{Spec}_{\mathrm{R}}(\mathbb{Z}/p^n\mathbb{Z}) = \{p^i \mid i \in \{0, \dots, n\}\}.$$

Proof. The $\subseteq$-inclusion follows from Corollary 2.2. For the other inclusion, we use Lemma 2.6. For $i \in \{0, \dots, n\}$, define $\varphi_i : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} : 1 \mapsto p^i + 1$. Since $\gcd(p^i + 1, p) = 1$, as p is odd, φ_i is an automorphism of $\mathbb{Z}/p^n\mathbb{Z}$. By Lemma 2.6, $R(\varphi_i) = p^i$. □

Remark. This approach fails for $p = 2$, for then the map φ_0 is not an automorphism of $\mathbb{Z}/2^n\mathbb{Z}$. Indeed, $\varphi_0 : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is given by $\varphi_0(1) = 2$, and since 2 is not invertible in $\mathbb{Z}/2^n\mathbb{Z}$, φ_0 is not an automorphism. We can argue, more generally, that there is no automorphism on $\mathbb{Z}/2^n\mathbb{Z}$ with no non-trivial fixed points: if $\varphi \in \mathrm{Aut}(\mathbb{Z}/2^n\mathbb{Z})$ is given by $\varphi(1) = k$, then k must be odd. Consequently, $k - 1$ is even and thus is

$$|\mathrm{Fix}(\varphi)| = R(\varphi) = \gcd(k - 1, 2^n) \geq 2$$

by Lemma 2.6. All other φ_i from Lemma 3.1, however, are automorphisms if $p = 2$, so $\mathrm{Spec}_{\mathrm{R}}(\mathbb{Z}/2^n\mathbb{Z})$ equals $\{2, 2^2, \dots, 2^n\}$.

For $e \in E(n)$, we put $\Sigma(e) := \sum_{i=1}^{n} e_i$. Then, for P a p-group of type e, we have $|P| = p^{\Sigma(e)}$.

Proposition 3.2. *Let p be an odd prime and P a finite abelian p-group of type $e \in E(n)$. Then*

$$\mathrm{Spec}_{\mathrm{R}}(P) = \{p^i \mid i \in \{0, \dots, \Sigma(e)\}\}.$$

In other words, $\mathrm{Spec}_{\mathrm{R}}(P)$ is the set of all divisors of $|P|$.

Proof. By Corollary 2.2, we only have to prove the $\supseteq$-inclusion, and this essentially boils down to Proposition 2.4. Let $m \in \{0, \dots, \Sigma(e)\}$ and let $j \in \{1, \dots, n + 1\}$ be the (unique) index such that

$$\sum_{l=1}^{j-1} e_l \leq m < \sum_{l=1}^{j} e_l,$$

where we put $e_{n+1} := \infty$ for convenience. By Lemma 3.1, there are automorphisms φ_i of $\mathbb{Z}/p^{e_i}\mathbb{Z}$ such that

$$R(\varphi_i) = \begin{cases} p^{e_i} & \text{if } i \leq j - 1, \\ p^{m - \sum_{l=1}^{j-1} e_l} & \text{if } i = j, \\ 1 & \text{if } i > j. \end{cases}$$

Then $\varphi := (\varphi_1, \ldots, \varphi_n)$ is an automorphism of P and

$$R(\varphi) = \prod_{i=1}^{n} R(\varphi_i) = p^{\sum_{l=1}^{j-1} e_l + m - \sum_{l=1}^{j-1} e_l} = p^m.$$

□

We explained earlier that $\mathrm{Spec}_{\mathrm{R}}(\mathbb{Z}/2^n\mathbb{Z}) = \{2, \ldots, 2^n\}$. As a consequence, the construction from Proposition 3.2 does not work either for $p = 2$, as we cannot find automorphisms with Reidemeister number 1 on the cyclic factors. If P is an abelian 2-group of type $e \in E(n)$, the smallest number in $\mathrm{Spec}_{\mathrm{R}}(P)$ we can find with that approach is 2^n, which comes from picking an automorphism with Reidemeister number 2 on each of the cyclic factors. However, computer calculations show that, for example, 2 is contained in the Reidemeister spectrum of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Thus, the minimum of $\mathrm{Spec}_{\mathrm{R}}(P)$ is not necessarily 2^n. On the other hand, the identity map on P has Reidemeister number $2^{\Sigma(e)} = |P|$, so determining the upper end of the Reidemeister spectrum should not yield major difficulties.

4. Fixed points on finite abelian *p*-groups

Due to the absence of 1 in the Reidemeister spectrum of cyclic 2-groups, we need a different approach to determine the Reidemeister spectrum of abelian 2-groups, especially a lower bound on the Reidemeister numbers. This different approach consists of studying a more general phenomenon concerning fixed points of automorphisms on abelian p-groups, which is valid for all prime numbers, not only for $p = 2$.

Let p be a prime number, $n \geq 1$ and $e \in E(n)$. Let $P := P_{p,e}$ be the finite abelian p-group of type e. For $i \in \mathbb{Z}$ coprime with p, let μ_i denote the automorphism of P given by $\mu_i(x) = ix$. For $\varphi \in \mathrm{Aut}(P)$, we then define

$$\Pi(\varphi) := \prod_{i=1}^{p-1} |\mathrm{Fix}(\mu_i \circ \varphi)|.$$

Finally, we put $\mathrm{Spec}_\Pi(P) := \{\Pi(\psi) \mid \psi \in \mathrm{Aut}(P)\}$. The goal is to fully determine $\mathrm{Spec}_\Pi(P)$. Note that $\Pi(\varphi)$ is always a power of p; hence, $\mathrm{Spec}_\Pi(P) \subseteq \{p^i \mid i \in \mathbb{N}\}$. If $p = 2$, then

$$\Pi(\varphi) = |\mathrm{Fix}(\mu_1 \circ \varphi)| = |\mathrm{Fix}(\varphi)| = R(\varphi)$$

by Proposition 2.1; hence, $\mathrm{Spec}_\Pi(P) = \mathrm{Spec}_{\mathrm{R}}(P)$ in that case. This shows that $\mathrm{Spec}_\Pi(P)$ is a generalization of $\mathrm{Spec}_{\mathrm{R}}(P)$ of some sort.

We start by determining an upper bound for $\mathrm{Spec}_\Pi(P)$, which can also be used to give an interpretation of $\Pi(\varphi)$ that resembles the notion of diagonalisable transformations from linear algebra[1]. Afterwards, we tackle the more difficult and involved problem of determining a lower bound for $\mathrm{Spec}_\Pi(P)$. Finally, we prove that every power of p lying between those two bounds lies in $\mathrm{Spec}_\Pi(P)$.

[1] A word of gratitude goes to the anonymous referee for suggesting this interpretation.

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

4.1. Upper bound

As said earlier, we start with the upper bound for $\mathrm{Spec}_\Pi(P)$.

Proposition 4.1. *Let P be a finite abelian p-group of type e. Let $\varphi \in \mathrm{Aut}(P)$. Then $\Pi(\varphi) \leq |P| = p^{\Sigma(e)}$.*

Proof. Fix $\varphi \in \mathrm{Aut}(P)$. We first prove that

$$\mathrm{Fix}(\mu_i \circ \varphi) \cap \langle \mathrm{Fix}(\mu_j \circ \varphi) \mid j \neq i \rangle$$

is trivial for all $i \in \{1, \ldots, p-1\}$. We proceed by induction, namely by proving that, for all $k \in \{1, \ldots, p-2\}$ and all $\mathcal{J} \subseteq (\{1, \ldots, p-1\} \setminus \{i\})$ with $|\mathcal{J}| = k$, the intersection

$$\mathrm{Fix}(\mu_i \circ \varphi) \cap \langle \mathrm{Fix}(\mu_j \circ \varphi) \mid j \in \mathcal{J} \rangle$$

is trivial. We start with $k = 1$, that is, with $\mathcal{J} = \{j\}$ with $j \neq i$. An element x in the intersection then satisfies $x = i\varphi(x) = j\varphi(x)$, or equivalently, $(i-j)\varphi(x) = 0$. As $i \neq j$ and both lie in $\{1, \ldots, p-1\}$, we know that $i - j$ is an invertible modulo p, hence $\varphi(x) = 0$. Since $x = i\varphi(x)$, we conclude that $x = 0$. This proves the claim for $k = 1$.

Now, suppose that it holds for all $\mathcal{J}$ of size k or less. Let $\mathcal{J}$ be a set of size $k+1$ not containing i and let x be an element in the intersection $\mathrm{Fix}(\mu_i \circ \varphi) \cap \langle \mathrm{Fix}(\mu_j \circ \varphi) \mid j \in \mathcal{J} \rangle$. Write $x = \sum_{j \in \mathcal{J}} x_j$, with $x_j \in \mathrm{Fix}(\mu_j \circ \varphi)$. On the one hand, we have

$$x = i\varphi(x) = i \sum_{j \in \mathcal{J}} \varphi(x_j) = \sum_{j \in \mathcal{J}} i\varphi(x_j),$$

while, on the other hand, we have

$$x = \sum_{j \in \mathcal{J}} x_j = \sum_{j \in \mathcal{J}} j\varphi(x_j).$$

Therefore,

$$0 = \sum_{j \in \mathcal{J}} (j - i)\varphi(x_j).$$

Now, let $j_0 \in \mathcal{J}$ be arbitrary but fixed and put $\mathcal{J}' := \mathcal{J} \setminus \{j_0\}$. We can rewrite the equality above to

$$(j_0 - i)\varphi(x_{j_0}) = \sum_{j \in \mathcal{J}'} -(j - i)\varphi(x_j).$$

Since φ is an automorphism, we can apply φ^{-1} to get

$$(j_0 - i)x_{j_0} = \sum_{j \in \mathcal{J}'} -(j - i)x_j$$

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

The left-hand side lies in $\mathrm{Fix}(\mu_{j_0} \circ \varphi)$, and the right-hand side is an element of $\langle \mathrm{Fix}(\mu_j \circ \varphi) \mid j \in \mathcal{J}' \rangle$. Applying the induction hypothesis to j_0 and $\mathcal{J}'$, we find that both sides are trivial, that is, $(j_0 - i)x_{j_0} = 0 = \sum_{j \in \mathcal{J}'} -(j - i)x_j$. As $i \neq j_0$, this implies $x_{j_0} = 0$.

Since $j_0 \in \mathcal{J}$ was arbitrary, we conclude that $x_j = 0$ for all $j \in \mathcal{J}$. This finishes the induction. The original claim then follows from the case where $\mathcal{J} = \{1, \dots, p-1\} \setminus \{i\}$.

From the above, it follows that

$$p^{\Sigma(e)} = |P| \geq |\langle \mathrm{Fix}(\mu_i \circ \varphi) \mid i \in \{1, \dots, p-1\} \rangle| = \prod_{i=1}^{p-1} |\mathrm{Fix}(\mu_i \circ \varphi)| = \Pi(\varphi),$$

which proves the upper bound. □

Remark. We can now give the aforementioned interpretation of the value $\Pi(\varphi)$ of an automorphism φ. Let $i \in \{1, \dots, p-1\}$. Then

$$\mathrm{Fix}(\mu_i \circ \varphi) = \{x \in P \mid i\varphi(x) = x\} = \{x \in P \mid \varphi(x) = jx\},$$

where j is the (multiplicative) inverse of i modulo p. In other words, $\mathrm{Fix}(\mu_i \circ \varphi)$ can be thought of as the eigenspace of the eigenvalue j for φ. In the proof of Proposition 4.1, we essentially showed that the subgroup generated by all of these eigenspaces splits as the direct sum of the individual eigenspaces, that is,

$$\langle \mathrm{Fix}(\mu_i \circ \varphi) \mid i \in \{1, \dots, p-1\} \rangle = \bigoplus_{i=1}^{p-1} \mathrm{Fix}(\mu_i \circ \varphi),$$

where the direct sum is an internal direct sum in this case. We then see that $\Pi(\varphi)$, which is the size of this internal direct sum, equals $|P|$ if and only if P equals this direct sum. In other words, $\Pi(\varphi) = |P|$ if and only if P decomposes as a direct sum of eigenspaces of φ. Using terminology from linear algebra, one could say that $\Pi(\varphi) = |P|$ if and only if φ is diagonalisable. So, $\Pi(\varphi)$ measures in some sense to what extent φ is diagonalisable.

4.2. Lower bound

Now, we determine a lower bound for $\mathrm{Spec}_\Pi(P)$. Throughout this section, let p be a prime number, $n \geq 1$ and $e \in E(n)$. Let $P := P_{p,e}$ be the finite abelian p-group of type e. To formulate the lower bound, we construct a decomposition of e.

Definition 4.2. *Given $e \in E(n)$, we construct the abc-decomposition of e into three types of blocks in the following way:*

Step 1: *Each maximal constant subsequence of $e_1, \dots, e_n$ of length at least 2 forms one block, which we call an a-block.*

Step 2: *Among the remaining numbers, we look for successive numbers e_i and e_{i+1} such that $e_{i+1} = e_i + 1$, starting from the left. Each such pair forms one block, which we call a b-block.*

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Step 3: *By Step 1 and Step 2, the remaining e_i are all distinct and differ at least 2 from each other. Each of these numbers forms one block, which we call a c-block.*

We define $a(e), b(e)$ and $c(e)$ to be the number of a-, b- and c-blocks, respectively, in this decomposition.

For instance, consider $e = (1, 1, 2, 3, 4, 4, 6, 7, 8, 10, 12, 13)$. We go through the steps one by one and mark the blocks in e. There are two a-blocks, namely $(1, 1)$ and $(4, 4)$, hence we get

$$((1, 1), 2, 3, (4, 4), 6, 7, 8, 10, 12, 13).$$

Next, there are three b-blocks, namely $(2, 3), (6, 7)$ and $(12, 13)$, so we get

$$((1, 1), (2, 3), (4, 4), (6, 7), 8, 10, (12, 13)).$$

The remaining elements, 8 and 10, each form a single c-block, which yields

$$((1, 1), (2, 3), (4, 4), (6, 7), (8), (10), (12, 13)).$$

Thus, in this example, $a(e) = 2,\ b(e) = 3$ and $c(e) = 2$.

Remark. This construction implies that if a b-block of the form $(e_i, e_i + 1)$ succeeds a c-block (e_{i-1}), then $e_i \geq e_{i-1} + 2$, since we form the b-blocks by starting from the left.

We now use this decomposition to formulate the lower bound of $\mathrm{Spec}_\Pi(P)$.

Theorem 4.3. *Let $\varphi \in \mathrm{Aut}(P)$. Then $\Pi(\varphi) \geq p^{b(e)+c(e)}$.*

Remark. While (the proof of) Proposition 4.1 tells us how far φ is from being completely diagonalisable, this theorem tells us to what minimal extent every automorphism on P is diagonalisable.

The remainder of this section is devoted to proving this theorem. To do so, we construct a suitable characteristic subgroup of P to which we then aim to apply Lemma 2.7 (recall that a subgroup H of a group G is called *characteristic* if $\varphi(H) = H$ for all $\varphi \in \mathrm{Aut}(G)$). This subgroup is of the following form:

Definition 4.4. *For non-negative integers $d_1, \ldots, d_n$ with $d_i \leq e_i$ for all i, we define $P(d_1, \ldots, d_n)$ to be the subgroup*

$$P(d_1, \ldots, d_n) := \bigoplus_{i=1}^{n} p^{d_i}\mathbb{Z}/p^{e_i}\mathbb{Z}$$

of P.

Equivalently, if we let $\pi : \mathbb{Z}^n \to P$ be the natural projection, then $P(d_1, \ldots, d_n) = \pi(p^{d_1}\mathbb{Z} \oplus \cdots \oplus p^{d_n}\mathbb{Z})$.

We also need to know the behaviour of the automorphism induced by φ on the characteristic subgroup. To that end, we use the general description of automorphisms of finite abelian p-groups, which is proven by Hillar and Rhea [11]. We write $\pi_P : \mathbb{Z}^n \to P$ for the natural projection. If P is clear from the context, we omit the subscript and simply write π. We write elements in $\mathbb{Z}^n$ as column vectors x^T.

Theorem 4.5. ([11, Theorems 3.3 and 3.6]). *Let P be a finite abelian p-group of type e. Put $A(P) := \{M \in \mathbb{Z}^{n\times n} \mid \forall j \leq i \in \{1, \dots, n\} : p^{e_i - e_j} \mid M_{ij}\}$ and let $\pi : \mathbb{Z}^n \to P$ be the natural projection. Define $\Psi : A(P) \to \mathrm{End}(P) : M \mapsto \Psi(M)$, where*

$$\Psi(M) : P \to P : \pi(x^\mathsf{T}) \mapsto \Psi(M)(\pi(x^\mathsf{T})) := \pi(Mx^\mathsf{T}).$$

Then $A(P)$ is a ring under the usual matrix operations, Ψ is a well-defined ring morphism and $\mathrm{Aut}(P)$ is precisely the image of $\{M \in A(P) \mid M \bmod p \in \mathrm{GL}(n, \mathbb{Z}/p\mathbb{Z})\}$ under Ψ.

If $\varphi \in \mathrm{Aut}(P)$ is the image of M under Ψ, we say that φ is *represented by M*.

Theorem 4.6. *Let $d_1, \dots, d_n$ be non-negative integers with $d_i \leq e_i$ for all i. Then $Q := P(d_1, \dots, d_n)$ is characteristic in P if and only if the following two conditions hold:*

(i) for all $i \in \{1, \dots, n-1\}$, we have $d_i \leq d_{i+1}$.
(ii) for all $i \in \{1, \dots, n-1\}$, we have $e_i - d_i \leq e_{i+1} - d_{i+1}$.

Moreover, if Q is characteristic, $d_i < e_i$ for all $i \in \{1, \dots, n\}$ and $\varphi \in \mathrm{Aut}(P)$ is represented by the matrix M as in Theorem 4.5, then the induced automorphism on Q is represented by the matrix $D^{-1}MD$, where $D := \mathrm{Diag}(p^{d_1}, \dots, p^{d_n})$.

Proof. For the first part, we use [12, Theorem 2.2]. There it is proven that the conditions on $d_1, \dots, d_n$ are equivalent with the subgroup $P(e_1 - d_1, \dots, e_n - d_n)$ being characteristic. However, if the n-tuple $d := (d_1, \dots, d_n)$ satisfies the two conditions, then so does the n-tuple $d' := (e_1 - d_1, \dots, e_n - d_n)$, and vice versa. Indeed, the second condition for d implies the first one for d', and by symmetry, the first for d implies the second for d'. Moreover, since $0 \leq d_i \leq e_i$ for all i, also $0 \leq e_i - d_i \leq e_i$ for all i. This proves the first part.

Suppose now that Q is characteristic in P and that $d_i < e_i$ for all $i \in \{1, \dots, n\}$. Fix $\varphi \in \mathrm{Aut}(P)$ and suppose that it is represented by M. In order to use Theorem 4.5 to talk about the matrix representation of automorphisms of Q, we have to write Q as a direct sum of cyclic groups of prime-power order. It is readily verified that

$$\Phi : \bigoplus_{i=1}^{n} \mathbb{Z}/p^{e_i - d_i}\mathbb{Z} \to \bigoplus_{i=1}^{n} p^{d_i}\mathbb{Z}/p^{e_i}\mathbb{Z} : (x_1, \dots, x_n) \mapsto (p^{d_1}x_1, \dots, p^{d_n}x_n)$$

is an isomorphism, which implies that Q is an abelian p-group of type $(e_1 - d_1, \dots, e_n - d_n)$. Let $\tilde{Q}$ denote the group on the left-hand side. Write $\pi_P : \mathbb{Z}^n \to P$ and $\pi_{\tilde{Q}} : \mathbb{Z}^n \to \tilde{Q}$ for the natural projections onto P and $\tilde{Q}$, respectively. Then $\varphi(\pi_P(x^\mathsf{T})) = \pi_P(Mx^\mathsf{T})$ for all $x^\mathsf{T} \in \mathbb{Z}^n$. Let φ_Q denote the induced automorphism on Q and put $\psi := \Phi^{-1} \circ \varphi_Q \circ \Phi$. Now, suppose that $x^\mathsf{T} \in \mathbb{Z}^n$ is such that $\pi_P(x^\mathsf{T}) \in Q$. Then we have

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

$x = (p^{d_1}y_1, \ldots, p^{d_n}y_n)$ for some $y_1, \ldots, y_n \in \mathbb{Z}$. Put $y := (y_1, \ldots, y_n)$. Then $x^\mathsf{T} = Dy^\mathsf{T}$ and therefore, $\pi_{\tilde{Q}}(y^\mathsf{T}) = \Phi^{-1}(\pi_P(x^\mathsf{T}))$. Thus,

$$\begin{aligned}\psi(\pi_{\tilde{Q}}(y^\mathsf{T})) &= (\Phi^{-1} \circ \varphi_Q \circ \Phi \circ \Phi^{-1})(\pi_P(x^\mathsf{T}))\\ &= \Phi^{-1}(\varphi_Q(\pi_P(x^\mathsf{T})))\\ &= \Phi^{-1}(\varphi(\pi_P(x^\mathsf{T})))\\ &= \Phi^{-1}(\pi_P(Mx^\mathsf{T}))\\ &= \Phi^{-1}(\pi_P(MDy^\mathsf{T})).\end{aligned}$$

Note that we can rewrite the equality $\pi_{\tilde{Q}}(y^\mathsf{T}) = \Phi^{-1}(\pi_P(x^\mathsf{T}))$ as

$$\pi_{\tilde{Q}}(y^\mathsf{T}) = \Phi^{-1}(\pi_P(Dy^\mathsf{T})),$$

which holds for arbitrary $y^\mathsf{T} \in \mathbb{Z}^n$. Since we know that $\pi_P(MDy^\mathsf{T}) \in Q$, we know that $D^{-1}MDy^\mathsf{T}$ is a well-defined element of $\mathbb{Z}^n$. Thus, using the equalities above, we get

$$\begin{aligned}\psi(\pi_{\tilde{Q}}(y^\mathsf{T})) &= \Phi^{-1}(\pi_P(MDy^\mathsf{T}))\\ &= \Phi^{-1}(\pi_P(DD^{-1}MDy^\mathsf{T}))\\ &= \pi_{\tilde{Q}}(D^{-1}MDy^\mathsf{T}).\end{aligned}$$

We conclude that the matrix representation of ψ is given by $D^{-1}MD$, which finishes the proof. □

We now construct the aforementioned suitable characteristic subgroup by specifying the non-negative integers d_i.

Definition 4.7. *Given $e \in E(n)$ and its abc-decomposition as in Definition 4.2, we define a new n-tuple $d = (d_1, \ldots, d_n)$ recursively. Put $d_1 := 0$. Given d_i, we define*

$$d_{i+1} := \begin{cases} d_i & \text{if } e_i \text{ and } e_{i+1} \text{ lie in the same block or } e_{i+1} \text{ lies in an } a\text{-block}\\ d_i + 1 & \text{if } e_i \text{ and } e_{i+1} \text{ do not lie in the same block and } e_{i+1} \text{ lies in a } b\text{- or } c\text{-block.}\end{cases}$$

We let $d(e)$ denote this sequence.

For example, given $e = ((1, 1), (2, 3), (4, 4), (6, 7), (8), (10), (12, 13))$ as before with its abc-decomposition marked, we find that

$$d(e) = (0, 0, 1, 1, 1, 1, 2, 2, 3, 4, 5, 5).$$

Lemma 4.8. *Given $e \in E(n)$, its associated n-tuple $d(e)$ has the following properties:*

(i) for all $i, j \in \{1, \ldots, n\}$ with $i < j$, we have $d_i \leq d_j$ with strict inequality if e_j is the first element of a b- or c-block.

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

(ii) *for all $i, j \in \{1, \ldots, n\}$ with $i < j$, we have $d_j - d_i \leq e_j - e_i$, with strict inequality if e_i is the first element of a b- or c-block.*
(iii) *for all $i \in \{1, \ldots, n\}$, we have $d_i < e_i$.*

Proof. The sequence $d(e)$ is non-decreasing by construction, which proves the inequality in the first item. For the strictness part, note that it follows by construction if $i = j-1$, and the general case follows from the chain $d_i \leq d_{j-1} < d_j$.

For the second item, we first prove it for $j = i + 1$. By definition, we have

$$d_{i+1} - d_i = \begin{cases} 0 & \text{if } e_i \text{ and } e_{i+1} \text{ lie in the same block or } e_{i+1} \text{ lies in an } a\text{-block} \\ 1 & \text{if } e_i \text{ and } e_{i+1} \text{ do not lie in the same block and } e_{i+1} \text{ lies in a } b\text{- or } c\text{-block.} \end{cases}$$

We now consider $e_{i+1} - e_i$. We distinguish several cases based on the type of blocks in which e_{i+1} and e_i lie:

- e_i and e_{i+1} lie in the same a-block: then $e_{i+1} - e_i = 0$, by definition of an a-block. Since $d_{i+1} - d_i = 0$, we have $d_{i+1} - d_i \leq e_{i+1} - e_i$.
- e_i and e_{i+1} lie in the same b-block: then $e_{i+1} - e_i = 1$, by definition of a b-block. Since $d_{i+1} - d_i = 0$, we have $d_{i+1} - d_i < e_{i+1} - e_i$.
- e_i lies in an a- or b-block, e_{i+1} does not lie in the same block: then $e_{i+1} - e_i \geq 1$, for otherwise e_{i+1} and e_i would be part of an a-block. Since $d_{i+1} - d_i \leq 1$, we have $d_{i+1} - d_i \leq e_{i+1} - e_i$.
- e_i lies in a c-block, e_{i+1} lies in an a-block: then $e_{i+1} - e_i \geq 1$ for the same reason as in the previous case. Since $d_{i+1} - d_i = 0$, we have $d_{i+1} - d_i < e_{i+1} - e_i$.
- e_i lies in a c-block, e_{i+1} lies in a b-block: then $e_{i+1} - e_i \geq 2$ by the remark following Definition 4.2. Since $d_{i+1} - d_i = 1$, we have $d_{i+1} - d_i < e_{i+1} - e_i$.
- e_i lies in a c-block, e_{i+1} lies in a c-block: then $e_{i+1} - e_i \geq 2$, for otherwise e_{i+1} and e_i would be part of an a-block or one or more b-blocks. Since $d_{i+1} - d_i = 1$, we have $d_{i+1} - d_i < e_{i+1} - e_i$.

We see that in all cases, the inequality $d_{i+1} - d_i \leq e_{i+1} - e_i$ holds. Moreover, in the cases where e_i is the first element of a b- or c-block, we have proven that in fact the strict inequality holds. This finishes the proof for $j = i + 1$.

We prove the general case by induction on $j - i$, with base case $j - i = 1$. Suppose it holds for all $i < j$ with $j - i < k$. Suppose that $j - i = k$. Note that

$$e_j - e_i - d_j + d_i = (e_j - e_{j-1} - d_j + d_{j-1}) + (e_{j-1} - e_i + d_i - d_{j-1}).$$

Both terms on the right-hand side are non-negative by the induction hypothesis; hence, the left-hand side is non-negative as well. Moreover, if e_i is the first element of a b- or c-block, then $e_{j-1} - e_i + d_i - d_{j-1} > 0$, which implies that also $e_j - e_i - d_j + d_i > 0$.

Finally, for the third item, we again proceed by induction. For $i = 1$, we have $d_1 = 0 < 1 \leq e_1$. So, suppose $d_i < e_i$. Then by the second item, we know that $d_{i+1} - d_i \leq e_{i+1} - e_i$. Adding the inequality $d_i < e_i$ side by side yields $d_{i+1} < e_{i+1}$. □

Corollary 4.9. *The subgroup $P(d_1, \ldots, d_n)$ is a characteristic subgroup of P.*

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Proof. By the previous lemma, $d(e)$ satisfies all the conditions from Theorem 4.6. □

We will use the subgroup $Q := P(d_1, \dots, d_n)$ to prove the lower bound on $\Pi(\varphi)$ from Theorem 4.3. Before doing so, we need two additional lemmata.

Lemma 4.10. *Let $\varphi \in \mathrm{Aut}(P)$ be represented by a matrix $M \in \mathbb{Z}^{n\times n}$. Put $D := Diag(p^{d_1}, \dots, p^{d_n})$ and let $i \neq j \in \{1, \dots, n\}$. Then the following hold:*

(i) $(D^{-1}MD)_{ij} \equiv 0 \bmod p$ *if e_j is the first element of a b- or c-block.*
(ii) $(D^{-1}MD)_{jj} \not\equiv 0 \bmod p$ *if e_j is the first element of a b- or c-block.*

Proof. For $a \in \mathbb{Z}$, let $\nu_p(a)$ denote the p-adic valuation of a. First, note that $(D^{-1}MD)_{ij} = D_{ii}^{-1}M_{ij}D_{jj}$, as D is diagonal. Next, by the properties of M and the definition of D, we have that

$$\nu_p((D^{-1}MD)_{ij}) = \nu_p(D_{ii}^{-1}M_{ij}D_{jj}) \geq \begin{cases} e_i - e_j + d_j - d_i & \text{if } i > j \\ d_j - d_i & \text{if } i < j. \end{cases}$$

Suppose that e_j is the first element of a b- or c-block. Then by Lemma 4.8, each of the expressions above is at least 1. Therefore, $(D^{-1}MD)_{ij} \equiv 0 \bmod p$.

For $(D^{-1}MD)_{jj}$, note that $D^{-1}MD$ is the matrix representation of φ_Q, by Theorem 4.6. Moreover, it has to be invertible modulo p in order to define an automorphism on Q/pQ. Since the jth column of $D^{-1}MD$ is zero modulo p everywhere above and below the diagonal entry, the entry on the diagonal must be non-zero modulo p. □

The quotient group P/pP is an abelian group of exponent p, hence it carries a $\mathbb{Z}/p\mathbb{Z}$-vector space structure. Note that the type of P/pP is then given by all ones vector of length n.

Lemma 4.11. *Let $\varphi \in \mathrm{Aut}(P)$ be represented by M. Let $z_i^\top \in \mathbb{Z}^n$ be the vector with a 1 on the ith place and zeroes elsewhere and let $\rho : \mathbb{Z}^n \to P/pP$ be the projection. If we view P/pP as a vector space over $\mathbb{Z}/p\mathbb{Z}$, the matrix representation of the induced automorphism on P/pP with respect to the basis $\{\rho(z_1^\top), \dots, \rho(z_n^\top)\}$ is the matrix $M \bmod p \in \mathrm{GL}(n, \mathbb{Z}/p\mathbb{Z})$.*

Proof. Let $\bar{\pi} : P \to P/pP$ be the projection and let $\bar{\varphi}$ be the induced automorphism on P/pP. Then $\bar{\pi} \circ \pi : \mathbb{Z}^n \to P/pP$ is the natural projection from $\mathbb{Z}^n$ onto P/pP. Therefore, $\rho = \bar{\pi} \circ \pi$. We also have that

$$\bar{\varphi}(\bar{\pi}(\pi(x^\top))) = \bar{\pi}(\varphi(\pi(x^\top))) = \bar{\pi}(\pi(Mx^\top)).$$

Now, this implies that

$$\bar{\varphi}(\rho(z_i^\top)) = \rho(Mz_i^\top),$$

which shows that $M \bmod p$ is the matrix representation of $\bar{\varphi}$. □

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Finally, we prove Theorem 4.3. For a matrix $A \in \mathbb{Z}^{n\times n}$, we write $\bar{A}$ for the matrix $A \bmod p \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$.

Proof of Theorem 4.3. Let $\varphi \in \mathrm{Aut}(P)$ be represented by $M \in \mathbb{Z}^{n\times n}$ and let $d_1, \ldots, d_n, Q$ and D be as before. Since $d_i < e_i$, the group Q has type $(e_1 - d_1, \ldots, e_n - d_n) \in E(n)$. The matrix representation of φ_Q is given by $N := D^{-1}MD$, by Theorem 4.6. Let $\bar{\varphi}$ denote the induced automorphism on the exponent-p factor group Q/pQ. By Lemma 4.11 applied to Q and $\bar{\varphi}$, the matrix representation of $\bar{\varphi}$ with respect to the basis $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ is given by $\bar{N}$. By Lemma 4.10, each column corresponding to a c-block and to a first element of a b-block in N is zero modulo p, except for the element on the diagonal.

Next, note that for $i \in \{1, \ldots, p-1\}$, the automorphism μ_i is represented by the matrix $X_i := \mathrm{Diag}(i, \ldots, i)$. The automorphism $\mu_i \circ \varphi$ is then represented by X_iM and the automorphism $\bar{\mu}_i \circ \bar{\varphi}$ on Q/pQ by $\bar{X}_i\bar{N}$. Fix $j \in \{1, \ldots, n\}$ such that e_j is the first element of a b- or c-block. Then $N_{jj} \not\equiv 0 \bmod p$ by Lemma 4.10; hence, there is a unique $i \in \{1, \ldots, p-1\}$ such that $iN_{jj} \equiv 1 \bmod p$. For that i, we have that the jth column of $\bar{X}_i\bar{N} - \bar{I}_n$ is zero.

Now, let $\mathcal{J}$ be the set of indices j such that e_j is the first element of a b- or c-block. For $i \in \{1, \ldots, p-1\}$, let $\mathcal{J}_i := \{j \in \mathcal{J} \mid iN_{jj} \equiv 1 \bmod p\}$. Note that $\mathcal{J}$ is the disjoint union of $\mathcal{J}_1$ up to $\mathcal{J}_{p-1}$ and that $|\mathcal{J}| = b(e) + c(e)$. Then by the arguments above, $\bar{\mu}_i \circ \bar{\varphi}$ has at least $p^{|\mathcal{J}_i|}$ fixed points. Indeed, for each $j \in \mathcal{J}_i$, the jth column of $\bar{X}_i\bar{N} - \bar{I}_n$ is zero; hence, $\ker(\bar{X}_i\bar{N} - \bar{I}_n)$ has at least dimension $|\mathcal{J}_i|$. By Proposition 2.1, we know that $R(\bar{\mu}_i \circ \bar{\varphi}) = |\mathrm{Fix}(\bar{\mu}_i \circ \bar{\varphi})|$ and $R(\mu_i \circ \varphi) = |\mathrm{Fix}(\mu_i \circ \varphi)|$. By Lemma 2.7, we know that

$$R(\bar{\mu}_i \circ \bar{\varphi}) \leq R\left((\mu_i \circ \varphi)\big|_Q \right) \leq R(\mu_i \circ \varphi).$$

Combining these inequalities, we conclude that

$$\prod_{i=1}^{p-1} |\mathrm{Fix}(\mu_i \circ \varphi)| \geq \prod_{i=1}^{p-1} p^{|\mathcal{J}_i|} = p^{\sum_{i=1}^{p-1} |\mathcal{J}_i|} = p^{|\mathcal{J}|} = p^{b(e)+c(e)}.$$

□

4.3. Filling in the gaps

We now completely determine $\mathrm{Spec}_\Pi(P)$.

Theorem 4.12. *Let P be a finite abelian p-group of type e. Then*

$$\mathrm{Spec}_\Pi(P) = \{p^m \mid m \in \{b(e) + c(e), \ldots, \Sigma(e)\}\}.$$

In order to prove this theorem, we first prove it for three special cases, one for each of the different block types in the abc-decomposition of e: $\mathbb{Z}/p^k\mathbb{Z}$ (corresponding to c-blocks), $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^{k+1}\mathbb{Z}$ (corresponding to b-blocks) and $\bigoplus_{i=1}^n \mathbb{Z}/p^k\mathbb{Z}$ with $n \geq 2$ (corresponding to a-blocks). We start with the first case that corresponds to c-blocks.

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Proposition 4.13. *Let* $k \geq 1$ *be a natural number. Then* $\mathrm{Spec}_\Pi(\mathbb{Z}/p^k\mathbb{Z}) = \{p^i \mid i \in \{1,\dots,k\}\}$.

Proof. Since the type of $\mathbb{Z}/p^k\mathbb{Z}$ is $e = (k)$, $b(e) = 0$ and $c(e) = 1$. The $\subseteq$-inclusion then follows from Proposition 4.1 and Theorem 4.3. Conversely, let $m \in \{1,\dots,k\}$ be arbitrary. Define $\varphi_m : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z} : 1 \mapsto p^m + 1$. Since $m \geq 1$, we know that $\gcd(p^m+1, p) = 1$. Therefore, φ_m defines an automorphism of $\mathbb{Z}/p^k\mathbb{Z}$. Moreover, for $i \in \{1,\dots,p-1\}$, we know by Proposition 2.1 and Lemma 2.6 that

$$|\mathrm{Fix}(\mu_i \circ \varphi_m)| = R(\mu_i \circ \varphi_m) = \gcd(i(p^m+1)-1, p^n) = \begin{cases} p^m & \text{if } i = 1,\\ 1 & \text{otherwise,}\end{cases}$$

as $i(p^m+1) - 1 \equiv i - 1 \not\equiv 0 \bmod p$ when $i \not\equiv 1 \bmod p$. Therefore, $\Pi(\varphi_m) = p^m$. □

Next, we move on the groups corresponding to b-blocks. Proposition 2.4 has the following analogue for $\mathrm{Spec}_\Pi(P)$:

Lemma 4.14. *Let* $P_1,\dots,P_n$ *be abelian* p*-groups and put* $P := P_1 \oplus \cdots \oplus P_n$. *For* $i \in \{1,\dots,n\}$, *let* $\varphi_i \in \mathrm{Aut}(P_i)$. *Put* $\varphi := (\varphi_1,\dots,\varphi_n) \in \mathrm{Aut}(P)$. *Then* $\Pi(\varphi) = \prod_{i=1}^n \Pi(\varphi_i)$. *Consequently,* $\prod_{i=1}^n \mathrm{Spec}_\Pi(P_i) \subseteq \mathrm{Spec}_\Pi(P)$.

Proof. Let μ_i be multiplication by i on P and let $\mu_{i,j}$ denote its restriction to P_j. We then have that

$$\begin{aligned}\Pi(\varphi) &= \prod_{i=1}^{p-1} |\mathrm{Fix}(\mu_i \circ \varphi)|\\ &= \prod_{i=1}^{p-1} \left|\mathrm{Fix}\left((\mu_{i,1}\circ\varphi_1,\dots,\mu_{i,n}\circ\varphi_n)\right)\right|\\ &= \prod_{i=1}^{p-1}\prod_{j=1}^{n} |\mathrm{Fix}(\mu_{i,j}\circ\varphi_j)|\\ &= \prod_{j=1}^{n}\prod_{i=1}^{p-1} |\mathrm{Fix}(\mu_{i,j}\circ\varphi_j)|\\ &= \prod_{j=1}^{n} \Pi(\varphi_j).\end{aligned}$$

□

Proposition 4.15. *Let* $k \geq 1$ *be a natural number and put* $P := \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^{k+1}\mathbb{Z}$. *Then* $\mathrm{Spec}_\Pi(P) = \{p^i \mid i \in \{1,\dots,2k+1\}\}$.

Proof. Since the type of P is $e := (k, k+1)$, $b(e) = 1$ and $c(e) = 0$. Consequently, the $\subseteq$-inclusion again follows from Theorem 4.3 and Proposition 4.1. Conversely, let

$m \in \{1, \ldots, 2k+1\}$. For $m \geq 2$, we can find an automorphism φ with $\Pi(\varphi) = p^m$ using Lemma 4.14 and Proposition 4.13. Thus, suppose that $m = 1$. Consider the matrix

$$M = \begin{pmatrix} 1 & 1 \\ p & 1 \end{pmatrix}.$$

By Theorem 4.5, M defines an automorphism φ on P. First, we determine the fixed points of φ. If $\varphi(\pi((x,y)^\top)) = \pi((x,y)^\top)$, then

$$\begin{cases} x + y \equiv x \bmod p^k \\ px + y \equiv y \bmod p^{k+1}. \end{cases}$$

This implies that $y \equiv 0 \bmod p^k$ as well as $x \equiv 0 \bmod p^k$. Therefore, the fixed points of φ lie in the subgroup $\left\langle \pi((0,p^k)^\top) \right\rangle$ and it is easily verified that $\varphi(\pi((0,p^k)^\top)) = \pi((0,p^k)^\top)$. Consequently, $|\mathrm{Fix}(\varphi)| = p$.

Now, let $i \in \{2, \ldots, p-1\}$ and consider $\mu_i \circ \varphi$. If $(\mu_i \circ \varphi)(\pi((x,y)^\top)) = \pi((x,y)^\top)$, then

$$\begin{cases} ix + iy \equiv x \bmod p^k \\ ipx + iy \equiv y \bmod p^{k+1}. \end{cases}$$

The second congruence yields $(i-1)y \equiv -ipx \bmod p^{k+1}$. Since $i \in \{2, \ldots, p-1\}$, the number $i-1$ has an inverse modulo p^{k+1}, say, j. Substituting $y = -jipx$ in the first congruence then yields

$$x(i - i^2 jp - 1) \equiv 0 \bmod p^k.$$

Since $i - i^2jp - 1 \equiv i - 1 \not\equiv 0 \bmod p$, it is invertible modulo p^k. Therefore, $x \equiv 0 \bmod p^k$. Combined with $(i-1)y \equiv -ipx \bmod p^{k+1}$, this yields $y \equiv 0 \bmod p^{k+1}$. Consequently, $|\mathrm{Fix}(\mu_i \circ \varphi)| = 1$. We conclude that $\Pi(\varphi) = p$. □

Lastly, we deal with the groups corresponding to a-blocks.

Lemma 4.16. *Let n, k be integers with $n \geq 2$, $k \geq 1$. Put $P := \bigoplus_{i=1}^n \mathbb{Z}/p^k\mathbb{Z}$. Let $\varphi \in \mathrm{Aut}(P)$ and let $\bar{\varphi}$ denote the induced automorphism on P/pP. If $\bar{\varphi}$ has no non-trivial fixed points, then neither does φ.*

Proof. We proceed by contraposition. Let φ be represented by M and let $\pi : \mathbb{Z}^n \to P$ be the natural projection. Suppose that $Mx^\top \equiv x^\top \bmod p^k$ for some $x^\top \in \mathbb{Z}^n$ with $\pi(x^\top) \neq 0$. Here, $Mx^\top \equiv x^\top \bmod p^k$ means that $(Mx^\top)_i \equiv x_i^\top \bmod p^k$ for each $i \in \{1, \ldots, n\}$. Write $x^\top = p^l y^\top$ with $y^\top \in \mathbb{Z}^n$ and l maximal. Then $l < k$, otherwise $\pi(x^\top) = 0$. In particular, $y^\top \not\equiv 0 \bmod p$.

Since $Mx^\top \equiv x^\top \bmod p^k$, we find $p^l My^\top \equiv p^l y^\top \bmod p^k$. Dividing by p^l yields $My^\top \equiv y^\top \bmod p^{k-l}$. As $l < k$, we have that $k - l \geq 1$. In particular, $My^\top \equiv y^\top \bmod p$. Thus, with

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

$\rho : P \to P/pP$ denoting the canonical projection, it follows that $\rho(\pi(y^\mathsf{T}))$ is a non-trivial fixed point of $\bar{\varphi}$, since $y^\mathsf{T} \not\equiv 0 \bmod p$. □

Proposition 4.17. *Let n, k be integers with $n \geq 2$ and $k \geq 1$. Put $P := \bigoplus_{i=1}^n \mathbb{Z}/p^k\mathbb{Z}$. Then $\mathrm{Spec}_\Pi(P) = \{p^i \mid i \in \{0, \dots, nk\}\}$.*

Proof. Here, the type of P is $e := (k, \dots, k)$ (with n occurrences of k). Hence, $b(e) = 0$ and $c(e) = 0$, thus the $\subseteq$-inclusion follows from Theorem 4.3 and Proposition 4.1. Conversely, for $m \geq n$, we can find an automorphism φ with $\Pi(\varphi) = p^m$ using Lemma 4.14 and Proposition 4.13. Thus, we are left with arguing that $p^m \in \mathrm{Spec}_\mathrm{R}(P)$ for $m \leq n-1$.

We start with $m = 0$. Using a primitive element of the finite field of p^n elements, we can find a polynomial f_n of degree n that is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Its companion matrix C_{f_n} (seen as matrix over $\mathbb{Z}$) is invertible modulo p. Consequently, it induces, by Theorem 4.5, an automorphism φ_{f_n} of P. Since f_n has no roots in $\mathbb{Z}/p\mathbb{Z}$ (recall that $n \geq 2$), the matrix C_{f_n} has no eigenvalues in $\mathbb{Z}/p\mathbb{Z}$. Therefore, iC_{f_n} does not have eigenvalue 1 for $i \in \{1, \dots, p-1\}$. Thus, Lemma 4.16 implies that $\mu_i \circ \varphi_{f_n}$ has no non-trivial fixed points for each $i \in \{1, \dots, p-1\}$. Consequently, $\Pi(\varphi_{f_n}) = 1$.

Next, we prove the result for $n = 2$. We already know that $\{1, p^2, p^3, \dots, p^{2k}\} \subseteq \mathrm{Spec}_\Pi(P)$. Thus, we have to find an automorphism ψ such that $\Pi(\psi) = p$. An argument similar to the one for Proposition 4.15 shows that the automorphism ψ induced by the matrix

$$M = \begin{pmatrix} 1 & 1 \\ p & 1 \end{pmatrix}$$

does the job. Consequently, $\mathrm{Spec}_\Pi(P) = \{p^i \mid i \in \{0, \dots, 2k\}\}$ for $n = 2$.

We now proceed to general n. So, let $n \geq 3$ be arbitrary. If n is even, write

$$P = \bigoplus_{i=1}^{\frac{n}{2}} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^2.$$

Then the result for $n = 2$ combined with Lemma 4.14 implies that

$$\begin{aligned} \mathrm{Spec}_\Pi\left(\left(\mathbb{Z}/p^k\mathbb{Z}\right)^2\right)^{\left(\frac{n}{2}\right)} &= \{p^i \mid i \in \{0, \dots, 2k\}\}^{\left(\frac{n}{2}\right)} \\ &= \{p^i \mid i \in \{0, \dots nk\}\} \\ &\subseteq \mathrm{Spec}_\Pi(P), \end{aligned}$$

which proves the result for n even. Next, suppose that n is odd. We know that $1 \in \mathrm{Spec}_\Pi(P)$ by the case $m = 0$ above. Write

$$P = \mathbb{Z}/p^k\mathbb{Z} \oplus \bigoplus_{i=1}^{\frac{n-1}{2}} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^2.$$

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Then the result for $n=2$ combined with Lemma 4.14 and Proposition 4.13 yields

$$\begin{aligned}\mathrm{Spec}_{\Pi}(\mathbb{Z}/p^k\mathbb{Z}) \cdot \mathrm{Spec}_{\Pi}\left(\left(\mathbb{Z}/p^k\mathbb{Z}\right)^2\right)^{\left(\frac{n-1}{2}\right)} &= \{p^i \mid i \in \{1,\dots,k\}\} \cdot \\ &\qquad \{p^i \mid i \in \{0,\dots,2k\}\}^{\left(\frac{n-1}{2}\right)} \\ &= \{p^i \mid i \in \{1,\dots,nk\}\} \\ &\subseteq \mathrm{Spec}_{\Pi}(P),\end{aligned}$$

which proves the result for n odd and finishes the proof. □

Finally, we can completely determine $\mathrm{Spec}_{\Pi}(P)$ for arbitrary finite abelian p-groups.

Proof of Theorem 4.12. We factorize P using the abc-decomposition of e, that is, we write

$$P = \left(\bigoplus_{i=1}^{a(e)} (\mathbb{Z}/p^{a_i}\mathbb{Z})^{n_i}\right) \oplus \left(\bigoplus_{i=1}^{b(e)} (\mathbb{Z}/p^{b_i}\mathbb{Z} \oplus \mathbb{Z}/p^{b_i+1}\mathbb{Z})\right) \oplus \left(\bigoplus_{i=1}^{c(e)} \mathbb{Z}/p^{c_i}\mathbb{Z}\right),$$

where all a_i, b_i, c_i are positive integers, the n_i are the lengths of the a-blocks in the abc-decomposition of e and satisfy $n_i \geq 2$ for all $i \in \{1,\dots,a(e)\}$, and where $c_i \geq c_{i-1}+2$ for all $i \in \{1,\dots,c(e)\}$. By Theorem 4.3 and Proposition 4.1, we know that

$$\mathrm{Spec}_{\Pi}(P) \subseteq \{p^i \mid i \in \{b(e)+c(e),\dots,\Sigma(e)\}\}.$$

Conversely, by Lemma 4.14 and Propositions 4.15, 4.13 and 4.17, $\mathrm{Spec}_{\Pi}(P)$ contains

$$\begin{aligned}&\prod_{i=1}^{a(e)} \mathrm{Spec}_{\Pi}\left((\mathbb{Z}/p^{a_i}\mathbb{Z})^{n_i}\right) \cdot \prod_{i=1}^{b(e)} \mathrm{Spec}_{\Pi}\left(\mathbb{Z}/p^{b_i}\mathbb{Z} \oplus \mathbb{Z}/p^{b_i+1}\mathbb{Z}\right) \cdot \prod_{i=1}^{c(e)} \mathrm{Spec}_{\Pi}\left(\mathbb{Z}/p^{c_i}\mathbb{Z}\right) \\ &= \prod_{i=1}^{a(e)} \{p^j \mid j \in \{0,\dots,a_i n_i\}\} \cdot \prod_{i=1}^{b(e)} \{p^j \mid j \in \{1,\dots,2b_i+1\}\} \cdot \prod_{i=1}^{c(e)} \{p^j \mid j \in \{1,\dots,c_i\}\} \\ &= \{p^i \mid i \in \{b(e)+c(e),\dots,\Sigma(e)\}\},\end{aligned}$$

which proves the theorem. □

In particular, since $\mathrm{Spec}_{\Pi}(P) = \mathrm{Spec}_{\mathrm{R}}(P)$ for finite abelian 2-groups, we have the following:

Corollary 4.18. *Let P be a finite abelian 2-group of type e. Then*

$$\mathrm{Spec}_{\mathrm{R}}(P) = \{2^i \mid i \in \{b(e)+c(e),\dots,\Sigma(e)\}\}.$$

At last, by combining Corollaries 2.5 and 4.18 and Proposition 3.2, we can determine the Reidemeister spectrum of an arbitrary finite abelian group.

https://doi.org/10.1017/S0013091523000500 Published online by Cambridge University Press

Theorem 4.19. *Let A be a finite abelian group. Suppose its Sylow 2-subgroup is of type e. Then*

$$\mathrm{Spec}_{\mathrm{R}}(A) = \{d \in \mathbb{N} \mid d \text{ divides } |A| \text{ and } \nu_2(d) \geq b(e) + c(e)\}.$$

In particular, for finite abelian groups of odd order, the Sylow 2-subgroup is trivial. So, in that case, the Reidemeister spectrum takes on a simple form:

Corollary 4.20. *Let A be a finite abelian group of odd order. Then* $\mathrm{Spec}_{\mathrm{R}}(A)$ *is the set of all divisors of* $|A|$.

Remark. The erratic behaviour of the Reidemeister numbers on finite abelian groups disappears when we consider all endomorphisms instead of only the automorphisms. Analogous to the Reidemeister spectrum, the *extended Reidemeister spectrum* of a group G is defined as the set

$$\mathrm{ESpec}_R(G) := \{R(\varphi) \mid \varphi \in \mathrm{End}(G)\}.$$

The analogues of Proposition 2.4 and Corollary 2.5 hold for endomorphisms and the extended Reidemeister spectrum, and the extended Reidemeister spectrum of a finite abelian group is also completely determined by the extended Reidemeister spectrum of its Sylow subgroups. For a finite abelian p-group P, the techniques from Lemma 3.1 and Proposition 3.2 can be used for all prime numbers to prove that $\mathrm{ESpec}_R(P)$ is the set of all divisors of $|P|$. Consequently, the extended Reidemeister spectrum of a finite abelian group A is the set of all divisors of $|A|$. For more details, we refer the reader to [15, Var. 9].

Acknowledgement. The author would like to thank Karel Dekimpe and the anonymous referee for their useful remarks and suggestions, the latter in particular for the interpretation of $\Pi(\varphi)$.

Funding Statement. This researcher was funded by FWO-fellowship fundamental research (file number 1112522N).

Competing Interests. The author declares no competing interests.

References

(1) C. Bleak, A. L. Fel'shtyn and D. L. Gonçalves, Twisted conjugacy classes in R. Thompson's group F, *Pacific J. Math.* **238**(1) (2008), 1–6. doi: 10.2140/pjm.2008.238.1.

(2) K. Dekimpe and D. L. Gonçalves, The R_∞ property for free groups, free nilpotent groups and free solvable groups, *Bull. Lond. Math. Soc.* **46**(4) (2014), 737–746. doi: 10.1112/blms/bdu029.

(3) K. Dekimpe and D. L. Gonçalves, The R_∞ property for abelian groups, *Topol. Methods Nonlinear Anal.* **46**(2) (2015), 773–784. doi: 10.12775/TMNA.2015.066.

(4) K. Dekimpe, T. Kaiser and S. Tertooy, The Reidemeister spectra of low dimensional crystallographic groups, *J. Algebra* **533** (2019), 353–375. doi: 10.1016/j.jalgebra.2019.04.038.

(5) K. Dekimpe, S. Tertooy and A. R. Vargas, Fixed points of diffeomorphisms on nilmanifolds with a free nilpotent fundamental group, *Asian J. Math.* **24**(1) (2020), 147–164. doi: 10.4310/AJM.2020.v24.n1.a6.

(6) A. L. Fel'shtyn and D. L. Gonçalves, Twisted conjugacy classes of automorphisms of Baumslag-Solitar groups, *Algebra Discrete Math.* **5**(3) (2006), 36–48.

(7) A. L. Fel'shtyn and R. Hill, The Reidemeister zeta function with applications to Nielsen Theory and a connection with Reidemeister torsion, *K-Theory* **8**(4) (1994), 367–393. doi: 10.1007/BF00961408.

(8) A. L. Fel'shtyn and T. Nasybullov, The R_∞ and S_∞ properties for linear algebraic groups, *J. Group Theory* **19**(5) (2016), 901–921. doi: 10.1515/jgth-2016-0004.

(9) B. Goldsmith, F. Karimi and N. White, On the Reidemeister spectrum of an Abelian group, *Forum Math.* **31**(1) (2019), 199–214. doi: 10.1515/forum-2017-0184.

(10) D. L. Gonçalves and P. N. Wong, Twisted conjugacy classes in nilpotent groups, *J. für die Reine und Angew. Math.* **2009**(633) (2009), 11–27. doi: 10.1515/CRELLE.2009.058.

(11) C. J. Hillar and D. L. Rhea, Automorphisms of finite abelian groups, *Amer. Math. Monthly* **114**(10) (2007), 917–923. doi: 10.1080/00029890.2007.11920485.

(12) B. Kerby and E. Rode, Characteristic subgroups of finite abelian groups, *Comm. Algebra* **39**(4) (2011), 1315–1343. doi: 10.1080/00927871003591843.

(13) T. Mubeena and P. Sankaran, Twisted conjugacy classes in abelian extensions of certain linear groups, *Canad. Math. Bull.* **57**(1) (2014), 132–140. doi: 10.4153/CMB-2012-013-7.

(14) V. Roman'kov, Twisted conjugacy classes in nilpotent groups, *J. Pure Appl. Algebra* **215**(4) (2011), 664–671. doi: 10.1016/j.jpaa.2010.06.015.

(15) P. Senden, How does the structure of a group determine its Reidemeister spectrum?. PhD thesis, KU Leuven, 2023.

(16) P. Senden, *The Reidemeister spectrum of split metacyclic groups*, arXiv:2109.12892 [math.GR], 2021. doi: 10.48550/arXiv.2109.12892.

(17) P. Senden, Twisted conjugacy in direct products of groups, *Comm. Algebra* **49**(12) (2021), 5402–5422. doi: 10.1080/00927872.2021.1945615.

(18) J. Taback and P. N. Wong, *A note on twisted conjugacy classes and generalized Baumslag-Solitar groups*, 2008. arXiv: 0606284v3 [math.GR]. doi: 10.48550/arXiv.math/0606284.

(19) S. Tertooy, *TwistedConjugacy, Computation with twisted conjugacy classes, Version 2.0.0.* https://sTertooy.github.io/TwistedConjugacy/. GAP package. 2021.