COMPUTING THE ADDITIVE STRUCTURE OF INDECOMPOSABLE MODULES OVER DEDEKIND-LIKE RINGS USING GRÖBNER BASES.

MARIA A. AVIÑO-DIAZ AND LUIS D. GARCIA-PUENTE

Abstract. We introduce a general constructive method to find a p-basis (and the Ulm invariants) of a finite Abelian p-group M. This algorithm is based on Gröbner bases theory. We apply this method to determine the additive structure of indecomposable modules over the following Dedeking-like rings: $\mathbb{Z}C_p$, where C_p is the cyclic group of order a prime p, and the $p-$pullback $\{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ of $\mathbb{Z} \oplus \mathbb{Z}$.

1. Introduction

Let R be an algebra. Finding the additive structure of an R-module as an Abelian group associated to a representation is a classical problem solved in a similar way to obtaining the Jordan canonical form of a matrix over a field, see [5, Chapter III] and [2, Chapter 12, §2]. This information is used, for example, to determine the matrices associated to the group representation. This is accomplished by finding a p-basis for the torsion part of the group that permits a unique matrix representation for this Abelian finite p-group. In 1949, Szekeres started the classification and matrix description of modules over $\mathbb{Z}_{p^n}C_p$. Since then it has been studied in detail, see [1, 3, 9, 10, 11, 12, 14]. In [9, 10], Levy studied these modules in the more general context of modules over a pullback of two Dedekind rings with a common field, which he called *Dedekind-like* rings.

Until now, the simplest way to find the additive structure of an R-module consists in writing the relations as a matrix with entries in $\mathbb{Z}$, performing elementary transformations over a Euclidean domain (like $\mathbb{Z}$), and using the division algorithm to write the matrix in a canonical form, see [5, Theorem 16.8]. This approach becomes rather difficult when the generating set is not minimal and there are several relations among the generators. In here, we present a different method that has the advantage of producing different group presentations by writing the relations as polynomials and changing the term orders used to reduce them. Furthermore, we show how to use this procedure to find a good p-basis which gives the *Ulm invariants* [7] of M and also the *type* of M.

1991 *Mathematics Subject Classification.* Primary: 13C05; Secondary: 13E15, 13P10, 20C05.

Key words and phrases. Dedekind-like rings, chain modules, finite Abelian p-groups, Gröbner bases.

The first author is supported by the National Institute of Health, PROGRAM SCORE, 2004-08, 546112, University of Puerto Rico-Rio Piedras Campus, IDEA Network of Biomedical Research Excellence, and the Laboratory Gauss University of Puerto Rico Research. She wants to thank Professor O. Moreno for his support during the last four years. The authors want to thank Professors L. Fuchs, L. S. Levy and R. Laubenbacher for their comments, support and helpful suggestions while preparing this paper.

The main contribution of this paper is a constructive method to find a p-basis (and the Ulm invariants) of a finite Abelian p-group M from a given presentation of M encoding the action of p. The algorithm is obtained by noting that there are some invariant properties between the order of elements in an Abelian group and the basis elements of certain *toric ideals* [13]. To accomplish this, we use several tools from *Gröbner bases* [4] and *chain-modules* [3]. Furthermore, this method can be used in general for modules over algebras on $\mathbb{Z}_{p^n}$ and $\mathbb{Z}$.

Let M be a finitely generated Abelian group. We assume that M is also finitely presented, that is, $M = \langle C, R\rangle$, where C is a non-minimal finite generating set, and R is a finite set of relations among the elements of C, see [6, 8]. For example

$$M = \langle c_1, \dots, c_n \mid \sum_{j=1}^{q} a_{ij}c_j = 0 \text{ with } a_{ij} \in \mathbb{Z}, \text{ for all } i = 1, \dots, n \text{ and } j = 1, \dots, q\rangle.$$

We want to find the *torsion-free rank* of M and the *Ulm invariants* of the p_j-Sylow subgroups of M. This is an old problem, the new aspects in this work are: (1) we use Gröbner bases to solve the problem, and (2) using the notation and classification introduced by Levy, we apply this method to determine the additive structure of indecomposable modules over certain Dedekind-like rings. In this case, the algorithm computes a p-basis for the torsion part of the group.

This paper is organized as follows: in Section 2, we introduce *toric ideals* associated to finitely generated Abelian groups. In Section 3, we give a description of the *reduced Gröbner basis* [4] of a toric ideal associated to a finitely generated Abelian p-group. As a consequence, in Section 4, we obtain an algorithm to compute the p-basis and the type of any finite Abelian p-group. As an application of this algorithm, in Section 5, we show how to obtain the additive structure of any indecomposable module over $\mathbb{Z}C_p$, where C_p is the cyclic group of order a prime p and over the $p-$pullback $\{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ of $\mathbb{Z} \oplus \mathbb{Z}$.

2. Gröbner bases associated to finitely generated Abelian groups

We start by reviewing some concepts in finitely generated Abelian group theory.

Definition 2.1 (type)**.** *If $p_1 < \cdots < p_r$ and M is a finitely generated Abelian group, such that*

$$M \cong \mathbb{Z}^{s_0} \oplus (\mathbb{Z}_{p_1}{}^{s_{11}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{n_1}}{}^{s_{1n_1}}) \oplus \cdots \oplus (\mathbb{Z}_{p_r}{}^{s_{r1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_r}}{}^{s_{rn_r}})$$

as an Abelian group, then the type *of M is*

$$\underline{t}(M) = (s_0, s_{11}, \dots, s_{1n_1}, \dots, s_{r1}, \dots, s_{rn_r}) \in \mathbb{Z}^{n_1+\cdots+n_r+1}.$$

The number s_0 is the *torsion-free rank* of M, the numbers $s_{i1}, \dots, s_{in_i}$ are the *Ulm invariants* of the p_i-Sylow subgroup $M_i = \mathbb{Z}_{p_i}{}^{s_{i1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{n_i}}{}^{s_{in_i}}$ of M, and the number n_i is the *torsion rank* of M_i.

Definition 2.2 (p-basis)**.** *If M is a p-group, for some prime number p, a set $B = \{b_1, \dots, b_d\} \subset M$ is called a p-basis of M if $M \cong_{\mathbb{Z}_{p^n}} \langle b_1\rangle \oplus \cdots \oplus \langle b_d\rangle$. A set B is a p-basis of M if and only if, for all $m \in M$ the sum $m = \sum_{i=1}^{d} l_i b_i$ is unique, where $0 \le l_i \le \operatorname{ord}(b_i)$ and $\operatorname{ord}(b_i)$ is the order of b_i in the group M, see* [7].

Let $M = \oplus_{t=1}^{r} M_t \oplus \mathbb{Z}^s$ be a finitely generated Abelian group, where M_t is the p_t-Sylow subgroup of M with p_t-rank equal to d_t. Consider a non minimal generating set C_t of each M_t, such that, $C_i \cap C_j = \emptyset$ for all $i \neq j$, and a generating set C_0 of $\mathbb{Z}^s$. If $C = \cup_{t=0}^r C_t = \{c_1, \ldots, c_q\}$, where $q \geq \sum_{t=1}^r d_t + s$, then $\langle C \rangle = M$. Consider the semigroup homomorphism

$$\gamma : \mathbb{N}^q \longrightarrow M, \qquad v = (v_1, \ldots, v_q) \longmapsto \sum_{i=1}^{q} v_i c_i.$$

Let k be an infinite field. The previous map lifts to the following short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\widetilde{\gamma}) \longrightarrow k[\mathbf{x}] \xrightarrow{\widetilde{\gamma}} k[M] \longrightarrow 0, \tag{2.1}$$

where $k[\mathbf{x}] = k[x_1, \ldots, x_q] \cong k[\mathbb{N}^q]$ is the polynomial ring in q indeterminates over k. The monomials in $k[\mathbf{x}]$ are denoted by $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_q^{a_q}$, where $\mathbf{a} = (a_1, \ldots, a_q) \in \mathbb{N}^q$. On the other hand, if $d = \sum_{t=1}^r d_t$, we have the following isomorphism

$$k[M] \cong k[\mathbf{t}] = k[t_1, \ldots, t_d, t_{d+1}, t_{d+1}^{-1}, \ldots, t_{d+s}, t_{d+s}^{-1}]/\langle t_1^{k_1} - 1, \ldots, t_d^{k_d} - 1\rangle,$$

where k_i is the order of the corresponding element in the external direct sum of M. Furthermore, in this external direct sum, the element $c_i \in C$ can be expressed as a tuple $\mathbf{c}_i = (c_{i1}, \ldots, c_{id}, c_{id+1}, \ldots, c_{id+s})$. So, we have a homomorphism of semigroup algebras

$$\widetilde{\gamma} : k[\mathbf{x}] \longrightarrow k[\mathbf{t}], \qquad x_i \longmapsto \mathbf{t}^{\mathbf{c}_i} = t_1^{c_{i1}} \cdots t_d^{c_{id}} t_{d+1}^{c_{i,d+1}} \cdots t_{d+s}^{c_{i,d+s}}.$$

We denote the kernel of $\widetilde{\gamma}$ by I_C. We will show how to obtain a minimal generating set that is a p-basis of M, from a certain Gröbner basis of this ideal. In the following, we assume that we have a term order $\prec$ defined in $k[\mathbf{x}]$. Then every nonzero polynomial $f \in k[\mathbf{x}]$ has a unique initial monomial, denoted $in_{\prec}(f)$. Observe that for any $v = (v_1, \ldots, v_q) \in \mathbb{Z}^q$, we can write $v = v^+ - v^-$, where $v^+ = (v_1^+, \ldots, v_q^+)$ and $v^- = (v_1^-, \ldots, v_q^-)$ are nonnegative integer tuples. Denote by $\mathrm{Ker}(\gamma)$ the subgroup of $\mathbb{Z}^q$ consisting of all elements v such that $\gamma(v^+) = \gamma(v^-)$. Let

$$P(\mathrm{Ker}(\gamma)) = \left\{\mathbf{x}^{v^+} - \mathbf{x}^{v^-} \mid v \in \mathrm{Ker}(\gamma)\right\}.$$

The following lemma follows immediately from [13, Lemma 4.1].

Lemma 2.3. *The ideal I_C is generated as a k-vector space by the set $P(\mathrm{Ker}(\gamma))$.*

Recall that C is a non-minimal finite generating set of M. We assume that there exists a finite set of defining relations $\mathcal{R}$ for C in M. We use the notation v^+ and v^- to write the relations as $\sum_{t=1}^q v_t^+ c_t = \sum_{t=1}^q v_t^- c_t$. These relations induce a subset of vectors in $\mathbb{Z}^q$ and a subset of polynomials in I_C

$$\overline{\mathcal{R}} = \left\{v \in \mathbb{Z}^q : \sum_{t=1}^{q} v_t^+ c_t = \sum_{t=1}^{q} v_t^- c_t \text{ is in } \mathcal{R}\right\} \subset \mathbb{Z}^q,$$
$$P(\overline{\mathcal{R}}) = \left\{P(v) = \mathbf{x}^{v^+} - \mathbf{x}^{v^-} \mid v \in \overline{\mathcal{R}}\right\} \subset I_C.$$

Let $G_{\overline{\mathcal{R}}}$ denote the reduced Gröbner basis of the ideal generated by $P(\overline{\mathcal{R}})$, with respect to the order $\prec$. Similarly, this Gröbner basis induces the set $\overline{\mathcal{R}}_{\mathcal{G}}$ of tuples

$$\overline{\mathcal{R}}_{\mathcal{G}} = \left\{v \in \mathbb{Z}^q \mid \mathbf{x}^{v^+} - \mathbf{x}^{v^-} \in \mathcal{G}_{\overline{\mathcal{R}}}\right\}$$

and the set $\mathcal{R}_\mathcal{G}$ of relations

$$R_\mathcal{G} = \{ \sum_{t=1}^{q} v_t^+ c_t = \sum_{t=1}^{q} v_t^- c_t \text{ such that } v \in \overline{\mathcal{R}}_\mathcal{G} \}.$$

Proposition 2.4. *Let $v_k \in \overline{\mathcal{R}}$ with $in_\prec(P(v_k)) = \mathbf{x}^{v_k^+}$ for $k \in 1, 2$. Also let $w_1, w_2 \in \mathbb{N}^q$ such that $w_1 + v_1^+ = w_2 + v_2^+$. If $P(v) = \mathbf{x}^{w_1} P(v_1) - \mathbf{x}^{w_2} P(v_2)$ then $v = v_1 - v_2$.*

Proof. We have $P(v) = \mathbf{x}^{w_1} P(v_1) - \mathbf{x}^{w_2} P(v_2) = \mathbf{x}^{w_2+v_2^-} - \mathbf{x}^{w_1+v_1^-}$. So

$v = (w_2+v_2^-)-(w_1+v_1^-) = (w_2+v_2^-)-(w_1+v_1^-)+(w_1+v_1^+)-(w_2+v_2^+) = v_1-v_2.$ □

Theorem 2.5. *The set $\mathcal{R}_\mathcal{G}$ is a set of relations for C in M.*

Proof. First observe that, if $v \in \mathrm{Ker}(\gamma)$, then $\sum_{t=1}^{q} v_t c_t = 0$. So $v \in \langle \overline{\mathcal{R}} \rangle$ and since $\langle \overline{\mathcal{R}} \rangle \subset \mathrm{Ker}(\gamma)$, then the set $\overline{\mathcal{R}}$ generates the subgroup $\mathrm{Ker}(\gamma)$. This implies that the ideal I_C is generated by $P(\overline{\mathcal{R}})$. Next, we use the Buchberger algorithm [4, Chapter 2, §7] to obtain the reduced Gröbner basis of I_C from $P(\overline{\mathcal{R}})$.

By Proposition 2.4, we have that the S-polynomial $S(P(u_1), P(u_2)) = P(v)$ satisfies $v = u_1 - u_2 \in \mathrm{Ker}(\gamma)$. Let S be the set of all nonzero S-polynomials obtained in the Buchberger algorithm and let $\overline{S} = \{v \in \mathbb{Z}^q \mid P(v) \in S\}$. Clearly $\langle \overline{\mathcal{R}} \rangle = \langle \overline{\mathcal{R}} \cup \overline{S} \rangle$. We denote by $\overline{\mathcal{R}'} = \overline{\mathcal{R}} \cup \overline{S}$. Now, we reduce the set of polynomials in $P(\overline{\mathcal{R}'})$. Suppose $in_\prec(P(v)) = \mathbf{x}^{v^+}$ divides $in_\prec(P(v_1)) = \mathbf{x}^{v_1^+}$, with $v, v_1 \in \overline{\mathcal{R}'}$. There exists $w \in \mathbb{N}^q$ such that $w + v^+ = v_1^+$ and $P(v_2) = P(v_1) - \mathbf{x}^w P(v)$. Hence $v_2 = v_1 - v \in \overline{\mathcal{R}'}$ by Proposition 2.4. Then $\langle \overline{\mathcal{R}} \rangle = \langle \overline{\mathcal{R}'} \rangle = \langle (\overline{\mathcal{R}'} \setminus \{v_1\}) \cup \{v_2\} \rangle$. So $\langle \overline{\mathcal{R}}_\mathcal{G} \rangle = \langle \overline{\mathcal{R}} \rangle$. This proves our claim. □

3. The reduced presentation of M

Given a generating set C of a finite Abelian p-group M, one can obtain a set of relations by studying the action of p over the elements in C. In the last section, we saw that any Gröbner basis of I_C gives a set of relations for M. In this section, we describe a particular Gröbner basis that gives a p-basis of M. We assume that the elements of C have orders $\mathrm{ord}(c_1) \geq \cdots \geq \mathrm{ord}(c_q)$. Consider the following chain of subgroups of M

$$\langle c_1 \rangle \subseteq \langle c_1, c_2 \rangle \subseteq \cdots \subseteq \langle c_1, c_2, \ldots, c_s \rangle \cdots \subseteq \langle C \rangle = M.$$

For $s \geq 2$, let $r_s = \min\{k \mid p^k c_s \in \langle c_1, c_2, \ldots, c_{s-1} \rangle\}$. There are two possibilities, either $r_s < \mathrm{ord}(c_s)$, or $r_s = \mathrm{ord}(c_s)$, in this case, $p^{r_s} c_s = 0 \in \langle c_1, c_2, \ldots, c_{s-1} \rangle$. Thus, we have the following set of relations

$$R_p = \{ \ p^{r_1} c_1 = 0, \ p^{r_s} c_s = p^{r_s} \sum_{t<s} a_{st} c_t, \ \textit{where } a_{st} \in \mathbb{Z}, \ \textit{for } 2 \leq s \leq q \}.$$

Proposition 3.1. *The relations R_p together with the set C is a presentation of the p-group M.*

Proof. Suppose $\sum_{t=1}^{q} \ell_t c_t = 0$. Dividing ℓ_q by p^{r_q}, we obtain $\ell_q = s_q p^{r_q} + s'_q$ with $0 \leq s'_q < p^{r_q}$. Therefore, $s_q p^{r_q} c_q + s'_q c_q + \sum_{t=1}^{q-1} \ell_t c_t = 0$. Suppose that $s'_q \neq 0$. Using the relation $p^{r_q} c_q = \sum_{t<q} p^{r_q} u_{qt} c_t$, we obtain $\sum_{t=1}^{q} \ell_t c_t = s'_q c_q + \sum_{t=1}^{q-1} \ell'_t c_t =$

0. If $\gcd(s'_q, p) = 1$, then $c_q = \sum_{t<q-1} l_t c_t$ and $\sum_{t=1}^{q} \ell_t c_t = \sum_{t=1}^{q-1} l_t c_t = 0$. If $\gcd(s'_q, p) = p$, let p^r be the maximum number such that p^r divides s'_q. Then $p^r c_q = -\sum_{t=1}^{q-1} \ell'_t c_t$. But this is impossible, because p^{r_q} is the minimum with this condition. Thus $\gcd(s'_q, p) = 1$.

Repetition of this argument shows that $\sum_{t=1}^{q} \ell_t c_t = l'_1 c_1 = 0$ with $\gcd(l'_1, p) = 1$. But this implies that $c_1 = \ldots = c_q = 0$ which is impossible. Then $s'_q = 0$ and the relation $\sum_{t=1}^{q} \ell_t c_t = 0$ is a linear combination of the relations in $\mathcal{R}$. □

Proposition 3.2. *Let $\prec$ be the lexicographic ordering with $x_1 \prec x_2 \prec \cdots \prec x_q$. Then, the reduced Gröbner basis of I_C with respect to $\prec$ equals*

$$\mathcal{G}_p = \{x_1^{p^{r_1}} - 1, x_2^{p^{r_2}} - x_1^{a_{21}p^{r_2}}, \ldots, x_q^{p^{r_q}} - \prod_{t=1}^{q-1} x_t^{a_{qt}p^{r_q}}\}.$$

Proof. Observe that $\mathcal{G}_p = P(\overline{\mathcal{R}_p})$. Thus, by Theorem 2.5, $\mathcal{G}_p$ generates I_C. Furthermore, $\mathcal{G}_p$ is a reduced Gröbner basis since $\gcd(in_\prec(p_1), in_\prec(p_2)) = 1$, for any p_1 and p_2 in $\mathcal{G}_p$. This forces all S-polynomials to be zero modulo $\mathcal{G}_p$, see [4]. □

Let pR be the following set of relations for C in M

$$pR = \{pc_q = 0, \quad pc_j = \sum_{t>j} a_{jt} c_t, \text{ for all } 1 \le j \le q-1, \text{ with } 0 \le a_{jt} \in \mathbb{Z}\}. \tag{3.1}$$

These relations can be used to find the order of any element in M, since pM is the *Frattini* subgroup of M. On the other hand, from the action of p, we can find the minimal number of generators of M, that is, the p-rank of M by the Burnside Basis Theorem for finite groups (M/pM). Let d be the p-rank of M. For each $t \ge 2$, let D_t be the set

$$D_t = \{c_t - \sum_{j=1}^{t-1} a_{ts} c_j \mid 0 \le a_{tj} \le \operatorname{ord}(c_j)\}.$$

If b_t is the element of maximal order in D_t, then $p^{r_t} = \operatorname{ord}(b_t)$. Therefore, we have the following set of relations, denoted by R_{pbasis}

$$\{p^{r_1} c_1 = 0,\ p^{r_t} c_t = p^{r_t} \sum_{j<t} a_{tj} c_s \text{ for } 2 \le t \le d, \text{ and } c_t = \sum_{j<d} a_{tj} c_j \text{ for } d < t \le q\}.$$

It is clear that $M = \langle b_1, b_2, \ldots, b_d \rangle$, so R_{pbasis} is a set of relations for C in M. As a corollary of Proposition 3.2, we have

Corollary 3.3. *Let $\prec$ be the lexicographic ordering with $x_1 \prec x_2 \prec \cdots \prec x_q$. Then, the reduced Gröbner basis of I_C, denoted by $\mathcal{G}_{pbasis}$, with respect to $\prec$ equals*

$$\{x_1^{p^{r_1}} - 1, \ldots, x_d^{p^{r_d}} - \prod_{t=1}^{d-1} x_t^{a_{dt}p^{r_d}}, x_{d+1} - \prod_{t=1}^{d} x_t^{a_{t,d+1}}, \ldots, x_q - \prod_{t=1}^{d} x_t^{a_{tq}}\}. \tag{3.2}$$

Note that $\mathcal{G}_{pbasis}$ is just a refinement of $\mathcal{G}_p$ obtained by setting some of the p^{r_j} equal to 1. The next theorem is the key to our algorithm. It says that the generating set obtained from $\mathcal{G}_{pbasis}$ is actually a p-basis of M.

Theorem 3.4. *The set $\overline{C} = \{c_1, \ldots, c_d - \sum_{t=1}^{d-1} a_{dt} c_t\}$ is a p-basis of M.*

Proof. We have seen that $M = \langle b_1, b_2, \ldots, b_d\rangle = \langle \overline{C}\rangle$. Now, we will prove that the sum $\langle b_1\rangle + \cdots + \langle b_d\rangle$ is actually a direct sum. If $y \in \langle b_t\rangle \cap \langle b_1, \ldots, b_{t-1}\rangle$. Then $y = \alpha_t b_t = \sum_{j=1}^{t-1} \alpha_s b_s$. Thus, $\alpha_t c_t = \sum_{j=1}^{t-1} \alpha'_j c_j$. The argument preceding this theorem shows that $\alpha_t \geq p^{r_t}$, so $\alpha_t = \alpha'_t p^{r_t} + \beta_t$, with $0 \leq \beta_t < p^{r_t}$. Thus $\beta_t c_t = \sum_{j=1}^{t-1} \alpha"_j c_j$ which implies $\beta_t = 0$ and $y = \alpha'_t p^{r_t} b_t = 0$. So $M = \oplus_{t=1}^{d} \langle b_t\rangle$. □

We can summarize the above results as follows.

Remark 3.5.

(1) *Given a presentation of a finite Abelian p-group $M = \langle C, \mathcal{R}\rangle$, there exists a term ordering such that the reduced Gröbner basis of the toric ideal I_C gives a p-basis for M.*
(2) *Given a homomorphism $\widetilde{\gamma}$ as in* (2.1). *The presentations for the corresponding finite Abelian group M can be obtained from Gröbner bases of the toric ideal* $\mathrm{Ker}(\widetilde{\gamma})$.

4. The p-basis algorithm and the additive structure of M

Corollary 3.3 gives an explicit description of a reduced Gröbner basis for I_C. Moreover, Theorem 3.4 shows that the corresponding set of generators is a p-basis of M. Nevertheless, we obtained this Gröbner basis from a very special set of relations whose definition was non constructive, namely $\mathcal{R}_{pbasis}$. In particular, this set of relations specified the ordering on the indeterminates for the specific lexicographic order needed in Corollary 3.3. In this section, we put all these results together to compute the invariants of a finite Abelian p-group M from a particular presentation.

Let pR be the finite presentation of M introduced in (3.1), that is, assume that the action of p in a generating set C is known. Following Remark 3.5, we need to find an ordering of the indeterminates, such that, the Gröbner basis with respect to the corresponding lexicographic order has the form (3.2). Note that there might be several such orderings. In the last section, we saw that if $\mathrm{ord}(c_i) < \mathrm{ord}(c_j)$ then $x_j \prec x_i$. We also need to break ties among the elements in C with the same order in the group.

In practice, one first break ties arbitrarily. If the Gröbner basis has the required form, we are done. Otherwise, there is an element in the Gröbner basis of the form $x_j^{p^{r_j}} - x_i \prod_{t=1, t\neq i}^{j-1} x_t^{a_{jt}p^{r_j}}$, with $\mathrm{ord}(c_j) = \mathrm{ord}(c_i)$. In this case, we need to invert the order of x_i and x_j to $x_j < x_i$. This process eventually terminates, moreover; it effectively gives the desired Gröbner basis since the p-basis itself always exists. The output of the algorithm consists on the p-basis and the Ulm invariants of M, that is, the type $\underline{t}(M)$.

Algorithm 4.1. *Input: C, pR.*

(A1) *Write the relations in pR as polynomials in $k[\mathbf{x}]$ as follows: $x_q^p - 1$, and $x_j^p - \prod_{t>j} x_t^{a_{jt}}$, for $1 \leq j \leq q$.*
(A2) *Find the order of all c_j by computing all the univariate polynomials in the ideal I generated by the polynomials obtained in (A1).*
(A3) *Find an ordering of the indeterminates, such that, the reduced lexicographic Gröbner basis $\mathcal{G}_p$ of I has the form* (3.2).

(A4) *Let d be the number of polynomials in $\mathcal{G}_p$ such that the initial term has exponent > 1. If $p^{r_j} > 1$ and $x_j^{p^{r_j}} - \prod_{t=1}^{j-1} x_t^{a_{jt}p^{r_j}} \in \mathcal{G}_p$, then add b_j to the p-basis, where b_j is the following element of order p^{r_j}:*

$$b_j = c_j - \sum_{t=1}^{j-1} a_{jt} c_t.$$

(A5) *To compute the type of M, let s_r be the number of elements with the same order p^r. Then $\underline{t}(M) = (s_1, \ldots, s_n)$.*

Output: $B = \{b_1, \ldots, b_d\}$ and $M \cong (\mathbb{Z}_p)^{s_1} \oplus \cdots \oplus (\mathbb{Z}_{p^n})^{s_n}$.

Example 4.2. *Let $M = \langle c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\rangle$ be a 5-group, with the following relations:*

$$5c_1 - c_8 - 4c_5 - 2c_6 - 3c_7 = 0, \quad 5c_2 - 4c_6 - 2c_7 = 0, \quad 5c_3 - 4c_7 = 0,$$
$$5c_4 = 0, \quad 5c_5 = 0, \quad 5c_6 = 0, \quad 5c_7 = 0, \quad 5c_8 = 0.$$

The corresponding polynomials are

$$\{x_1^5 - x_8x_5^4x_6^2x_7^3, x_2^5 - x_6^4x_7^2, x_3^5 - x_7^4, x_4^5 - 1, x_5^5 - 1, x_6^5 - 1, x_7^5 - 1, x_8^5 - 1\}.$$

The reduced lexicographic Gröbner basis equals

$$\{x_1^{25} - 1, \quad x_2^{25} - 1, \quad x_3^{25} - 1, \quad x_4^5 - 1, \quad x_5^5 - 1$$
$$x_6 - x_3^{15}x_2^{20}, \quad x_7 - x_3^{20}, \quad x_8 - x_5x_3^{10}x_2^{10}x_1^5\}.$$

In this case, $d = 5$. So, the Gröbner basis gives the following information

$$25c_1 = 0, \quad 25c_2 = 0, \quad 25c_3 = 0, \quad 5c_4 = 0, \quad 5c_5 = 0,$$
$$c_6 = 15c_3 + 20c_2, \quad c_7 = 20c_3, \quad c_8 = c_5 + 10c_3 + 10c_2 + 5c_1.$$

Hence, the p-basis is equal to $B = \{c_1, c_2, c_3, c_4, c_5\}$, $M \cong {\mathbb{Z}_5}^2 \oplus {\mathbb{Z}_{25}}^3$, and $\underline{t}(M) = (2, 3)$.

The classical way to solve this problem, using matrix transformations over a Euclidean domain, appears in [2]. We remark that it is possible to perform the second step in the algorithm because by definition, I_C is a zero-dimensional ideal. Moreover, each univariate polynomial in I_C has the form $x_j^{\mathrm{ord}(c_j)} - 1$.

5. Indecomposable modules over Dedekind-like rings

Let R_1 and R_2 be two rings. Let R be the pullback ring of the rings R_i over a common ring $\overline{R}$, that is, $R = \{R_1 \to \overline{R} \leftarrow R_2\}$. In [9], L. Levy studied the separated representation of an R-module M. In [10], he described the indecomposable R-modules when R_1 and R_2 are Dedekind domains and $\overline{R}$ is a field k (R is called a Dedekind-like ring). In particular, he studied modules over two rings: $\mathbb{Z}C_p$, where C_p is the cyclic group of order a prime number p, and the $p-$pullback $\{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ of $\mathbb{Z} \oplus \mathbb{Z}$.

An R-module S is separated if it is an R-submodule of a direct sum $S_1 \oplus S_2$, where each S_i is an R_i-module. A separated representation of an R-module M is an R-module epimorphism $\phi : S \longrightarrow M$, such that, S is a separated R-module and if ϕ admits a factorization $\phi : S \xrightarrow{f} S' \longrightarrow M$ with S' also a separated R-module, then f must be one to one. Let $P_i = \ker(R_i \longrightarrow k)$, then $P = \{P_1 \to 0 \leftarrow P_2\}$ is an ideal of R . We call an R-module M P-mixed, if each *torsion* element m is annihilated by some power of P. The separated modules $S = \{S_1 \xrightarrow{f_1} k \xleftarrow{f_2} S_2\}$ satisfying one of the following two conditions: (1) $S_i \cong$ nonzero ideal of R_i, or (2) $S_i \cong R_i/P_i^e$ form the basic building blocks for all finitely generated, P-mixed R-modules. If S is a building block, then S has exactly one submodule which has the form $\{X \to 0 \leftarrow 0\}$ and is R-isomorphic to k (left k of S). Similarly, S has a right k of S.

Definition 5.1. *(Deleted Cycle and Block Cycle Indecomposables)*

(a) *Let $S^{(1)}, \dots, S^{(m)}$ be a sequence of basic building blocks, such that,*

$$\begin{array}{ccccccccc} S^{(1)} & \longrightarrow & S_{21} & S^{(i)} & \longrightarrow & S_{2i} & S^{(m)} & \longrightarrow & S_{2m} \\ \big\downarrow & & \sigma_{21}\big\downarrow \ \cdots & \big\downarrow & & \sigma_{2i}\big\downarrow \ \cdots & \big\downarrow & & \sigma_{2m}\big\downarrow \\ S_{11} & \xrightarrow{\sigma_{11}} & k & S_{1i} & \xrightarrow{\sigma_{1i}} & k & S_{1m} & \xrightarrow{\sigma_{1m}} & k \end{array}$$

and suppose that for $1 \le i \le m$, $S^{(i)}$ has a right k and $S^{(i+1)}$ has a left k. A deleted cycle indecomposable M is the direct sum $S = \oplus_{i=1}^m S^{(i)}$ modulo a relation which identifies the right k of $S^{(i)}$ with the left k of $S^{(i+1)}$, that is, first choose $p_j \in P_j - P_j^2$ for $j = 1, 2$, then make the following identification

$$p_2^{d(2,i)-1} s_{2i} = -p_1^{d(1,i+1)-1} s_{1,i+1}, \text{ where } s_{ji} \in S_{ji}, \text{ with } \sigma_{ji}(s_{ji}) = \overline{1}$$

for $j = 1, 2$, $1 \le i \le m-1$, and $d(j,i)$ the length of S_{ji}. In other words, it is the direct sum S modulo

$$\big\{p_2^{d(2,1)-1} s_{21} + p_1^{d(1,2)-1} s_{12}, \dots, p_2^{d(2,m-1)-1} s_{2,m-1} + p_1^{d(1,m)-1} s_{1m}\big\}.$$

(b) *Let $S^{(1)}, \dots, S^{(m)}$ be a sequence of basic building blocks*

$$\begin{array}{ccccccccc} S^{(1)} & \longrightarrow & S_{21} & S^{(i)} & \longrightarrow & S_{2i} & S^{(m)} & \longrightarrow & S_{2m} \\ \big\downarrow & & \sigma_{21}\big\downarrow \ \cdots & \big\downarrow & & \sigma_{2i}\big\downarrow \ \cdots & \big\downarrow & & \sigma_{2m}\big\downarrow \\ S_{11} & \xrightarrow{\sigma_{11}} & k & S_{1i} & \xrightarrow{\sigma_{1i}} & k & S_{1m} & \xrightarrow{\sigma_{1m}} & k \end{array}$$

each with a left and a right k. Write $m = l\underline{m}$, where $\underline{m}$ is the unique smallest positive integer, such that, for all i, $S^{(i)} \cong S^{(i+\underline{m})}$. Let $f(z) = \lambda_o + \lambda_1 z + \cdots + \lambda_{l-1} z^{l-1} + z^l$ be a power of an irreducible polynomial in $k[z]$. A block cycle indecomposable M is a deleted cycle indecomposable modulo the following relation $-p_2^{d(2,m)-1} s_{2m} = \sum_{j=0}^{l-1} \lambda_j p_1^{d(1,j)-1} s_{1,j\underline{m}+1}$, which identifies the right k of $S^{(m)}$ with a one-dimensional subspace of $S_{11} \oplus S_{1,\underline{m}+1} \oplus S_{1,2\underline{m}+1} \oplus \cdots$. In other words, it is the direct sum S modulo

$$\big\{p_2^{d(2,1)-1} s_{21} + p_1^{d(1,2)-1} s_{12}, \dots, p_2^{d(2,m-1)-1} s_{2,m-1} + p_1^{d(1,m)-1} s_{1m},$$
$$p_2^{d(2,m)-1} s_{2m} + \sum_{j=0}^{l-1} \lambda_j p_1^{d(1,j)-1} s_{1,j\underline{m}+1}\big\}.$$

As a consequence, if M is a deleted cycle then $1 \leq d(2,i) \neq \infty$, for $1 \leq i \leq m-1$ and $1 \leq d(1,i) \neq \infty$, for $2 \leq i \leq m$. But the length of either one of S_{11} or S_{2n} may be infinite. If M is a block cycle, then $1 \leq d(j,i) \neq \infty$ for $1 \leq i \leq m$ and $j = 1, 2$.

Remark 5.2. *The indecomposable, finitely generated, P-mixed modules are deleted cycle indecomposables and block cycle indecomposables. Every separated R-module is a direct sum of basic building blocks. Moreover, basic building blocks are always indecomposable R-modules, see* [10].

5.1. **Additive descriptions.** Using Algorithm 4.1, we describe the additive structure of the indecomposable R-modules when R is one of the following rings: $\mathbb{Z}C_p$ or the p-pullback of $\mathbb{Z} \oplus \mathbb{Z}$, $\{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$. In these two cases the concept of P-mixed coincides with p-mixed.

The ring $\mathbb{Z}C_p$:

$$\begin{array}{ccc} \mathbb{Z}C_p & \longrightarrow & \mathbb{Z}[\zeta] \\ \Big\downarrow & & \Big\downarrow{\scriptstyle \nu_2} \\ \mathbb{Z} & \xrightarrow{\nu_1} & \mathbb{Z}_p \end{array}$$

Let ζ be a primitive pth root of unity, and let x be a generator of C_p. Then $\mathbb{Z}C_p \cong \{\mathbb{Z} \xrightarrow{\nu_1} \mathbb{Z}_p \xleftarrow{\nu_2} \mathbb{Z}[\zeta]\}$, where the isomorphism is given by $x \longrightarrow (1 \to \overline{1} \leftarrow \zeta)$. The action of p_1 and p_2 in $\Lambda = \mathbb{Z}C_p$ is given by the following formulas

$$p_1 = x^{p-1} + x^{p-2} + \cdots + x + 1 = \left\{p \to 0 \leftarrow \zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta + 1\right\} \text{ and}$$
$$p_2 = x - 1 = \{0 \to 0 \leftarrow \zeta - 1\}, \quad p = (p,p) = p_1 + p_2^{p-1}\sigma(p_2), \quad p_1 p_2 = 0,$$

where $\sigma(p_2)$ is a polynomial in p_2, with degree less or equal than $p-1$, which exists because the sum equals p. Thus every element m of a $\mathbb{Z}C_p$-module $M = \langle a_1, \ldots, a_n \rangle$ is a linear combination of these generators and the elements resulting from the action of p_1 and p_2 over them.

Example 5.3. *Let $\Lambda = \mathbb{Z}C_3$ and $M = \langle a \rangle_{\mathbb{Z}C_3}$ be a deleted cycle indecomposable with $d(1) = d(2) = 3$, and $3 = p_1 + 2{p_2}^2$. We need to compute the action of p in Λ over the generator a to obtain a generating set for M over $\mathbb{Z}$. This is the classical way to begin this problem in Abelian group theory. Thus,*

$$3a = p_1 a + 2p_2^2 a,\ 3p_1 a = p_1^2 a,\ 3p_1^2 a = 0,\ 3p_2 a = p_2^2 a,\ 3p_2^2 a = 0.$$

The generating set is $C = \{a, p_2 a, p_1 a, p_2^2 a, p_1^2 a\}$, the corresponding ideal is generated by the binomials

$$\left\{x_1^3 - x_3 x_4^2,\ x_3^3 - x_5,\ x_5^3 - 1,\ x_2^3 - x_4,\ x_4^3 - 1\right\}.$$

The order of each element in C is $\{27, 9, 9, 3, 3\}$. The reduced Gröbner basis is equal to

$$\left\{x_1^{27} - 1,\ x_2^9 - 1,\ x_3 - x_2^3 x_1^3,\ x_4 - x_2^3,\ x_5 - x_1^9\right\}.$$

So, Algorithm 4.1 outputs

$$B = \left\{a,\ p_2 a\right\},\ M \cong \mathbb{Z}_9 \oplus \mathbb{Z}_{27},\ \underline{t}(M) = (0,0,1,1).$$

The extra zero in the type means that the torsion-free rank equals 0. Therefore, the action of Λ does not change if we consider M as a module over $\mathbb{Z}_{27}C_3$.

Example 5.4. *Let $\Lambda = \mathbb{Z}C_3$ and $M = \langle a\rangle_{\mathbb{Z}C_3}$ be a block cycle indecomposable with $d(1) = 4,\ d(2) = 4$, and $f(z) = z-2$. The action of $p = 3$ is given by $3 = p_1 + 2{p_2}^2$. We also have the relation $p_1^3 a = 2p_2^3 a$. The action of $p = 3$ over a is given by*

$$3a = p_1a + 2p_2^2a,\ 3p_1a = p_1^2a,\ 3p_1^2a = p_1^3a,\ 3p_1^3a = 0, 3p_2a = 2p_2^3a,\ 3p_2^2a = 0.$$

The generating set is $C = \{a, p_1a, p_2a, p_1^2a, p_2^2a, p_1^3a, p_2^3a\}$. In this case, the corresponding toric ideal is generated by

$$\{x_1^3 - x_2x_5^2,\ x_2^3 - x_4,\ x_4^3 - x_6,\ x_6^3 - 1,\ x_3^3 - x_7^2,\ x_5^3 - 1,\ x_7^3 - 1,\ x_6 - x_7^2\}.$$

The order of each element in C is $\{81, 27, 9, 9, 3, 3, 3\}$. The reduced Gröbner basis is equal to

$$\{x_1^{81} - 1,\ x_2^3 - x_1^9,\ x_3^3 - x_1^{27},\ x_4 - x_1^9,\ x_5 - x_2x_1^{78},\ x_6 - x_1^{27},\ x_7 - x_1^{54}\}.$$

Hence, Algorithm 4.1 outputs

$$B = \{a,\ p_1a - 3a,\ p_2a - 9a\},\ M \cong {\mathbb{Z}_3}^2 \oplus \mathbb{Z}_{81},\ \underline{t}(M) = (0, 2, 0, 0, 1).$$

The p-pullback ring of $\mathbb{Z} \oplus \mathbb{Z}$: The p-pullback of $\mathbb{Z} \oplus \mathbb{Z}$ is the subring $\Lambda = \{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ of $\mathbb{Z} \oplus \mathbb{Z}$. In this case, let $p_1 = (p, 0)$ and $p_2 = (0, p)$. Then $p = (p, p) = p_1 + p_2$.

Example 5.5. *Consider the pullback ring $\Lambda = \{\mathbb{Z} \to \mathbb{Z}_3 \leftarrow \mathbb{Z}\}$ and a deleted cycle indecomposable module $M = \langle a_1, a_2\rangle_\Lambda$, with $d(1,1) = 3$, $d(1,2) = 3$, $d(2,1) = 3$, $d(2,2) = 3$, and $-4p_2^2a_1 = p_1^2a_2$. Note that the order of these elements is 3, since they are in the* socle *$M[p]$ of M; thus, the last relation is $2p_2^2a_1 = p_1^2a_2$. Also $p = p_1 + p_2$. Therefore, the generators are*

$$C = \{a_1,\ a_2,\ p_1a_1,\ p_2a_1,\ p_1a_2,\ p_2a_2,\ p_1^2a_1,\ p_2^2a_1,\ p_1^2a_2,\ p_2^2a_2\}.$$

Besides the previous relation $p_1^2a_2 = 2p_2^2a_1$, the relations obtained from the action of p are

$$3a_1 = p_1a_1 + p_2a_1,\ 3p_1a_1 = p_1^2a_1,\ 3p_2a_1 = p_2^2a_1,\ 3p_1^2a_1 = 0,\ 3p_2^2a_1 = 0,$$
$$3a_2 = p_1a_2 + p_2a_2,\ 3p_1a_2 = p_1^2a_2,\ 3p_2a_2 = p_2^2a_2,\ 3p_1^2a_2 = 0,\ 3p_2^2a_2 = 0.$$

The toric ideal is generated by

$$\{x_1^3 - x_3x_4,\ x_3^3 - x_7,\ x_4^3 - x_8,\ x_7^3 - 1,\ x_8^3 - 1,$$
$$x_2^3 - x_5x_6,\ x_5^3 - x_9,\ x_6^3 - x_{10},\ x_9^3 - 1,\ x_{10}^3 - 1,\ x_9 - x_8^2\}.$$

The order of each element in C is $\{27, 27, 9, 9, 9, 9, 3, 3, 3, 3\}$. The Gröbner basis is equal to

$$\{x_1^{27} - 1,\ x_2^{27} - 1, x_3^9 - 1,\ x_4 - x_3^8x_1^3,\ x_5^3 - x_3^3x_1^{18},\ x_6 - x_5^2x_3^6x_2^3x_1^9,$$
$$x_7 - x_3^3,\ x_8 - x_3^6x_1^9,\ x_9 - x_3^3x_1^{18},\ x_{10} - x_3^6x_2^9x_1^9\}.$$

Using the algorithm, we obtain the p-basis

$$B = \{a_1,\ a_2,\ p_1a_1,\ p_1a_2 - p_1a_1 - 6a_1\},\ M \cong \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus {\mathbb{Z}_{27}}^2,\ \underline{t}(M) = (0, 1, 1, 2).$$

Let M be an indecomposable R-module and let $S = \oplus_{i=1}^m S^{(i)}$ be the separated representation of M. If $m = 1$, then $S = \{S_1 \to k \leftarrow S_2\} = \langle a\rangle$ is a basic building block, and length$(S_j) = d(j) \neq \infty$, for $j = 1, 2$, because M is $\mathbb{Z}_{p^n}$-free. Thus, the subset $A = \{a, p_1a, \ldots, p_1^{d(1)-1}a, p_2a, \ldots, p_2^{d(2)-1}a\}$ generates S as an Abelian group over $\mathbb{Z}$. The next theorem shows how to use Algorithm 4.1 to obtain the type and a p-basis of any basic building block with torsion part.

Theorem 5.6. *Let $S = \{S_1 \to k \leftarrow S_2\} = \langle a\rangle$ be a basic building block. Then*

(i) *If $d(1)\cdot d(2) < \infty$, then Algorithm 4.1 gives a p-basis for S using the presentation $S = \langle A, pA\rangle$.*
(ii) *If $d(j) = \infty$ for exactly one j, one can obtain a basis for S, by adding to the input of Algorithm 4.1 the number* $\exp(t(S)) + 2$, *where* $\exp(t(S))$ *denotes the exponent of the torsion subgroup of $(S, +)$.*
(iii) *If both lengths are infinite then the Abelian group $(S, +)$ is torsion free. In this case, the rank is p, and $\{a, p_2a, \dots, p_2^{p-1}a\}$ is a p-basis for $R = \mathbb{Z}C_p$. If $R = \{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ is the p-pullback of $\mathbb{Z}\oplus\mathbb{Z}$, then either $\{a, p_1a\}$ or $\{a, p_2a\}$ is a p-basis for S.*

Proof. In part (iii), the case $R = \mathbb{Z}C_p$ is a direct consequence of [10, Application 1.10] and the case $R = \{\mathbb{Z} \to \mathbb{Z}_p \leftarrow \mathbb{Z}\}$ is trivial. If $d(1) < \infty$ and $d(2) < \infty$, then S is an R_p-module. So, $\langle A, pA\rangle$ is a presentation of S. Hence, applying Algorithm 4.1, we obtain a p-basis. If $d(1) = \infty$ or $d(2) = \infty$, we change the infinite length for $\exp(t(S)) + 2$. After this, we can apply Algorithm 4.1 to get a p-basis. Using the proof of Theorem 11.6 in [10], we can recover the basis for S. If $R = \mathbb{Z}C_p$ and $d(2) = \infty$, there are $p-1$ elements of order $\exp(t(S)) + 2$ in the basis, by [10, Application 1.10]. These elements have infinite order and the remaining elements in the basis form the p-basis for the torsion part. If $d(1) = \infty$, then there is one element with infinite order in the basis. If R is the p-pullback of $\mathbb{Z}\oplus\mathbb{Z}$, we have one element of infinite order in the basis. □

Theorem 5.7 describes how to find the additive structure, in general, for any indecomposable R-module after computing the p-height of the elements that connect the building blocks in M. Let d_{ji} denote $d(j, i)$. Also let $\mathtt{d}_i = p_2^{d_{2i}-1}s_{2i} = -p_1^{d_{1,i+1}-1}s_{1,i+1}$ for $1 \le i \le m-1$. If $d_{11} \ne \infty$, let $\mathtt{d}_0 = p_1^{d_{11}-1}s_{11}$, and if $d_{2m} \ne \infty$, let $\mathtt{d}_m = p_2^{d_{2m}-1}s_{2m}$. The p-height of the element $\mathtt{d}_i = p^{k-1}d'$ is $h_p(\mathtt{d}_i) = k-1$ in the Abelian group $t(M)$. Let ℓ_α be the number of elements $\mathtt{d}_i$ such that $h_p(\mathtt{d}_i) = \alpha - 1$, see [7].

Let $S = \oplus_i S^{(i)}$ be a separated representation of an indecomposable R-module M. If M is a block cycle, then we consider the separated module $S' = \oplus_i S'^{(i)}$ such that $d'_{ji} = d_{ji} - 1$ for all (j, i). If M is a deleted cycle, then we consider the separated module $S' = \oplus_i S'^{(i)}$ such that $d'_{ji} = d_{ji} - 1$ for $(j, i) \ne (1, 1)$ and $(j, i) \ne (2, m)$.

Theorem 5.7. *Let M be an indecomposable R-module, and let $S = \oplus_{i=1}^m S^{(i)}$ be the separated representation of M. Then*

$$\underline{t}(M) = \sum_{i=1}^{m} \underline{t}(S'^{(i)}) + (0, \ell_1 - \ell_2, \dots, \ell_{n-1} - \ell_n, \ell_n),$$

where $n = \exp(t(M))$.

Proof. First, suppose that $M = \langle a_1, \dots, a_m\rangle$ is a deleted cycle indecomposable R-module. If $m = 1$, the theorem is obviously true. Suppose the result is proved for $m-1$. Then consider $M/\langle \mathtt{d}_1\rangle = S'^{(1)} \oplus M'$, where $M' = \langle a_2, \dots, a_n\rangle/\langle \mathtt{d}_1\rangle$. Since

M' is generated by $m-1$ elements, we can apply induction. By [3, Corollary 3.3], if $h_p(\mathtt{d}_1) = \beta$ then

$$\begin{aligned} \underline{t}(M) &= \underline{t}(M/\langle \mathtt{d}_1 \rangle) + v(\beta) \\ &= \underline{t}(S'^{(1)}) + \sum_{k=2}^{n} \underline{t}(S'^{(k)}) + (0, \ell'_1 - \ell'_2, \dots, \ell'_{n-1} - \ell'_n, \ell'_n) + v(\beta), \end{aligned}$$

where ℓ'_α is the number of elements $\mathtt{d}'_k$ such that $h_p(\mathtt{d}'_k) = \alpha - 1$ in M'. The vector $v(\beta) = (v_0, v_1, \dots, v_n) \in \mathbb{Z}^{n+1}$ satisfies $v_{\beta-1} = -1$, $v_\beta = 1$ and $v_i = 0$ otherwise. It is clear that $h_p(\mathtt{d}'_k) = h_p(\mathtt{d}_k)$ for $k \geq 2$. So our claim holds.

Now suppose M is a block cyclic indecomposable module. Observe that the result holds for the module $M' = M/\langle \mathtt{d}_0 \rangle$, since M' is a deleted cyclic module. Hence our claim holds by [3, Corollary 3.3]. □

References

[1] D. Arnold and R. Laubenbacher, *Finitely generated modules over pullback rings*, J. Algebra **184** (1996), no. 1, 304–332.

[2] M. Artin, *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[3] M. A. Aviñó and R. Bautista, *The additive structure of indecomposable $\mathbb{Z}_{p^n}C_p$-modules*, Comm. Algebra **24** (1996), no. 8, 2567–2595.

[4] D. Cox J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*. Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[5] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*. Reprint of the 1962 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1988.

[6] M. I. Kargapolov and Yu. I. Merzlyakov, Основы теории групп. (Russian) [*Fundamentals of group theory*]. Fourth edition. Fizmatlit "Nauka", Moscow, 1996.

[7] L. Fuchs, *Infinite abelian groups*. Vol. I/II, Pure and Applied Mathematics. Vol. 36-I/II. Academic Press, New York-London, 1970/73.

[8] D. Gorenstein, *Finite groups*. Harper & Row, Publishers, New York-London, 1968.

[9] L. S. Levy, *Modules over pullbacks and subdirect sums*, J. Algebra **71** (1981), 50-61.

[10] L. S. Levy, *Mixed modules over $\mathbb{Z}G$, G cyclic of prime order, and over related Dedekind pullbacks*, J. Algebra **71** (1981), no. 1, 62-114.

[11] L. A. Nazarova and A. V. Roĭter, *Finitely generated modules over a dyad of two local Dedekind rings, and finite groups which possess an abelian normal divisor of index p*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 65–89.

[12] L. A. Nazarova, A. V. Roĭter,V. V. Sergeĭčuk, and V. M. Bondarenko, *Application of modules over a dyad to the classification of finite p-groups that have an abelian subgroup of index p and to the classification of pairs of mutually annihilating operators*, (Russian) Investigations on the theory of representations. Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **28** (1972), 69–92.

[13] B. Sturmfels, *Gröbner bases and convex polytopes*. University Lectures Series. Vol **8**. American Mathematical Society, Providence, RI, 1996.

[14] G. Szekeres, *Determination of a certain family of finite metabelian groups*, Trans. Amer. Math. Soc. **66** (1949), 1-43.

Department of Mathematics, UPR-Cayey , PR 00736
E-mail address: mavino@uprr.pr

Department of Mathematics Texas A&M University, College Station, TX 77843-3368
E-mail address: lgp@math.tamu.edu