http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (202x), pp. xx-xx.
© 202x University of Isfahan
www.ui.ac.ir

ORBITS CLASSIFYING EXTENSIONS OF PRIME POWER ORDER GROUPS

OIHANA GARAIALDE OCAÑA* AND MIMA STANOJKOVSKI

Abstract. The strong isomorphism classes of extensions of finite groups are parametrized by orbits of a prescribed action on the second cohomology group. We study these orbits in the case of extensions of a finite abelian p-group by a cyclic factor of order p. As an application, we compute the number and sizes of these orbits when the initial p-group is generated by at most 3 elements.

1. Introduction

An established way of constructing finite groups is via *group extensions*. A group E is said to be an *extension* of a group G by a group N if there exists a short exact sequence of groups

$$1 \to N \longrightarrow E \longrightarrow G \to 1. \tag{1.1}$$

Every finite group can be constructed inductively in this way by iterating extensions by simple (composition) factors. In particular, if p is a prime number, then every finite p-group can be realized via consecutive extensions with kernel N of order p and, moreover, such extensions are *central* (it is indeed well-known that non-trivial p-groups have non-trivial center). An extension like (1.1) is called central if N is central in E equivalently, if the action of G on N is trivial. Every group of order p^n being a central extension of a group of order p^{n-1} by $\mathbb{F}_p$, one could hope to *classify p-groups by classifying extensions*. The famous p-group generation algorithm of Newman and O'Brien [16] builds upon a structural refinement of this idea.

Communicated by Gustavo Adolfo Fernández-Alcober.

MSC(2010): Primary: 20D15, Secondary: 20E22, 20J05, 20J06.

Keywords: Cohomology of finite p-groups, group extensions, strong isomorphism, orbit sizes.

Manuscript Type: Research Paper.

Received: 13 October 2020, Accepted: 25 December 2022.

*Corresponding author.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651 .

A challenging task in the framework of classifying groups via extensions is that of determining whether two extensions E and E' are isomorphic as groups, in symbols $E \cong E'$. Because of this, it is sometimes worth it to start by testing isomorphism in a slightly stronger form. Two group extensions

$$1 \to N \xrightarrow{\iota} E \longrightarrow G \to 1 \quad \text{and} \quad 1 \to N \xrightarrow{\iota'} E' \longrightarrow G \to 1$$

of G by N are *strongly isomorphic* (following [8, Def. 17.20]), denoted $E \cong_s E'$, if there exists an isomorphism $\phi : E \to E'$ inducing an isomorphism $\iota(N) \to \iota'(N)$. The extensions E and E' are *equivalent*, denoted $E \sim E'$, if ϕ induces the identity on both $\iota(N) \to \iota'(N)$ and $G \to G$. In particular, it holds that

$$E \sim E' \implies E \cong_s E' \implies E \cong E'$$

which in a straightforward manner implies that

$$\#\{\text{isomorphism classes}\} \leq \#\{\text{strong isomorphism classes}\} \leq \#\{\text{equivalence classes}\}.$$

The equivalence classes of extensions of G by N are in bijection with the elements of the *second cohomolo group* $\mathrm{H}^2(G;N)$, while the strong isomorphism classes are parametrized by orbits of $A = \mathrm{Aut}(G) \times \mathrm{Aut}(N)$ on $\mathrm{H}^2(G;N)$; cf. Theorem A. If $C^2(G;N)$ denotes the collection of 2-cocycles $G \times G \to N$ and composition in $\mathrm{Aut}(G)$ is taken from right to left (i.e. $\tau \circ \sigma(x) = \tau(\sigma(x))$), then the action of A on $C^2(G;N)$ is defined from the following data:

- the right diagonal action of $\mathrm{Aut}(G)$ on $C^2(G;N)$ given by

$$C^2(G;N) \times \mathrm{Aut}(G) \longrightarrow C^2(G;N), \quad (c,\sigma) \longmapsto ((x,y) \mapsto c(\sigma(x),\sigma(y))),$$

- the natural left action of $\mathrm{Aut}(N)$ on $C^2(G;N)$ given by

$$\mathrm{Aut}(N) \times C^2(G;N) \longrightarrow C^2(G;N), \quad (\lambda,c) \longmapsto ((x,y) \mapsto \lambda(c(x,y))).$$

The last actions respect coboundaries and therefore, if $\mathrm{Aut}(N)$ is abelian, we derive the following left action of A on $\mathrm{H}^2(G;N)$:

$$A \longrightarrow \mathrm{Sym}(\mathrm{H}^2(G;N)), \quad (\sigma,\lambda) \ \mapsto \ ([c] \mapsto [\lambda c \sigma^{-1}]),$$

where $[c]$ denotes the cohomology class of c. The following result is a weaker version of [1, Thm. 4.7].

Theorem A. *Let p be a prime number, G a finite group, and N a trivial $\mathbb{F}_pG$-module. Then the set of strong isomorphism classes of extensions of G by N is in natural bijection with the collection of orbits of the action of A on $\mathrm{H}^2(G;N)$.*

We have decided to state the last result only in terms of central extensions, because those are the ones we will be concerned with. The more general version from [1] allows N to be any $\mathbb{F}_pG$-module (actually the proof works for any $\mathbb{Z}G$-module) and parametrizes strong isomorphism classes in terms of an action of the *compatible pairs* of A (in our case, all elements of A). Compatible pairs were introduced in [17] in the context of computing automorphism groups of extensions. A version of Theorem A for non-fixed

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

module structure on N can be found in [11, Satz 1.2]. Many are the applications of Theorem A in the literature: see for example [1],[6],[4],[5],[9]. Moreover, results similar to Theorem A are employed to count Lie algebras by extensions; see for instance [13, Thm. 2].

Despite their relevance to the isomorphism problem for finite groups, not much is known about the sizes of the orbits from Theorem A. In the present paper, we concern ourselves with the case in which G is an abelian p-group and $N = \mathbb{F}_p$: our goal is to determine the orbits of the action of $\tilde{A} = \mathrm{Aut}(G) \times \mathbb{F}_p^*$ on $\mathrm{H}^2(G;\mathbb{F}_p)$. We remark that, under these last assumptions, the extensions parametrized by $\mathrm{H}^2(G;\mathbb{F}_p)$ are abelian or with commutator subgroup of order p. The latter class of groups has been classified in [2] with respect to the group order and relies on the classification of bilinear forms. Our techniques are different and the results are difficult to compare outside of small order cases. Moreover, we hope that our approach can be generalized to the study of extensions where N is cyclic or elementary abelian.

1.1. **Summary of the main results.** Let p be an odd prime number and let G be a finite abelian p-group. In this paper we are concerned with the orbits of the action of $\tilde{A} = \mathrm{Aut}(G)\times\mathbb{F}_p^*$ on $\mathrm{H}^2(G;\mathbb{F}_p)$, where $\mathbb{F}_p$ is viewed as a trivial $\mathbb{F}_pG$-module. In this very case, such orbits parametrize the isomorphism classes of extensions of G by $\mathbb{F}_p$, see Proposition 4.4, and we determine them completely when G is generated by at most 3 elements. For a minimal generating set of larger size, we describe the orbits within a specific $\tilde{A}$-stable subset of $\mathrm{H}^2(G;\mathbb{F}_p)$ as we now explain.

Under our assumptions, $\mathrm{H}^2(G;\mathbb{F}_p)$ is an $\mathbb{F}_p$-vector space endowed with a map

$$\cup : \mathrm{Hom}(G,\mathbb{F}_p) \times \mathrm{Hom}(G,\mathbb{F}_p) \to \mathrm{H}^2(G;\mathbb{F}_p)$$

corresponding to the restriction of the *cup product* in the full cohomology ring of G. A distinguished subspace of $\mathrm{H}^2(G;\mathbb{F}_p)$ is $\mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p)$, which parametrizes the equivalence classes of abelian extensions of G by $\mathbb{F}_p$ and, together with the $\mathbb{F}_p$-span of the image of $\cup$, figures in the following convenient decomposition as $\mathbb{F}_p\tilde{A}$-modules: $\mathrm{H}^2(G;\mathbb{F}_p) = \mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p) \oplus \langle \mathrm{Im}\cup \rangle$.

The $\tilde{A}$-stable subset we analyze is $\mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p) \times \mathrm{Im}\cup$ and we do this "projectively". We write $V = G/pG$, $d = \dim_{\mathbb{F}_p}(V)$, and $\mathcal{G}(k,V)$ for the collection of subspaces of dimension k of V. We show that there is a somewhat natural bijection of $\tilde{A}$-sets

$$\mathbb{P}\,\mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p) \times \mathbb{P}\,\mathrm{Im}\cup \to \mathcal{G}(d-1,V) \times \mathcal{G}(d-2,V)$$

which shifts the original problem to the determination of $\mathrm{Aut}(G)$-orbits of pairs of subgroups of G. Our main Theorem 6.1 gives a combinatorial description of the $\tilde{A}$-orbits of $\mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p) \times \mathrm{Im}\cup$ in terms of vectors of data parametrizing the $\tilde{A}$-orbits of such pairs and thus allows the computation of the orbit sizes. Moreover, this result yields a lower bound on the number of isomorphism types of extensions of G by $\mathbb{F}_p$ and, specifically, the number of isomorphism classes of extensions with centre of index at most p^2. It is worth mentioning that the orbit sizes are, under our assumptions, given by vectors of polynomials in p. Though maybe not quite surprising given the "low complexity" of the groups we consider, this raises the question of whether this is always the case.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

We remark that our results also hold true for many 2-groups; see Section 1.2.

1.2. **Assumptions and notation.** In this section, we set the notation that will hold throughout the whole paper. Let p be a prime number and let G be a finite abelian p-group, written in additive notation, of exponent $\exp(G) = p^n$ and with $\mathrm{d}(G) = r + 1 \geq 1$, i.e. G is $(r+1)$-generated but not r-generated. In particular, G is non-trivial and $n \geq 1$. Let, moreover, C denote a cyclic group of order p^{n+1} equipped with a trivial G-action. For each subgroup K of G and nonnegative integer m, we write $K[m]$ for the m-th torsion subgroup of K, i.e. $K[m] = \{x \in K \mid mx = 0\}$. We now fix a decomposition of G into cyclic summands. For this, we let

- t a positive integer,
- integers $1 \leq n_1 \leq n_2 \leq \cdots \leq n_t = n$,
- integers $1 \leq r_1, \ldots, r_t$ such that $r + 1 = r_1 + \cdots + r_t$,
- for each $j \in \{1, \ldots, t\}$ and $k \in \{1, \ldots, r_j\}$, a cyclic group I_{jk} of order p^{n_j},
- for each $j \in \{1, \ldots, t\}$, a free $\mathbb{Z}/(p^{n_j})$-module I_j of rank r_j,

be such that

$$G = \bigoplus_{j=1}^{t} I_j = \bigoplus_{j=1}^{t} \bigoplus_{k=1}^{r_j} I_{jk} \text{ with } I_j = \bigoplus_{k=1}^{r_j} I_{jk}.$$

We additionally assume that, if $p = 2$, then $n_1 > 1$ holds in the above decomposition, equivalently G does not admit cyclic factors of order 2: the reason for this choice is clarified in Remark 2.1.

We fix generators γ_{jk} of I_{jk} and $\tilde{\gamma}$ of C. We denote by γ the image of $\tilde{\gamma}$ under the natural projection $C \to C/p^nC$, and so γ generates C/p^nC. Set, moreover, $V = G/pG$ and denote by π the natural projection $G \to V$. For each $j \in \{1, \ldots, t\}$ and $k \in \{1, \ldots, r_j\}$, we write $v_{jk} = \pi(\gamma_{jk})$ and observe that, as a consequence of their definition, the v_{jk}'s form a basis of V. Denote by $\widehat{V} = \mathrm{Hom}(V, \mathbb{F}_p)$ the dual of V of which a basis is given by the homomorphisms $v_{jk}^* : V \to \mathbb{F}_p$ satisfying

$$v_{jk}^*(v_{hl}) = \delta_{(j,k),(h,l)} = \begin{cases} 1 & \text{if } (j,k) = (h,l), \\ 0 & \text{otherwise.} \end{cases}$$

Let $\phi_1 : V \to \widehat{V}$ denote the isomorphism of vector spaces defined by $v_{jk} \mapsto v_{jk}^*$. Write $\mathrm{Aut}(G)$ for the automorphism group of G and, for each $\sigma \in \mathrm{Aut}(G)$, denote by $\overline{\sigma}$ the element of $\mathrm{Aut}(V)$ that is induced by σ. Write $\mathbb{Z}_p$ for the ring of p-adic integers, $\mathbb{Z}_p^*$ for its group of units, and set $A = \mathrm{Aut}(G) \times \mathbb{Z}_p^*$. Denote by $\mathbb{F}_p$ the field of p elements, considered as a trivial $\mathbb{Z}_pG$-module, and by $\mathbb{F}_p^*$ its group of units. We now define a series of left actions of A on sets associated to G. For K a finite $\mathbb{Z}_pG$-module, the group A acts on

- $\mathrm{H}^m(G; K)$ via the map

$$A \longrightarrow \mathrm{Sym}(\mathrm{H}^m(G;K)) \text{ defined by } (\sigma, \lambda) \mapsto ([c] \mapsto \lambda[c]\sigma^{-1} = [\lambda c \sigma^{-1}]); \tag{1.2}$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

- V via the map

$$A \longrightarrow \mathrm{Aut}(V) \text{ defined by } (\sigma, \lambda) \ \mapsto \ (v \mapsto \lambda\overline{\sigma}(v)); \tag{1.3}$$

- the collection $\mathcal{S}_G$ of subgroups of G via

$$A \to \mathrm{Sym}(\mathcal{S}_G) \text{ defined by } (\sigma, \lambda) \mapsto (H \mapsto \sigma(H)); \tag{1.4}$$

- $\mathbb{P}\,\mathrm{H}^2(G; K)$ via the map

$$A \longrightarrow \mathrm{Sym}(\mathbb{P}\,\mathrm{H}^2(G; K)) \text{ defined by } (\sigma, \lambda) \ \mapsto \ ([c] \mapsto [c\sigma^{-1}]). \tag{1.5}$$

If two objects X and Y belong to the same A-orbit, we write $X \sim_A Y$. We write A_X meaning the stabilizer of X in A and, if two elements Y, Z are in the same orbit under the induced action by A_X, we write $Y \sim_{A_X} Z$. To lighten the notation, if $X = [c] \in \mathrm{H}^2(G; \mathbb{F}_p)$, we write A_c instead of $A_{[c]}$.

1.3. **Organization and strategy.** We describe here briefly the internal structure of this article and the strategy behind the proofs of our main results.

In Section 2, we briefly describe the cohomological objects we will be dealing with and list a number of their properties; we also provide more detailed references for the interested reader. We show in Section 2.4 that the abelian extensions of G are parametrized by the elements in the image of the *higher order Bockstein homomorphism*. In Sections 2.5 and 2.6, we give two correspondences involving respectively $\mathrm{Ext}^1_{\mathbb{Z}_p G}(G, \mathbb{F}_p)$ and the image of the cup product $\cup : \mathrm{Hom}(G, \mathbb{F}_p) \times \mathrm{Hom}(G, \mathbb{F}_p) \to \mathrm{H}^2(G; \mathbb{F}_p)$ and interpret the A-orbits thereof in terms of orbits of subspaces of V.

In Section 3, we define the numbers that will allow us to describe the A-orbits in $\mathrm{H}^2(G; \mathbb{F}_p)$ combinatorially and prove some compatibility results regarding the correspondences defined in the previous section. Such numbers are called the *levels* of the pairs of subgroups associated to a given element of $\mathrm{Ext}^1_{\mathbb{Z}_p G}(G, \mathbb{F}_p) \times \mathrm{Im}\cup$ and tell us how the two subgroups "relatively sit in G".

Section 4 is devoted to the analysis of the action of A on $\mathrm{Ext}^1_{\mathbb{Z}_p G}(G, \mathbb{F}_p)$. Here we heavily rely on the properties of the Bockstein homomorphism and the equivalence relation it induces on $\mathrm{Hom}(G, C/(p^n C))$, which we name the *Bockquivalence relation*. Roughly speaking, the Bockstein homomorphism controls the map $x \mapsto x^p$ on the extensions of G by $\mathbb{F}_p$. In this section, we also show that in fact the strong isomorphism classes coincide with the isomorphism classes of extensions of G by $\mathbb{F}_p$.

In Section 5, we describe the orbits of $\mathrm{Im}\cup$ under the action of A_c, where $[c]$ denotes an element in $\mathrm{Ext}^1_{\mathbb{Z}_p G}(G, \mathbb{F}_p)$. We do this by separating the cases according to the value of the *c-index*, which we defined in Section 3.

Section 6 collects our main result, applications of it, and some closing remarks. In Section 6.1, we give and prove our Main Theorem 6.1 combining the efforts from Sections 4 and 5. In Sections 6.2 and 6.3 we give respectively the orbit counts for 2-generated and 3-generated groups. In Section 6.4, we give an example and ideas for future work.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

2. Homological algebra

The aim of this section is to set the notation that will be used in the next sections and to shortly describe the objects we will be working with. For reasons of brevity, we work under the assumptions listed in Section 1.2; for a more general view on the topic, we refer the reader to [3], [7], [19].

2.1. **Cohomology of groups.** Throughout we suppose that, for $n \geq 0$, the n-th cohomology group $\mathrm{H}^n(G;\mathbb{F}_p)$ of G with coefficients in $\mathbb{F}_p$ is computed by applying the left-exact functor $\mathrm{Hom}_{\mathbb{F}_pG}(;\mathbb{F}_p)$ to the standard or bar resolution $B_n(G;\mathbb{Z})$ of $\mathbb{Z}$, i.e. $\mathrm{H}^n(G;\mathbb{F}_p) = \mathrm{H}^n(C^m(G;\mathbb{F}_p),\partial_m)$, where

$$C^m(G;\mathbb{F}_p) = \{f : G^m = \underbrace{G \times \cdots \times G}_{m \text{ times}} \to \mathbb{F}_p \text{ functions}\}$$

and $\partial_m : C^m(G;\mathbb{F}_p) \to C^{m+1}(G;\mathbb{F}_p)$ is defined by sending $f \in C^m(G;\mathbb{F}_p)$ to

$$\begin{aligned}\partial_m(f)(g_1,\ldots,g_{m+1}) =& f(g_2,\ldots,g_{m+1}) + \sum_{i=1}^{m}(-1)^i f(g_1,\ldots,g_i+g_{i+1},\ldots,g_{m+1})\\ &+ (-1)^{m+1} f(g_1,\ldots,g_m).\end{aligned}$$

If $f \in C^m(G;\mathbb{F}_p)$, we say that f has degree m, written $|f| = m$, and we denote by $[f]$ its cohomology class in $\mathrm{H}^m(G;\mathbb{F}_p)$. The cohomology group of G with coefficients in $\mathbb{F}_p$ is the graded abelian group

$$\mathrm{H}^*(G;\mathbb{F}_p) = \bigoplus_{n\geq 0} \mathrm{H}^n(G;\mathbb{F}_p).$$

For all integers $n, m \geq 0$, the cup product $\cup : C^n(G;\mathbb{F}_p) \times C^m(G;\mathbb{F}_p) \to C^{n+m}(G;\mathbb{F}_p)$ is defined by sending the pair $(c,d) \in C^n(G;\mathbb{F}_p) \times C^m(G;\mathbb{F}_p)$ to the map $G^n \times G^m \to \mathbb{F}_p$ that is given by

$$(x,y) \longmapsto (c \cup d)(x,y) = c(x)d(y).$$

By slight abuse of notation, we also write $\cup$ for the induced cup product in cohomology

$$\cup : \mathrm{H}^n(G;\mathbb{F}_p) \times \mathrm{H}^m(G;\mathbb{F}_p) \longrightarrow \mathrm{H}^{n+m}(G;\mathbb{F}_p),$$

i.e., for each $x \in G^n$ and $y \in G^m$, the cup product of $[c] \in \mathrm{H}^n(G;\mathbb{F}_p)$ and $[d] \in H^m(G;\mathbb{F}_p)$ is given by

$$[c] \cup [d](x,y) = [c \cup d](x,y) \in \mathrm{H}^{n+m}(G;\mathbb{F}_p).$$

For more on cup products, see for example [3, Sec. I.5, Sec. V.3]. We remark that the abelian group $\mathrm{H}^*(G;\mathbb{F}_p)$ together with the cup product is a graded-commutative ring, equivalently, for $[c] \in \mathrm{H}^n(G;\mathbb{F}_p)$ and $[d] \in \mathrm{H}^m(G;\mathbb{F}_p)$, the equality $[c] \cup [d] = (-1)^{nm}[d] \cup [c]$ holds.

In this paper we will work only with the first $\mathrm{H}^1(G;\mathbb{F}_p)$ and the second $\mathrm{H}^2(G;\mathbb{F}_p)$ cohomology groups. These have a group theoretic interpretation and are very well understood. Since the action of G on $\mathbb{F}_p$ is trivial, we have $\mathrm{H}^1(G;\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p)$. Moreover, there is a one-to-one correspondence between the cohomology classes $[c] \in \mathrm{H}^2(G;\mathbb{F}_p)$ and the equivalence classes of (central) group extensions

$$0 \longrightarrow \mathbb{F}_p \xrightarrow{\iota} E \xrightarrow{\rho} G \longrightarrow 0, \tag{2.1}$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

where the equivalence is defined as follows. For a group H, let id_H denote the identity map on H. Two group extensions E and E' are *equivalent* if there exists an isomorphism $\varphi : E \to E'$ making the next diagram commutative

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F}_p & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{\mathbb{F}_p}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_G} & & \\ 0 & \longrightarrow & \mathbb{F}_p & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

Following [3, Sec. IV. 3], we outline the aforementioned correspondence. Given an extension E of G by $\mathbb{F}_p$ as in (2.1), we fix a set-theoretic map $s : G \to E$ with $\rho \circ s = \mathrm{id}_G$ and define $c \in C^2(G; \mathbb{F}_p)$ to be the 2-cocycle such that, for each $g_1, g_2 \in G$, the equality

$$\iota(c(g_1, g_2)) = s(g_1)s(g_2)s(g_1 + g_2)^{-1}$$

is satisfied. It can be shown that $[c]$ does not depend on the choice of s. Similarly, given $[c] \in \mathrm{H}^2(G; \mathbb{F}_p)$, we construct a group extension as in (2.1). For this, we choose a representative $c \in C^2(G; \mathbb{F}_p)$ and consider the set $E_c = G \times \mathbb{F}_p$, endowed with the product

$$(g_1, m_1) \cdot (g_2, m_2) = (g_1 + g_2, m_1 + m_2 + c(g_1, g_2)).$$

With the definition of

$$\begin{aligned} \iota : \mathbb{F}_p \longrightarrow E_c, \quad m \longmapsto \iota(m) = (0, m), \\ \rho : E_c \longrightarrow G, \quad (g, a) \longmapsto \rho(g, a) = g, \end{aligned}$$

we get that $0 \to \mathbb{F}_p \xrightarrow{\iota} E_c \xrightarrow{\rho} G \to 0$ is indeed a group extension.

2.2. **Cohomology of abelian p-groups.** We proceed by describing the cohomology ring structure for finite abelian p-groups. To that aim, we observe that the cohomology ring of the cyclic p-group $\mathbb{Z}/(p^k)$ of order p^k is given, as a graded ring, by the following:

$$\mathrm{H}^*(\mathbb{Z}/(p^k); \mathbb{F}_p) \cong \Lambda(y) \otimes \mathbb{F}_p[x] \text{ for } \begin{cases} k \geq 1 & \text{if } p > 2, \\ k > 1 & \text{if } p = 2. \end{cases}$$

Here $\Lambda(\cdot)$ denotes the exterior algebra and the generators $[y], [x] \in \mathrm{H}^*(\mathbb{Z}/(p^k); \mathbb{F}_p)$ are of degrees $|y| = 1$ and $|x| = 2$. Following the notation and assumptions in Section 1.2, using the Künneth formula for cohomology [7, Sec. 2.5] and the fact that $\mathbb{F}_p$ is a field, we obtain the following isomorphism of graded rings

$$\mathrm{H}^*(G; \mathbb{F}_p) \cong \Lambda(y_1, \ldots, y_{r+1}) \otimes \mathbb{F}_p[x_1, \ldots, x_{r+1}], \tag{2.2}$$

where the generators $[y_i]$ and $[x_i]$ have degrees $|y_i| = 1$ and $|x_i| = 2$ for $i \in \{1, \ldots, r+1\}$ (see [3, Sec. V.6]). Moreover, for every $i \in \{1, \ldots, r+1\}$, the element x_i can be chosen to be $\beta(y_i)$, where β is an appropriate higher order Bockstein homomorphism; see [12, Sec. 6.2, Proof of Thm. 6.21] and Section 2.4.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Remark 2.1. *If we allowed p to be 2 with not all n_j's at least 2, then the cohomology ring of G would not be isomorphic to the tensor product in (2.2) anymore (see for instance [7, Sec. 3.3]). For this reason, we excluded such cases from our study.*

As we have seen in Section 2.1, the elements of $\mathrm{H}^2(G;\mathbb{F}_p)$ correspond to central extensions of G by $\mathbb{F}_p$; we denote by $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ the subset of those that correspond to abelian extensions. We remark that $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ is in fact the abelian group $\mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p)$ [19, Thm. 3.4.3], whose elements are the abelian extension classes of $\mathbb{Z}_pG$-modules with trivial G-action and whose operation is the Baer sum; for more detail, see for example [19, Sec. 3.4]. Moreover, $\mathrm{H}^2(G;\mathbb{F}_p)$ decomposes as a sum of the following $\mathbb{F}_p$-vector spaces (see [7, Sec. 3.4] or [17, 11.4.16 and 11.4.18]):

$$\mathrm{H}^2(G;\mathbb{F}_p) = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \oplus \langle \mathrm{Im}\cup \rangle \cong \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \oplus \langle y_i \cup y_j \ : 1 \leq i < j \leq r+1 \rangle.$$

In addition, we have that

$$\dim_{\mathbb{F}_p} \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) = r+1 \text{ and } \dim_{\mathbb{F}_p} \Lambda^2(y_1,\dots,y_{r+1}) = \binom{r+1}{2}$$

so, in particular, if G is cyclic, then $\mathrm{H}^2(G;\mathbb{F}_p) = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$.

2.3. **Pontryagin dual.** We define here the Pontryagin dual of G following [14, Ch. 3] and stress that this notion can be extended to arbitrary locally compact groups. Let $\mathbb{T} = \{z \in \mathbb{C} : \ |z| = 1\}$ denote the circle group.

Definition 2.2. *The Pontryagin dual of G is the abelian group $\widehat{G} = \mathrm{Hom}(G,\mathbb{T})$ consisting of all homomorphisms from G to $\mathbb{T}$.*

Since the exponent of G is p^n, each element of $\widehat{G} = \mathrm{Hom}(G,\mathbb{T})$ will have image contained in $\mathbb{T}[p^n]$, the p^n-th torsion subgroup of $\mathbb{T}$, which is cyclic of order p^n. Without loss of generality, we identify $\widehat{G}$ with $\mathrm{Hom}(G, C/(p^nC))$. As the Hom functor commutes with direct sums, we have that

$$\begin{aligned}\widehat{G} = \mathrm{Hom}(G,C/(p^nC)) &= \mathrm{Hom}(\bigoplus_{j=1}^{t} I_j, C/(p^nC)) \cong \bigoplus_{j=1}^{t} \mathrm{Hom}(I_j, C/(p^nC)) = \bigoplus_{j=1}^{t} \widehat{I_j} \\ &= \mathrm{Hom}(\bigoplus_{j=1}^{t}\bigoplus_{k=1}^{r_j} I_{jk}, C/(p^nC)) \cong \bigoplus_{j=1}^{t}\bigoplus_{k=1}^{r_j} \mathrm{Hom}(I_{jk}, C/(p^nC)) = \bigoplus_{j=1}^{t}\bigoplus_{k=1}^{r_j} \widehat{I_{jk}};\end{aligned}$$

see for example also [14, Thm. 13]. The last series of maps induces the following isomorphism

$$\widehat{\phi_1} : G \longrightarrow \widehat{G} = \mathrm{Hom}(G, C/(p^nC)), \quad \gamma_{jk} \mapsto (\gamma_{jk}^* : \gamma_{ih} \longmapsto \delta_{(j,k),(i,h)} p^{n-n_j}\gamma), \tag{2.3}$$

which generalizes the isomorphism $\phi_1 : V \to \widehat{V}$ from Section 1.2.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

2.4. **Higher Bockstein homomorphism.** We give here another characterization of $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$. To this end, we let A act on $\mathrm{Hom}(G,C)$ and on $\mathrm{Hom}(G,C/p^nC)$ as described in (1.2) and observe that the natural short exact sequence

$$0 \longrightarrow C[p] \longrightarrow C \xrightarrow{\pi} C/(p^nC) \longrightarrow 0,$$

induces a long exact sequence of $\mathbb{Z}_pA$-modules

$$\begin{array}{ccccccc} 0 & \longrightarrow & C[p] & \longrightarrow & C & \longrightarrow & C/(p^nC) \\ & & \mathrm{Hom}(G,C[p]) & \longrightarrow & \mathrm{Hom}(G,C) & \xrightarrow{\pi_B} & \mathrm{Hom}(G,C/(p^nC)) \\ & & \mathrm{H}^2(G;C[p]) & \longrightarrow & \mathrm{H}^2(G;C) & \longrightarrow & \mathrm{H}^2(G;C/(p^nC)) \longrightarrow \dots, \end{array}$$

where $\pi_B(f) = \pi \circ f$ and β is the connecting homomorphism [19, Sec. 1.3, Add. 1.3.3]. The homomorphism β is classically known as the *(higher order) Bockstein homomorphism*; see for instance [10, Sec. 5.2], [12, Sec. 6.2, p. 197]. We write $\operatorname{Im}\pi_B = \pi_B(G)$ and stress that π_B respects the action of A. Observe, moreover, that $\mathrm{H}^2(G;C[p])$ is naturally isomorphic to $\mathrm{H}^2(G;\mathbb{F}_p)$ and so we identify them.

Lemma 2.3. *The image of β is an $\mathbb{F}_p$-vector space of dimension $\mathrm{d}(G)$ and the following equalities hold*

$$\operatorname{Im}\beta = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) = \mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p).$$

Proof. We start by showing that $\operatorname{Im}\beta$ is contained in $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$. For this, let $[c] \in \operatorname{Im}\beta$ and let E_c be an extension of G by $\mathbb{F}_p$ represented by $[c]$. By definition of β, there exists a map $\tilde{c} : G \to C$ such that, for all $x, y \in G$, one has $c(x,y) = \tilde{c}(x) + \tilde{c}(y) - \tilde{c}(x+y)$. Then, for all $g_1, g_2 \in G$ and $m_1, m_2 \in C[p]$, we have that

$$\begin{aligned}(g_1,m_1)\cdot(g_2,m_2) - (g_2,m_2)\cdot(g_1,m_1) &= (0, c(g_1,g_2) - c(g_2,g_1)) \\ &= (0, -\tilde{c}(g_1+g_2) + \tilde{c}(g_2+g_1)) = (0,0)\end{aligned}$$

and thus E_c is abelian. This shows that $\operatorname{Im}\beta \subseteq \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$. Now we show that the following holds:

$$\ker\beta = \{\sum_{j=1}^{t}\sum_{k=1}^{r_j} \alpha_{jk}\gamma_{jk}^* \mid \alpha_{jk} \in p\mathbb{Z}_p\} = p\hat{G}. \tag{2.4}$$

For this, note that β's image is contained in the elementary abelian p-group $\mathrm{H}^2(G;\mathbb{F}_p)$ and so it follows that $p\,\mathrm{Hom}(G,C/(p^nC)) \subseteq \ker\beta$. We also have that

$$\frac{\hat{G}}{p\hat{G}} = \frac{\mathrm{Hom}(G,C/(p^nC))}{p\,\mathrm{Hom}(G,C/(p^nC))} \cong \frac{G}{pG}$$

and $\dim_{\mathbb{F}_p}\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) = r+1$ thus the first isomorphism theorem yields (2.4). It follows that $\widehat{\phi_1}$ induces an isomorphism $V \to \widehat{G}/\ker\beta$ and $\operatorname{Im}\beta$ is an $\mathbb{F}_p$-vector space of dimension $\dim_{\mathbb{F}_p} V = \dim_{\mathbb{F}_p}\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$. We derive that $\operatorname{Im}\beta = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) = \mathrm{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p)$. □

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Remark 2.4. *Observe that* $\operatorname{Im}\beta = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) = \operatorname{Ext}^1_{\mathbb{Z}_pG}(G,\mathbb{F}_p)$ *is precisely the collection of equivalence classes of symmetric 2-cocycles, i.e. cocycles* c *with the property that, for all* $g_1, g_2 \in G$*, the equality* $c(g_1,g_2) = c(g_2,g_1)$ *holds. Since* A *maps symmetric 2-cocycles to symmetric 2-cocycles, the action of* A *on* $\mathrm{H}^2(G;\mathbb{F}_p)$ *induces an action of* A *on* $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$*. This can also be derived from Lemma 2.3.*

2.5. **Maximal subgroups.** In this section we describe a map that associates each cohomology class in $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ to a subgroup of index at most p in G. Recall that $\widehat{V} = \operatorname{Hom}(V,\mathbb{F}_p)$ denotes the dual of V and $\widehat{G} = \operatorname{Hom}(G, C/(p^nC))$ the Pontryagin dual of G. Let $\phi : \widehat{G} \to \widehat{V}$ be the homomorphism defined by $\gamma^*_{jk} \mapsto v^*_{jk}$, in other words, $\phi = \phi_1 \pi \widehat{\phi_1}^{-1}$. It follows that

$$\ker\phi = \{f \in \operatorname{Hom}(G, C/(p^nC)) \mid f(I_j) \subseteq (p^{n-n_j+1}C)/(p^nC),\ 1 \le j \le t\} = p\operatorname{Hom}(G, C/(p^nC)) = \ker\beta$$

and thus ϕ induces an isomorphism

$$\phi_2 : \widehat{G}/\ker\beta = \operatorname{Hom}(G, C/(p^nC))/\ker\beta \longrightarrow \widehat{V} = \operatorname{Hom}(V,\mathbb{F}_p).$$

Let now ϕ_3 be the isomorphism induced by β, i.e.

$$\phi_3 : \operatorname{Hom}(G, C/(p^nC))/\ker\beta \longrightarrow \operatorname{Im}\beta = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p),$$

where the fact that $\operatorname{Im}\beta = \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ is ensured by Lemma 2.3. Now, the map $\phi_4 = \phi_3 \circ \phi_2^{-1}$ is an isomorphism and we obtain the following commutative diagram:

(2.5)
$$\begin{array}{ccccc} & & \widehat{V} & \xleftarrow{\phi_1} & V \xleftarrow{\pi} G \\ & \overset{\phi_2}{\nearrow} & \downarrow{\scriptstyle \phi_4} & & \\ \widehat{G}/\ker\beta & \xrightarrow{\phi_3} & \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p). & & \end{array}$$

Lemma 2.5. *The isomorphisms* ϕ_2, ϕ_3, ϕ_4 *respect the action of* A*.*

Proof. Since ϕ_3 clearly respects the action of A, it suffices to show that ϕ_2 is an A-isomorphism on the generators $\gamma^*_{jk} \in \widehat{G}$ described in (2.3). Let $(\sigma,\lambda) \in A$. Since $\sigma(\ker\beta) \subseteq \ker\beta$, the following equalities hold

$$\phi_2((\sigma,\lambda)(\gamma^*_{jk} + \ker\beta)) = \phi_2(\lambda\gamma^*_{jk}\sigma^{-1} + \ker\beta) = \lambda v^*_{jk}\overline{\sigma}^{-1} = (\sigma,\lambda)\phi_2(\gamma^*_{jk} + \ker\beta)$$

and thus both ϕ_2 and $\phi_4 = \phi_3 \circ \phi_2^{-1}$ are A-isomorphisms. □

We rely on the commutative diagram (2.5) to define the following function

$$\begin{aligned} \tau : \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) &\longrightarrow \{\text{subspaces of codimension at most 1 of } V\} \\ [c] &\longmapsto \ker(\phi_4^{-1}([c])) \end{aligned}$$

and remark that, by construction, $\tau([c]) = V$ if and only if $[c] = [0]$. In particular τ induces a bijection

$$\mathrm{t}_V : \mathbb{P}\,\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \longrightarrow \{\text{hyperplanes of } V\},$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

equivalently, postcomposing with π^{-1}, a bijection

$$\mathfrak{t}_G : \mathbb{P}\,\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \longrightarrow \{\text{subgroups of index } p \text{ of } G\}. \tag{2.6}$$

We will show in Section 3.2 that the maps $\mathfrak{t}_G$ and $\mathfrak{t}_V$ are compatible with the actions of A as given in (1.4) and (1.5); see Corollary 3.11. In particular, it will follow that each non-trivial orbit of A in $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ has cardinality divisible by $p-1$. This is true in higher generality. We warn the reader that in the sequel we will often, by a slight abuse of notation, write $\mathfrak{t}_G([c])$ meaning the image under $\mathfrak{t}_G$ of the projective class of $[c]$.

Lemma 2.6. *Let $\lambda \in \mathbb{Z}_p^*$, $[c] \in \mathrm{H}^2(G;\mathbb{F}_p)$, and $[\omega] \in \langle \mathrm{Im}\cup \rangle$. Then the following hold:*

(1) *$\lambda[c] = [c]$ if and only if $[c] = 0$ or $\lambda = 1$,*
(2) *if $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$, then $(\lambda,\lambda)[c] = [c]$ and $(\lambda,\lambda)[\omega] = \lambda^{-1}[\omega]$.*

Moreover, every non-trivial orbit of $\mathrm{H}^2(G;\mathbb{F}_p)$ has cardinality divisible by $p-1$.

Proof. (1) Suppose that $\lambda[c] = [c]$, i.e. there exists $f \in C^1(G;\mathbb{F}_p)$ such that for all $x, y \in G$,

$$\lambda c(x,y) = c(x,y) + \partial_1(f)(x,y) \iff (\lambda-1)c(x,y) = \partial_1(f)(x,y).$$

If $\lambda \neq 1$, then, for all $x, y \in G$, it holds that $c(x,y) = (\lambda-1)^{-1}\partial_1(f)(x,y)$. Now define $\tilde{f} = (\lambda-1)^{-1}f$ to obtain that $c(x,y) = \partial_1(\tilde{f})(x,y)$ and thus $[c] = [0]$. The other implication is clear.

(2) Let $\tilde{c} \in \mathrm{Hom}(G, C/(p^nC))$ be such that $[c] = \beta(\tilde{c})$ and note that $\tilde{c}$ exists by Lemma 2.3. Let, moreover, $f, g \in \mathrm{Hom}(G,\mathbb{F}_p)$. Then, for each $x, y \in G$, we have

$$(\lambda,\lambda)[c] = \beta(\lambda\tilde{c}\lambda^{-1}) = \beta(\tilde{c}) = [c],$$
$$(\lambda,\lambda)(f\cup g)(x,y) = \lambda f(\lambda^{-1}x)g(\lambda^{-1}y) = \lambda\lambda^{-2}f(x)g(y) = \lambda^{-1}(f\cup g)(x,y).$$

We are now done since $\langle \mathrm{Im}\cup\rangle$ is the linear span of elements of the form $[f\cup g]$. □

Definition 2.7. *Let $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and let M be a subgroup of G. Then the*

(1) kernel of $[c]$ in G *is the subgroup*

$$T_c = \begin{cases} G & \text{if } [c] = 0, \\ \mathfrak{t}_G([c]) & \text{otherwise.} \end{cases}$$

(2) *c-index of M is the number $i_c(M) = \dim_{\mathbb{F}_p}((M+T_c)/T_c) \in \{0,1\}$.*

We will often write T for T_c if the cohomology class $[c]$ is clear from the context.

Example 2.8. *Let $j \in \{1,\dots,t\}$ and $k \in \{1,\dots,r_j\}$ and let β be as in Section 2.4. Set $[c] = \beta(\gamma^*_{jk})$. Then $\phi_4^{-1}([c]) = v^*_{jk}$ and it follows that the kernel of $[c]$ is $T = \mathfrak{t}_G([c]) = \pi^{-1}(\ker v^*_{jk}) = \ker(\gamma^*_{jk}) + pG$.*

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

2.6. **Plücker embedding.** Recall the definition of the cup product $\cup : \mathrm{H}^1(G;\mathbb{F}_p) \times \mathrm{H}^1(G;\mathbb{F}_p) \longrightarrow \mathrm{H}^2(G;\mathbb{F}_p)$ as given in Section 2.1. In the present section, we construct maps on $\operatorname{Im}\cup$ that will allow us to interpret $\operatorname{Im}\cup$ as a specific family of subgroups of G. This construction is based on the Plücker embedding for Grassmannians; see for example [18, Sec. 1.24],[15, Ch. 5]. Until the end of the current section, for each positive integer k and $\mathbb{F}_p$-vector space W, we denote by $\mathcal{G}(k,W)$ the Grassmannian of k-dimensional linear subspaces of W. Denote, moreover, by $\wedge$ the exterior product map $W \times W \to \Lambda^2 W$.

We start by remarking that the vector spaces $\langle \operatorname{Im}\cup\rangle$ and $\Lambda^2\widehat{V}$ are naturally isomorphic. The cup product being bilinear and alternating, the universal property of wedge products yields the surjective homomorphism

$$\psi_G : \Lambda^2 \operatorname{Hom}(G,\mathbb{F}_p) \longrightarrow \langle \operatorname{Im}\cup\rangle \text{ satisfying } f\wedge g \longmapsto [f\cup g].$$

Observe that the last map is our announced isomorphism, since $\operatorname{Hom}(G,\mathbb{F}_p)$ and $\operatorname{Hom}(V,\mathbb{F}_p) = \widehat{V}$ are naturally isomorphic and the dimensions of $\Lambda^2\widehat{V}$ and $\langle \operatorname{Im}\cup\rangle$ are the same. Moreover, by its definition, ψ_G satisfies $\psi_G(\operatorname{Im}\wedge) = \operatorname{Im}\cup$ and thus induces a bijection $\mathbb{P}\operatorname{Im}\wedge \to \mathbb{P}\operatorname{Im}\cup$.

We proceed by describing the Plücker embedding $s : \mathcal{G}(2,\widehat{V}) \to \mathbb{P}(\Lambda^2\widehat{V})$. For each 2-dimensional subspace U of $\widehat{V}$, fix an $\mathbb{F}_p$-basis (f_u, g_u) of U and define $s(U) = [f_u \wedge g_u]$. It is not difficult to show that s is well-defined and that its image is equal to $\mathbb{P}\operatorname{Im}\wedge$. We use now the map s to define a bijection $\mathcal{G}(\mathrm{d}(G)-2,V) \to \mathbb{P}\operatorname{Im}\cup$. For that, we start by identifying $\mathcal{G}(2,\widehat{V})$ and $\mathcal{G}(\mathrm{d}(G)-2,V)$ via

$$\mathcal{G}(2,\widehat{V}) \longrightarrow \mathcal{G}(\mathrm{d}(G)-2,V), \quad U = \mathbb{F}_p f_u \oplus \mathbb{F}_p g_u \longmapsto \ker f_u \cap \ker g_u.$$

Composing maps in the obvious way, we get the following well-defined bijection

$$\mathfrak{m}_V : \mathbb{P}\operatorname{Im}\cup \longrightarrow \mathcal{G}(\mathrm{d}(G)-2,V), \quad [\omega] = [f\cup g] \longmapsto \mathfrak{m}_V([\omega]) = \pi(\ker f \cap \ker g),$$

inducing the bijection

$$\mathfrak{m}_G : \mathbb{P}\operatorname{Im}\cup \longrightarrow \{\pi^{-1}(U) \mid U \in \mathcal{G}(\mathrm{d}(G)-2,V)\}, \quad [\omega] = [f\cup g] \longmapsto \mathfrak{m}_G([\omega]) = \ker f \cap \ker g. \tag{2.7}$$

The last map identifies each element of $\mathbb{P}\operatorname{Im}\cup$ with a subgroup M of G of index p^2 that contains pG. We next show that $\mathfrak{m}_G$ respects the action of A. As for the case of $\mathfrak{t}_G$ we will slightly abuse notation writing $\mathfrak{m}_G([\omega])$ for the image of the projective class of $[\omega]$ under $\mathfrak{m}_G$.

Lemma 2.9. *Let $[\omega] \in \mathbb{P}\operatorname{Im}\cup$ and $(\sigma,\lambda) \in A$. Then the equality $\sigma(\mathfrak{m}_G([\omega])) = \mathfrak{m}_G((\sigma,\lambda)[\omega])$ holds.*

Proof. Write $[\omega] = [f\cup g]$ with $f, g \in \operatorname{Hom}(G;\mathbb{F}_p)$. Then, for each choice of $x, y \in G$, we have

$$(\sigma,\lambda)(f\cup g)(x,y) = \lambda(f\cup g)(\sigma^{-1}(x),\sigma^{-1}(y)) = \lambda f(\sigma^{-1}(x))g(\sigma^{-1}(y)).$$

In other words, $(\sigma,\lambda)(f\cup g) = (\lambda f\sigma^{-1})\cup(g\sigma^{-1})$ and we derive that

$$\mathfrak{m}_G((\sigma,\lambda)[\omega]) = \ker(\lambda f\sigma^{-1}) \cap \ker(g\sigma^{-1}) = \sigma(\ker f)\cap\sigma(\ker g) = \sigma(\ker f\cap\ker g) = \sigma(\mathfrak{m}_G([\omega])).$$

This concludes the proof. □

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Corollary 2.10. *The map*

$$\mathfrak{m}_G : \mathbb{P}\operatorname{Im}\cup \to \{M \text{ subgroup of } G \text{ with } G/M \text{ elementary abelian of rank } 2\}$$

is a bijection respecting the action of A.

Definition 2.11. *Let* $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ *and* $[\omega] \in \operatorname{Im}\cup$. *Then the*

(1) kernel of $[\omega]$ in G *is the subgroup*

$$M_\omega = \begin{cases} G & \text{if } [\omega] = 0, \\ \mathfrak{m}_G([\omega]) & \text{otherwise.} \end{cases}$$

(2) c-index of $[\omega]$ *is the number* $i_c([\omega]) = i_c(M_\omega)$.

We remark that, with the notation from Definition 2.11, it is not difficult to show that, if E is an extension defined by $[\omega]$, then the image of $\mathrm{Z}(E)$ in G coincides with M_ω.

Lemma 2.12. *Let* $[\omega] \in \operatorname{Im}\cup$ *and let* $M = M_\omega$ *be the kernel of* $[\omega]$ *in* G. *Let* $M \subseteq H, K \subseteq G$ *be distinct maximal subgroups of* G. *Then there exist* $f, g \in \operatorname{Hom}(G, \mathbb{F}_p)$ *such that* $H = \ker f$, $K = \ker g$, *and* $[\omega] = [f \cup g]$.

Proof. Any maximal subgroup can be written as the kernel of a homomorphism $G \to \mathbb{F}_p$. Now, H and K being distinct, the claim follows from the fact that the map $\mathfrak{m}_G$ from (2.7) is well-defined. □

3. Subgroup levels and compatibility

We recall briefly the notation introduced in Section 1.2 that will be relevant here. If two elements $[c], [d] \in \mathrm{H}^2(G;\mathbb{F}_p)$ belong to the same A-orbit, we will write $[c] \sim_A [d]$. For $[c] \in \mathrm{H}^2(G;\mathbb{F}_p)$, we will write A_c meaning the stabilizer of $[c]$ in A and, if two elements $[d], [e]$ are in the same orbit under the induced action by A_c, we will write $[d] \sim_{A_c} [e]$. For a subgroup K of G, we denote by A_K the stabilizer of K in A with respect to the action from (1.4).

3.1. Subgroup levels.

The aim of this section is to introduce subgroup levels and prove basic properties about them. Subgroup levels are the key objects allowing us to describe the A-orbits on $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \times \operatorname{Im}\cup$ combinatorially.

Definition 3.1. *Let* M *and* T *be subgroups of* G. *Then the* T-levels of M *are the entries of the pair* $\ell\mathrm{L}_T(M) = (\ell_T(M), \mathrm{L}_T(M))$ *where*

(1) $\ell_T(M) = 1 + \max\{0 \le i \le \log_p \exp(T) \,:\, T[p^i] \subseteq M \cap T\}$,

(2) $\mathrm{L}_T(M) = \min\{j \in \mathbb{Z}_{\ge 0} \,:\, T[p^j] + (M \cap T) = T\}$.

If $T = G$, *simply write* $\ell\mathrm{L}(M) = (\ell(M), \mathrm{L}(M))$ *for* $\ell\mathrm{L}_G(M)$.

Example 3.2.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

(1) *The G-levels vector of G is $(n+1,0)$ and its T-levels vector is $(\log_p \exp(T)+1,0)$.*
(2) *Assume that $G=\mathbb{Z}/(p^2)\oplus\mathbb{Z}/(p^2)\oplus\mathbb{Z}/(p^3)\oplus\mathbb{Z}/(p^3)=\langle\gamma_{11},\gamma_{12},\gamma_{21},\gamma_{22}\rangle$, and define*

$$T=\langle\gamma_{12},\gamma_{21},\gamma_{22}\rangle+pG=\{(pt_1,t_2,t_3,t_4)\mid t_i\in\mathbb{Z}_p\}\subseteq G,$$
$$M=\langle\gamma_{12},\gamma_{21}-\gamma_{22}\rangle+pG=\{(pm_1,m_2,m_3,-m_3+pm_4)\mid m_i\in\mathbb{Z}_p\}\subseteq G.$$

It follows that $\ell\mathrm{L}(M)=(2,3)$ and $\ell\mathrm{L}_T(M)=(3,3)$. Since T is a maximal subgroup of G, we can associate to it an element $[c]\in\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)\setminus\{0\}$ via (2.6). For such a cohomology class $[c]$, the c-index of M is $i_c(M)=0$, because M is contained in T (see Definition 2.7).

We generalize the last example in the form of the following proposition.

Proposition 3.3. *Let X be a proper subgroup of G containing pG and with $|G:X|=p^k$. Let*

$$p^{\alpha_1}\geq\cdots\geq p^{\alpha_{r+1}}\quad\text{and}\quad p^{\beta_1}\geq\cdots\geq p^{\beta_{r+1}}$$

be the elementary divisors of G and X, respectively. Then there are indices $r+1\geq i_1>\cdots>i_k\geq 1$ such that the following holds:

$$\beta_i-\alpha_i=\begin{cases}1 & \text{if } i\in\{i_1,\ldots,i_k\},\\ 0 & \text{otherwise.}\end{cases}$$

Moreover, one has $\ell(X)=\alpha_{i_k}$ and $\mathrm{L}(X)=\alpha_{i_1}$.

Proof. Since X contains pG and $|G:X|=p^k$, it is clear that the sequence $r+1\geq i_1>\ldots>i_k\geq 1$ of integers exists. From the definition of the i_j's it is now easy to see that $\ell(X)=\alpha_{i_k}$ and $\mathrm{L}(X)=\alpha_{i_1}$. □

Corollary 3.4. *If T is a maximal subgroup of G, then $\ell(T)=\mathrm{L}(T)$.*

Corollary 3.5. *Let X,Y be subgroups of G containing pG and satisfying $|G:X|=|G:Y|\leq p^2$. Then the following are equivalent:*

(1) *X and Y are isomorphic,*
(2) *$\ell\mathrm{L}(X)=\ell\mathrm{L}(Y)$.*

It would be interesting to generalize the concept of G-levels in order to get a version of Corollary 3.5 holding for all subgroups of G containing pG.

Definition 3.6. *Let $[c],[d]$ be elements of $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)\cup\mathrm{Im}\cup$ and let K and H be the kernels of $[c]$ resp. $[d]$ in G. Let T be a subgroup of G. Then the T-levels and $[d]$-levels of $[c]$ are defined respectively as*

$$\ell\mathrm{L}_T([c])=\ell\mathrm{L}_T(K)\text{ and }\ell\mathrm{L}_d([c])=\ell\mathrm{L}_H(K).$$

If $T=G$ or $[d]=0$, simply write $\ell\mathrm{L}([c])=(\ell([c]),\mathrm{L}([c]))$ for $\ell\mathrm{L}_G([c])$ and $\ell\mathrm{L}_0([c])$.

Below, we give some properties of T-levels.

Lemma 3.7. *Let M and T be subgroups of G. Then the following hold:*

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

(1) $1 \leq \ell_T(M)$ *and* $\mathrm{L}_T(M) \leq \log_p \exp(T)$.
(2) *if* $z \in T \setminus (M \cap T)$, *then* $|z| \geq p^{\ell_T(M)}$.
(3) *if* $\mathrm{L}_T(M) = \ell_T(M) - 1$, *then* $T = \{0\}$.
(4) *if* $T \not\subseteq M$, *then* $\ell_T(M) - 1 < \mathrm{L}_T(M)$.

Proof. Set $l_T = \ell_T(M)$ and $L_T = \mathrm{L}_T(M)$. Items (1)-(2) are straightforward. To prove (3)-(4), we start by observing that, when T is contained in M, then $l_T = \log_p \exp(T) + 1$ and $L_T = 0$. Assume now that M does not contain T. Then $T \neq \{0\}$, $L_T \neq 0$, and, since $T[p^{l_T - 1}]$ is contained in M but $T[p^{L_T}]$ is not, we have that $l_T - 1 \leq L_T$. □

Lemma 3.8. *Let* M *and* T *be subgroups of* G *such that* $|G : T| = p$ *and* $|G : M| = p^2$. *Define* $\ell\mathrm{L}(M) = (l, L)$ *and* $\ell\mathrm{L}_T(M) = (l_T, L_T)$. *Then the following inequalities hold:*

$$l \leq l_T \leq \min\{L, L_T\} = \begin{cases} L & \text{if } M \not\subseteq T, \\ L_T & \text{if } M \subseteq T. \end{cases}$$

Proof. The inequality $l \leq l_T$ follows from the fact that, for each $m \in \mathbb{Z}_{\geq 0}$, one has

$$G[p^m] \subseteq M \Longrightarrow T[p^m] = G[p^m] \cap T \subseteq M \cap T.$$

We now show that $l_T \leq L$. For a contradiction, assume that $l_T > L$. It follows from the definition of $\ell\mathrm{L}_T(M)$ that $T[p^L]$ is contained in $M \cap T$. In particular, since $T[p^L] = G[p^L] \cap T$, we have that $T[p^L]$ is contained in $M \cap G[p^L]$. Now, since $|G : T| = p$, we get that $|G[p^L] : T[p^L]| \leq p$ and consequently

$$p^2 = |G : M| = |(M + G[p^L]) : M| = |G[p^L] : (M \cap G[p^L])| \leq |G[p^L] : T[p^L]| \leq p$$

providing a contradiction. So we have proven that $l_T \leq L$. The inequality $l_T \leq L_T$ follows from Lemma 3.7 and thus yields that $l_T \leq \min\{L, L_T\}$.

For the last equality, assume first that M is contained in T. Since $G = M + G[p^L]$, we have that $T \cap G = T = M + T[p^L]$. By definition of L_T, we have $L_T \leq L$. To conclude, assume that M is not contained in T. From

$$T = (M \cap T) + T[p^{L_T}] = (M + T[p^{L_T}]) \cap T$$

we get that $G = M + T[p^{L_T}] = M + G[p^{L_T}]$. It follows from the minimality of L that $L \leq L_T$. □

Example 3.9.

(1) *Assume that* G *is a free* $\mathbb{Z}/(p^3)$*-module of rank* 2. *Then* $M = G[p^2] = pG$ *has index* p^2 *in* G *and is contained in every maximal subgroup of* G. *For each* T *maximal in* G, *it then holds that* $3 = \ell(M) = \ell_T(M) = \mathrm{L}_T(M) = \mathrm{L}(M)$.
(2) *Let* $G = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p^3) \oplus \mathbb{Z}/(p^4) = \langle \gamma_{11}, \gamma_{21}, \gamma_{31}, \gamma_{41} \rangle$, *and define*

$$T = \langle \gamma_{21}, \gamma_{31}, \gamma_{41} \rangle = \{(0, t_2, t_3, t_4) \mid t_i \in \mathbb{Z}_p\} \subseteq G,$$

$$M = \langle \gamma_{11} - \gamma_{31} - \gamma_{41}, \gamma_{21} \rangle + pG = \{(m_1, m_2, -m_1 + pm_3, -m_1 + pm_4) \mid m_i \in \mathbb{Z}_p\} \subseteq G.$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

It follows that $M \cap T = \langle \gamma_{21} \rangle + pG$ *and therefore* $1 = \ell(M) < 3 = \ell_T(M) = \mathrm{L}(M) < 4 = \mathrm{L}_T(M)$. *We conclude by observing that, since* M *is not contained in* T, *the c-index of* M *in* G *will be* 1 *for each* $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ *that realizes* T *in the sense of* (2.6).

3.2. **Compatibility.** The following proposition collects a number of basic properties shared by elements belonging to the same A-orbit.

Proposition 3.10. *Let* $[c], [d] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ *and let* T_c *and* T_d *denote respectively the kernels of* $[c]$ *and* $[d]$. *Let, moreover,* $a = (\sigma, \lambda) \in A$ *be such that* $[d] = a \cdot [c]$. *Let* $[\omega] = [f \cup g] \in \mathrm{Im} \cup$ *and let* $M = M_\omega$ *be the kernel of* $[\omega]$. *Define*

$$f_a = \lambda f \sigma^{-1} \text{ and } g_a = g\sigma^{-1}$$

and let M_a *be the kernel of* $[\omega_a] = [f_a \cup g_a]$. *Then* $a \cdot ([c] + [\omega]) = [d] + [\omega_a]$ *and the following hold:*

(1) *The following maps are inverses to each other:*

$$\phi : \mathrm{Im} \cup / A_c \longrightarrow \mathrm{Im} \cup / A_d, \quad A_c[\omega] \longmapsto A_d(a \cdot [\omega]),$$
$$\psi : \mathrm{Im} \cup / A_d \longmapsto \mathrm{Im} \cup / A_c \quad A_d[\omega] \mapsto A_c(a^{-1} \cdot [\omega]).$$

(2) $T_d = \sigma(T_c)$ *and* $M_a = \sigma(M)$.

(3) $\ell\mathrm{L}(M) = \ell\mathrm{L}(M_a)$, $\ell\mathrm{L}_c(M) = \ell\mathrm{L}_d(M_a)$, $\ell\mathrm{L}(T_c) = \ell\mathrm{L}(T_d)$ *and* $i_c(M) = i_d(M_a)$.

Proof. To show that $a \cdot ([c] + [f \cup g]) = [d] + [f_a \cup g_a]$ is an easy computation.

(1) Straightforward.

(2) That $\sigma(M) = M_a$ is a straight consequence of Lemma 2.9. We prove that $\sigma(T_d) = T_c$. We use the bar notation for the subspaces of $V = G/pG$ and we refer to the notation in (2.5) and (1.3). The map σ being an isomorphism, it follows from Lemma 2.5 that

$$\begin{aligned}
\overline{T_d} &= \ker(\phi_4^{-1}([d])) = \ker(\phi_4^{-1}(a \cdot [c])) \\
&= \ker(a \cdot \phi_4^{-1}([c])) = \ker(\lambda \phi_4^{-1}([c]) \circ \overline{\sigma}^{-1}) \\
&= \ker(\phi_4^{-1}([c]) \circ \overline{\sigma}^{-1}) = \overline{\sigma} \ker(\phi_4^{-1}([c])) \\
&= \overline{\sigma}(\overline{T_c}).
\end{aligned}$$

Lifting everything back to G, we get $T_d = \sigma(T_c)$.

(3) This is a direct consequence of (2) and Definitions 2.7 and 2.11. □

In the next result, let $\mathfrak{t}_G$ and $\mathfrak{m}_G$ denote respectively the maps from (2.6) and (2.7). For each $k \in \{1, \dots, d\}$, we write moreover

$$\begin{aligned}
\mathcal{S}_G^{(k)} &= \{\pi^{-1}(W) \mid W \text{ subspace of codimension } k \text{ of } V\} \\
&= \{K \text{ subgroup of } G \text{ with } G/K \text{ elementary abelian of rank } k\}
\end{aligned}$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

and note that the action of A given in (1.4) naturally induces an action of A on each $\mathcal{S}_G^{(k)}$ and, componentwise, on any of their products.

Corollary 3.11. *The following is an isomorphism of A-sets:*

$$(\mathfrak{t},\mathfrak{m})_G : \mathbb{P}\,\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \times \mathbb{P}\,\mathrm{Im}\cup \longrightarrow \mathcal{S}_G^{(1)} \times \mathcal{S}_G^{(2)}, \quad ([c],[\omega]) \longmapsto (\mathfrak{t}_G([c]),\mathfrak{m}_G([\omega])).$$

Moreover, for each $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p) \setminus \{0\}$ with kernel T, the stabilizer A_c is a subgroup of A_T of index $|A_T : A_c| = p-1$.

Proof. The map $(\mathfrak{t},\mathfrak{m})_G$ is an isomorphism of A-sets as a consequence of Corollary 2.10 and Proposition 3.10(2). Therefore, we get that, for each element $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;F_p)$, if $T = \mathfrak{t}_G([c])$, then $A_c \subseteq A_T$ and $|A_T : A_c| = p-1$. □

We point out the connection between Corollary 3.11 and Lemma 2.6. The last corollary clearly describes the projective nature of the orbits in terms of subgroups of G. It would be interesting to know whether the map $(\mathfrak{t},\mathfrak{m})_G$ can be extended to the whole of $\mathbb{P}\,\mathrm{H}^2(G;\mathbb{F}_p)$; see also Section 6.4.

4. **Abelian extensions**

In this section we classify the A-orbits of $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ via classifying the A-orbits in $\mathrm{Hom}(G, C/p^nC)/\ker\beta$, where β is the homomorphism introduced in Section 2.4. We also show that, under our assumptions, strong isomorphism classes and isomorphism types of extensions of G by $\mathbb{F}_p$ coincide.

Until the end of Section 4, the following assumptions will hold. For $j \in \{1,\dots,t\}$ and $k \in \{1,\dots,n_j\}$, let γ_{jk}^* be the dual of γ_{jk} as defined in (2.3), within Section 2.3. For $j \in \{1,\dots,t\}$, define moreover $\gamma_j^* = \gamma_{j1}^*$ and denote by $\widehat{\pi}_j$ the natural projection $\widehat{G} = \bigoplus_{j=1}^t \widehat{I}_j \to \widehat{I}_j$. The next proposition is the main result of the current section.

Proposition 4.1. *Let $[c],[d] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$. Then the following are equivalent:*

(1) $[c] \sim_A [d]$;
(2) $[c] = [d] = 0$ *or there exists* $i \in \{1,\dots,t\}$ *such that* $[c] \sim_A \beta(\gamma_i^*) \sim_A [d]$;
(3) $\ell\mathrm{L}([c]) = \ell\mathrm{L}([d])$;
(4) $\ell([c]) = \ell([d])$;
(5) $\mathrm{L}([c]) = \mathrm{L}([d])$.

4.1. **Bockquivalence relation.** In this section we prove Proposition 4.1 via studying the action of A on $\widehat{G} = \mathrm{Hom}(G, C/(p^nC))$. We recall from Section 2.4 that, since β respects the action of A, Lemma 2.3 yields that the A-orbits of $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ are in natural bijection with the A-orbits of $\widehat{G}/\ker\beta$.

Definition 4.2 (Bockquivalence relation)**.** *Two elements $f,g \in \widehat{G}$ are* Bockquivalent*, written $f \approx_G g$, if there exist $(\sigma,\lambda) \in A$ and $\varepsilon \in \pi_B(G)$ such that $g = \lambda f \sigma^{-1} + \varepsilon$.*

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

The just defined Bockquivalence relation is clearly an equivalence relation, because it describes the A-orbits of $\mathrm{Hom}(G, C/(p^nC))/\ker\beta$. We will refer to the corresponding equivalence classes as *Bockquivalence classes* and, if $f \in \mathrm{Hom}(G, C/(p^nC))$, we will write $[\![f]\!]$ to denote the Bockquivalence class of f. Our immediate goal is to determine representatives for the Bockquivalence classes of G.

Proposition 4.3. *Let $\Gamma = \{\gamma_j^* : j = 1, \dots, t\} \cup \{0\}$. Then Γ is a set of representatives for the Bockquivalence classes of G and, for each $j \in \{1, \dots, t\}$, the following equality holds:*

$$[\![\gamma_j^*]\!] = \{c \in \widehat{G} : |\operatorname{Im}\widehat{\pi}_j(c)| = p^{n_j}, |\operatorname{Im}\widehat{\pi}_l(c)| < p^{n_l} \text{ for } l > j\}.$$

Moreover, G has exactly $t+1$ Bockquivalence classes.

Proof. We start by recalling that $\ker\beta = p\hat{G}$, as given in (2.4). We will show that the images of the maps γ_i^* in the quotient $\hat{G}/p\hat{G} = \hat{G}/\ker\beta$ constitute a set of representatives for the nonzero orbits of the action of A on the last quotient. We first show that each nonzero orbit can be represented by one of the γ_i^*'s. To this end, for every non-trivial orbit choose a representative $f \in \hat{G} \setminus p\hat{G}$ of the form

$$f = \sum_{j=1}^{t}\sum_{k=1}^{r_j} \alpha_{jk}\gamma_{jk}^*, \text{ with } \alpha_{jk} \in \mathbb{Z}_p^* \cup \{0\}$$

and let $i \in \{1, \dots, t\}$ be maximal such that there exists $s \in \{1, \dots, r_i\}$ with $\alpha_{is} \in \mathbb{Z}_p^*$. It follows from the maximality of i that $f(G)$ is generated by $p^{n-n_i}\gamma$ and so the first isomorphism theorem yields that $G = \langle\gamma_{is}\rangle \oplus \ker f$. Set now $H = \langle\gamma_{jk} \mid (j,k) \neq (i,1)\rangle$ and note that $G = \langle\gamma_{i1}\rangle \oplus H$. Since γ_{i1} and γ_{is} have the same order, the elementary divisor theorem yields an automorphism σ of G sending γ_{is} to γ_{i1} and $\ker f$ to H. As a consequence, $(\sigma, 1)f = \gamma_i^*$ and f is in the orbit of γ_i^*.

We now show that any two γ_i^*'s represent distinct orbits. To this end, let $i \geq j$ be such that γ_i^* and γ_j^* represent the same A-orbit in $\hat{G}/p\hat{G}$ and let $(\sigma, \lambda) \in A$ and $g \in \hat{G}$ be such that $\gamma_i^* = (\sigma, \lambda)\gamma_j^* + pg$. It follows that

$$p^{n-n_i}\gamma = \gamma_i^*(\gamma_{i1}) = (\sigma, \lambda)\gamma_j^*(\gamma_{i1}) + pg(\gamma_{i1})$$

and so, by taking orders, we derive that $n_i = \max\{|\gamma_j^*(\sigma^{-1}(\gamma_{i_1}))|, n_i - 1\} \leq \max\{n_j, n_i - 1\}$. From the fact that $i \geq j$, that is $n_i \geq n_j$, we conclude that $i = j$. □

Proof of Proposition 4.1. (1) ⇔ (2) This is Proposition 4.3.

(2) ⇔ (3) ⇔ (4) ⇔ (5) Thanks to Proposition 4.3, a set of representatives of the A-orbits of $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ is given by $0, \beta(\gamma_1^*), \dots, \beta(\gamma_t^*)$. As a consequence of Example 2.8 and Proposition 3.10(2), the A-orbits are uniquely determined by their G-levels, which are respectively $(n+1, 0), (n_1, n_1), \dots, (n_t, n_t)$. □

4.2. **Convenient orbit representatives.** The goal of this section is to produce, for each given $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$, a representative of the A-orbit of $[c]$ that can be conveniently expressed in terms of the choice of generators we made in Section 1.2 and is thus more suitable to computations. We essentially want to be able to regard elements of $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ as if they were images of the generators of $\widehat{G}$.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Let $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and let $\tilde{c}$ be an element of $\widehat{G}$ such that $[c] = \beta(\tilde{c})$; recall that $\tilde{c}$ exists thanks to Lemma 2.3. Then, thanks to Proposition 4.1, there exists $a \in A$ and

$$b \in \mathcal{B} = \{\gamma_{jk} \mid 1 \leq j \leq t, 1 \leq k \leq n_j\}$$

such that, for $\{b_1, \ldots, b_r\} = \mathcal{B} \setminus \{b\}$, the following hold

$$\ker(a \cdot \tilde{c}) = \bigoplus_{i=1}^{r} \langle b_i \rangle \text{ and } G = \langle b \rangle \oplus \ker(a \cdot \tilde{c}) = \langle b \rangle \oplus \bigoplus_{i=1}^{r} \langle b_i \rangle.$$

Set $\tilde{d} = a \cdot \tilde{c}$ and $[d] = \beta(\tilde{d}) = [a \cdot c]$. Let, moreover, T_c and T_d denote the kernels of respectively $[c]$ and $[d]$. Then, thanks to Example 2.8, we know that $T_d = \ker \tilde{d} + pG$ and so we have a very concrete description of T_d in terms of the elements of $\mathcal{B}$. Moreover, if we are interested in the action of A_c on $\operatorname{Im} \cup$, we can as well consider the action of A_d on $\operatorname{Im} \cup$, thanks to Proposition 3.10(1).

4.3. **Strong isomorphism.** We close Section 4 by showing that strong isomorphism classes of G by $\mathbb{F}_p$ coincide with isomorphism classes of extensions of G by $\mathbb{F}_p$.

Proposition 4.4. *Let E_c and E_d be central extensions of G by $\mathbb{F}_p$ represented by the cohomology classes $[c]$ and $[d]$ in $\mathrm{H}^2(G;\mathbb{F}_p)$, respectively. Then, E_c and E_d are isomorphic if and only if $[c] \sim_A [d]$.*

Proof. If $c \sim_A d$, then, thanks to Theorem A, the extensions E_c and E_d are strongly isomorphic, so in particular isomorphic. Assume now that E_c and E_d are isomorphic. If E_c is nonabelian, then $[E_c, E_c]$ has order p and is mapped, by any isomorphism $E_c \to E_d$, to $[E_d, E_d]$. So, E_c and E_d are strongly isomorphic and we are done by Theorem A. We conclude by observing that each isomorphism class of extensions of G by $\mathbb{F}_p$ is a union of strong isomorphism classes. It is well-known that there are $t+1$ possible isomorphism types of abelian extensions of G by $\mathbb{F}_p$ and now, thanks to Proposition 4.3, we know that there are exactly $t+1$ strong isomorphism classes of such extensions. As the numbers are the same, we are done. □

5. Nonabelian extensions

Let $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and denote by A_c the stabilizer of $[c]$ in A. The aim of this section is to determine the orbits of the action of A_c on the image of the cup product $\cup : \mathrm{Hom}(G,\mathbb{F}_p) \times \mathrm{Hom}(G,\mathbb{F}_p) \to \mathrm{H}^2(G;\mathbb{F}_p)$. We will prove the following result.

Proposition 5.1. *Let $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and $[\omega]$, $[\vartheta]$ be elements of $\operatorname{Im} \cup$. The following are equivalent:*

(1) $[\omega] \sim_{A_c} [\vartheta]$,
(2) $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega]), i_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta]), i_c([\vartheta]))$.

Until the end of Section 5, the following assumptions will be satisfied. Let $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and $[\omega], [\vartheta] \in \operatorname{Im} \cup$ be fixed. As a consequence of the discussion from Section 4.2, without loss of generality,

we will work under the following additional assumptions. Let $\mathcal{B} = \{b_0 = b, b_1, \dots, b_r\}$ be a minimal set of generators of cardinality $r+1$ such that

$$G = \langle b \rangle \oplus \bigoplus_{i=1}^{r} \langle b_i \rangle.$$

Let $\tilde{c} \in \widehat{G}$ be such that $[c] = \beta(\tilde{c})$ and, if $[c] \neq 0$, assume that $\operatorname{Im} \tilde{c} \cong \langle b \rangle$ and that

$$\ker \tilde{c} = \bigoplus_{i=1}^{r} \langle b_i \rangle \text{ and } G = \langle b \rangle \oplus \ker \tilde{c}.$$

Let T be the kernel of $[c]$ and, if $[c] \neq 0$, observe that $T = \ker \tilde{c} + pG$ is maximal in G, analogously to Example 2.8. Write, moreover, M_ω and M_ϑ respectively for the kernels of $[\omega]$ and $[\vartheta]$, respectively. The case $[c] = 0$ is covered in Section 5.1. If $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p) \setminus \{0\}$, then we study the action of A_c on cup products in two parts. The case where $M_\omega + M_\vartheta \subseteq T$ is discussed in Section 5.2 and the case where $G = M_\omega + T = M_\vartheta + T$ is considered in Section 5.3. We remark that, the condition $i_c([w]) = i_c([\vartheta])$ imposed in (2) prevents the existence of any other case. We last let M be a subgroup of index p^2 of G containing pG and observe that M is the kernel of some element of $\operatorname{Im} \cup \setminus \{0\}$; see Section 2.6.

Lemma 5.2. *Write $\ell\mathrm{L}(M) = (l, L)$. Let, moreover, $\tilde{M}$ be a subgroup of M and $\mathcal{C} \subseteq \mathcal{B}$ such that $G = \langle \mathcal{C} \rangle \oplus \tilde{M}$. Then there exist $x, y \in \mathcal{C}$ such that $|x| = p^l$, $|y| = p^L$, and $G = \langle x, y \rangle + M$.*

Proof. We start by showing that there exists $x \in \mathcal{C}$ such that $|x| = p^l$ and $x \notin M$. For a contradiction, assume this is not true and write $C = \langle \mathcal{C} \rangle$. Then $G[p^l] = C[p^l] + \tilde{M}[p^l] \subseteq C[p^{l-1}] + M = M$, which is a contradiction to the maximality of l. Fix now such an element x and define $\tilde{H} = \langle x \rangle \oplus \tilde{M}$, which satisfies $G = \langle \mathcal{C} \setminus \{x\} \rangle \oplus \tilde{H}$. Note that $\tilde{H}$ is a subgroup of the maximal subgroup $H = \langle x \rangle + M$ of G. We now claim that there exists $y \in \mathcal{C} \setminus \{x\}$ of order p^L. If this is not the case and $D = \langle \mathcal{C} \setminus \{x\} \rangle$, then

$$G[p^L] = D[p^L] + \tilde{H}[p^L] \subseteq D[p^{L-1}] + H \subseteq G[p^{L-1}] + H$$

from which it follows that

$$G = G[p^L] + M = G[p^{L-1}] + H = G[p^{L-1}] + \langle x \rangle + M.$$

The minimality of L yields that $l = L$ and so that $G = \langle x \rangle + M$. In particular, $|G : M| = |\langle x \rangle : \langle px \rangle| = p$. Contradiction. □

Theorem 5.3. *Write $\ell\mathrm{L}(M) = (l, L)$ and let $x, y \in \mathcal{B}$ be such that $G = \langle x, y \rangle + M$ and $(|x|, |y|) = (p^l, p^L)$. Let, moreover, H be a subgroup of G such that $x, y \in H$. Then there exists a subgroup $\tilde{M} \subseteq H \cap M$ such that $H = \langle x \rangle \oplus \langle y \rangle \oplus \tilde{M}$.*

Proof. Let J be a subgroup of G such that $G = \langle x \rangle \oplus \langle y \rangle \oplus J$ and note that J exists because $x, y \in \mathcal{B}$. Moreover, thanks to Dedekind's Law, we also have that $H = \langle x \rangle \oplus \langle y \rangle \oplus (H \cap J)$. Write now $I = \langle x \rangle \oplus \langle y \rangle$.

We will show that $H \cap J$ can be replaced by a complement of I in H that is contained in M. For this, we consider all decompositions of H of the form

$$H = I \oplus \langle z_1 \rangle \oplus \cdots \oplus \langle z_s \rangle$$

and we choose one such that $m = |\{i \mid z_i \notin M\}|$ is minimal. We will prove that $m = 0$, in other words that $C = \langle z_1 \rangle \oplus \cdots \oplus \langle z_s \rangle$ is the desired complement. We argue by contradiction, assuming that $z_1 \notin M$. It follows that $|z_1| \geq p^l$ and, from $G = \langle x, y \rangle + M$ and $pG \subseteq M$, that z_1 can be expressed as

$$z_1 = \eta x + \kappa y + z_1' \quad \text{with} \quad \eta, \kappa \in \{0, \dots, p-1\},\ z_1' \in H \cap M. \tag{5.1}$$

We claim that $C' = \langle z_1' \rangle \oplus \langle z_2 \rangle \oplus \cdots \oplus \langle z_s \rangle$ is a complement of I in H. We will show this by means of proving that $I \oplus \langle z_1 \rangle = I \oplus \langle z_1' \rangle$. Since the equality $I + \langle z_1 \rangle = I + \langle z_1' \rangle$ is clear, it suffices to verify that $I \cap \langle z_1' \rangle = 0$ holds. For this, let $\lambda, \mu, \nu \in \mathbb{Z}_p$ be such that $\lambda x + \mu y + \nu z_1' = 0$. It follows that

$$(\lambda - \nu\eta)x + (\mu - \nu\kappa)y + \nu z_1 = 0,$$

from which we derive that $(\lambda - \nu\eta)x = (\mu - \nu\kappa)y = \nu z_1 = 0$. Then $\nu \geq |z_1| \geq p^l$ and, the order of x being p^l yields that $0 = (\lambda - \nu\eta)x = \lambda x$. If, additionally $|z_1| \geq p^L$ or $\kappa = 0$, in a similar fashion we obtain that $\mu y = 0$. We assume now that $|z_1| < p^L$ and that $\kappa \neq 0$. Then $|x|$ is also smaller than p^L. Moreover, κ is invertible modulo p and so (5.1) yields that y belongs to $\langle x, z_1 \rangle + M$. We deduce that

$$G = \langle x, y \rangle + M = \langle x, z_1 \rangle + M = G[p^{L-1}] + M,$$

which contradicts the definition of $L = \mathrm{L}(M)$. This concludes the proof that $I \oplus \langle z_1 \rangle = I \oplus \langle z_1' \rangle$.

We have shown that C' is a complement of I in H with a smaller number of generators outside of M; contradiction to the minimality of m. □

5.1. **Full stabilizer.** Until the end of Section 5.1, we work under the assumption that $[c] = [0] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$; then $A = A_c$ and we are simply studying the action of A on the cup product. In this section we prove thus Proposition 5.1 under these assumptions and in the following form.

Proposition 5.4. *One has* $[\omega] \sim_A [\vartheta]$ *if and only* $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta])$.

To that aim, we prove the following lemma, which will be used in the next section, too.

Lemma 5.5. *Write* $\ell\mathrm{L}(M) = (l, L)$. *Then there exist* $f, g \in \mathrm{Hom}(G, \mathbb{F}_p)$, $x, y \in \mathcal{B}$ *of orders respectively* p^l *and* p^L, *and* $\tilde{M} \subseteq M$ *such that the following hold:*

(1) $M = \ker f \cap \ker g$,
(2) $f(x) = 1$, $g(x) = 0$, $f(y) = 0$, *and* $g(y) = 1$,
(3) $G = \langle x \rangle \oplus \langle y \rangle \oplus \tilde{M}$.

Proof. Let x, y be as in Lemma 5.2, where $\mathcal{C}$ is taken to be $\mathcal{B}$. Now (1)-(2) are direct consequences of Lemma 2.12 while (3) follows from Theorem 5.3 to $H = G$. □

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Proof of Proposition 5.4. Assume first that $[\omega] \sim_A [\vartheta]$. If $[\omega] = [\vartheta] = 0$, then we are clearly done. If $[\omega], [\vartheta]$ are non-trivial elements of $\operatorname{Im}\cup$, then Proposition 3.10(3) yields that $\ell\mathrm{L}(M_\omega) = \ell\mathrm{L}(M_\vartheta)$.

For the other implication, we start by observing that $\ell\mathrm{L}([\omega]) = (n+1, 0)$ if and only if $M_\omega = G$. In particular, the trivial class is determined by its G-levels. We assume now that $[\omega], [\vartheta]$ are non-trivial and write $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) = (l, L)$. We will construct $(\sigma, \lambda) \in A$ such that $[\vartheta] = (\sigma, \lambda)[\omega]$. To this end, we let $x_\omega, y_\omega \in G$, $f_\omega, g_\omega \in \operatorname{Hom}(G; \mathbb{F}_p)$, and $\tilde{M}_\omega \leq M_\omega$ be equivalents of $x, y, f, g, \tilde{M}$ in Lemma 5.5 for M_ω. Analogously, we let $x_\vartheta, y_\vartheta, f_\vartheta, g_\vartheta$, and $\tilde{M}_\vartheta$ be associated with M_ϑ. Observe that $[\omega] = [f_\omega \cup g_\omega]$ and $[\vartheta] = [f_\vartheta \cup g_\vartheta]$. We now choose an isomorphism $\tilde{M}_\omega \to \tilde{M}_\vartheta$ and extend it to an automorphism $\sigma \in \operatorname{Aut}(G)$ satisfying $\sigma(x_\omega) = x_\vartheta$ and $\sigma(y_\omega) = y_\vartheta$. It is now a straightforward calculation to show that $(\sigma, 1)[\omega] = [\vartheta]$. □

5.2. **Inclusion of the kernels.** Until the end of Section 5.2, we work under the assumption that $[c] \neq 0$; then $T = \ker \tilde{c} + pG$ is maximal in G. We additionally assume that $M + M_\omega + M_\vartheta \subseteq T$ and observe that $[\omega], [\vartheta] \neq 0$ and $i_c([\omega]) = i_c([\vartheta]) = 0$. In this section we prove Proposition 5.6, which coincides with Proposition 5.1 under the last assumptions.

Proposition 5.6. *One has $[\omega] \sim_{A_c} [\vartheta]$ if and only if $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta])$.*

The next result explains why the values $\ell\mathrm{L}_c([\omega])$ and $\ell\mathrm{L}_c([\vartheta])$ do not appear in Proposition 5.6.

Proposition 5.7. *Write $\ell\mathrm{L}(M) = (l, L)$ and $\ell\mathrm{L}_T(M) = (l_c, L_c)$. Then the following hold:*

(1) *$G[p^l] \subseteq T$ is equivalent to $l = l_c = L_c < L$,*
(2) *$G[p^l] \not\subseteq T$ is equivalent to $l \leq l_c = L_c = L$.*

Proof. By Lemma 3.8, we have $l \leq l_c \leq L_c \leq L$ and, since T is maximal, Corollary 3.4 yields $l_c = L_c$.

(1) Assume, for a start, that $G[p^l] \subseteq T$. Since $G[p^l]$ is not contained in M, we have that

$$T = G[p^l] + M = T[p^l] + M = T[p^l] + (M \cap T)$$

so the minimality of L_c yields $l = L_c$. Moreover, since $G = G[p^L] + M$, we also have that $L > l$.

Assume now that $l = l_c = L_c < L$ and, for a contradiction, that $G[p^l]$ is not contained in T. We then have that

$$G = G[p^l] + T = G[p^l] + M + T[p^{L_c}] = G[p^l] + M,$$

contradicting the minimality of L.

(2) Assume first that $G[p^l]$ is not contained in T. Then we have

$$G = T + G[p^l] = M + T[p^{L_c}] + G[p^l] = M + G[p^{L_c}]$$

and so the minimality of L yields $L = L_c$. The other implication follows from (1). □

The rest of the section is devoted to proving Proposition 5.6.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Lemma 5.8. *Write* $\ell\mathrm{L}(M) = (l, L)$. *Then there exist* $y \in \mathcal{B}$ *and* $\tilde{M} \subseteq M$ *such that* $G = \langle b \rangle \oplus \langle y \rangle \oplus \tilde{M}$ *and*

$$(|b|, |y|) = \begin{cases} (p^l, p^L) & \text{if } G[p^l] \not\subseteq T, \\ (p^L, p^l) & \text{if } G[p^l] \subseteq T. \end{cases}$$

Proof. Let x, y, and $\tilde{M}$ be as in Lemma 5.5: since T/M is cyclic of order p, we have that $x = b$ or $y = b$. By renaming y to be the element of $\{x, y\}$ that is not equal to b, we get the claim. □

Proof of Proposition 5.6. The implication from left to right follows in a straightforward way from Proposition 3.10. We now show that the other direction also holds true. For this, write $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) = (l, L)$. Let $(y_\omega, \tilde{M}_\omega)$ and $(y_\vartheta, \tilde{M}_\vartheta)$ be the equivalents of the pair $(y, \tilde{M})$ from Lemma 5.8 respectively for M_ω and M_ϑ. It follows that $|y_\omega| = |y_\vartheta|$ and $\tilde{M}_\omega \cong \tilde{M}_\vartheta$. We now let $\sigma \in \mathrm{Aut}(G)$ be such that

$$\sigma(b) = b, \quad \sigma(y_\omega) = y_\vartheta, \quad \sigma(\tilde{M}_\omega) = \tilde{M}_\vartheta.$$

By construction, $(\sigma, 1)$ stabilizes T and satisfies $(\sigma, 1) \cdot M_\vartheta = M_\omega$. Let $\lambda \in \mathbb{Z}_p^*$ be such that $(\sigma, \lambda) \in A_c$, the existence of λ being guaranteed by Corollary 3.11. Set $a = (\sigma, \lambda)$. Then we have that $a \in A_c$ satisfies $a(T, M_\vartheta) = (T, M_\omega)$ and thus, as a consequence of Corollary 3.11, the elements $[\omega]$ and $[\vartheta]$ are conjugate under A_c up to a scalar. Lemma 2.6(2) yields the claim. □

5.3. **Incomparable kernels.** Until the end of Section 5.3, we work under the following additional assumptions. Assume that $[c] \neq 0$ and thus that $T = \ker \tilde{c} + pG$ is a maximal subgroup of G. We assume, moreover, that M, M_ω, M_ϑ are not contained in T and that $[\omega], [\vartheta] \neq 0$. In particular, we have that $i_c([\omega]) = i_c([\vartheta]) = 1$ and that $G = M + T = M_\omega + T = M_\vartheta + T$. The goal of the present section is to prove Proposition 5.9, which coincides with Proposition 5.1 under the last assumptions.

Proposition 5.9. *One has* $[\omega] \sim_{A_c} [\vartheta]$ *if and only if* $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta]))$.

The proof of Proposition 5.9 is divided into cases depending on the relations between G-levels and T-levels.

Lemma 5.10. *Write* $\ell\mathrm{L}(M) = (l, L)$ *and* $\ell\mathrm{L}_T(M) = (l_c, L_c)$. *Then there exist* $f, g \in \mathrm{Hom}(G, \mathbb{F}_p)$, $x, y \in \{b_1, \ldots, b_r\}$ *of orders respectively* p^{l_c} *and* p^{L_c}, *and* $\tilde{M} \subseteq \ker \tilde{c} \cap M$ *such that the following hold:*

(1) $M = \ker f \cap \ker g$,
(2) $f(x) = 1$, $g(x) = 0$, $f(y) = 0$, *and* $g(y) = 1$,
(3) $G = \langle b \rangle \oplus \langle x \rangle \oplus \langle y \rangle \oplus \tilde{M}$.

Moreover, there exist two distinct elements in $\{b, x, y\}$ *of orders respectively* p^l *and* p^L.

Proof. Let x, y be as in Lemma 5.2, where $\mathcal{C}$ is taken to be $\mathcal{B}$. Then (1) and (2) follow directly from Lemma 2.12. We now prove (3). To this end, define $\mathcal{B}' = \{pb, b_1, \ldots, b_{r+1}\}$ and let $M' = M \cap T$, which has index p^2 in T and contains pG. Then, with T, $\mathcal{B}'$ and M' in the roles of G, $\mathcal{C}$ and M, Lemma 5.2 yields $x, y \in \mathcal{B}'$ such that $T = \langle x, y \rangle + M'$ and $(|x|, |y|) = (p^{l_c}, p^{L_c})$. Since $pb \in M'$, we derive that $x, y \in \mathcal{B} \setminus \{b\}$

and in particular $x, y \in \ker \tilde{c}$. Now applying Theorem 5.3 to T, M' and $H = \ker \tilde{c}$, we get a subgroup $\tilde{M} \subseteq M' \cap \ker \tilde{c}$ such that $\ker \tilde{c} = \langle x \rangle \oplus \langle y \rangle \oplus \tilde{M}$. Thanks to Lemma 5.2, two elements out of $\mathcal{C} = \{b, x, y\}$ have orders p^l and p^L and so we are done. □

Recall that, by Lemma 3.8, we have that $\ell(M) \leq \ell_T(M) \leq \mathrm{L}(M) \leq \mathrm{L}_T(M)$ and so, from the last result, we derive the following corollary in a straightforward way.

Corollary 5.11. *One has $\ell(M) = \ell_T(M)$ or $\ell_T(M) = \mathrm{L}(M)$ or $\mathrm{L}(M) = \mathrm{L}_T(M)$.*

Until the end of Section 5.3, we let x, y, and $\tilde{M}$ be as in Lemma 5.10. We also write $\ell\mathrm{L}(M) = (l, L)$ and $\ell\mathrm{L}_T(M) = (l_c, L_c)$.

Lemma 5.12. *There exist $\alpha, \delta \in \mathbb{Z}_p$ such that $b_M = b - \alpha x - \delta y \in M \setminus (M \cap T)$ and*

$$(\alpha, \delta) \in \begin{cases} \mathbb{Z}_p \times \mathbb{Z}_p & \text{if } l = l_c \leq L = L_c, \\ \mathbb{Z}_p^* \times \{0\} & \text{if } l < l_c < L = L_c, \\ \mathbb{Z}_p \times \mathbb{Z}_p^* & \text{otherwise.} \end{cases}$$

Moreover, if $l = l_c \leq L = L_c$, then b_M and b have the same order.

Proof. We start by recalling that $G = \langle x, y \rangle + M$ and M contains pG and has index p^2 in G. As a consequence there exist uniquely determined $\alpha, \delta \in \{0, \ldots, p-1\}$ and $b_M \in M$ with the property that $b = \alpha x + \delta y + b_M$. Fix such triple and note that $b_M \notin M \cap T$ because $b \notin T$ while $x, y \in T$. We will prove the following:

(*i*) if $l = l_c \leq L = L_c$, then $|b| = |b_M|$,
(*ii*) if $l < l_c < L = L_c$, then $\alpha \neq 0$ and $\delta = 0$,
(*iii*) in all other cases $\delta \neq 0$.

We start by assuming that $l = l_c \leq L = L_c$. If $|b| \geq p^L$, then clearly $|b| = |b_M|$ and, if $|b| < p^l$, then $b \in M$ and thus again $|b| = |b_M|$. We assume in conclusion that $p^l \leq |b| < p^L$. In this case $\delta = 0$ because otherwise $y \in \langle b, x \rangle + M$ yielding to the contradiction $G = \langle b, x \rangle + M = G[p^{L-1}] + M$. Since $\delta = 0$, we readily derive $|b| = |b_M|$.

Assume now that $l < l_c < L = L_c$. As one of b, x, y has order p^l, we have that $|b| = p^l$. Thus, if δ were nonzero, we would get a similar contradiction as the one from the previous case. Note that, δ being zero, α cannot be otherwise we would have $b \in M$. This would yield a contradiction because, in such case, we would have that

$$G[p^l] = \langle x^{p^{l_c - l}} \rangle \oplus \langle y^{p^{L_c - l}} \rangle \oplus \langle b \rangle \oplus \tilde{M}[p^l] \subseteq pG + M = M,$$

contradicting the minimality of l.

We conclude by looking at the remaining cases. Assume first that $L < L_c$. Since two of the elements b, x, y have order p^l and p^L, we have $|b|, |x| \leq p^L < p^{L_c}$. If, for a contradiction, δ were zero, we would have

$|b_M| < p^{L_c}$ and consequently

$$G = M + G[p^L] = (M \cap T) + \langle b_M \rangle + G[p^L] = (M \cap T) + G[p^{L_c - 1}].$$

In particular, this would imply that $T = (M \cap T) + T[p^{L_c-1}]$, contradicting the definition of L_c. We are now left with considering the case $l < l_c = L = L_c$. It follows from Lemma 5.10 that $|b| = p^l$ and, in particular, b is not contained in M. Now, the elements x and y having the same orders, we assume without loss of generality that δ is invertible. □

Lemma 5.13. *Assume that* $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta])) = (l, L, l_c, L_c)$ *and, additionally, that* $l = l_c \leq L = L_c$. *Then one has* $[\omega] \sim_{A_c} [\vartheta]$.

Proof. Let $f_\omega, g_\omega, f_\vartheta, g_\vartheta$ play the roles of f and g from Lemma 5.10 respectively for M_ω and M_ϑ. Let, analogously $x_\omega, y_\omega, x_\vartheta, y_\vartheta \in \ker \tilde{c}$ play the roles of x and y and let moreover $\tilde{M}_\omega$ and $\tilde{M}_\vartheta$ play the roles of $\tilde{M}$. Write b_ω and b_ϑ for the equivalents of b_M, which we know have the same order thanks to the case $l = l_c \leq L = L_c$ in Lemma 5.12. We have that

$$G = \langle b_\omega \rangle \oplus \langle x_\omega \rangle \oplus \langle y_\omega \rangle \oplus \tilde{M}_\omega = \langle b_\vartheta \rangle \oplus \langle x_\vartheta \rangle \oplus \langle y_\vartheta \rangle \oplus \tilde{M}_\vartheta.$$

Let now $\lambda \in \mathbb{Z}_p$ be such that $\tilde{c}(b_\vartheta) = \lambda \tilde{c}(b_\omega)$ and note that such λ exists by the definition of b_M. Let, moreover, $\sigma : G \to G$ be an isomorphism satisfying

$$x_\omega \mapsto x_\vartheta, \quad y_\omega \mapsto \lambda y_\vartheta, \quad b_\omega \mapsto b_\vartheta, \quad \sigma(\tilde{M}_\omega) = \tilde{M}_\vartheta.$$

By construction, $a = (\sigma, \lambda)$ belongs to A_c and satisfies $a[\omega] = [\vartheta]$. □

Lemma 5.14. *Assume that* $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta])) = (l, L, l_c, L_c)$ *and, additionally, that* $l < l_c < L = L_c$. *Then one has* $[\omega] \sim_{A_c} [\vartheta]$.

Proof. Let $f_\omega, g_\omega, f_\vartheta, g_\vartheta$ play the roles of f and g from Lemma 5.10 respectively for M_ω and M_ϑ. Let, analogously $x_\omega, y_\omega, x_\vartheta, y_\vartheta \in \ker \tilde{c}$ play the roles of x and y and let moreover $\tilde{M}_\omega$ and $\tilde{M}_\vartheta$ play the roles of $\tilde{M}$. Write $b_\omega = b - \alpha_\omega x_\omega$ and $b_\vartheta = b - \alpha_\vartheta x_\vartheta$ for the equivalents of b_M from Lemma 5.12; then $b_\omega \in \ker g_\omega$ and $b_\vartheta \in \ker g_\vartheta$. Let now $\lambda = \alpha_\vartheta \alpha_\omega^{-1}$ and let $\sigma : G \to G$ be an isomorphism satisfying

$$x_\omega \mapsto \lambda x_\vartheta, \quad y_\omega \mapsto \lambda^{-1} y_\vartheta, \quad b \mapsto b, \quad \sigma(\tilde{M}_\omega) = \tilde{M}_\vartheta.$$

By construction we have $(\sigma, 1)\tilde{c} = \tilde{c}$ and $(\sigma, 1)[\omega] = [\vartheta]$. □

Lemma 5.15. *Assume that* $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta])) = (l, L, l_c, L_c)$ *and, additionally, that* $l < l_c = L = L_c$ *or* $L < L_c$. *Then one has* $[\omega] \sim_{A_c} [\vartheta]$.

Proof. Let $f_\omega, g_\omega, f_\vartheta, g_\vartheta$ play the roles of f and g from Lemma 5.10 respectively for M_ω and M_ϑ. Let, analogously $x_\omega, y_\omega, x_\vartheta, y_\vartheta \in \ker \tilde{c}$ play the roles of x and y and let moreover $\tilde{M}_\omega$ and $\tilde{M}_\vartheta$ play the roles of

$\tilde{M}$. Write $b_\omega = b - \alpha_\omega x_\omega - \delta_\omega y_\omega$ and $b_\vartheta = b - \alpha_\vartheta x_\vartheta - \delta_\vartheta y_\vartheta$ for the equivalents of b_M from Lemma 5.12. Let now $\lambda = \delta_\vartheta \delta_\omega^{-1}$ and let $\sigma : G \to G$ be an isomorphism satisfying

$$x_\omega \mapsto x_\vartheta, \quad y_\omega \mapsto \lambda y_\vartheta - \delta_\omega^{-1}(\alpha_\omega - \alpha_\vartheta)x_\vartheta, \quad b \mapsto b, \quad \sigma(\tilde{M}_\omega) = \tilde{M}_\vartheta.$$

We start by observing that by construction $(\sigma, 1)\tilde{c} = \tilde{c}$; moreover, $\sigma(M_\omega) = M_\vartheta$ and $\sigma(T) = T$. It follows from Corollary 3.11 that, up to a scalar, the elements $[\omega]$ and $[\vartheta]$ are conjugate under A_c. Lemma 2.6(2) yields the claim. □

Proof of Proposition 5.9. The implication from left to right follows in a straightforward way from Proposition 3.10. We show the opposite one holds, too. Assume that $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) = (l, L)$ and $\ell\mathrm{L}_c([\omega]) = \ell\mathrm{L}_c([\vartheta]) = (l_c, L_c)$. By Lemma 3.8 we have that $l \leq l_c \leq L \leq L_c$. In case $(l, L) = (l_c, L_c)$, we are done by Lemma 5.13. Morover, if $l < l_c < L$, then we apply Lemma 5.14. The leftover cases are $L < L_c$ and $l < l_c = L = L_c$, which we resolve using Lemma 5.15. □

Proof of Proposition 5.1. The implication (1) ⇒ (2) is given by Proposition 3.10(3). We now prove that (2) ⇒ (1). For this, we assume that $(\ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega]), i_c([\omega])) = (\ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_c([\vartheta]), i_c([\vartheta]))$. If $[c] = 0$, then $i_c([\omega]) = i_c([\vartheta]) = 0$ and $\ell\mathrm{L}_c([\omega]) = \ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) = \ell\mathrm{L}_c([\vartheta])$; we conclude by applying Proposition 5.4. Assume now that $[c] \neq 0$. We note that $\ell\mathrm{L}([\omega]) = (n+1, 0)$ if and only if $M_\omega = G$, equivalently $[\omega] = 0$. In particular, if $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) = (n+1, 0)$, then $[\omega] = [\vartheta]$. Assume now that $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta]) \neq (n+1, 0)$ and so $[\omega]$ and $[\vartheta]$ are non-trivial. We finish by applying Propositions 5.6 and 5.9. □

6. Main result and applications

We devote the present section to the proof of our main Theorem 6.1 and to presenting some of its applications. In Sections 6.2 and 6.3 we explicitly compute the orbit sizes of the action of A on $\mathrm{H}^2(G; \mathbb{F}_p)$ respectively in the cases of 2-generated and 3-generated abelian p-groups, equivalently the cases when $r = 1$ resp. $r = 2$. We remark that in such cases the sizes of orbits are polynomial in p. We do not discuss the case of cyclic G, i.e. $r = 0$, as in such case $\mathrm{H}^2(G; \mathbb{F}_p) = \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$; see Section 2.2. In Section 6.4, we collect some general remarks regarding the computability of the A-orbits in $\mathrm{H}^2(G; \mathbb{F}_p)$. Until the end of Section 6, we denote by $\mathcal{O}$ the collection of orbits of the action of A on $\mathrm{H}^2(G; \mathbb{F}_p)$ and by $\mathfrak{S} = (|o|)_{o \in \mathcal{O}}$ the vector of the orbit sizes. For a more informative presentation of the data, the vector $\mathfrak{S}$ will be decorated by vertical bars to isolate

- the vector $\mathbf{o}$ of orbits associated to elements of $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$,
- each vector of orbits derived from a fixed orbit choice in $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$, following the order in $\mathbf{o}$.

Redundant brackets are ignored in the display of $\mathfrak{S}$.

6.1. The main theorem.

The following is our main result, which gives a combinatorial description of the A-orbits of the A-stable subset $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p) \times \mathrm{Im}\cup$ of $\mathrm{H}^2(G; \mathbb{F}_p)$.

Theorem 6.1. *Let $[c], [d] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ and $[\omega], [\vartheta] \in \mathrm{Im}\cup$. Then the following are equivalent:*

(1) $[c]+[\omega] \sim_A [d]+[\vartheta]$, *and*
(2) $(\ell\mathrm{L}([c]), \ell\mathrm{L}([\omega]), \ell\mathrm{L}_c([\omega]), i_c([\omega])) = (\ell\mathrm{L}([d]), \ell\mathrm{L}([\vartheta]), \ell\mathrm{L}_d([\vartheta]), i_d([\vartheta]))$.

Proof. (1) $\Rightarrow$ (2) Assume that $[c]+[\omega] \sim_A [d]+[\vartheta]$ and let $a=(\sigma,\lambda)\in A$ be such that $a\cdot[c]+a\cdot[\omega] = a\cdot([c]+[\omega]) = [d]+[\vartheta]$. With the notation from Proposition 3.10, we then have that $[\vartheta] = a\cdot[\omega] = [\omega_a]$ and thus $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta])$, $\ell\mathrm{L}_c([\omega]) = \ell\mathrm{L}_d([\vartheta])$, $\ell\mathrm{L}([c]) = \ell\mathrm{L}([d])$, and $i_c([\omega]) = i_d([\vartheta])$.

(2) $\Rightarrow$ (1) Assume that $\ell\mathrm{L}([\omega]) = \ell\mathrm{L}([\vartheta])$, $\ell\mathrm{L}_c([\omega]) = \ell\mathrm{L}_d([\vartheta])$, $\ell\mathrm{L}([c]) = \ell\mathrm{L}([d])$, and $i_c([\omega]) = i_d([\vartheta])$. Then, thanks to Proposition 4.1, there exists $a\in A$ such that $a\cdot[c]=[d]$. Fix such a. Then, by Proposition 3.10, we have that $a\cdot([c]+[\omega]) = [d]+[\omega_a]$ and, as a consequence, also that $\ell\mathrm{L}([\vartheta]) = \ell\mathrm{L}([\omega_a])$, $\ell\mathrm{L}_d([\vartheta]) = \ell\mathrm{L}_d([\omega_a])$, and $i_d([\vartheta]) = i_d([\omega_a])$. Now, Proposition 5.1 yields that there exists $a'\in A_d$ such that $a'\cdot[\omega_a]=[\vartheta]$ and thus such that $a'a\cdot([c]+[\omega]) = [d]+[\vartheta]$. □

We remark that, in view of Proposition 4.1, one could replace $\ell\mathrm{L}([c])$ in Theorem 6.1 with any of $\ell([c])$ or $\mathrm{L}([c])$ and, symmetrically, $\ell\mathrm{L}([d])$ with $\ell([d])$ or $\mathrm{L}([d])$. We explicitly compute the vectors in Theorem 6.1(2) in Sections 6.2 and 6.3, in the case when G has a minimal generating set of 2 or 3 elements, respectively. It would be interesting to understand the combinatorial nature of the collection of such vectors for an arbitrary number of generators.

6.2. **The case of 2-generated groups.** Assume that $G = \mathbb{Z}/(p^{m_1})\oplus\mathbb{Z}/(p^{m_2})$ for positive integers $m_1\le m_2$ and, in the case that $p=2$, assume that $m_1>1$. We will show that the following hold:

$$|\mathcal{O}| = \begin{cases} 4 & \text{if } m_1=m_2,\\ 6 & \text{otherwise},\end{cases}$$

and

$$\mathfrak{S} = \begin{cases} (1, p^2-1 \mid p-1, (p-1)(p^2-1)) & \text{if } m_1=m_2,\\ (1, p-1, p^2-p \mid p-1, (p-1)^2, (p-1)(p^2-p)) & \text{otherwise.}\end{cases}$$

Thanks to Proposition 4.1, the subspace $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ consists of 2 or 3 orbits under A respectively when $m_1=m_2$ or $m_1\neq m_2$. Let now $[\omega]\in\operatorname{Im}\cup$. Then we have that

$$M_\omega = \begin{cases} G & \text{if } [\omega]=0,\\ pG & \text{otherwise,}\end{cases}$$

and, in particular, $i_c([\omega])=1$ if and only if $[c]\neq 0$ and $[\omega]=0$. Since both G and pG are characteristic in G, it follows from Lemma 2.6 that, for each $[c]\in\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$, the set $\operatorname{Im}\cup$ is the union of two orbits under A_c with cardinalities 1 and $p-1$. Now, the cup product being surjective (see Section 2.6) onto $\langle\operatorname{Im}\cup\rangle$, it follows that the number of orbits is twice the number of orbits in $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ and their sizes are

$$\mathfrak{S} = \begin{cases} (1, p^2-1 \mid p-1, (p-1)(p^2-1)) & \text{if } m_1=m_2,\\ (1, p-1, p^2-p \mid p-1, (p-1)^2, (p-1)(p^2-p)) & \text{otherwise.}\end{cases}$$

For completeness, we include the levels-indices vectors from Theorem 6.1(2). If $\boxed{m_1=m_2}$, then we have

	$[\omega]=0$	$[\omega]\neq 0$
$[c]=0$	$(m_1+1,0 \mid m_1+1,0 \mid m_1+1,0 \mid 0)$	$(m_1+1,0 \mid m_1,m_1 \mid m_1,m_1 \mid 0)$
$[c]\neq 0$	$(m_1,m_1 \mid m_1+1,0 \mid m_1+1,0 \mid 1)$	$(m_1,m_1 \mid m_1,m_1 \mid m_1,m_1 \mid 0)$

while, if $\boxed{m_1 \neq m_2}$, the vectors are

	$[\omega]=0$	$[\omega]\neq 0$
$[c]=0$	$(m_2+1,0 \mid m_2+1,0 \mid m_2+1,0 \mid 0)$	$(m_2+1,0 \mid m_2,m_2 \mid m_2,m_2 \mid 0)$
$[c]=\beta(\gamma_1^*)$	$(m_1,m_1 \mid m_2+1,0 \mid m_2+1,0 \mid 1)$	$(m_1,m_1 \mid m_1,m_2 \mid m_2,m_2 \mid 0)$
$[c]=\beta(\gamma_2^*)$	$(m_2,m_2 \mid m_2+1,0 \mid m_2,0 \mid 1)$	$(m_2,m_2 \mid m_1,m_2 \mid m_1,m_1 \mid 0)$

6.3. **The case of 3-generated groups.** Assume that $G=\mathbb{Z}/(p^{m_1})\oplus\mathbb{Z}/(p^{m_2})\oplus\mathbb{Z}/(p^{m_3})$ where $m_1\leq m_2\leq m_3$ are positive integers with the additional condition that, if $p=2$, then $m_1>1$. We will show that the following hold:

$$\mid\mathcal{O}\mid=\begin{cases}5 & \text{if } m_1=m_2=m_3,\\ 11 & \text{if } m_1<m_2=m_3,\\ 11 & \text{if } m_1=m_2<m_3,\\ 19 & \text{if } m_1<m_2<m_3.\end{cases}$$

We will, additionally, give the orbit sizes in each of the listed cases. For this, note that, as a consequence of Proposition 4.1, the sizes of the A-orbits of $\mathrm{H}^2_{\mathrm{ab}}(G;\mathbb{F}_p)$ are

$$\mathfrak{S}_{\mathrm{ab}}=\begin{cases}(1,p^3-1) & \text{if } m_1=m_2=m_3,\\ (1,p-1,p^3-p) & \text{if } m_1<m_2=m_3,\\ (1,p^2-1,p^3-p^2) & \text{if } m_1=m_2<m_3,\\ (1,p-1,p^2-p,p^3-p^2) & \text{if } m_1<m_2<m_3.\end{cases}$$

We proceed by looking at the specific cases, one by one. For this, observe that $\mathrm{Im}\cup=\langle\mathrm{Im}\cup\rangle$ and $\dim_{\mathbb{F}_p}\mathrm{Im}\cup=3$; see Sections 2.2 and 2.6.

We start by assuming that $\boxed{m_1=m_2=m_3}$. Let $[c]\in\{0,\beta(\gamma_1^*)\}$ and write $[\omega]$ for a generic element in $\mathrm{Im}\cup$. Then, following the notation in Theorem 6.1(2), we obtain the following possible values parametrizing the A-orbits in $\mathrm{H}^2(G;\mathbb{F}_p)$:

	$[0]$	$[\omega]\neq 0$
$[c]=0$	$(m_1+1,0 \mid m_1+1,0 \mid m_1+1,0 \mid 0)$	$(m_1+1,0 \mid m_1,m_1 \mid m_1+1,0 \mid 0)$
$[c]\neq 0$	$(m_1,m_1 \mid m_1+1,0 \mid m_1+1,0 \mid 1)$	$(m_1,m_1 \mid m_1,m_1 \mid m_1,m_1 \mid 0)$
		$(m_1,m_1 \mid m_1,m_1 \mid m_1,m_1 \mid 1)$

In particular, $\mathrm{Im}\cup\setminus\{0\}$ consists of a unique A-orbit of cardinality p^3-1. Assume now that $[c]=\beta(\gamma_1^*)$. In this case, we obtain

- $\mathcal{I}_0=\{[\omega]\in\mathrm{Im}\cup\setminus\{0\}: i_c([\omega])=0\}=\{\lambda_1[v_{11}^*\cup v_{21}^*]+\lambda_2[v_{11}^*\cup v_{31}^*]:\lambda_i\in\mathbb{F}_p,(\lambda_1,\lambda_2)\neq(0,0)\}$,

- $\mathcal{I}_1 = \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : i_c([\omega]) = 1\} = \{\lambda_1[v_{11}^* \cup v_{21}^*] + \lambda_2[v_{11}^* \cup v_{31}^*] + \lambda_3[v_{21}^* \cup v_{31}^*] : \lambda_i \in \mathbb{F}_p,\ \lambda_3 \neq 0\}$.

It follows that $|\mathcal{I}_0| = p^2 - 1$ and $|\mathcal{I}_1| = p^3 - p^2$ and thus Proposition 5.1 yields that

$$\mathfrak{S} = (1, p^3 - 1 \mid p^3 - 1 \mid (p^3 - 1)(p^2 - 1), (p^3 - 1)(p^3 - p^2)).$$

Assume now that $\boxed{m_1 < m_2 = m_3}$. Define $[c_1] = \beta(\gamma_1^*)$ and $[c_2] = \beta(\gamma_2^*)$. Write, moreover, $[\omega]$ for a generic element in $\mathrm{Im}\cup$. Then, following the notation in Theorem 6.1(2), the values parametrizing the A-orbits in $\mathrm{H}^2(G;\mathbb{F}_p)$ are collected below:

	$[\omega] = 0$	$[\omega] \neq 0$
$[c] = 0$	$(m_2+1, 0 \mid m_2+1, 0 \mid m_2+1, 0 \mid 0)$	$(m_2+1, 0 \mid m_1, m_2 \mid m_1, m_2 \mid 0)$
		$(m_2+1, 0 \mid m_2, m_2 \mid m_2, m_2 \mid 0)$
$[c_1] = \beta(\gamma_1^*)$	$(m_1, m_1 \mid m_2+1, 0 \mid m_2+1, 0 \mid 1)$	$(m_1, m_1 \mid m_1, m_2 \mid m_2, m_2 \mid 0)$
		$(m_1, m_1 \mid m_1, m_2 \mid m_2, m_2 \mid 1)$
		$(m_1, m_1 \mid m_2, m_2 \mid m_2, m_2 \mid 1)$
$[c_2] = \beta(\gamma_2^*)$	$(m_2, m_2 \mid m_2+1, 0 \mid m_2+1, 0 \mid 1)$	$(m_2, m_2 \mid m_1, m_2 \mid m_1, m_1 \mid 0)$
		$(m_2, m_2 \mid m_1, m_2 \mid m_1, m_2 \mid 1)$
		$(m_2, m_2 \mid m_2, m_2 \mid m_2, m_2 \mid 0)$

Note also that the two A-orbits in $\mathrm{Im}\cup \setminus \{0\}$ are represented by $[v_{11}^* \cup v_{21}^*]$ and $[v_{21}^* \cup v_{22}^*]$ and correspond respectively to the G-levels (m_1, m_2) and (m_2, m_2). It is a straightforward computation to show that the following hold:

$$\begin{aligned}
\mathcal{I}_0^1(m_1,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_1,m_2), i_{c_1}([\omega]) = 0\}\\
&= \{\lambda_1[v_{11}^* \cup v_{21}^*] + \lambda_2[v_{11}^* \cup v_{22}^*] : \lambda_i \in \mathbb{F}_p, (\lambda_1,\lambda_2) \neq (0,0)\},\\
\mathcal{I}_1^1(m_1,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_1,m_2), i_{c_1}([\omega]) = 1\}\\
&= \{\lambda_1[v_{11}^* \cup v_{21}^*] + \lambda_2[v_{11}^* \cup v_{22}^*] + \lambda_3[v_{21}^* \cup v_{22}^*] : \lambda_i \in \mathbb{F}_p,\ (\lambda_1,\lambda_2) \neq (0,0), \lambda_3 \neq 0\},\\
\mathcal{I}_1^1(m_2,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_2,m_2), i_{c_1}([\omega]) = 1\}\\
&= \{\lambda_3[v_{21}^* \cup v_{22}^*] : \lambda_3 \in \mathbb{F}_p,\ \lambda_3 \neq 0\},\\
\mathcal{I}_0^2(m_1,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_1,m_2), i_{c_2}([\omega]) = 0\}\\
&= \{\lambda_1[v_{11}^* \cup v_{21}^*] + \lambda_2[v_{21}^* \cup v_{22}^*] : \lambda_i \in \mathbb{F}_p, \lambda_1 \neq 0\},\\
\mathcal{I}_0^2(m_2,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_2,m_2), i_{c_2}([\omega]) = 0\}\\
&= \{\lambda_2[v_{21}^* \cup v_{22}^*] : \lambda_2 \in \mathbb{F}_p, \lambda_2 \neq 0\},\\
\mathcal{I}_1^2(m_1,m_2) &= \{[\omega] \in \mathrm{Im}\cup \setminus \{0\} : \ell\mathrm{L}([\omega]) = (m_1,m_2), i_{c_2}([\omega]) = 1\}\\
&= \{\lambda_1[v_{11}^* \cup v_{21}^*] + \lambda_2[v_{21}^* \cup v_{22}^*] + \lambda_3[v_{11}^* \cup v_{22}^*] : \lambda_i \in \mathbb{F}_p,\ \lambda_3 \neq 0\}.
\end{aligned}$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

It follows that

$$|\mathcal{I}_0^1(m_1,m_2)| = p^2-1, \quad |\mathcal{I}_1^1(m_2,m_2)| = p-1, \quad |\mathcal{I}_1^1(m_1,m_2)| = p^3-p^2-p+1,$$
$$|\mathcal{I}_0^2(m_1,m_2)| = p^2-p, \quad |\mathcal{I}_0^2(m_2,m_2)| = p-1, \quad |\mathcal{I}_1^2(m_1,m_2)| = p^3-p^2,$$

and so we derive from our table of possibilities and Theorem 6.1 that

$$\begin{aligned}\mathfrak{S} = (&1, p-1, p^3-p \mid p^3-p, p-1 \mid \\ &(p-1)(p^2-1), (p-1)^2, (p-1)(p^3-p^2-p+1) \mid \\ &(p^3-p)(p^2-p), (p^3-p)(p-1), (p^3-p)(p^3-p^2)).\end{aligned}$$

We have developed the current case in full detail to show how Theorem 6.1 yields the orbit count. One can compute the orbit sizes in the remaining cases in a similar manner and so we present them in a slightly more synthetic way.

Assume that $\boxed{m_1 = m_2 < m_3}$. Write $[c_1] = \beta(\gamma_1^*)$ and $[c_2] = \beta(\gamma_2^*)$. We also write $[\omega]$ for a generic element in $\mathrm{Im}\cup$. Then, following the notation in Theorem 6.1(2), the values parametrizing the A-orbits in $\mathrm{H}^2(G;\mathbb{F}_p)$ are listed in the next table:

	$[\omega]=0$	$[\omega]\neq 0$
$[c]=0$	$(m_3+1,0 \mid m_3+1,0 \mid m_3+1 \mid 0)$	$(m_3+1,0 \mid m_1,m_1 \mid m_1,m_1 \mid 0)$
		$(m_3+1,0 \mid m_1,m_3 \mid m_1,m_3 \mid 0)$
$[c_1]=\beta(\gamma_1^*)$	$(m_1,m_1 \mid m_3+1,0 \mid m_3+1,0 \mid 1)$	$(m_1,m_1 \mid m_1,m_1 \mid m_1,m_1 \mid 0)$
		$(m_1,m_1 \mid m_1,m_1 \mid m_1,m_3 \mid 1)$
		$(m_1,m_1 \mid m_1,m_3 \mid m_3,m_3 \mid 0)$
		$(m_1,m_1 \mid m_1,m_3 \mid m_1,m_3 \mid 1)$
$[c_2]=\beta(\gamma_2^*)$	$(m_3,m_3 \mid m_3+1,0 \mid m_3,0 \mid 1)$	$(m_3,m_3 \mid m_1,m_1 \mid m_1,m_1 \mid 1)$
		$(m_3,m_3 \mid m_1,m_3 \mid m_1,m_1 \mid 0)$

We observe that the two A-orbits in $\mathrm{Im}\cup\setminus\{0\}$ are represented by $[v_{11}^*\cup v_{12}^*]$ and $[v_{11}^*\cup v_{21}^*]$ and correspond respectively to the G-levels (m_1,m_1) and (m_1,m_3): these orbits have sizes respectively p^2-1 and p^3-p^2. Analogously to the previous case, one can compute that

$$\begin{aligned}\mathfrak{S} = (&1, p^2-1, p^3-p^2 \mid p^3-p^2, p^2-1 \mid \\ &(p^2-1)(p^2-p), (p^2-1)(p^3-2p^2+p), (p^2-1)(p-1), (p^2-1)(p^2-p) \mid \\ &(p^3-p^2)^2, (p^3-p^2)(p^2-1)).\end{aligned}$$

We conclude with the case $\boxed{m_1 < m_2 < m_3}$. Write $[c_1] = \beta(\gamma_1^*)$, $[c_2] = \beta(\gamma_2^*)$, and $[c_3] = \beta(\gamma_3^*)$. Analogously to the previous cases, we collect the possible levels-indices vectors from Theorem 6.1(2) in the next table:

	$[\omega]=0$	$[\omega]\neq 0$
$[c]=0$	$(m_3+1,0 \mid m_3+1,0 \mid m_3+1 \mid 0)$	$(m_3+1,0 \mid m_1,m_2 \mid m_1,m_2 \mid 0)$
		$(m_3+1,0 \mid m_1,m_3 \mid m_1,m_3 \mid 0)$
		$(m_3+1,0 \mid m_2,m_3 \mid m_2,m_3 \mid 0)$
$[c_1]=\beta(\gamma_1^*)$	$(m_1,m_1 \mid m_3+1,0 \mid m_3+1,0 \mid 1)$	$(m_1,m_1 \mid m_1,m_2 \mid m_2,m_2 \mid 0)$
		$(m_1,m_1 \mid m_1,m_2 \mid m_2,m_3 \mid 1)$
		$(m_1,m_1 \mid m_1,m_3 \mid m_3,m_3 \mid 0)$
		$(m_1,m_1 \mid m_1,m_3 \mid m_2,m_3 \mid 1)$
		$(m_1,m_1 \mid m_2,m_3 \mid m_2,m_3 \mid 1)$
$[c_2]=\beta(\gamma_2^*)$	$(m_2,m_2 \mid m_3+1,0 \mid m_3+1,0 \mid 1)$	$(m_2,m_2 \mid m_1,m_2 \mid m_1,m_1 \mid 0)$
		$(m_2,m_2 \mid m_1,m_2 \mid m_1,m_3 \mid 1)$
		$(m_2,m_2 \mid m_1,m_3 \mid m_1,m_3 \mid 1)$
		$(m_2,m_2 \mid m_2,m_3 \mid m_3,m_3 \mid 0)$
$[c_3]=\beta(\gamma_3^*)$	$(m_3,m_3 \mid m_3+1,0 \mid m_3,0 \mid 1)$	$(m_3,m_3 \mid m_1,m_2 \mid m_1,m_2 \mid 1)$
		$(m_3,m_3 \mid m_1,m_3 \mid m_1,m_1 \mid 0)$
		$(m_3,m_3 \mid m_2,m_3 \mid m_2,m_2 \mid 0)$

Representatives of the A-orbits of $\mathrm{Im}\cup \setminus \{0\}$ are $[v_{11}^* \cup v_{21}^*]$, $[v_{11}^* \cup v_{31}^*]$, and $[v_{21}^* \cup v_{31}^*]$ corresponding respectively to the levels (m_1,m_2), (m_1,m_3), and (m_2,m_3). As a consequence, one computes that

$$\begin{aligned}\mathfrak{S} = (&1, p-1, p^2-p, p^3-p^2 \mid p^3-p^2, p^2-p, p-1 \mid\\ &(p-1)^2p, (p-1)^3p, (p-1)^2, (p-1)^3, (p-1)^2 \mid\\ &(p^2-p)^2, (p^2-p)(p^3-2p^2+p), (p^2-p)^2, (p^2-p)(p-1) \mid\\ &(p^3-p^2)^2, (p^3-p^2)(p^2-p), (p^3-p^2)(p-1)).\end{aligned}$$

6.4. **Higher number of generators.** In Sections 6.2 and 6.3, we have made use of Theorem 6.1 to compute the orbit sizes of the action of A on $\mathrm{H}^2(G;\mathbb{F}_p)$. As the careful reader might have observed, however, we did not need the full information from the vectors in Theorem 6.1(2) to exploit the cases of 2- and 3-generated groups. In the case of 2-generated groups, the c-levels and c-index can always be derived from the knowledge of $\ell\mathrm{L}([c])$ and $\ell\mathrm{L}([\omega])$ because V has dimension 2. In the case of 3-generated groups, the knowledge of the vector $(\ell\mathrm{L}([c]), \ell\mathrm{L}([\omega]), i_c([\omega]))$ suffices for the computation of $\ell\mathrm{L}_c([\omega])$ because V has only dimension 3. When G requires a generating set of larger cardinality, the full information carried by the vectors described in Theorem 6.1(2) is needed, as the following example shows.

Example 6.2. *Assume p is odd and G is given by*

$$G = \mathbb{Z}/(p) \oplus (\mathbb{Z}/(p^2))^2 \oplus \mathbb{Z}/(p^3) \oplus (\mathbb{Z}/(p^4))^2 = \langle \gamma_{11}, \gamma_{21}, \gamma_{22}, \gamma_{31}, \gamma_{41}, \gamma_{42} \rangle.$$

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

Let moreover T, M, M' be subgroups of G given by

$$T = \langle \gamma_{11}, \gamma_{22}, \gamma_{31}, \gamma_{41}, \gamma_{42} \rangle + pG,$$
$$M = \langle \gamma_{11}, \gamma_{21} - \gamma_{31}, \gamma_{22}, \gamma_{42} \rangle + pG,$$
$$M' = \langle \gamma_{11}, \gamma_{21}, \gamma_{31}, \gamma_{41} \rangle + pG,$$

and observe that T is maximal in G, while G/M and G/M' are elementary abelian of rank 2. Additionally, we have that $\ell\mathrm{L}(M) = (2,4) = \ell\mathrm{L}(M')$ and

$$M \cap T = \langle \gamma_{11}, \gamma_{22}, \gamma_{42} \rangle + pG \text{ and } M' \cap T = \langle \gamma_{11}, \gamma_{31}, \gamma_{41} \rangle + pG$$

and so, in particular, M and M' are not contained in T. Equivalently, if $[c] \in \mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p)$ represents T via (2.6), then $i_c(M) = i_c(M') = 1$. Nevertheless, the T-levels of M and M' do not coincide: indeed one can compute $\ell\mathrm{L}_T(M) = (3,4) \neq (2,4) = \ell\mathrm{L}_T(M')$.

We close the current section and the paper with some observations concerning the determination of the A-orbits in $\mathrm{H}^2(G; \mathbb{F}_p)$ for arbitrary G. Our main theorem allows us to compute the orbits contained in $\mathrm{H}^2_{\mathrm{ab}}(G; \mathbb{F}_p) \times \mathrm{Im}\cup$, which is – for $\mathrm{d}(G) \geq 4$ – a proper subset of $\mathrm{H}^2(G; \mathbb{F}_p)$. A key ingredient in the proof of Theorem 6.1 is Corollary 3.11 and we are confident that a generalization of it to elements of higher rank in $\mathbb{P}\langle \mathrm{Im}\cup \rangle$ will yield a description of the orbits of $\mathrm{H}^2(G; \mathbb{F}_p)$. Such a generalization will most likely build upon the geometry of $\mathbb{P}(\Lambda^2 V)$, which is very well-understood, via identifying its elements with equivalence classes of tuples of subspaces of V. We hope to come back to this interesting problem in a future paper.

Acknowledgments

The authors are very thankful to Bettina Eick for helpful feedback and clarifications regarding this project. The authors also wish to thank the universities of Bielefeld and Düsseldorf, in particular the groups of Christopher Voll respectively Benjamin Klopsch, where part of this collaboration took place. The authors also wish to thank the universities of Bielefeld and D¨usseldorf together with the Max-PlanckInstitute for Mathematics in the Sciences (in particular the groups of Christopher Voll, Benjamin Klopsch, and Bernd Sturmfels), where part of this collaboration took place. The first author was supported by the Spanish Government project PID2020-117281GB-I00, partially by FEDER funds and, by the Basque Government project IT483- 22.

References

[1] H. U. Besche and B. Eick, Construction of finite groups, *J. Symbolic Comput.*, **27** (1999) 387–404.

[2] S. R. Blackburn, Groups of prime power order with derived subgroup of prime order, *J. Algebra*, **219** (1999) 625–657.

[3] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, **87**, Springer–Verlag, New York–Berlin, 1982.

[4] H. Dietrich and B. Eick, *On the groups of cube-free order*, J. Algebra, **292** (2005) 122–137.

http://dx.doi.org/10.22108/ijgt.2022.125417.1651

[5] H. Dietrich, B. Eick and D. Feichtenschlager, Investigating p-groups by coclass with GAP, Computational group theory and the theory of groups, Contemp. Math., **470**, *Amer. Math. Soc.*, Providence, RI, 2008 45–61.

[6] B. Eick and E. A. O'Brien, Enumerating p-groups, *J. Austral. Math. Soc. Ser. A*, **67** (1999) 191–205.

[7] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991.

[8] H. Fitting, Beiträge zur Theorie der Gruppen endlicher Ordnung, *Jahresber. Dtsch. Math.-Ver.*, **48** (1938) 77–141.

[9] J. A. Grochow and Y. Qiao, Algorithms for group isomorphism via group extensions and cohomology, *SIAM J. Comput.*, **46** (2017) 1153–1216.

[10] J. R. Harper, *Secondary cohomology operations*, Graduate Studies in Mathematics, **49**, American Mathematical Society, Providence, RI, 2002.

[11] R. Laue, Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen, *Bayreuth. Math. Schr.*, No. 9 (1982).

[12] J. McCleary, *A user's guide to spectral sequences*, 2nd ed., Cambridge University Press, 2001.

[13] D. V. Millionshchikov and R. Khimenes, Geometry of central extensions of nilpotent Lie algebras, *Tr. Mat. Inst. Steklova*, **305** (2019) 225–249.

[14] S. A. Morris, *Pontryagin duality and the structure of locally compact abelian groups*, London Mathematical Society Lecture Note Series, No. 29, Cambridge University Press, Cambridge-New York-Melbourne, 1977.

[15] M. Michałek and B. Sturmfels, *Invitation to nonlinear algebra*, Graduate Studies in Mathematics, **211**, American Mathematical Society, Providence, RI, 2021.

[16] E. A. O'Brien, The p-group generation algorithm, Computational group theory, Part 1, *J. Symbolic Comput.*, **9** (1990) 677–698.

[17] D. J. S. Robinson, *Applications of cohomology to the theory of groups*, In Campbell, C. M. Groups - St. Andrews 1981, LMS Lecture Note Series, **71**, Cambridge, Cambridge University Press, 1981.

[18] I. R. Shafarevich, *Basic algebraic geometry 1*, Varieties in projective space. Third edition, Translated from the 2007 third Russian edition, Springer, Heidelberg, 2013.

[19] A. C. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, **38**, Cambridge University Press, Cambridge, 1994.

Oihana Garaialde Ocaña

Matematika Saila, Euskal Herriko Unibertsitatearen Zientzia eta Teknologia Fakultatea, Posta-kutxa 644, 48080 Bilbo, Spain

Email: oihana.garayalde@ehu.eus

Mima Stanojkovski

Dipartimento di Matematica, Università di Trento, via Sommarive 14, 38123 Povo (Trento), Italy

Email: mima.stanojkovski@unitn.it

http://dx.doi.org/10.22108/ijgt.2022.125417.1651