ON THE LIFTING PROBLEM OF REPRESENTATIONS OF A METACYCLIC GROUP.

ARISTIDES KONTOGEORGIS AND ALEXIOS TEREZAKIS

Abstract. We give a necessary and sufficient condition for a modular representation of a group $G = C_{p^h} \rtimes C_m$ in a field of characteristic $p > 0$ to be lifted to a representation over local principal ideal domain of characteristic zero containing the p^h roots of unity.

1. Introduction

The lifting problem for a representation

$$\rho : G \to \mathrm{GL}_n(k),$$

where k is a field of characteristic $p > 0$, is about finding a local ring R of characteristic 0, with maximal ideal $\mathfrak{m}_R$ such that $R/\mathfrak{m}_R = k$, so that the following diagram is commutative:

$$\begin{tikzcd} & \mathrm{GL}_n(R) \arrow[d] \\ G \arrow[ur] \arrow[r] & \mathrm{GL}_n(k) \end{tikzcd}$$

Equivalently one asks if there is a free R-module V, which is also an $R[G]$-module such that $V \otimes_R R/\mathfrak{m}_R$ is the $k[G]$-module corresponding to our initial representation. We know that projective $k[G]$-modules lift to characteristic zero, [16, chap. 15], but for a general $k[G]$-module such a lifting is not always possible, for example, see [10, prop. 15]. This article aims to study the lifting problem for the group $G = C_q \rtimes C_m$, where C_q is a cyclic group of order p^h and C_m is a cyclic group of order m, $(p, m) = 1$, and also gives a necessary and sufficient condition in order to lift. We assume that the local ring R contains the q-th roots of unity and k is algebraically closed, and we might need to consider a ramified extension of R, in order to ensure that certain q-roots of unit are distant in the $\mathfrak{m}_R$-topology, see remark 36. An example of such a ring R is the ring of Witt vectors $W(k)[\zeta_q]$ with the q-roots of unity adjoined to it.

We notice that a decomposable $R[G]$-module V gives rise to a decomposable R-module modulo $\mathfrak{m}_R$ and also an indecomposable $R[G]$-module can break in the reduction modulo $\mathfrak{m}_R$ into a direct sum of indecomposable $k[G]$-summands. We also give a classification of $k[C_q \rtimes C_m]$-modules in terms of Jordan decomposition

Date: March 14, 2024.

2020 *Mathematics Subject Classification.* 20C20,20C10,14H37.

Key words and phrases. Lifting of representations, modular representation theory, integral representation theory, Generalized Oort conjecture, metacyclic groups.

and give the relation with the more usual uniserial description in terms of their socle [1].

Our interest to this problem comes from the problem of lifting local actions. The local lifting problem considers the following question: Does there exist an extension $\Lambda/W(k)$, and a representation

$$\tilde{\rho} : G \hookrightarrow \mathrm{Aut}(\Lambda[[T]]),$$

such that if t is the reduction of T, then the action of G on $\Lambda[[T]]$ reduces to the action of G on $k[[t]]$?

If the answer to the above question is positive, then we say that the G-action lifts to characteristic zero. A group G for which every local G-action on $k[[t]]$ lifts to characteristic zero is called *a local Oort group for k*. Notice that cyclic groups are always local Oort groups. This result was known as the "Oort conjecture", which was recently proved by F. Pop [15] using the work of A. Obus and S. Wewers [14].

There are a lot of obstructions that prevent a local action from lifting to characteristic zero. Probably the most important of these obstructions is the KGB-obstruction [4]. It is believed that this is the only obstruction for the local lifting problem, see [11], [12]. *In* [10, Thm. 3] *the authors have given a criterion for the local lifting, which involves the lifting of a linear representation of the same group.* The case $G = C_q \rtimes C_m$ and especially the case of dihedral groups $D_q = C_q \rtimes C_2$, is a problem of current interest in the theory of local liftings, see [12], [6], [18]. For more details on the local lifting problem we refer to [3], [4], [5], [11].

Keep also in mind that the $C_q \rtimes C_m$ groups were important to the study of group actions on holomorphic differentials of curves defined over fields of positive characteristic p, where the group involved has cyclic p-Sylow subgroup, see [2].

Let us now describe the method of proof. For understanding the splitting of indecomposable $R[G]$-modules modulo $\mathfrak{m}_R$, we develop a version of Jordan normal form in lemma 17 for endomorphisms $T : V \to V$ of order p^h, where V is a free module of rank d. We give a way to select this basis, by selecting an initial suitable element $E \in V$, see lemma 16. The normal form (as given in eq. (11)) of the element T of order q, determines the decomposition of the reduction. We show that for every indecomposable summand V_i of V, we can select E as an eigenvalue of the generator σ of C_m and then by forcing the relation $\Gamma T = T^\alpha \Gamma$ to hold, we see how the action of σ can be extended recursively to an action of σ on V_i, this is done in lemma 25. Proving that this construction gives rise to a well-defined action is a technical computation and is done in lemmata 27, 28, 29, 33, 34.

The important thing here, is that the definition of the action of σ on E is the "initial condition" of a dynamical system that determines the action of C_m on the indecomposable summand V_i. The $R[C_q \rtimes C_m]$ indecomposable module V_i can break into a direct sum $V_\alpha(\epsilon_\nu, \kappa_\nu)$-modules $1 \leq \nu \leq s$ (for a precise definition of them see definition 9, notice that κ_i denotes the dimension). The action of σ on each $V_\alpha(\epsilon_\nu, \kappa_\nu)$ can be uniquely determined by the action of σ on an initial basis element as shown in section 3, again by a "dynamical system" approach, where we need s initial conditions, one for each $V_\alpha(\epsilon_\nu, \kappa_\nu)$. The lifting condition essentially means that the indecomposable summands $V_\alpha(\epsilon, \kappa)$ of the special fibre, should be able to be rearranged in a suitable way, so that they can be obtained as reductions of indecomposable $R[C_q \rtimes C_m]$-modules. The precise expression of our lifting criterion is given in the following theorem:

Theorem 1. *Consider a $k[G]$-module M which is decomposed as a direct sum*

$$M = V_\alpha(\epsilon_1, \kappa_1) \oplus \cdots \oplus V_\alpha(\epsilon_s, \kappa_s).$$

The module lifts to an $R[G]$-module if and only if the set $\{1, \ldots, s\}$ can be written as a disjoint union of sets I_ν, $1 \leq \nu \leq t$ so that

a. $\sum_{\mu \in I_\nu} \kappa_\mu \leq q$*, for all* $1 \leq \nu \leq t$.

b. $\sum_{\mu \in I_\nu} \kappa_\mu \equiv a \bmod m$ *for all* $1 \leq \nu \leq t$*, where* $a \in \{0, 1\}$.

c. For each ν, $1 \leq \nu \leq t$ there is an enumeration $\sigma : \{1, \ldots, \#I_\nu\} \rightarrow I_\nu \subset \{1, .., s\}$, such that

$$\epsilon_{\sigma(2)} = \epsilon_{\sigma(1)} \alpha^{\kappa_{\sigma(1)}}, \epsilon_{\sigma(3)} = \epsilon_{\sigma(2)} \alpha^{\kappa_{\sigma(2)}}, \ldots, \epsilon_{\sigma(s)} = \epsilon_{\sigma(s-1)} \alpha^{\kappa_{\sigma(s-1)}}.$$

In the above proposition, each set I_ν corresponds to a collection of modules $V_\alpha(\epsilon_\mu, \kappa_\mu)$, $\mu \in I_\nu$ which come as the reduction of an indecomposable $R[C_q \rtimes C_m]$-module V_ν of V.

Aknowledgements A. Terezakis is a recipient of financial support in the context of a doctoral thesis (grant number MIS-5113934). The implementation of the doctoral thesis was co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme—Human Resources Development, Education and Lifelong Learning—in the context of the Act—Enhancing Human Resources Research Potential by undertaking a Doctoral Research—Sub-action 2: IKY Scholarship Programme for Ph.D. candidates in the Greek Universities.

Ευρωπαϊκή Ένωση
European Social Fund

Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union

ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

2. Notation

Let τ be a generator of the cyclic group C_q and σ be a generator of the cyclic group C_m. The group G is given in terms of generators and relations as follows:

$$G = \langle \sigma, \tau | \tau^q = 1, \sigma^m = 1, \sigma\tau\sigma^{-1} = \tau^\alpha \text{ for some } \alpha \in \mathbb{N}, 1 \leq \alpha \leq p^h - 1, (\alpha, p) = 1 \rangle.$$

The integer α satisfies the following congruence:

$$\alpha^m \equiv 1 \bmod q \tag{1}$$

as one sees by computing $\tau = \sigma^m \tau \sigma^{-m} = \tau^{\alpha^m}$. Also the integer α can be seen as an element in the finite field $\mathbb{F}_p$, and it is a $(p-1)$-th root of unity, not necessarily primitive. In particular the following holds:

Lemma 2. *Let $\zeta_m \in k$ be a fixed primitive m-th root of unity. There is a natural number a_0, $0 \leq a_0 < m - 1$ such that $\alpha = \zeta_m^{a_0}$.*

Proof. The integer α if we see it as an element in k is an element in the finite field $\mathbb{F}_p \subset k$, therefore $\alpha^{p-1} = 1$ as an element in $\mathbb{F}_p$. Let $\mathrm{ord}_p(\alpha)$ be the order of α in $\mathbb{F}_p^*$. By eq. (1) we have that $\mathrm{ord}_p(\alpha) \mid p-1$ and $\mathrm{ord}_p(\alpha) \mid m$, that is $\mathrm{ord}_p(\alpha) \mid (p-1, m)$.

The primitive m-th root of unity ζ_m generates a finite field $\mathbb{F}_p(\zeta_m) = \mathbb{F}_{p^\nu}$ for some integer ν, which has cyclic multiplicative group $\mathbb{F}_{p^\nu} \backslash \{0\}$ containing both the cyclic groups $\langle \zeta_m \rangle$ and $\langle \alpha \rangle$. Since for every divisor δ of the order of a cyclic group C there is a unique subgroup $C' < C$ of order δ we have that $\alpha \in \langle \zeta_m \rangle$, and the result follows. $\square$

Definition 3. For each $p^i \mid q$ we define $\mathrm{ord}_{p^i}\alpha$ to be the smallest natural number o such that $\alpha^o \equiv 1 \bmod p^i$.

It is clear that for $\nu \in \mathbb{N}$

$$\alpha^\nu \equiv 1 \bmod p^i \Rightarrow \alpha^\nu \equiv 1 \bmod p^j \text{ for all } j \leq i.$$

Therefore

$$\mathrm{ord}_{p^j}\alpha \mid \mathrm{ord}_{p^i}\alpha \text{ for } j \leq i.$$

On the other hand $\alpha \in \mathbb{N}$ and $\alpha^{p-1} \equiv 1 \bmod p$ so $\mathrm{ord}_p\alpha \mid p-1$. Also since $\sigma^t\tau\sigma^{-t} = \tau^{\alpha^t}$ we have that $\alpha^m \equiv 1 \bmod p^h$, therefore $\mathrm{ord}_p\alpha \mid \mathrm{ord}_{p^i}\alpha \mid \mathrm{ord}_{p^h}\alpha \mid m$, for $1 \leq i \leq h$.

Lemma 4. *The center* $\mathrm{Cent}_G(\tau) = \langle \tau, \sigma^{\mathrm{ord}_{p^h}\alpha}\rangle$. *Moreover*

$$\frac{|\mathrm{Cent}_G(\tau)|}{p^h} = \frac{m}{\mathrm{ord}_{p^h}(\alpha)} =: m'$$

Proof. The result follows by observing $(\tau^\nu\sigma^t)\tau(\tau^\nu\sigma^t)^{-1} = \tau^{\alpha^t}$, for all $1 \leq \nu \leq q$, $1 \leq t \leq m$. □

Remark 5. If $\mathrm{ord}_p\alpha = m$ then $\mathrm{ord}_{p^i}\alpha = m$ for all $1 \leq i \leq h$.

Lemma 6. *If the group $G = C_q \rtimes C_m$ is a subgroup of* $\mathrm{Aut}(k[[t]])$, *then all orders* $\mathrm{ord}_{p^i}\alpha = m/m'$, *for all* $1 \leq i \leq h$.

Proof. We will use the notation of the book of J.P.Serre on local fields [17]. By [13, Th.1.1b] we have that the first gap i_0 in the lower ramification filtration of the cyclic group C_q satisfies $(m, i_0) = m'$.

The ramification relation [17, prop. 9 p. 69]

$$\alpha\theta_{i_0}(\tau) = \theta_{i_0}(\tau^\alpha) = \theta_{i_0}(\sigma\tau\sigma^{-1}) = \theta_0(\sigma)^{i_0}\theta_{i_0}(\tau),$$

implies that $\theta_0(\sigma)^{i_0} = \alpha \in \mathbb{N}$. From $(m, i_0) = m'$ and the fact that $\mathrm{ord}\theta_0(\sigma) = m$ we obtain

$$\frac{m}{m'} = \mathrm{ord}\theta_0(\sigma)^{i_0} = \mathrm{ord}_p(\alpha).$$

Thus

$$\frac{m}{m'} = \mathrm{ord}_p\alpha | \mathrm{ord}_{p^i}\alpha | \mathrm{ord}_{p^h}\alpha = \frac{m}{m'}.$$

Hence all orders $\mathrm{ord}_{p^i}\alpha = m/m'$. □

Remark 7. If the KGB-obstruction vanishes and $\alpha \neq 1$, then by [11][prop. 5.9] $i_0 \equiv -1 \bmod m$ and $\mathrm{ord}_{p^i}\alpha = m$ for all $1 \leq i \leq h$.

3. Indecomposable $C_q \rtimes C_m$ modules, modular representation theory

In this section we will describe the indecomposable $C_q \rtimes C_m$-modules. We will give two methods in studying them. The first one is needed since it is in accordance with the method we will give in order to describe indecomposable $R[C_q \rtimes C_m]$-modules. The second one, using the structure of the socle, is the standard method of describing $k[C_q \rtimes C_m]$-modules in modular representation theory.

3.1. **Linear algebra method.** The indecomposable modules for the group C_q are determined by the Jordan normal forms of the generator τ of the cyclic group C_q. So for each $1 \leq \kappa \leq p^h$ there is exactly one C_q indecomposable module of dimension κ denoted by J_κ. Therefore, we have the following decomposition of an indecomposable $C_q \rtimes C_m$-module M considered as a C_q-module.

$$M = J_{\kappa_1} \oplus \cdots \oplus J_{\kappa_r}. \tag{2}$$

Lemma 8. *In the indecomposable module J_κ, for every element E such that*

$$(\tau - \mathrm{Id}_\kappa)^{\kappa-1} E \neq 0$$

the elements $B = \{E, (\tau - \mathrm{Id}_\kappa)E, \ldots, (\tau - \mathrm{Id}_\kappa)^{\kappa-1}E\}$ form a basis of J_κ such that the matrix of τ with respect to this basis is given by

$$\tau = \mathrm{Id}_\kappa + \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \tag{3}$$

In the above notation Id_κ denotes the $\kappa \times \kappa$ identity matrix.

Proof. Since the set B has κ-elements it is enough to prove that it consists of linear independent elements. Indeed, consider a linear relation

$$\lambda_0 E + \lambda_1(\tau - \mathrm{Id}_\kappa)E + \cdots + \lambda_{\kappa-1}(\tau - \mathrm{Id}_\kappa)^{\kappa-1}E = 0.$$

By applying $(\tau - \mathrm{Id}_\kappa)^{\kappa-1}$ we obtain $\lambda_0(\tau - \mathrm{Id}_\kappa)^{\kappa-1}E = 0$, which gives us $\lambda_0 = 0$. We then apply $(\tau - \mathrm{Id}_\kappa)^{\kappa-2}$ to the linear relation and by the same argument we obtain $\lambda_1 = 0$ and we continue this way proving that $\lambda_0 = \cdots = \lambda_{\kappa-1} = 0$. The matrix form of τ with respect to this basis is immediate. ☐

Equation (2) is a decomposition of an indecomposable $C_q \rtimes C_m$-module in terms of indecomposable C_q-modules. If we prove that σ acts on each C_q-indecomposable summand J_κ of eq. (2), then this implies that there is only one indecomposable C_q summand in the decomposition, that is $r = 1$. Since the field k is algebraically closed and $(m, p) = 1$ we know that there is a basis of M consisting of eigenvectors of σ. Set $\kappa = \kappa_1$ and $E = E_1$. There is an eigenvector E of σ, which is not in the kernel of $(\tau - \mathrm{Id}_\kappa)^{\kappa-1}$. Then the elements of the set $B = \{E, (\tau - \mathrm{Id}_\kappa)E, \ldots, (\tau - \mathrm{Id}_\kappa)^{\kappa-1}E\}$ are linearly independent and form a direct C_q summand of M isomorphic to J_κ.

We will now show that this module is an $k[C_q \rtimes C_m]$-module. For this, we have to show that the generator σ of C_m acts on the basis B. Observe that for every $0 \leq i \leq \kappa - 1 < p^h$

$$\sigma(\tau - 1)^{i-1} = (\tau^\alpha - 1)^{i-1}\sigma.$$

This means that the action of σ on E determines the action of σ on all other basis elements $e_\nu := (\tau - 1)^{\nu-1}e$, $1 \leq \nu \leq \kappa$.

Let us compute:

$$\sigma e_{i+1} = \sigma(\tau - 1)^i e = (\tau^\alpha - 1)^i \zeta_m^\lambda e$$

On the basis $\{e_1,\ldots,e_\kappa\}$ the matrix τ is given by eq. (3) hence using the binomial formula we compute

$$\tau^\alpha = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \binom{\alpha}{1} & 1 & \ddots & & & \vdots \\ \binom{\alpha}{2} & \binom{\alpha}{1} & \ddots & \ddots & & \vdots \\ \binom{\alpha}{3} & \binom{\alpha}{2} & \ddots & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \binom{\alpha}{1} & 1 & 0 \\ \binom{\alpha}{k} & \binom{\alpha}{k-1} & \cdots & \binom{\alpha}{2} & \binom{\alpha}{1} & 1 \end{pmatrix}. \tag{4}$$

Thus $\tau^\alpha - 1$ is a nilpotent matrix $A=(a_{ij})$ of the form:

$$a_{ij} = \begin{cases} \binom{\alpha}{\mu} & \text{if } j = i-\mu \text{ for some } \mu, 1 \leq \mu \leq \kappa \\ 0 & \text{if } j \geq i \end{cases}$$

The ℓ-th power $A^\ell = (a_{ij}^{(\ell)})$ of A is then computed by (keep in mind that $a_{ij}=0$ for $i \leq j$)

$$a_{ij}^{(\ell)} = \sum_{i<\nu_1<\cdots<\nu_{\ell-1}<j} a_{i,\nu_1} a_{\nu_1,\nu_2} a_{\nu_2,\nu_3} \cdots a_{\nu_{\ell-1},j}$$

This means that we need $i-j>\ell$ in order to have $a_{ij}\neq 0$. Moreover for $i=j+\ell$ (which is the first non zero diagonal below the main diagonal) we have

$$a_{i,i+\ell} = a_{i,i+1}a_{i+1,i+2}\cdots a_{i+\ell-1,i+\ell} = \binom{\alpha}{1}^\ell = \alpha^\ell.$$

Therefore, the matrix of A^ℓ is of the following form:

$$\begin{array}{c} \overbrace{\qquad\qquad\qquad}^{k-\ell} \quad \overbrace{\qquad\qquad}^{\ell} \\ \begin{pmatrix} 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \alpha^\ell & \ddots & & 0 & \vdots & & \vdots \\ * & \alpha^\ell & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ * & \cdots & * & \alpha^\ell & 0 & \cdots & 0 \end{pmatrix} \end{array} \tag{5}$$

Definition 9. We will denote by $V_\alpha(\lambda,\kappa)$ the indecomposable κ-dimensional G-module given by the basis elements $\{(\tau-1)^\nu e, \nu=0,\ldots,\kappa-1\}$, where $\sigma e = \zeta_m^\lambda e$.

This definition is close to the notation used in [9].

Lemma 10. *The action of σ on the basis element e_i of $V_\alpha(\lambda,\kappa)$ is given by:*

$$\sigma e_i = \alpha^{i-1}\zeta_m^\lambda e_i + \sum_{\nu=i+1}^{\kappa} a_\nu e_\nu, \tag{6}$$

for some coefficients $a_i \in k$. In particular the matrix of σ with respect to the basis $e_1,\ldots,e_\kappa$ is lower triangular.

Proof. Recall that $e_i = (\tau-1)^{i-1}e_1$. Therefore

$$\sigma e_i = \sigma(\tau-1)^{i-1}e_1 = (\tau^\alpha - 1)^{i-1}\sigma e_1 = \zeta_m^\lambda(\tau^\alpha-1)^{i-1}e_1.$$

The result follows by eq. (5) □

We have constructed a set of indecomposable modules $V_\alpha(\lambda,\kappa)$. Apparently $V_\alpha(\lambda,\kappa)$ can not be isomorphic to $V_\alpha(\lambda',\kappa')$ if $\kappa \neq \kappa'$, since they have different dimensions.

Assume now that $\kappa=\kappa'$. Can the modules $V_\alpha(\lambda,\kappa)$ and $V_\alpha(\lambda',\kappa)$ be isomorphic for $\lambda\neq\lambda'$?

The eigenvalues of the prime to p generator σ on $V_\alpha(\lambda,\kappa)$ are

$$\zeta_m^\lambda, \alpha\zeta_m^\lambda, \ldots, \alpha^{\kappa-1}\zeta_m^\lambda.$$

Similarly the eigenvalues for σ when acting on $V_\alpha(\lambda',\kappa)$ are

$$\zeta_m^{\lambda'}, \alpha\zeta_m^{\lambda'}, \ldots, \alpha^{\kappa-1}\zeta_m^{\lambda'}.$$

If the two sets of eigenvalues are different then the modules can not be isomorphic. But even if $\lambda\neq\lambda' \bmod m$ the two sets of eigenvalues can still be equal. Even in this case the modules can not be isomorphic.

Lemma 11. *The modules $V_\alpha(\lambda_1,\kappa)$ and $V_\alpha(\lambda_2,\kappa)$ are isomorphic if and only if $\lambda_1\equiv\lambda_2 \bmod m$.*

Proof. Indeed, the module $V_\alpha(\lambda_1,\kappa)$ has an element e so that the vectors

$$e, (\tau-1)e, (\tau-1)^2e, \ldots, (\tau-1)^{\kappa-1}e \tag{7}$$

form a basis of $V_\alpha(\lambda_1,\kappa)$, so that $\sigma e = \zeta_m^{\lambda_1}e$. Let $\phi: V_\alpha(\lambda_2,\kappa)\rightarrow V_\alpha(\lambda_1,\kappa)$ be an isomorphism. Let $e'\in V_\alpha(\lambda_2,\kappa)$ be an eigenvalue of σ with $\sigma e' = \zeta_m^{\lambda_2}e'$ so that $e',(\tau-1)e',\ldots,(\tau-1)^{\kappa-1}e'$ form a basis of $V_\alpha(\lambda_2,\kappa)$. Set $V_\alpha(\lambda_1,\kappa)\ni E=\phi(e')$. We now express E in the basis of $V_\alpha(\lambda_1,\kappa)$:

$$E = \sum_{\nu=0}^{\kappa-1}\xi_\nu(\tau-1)^\nu e,$$

for some $\xi_\nu\in k$. Observe that $\xi_0\neq 0$. Indeed, since ϕ is an equivariant isomorphism, the elements $E,(\tau-1)E,\ldots,(\tau-1)^{\kappa-1}$ should be a basis of $V_\alpha(\lambda_1,\kappa)$ and if $\xi_0=0$, then $(\tau-1)^{\kappa-1}E=0$.

Using eq. (6) we see that σ with respect to the basis given in eq. (7) admits the matrix form:

$$\begin{pmatrix} \zeta_m^{\lambda_1} & 0 & \cdots & \cdots & 0 \\ 0 & \alpha\zeta_m^{\lambda_1} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & \alpha^{\kappa-1}\zeta_m^{\lambda_1} \end{pmatrix}.$$

Therefore,

$$\sigma(E) = \sum_{\nu=0}^{\kappa-1}\xi_i\alpha^\nu\zeta_m^{\lambda_1}(\tau-1)^\nu e \tag{8}$$

and on the other hand $\sigma(E) = \zeta_m^{\lambda_2} E$, since ϕ is an equivariant isomorphism, therefore

$$\sigma(E) = \sum_{\nu=0}^{\kappa-1} \zeta_m^{\lambda_2} \xi_i (\tau-1)^{\nu} e \tag{9}$$

By comparing the coefficients of the basis element e in expresions (8), (9) we arrive at

$$\xi_0(\zeta_m^{\lambda_1} - \zeta_m^{\lambda_2}) = 0,$$

and since $\xi_0 \neq 0$ we have that $\lambda_1 \equiv \lambda_2 \bmod m$ as desired.

□

3.2. **The uniserial description.** We will now give an alternative description of the indecomposable $C_q \rtimes C_m$-modules, which is used in [2].

It is known that $\mathrm{Aut}(C_q) \cong \mathbb{F}_p^* \times Q$, for some abelian p-group Q. The representation $\psi : C_m \to \mathrm{Aut}(C_q)$ given by the action of C_m on C_q is known to factor through a character $\chi : C_m \to \mathbb{F}_p^*$. The order of χ divides $p-1$ and $\chi^{p-1} = \chi^{-(p-1)}$ is the trivial one dimensional character.

For all $i \in \mathbb{Z}$, χ^i defines a simple $k[C_m]$-module of k dimension one, which we will denote by S_{χ^i}. For $0 \leq \ell \leq m-1$ denote by S_ℓ the simple module where σ acts as ζ_m^ℓ. Both S_{χ^i}, S_ℓ can be seen as $k[C_q \rtimes C_m]$-modules using inflation. Finally for $0 \leq \ell \leq m-1$ we define $\chi^i(\ell) \in \{0, 1, \ldots, m-1\}$ such that $S_{\chi^i(\ell)} \cong S_\ell \otimes_k S_{\chi^i}$.

There are $q \cdot m$ isomorphism classes of indecomposable $k[C_q \rtimes C_m]$-modules and are all uniserial. An indecomposable $k[C_q \rtimes C_m]$-module U is unique determined by its socle, which is the kernel of the action of $\tau - 1$ on U, and its k-dimension. For $0 \leq \ell \leq m-1$ and $1 \leq \mu \leq q$, let $U_{\ell,\mu}$ be the indecomposable $k[C_q \rtimes C_m]$ module with socle S_a and k-dimension μ. Then $U_{\ell,\mu}$ is uniserial and its μ ascending composition factors are the first μ composition factors of the sequence

$$S_\ell, S_{\chi^{-1}(\ell)}, S_{\chi^{-2}(\ell)}, \ldots, S_{\chi^{-(p-2)}(\ell)}, S_\ell, S_{\chi^{-1}(\ell)}, S_{\chi^{-2}(\ell)}, \ldots, S_{\chi^{-(p-2)}(\ell)}.$$

Lemma 12. *There is the following relation between the two different notations for indecomposable modules:*

$$V_\alpha(\lambda, \kappa) = U_{(\lambda + a_0(\kappa-1)) \bmod m, \kappa)},$$

recall that $\alpha = \zeta_m^{a_0}$. In particular, for the case of dihedral groups D_q we have the relation

$$V_\alpha(\lambda, \kappa) = U_{\lambda+\kappa-1 \bmod 2, \kappa}.$$

Proof. Indeed, in the $V_\alpha(\lambda, \kappa)$ notation we describe the action of σ on the generator e, by assuming that $\sigma e = \zeta_m^\lambda e$. We can then describe the action on every basis element $e_i = (\tau-1)^{i-1} e$, using the group relations

$$\sigma e_i = \sigma(\tau-1)^{i-1} e = (\tau^\alpha - 1)^{i-1} \sigma e = \zeta_m^\lambda (\tau^\alpha - 1)^{i-1} e$$

We will use eq. (10) and in particular

$$\sigma e_\kappa = \alpha^{\kappa-1} \zeta_m^\lambda.$$

In the $U_{\mu,\kappa}$ notation, μ is the action on the one-dimensional socle which is the τ-invariant element $e_\kappa = (\tau-1)^{\kappa-1} e$, i.e. $\sigma(e_\kappa) = \zeta_m^\mu$. Putting all this together we have

$$\mu = \lambda + (\kappa-1) a_0 \bmod m.$$

In the case of dihedral group D_q, $m = 2$ and $\alpha = -1^{a_0}$, i.e. $a_0 = 1$, we have $V_\alpha(\lambda, \kappa) = U_{\lambda+\kappa-1 \bmod 2, \kappa}$. □

Remark 13. The condition $\mathrm{ord}_{p^i} \alpha = m$ for all $1 \leq i \leq h$, is equivalent to requiring that $\psi_i : C_m \to \mathrm{Aut}(C_{p^i})$ is faithful for all i.

4. Lifting of representations

Proposition 14. *Let $G = C_q \rtimes C_m$. Assume that for all $1 \leq i \leq h$, $ord_{p^i} \alpha = m$. If the $k[G]$-module $\bar{V}$ lifts to an $R[G]$-module V, where $K = \mathrm{Quot(R)}$ is a field of characterstic zero, then*

$$m \mid \left(\dim(V \otimes_R K) - \dim V \otimes_R K)^{C_q} \right).$$

Let $T : V \to V$ be a lift of the generator τ of C_q and $S : V \to V$ is a lift of the generator σ of C_m satisfying

$$S^m = 1, T^q = 1, STS^{-1} = T^\alpha.$$

If $V(\zeta_q^{\alpha^i \kappa})$ is the eigenspace of the eigenvalue $\zeta_q^{\alpha^i \kappa}$ of T acting on V, then

$$\dim V(\zeta_q^\kappa) = \dim V(\zeta_q^{\alpha\kappa}) = \dim V(\zeta_q^{\alpha^2 \kappa}) = \cdots = \dim V(\zeta_q^{\alpha^{m-1}\kappa}).$$

Proof. Consider a lifting V of V. The generator τ of the cyclic part C_q has eigenvalues $\lambda_1, \ldots, \lambda_s$ which are p^h-roots of unity. Let ζ_q be a primitive q-root of unity. Consider any eigenvalue $\lambda \neq 1$. It is of the form $\lambda = \zeta_q^\kappa$ for some $\kappa \in \mathbb{N}, q \nmid \kappa$. If E is an eigenvector of T corresponding to λ, that is $TE = \zeta_q^\kappa E$ then

$$TS^{-1}E = S^{-1}T^\alpha E = \zeta_q^{\kappa\alpha} S^{-1}E$$

and we have a series of eigenvectors $E, S^{-1}E, S^{-2}E, \cdots$ with corresponding eigenvalues $\zeta_q^\kappa, \zeta_q^{\kappa\alpha}, \zeta_q^{\kappa a^2} \cdots, \zeta_q^{\kappa\alpha^{o-1}}$, where $o = \mathrm{ord}_{q/(q,\kappa)}\alpha$. Indeed, the integer o satisfies the relation

$$\kappa\alpha^o \equiv \kappa \bmod q \Rightarrow \alpha^o \equiv 1 \bmod \frac{q}{(q,\kappa)}.$$

Using lemma 6 we obtain $o = m$. Therefore the eigenvalues $\lambda \neq 1$ form orbits of size m, while the eigenspace of the eigenvalue 1 is just the invariant space V^G and the result follows. □

5. Indecomposable $C_q \rtimes C_m$ modules, integral representation theory

From now on V is a free R-module, where R is an integral local principal ideal domain with maximal ideal $\mathfrak{m}_R$, R has characteristic zero and R contains all q-th roots of unity. Let $K = \mathrm{Quot}(R)$.

The indecomposable modules for a cyclic group both in the ordinary and in the modular case are described by writing down the Jordan normal form of a generator of the cyclic group. Since in integral representation theory there are infinitely many non-isomorphic indecomposable C_q-modules for $q = p^h$, $h \geq 3$, one is not expecting to have a theory of Jordan normal forms even if one works over complete local principal ideal domains [7], [8].

Lemma 15. *Let T be an element of order $q = p^h$ in $\mathrm{End}(V)$. The minimal polynomial of T has simple eigenvalues and T is diagonalizable when seen as an element in* $\mathrm{End}(V \otimes K)$.

Proof. Since $T^q = \mathrm{Id}_V$, the minimal polynomial of T divides $x^q - 1$, which has simple roots over a field of characteristic zero. This ensures that $T \in \mathrm{End}(V \otimes K)$ is diagonalizable. □

Lemma 16. *Let $f(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_d)$ be the minimal polynomial of T on V. There is an element $E \in V$, such that*

$$E, (T - \lambda_1 \mathrm{Id}_V)E, (T - \lambda_2 \mathrm{Id}_V)(T - \lambda_1 \mathrm{Id}_V)E, \ldots, (T - \lambda_{d-1}\mathrm{Id}_V) \cdots (T - \lambda_1 \mathrm{Id}_V)E$$

are linear independent elements in $V \otimes K$.

Proof. Consider the endomorphisms for $i = 1, \ldots, d$

$$\Pi_i = \prod_{\substack{\nu=1 \\ \nu \neq i}}^{d} (T - \lambda_\nu \mathrm{Id}_V).$$

In the above product notice that $T - \lambda_i \mathrm{Id}_V$, $T - \lambda_j \mathrm{Id}_V$ are commuting endomorphisms. Since the minimal polynomial of T has degree d all R-modules $\mathrm{Ker}\Pi_i$ are proper subsets of V. Since V can not be a finite union of proper submodules there is an element $E \in V$ such that $E \notin \mathrm{Ker}(\Pi_i)$ for all $1 \leq i \leq d$. Consider a relation

$$\sum_{\mu=0}^{d} \gamma_\mu \prod_{\nu=0}^{\mu} (T - \lambda_\mu \mathrm{Id}_V)E, \tag{10}$$

where $\prod_{\nu=0}^{0}(T - \lambda_\nu \mathrm{Id}_V)E = E$. We fist apply the operator $\prod_{\nu=2}^{d}(T - \lambda_\nu \mathrm{Id}_V)$ to eq. (10) and we obtain

$$0 = \gamma_0 \Pi_1 E,$$

and by the selection of E we have that $\gamma_0 = 0$. We now apply $\prod_{\nu=3}^{d}(T - \lambda_\nu \mathrm{Id}_V)$ to eq. (10). We obtain that

$$0 = \gamma_1 \prod_{\nu=3}^{d} (T - \lambda_\nu \mathrm{Id}_V)(T - \lambda_1 \mathrm{Id}_V) = \gamma_1 \Pi_2 E,$$

and by the selection of E we have that $\gamma_1 = 0$. We now apply $\prod_{\nu=4}^{d}(T - \lambda_\nu \mathrm{Id}_V)$ to eq. (10) and we obtain

$$0 = \gamma_2 \prod_{\nu=4}^{d} (T - \lambda_\nu \mathrm{Id}_V)(T - \lambda_2 \mathrm{Id}_V)(T - \lambda_1 \mathrm{Id}_V)E = \gamma_2 \Pi_3 E$$

and by the selection of E we obtain $\gamma_3 = 0$. Continuing this way we finally arrive at $\gamma_0 = \gamma_1 = \cdots = \gamma_{d-1} = 0$. □

Lemma 17. *Let V be a free R-module of rank d acted on by an automorphism $T : V \to V$ of order p^h. Assume that the minimal polynomial of T is of degree d and has roots $\lambda_1, \ldots, \lambda_d$. Then $T = (t_{ij})$ can be written as a matrix with respect to* *the basis as follows:*

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & \cdots & 0 \\ a_1 & \lambda_2 & \ddots & & \vdots \\ 0 & a_2 & \lambda_3 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{d-1} & \lambda_d \end{pmatrix} \tag{11}$$

i.e.

$$t_{ij} = \begin{cases} \lambda_i & \text{if } i = j \\ a_j & \text{if } i = j+1 \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Proof. By lemma 16 the elements

$$E, (T - \lambda_1 \mathrm{Id}_V)E, (T - \lambda_2 \mathrm{Id}_V)(T - \lambda_1 \mathrm{Id}_V)E, \ldots, (T - \lambda_{d-1}\mathrm{Id}_V) \cdots (T - \lambda_1 \mathrm{Id}_V)E$$

form a free submodule of V of rank d. The theory of submodules of principal ideal domains, there is a basis $E_1, E_2, \ldots, E_d$ of the free module V such that

$$\begin{aligned} E_1 &= E, \\ a_1 E_2 &= (T - \lambda_1 \mathrm{Id}_V)E_1, \\ a_2 E_3 &= (T - \lambda_2 \mathrm{Id}_V)E_2, \\ &\cdots \\ a_{d-1} E_d &= (T - \lambda_{d-1} \mathrm{Id}_V)E_{d-1}. \end{aligned} \tag{13}$$

Let us consider the module $V_1 = \langle E_1, \ldots, E_d \rangle \subset V$. By construction, the map T restricts to an automorphism $V_1 \to V_1$ that has the desired matrix form with respect to the basis $E_1, \ldots, E_d$. We then consider the free module V/V_1 and we repeat the procedure for the minimal polynomial of T, which again acts on V/V_1. The desired result follows. □

Remark 18. The element T as defined in eq. (11) has order equal to the higher order of the eigenvalues $\lambda_1, \ldots, \lambda_d$ involved. Indeed, since we have assumed that the eigenvalues are different the matrix is diagonalizable in Quot(R) and has order equal to the maximal order of the eigenvalues involved. In particular it has order q if there is at least one λ_i that is a primitive q-root of unity. The statement about the order of T is not necessarily true if some of the eigenvalues are the same. For instance the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ has infinite order over a field of characteristic zero.

Remark 19. The number of indecomposable $R[T]$-summands of V is given by $\#\{i : a_i = 0\} + 1$.

A lift of a sum of indecomposable kC_q-modules $J_{\kappa_1} \oplus \cdots \oplus J_{\kappa_n}$ can form an indecomposable RC_q-module. For example, the indecomposable module where the generator T of C_q has the form

$$T = \begin{pmatrix} \lambda_1 & 0 & \cdots & \cdots & 0 \\ a_1 & \lambda_2 & \ddots & & \vdots \\ 0 & a_2 & \lambda_3 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{d-1} & \lambda_d \end{pmatrix}$$

where $a_1 = \cdots = a_{\kappa_1 - 1} = 1$, $a_{\kappa_1} \in \mathfrak{m}_R$, $a_{\kappa_1+1}, \ldots, a_{\kappa_2+\kappa_1-1} = 1$, $a_{\kappa_2+\kappa_1} \in \mathfrak{m}_R$, etc reduces to a decomposable direct sum of Jordan normal forms of sizes $\kappa_1, \kappa_2, \ldots$.

Remark 20. It is an interesting question to classify these matrices up to conjugation with a matrix in $\mathrm{GL}_d(R)$. It seems that the valuation of elements a_i should also play a role.

Definition 21. Let $h_i(x_1, \ldots, x_j)$ be the complete symmetric polynomial of degree i in the variables $x_1, \ldots, x_j$. For instance

$$h_3(x_1, x_2, x_3) = x_1^3 + x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_2 x_3 + x_1 x_3^2 + x_2^3 + x_2^2 x_3 + x_2 x_3^2 + x_3^3.$$

Set

$$L(\kappa, j, \nu) = h_\kappa(\lambda_j, \lambda_{j+1}, \ldots, \lambda_{j+\nu})$$
$$A(i,j) = \begin{cases} a_i a_{i+1} \cdots a_{i+j} & \text{if } j \geq 0 \\ 0 & \text{if } j < 0 \end{cases}$$

Lemma 22. *The matrix $T^\alpha = (t_{ij}^{(\alpha)})$ is given by the following formula:*

$$t_{ij}^{(\alpha)} = \begin{cases} \lambda_i^\alpha & \text{if } i = j \\ A(j, i-j-1) \cdot L(\alpha - (i-j), j, i-j) & \text{if } j < i \\ 0 & \text{if } j > i \end{cases}$$

Proof. For $j \geq i$ the proof is trivial. When $j < i$ and $\alpha = 1$ it is immediate, since $L(x, \cdot, \cdot) \equiv 0$, for every $x \leq 0$. Assume this holds for $\alpha = n$. Set $\alpha = n+1$, we consider first the case $j+1 < i$, using eq. (12)

$$\begin{aligned} t_{ij}^{(n+1)} &= \sum_{k=1}^{r} t_{ik}^{(n)} t_{kj} = \lambda_j t_{ij}^{(n)} + a_j t_{i,j+1}^{(n)} = \lambda_j A(j, i-j-1) L(n-(i-j), j, i-j) + \\ &+ a_j A(j+1, i-j-2) L(n-(i-j-1), j+1, i-j-1) = \\ &= A(j, i-j-1) \left(\lambda_j h_{n-(i-j)}(\lambda_j, \ldots, \lambda_i) + h_{n-(i-j)+1}(\lambda_{j+1}, \ldots, \lambda_i) \right) = \\ &= A(j, i-j-1) h_{n-(i-j)+1}(\lambda_j, \ldots, \lambda_i) = \\ &= A(j, i-j-1) L(n-(i-j)+1, i, i-j). \end{aligned}$$

If $j+1=i$ then we compute

$$\begin{aligned} t_{ij}^{(n+1)} &= \sum_{k=1}^{r} t_{ik}^{(n)} t_{kj} = \lambda_j t_{ij}^{(n)} + a_j t_{i,j+1}^{(n)} \\ &= \lambda_j A(j, i-j-1) L(n-(i-j), j, i-j) + a_j \lambda_{j+1,j+1}^{(n)} \\ &= \lambda_j A(j,0) L(n-1, j, 1) + a_j \lambda_{j+1,j+1}^{(n)} \\ &= A(j,0)\left(\lambda_j h_{n-1}(\lambda_j, \lambda_{j+1}) + h_n(\lambda_{j+1})\right) \\ &= A(j,0) h_n(\lambda_j, \lambda_{j+1}) \\ &= A(j, i-j-1) L(n-(i-j)+1, i, i-j). \end{aligned}$$

□

Remark 23. The space of homogeneous polynomials of degree c in n-variables has dimension $\binom{n-1+c}{n-1}$. Since all q-roots of unity are reduced to 1 modulo $\mathfrak{m}_R$ the quantity $L(\alpha-(i-j), j, i-j)$ is reduced to the number of terms in $h_{\alpha-(i-j)}(\lambda_j, \ldots, \lambda_i)$, which is equal to dimension of homogeneous polynomials of degree $c = \alpha - (i-j)$ in $n = (i-j)+1$ variables, that is

$$L(\alpha-(i-j), j, i-j) \equiv \binom{n-1+c}{n-1} = \binom{\alpha}{i-j} \bmod \mathfrak{m}_R.$$

This computation is compatible with the computation of τ^α given in eq. (4).

Recall that we have defined in proposition 14 the element $S: V \to V$ to be a lift of the element σ generating C_m.

Lemma 24. *There is an eigenvector E of the lift S, which is a generator of the cyclic group C_m, so that E is not an element in $\bigcup_{i=1}^{s} \mathrm{Ker}(\Pi_i \otimes K)$.*

Proof. The eigenvectors $E_1, \ldots, E_d$ of S form a basis of the space $V \otimes K$. By multiplying by certain elements in R, if necessary, we can assume that all E_i are in V and their reductions $E_i \otimes R/\mathfrak{m}_R$, $1 \le i \le d$ give rise to a basis of eigenvectors of a generator of the cyclic group C_m acting on $V \otimes R/\mathfrak{m}_R$. If every eigenvector E_i is an element of some $\mathrm{Ker}(\Pi_\nu)$ for $1 \le i \le d$, then their reductions will be elements in $\mathrm{Ker}(T-1)^{d-1}$, a contradiction since the later kernel has dimension $< d$. □

Lemma 25. *Let V be a free $C_q \rtimes C_m$-module, which is indecomposable as a C_q-module. Consider the basis given in lemma 17. Then the value of $S(E_1)$ determines $S(E_i)$ for $2 \le i \le d$.*

Proof. Let $S: V \to V$ be a generator of the cyclic group C_m. We will use the notation of lemma 16. We use lemma 24 in order to select a suitable eigenvector of E_1 of S and then form the basis $E_1, E_2, \ldots, E_d$ as given in eq. (13). We can compute the action of S on all basis elements E_i by

$$S(a_{i-1}E_i) = S(T - \lambda_{i-1}\mathrm{Id}_V)E_{i-1} = (T^a - \lambda_{i-1}\mathrm{Id}_V)S(E_{i-1}). \tag{14}$$

This means that one can define recursively the action of S on all elements E_i. Indeed, assume that

$$S(E_{i-1}) = \sum_{\nu=1}^{d} \gamma_{\nu,i-1} E_\nu.$$

We now have

$$(T^a - \lambda_{i-1}\mathrm{Id}_V)E_\nu = \sum_{\mu=1}^{d} t^{(\alpha)}_{\mu,\nu} E_\mu - \lambda_{i-1}E_\nu$$
$$= (\lambda_\nu^\alpha - \lambda_{i-1})E_\nu + \sum_{\mu=\nu+1}^{d} t^{(\alpha)}_{\mu,\nu} E_\mu.$$

We combine all the above to

$$a_{i-1}S(E_i) = \sum_{\nu=1}^{d} \gamma_{\nu,i-1}(\lambda_\nu^\alpha - \lambda_{i-1})E_\nu + \sum_{\nu=1}^{d} \gamma_{\nu,i-1} \sum_{\mu=\nu+1}^{d} t^{(\alpha)}_{\mu,\nu} E_\mu$$
$$= \sum_{\nu=1}^{d} \tilde{\gamma}_{\nu,i} E_\nu, \tag{15}$$

for a selection of elements $\tilde{\gamma}_{\nu,i} \in R$, which can be explicitly computed by collecting the coefficients of the basis elements $E_1, \ldots, E_d$.

Observe that the quantity on the right hand side of eq. (15) must be divisible by a_{i-1}. Indeed, let v be the valuation of the local principal ideal domain R. Set

$$e_0 = \min_{1 \le \nu \le d} \{v(\tilde{\gamma}_{\nu,i})\}.$$

If $e_0 < v(a_{i-1})$, then we divide eq. (15) by π^{e_0}, where π is the local uniformizer of R, that is $\mathfrak{m}_R = \pi R$. We then consider the divided equation modulo $\mathfrak{m}_R$ to obtain a linear dependence relation among the elements $E_i \otimes k$, which is a contradiction. Therefore $e_0 \ge v(a_{i-1})$ and we obtain an equation

$$S(E_i) = \sum_{\nu=1}^{d} \frac{\tilde{\gamma}_{\nu,i}}{a_{i-1}} E_\nu = \sum_{\nu=1}^{d} \gamma_{\nu,i} E_\nu.$$

□

For example $S(E_1) = \zeta_m^\epsilon E_1$. We compute that

$$a_1 S(E_2) = (T^\alpha - \lambda_1 \mathrm{Id}) S(E_1)$$

and

$$S(E_2) = \frac{(\lambda_1^\alpha - \lambda_1)}{a_1} \zeta_\mu^\epsilon E_1 + \zeta_m^\epsilon \sum_{\mu=2}^{d} \frac{t^{(\alpha)}_{\mu,1}}{a_1} E_\mu$$
$$= \frac{(\lambda_1^\alpha - \lambda_1)}{a_1} \zeta_\mu^\epsilon E_1 + \zeta_m^\epsilon \sum_{\mu=2}^{d} \frac{A(1,\mu-2)L(\alpha-(\mu-1),1,\mu-1)}{a_1} E_\mu$$
$$= \frac{(\lambda_1^\alpha - \lambda_1)}{a_1} \zeta_\mu^\epsilon E_1 + \zeta_m^\epsilon \sum_{\mu=2}^{d} \frac{a_1 a_2 \cdots a_{\mu-1} h_{\alpha-(\mu-1)}(\lambda_1, \lambda_2, \ldots, \lambda_\mu)}{a_1} E_\mu.$$

Proposition 26. *Assume that no element $a_1, \ldots, a_{d-1}$ given in eq. (11) is zero. Given $\alpha \in \mathbb{N}, \alpha \ge 1$ and an element E_1, which is not an element in $\bigcup_{i=1}^d \mathrm{Ker}(\Pi_i \otimes K)$. If there is a matrix $\Gamma = (\gamma_{i,j})$, such that $\Gamma T \Gamma^{-1} = T^\alpha$ and $\Gamma E_1 = \zeta_m^\epsilon E_1$, then this matrix Γ is unique.*

Proof. We will use the idea leading to equation (14) replacing S with Γ. We will compute recursively and uniquely the entries $\gamma_{\mu,i}$, arriving at the explicit formula of eq. (21).

Observe that trivially $\gamma_{\nu,1}=0$ for all $\nu<1$ since we only allow $1\leq \nu\leq d$. We compute

(16)
$$\begin{aligned}\tilde{\gamma}_{\mu,i} &= \gamma_{\mu,i-1}(\lambda_\mu^\alpha-\lambda_{i-1})+\sum_{\nu=1}^{\mu-1}\gamma_{\nu,i-1}t^{(\alpha)}_{\mu,\nu}\\ &= \gamma_{\mu,i-1}(\lambda_\mu^\alpha-\lambda_{i-1})+\sum_{\nu=1}^{\mu-1}\gamma_{\nu,i-1}A(\nu,\mu-\nu-1)L\big(\alpha-(\mu-\nu),\nu,\mu-\nu\big)\\ &= \gamma_{\mu,i-1}(\lambda_\mu^\alpha-\lambda_{i-1})+\sum_{\nu=1}^{\mu-1}\gamma_{\nu,i-1}a_\nu a_{\nu+1}\cdots a_{\mu-1}h_{\alpha-\mu+\nu}(\lambda_\nu,\lambda_{\nu+1},\ldots,\lambda_\mu).\end{aligned}$$

Define

$$[\lambda_m^\alpha-\lambda_x]_i^j=\prod_{x=i}^{j}(\lambda_\mu^\alpha-\lambda_x)$$
$$[a]_i^j=\prod_{x=i}^{j}a_x$$

for $i\leq j$. If $i>j$ then both of the above quantities are defined to be equal to 1.

Observe that for $\mu=1$ eq. (16) becomes

$$\gamma_{1,i}=\frac{1}{a_{i-1}}\gamma_{1,i-1}(\lambda_1^\alpha-\lambda_{i-1}) \tag{17}$$

and we arrive at (assuming that $\Gamma(E_1)=\zeta_m^\epsilon E_1$)

$$\gamma_{1,i}=\frac{\zeta_m^\epsilon}{a_1a_2\cdots a_{i-1}}\prod_{x=1}^{i-1}(\lambda_1^\alpha-\lambda_x)=\frac{\zeta_m^\epsilon}{a_1a_2\cdots a_{i-1}}[\lambda_1^\alpha-\lambda_x]_1^{i-1}. \tag{18}$$

For $\mu\geq 2$ we have $\gamma_{\mu,1}=0$, since by assumption $\Gamma E_1=\zeta_m^\epsilon E_1$. Therefore eq. (16) gives us

$$\begin{aligned}\gamma_{\mu,i} &= \sum_{\kappa_1=0}^{i-2}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-\kappa_1}^{i-1}}{[a]_{i-1-\kappa_1}^{i-1}}\sum_{\mu_2=1}^{\mu-1}\gamma_{\mu_2,i-1-\kappa_1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\\ &= \sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\sum_{\kappa_1=0}^{i-2}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-\kappa_1}^{i-1}}{[a]_{i-1-\kappa_1}^{i-1}}\gamma_{\mu_2,i-1-\kappa_1}.\end{aligned} \tag{19}$$

We will now prove eq. (19) by induction on i, using equation (16). For $i=2,\mu\geq 2$

$$\begin{aligned}\gamma_{\mu,2} &= \frac{1}{a_1}\gamma_{\mu,1}(\lambda_\mu^\alpha-\lambda_1)+\frac{1}{a_1}\sum_{\mu_2=1}^{\mu-1}\gamma_{\mu_2,1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\\ &= \frac{1}{a_1}[a]_1^{\mu-1}h_{\alpha-\mu+1}(\lambda_1,\ldots,\lambda_\mu)\gamma_{1,1}.\end{aligned}$$

Assume now that eq. (19) holds for computing $\gamma_{\mu,i-1}$. We will treat the $\gamma_{\mu,i}$ case. Using eq. (16)

$$\begin{aligned}
\gamma_{\mu,i} &= \frac{(\lambda_\mu^\alpha - \lambda_{i-1})}{a_{i-1}}\gamma_{\mu,i-1} + \frac{1}{a_{i-1}}\sum_{\mu_2=1}^{\mu-1}\gamma_{\mu_2,i-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\\
&= \frac{(\lambda_\mu^\alpha - \lambda_{i-1})}{a_{i-1}}\sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\sum_{\kappa_1=0}^{i-3}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-1-\kappa_1}^{i-2}}{[a]_{i-2-\kappa_1}^{i-2}}\gamma_{\mu_2,i-2-\kappa_1}\\
&+ \frac{1}{a_{i-1}}\sum_{\mu_2=1}^{\mu-1}\gamma_{\mu_2,i-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\\
&= \sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\sum_{\kappa_1=0}^{i-3}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-1-\kappa_1}^{i-1}}{[a]_{i-2-\kappa_1}^{i-1}}\gamma_{\mu_2,i-2-\kappa_1}\\
&+ \frac{1}{a_{i-1}}\sum_{\mu_2=1}^{\mu-1}\gamma_{\mu_2,i-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\\
&= \sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\sum_{\kappa_1=1}^{i-2}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-\kappa_1}^{i-1}}{[a]_{i-1-\kappa_1}^{i-1}}\gamma_{\mu_2,i-1-\kappa_1}\\
&+ \sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\frac{1}{a_{i-1}}\gamma_{\mu_2,i-1}\\
&= \sum_{\mu_2=1}^{\mu-1}[a]_{\mu_2}^{\mu-1}h_{\alpha-\mu+\mu_2}(\lambda_{\mu_2},\ldots,\lambda_\mu)\sum_{\kappa_1=0}^{i-2}\frac{[\lambda_\mu^\alpha-\lambda_x]_{i-\kappa_1}^{i-1}}{[a]_{i-1-\kappa_1}^{i-1}}\gamma_{\mu_2,i-1-\kappa_1}
\end{aligned}$$

and equation (19) is now proved.

We proceed recursively applying eq. (19) to each of the summands $\gamma_{\mu_2,i-1-\kappa_1}$ if $\mu_2 > 1$ and $i-1-\kappa_1 > 1$. If $\mu_2 = 1$, then $\gamma_{\mu_2,i-1-\kappa_1}$ is computed by eq. (17) and if $\mu_2 > 1$ and $i-1-\kappa_1 \le 1$ then $\gamma_{\mu_2,i-1-\kappa_1} = 0$. We can classify all iterations needed by the set Σ_μ of sequences $(\mu_s,\mu_{s-1},\ldots,\mu_3,\mu_2)$ such that

$$1 = \mu_s < \mu_{s-1} < \cdots < \mu_3 < \mu_2 < \mu = \mu_1. \tag{20}$$

For example for $\mu = 5$ the set of such sequences is given by

$$\Sigma_\mu = \{(1),(1,2),(1,3),(1,2,3),(1,4),(1,2,4),(1,3,4),(1,2,3,4)\}$$

corresponding to the tree of iterations given in figure 1. The length of the sequence $(\mu_s,\mu_{s-1},\ldots,\mu_2)$ is given in eq. (20) is $s-1$. In each iteration in the sum of eq. (19) the i changes to $i-1-k$ thus we have the following sequence of indices

$$i_1 = i \to i_2 = i-1-\kappa_1 \to i_3 = i-2-(\kappa_1+\kappa_2) \to \cdots \to i_s = i-(s-1)-(\kappa_1+\cdots+\kappa_{s-1})$$

For the sequence $i_1, i_2, \ldots,$ we might have $i_t = 1$ for $t < s-1$. But in this case, we will arrive at the element $\gamma_{\mu_t,i_t} = \gamma_{\mu_t,1} = 0$ since $\mu_t > 1$. This means that we will have to consider only selections $\kappa_1,\ldots,\kappa_{s-1}$ such that $i_{s-1} \ge 1$. Therefore we

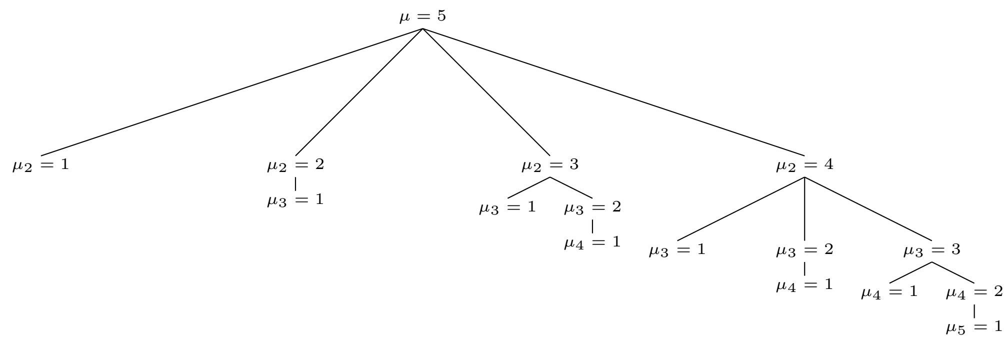

FIGURE 1. Iteration tree for $\mu = 5$

arrive at the following expression for $\mu \geq 2$

$$\begin{aligned}
\gamma_{\mu,i} = & \sum_{(\mu_s,\ldots,\mu_2)\in\Sigma_\mu} [a]_{\mu_2}^{\mu-1}[a]_{\mu_3}^{\mu_2-1}\cdots[a]_{\mu_s}^{\mu_{s-1}-1}\prod_{\nu=2}^{s} h_{\alpha-\mu_{\nu-1}+\mu_\nu}(\lambda_{\mu_\nu},\ldots,\lambda_{\mu_{\nu-1}}) \\
& \cdot \sum_{i=i_1>i_2>\cdots>i_s\geq 1}\prod_{\nu=1}^{s-1}\frac{[\lambda_{\mu_\nu}^{\alpha}-\lambda_x]_{i_{\nu+1}+1}^{i_\nu-1}}{[a]_{i_{\nu+1}}^{i_\nu-1}}\cdot\gamma_{1,i_s} \\
& \overset{(19)}{=} \sum_{(\mu_s,\ldots,\mu_2)\in\Sigma_\mu}\prod_{\nu=2}^{s} h_{\alpha-\mu_{\nu-1}+\mu_\nu}(\lambda_{\mu_\nu},\ldots,\lambda_{\mu_{\nu-1}}) \\
& \cdot \sum_{i=i_1>i_2>\cdots>i_s\geq 1}\frac{[a]_1^{\mu-1}}{[a]_{i_s}^{i-1}}\prod_{\nu=1}^{s-1}[\lambda_{\mu_\nu}^{\alpha}-\lambda_x]_{i_{\nu+1}+1}^{i_\nu-1}\frac{\zeta_m^{\epsilon}[\lambda_1^{\alpha}-\lambda_x]_1^{i_s-1}}{[a]_1^{i_s-1}} \\
& = \sum_{(\mu_s,\ldots,\mu_2)\in\Sigma_\mu}\prod_{\nu=2}^{s} h_{\alpha-\mu_{\nu-1}+\mu_\nu}(\lambda_{\mu_\nu},\ldots,\lambda_{\mu_{\nu-1}})\frac{[a]_1^{\mu-1}}{[a]_1^{i-1}}\zeta_m^{\epsilon}\sum_{i=i_1>i_2>\cdots>i_s\geq 1}\prod_{\nu=1}^{s}[\lambda_{\mu_\nu}^{\alpha}-\lambda_x]_{i_{\nu+1}+1}^{i_\nu-1}
\end{aligned} \tag{21}$$

where $i_{s+1}+1=1$ that is $i_{s+1}=0$. Since $\gamma_{\mu,i}$ are uniquelly determined the uniquenss of Γ follows. □

We will now prove that the matrix Γ of lemma 26 exists by cheking that $\Gamma T = T^{\alpha}\Gamma$. Set $(a_{\mu,i}) = \Gamma T$, $(b_{\mu,i}) = T^{\alpha}\Gamma$. For $i < d$ we have

$$\begin{aligned}
a_{\mu,i} &= \sum_{\nu=1}^{d}\gamma_{\mu,\nu}t_{\nu,i} = \gamma_{\mu,i}t_{ii} + \gamma_{\mu,i+1}t_{i+1,i} \\
&\overset{(16)}{=} \gamma_{\mu,i}\lambda_i + \gamma_{\mu,i}(\lambda_\mu^{\alpha}-\lambda_i) + \sum_{\nu=1}^{\mu-1}\gamma_{\nu,i}t_{\mu,\nu}^{(\alpha)} \\
&= \gamma_{\mu,i}\lambda_\mu^{\alpha} + \sum_{\nu=1}^{\mu-1}\gamma_{\nu,i}t_{\mu,\nu}^{(\alpha)} = \sum_{\nu=1}^{\mu}t_{\mu,\nu}^{(\alpha)}\gamma_{\nu,i} = b_{\mu,i}.
\end{aligned}$$

For $i = d$ we have:

$$a_{\mu,d} = \sum_{\nu=1}^{d} \gamma_{\mu,\nu} t_{\nu,d} = \gamma_{\mu,d} t_{d,d} = \gamma_{\mu,d}\lambda_d$$

while, recall lemma 22,

$$b_{\mu,d} = \sum_{\nu=1}^{d} t^{(\alpha)}_{\mu,\nu}\gamma_{\nu,d} = \sum_{\nu=1}^{\mu-1} t^{(\alpha)}_{\mu,\nu}\gamma_{\nu,d} + \lambda^{\alpha}_{\mu}\gamma_{\mu,d}.$$

This gives us the relation

$$(\lambda_d - \lambda^{\alpha}_{\mu})\gamma_{\mu,d} = \sum_{\nu=1}^{\mu-1} t^{(\alpha)}_{\mu,\nu}\gamma_{\nu,d} \tag{22}$$

For $\mu = 1$ using eq. (18) we have

$$\gamma_{1,d}\lambda_d = \gamma_{1,d}\lambda^{\alpha}_1 \Rightarrow [\lambda^{\alpha}_1 - \lambda_x]^d_1 = 0.$$

This relation is satisfied if λ^{α}_1 is one of $\{\lambda_1, \ldots, \lambda_d\}$. Without loss of generality we assume that

$$\lambda^{\alpha}_i = \begin{cases} \lambda_{i+1} & \text{if } m \nmid i \\ \lambda_{i-m+1} & \text{if } m \mid i \end{cases} \tag{23}$$

We have the following conditions:

$$\begin{array}{rl}
\mu = 2 & (\lambda_d - \lambda^{\alpha}_2)\gamma_{2,d} = t^{(\alpha)}_{2,1}\gamma_{1,d} \\
\mu = 3 & (\lambda_d - \lambda^{\alpha}_3)\gamma_{3,d} = t^{(\alpha)}_{3,1}\gamma_{1,d} + t^{(\alpha)}_{3,2}\gamma_{2,d} \\
\mu = 4 & (\lambda_d - \lambda^{\alpha}_4)\gamma_{4,d} = t^{(\alpha)}_{4,1}\gamma_{1,d} + t^{(\alpha)}_{4,2}\gamma_{2,d} + t^{(\alpha)}_{4,3}\gamma_{3,d} \\
\vdots & \vdots \\
\mu = d-1 & (\lambda_d - \lambda^{\alpha}_{d-1})\gamma_{d-1,d} = t^{(\alpha)}_{d-1,1}\gamma_{1,d} + t^{(\alpha)}_{d-1,2}\gamma_{2,d} + \cdots + t^{(\alpha)}_{d-1,d-2}\gamma_{d-1,d}.
\end{array}$$

All these equations are true provided that

$$\gamma_{1,d}, \ldots, \gamma_{d-2,d} = 0. \tag{24}$$

Finally, for $\mu = d$, we have

$$(\lambda_d - \lambda^{\alpha}_d)\gamma_{d,d} = \sum_{\nu=1}^{d-1} t^{(\alpha)}_{d,\nu}\gamma_{\nu,d}, \tag{25}$$

which is true provided that $(\lambda_d - \lambda^{\alpha}_d)\gamma_{d,d} = t^{(a)}_{d,d-1}\gamma_{d-1,d}$. In lemma 29 we will prove that eq. (24) holds and eq. (25) will be proved in lemma 34.

Lemma 27. *For $n \geq 2$ the vertical sum S_n of the products of every line of the following array*

$$
\begin{array}{c|cccccc}
y & & & & & & \\
\hline
1 & 1 & (x_1-x_2) & (x_1-x_3) & \cdots & \cdots & (x_1-x_n) \\
2 & (z-x_1) & 1 & (x_1-x_3) & \cdots & \cdots & (x_1-x_n) \\
3 & (z-x_1) & (z-x_2) & 1 & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \vdots \\
\vdots & \vdots & & & \ddots & & \vdots \\
n-1 & (z-x_1) & (z-x_2) & \cdots & (z-x_{n-2}) & 1 & (x_1-x_n) \\
n & (z-x_1) & (z-x_2) & \cdots & (z-x_{n-2}) & (z-x_{n-1}) & 1
\end{array}
$$

is given by

$$S_n = \sum_{y=1}^{n} \prod_{\nu=y+1}^{n} (x_1 - x_\nu) \prod_{\mu=1}^{y-1} (z - x_\mu) = (z - x_2) \cdots (z - x_n).$$

In particular when $z = x_n$ the sum is zero.

Proof. We will prove the lemma by induction. For $n = 2$ we have $S_2 = (x_1 - x_2) + (z - x_1) = z - x_2$. Assume that the equality holds for n. The sum S_{n+1} corresponds to the array:

$$
\begin{array}{c|cccccc}
y & & & & & & \\
\hline
1 & 1 & (x_1-x_2) & (x_1-x_3) & \cdots & (x_1-x_n) & (x_1-x_{n+1}) \\
2 & (z-x_1) & 1 & (x_1-x_3) & \cdots & (x_1-x_n) & (x_1-x_{n+1}) \\
3 & (z-x_1) & (z-x_2) & 1 & \ddots & \vdots & \vdots \\
\vdots & \vdots & & \ddots & \ddots & \vdots & \vdots \\
n-1 & (z-x_1) & \cdots & (z-x_{n-2}) & 1 & (x_1-x_n) & (x_1-x_{n+1}) \\
n & (z-x_1) & (z-x_2) & \cdots & (z-x_{n-1}) & 1 & (x_1-x_{n+1}) \\
n+1 & (z-x_1) & (z-x_2) & \cdots & (z-x_{n-1}) & (z-x_n) & 1
\end{array}
$$

We have by definition $S_{n+1} = S_n(x_1 - x_{n+1}) + (z - x_1)(z - x_2) \cdots (z - x_n)$, which by induction gives

$$
\begin{aligned}
S_{n+1} &= (z - x_2) \cdots (z - x_n)(x_1 - x_{n+1}) + (z - x_1)(z - x_2) \cdots (z - x_n) \\
&= (z - x_2) \cdots (z - x_n)(x_1 - x_{n+1} + z - x_1)
\end{aligned}
$$

and gives the desired result. $\square$

Lemma 28. *Consider $A < l < L < B$. The quantity*

$$\sum_{l \leq y \leq L} [\lambda_a - \lambda_x]_A^{y-1} \cdot [\lambda_b - \lambda_x]_{y+1}^{B}$$

is equal to

$$[\lambda_a - \lambda_x]_A^{l-1} \cdot [\lambda_b - \lambda_x]_{L+1}^{B} \cdot \frac{[\lambda_a - \lambda_x]_l^L - [\lambda_b - \lambda_x]_l^L}{(\lambda_a - \lambda_b)}.$$

Proof. We write

$$\sum_{l \leq y \leq L} [\lambda_a - \lambda_x]_A^{y-1} \cdot [\lambda_b - \lambda_x]_{y+1}^{B}$$

$$= [\lambda_a - \lambda_x]_A^{l-1} \cdot [\lambda_b - \lambda_x]_{L+1}^B \cdot \sum_{l \le y \le L} [\lambda_a - \lambda_x]_l^{y-1} \cdot [\lambda_b - \lambda_x]_{y+1}^L$$

The last sum can be read as the vertical sum S of the products of every line in the following array:

$$\begin{array}{c|cccccc}
y & & & & & & \\
\hline
l & 1 & (\lambda_b - \lambda_{l+1}) & (\lambda_b - \lambda_{l+2}) & \cdots & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
l+1 & (\lambda_a - \lambda_l) & 1 & (\lambda_b - \lambda_{l+2}) & \cdots & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
l+2 & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & 1 & & \vdots & \vdots \\
\vdots & \vdots & \vdots & & & \vdots & \vdots \\
L-2 & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & 1 & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
L-1 & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & (\lambda_a - \lambda_{L-2}) & 1 & (\lambda_b - \lambda_L) \\
L & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & (\lambda_a - \lambda_{L-2}) & (\lambda_a - \lambda_{L-1}) & 1
\end{array}$$

If $l = b$, then lemma 27 implies that $S = [\lambda_a - \lambda_x]_{b+1}^L$. Furthermore, if $L = a$ then $S = 0$.

The quantity S cannot be directly computed using lemma 27, if $l \neq b$. We proceed by forming the array:

$$\begin{array}{c|ccc|cccccc}
y & & & & & & & & & \\
\hline
b & 1 & (\lambda_b - \lambda_{b+1}) & \cdots & (\lambda_b - \lambda_l) & \cdots & \cdots & \cdots & \cdots & (\lambda_b - \lambda_L) \\
\vdots & & & & \vdots & & & & & \vdots \\
l-1 & (\lambda_a - \lambda_b) & \cdots & 1 & (\lambda_b - \lambda_l) & \cdots & \cdots & \cdots & \cdots & (\lambda_b - \lambda_L) \\
\hline
l & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & 1 & (\lambda_b - \lambda_{l+1}) & (\lambda_b - \lambda_{l+2}) & \cdots & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
l+1 & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & (\lambda_a - \lambda_l) & 1 & (\lambda_b - \lambda_{l+2}) & \cdots & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
l+2 & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & 1 & & \vdots & \vdots \\
\vdots & & & & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
L-2 & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & 1 & (\lambda_b - \lambda_{L-1}) & (\lambda_b - \lambda_L) \\
L-1 & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & (\lambda_a - \lambda_{L-2}) & 1 & (\lambda_b - \lambda_L) \\
L & (\lambda_a - \lambda_b) & \cdots & (\lambda_a - \lambda_{l-1}) & (\lambda_a - \lambda_l) & (\lambda_a - \lambda_{l+1}) & \cdots & (\lambda_a - \lambda_{L-2}) & (\lambda_a - \lambda_{L-1}) & 1
\end{array}$$

The value of this array is computed using lemma 27 to be equal to $[\lambda_a - \lambda_x]_{b+1}^L$. We observe that the sum of the products of the top left array can be computed using lemma 27, while the sum of the products of the lower right array is S.

$$[\lambda_a - \lambda_x]_b^{l-1} \cdot S + [\lambda_a - \lambda_x]_{b+1}^{l-1} \cdot [\lambda_b - \lambda_x]_l^L = [\lambda_a - \lambda_x]_{b+1}^L$$

we arrive at

$$[\lambda_a - \lambda_x]_b^{l-1} S = [\lambda_a - \lambda_x]_{b+1}^{l-1} \left([\lambda_a - \lambda_x]_l^L - [\lambda_b - \lambda_x]_l^L \right)$$

or equivalently

$$(\lambda_a - \lambda_b) \cdot S = [\lambda_a - \lambda_x]_l^L - [\lambda_b - \lambda_x]_l^L.$$

□

Lemma 29. *For all $1 \le \mu \le d - 2$ we have $\gamma_{\mu,d} = 0$.*

Proof. Let $\mu_1 = \mu > \mu_2 > \cdots > \mu_s = 1 \in \Sigma_\mu$ be a selection of iterations and $d = i_1 > i_2 > \cdots > i_s \ge 1 > i_{s+1} = 0$ be the sequence of i's. Using eq. (23) we see that the quantity $[\lambda^\alpha_{\mu_\nu} - \lambda_x]^{i_\nu -1}_{i_{\nu+1}+1} \neq 0$ if and only if one of the following two inequalities hold:

$$\text{either} \qquad i_{\nu+1} > \mu_\nu - m f(\mu_\nu) \tag{26}$$

$$\text{or} \qquad i_\nu < \mu_\nu + 2 - m f(\mu_\nu), \tag{27}$$

where

$$f(x) = \begin{cases} 1 & \text{if } m \mid x \\ 0 & \text{if } m \nmid x \end{cases}$$

We will denote the above two inequalities by $(26)_\nu$,$(27)_\nu$ when applied for the integer ν. Assume that for all $1 \leq \nu \leq s$ one of the two inequalities $(26)_\nu$,$(27)_\nu$ hold, that is $[\lambda^\alpha_{\mu_\nu} - \lambda_x]^{i_\nu -1}_{i_{\nu+1}+1} \neq 0$. Inequality $(26)_s$ can not hold for $\nu = s$ since it gives us $0 = i_{s+1} > 1 = \mu_s$, we have $m \nmid 1 = \mu_s$.

We will keep the sequence $\bar{\mu} : \mu_1 > \mu_2 > \cdots > \mu_s$ fixed and we will sum over all possible selections of sequences of $i_1 > \cdots i_s > i_{s+1} = 0$, that is we will show that the sum

$$\Gamma_{\bar{\mu},i} := \sum_{i=i_1 > i_2 > \cdots > i_s \geq 1} \prod_{\nu=1}^{s} [\lambda^\alpha_{\mu_\nu} - \lambda_x]^{i_\nu -1}_{i_{\nu+1}+1} \tag{28}$$

is zero, which will show that $\gamma_{\mu,d} = 0$ using eq. (21).

Observe now that if $(27)_\nu$ holds and $m \nmid \mu_\nu, \mu_{\nu-1}$, then $(27)_{\nu-1}$ also holds. Indeed the combination of $(27)_\nu$ and $(26)_{\nu-1}$ gives the impossible inequality

$$\mu_\nu + 2 \overset{(27)_\nu}{>} i_\nu \overset{(26)_{\nu-1}}{>} \mu_{\nu-1}.$$

Assume now that $m \mid \nu$ and $(27)_\nu$ holds, then $(27)_{\nu-1}$ also holds. Indeed the combination of $(27)_\nu$ and $(26)_{\nu-1}$ gives us

$$\mu_\nu + 2 - m \overset{(27)_\nu}{>} i_\nu \overset{(26)_{\nu-1}}{>} \mu_{\nu-1} - m f(\mu_{\nu-1}).$$

If $m \nmid \mu_{\nu-1}$, then the above inequality is impossible since it implies that

$$\mu_\nu + 2 - m > \mu_{\nu-1} > \mu_\nu.$$

If $m \mid \mu_{\nu-1}$, then the inequality is also impossible since it implies that $\mu_\nu + 2 > \mu_{\nu-1}$ so if we write $\mu_{\nu-1} = k'm$ and $\mu_\nu = km$, $k, k' \in \mathbb{N}$, $k' > k$, we arrive at $2 > (k' - k)m \geq m$. This proves the following

Lemma 30. *The inequality $(26)_{\nu-1}$ might be correct only in cases where $m \mid \mu_{\nu-1}$, $m \nmid \mu_\nu$.*

Assume that for all ν inequality (27) holds. Then for $\nu = 1$ it gives us (recall that $\mu \leq d - 2$)

$$\mu + 2 \leq d = i_1 < \mu_1 + 2 - m f(\mu_1) = \mu + 2 - m f(\mu), \tag{29}$$

which is impossible. Therefore either there are ν such that none of the two inequalities $(26)_\nu$, $(27)_\nu$ hold (in this case the contribution to the sum is zero) or there are cases where (26) holds.

The summands appearing in eq. (28) can be non-zero, for example the sequence $\mu_1 = m > \mu_2 = 1$ with $i_2 = 2 < i_1 = d$, $s = 2$ give the contribution

$$[\lambda^\alpha_{\mu_2} - \lambda_x]^{i_2 -1}_1 [\lambda^\alpha_{\mu_1} - \lambda_x]^{d-1}_{i_2} = [\lambda^\alpha_1 - \lambda_x]^1_1 [\lambda^\alpha_m - \lambda_x]^{d-1}_{i_2+1} = (\lambda_2 - \lambda_1)[\lambda_1 - \lambda_x]^{d-1}_3$$

while for $i_2 = 1 < i_1 = d$ it gives the contribution

$$[\lambda^\alpha_{\mu_2} - \lambda_x]_1^{i_2-1}[\lambda^\alpha_{\mu_1} - \lambda_x]_{i_2+1}^{d-1} = [\lambda^\alpha_1 - \lambda_x]_1^0[\lambda^\alpha_m - \lambda_x]_2^{d-1} = [\lambda_1 - \lambda_x]_2^{d-1}.$$

It is clear that these non-zero contributions cancel out when added.

Lemma 31. *Assume that $m \mid \mu_{\nu_0-1}$ and $m \nmid \mu_{\nu_0}$, where (27)$_{\nu_0}$ and (26)$_{\nu_0-1}$ hold. Then, we can eliminate μ_{ν_0-1} and i_{ν_0} from both selections of the sequence of μ's and i's, i.e. we can form the sequence of length $s-1$*

$$\bar{\mu}_{s-1} = \mu_s < \bar{\mu}_{s-2} = \mu_{s-1} < \cdots < \bar{\mu}_{\nu_0-1} = \mu_{\nu_0} < \bar{\mu}_{\nu_0-2} = \mu_{\nu_0-2} < \cdots < \bar{\mu}_1 = \mu_1.$$

and the corresponding sequence of equal length

$$\bar{i}_{s-1} = i_s < \bar{i}_{s-2} = i_{s-1} < \cdots < \bar{i}_{\nu_0} = i_{\nu_0+1} < \bar{i}_{\nu_0-1} = i_{\nu_0-1} < \cdots < \bar{i}_1 = i_1 = d,$$

so that

$$\Gamma_{\bar{\mu},i} = \sum_{i_1 > \cdots > i_s} \prod_{\nu=1}^{s} [\lambda^\alpha_{\mu_\nu} - \lambda_x]_{i_{\nu+1}+1}^{i_\nu - 1} = (\star) \sum_{\bar{i}_1 > \cdots > \bar{i}_{s-1}} \prod_{\substack{\nu=1 \\ \nu \neq \nu_0-1}}^{s} [\lambda^\alpha_{\mu_\nu} - \lambda_x]_{\bar{i}_{\nu+1}+1}^{\bar{i}_\nu - 1},$$

where $(\star)$ is a non zero element.

Proof. (of lemma 31) We are in the case $m \mid \mu_{\nu_0-1}$ and $m \nmid \mu_{\nu_0}$, where (27)$_{\nu_0}$ and (26)$_{\nu_0-1}$ hold,

$$\mu_{\nu_0-1} - m \overset{(26)_{\nu_0-1}}{<} i_{\nu_0} \overset{(27)_{\nu_0}}{<} \mu_{\nu_0} + 2, \tag{30}$$

or equivalently

$$\mu_0 := \mu_{\nu_0-1} - m + 1 \leq i_{\nu_0} \leq \mu_{\nu_0} + 1$$

For i_{ν_0+1} the inequality (26)$_{\nu_0}$ $i_{\nu_0+1} > \mu_{\nu_0} - mf(\mu_{\nu_0})$ can not hold, since it implies

$$i_{\nu_0+1} < i_{\nu_0} \overset{(27)_{\nu_0}}{<} \mu_{\nu_0} + 2 < i_{\nu_0+1} + 2.$$

Observe that also

$$i_{\nu_0+1} + 1 \leq i_{\nu_0} \leq i_{\nu_0-1} - 1.$$

Set $l = \max\{\mu_0, i_{\nu_0+1}+1\}$ and $L = \min\{\mu_{\nu_0}+1, i_{\nu_0-1}-1\}$. Then $y = i_{\nu_0}$ satisfies

$$l \leq y \leq L.$$

By lemma 28 the quantity

$$\sum_{l \leq y \leq L} [\lambda_{\mu_{\nu_0}+1} - \lambda_x]_{i_{\nu_0+1}+1}^{y-1} \cdot [\lambda_{\mu_0} - \lambda_x]_{y+1}^{i_{\nu_0-1}-1}$$

equals to

$$[\lambda_{\mu_{\nu_0}+1} - \lambda_x]_{i_{\nu_0+1}+1}^{l-1} \cdot [\lambda_{\mu_0} - \lambda_x]_{L+1}^{i_{\nu_0-1}-1} \cdot \frac{[\lambda_{\mu_{\nu_0}+1} - \lambda_x]_l^L - [\lambda_{\mu_0} - \lambda_x]_l^L}{(\lambda_{\mu_{\nu_0}+1} - \lambda_{\mu_0})}$$

$$\frac{[\lambda_{\mu_{\nu_0}+1} - \lambda_x]_{i_{\nu_0+1}+1}^{L} \cdot [\lambda_{\mu_0} - \lambda_x]_{L+1}^{i_{\nu_0-1}-1} - [\lambda_{\mu_{\nu_0}+1} - \lambda_x]_{i_{\nu_0+1}+1}^{l-1} \cdot [\lambda_{\mu_0} - \lambda_x]_{l}^{i_{\nu_0-1}-1}}{(\lambda_{\mu_{\nu_0}+1} - \lambda_{\mu_0})}. \tag{31}$$

Case A1 $l = \mu_0 \geq i_{\nu_0+1} + 1$. Then $[\lambda_{\mu_0} - \lambda_x]_l^L = 0$.
Case A2 $l = i_{\nu_0+1} + 1 > \mu_0$. We set $z := i_{\nu_0+1}$, which is bounded by eq. (27)$_{\nu_0+1}$ that is

$$\mu_0 \overset{\text{Case A2}}{\leq} z \overset{(27)_{\nu_0+1}}{\leq} \mu_{\nu_0+1} + 1.$$

Notice that in this case $m \nmid \mu_{\nu_0+1}$. If $m \mid \mu_{\nu_0+1}$, then since we have assumed that inequality $(27)_{\nu_0+1}$ holds we have

$$\mu_{\nu_0-1} - m = \mu_0 - 1 \overset{\text{(Case A2)}}{<} i_{\nu_0+1} \overset{(27)_{\nu_0+1}}{<} \mu_{\nu_0+1} + 2 - m,$$

which implies that $\mu_{\nu_0-1} < \mu_{\nu_0+1} + 2$, a contradiction. Thus for $l = z+1$ we compute

$$\sum_{\mu_0 \leq z \leq \mu_{\nu_0+1}+1} [\lambda^{\alpha}_{\mu_{\nu_0+1}} - \lambda_x]^{i_{\nu_0+1}-1}_{i_{\nu_0+2}+1} \cdot [\lambda_{\mu_0} - \lambda_x]^L_l =$$

$$= \sum_{\mu_0 \leq z \leq \mu_{\nu_0+1}+1} [\lambda_{\mu_{\nu_0+1}+1} - \lambda_x]^{z-1}_{i_{\nu_0+2}+1} \cdot [\lambda_{\mu_0} - \lambda_x]^L_{z+1} =$$

$$= (\star) \cdot \frac{[\lambda_{\mu_{\nu_0+1}+1} - \lambda_x]^{\mu_{\nu_0+1}+1}_{\mu_0} - [\lambda_{\mu_0} - \lambda_x]^{\mu_{\nu_0+1}+1}_{\mu_0}}{\lambda_{\mu_{\nu_0+1}+1} - \lambda_{\mu_0+1}} = 0.$$

Case B1 $L = \mu_{\nu_0} + 1 \leq i_{\nu_0-1} - 1$. In this case $[\lambda_{\mu_{\nu_0}+1} - \lambda_x]^L_l = 0$.
Case B2 $L = i_{\nu_0-1} - 1 < \mu_{\nu_0} + 1$. In this case eq. (31) is reduced to

$$\frac{[\lambda_{\mu_{\nu_0}+1} - \lambda_x]^{i_{\nu_0-1}-1}_{i_{\nu_0+1}+1}}{(\lambda_{\mu_{\nu_0}+1} - \lambda_{\mu_0})}$$

This means that we have erased the μ_{ν_0-1} from the product and we have

$$\sum_{i_1 > \cdots > i_s} \prod_{\nu=1}^{s} [\lambda^{\alpha}_{\mu_\nu} - \lambda_x]^{i_\nu - 1}_{i_{\nu+1}+1} = (\star) \sum_{i_1 > \cdots > i_s} \prod_{\substack{\nu=1 \\ \nu \neq \nu_0 - 1}}^{s} [\lambda^{\alpha}_{\mu_\nu} - \lambda_x]^{i_\nu - 1}_{i_{\nu+1}+1},$$

where $(\star)$ is a non zero element. This procedure gives us that the original quantity

$$[\lambda^{\alpha}_{\mu_{\nu_0}} - \lambda_x]^{i_{\nu_0}-1}_{i_{\nu_0+1}+1} \cdot [\lambda^{\alpha}_{\mu_{\nu_0-1}} - \lambda_x]^{i_{\nu_0-1}-1}_{i_{\nu_0}+1}$$

after summing over i_{ν_0} becomes the quantity

$$[\lambda^{\alpha}_{\mu_{\nu_0}} - \lambda_x]^{i_{\nu_0-1}-1}_{i_{\nu_0+1}+1} = [\lambda^{\alpha}_{\bar{\mu}_{\nu_0-1}} - \lambda_x]^{\bar{i}_{\nu_0-1}-1}_{\bar{i}_{\nu_0}+1},$$

that is we have eliminated the μ_{ν_0-1} and i_{ν_0} from both selections of the sequence of μ's and i's, i.e. we have the sequence of length $s-1$

$$\bar{\mu}_{s-1} = \mu_s < \bar{\mu}_{s-2} = \mu_{s-1} < \cdots < \bar{\mu}_{\nu_0-1} = \mu_{\nu_0} < \bar{\mu}_{\nu_0-2} = \mu_{\nu_0-2} < \cdots < \bar{\mu}_1 = \mu_1.$$

and the corresponding sequence of equal length

$$\bar{i}_{s-1} = i_s < \bar{i}_{s-2} = i_{s-1} < \cdots < \bar{i}_{\nu_0} = i_{\nu_0+1} < \bar{i}_{\nu_0-1} = i_{\nu_0-1} < \cdots < \bar{i}_1 = i_1 = d,$$

□

Remark 32. One should be careful here since $\bar{i}_{\nu_0-1} = i_{\nu_0-1} > i_{\nu_0} > \bar{i}_{\nu_0} = i_{\nu_0+1}$, so $\bar{i}_{\nu_0-1} > \bar{i}_{\nu_0} + 1$. This means that the new sequence of $\bar{i}_{s-1} > \cdots > \bar{i}_1$ satisfies a stronger inequality in the ν_0 position, unless $\nu_0 - 1 = d$ in the computation of $\gamma_{d,d}$.

Consider the set $s, s-1, \ldots, \nu_0$ such that $m \nmid \mu_\nu$ for $s \geq \nu \geq \nu_0$ and assume that $m \mid \mu_{\nu_0-1}$ and $(27)_{\nu_0}$ and $(26)_{\nu_0-1}$ hold. We apply lemma 31 and we obtain a new sequence of μ's with μ_{ν_0-1} removed, provided that $\nu_0 - 1 > 1$. We continue this way and in the sequence of μ's we eliminate all possible inequalities like (30) obtaining a series of μ which involves only inequalities of type (27). But this is not possible if $\mu \leq d-2$, according to equation (29). This proves that all $\gamma_{\mu,d} = 0$ for $1 \leq \mu \leq d-2$, and completes the proof of lemma 29. □

Lemma 33. *If $\mu_2 \neq d-1$, then the contribution of the corresponding summand $\Gamma_{\bar{\mu},i}$ to $\gamma_{d,d}$ is zero.*

Proof. We are in the case $\mu = d = i$. We begin the procedure of eliminating all sequences of inequalities of the form $(23)_{\nu_0}, (22)_{\nu_0-1}$, where $m \mid \nu_0 - 1$, $m \nmid \nu_0$, using lemma 31. For $\nu = 1$ inequality $(27)_1$ can not hold since it implies the impossible inequality $d = i_1 < d + 2 - m$. Therefore, $(26)_1$ holds, that is $i_2 > d - m$. On the other hand we can assume that $(27)_2$ holds by the elimination process, so we have

$$d - m \overset{(26)_1}{<} i_2 \overset{(27)_2}{<} \mu_2 + 2.$$

Following the analysis of the proof of lemma 29 we see that the contribution to $\gamma_{d,d}$ is non zero if case B2 holds, that is ($\nu_0 = 2$ in this case) $d - 1 = i_{\nu_0-1} - 1 < \mu_2 + 1$, obtaining that $\mu_2 = d - 1$. ☐

Lemma 34. *Equation (25) holds, that is*

$$(\lambda_d - \lambda_d^\alpha)\gamma_{d,d} = \sum_{\nu=1}^{d-1} t_{d,\nu}^{(\alpha)} \gamma_{\nu,d} = t_{d,d-1}^{(\alpha)} \gamma_{d-1,d}.$$

Proof. We will use the procedure of the proof of lemma 31. We recall that for each fixed sequence of $\mu_s > \cdots > \mu_1$ we summed over all possible sequences $i_1 > \cdots > i_{s+1} = 0$. In the final step the inequality (30) appears, for $\nu_0 = 2$, and $\mu_{\nu_0} = \mu_2 = d - 1$ and $\nu_0 - 1 = 1$ and $\mu_{\nu_0-1} = \mu = d$, that is:

$$0 = \mu_{\nu_0-1} - m \overset{(26)_2}{<} i_{\nu_0} \overset{(27)_1}{<} \mu_{\nu_0} + 2 = d + 1.$$

As in the proof of lemma 31 we sum over $y = i_\nu$ and the result is either zero in case B1 or in the B2 case, where $\mu_{\nu_0} = \mu_2 = d - 1$ and $\mu_0 = \mu_{\nu_0-1} - m + 1 = d - m + 1$, the contribution is computed to be equal to

$$\frac{[\lambda^\alpha_{\mu_{\nu_0}+1} - \lambda_x]_{i_{\nu_0+1}+1}^{i_{\nu_0-1}-1}}{(\lambda_{\mu_{\nu_0}+1} - \lambda_{\mu_0})} = \frac{[\lambda_d^\alpha - \lambda_x]_{i_3+1}^{d-1}}{\lambda_d - \lambda_d^\alpha}.$$

The last $\mu_{\nu_0-1} = \mu_1 = d$ is eliminated in the above expression. This means that for a fixed sequence $\mu_1 > \ldots > \mu_s$ the contribution of the inner sum in eq. (28) is given by

$$\frac{1}{\lambda_d - \lambda_d^\alpha} \cdot \sum_{d-1=i_2>i_3>\cdots>i_s\geq 1} \prod_{\nu=2}^{s} [\lambda^\alpha_{\mu_\nu} - \lambda_x]_{i_{\nu+1}+1}^{i_\nu - 1}.$$

Observe that $\mu_1 = d$ does not appear in this expression and this expression corresponds to the sequence $\bar{\mu}_1 = \mu_2 = d - 1 > \bar{\mu}_2 = \mu_3 > \cdots > \bar{\mu}_{s-1} = \bar{\mu}_s = 1$. Notice, also that the problem described in remark 32 does not appear here, since we erased i_1 which is not between some i's but the first one. Therefore, we can relate it to a similar expression that contributes to $\gamma_{d-1,d}$. Conversely every contribution of $\gamma_{d-1,d}$ gives rise to a contribution in $\gamma_{d,d}$, by multiplying by $\lambda_d - \lambda_d^\alpha$. The desired result follows by the expression of $\gamma_{\mu,d}$ given in eq. (21). ☐

We have shown so far how to construct matrices Γ, T so that

$$T^q = 1, \Gamma T \Gamma^{-1} = T^\alpha. \tag{32}$$

We will now prove that Γ has order m. By equation (32) Γ^k should satisfy the equation

$$\Gamma^k T \Gamma^{-k} = T^{\alpha^k}.$$

Using proposition 26 asserting the uniqueness of such Γ^k with α replaced by α^k we have that the matrix multiplication of the entries of Γ giving rise to $(\gamma_{\mu,i}^{(k)}) = \Gamma^k$ coincide to the values by the recursive method of proposition 26 applied for $\Gamma' = \Gamma^k$, $\alpha' = \alpha^k$ and $\Gamma' E_1 = \zeta_m^{\epsilon k} E_1$. In particular for $k = m$, we have $\alpha^m \equiv 1 \operatorname{mod} p^\nu$ for all $1 \leq \nu \leq h$, that is the matrix Γ^k should be recursively constructed using proposition 26 for the relation $\Gamma^m T \Gamma^m = T$, $\Gamma^m E_1 = E_1$, leading to the conclusion $\Gamma^m = \mathrm{Id}$. Notice that the first eigenvalue of Γ is a primitive root of unity, therefore Γ has order exactly m.

By lemma 10 the action of σ in the special fibre is given by a lower triangular matrix. Therefore, we must have

$$\gamma_{\nu,i} \in \mathfrak{m}_R \text{ for } \nu < i. \tag{33}$$

Proposition 35. *If*

$$v(\lambda_i - \lambda_j) > v(a_\nu) \textit{ for all } 1 \leq i, j \leq d \textit{ and } 1 \leq \nu \leq d-1, \tag{34}$$

then the matrix $(\gamma_{\mu,i})$ has entries in the ring R and is lower triangular modulo $\mathfrak{m}_R$.

Proof. Assume that the condition of eq. (34) holds. In equation (21) we compute the fraction

$$\frac{[a]_1^{\mu-1}}{[a]_1^{i-1}} = \begin{cases} \frac{1}{[a]_\mu^{i-1}} & \text{if } i > \mu \\ 1 & \text{if } i = \mu \\ [a]_i^{\mu-1} & \text{if } i < \mu \end{cases} \tag{35}$$

The number of $(\lambda_\mu^\alpha - \lambda_x)$ factors in the numerator is equal to (recall that $i_{s+1} = 0$)

$$\sum_{\nu=1}^{s} (i_\nu - 1 - i_{\nu+1} - 1 + 1) = i - s,$$

and $i > \mu \geq s$, so $i - s > 0$. Therefore, for the upper part of the matrix $i > \mu$ we have $i - s$ factors of the form $(\lambda_i^\alpha - \lambda_j)$ in the numerator and $i - \mu$ factors a_x in the denominator. Their difference is equal to $(i - s) - (i - \mu) = \mu - s \geq 0$. By assumption the matrix reduces to an upper triangular matrix modulo $\mathfrak{m}_R$. ☐

Remark 36. The condition given in equation (34) can be satisfied in the following way: It is clear that $\lambda_i - \lambda_j \in \mathfrak{m}_R$. Even in the case $v_{\mathfrak{m}_R}(\lambda_i - \lambda_j) = 1$ we can consider a ramified extension R' of the ring R with ramification index e, in order to make the valuation $v_{\mathfrak{m}_{R'}}(\lambda_i - \lambda_j) = e$ and then there is space to select $v_{\mathfrak{m}_{R'}}(a_i) < v_{\mathfrak{m}_{R'}}(\lambda_i - \lambda_j)$.

Proposition 37. *We have that*

$$\gamma_{i,i} \equiv \zeta_m^\epsilon \alpha^{i-1} \operatorname{mod} \mathfrak{m}_R \tag{36}$$

Let $A = \{a_1, \ldots, a_{d-1}\} \in R$ be the set of elements below the diagonal in eq. (11). If $a_i \in \mathfrak{m}_R$, then

$$\gamma_{\mu,i} \in \mathfrak{m}_R \textit{ for } \mu \neq i,$$

that is E_i is an eigenvector for the reduced action of Γ modulo $\mathfrak{m}_R$. If $a_{\kappa_1}, \ldots, a_{\kappa_r}$ are the elements of the set A which are in $\mathfrak{m}_R$, then the reduced matrix of Γ has *the form:*

$$\begin{pmatrix} \Gamma_1 & 0 & \cdots & 0 \\ 0 & \Gamma_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \Gamma_r \end{pmatrix}$$

where $\Gamma_1, \Gamma_2, \ldots, \Gamma_{r+1}$ *for* $1 \leq \nu \leq r+1$ *are* $(\kappa_\nu - \kappa_{\nu-1}) \times (\kappa_\nu - \kappa_{\nu-1})$ *lower triangular matrices (we set* $\kappa_0 = 0, \kappa_{r+1} = d$*).*

Proof. Consider the matrix Γ:

$$\left(\begin{array}{cccc}
\boxed{\begin{matrix} \gamma_{11} & & \\ \vdots & \ddots & \\ \gamma_{\kappa_1,1} & \cdots & \gamma_{\kappa_1,\kappa_1} \end{matrix}} & & & 0 \\
\boxed{\begin{matrix} \gamma_{\mu,i} \\ 1 \leq i \leq \kappa_1 < m \leq d \end{matrix}} & \boxed{\begin{matrix} \gamma_{\kappa_1+1,\kappa_1+1} & & \\ \vdots & \ddots & \\ \gamma_{\kappa_2,\kappa_1+1} & \cdots & \gamma_{\kappa_2,\kappa_2} \end{matrix}} & & \\
 & \boxed{\begin{matrix} \gamma_{\mu,i} \\ \kappa_1 < i \leq \kappa_2 < \mu \leq d \end{matrix}} & \ddots & \\
 & & \cdots & \boxed{\begin{matrix} \gamma_{\kappa_r+1,\kappa_r+1} & & \\ \vdots & \ddots & \\ \gamma_{d,\kappa_r+1} & \cdots & \gamma_{d,d} \end{matrix}}
\end{array}\right)$$

We have that $\mu = i$ and the only element in Σ_μ which does not have any factor of the form $(\lambda_y^\alpha - \lambda_x)$ is the sequence

$$1 = \mu_s = \mu_{s-1} - 1 < \mu_{s-1} < \cdots < \mu_2 = \mu_1 - 1 < \mu_1 = \mu$$

For this sequence eq. (21) becomes

$$\gamma_{i,i} = \prod_{\nu=2}^{s} h_{\alpha-1}(\lambda_{\mu_\nu}, \lambda_{\mu_{\nu-1}}) \zeta_m^\epsilon \operatorname{mod} \mathfrak{m}_R,$$

which gives the desired result since $h_{\alpha-1}(\lambda_{\mu_\nu}, \lambda_{\mu_{\nu-1}}) \equiv \binom{\alpha}{1} = \alpha \operatorname{mod} \mathfrak{m}_R$.

For proving that all entries $\gamma_{\mu,i} \in \mathfrak{m}_R$ for $\kappa_\nu < i \leq \kappa_{\nu+1} < \mu \leq d$, that is for all entries below the central blocks, we observe that from equation (21) combined with eq. (35) that $\gamma_{\mu,i}$ is divisible by $[a]_i^{\mu-1} = a_i a_{i+1} \cdots a_{\kappa_\nu+1} \cdots a_{\mu-1} \in \mathfrak{m}_R$. □

Recall that by lemma 2 there is an $1 \leq a_0 \leq m$ such that $\alpha = \zeta_m^{a_0}$.

Proposition 38. *The indecomposable module* V *modulo* $\mathfrak{m}_R$ *breaks into a direct sum of* $r+1$ *indecomposable* $k[C_q \rtimes C_m]$ *modules* V_ν*,* $1 \leq \nu \leq r+1$*. Each* V_ν *is isomorphic to* $V_\alpha(\epsilon + a_0\kappa_{\nu-1}, \kappa_\nu - \kappa_{\nu-1})$*.*

Proof. By eq. (36) the first eigenvalue of the reduced matrix block Γ_ν is

$$\zeta_m^\epsilon \alpha^{\kappa_{\nu-1}} = \zeta_m^{\epsilon + (\kappa_{\nu-1})a_0}.$$

Since that first eigenvalue together with the size of the block determine the last eigenvalue, that is the action of C_m on the socle the reduced block is uniquely determined up to isomorphism. □

This way we arrive at a new obstruction. Assume that the indecomposable representation given by the matrix T as in lemma 17 reduces modulo $\mathfrak{m}_R$ to a sum of Jordan blocks. Then the σ action on the leading elements of each Jordan block in the special fibre should be described by the corresponding action of σ on the leading eigenvector E of V. The corresponding actions on the special fibre should be compatible.

This observation is formally given in theorem 1, which we now prove. Recall that the $k[G]$-module M is decomposed as a direct sum

$$M = V_\alpha(\epsilon_1, \kappa_1) \oplus \cdots \oplus V_\alpha(\epsilon_s, \kappa_s).$$

Each set I_ν, $1 \leq \nu \leq t$ corresponds to an indecomposable $R[G]$-module, which decomposes to the indecomposables $V_\alpha(\epsilon_\mu, \kappa_\mu)$, $\nu \in I_\nu$ of the special fiber. Indecomposable summands have different roots of unity in R, therefore $\sum_{\mu \in I_\nu} k_\mu \leq q$, this is condition (1.a.). The second condition (1.b.) comes from proposition 14. If 1 is one of the possible eigenvalues of the lift T, then $\sum_{\mu \in I_\nu} \kappa_\mu \equiv 1 \bmod m$. If all eigenvalues of the lift T are different than one, then $\sum_{\mu \in I_\nu} \kappa_\mu \equiv 0 \bmod m$. If $\# I_\nu = q$, then there is one zero eigenvalue and the sum equals $1 \bmod m$.

It is clear by eq. (36) that condition (1.c.) is a necessary condition. On the other hand if (1.c.) is satisfied we can write (after a permutation if necessary) the set $\{1, \ldots, s\}$, $s = \sum_{\nu=1}^t \# I_\nu$ as a disjoint union

$$\{1, \ldots, s\} = I_1 \cup I_2 \cup \cdots \cup I_t$$

where each set I_ν, $1 \leq \nu \leq t$ contains the indecomposable representations $V_\alpha(\epsilon_\mu, k_\mu)$ that will form the reduction of an indecomposable representation of $R[G]$. Assume that the representations indexed by the set I_1 have dimensions $\{\kappa_1^{(1)}, \ldots, \kappa_{r_1}^{(1)}\}$, where $r_1 = \# I_1$, the represetnations indexed by I_2 have dimensions $\{\kappa_1^{(2)}, \ldots, \kappa_{r_2}^{(2)}\}$, where $r_2 = \# I_2$ and finally the representations indexed by I_t have dimensions $\{\kappa_1^{(t)}, \ldots, \kappa_{r_t}^{(t)}\}$, where $r_t = \# I_t$. We define

$$\begin{aligned}
b_1 &= \sum_{j=1}^{r_1} k_j^{(1)}, \\
b_2 &= b_1 + \sum_{j=1}^{r_2} k_j^{(2)}, \\
b_3 &= b_1 + b_2 + \sum_{j=1}^{r_3} k_j^{(3)}, \\
&\vdots \\
b_{t-1} &= b_1 + \cdots + b_{t-2} + \sum_{j=1}^{r_{t-1}} k_j^{(t-1)}.
\end{aligned}$$

The matrix given in eq. (11), where

$$a_i = \begin{cases} 0 & \text{if } i \in \{b_1, \ldots, b_{s-1}\} \\ \pi & \text{if } i \in \{\kappa_1^{(\nu)}, \kappa_1^{(\nu)} + \kappa_2^{(\nu)}, \kappa_1^{(\nu)} + \kappa_2^{(\nu)} + \kappa_3^{(\nu)}, \ldots, \kappa_1^{(\nu)} + \kappa_2^{(\nu)} + \cdots + \kappa_{r_\nu - 1}^{(\nu)}\} \\ 1 & \text{otherwise} \end{cases}$$

lifts the τ generator, and by (15) there is a well defined extended action of the σ as well.

Example: Consider the group $q = 5^2, m = 4, \alpha = 7$,

$$G = C_{5^2} \rtimes C_4 = \langle \sigma, \tau | \sigma^4 = \tau^{25} = 1, \sigma\tau\sigma^{-1} = \tau^7 \rangle.$$

Observe that $\mathrm{ord}_5 7 = \mathrm{ord}_{5^2} 7 = 4$.

- The module $V_\alpha(\epsilon, 25)$ is projective and is known to lift in characteristic zero. This fits well with theorem 1, since $4 \mid 25 - 1 = 4 \cdot 6$.
- The modules $V_\alpha(\epsilon, \kappa)$ do not lift in characteristic zero if $4 \nmid \kappa$ or $4 \nmid \kappa - 1$. Therefore only $V_\alpha(\epsilon, 1)$, $V_\alpha(\epsilon, 4)$, $V_\alpha(\epsilon, 5)$, $V_\alpha(\epsilon, 8)$, $V_\alpha(\epsilon, 9)$, $V_\alpha(\epsilon, 12)$, $V_\alpha(\epsilon, 13)$, $V_\alpha(\epsilon, 16)$, $V_\alpha(\epsilon, 17)$, $V_\alpha(\epsilon, 20)$, $V_\alpha(\epsilon, 21)$, $V_\alpha(\epsilon, 24)$, $V_\alpha(\epsilon, 25)$ lift.
- The module $V_\alpha(1, 2) \oplus V_\alpha(3, 2)$ lift to characteristic zero, where the matrix of T with respect to a basis E_1, E_2, E_3, E_4 is given by
$$T = \begin{pmatrix} \zeta_q & 0 & 0 & 0 \\ 1 & \zeta_q^2 & 0 & 0 \\ 0 & \pi & \zeta_q^3 & 0 \\ 0 & 0 & 1 & \zeta_q^4 \end{pmatrix}$$
and $S(E_1) = \zeta_q E_1$.
- The module $V_\alpha(1, 2) \oplus V_\alpha(1, 2)$ does not lift in characteristic zero. There is no way to permute the direct summands so that the eigenvalues of a lift S of σ are given by $\zeta_m^\epsilon, \alpha\zeta_m^\epsilon, \alpha^2\zeta_m^\epsilon, \alpha^3\zeta_m^\epsilon$. Notice that $\alpha = 2 = \zeta_m$.
- The module $V_\alpha(\epsilon_1, 21) \oplus V_\alpha(2^{21} \cdot \epsilon_1, 23)$ does not lift in characteristic zero. The sum $21 + 23$ is divisible by 4, $\epsilon_2 = 2^{21}\epsilon_1$ is compatible, but $21 + 23 = 44 > 25$ so the representation of T in the supposed indecomposable module formed by their sum can not have different eigenvalues which should be 25-th roots of unity.

References

[1] J. L. Alperin. *Local representation theory*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups.

[2] Frauke M. Bleher, Ted Chinburg, and Aristides Kontogeorgis. Galois structure of the holomorphic differentials of curves. *J. Number Theory*, 216:1–68, 2020.

[3] T. Chinburg, R. Guralnick, and D. Harbater. Oort groups and lifting problems. *Compos. Math.*, 144(4):849–866, 2008.

[4] Ted Chinburg, Robert Guralnick, and David Harbater. The local lifting problem for actions of finite groups on curves. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(4):537–605, 2011.

[5] Ted Chinburg, Robert Guralnick, and David Harbater. Global Oort groups. *J. Algebra*, 473:374–396, 2017.

[6] Huy Dang, Soumyadip Das, Kostas Karagiannis, Andrew Obus, and Vaidehee Thatte. Local oort groups and the isolated differential data criterion, 2019.

[7] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers. I. *Ann. of Math. (2)*, 76:73–92, 1962.

[8] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers. II. *Ann. of Math. (2)*, 77:318–328, 1963.

[9] Sotiris Karanikolopoulos and Aristides Kontogeorgis. Representation of cyclic groups in positive characteristic and Weierstrass semigroups. *J. Number Theory*, 133(1):158–175, 2013.

[10] Aristides Kontogeorgis and Alexios Terezakis. The canonical ideal and the deformation theory of curves with automorphisms, 2021.

[11] Andrew Obus. The (local) lifting problem for curves. In *Galois-Teichmüller theory and arithmetic geometry*, volume 63 of *Adv. Stud. Pure Math.*, pages 359–412. Math. Soc. Japan, Tokyo, 2012.

[12] Andrew Obus. A generalization of the Oort conjecture. *Comment. Math. Helv.*, 92(3):551–620, 2017.

[13] Andrew Obus and Rachel Pries. Wild tame-by-cyclic extensions. *J. Pure Appl. Algebra*, 214(5):565–573, 2010.

[14] Andrew Obus and Stefan Wewers. Cyclic extensions and the local lifting problem. *Ann. of Math. (2)*, 180(1):233–284, 2014.

[15] Florian Pop. The Oort conjecture on lifting covers of curves. *Ann. of Math. (2)*, 180(1):285–322, 2014.

[16] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[17] Jean-Pierre Serre. *Local fields*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[18] Bradley Weaver. The local lifting problem for D_4. *Israel J. Math.*, 228(2):587–626, 2018.

Department of Mathematics, National and Kapodistrian University of Athens Panepistimioupolis, 15784 Athens, Greece

Email address: kontogar@math.uoa.gr

Department of Mathematics, National and Kapodistrian University of Athens, Panepistimioupolis, 15784 Athens, Greece

Email address: aleksistere@math.uoa.gr