Séminaire Lotharingien de Combinatoire **70** (2014), Article B70h

ORBITS OF PAIRS IN ABELIAN GROUPS

C. P. ANILKUMAR AND AMRITANSHU PRASAD

Abstract. We compute the number of orbits of pairs in a finitely generated torsion module (more generally, a module of bounded order) over a discrete valuation ring. The answer is found to be a polynomial in the cardinality of the residue field whose coefficients are integers which depend only on the elementary divisors of the module, and not on the ring in question. The coefficients of these polynomials are conjectured to be non-negative integers.

1. Introduction

Let R be a discrete valuation ring with maximal ideal P generated by a uniformizing element π and residue field $\mathbf{k} = R/P$. An R-module M is said to be of bounded order if $P^N M = 0$ for some positive integer N. Let Λ denote the set of all sequences of the form

$$\lambda = (\lambda_1^{m_1}, \lambda_2^{m_2}, \dots, \lambda_l^{m_l}), \tag{1.1}$$

where $\lambda_1 > \lambda_2 > \dots > \lambda_l$ is a strictly decreasing sequence of positive integers and $m_1, m_2, \dots, m_l$ are non-zero cardinal numbers. We allow the case where $l = 0$, resulting in the empty sequence, which we denote by $\emptyset$. Every R-module of bounded order is, up to isomorphism, of the form

$$M_\lambda = (R/P^{\lambda_1})^{\oplus m_1} \oplus \dots \oplus (R/P^{\lambda_l})^{\oplus m_l} \tag{1.2}$$

for a unique $\lambda \in \Lambda$. We will, at times, wish to restrict ourselves to those $\lambda \in \Lambda$ for which all the cardinals $m_1, m_2, \dots, m_l$ are finite. We denote by Λ_0 this subset of Λ, which is the set of all partitions. The R-module M_λ is of finite length if and only if $\lambda \in \Lambda_0$.

Fix $\lambda \in \Lambda$, and write M for M_λ. Let G denote the group of R-module automorphisms of M. Then G acts on M^n by the diagonal action

$$g \cdot (x_1, \dots, x_n) = (g(x_1), \dots, g(x_n)) \text{ for } x_i \in M \text{ and } g \in G.$$

For $n = 1$, this is just the action on M of its automorphism group. A description of the orbits for this group action has been available for

2010 *Mathematics Subject Classification.* 20K01, 20K30, 05E15.

Key words and phrases. Finite Abelian groups, automorphism orbits, modules over discrete valuation rings.

more than a hundred years (see Miller [11], Birkhoff [1], and Dutta and Prasad [4]). Some qualitative results concerning G-orbits in M^n for general n were obtained by Calvert, Dutta and Prasad in [2]. In this paper we describe the set of G-orbits in M^n under the above action for $n = 2$. For instance, we prove the following result (see Theorem 5.11).

Theorem. *For every $\lambda \in \Lambda$, there exists a monic polynomial $n_\lambda(t) \in \mathbf{Z}[t]$ of degree λ_1 such that for every discrete valuation ring R with finite residue field of order q, if M is the R-module defined by* (1.2) *and G is the automorphism group of M, then*

$$|G\backslash(M \times M)| = n_\lambda(q).$$

This general set-up includes two important special cases, namely, finite Abelian p-groups and finite dimensional primary $K[t]$-modules where K is a field (isomorphism classes of which correspond to similarity classes of matrices with entries in K). The case of finite Abelian p-groups arises when R is the ring of p-adic integers and $\lambda \in \Lambda_0$. The case of finite dimensional primary $K[t]$-modules arises when R is the ring $\mathbf{k}[[u]]$ of formal power series with coefficients in $\mathbf{k} = K[t]/p(t)$ for some irreducible polynomial $p(t) \in K[t]$, and $\lambda \in \Lambda_0$. The exact interpretation of this problem in terms of linear algebra is explained in Section 7. Specifically, the identities (7.4) and (7.5) relate the numbers of G-orbits in $M \times M$ with the problem of counting the number of isomorphism classes of representations of a certain quiver with certain dimension vectors.

Our key result (Theorem 5.1) is a description of the G-orbit of a pair in $M \times M$. From this, when $\mathbf{k}$ is finite of order q and $\lambda \in \Lambda_0$, we are able to show that the cardinality of each orbit is a monic polynomial in q (Theorem 5.4) with integer coefficients which do not depend on R. Moreover, the number of orbits of a given cardinality is also a monic polynomial in q with integer coefficients which do not depend on R (Theorem 5.6). Theorem 5.6 gives an algorithm for computing the number of G-orbits in $M \times M$ of a given cardinality as a formal polynomial in q. In particular, we obtain an algorithm for computing, for each $\lambda \in \Lambda_0$, the polynomial $n_\lambda(t) \in \mathbf{Z}[t]$ for which $n_\lambda(q)$ is the number of G-orbits in $M \times M$ whenever R has residue field of order q. By implementing this algorithm in Sage we have computed $n_\lambda(q)$ for all partitions λ of integers up to 19 at the time of writing. A sample of results obtained is given in Table 1. The Sage program and a list of all $n_\lambda(q)$ are available from the web page `http://www.imsc.res.in/~amri/pairs/`. Our data lead us to make the following conjecture.

$\mathbf{n = 1}$	
(1)	$q + 2$
$\mathbf{n = 2}$	
(2)	$q^2 + 2q + 2$
$(1, 1)$	$q + 3$
$\mathbf{n = 3}$	
(3)	$q^3 + 2q^2 + 2q + 2$
$(2, 1)$	$q^2 + 5q + 5$
$(1, 1, 1)$	$q + 3$
$\mathbf{n = 4}$	
(4)	$q^4 + 2q^3 + 2q^2 + 2q + 2$
$(3, 1)$	$q^3 + 5q^2 + 7q + 4$
$(2, 2)$	$q^2 + 3q + 5$
$(2, 1, 1)$	$q^2 + 5q + 6$
$(1, 1, 1, 1)$	$q + 3$
$\mathbf{n = 5}$	
(5)	$q^5 + 2q^4 + 2q^3 + 2q^2 + 2q + 2$
$(4, 1)$	$q^4 + 5q^3 + 7q^2 + 6q + 4$
$(3, 2)$	$q^3 + 5q^2 + 10q + 7$
$(3, 1, 1)$	$q^3 + 5q^2 + 8q + 6$
$(2, 2, 1)$	$q^2 + 6q + 8$
$(2, 1, 1, 1)$	$q^2 + 5q + 6$
$(1, 1, 1, 1, 1)$	$q + 3$

TABLE 1. The polynomials $n_\lambda(q)$

Conjecture. *For each $\lambda \in \Lambda$, the polynomial $n_\lambda(t)$ has non-negative coefficients.*

We are able to refine the results described above: the total number of G-orbits in $M \times M$ can be broken up into the sum of G-orbits in $A \times B$, as A and B run over G-orbits in M. The parametrization of G-orbits in M is purely combinatorial and does not depend on R, or even on q (see Dutta and Prasad [4]). The orbits are parametrized by a certain set $\mathcal{J}(\mathbf{P})_\lambda$ of order ideals in a lattice (see Section 2 for details). For $I \in \mathcal{J}(\mathbf{P})_\lambda$, let M_I^* denote the orbit in M parametrized by I. For each pair $I, J \in \mathcal{J}(\mathbf{P})_\lambda$, we are able to show (Theorem 6.3) that the number of G-orbits in $M_I^* \times M_J^*$ of any given cardinality is a polynomial in q with integer coefficients which do not depend on R.

Our analysis of stabilizers in G of elements of M allows us to show that, for any $\lambda \in \Lambda$, the number of G-orbits in $M \times M$ does not change when $\lambda \in \Lambda$ is replaced by the partition derived from λ by reducing each of the multiplicities m_i of (1.1) to $\min(m_i, 2)$ (Corollary 4.5). Thus, our calculations for the number of G-orbits in $M_I^* \times M_J^*$ extend to all $\lambda \in \Lambda$.

2. Orbits of elements

The G-orbits in M have been understood quite well for over a hundred years (see Miller [11], Birkhoff [1], for $\lambda \in \Lambda_0$, and relatively recent work by Schwachhöfer and Stroppel [12], for general $\lambda \in \Lambda$). For the present purposes, however, the combinatorial description of orbits due to Dutta and Prasad [4] is more relevant. This section will be a quick recapitulation of those results.

It turns out that for any module M of the form (1.2), the G-orbits in M are in bijective correspondence with a certain class of ideals in a poset $\mathbf{P}$, which we call the fundamental poset. As a set,

$$\mathbf{P} = \{(v, k) \mid k \text{ is a positive integer, and } 0 \leq v < k\}.$$

The partial order on $\mathbf{P}$ is defined by setting

$$(v, k) \leq (v', k') \text{ if and only if } v \geq v' \text{ and } k - v \leq k' - v'.$$

The Hasse diagram of the fundamental poset $\mathbf{P}$ is shown in Figure 1.

Remark. In [4], the notation (p^v, k) is used for the element (v, k) of $\mathbf{P}$ defined above.

Let $\mathcal{J}(\mathbf{P})$ denote the lattice of order ideals in $\mathbf{P}$. A typical element of M from (1.2) is a vector of the form

$$x = (x_{\lambda_i, r_i}), \tag{2.1}$$

where i runs over the set $\{1, \ldots, l\}$, and, for each i, r_i runs over a set of cardinality m_i. To $x \in M$ we associate the order ideal $I(x) \in \mathcal{J}(\mathbf{P})$ generated by the elements

$$(v(x_{\lambda_i, r_i}), \lambda_i)$$

for all pairs (i, r_i) such that $x_{\lambda_i, r_i} \neq 0$ in R/P^{λ_i}. Here, for any $m \in M$, $v(m)$ denotes the largest k for which $m \in P^k M$ (in particular, $v(0) = \infty$).

Consider for example, in the finite Abelian p-group (or $\mathbf{Z}_p$-module)

$$M = \mathbf{Z}/p^5\mathbf{Z} \oplus \mathbf{Z}/p^4\mathbf{Z} \oplus \mathbf{Z}/p^4\mathbf{Z} \oplus \mathbf{Z}/p^2\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}, \tag{2.2}$$

the order ideal $I(0, up, p^2, vp, 1)$, when u and v are coprime to p. This order ideal is represented inside $\mathbf{P}$ by filled-in circles (both gray and

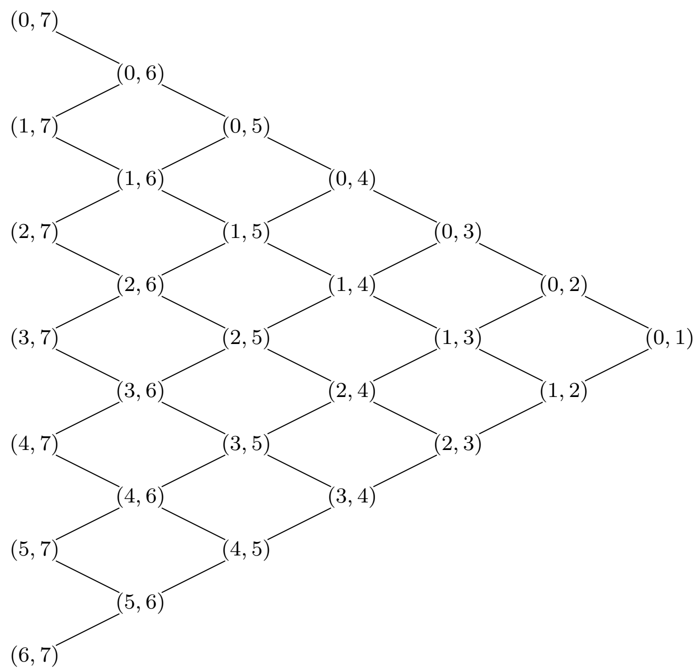


Figure 1. The Fundamental Poset

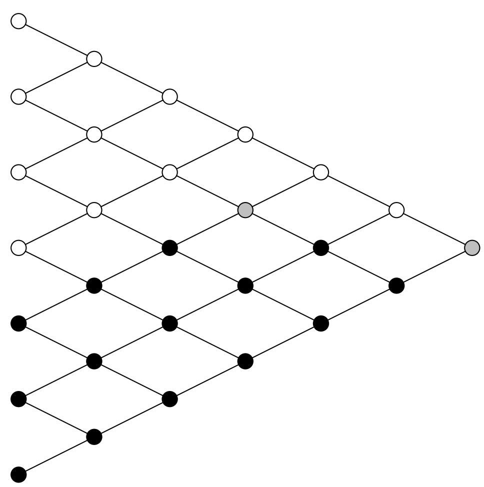


Figure 2. The ideal $I(0, up, p^2, vp, 1)$

black; the significance of the shades will be explained later) in Figure 2. Since the labels of the vertices can be inferred from their positions, they are omitted.

A key observation of [4] is the following theorem.

Theorem 2.3. *Let M and N be two R-modules of bounded order. An element $y \in N$ is a homomorphic image of $x \in M$ (in other words, there exists a homomorphism $\phi : M \to N$ such that $\phi(x) = y$) if and only if $I(y) \subset I(x)$.*

It follows that, if $y \in M$ lies in the G-orbit of $x \in M$, then $I(x) = I(y)$. It turns out that the converse is also true.

Theorem 2.4. *If $I(x) = I(y)$ for any $x, y \in M$, then x and y lie in the same G-orbit.*

Note that the orbit of 0 corresponds to the empty ideal.

For each $\lambda \in \Lambda$, let $\mathcal{J}(\mathbf{P})_\lambda$ denote the sublattice of $\mathcal{J}(\mathbf{P})$ consisting of ideals such that $\max I$ is contained in the set

$$\mathbf{P}_\lambda = \{(v, k) \mid k = \lambda_i \text{ for some } 1 \leq i \leq l\}.$$

Then the G-orbits in M are in bijective correspondence with this set $\mathcal{J}(\mathbf{P})_\lambda$ of order ideals[1]. For each order ideal $I \in \mathcal{J}(\mathbf{P})_\lambda$, we use the notation

$$M_I^* = \{x \in M \mid I(x) = I\}$$

for the orbit corresponding to I.

A convenient way to think about ideals in $\mathbf{P}$ is in terms of what we call their boundaries: for each positive integer k define the boundary valuation of I at k to be

$$\partial_k I = \min\{v \mid (v, k) \in I\}.$$

We denote the sequence $\{\partial_k I\}$ of boundary valuations by ∂I and call it the boundary of I. This is indeed the boundary of the region with colored dots in Figure 2.

For each order ideal $I \subset \mathbf{P}$, let $\max I$ denote its set of maximal elements. The ideal I is completely determined by $\max I$: in fact, taking I to $\max I$ gives a bijection from the lattice $\mathcal{J}(\mathbf{P})_\lambda$ to the set of antichains in $\mathbf{P}_\lambda$. For example, the maximal elements of the ideal in Figure 2 are represented by gray circles.

Theorem 2.5. *The orbit M_I^* consists of elements $x = (x_{\lambda_i, r_i})$ such that $v(x_{\lambda_i, r_i}) \geq \partial_{\lambda_i} I$ for all λ_i and r_i, and such that $v(x_{\lambda_i, r_i}) = \partial_{\lambda_i} I$ for at least one r_i if $(\partial_{\lambda_i} I, \lambda_i) \in \max I$.*

In other words, the elements of M_I^* are those elements all of whose coordinates have valuations not less than the corresponding boundary valuation, and at least one coordinate corresponding to each maximal

[1] The lattice $\mathcal{J}(\mathbf{P})_\lambda$ is isomorphic to the lattice $\mathcal{J}(\mathbf{P}_\lambda)$ of order ideals in the induced subposet $\mathbf{P}_\lambda$. In [4], $\mathcal{J}(\mathbf{P}_\lambda)$ is used in place of $\mathcal{J}(\mathbf{P})_\lambda$.

element of I has valuation exactly equal to the corresponding boundary valuation.

In the running example with M as in (2.2) and I as in Figure 2, the conditions for $x = (x_{5,1}, x_{4,1}, x_{4,2}, x_{2,1}, x_{1,1})$ to be in M_I^* are:

- $v(x_{5,1}) \geq 4$,
- $\min(v(x_{4,1}), v(x_{4,2})) = 1$,
- $v(x_{2,1}) \geq 1$,
- $v(x_{1,1}) = 0$.

For each $I \in \mathcal{J}(\mathbf{P})_\lambda$ with

$$\max I = \{(v_1, k_1), \dots, (v_s, k_s)\},$$

define an element $\gamma(I)$ of M whose coordinates are given by

$$x_{\lambda_i, r_i} = \begin{cases} \pi^{v_j}, & \text{if } \lambda_i = k_j \text{ and } r_j = 1, \\ 0, & \text{otherwise.} \end{cases}$$

In other words, for each element (v_j, k_j) of $\max I$, pick λ_i such that $\lambda_i = k_j$. In the summand $(R/P^{\lambda_i})^{\oplus m_i}$, set the first coordinate of $\gamma(I)$ to π^{v_j}, and the remaining coordinates to 0. For example, in the finite Abelian p-group of (2.2), and the ideal I of Figure 2,

$$\gamma(I) = (0, p, 0, 0, 1).$$

Theorem 2.6. *Let $M = M_\lambda$ be an R-module of bounded order as in (1.2). The functions $x \mapsto I(x)$ and $I \mapsto \gamma(I)$ induce mutually inverse bijections between the set of G-orbits in M and the set of order ideals in $\mathcal{J}(\mathbf{P})_\lambda$.*

For any ideal $I \in \mathcal{J}(\mathbf{P})$, define

$$M_I = \coprod_{\{J \in \mathcal{J}(\mathbf{P})_\lambda \mid J \subset I\}} M_I^*.$$

This submodule, being a union of G-orbits, is G-invariant. The description of M_I in terms of valuations of coordinates and boundary valuations is very simple:

$$M_I = \{x = (x_{\lambda_i, r_i}) \mid v(x_{\lambda_i, r_i}) \geq \partial_{\lambda_i} I\}. \tag{2.7}$$

Note that the map $I \mapsto M_I$ is not injective on $\mathcal{J}(\mathbf{P})$. It becomes injective when restricted to $\mathcal{J}(\mathbf{P})_\lambda$. For example, if J is the order ideal in $\mathbf{P}$ generated by $(2, 6)$, $(1, 4)$ and $(0, 1)$, then the ideal J is strictly larger than the ideal I of Figure 2, but when M is as in (2.2), $M_I = M_J$.

The G-orbits in M are parametrized by the finite distributive lattice $\mathcal{J}(\mathbf{P})_\lambda$. Moreover, each order ideal $I \in \mathcal{J}(\mathbf{P})_\lambda$ gives rise to a G-invariant submodule M_I of M. The lattice structure of $\mathcal{J}(\mathbf{P})_\lambda$ gets reflected in the poset structure of the submodules M_I when they are partially ordered by inclusion.

Theorem 2.8. *The map $I \mapsto M_I$ gives an isomorphism from $\mathcal{J}(\mathbf{P})_\lambda$ to the poset of G-invariant submodules of M of the form M_I.*

In other words, for ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$,

$$M_{I\cup J} = M_I + M_J \text{ and } M_{I\cap J} = M_I \cap M_J.$$

In fact, when the residue field $\mathbf{k}$ of R has at least three elements, every G-invariant submodule is of the form M_I, therefore $\mathcal{J}(\mathbf{P})_\lambda$ is isomorphic to the lattice of G-invariant submodules (Kerby and Rode [9]).

When M is a finite R-module (this happens when the residue field $\mathbf{k}$ of R is finite and $\lambda \in \Lambda_0$), then the G-orbits in M are also finite. The cardinality of the orbit M_I^* is given by (see [4, Theorem 8.5])

$$|M_I^*| = q^{[I]_\lambda} \prod_{(v_i,\lambda_i)\in \max I} (1 - q^{-m_i}). \tag{2.9}$$

Here $[I]_\lambda$ denotes the number of points in $I \cap P_\lambda$ counted *with multiplicity*,

$$[I]_\lambda = \sum_{i=1}^{l} \sum_{\{v \mid (v,\lambda_i)\in I\}} m_i.$$

In particular, we have the following result.

Theorem 2.10. *For every $\lambda \in \Lambda_0$ and $I \in \mathcal{J}(\mathbf{P})_\lambda$, consider the monic polynomial $\omega_{\lambda,I}(t) \in \mathbf{Z}[t]$ of degree $[I]_\lambda$ defined by*

$$\omega_{I,t}(t) = t^{[I]_\lambda} \prod_{(v_i,\lambda_i)\in \max I} (1 - t^{-m_i}).$$

Then, for any discrete valuation ring R with finite residue field of order q, if M is the R-module defined by (1.2)*, we have*

$$|M_I^*| = \omega_{\lambda,I}(q).$$

The formula for the cardinality of the G-invariant submodule is much simpler:

$$|M_I| = q^{[I]_\lambda}. \tag{2.11}$$

3. Sum of orbits

This section proves a combinatorial lemma on the sum of two G-orbits in M which will be needed in Section 4. Given order ideals $I, J \subset \mathcal{J}(\mathbf{P})_\lambda$, the set

$$M_I^* + M_J^* = \{x + y \mid x \in M_I^* \text{ and } y \in M_J^*\}$$

is clearly G-invariant, and therefore a union of G-orbits. In this section, we determine exactly which G-orbits occur in $M_I^* + M_J^*$.

Lemma 3.1. *For $I, J \in \mathcal{J}(\mathbf{P})_\lambda$, every element (x_{λ_i, r_i}) of $M_I^* + M_J^*$ satisfies the conditions*

(3.1.1) $v(x_{\lambda_i,r_i}) \geq \min(\partial_{\lambda_i} I, \partial_{\lambda_i} J)$.
(3.1.2) *If $(\partial_{\lambda_i} I, \lambda_i) \in \max I - J$, then* $\min_{r_i} v(x_{\lambda_i,r_i}) = \partial_{\lambda_i} I$.
(3.1.3) *If $(\partial_{\lambda_i} J, \lambda_i) \in \max J - I$, then* $\min_{r_i} v(x_{\lambda_i,r_i}) = \partial_{\lambda_i} J$.

If the residue field of R has at least three elements, then every element of M satisfying these three conditions is in $M_I^* + M_J^*$.

To see why the condition on the residue field is necessary, consider the case where $M = \mathbf{Z}/2\mathbf{Z}$ and M_I^* is the non-zero orbit (corresponding to the ideal I in $\mathbf{P}$ generated by $(0, 1)$), $M_I^* + M_I^*$ consists only of 0. If, on the other hand, the residue field has at least three elements, then it has non-zero elements x and y such that $x + y$ is also non-zero, and this phenomenon does not occur.

Proof of the lemma. Let $M^{(i)}$ denote the summand $(R/P^{\lambda_i})^{\oplus m_i}$ of M in the decomposition (1.2). Let $M^{(i)*} = M^{(i)} - \pi M^{(i)}$. By Theorem 2.5 it suffices to show that

$$\pi^k M^{(i)*} + \pi^l M^{(i)*} = \begin{cases} \pi^{\min(k,l)} M^{(i)*}, & \text{if } k \neq l, \\ \pi^k M^{(i)}, & \text{if } k = l \text{ and } |R/P| \geq 3. \end{cases} \tag{3.2}$$

This follows from the well-known non-Archimedean inequality

$$v(x + y) \geq \min(v(x), v(y)),$$

and the fact that strict inequality is possible only if $v(x) = v(y)$. □

Together with Theorem 2.5, the above lemma gives the following description of the set of orbits which occur in $M_I^* + M_J^*$.

Theorem 3.3. *Assume that the residue field of R has at least three elements. For ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$, we have*

$$M_I^* + M_J^* = \coprod_{K \subset I \cup J,\ \max K \supset (\max I - J) \cup (\max J - I)} M_K^*.$$

In the following lemma the restriction on the residue field of R in Lemma 3.1 is not needed.

Lemma 3.4. *For ideals I and J in $\mathcal{J}(\mathbf{P})_\lambda$, an element (x_{λ_i,r_i}) is in $M_I^* + M_J$ if and only if the following conditions are satisfied:*

(3.4.1) $v(x_{\lambda_i,r_i}) \geq \min(\partial_{\lambda_i} I, \partial_{\lambda_i} J)$.

(3.4.2) *If* $(\partial_{\lambda_i} I, \lambda_i) \in \max I - J$, *then* $\min_{r_i} v(x_{\lambda_i,r_i}) = \partial_{\lambda_i} I$.

Proof. The proof is similar to that of Lemma 3.1, except that, instead of (3.2), we use

$$\pi^k M^{(i)} + \pi^l M^{(i)*} = \begin{cases} \pi^k M^{(i)}, & \text{if } k \leq l, \\ \pi^l M^{(i)*}, & \text{if } k > l. \end{cases}$$

□

The above lemma allows us to describe the sum of an orbit and a characteristic submodule.

Theorem 3.5. *For ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$, we have*

$$M_I^* + M_J = \coprod_{K \subset I \cup J,\ \max K \supset \max I - J} M_K^*. \tag{3.6}$$

4. Stabilizers of $\gamma(I)$'s

By Theorem 2.6, every G-orbit of pairs of elements $(x_1, x_2) \in M^2$ contains a pair of the form $(\gamma(I), x)$, for some $I \in \mathcal{J}(\mathbf{P})_\lambda$ and $x \in M$. Now fix an ideal $I \in \mathcal{J}(\mathbf{P})_\lambda$. Let G_I denote the stabilizer in G of $\gamma(I)$. Then the G-orbits of pairs in M^2 which contain an element of the form $(\gamma(I), x)$ are in bijective correspondence with G_I-orbits in M. In this section, we give a description of G_I which facilitates the classification of G_I-orbits in M.

The main idea here is to decompose M into a direct sum of two R-modules (this decomposition depends on I):

$$M = M' \oplus M'', \tag{4.1}$$

where M' consists of those cyclic summands in the decomposition (1.2) of M where $\gamma(I)$ has non-zero coordinates, and M'' consists of the remaining cyclic summands. In the running example with M given by (2.2) and I the ideal in Figure 2, we have

$$M' = \mathbf{Z}/p^4\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}, \quad M'' = Z/p^5\mathbf{Z} \oplus \mathbf{Z}/p^4\mathbf{Z} \oplus \mathbf{Z}/p^2\mathbf{Z}.$$

Note that $\gamma(I) \in M'$. The reason for introducing this decomposition is that the description of the stabilizer of $\gamma(I)$ in the automorphism group of M' is quite nice.

Lemma 4.2. *The stabilizer of $\gamma(I)$ in $\mathrm{Aut}_R(M')$ is*

$$G'_I = \{\mathrm{id}_{M'} + u \mid u \in \mathrm{End}_R M' \text{ satisfies } u(\gamma(I)) = 0\}.$$

Proof. Obviously, the elements of G'_I are all the elements of $\mathrm{End}_R M'$ which map $\gamma(I)$ to itself. The only thing to check is that they are all invertible. For this, it suffices to show that, if $u(\gamma(I)) = 0$, then u is nilpotent, which will follow from Lemma 4.3 below. ☐

Lemma 4.3. *For any R-module of the form*

$$L = R/P^{\mu_1} \oplus \cdots \oplus R/P^{\mu_m},$$

with $\mu_1 > \cdots > \mu_m$, and $x = (\pi^{v_1}, \ldots, \pi^{v_m}) \in L$ such that the set

$$(v_1, \mu_1), \ldots, (v_m, \mu_m)$$

is an antichain in $\mathbf{P}$, if $u \in \mathrm{End}_R L$ is such that $u(x) = 0$, then u is nilpotent.

Proof. Write u as a matrix (u_{ij}), where $u_{ij} : R/P^{\lambda_j} \to R/P^{\lambda_i}$. We have

$$u(\pi^{v_1}, \ldots, \pi^{v_m})_i = u_{ii}(\pi^{v_i}) + \sum_{j \neq i} u_{ij}(\pi^{v_j}) = 0,$$

for $1 \leq i \leq m$. If $u_{ii}1$ is a unit, then $u_{ii}\pi^{v_i}$ has valuation v_i, hence at least one of the summands $u_{ij}\pi^{v_j}$ must have valuation v_i or less. It follows from Theorem 2.3 (applied to $M = R/P^{\mu_j}$ and $N = R/P^{\mu_i}$) that $(v_i, \mu_i) \leq (v_j, \mu_j)$ contradicting the antichain hypothesis. Thus, for each i, $u_{ii}(1) \in PR/P^{\mu_i}$. It follows that u lies in the radical of the ring $\mathrm{End}_R L$ (see Dubey, Prasad and Singla [3, Section 6]), and therefore u is nilpotent. ☐

Every endomorphism of M can be written as a matrix $\begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$, where $g_{11} : M' \to M'$, $g_{22} : M'' \to M'$, $g_{21} : M'' \to M'$, and $g_{22} : M'' \to M''$ are homomorphisms.

We are now ready to describe the stabilizer of $\gamma(I)$ in M.

Theorem 4.4. *The stabilizer of $\gamma(I)$ in G consists of matrices of the form*

$$\begin{pmatrix} \mathrm{id}_{M'} + u & g_{12} \\ g_{21} & g_{22} \end{pmatrix},$$

where $u \in \mathrm{End}_R M'$ satisfies $u(\gamma(I)) = 0$, $g_{12} \in \mathrm{Hom}_R(M'', M')$ is arbitrary, $g_{21} \in \mathrm{Hom}_R(M', M'')$ satisfies $g_{21}(\gamma(I)) = 0$, and $g_{22} \in \mathrm{End}_R(M'')$ is invertible.

Proof. Clearly, all the endomorphisms of M which fix $\gamma(I)$ are of the form stated in the theorem, except that g_{22} need not be invertible. We need to show that the invertibility of such an endomorphism is equivalent to the invertibility of g_{22}.

To begin with, consider the case where $M = (R/P^k)^n$ for some positive integer k and some cardinal n. Then, if $\gamma(I) \neq 0$ (the case $\gamma(I) = 0$ is trivial), then $M' = R/P^k$, and $M'' = (R/P^k)^{n-1}$. The endomorphisms which fix $\gamma(I)$ are represented by block matrices of the form

$$\begin{pmatrix} 1+u & g_{12} \\ g_{21} & g_{22} \end{pmatrix},$$

where u, and each coordinate of g_{21} lie in P. Such endomorphisms, being block upper-triangular modulo P, are invertible if and only if g_{22} is invertible, proving the claim when $M = (R/P^k)^n$. In general, M is a sum of such modules, and an endomorphism of M is invertible if and only if its diagonal block corresponding to each of these summands is invertible. Therefore the claim follows in general as well. □

Corollary 4.5 (Independence of multiplicities larger than two)**.** *Consider the partition $\lambda^{(m)}$ derived from λ by*

$$\lambda^{(m)} = (\lambda_1^{\min(m_1,m)}, \lambda_2^{\min(m_2,m)}, \dots, \lambda_l^{\min(m_l,m)}).$$

Let M_m denote the R-module corresponding to $\lambda^{(m)}$, with automorphism group G_m. Then the standard inclusion map $M_2 \hookrightarrow M$ induces a bijection

$$G_2\backslash(M_2 \times M_2) \tilde{\to} G\backslash(M \times M). \tag{4.6}$$

Proof. We shall use the fact that the canonical forms $\gamma(I)$ of Theorem 2.6 lie in $M_1 \subset M$. Thus, given a pair $(x, y) \in M \times M$, we can reduce x to $\gamma(I) \in M_1$ using automorphisms of M. Theorem 4.4 shows that, while preserving $\gamma(I)$, automorphisms of M can be used to further reduce y to an element of $M' \oplus M_1'' \subset M_2$. This proves the surjectivity of the map in (4.6).

To see injectivity, suppose that two pairs (x_1, y_1) and (x_2, y_2) in $M_2 \times M_2$ lie in the same G-orbit. Since M_2 is a direct summand of M, we can write $M = M_2 \oplus N$. If $g \in G$ has matrix $\begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$ with respect to this decomposition, then $g_{11} \in G_2$ also maps $(x_1, y_1) \in M_2 \times M_2$ to $(x_2, y_2) \in M_2 \times M_2$. □

Remark 4.7. Corollary 4.5 and its proof remain valid if we restrict ourselves to G-orbits in $M_I^* \times M_J^*$ for order ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$.

5. The stabilizer orbit of an element

Let G_I denote the stabilizer of $\gamma(I) \in M$. Write each element $x \in M$ as $x = (x', x'')$ with respect to the decomposition (4.1) of M. Also, for any $x' \in M'$, let $\bar{x}'$ denote the image of x' in $M'/R\gamma(I)$.

Theorem 4.4 allows us to describe the orbit of x under the action of G_I, which is the same as describing the G-orbits in M^2 whose first component lies in the orbit M_I^* of $\gamma(I)$.

Theorem 5.1. *Given x and y in M, y lies in the G_I-orbit of x in M if and only if the following conditions hold:*

(5.1.1) $y' \in x' + M'_{I(\bar{x}') \cup I(x'')}$.
(5.1.2) $y'' \in {M''}^*_{I(x'')} + M''_{I(\bar{x}')}$.

Proof. By Theorem 4.4, y lies in the G_I-orbit of x if and only if

$$y' = x' + \bar{u}(\bar{x}') + g_{12}(x'') \text{ and } y'' = \bar{g}_{21}(\bar{x}') + g_{22}(x'')$$

for homomorphisms $\bar{u} \in \mathrm{Hom}_R(M'/R\gamma(I), M')$, $g_{12} \in \mathrm{Hom}_R(M'', M')$, $\bar{g}_{21} \in \mathrm{Hom}_R(M'/R\gamma(I), M'')$, and $g_{22} \in \mathrm{Aut}_R(M'')$. By Theorems 2.3 and 2.4, this means

$$y' \in x' + M'_{I(\bar{x}')} + M'_{I(x'')} \text{ and } y'' \in M''_{I(\bar{x}')} + {M''}^*_{I(x'')}.$$

By the remark following Theorem 2.8, $M'_{I(\bar{x}')} + M'_{I(x'')} = M'_{I(\bar{x}') \cup I(x'')}$, giving the conditions in the lemma. □

Given $x = (x', x'') \in M$, the ideals $I(\bar{x}')$ and $I(x'')$ may be regarded as combinatorial invariants of x. Suppose that the residue field $\mathbf{k}$ of R is finite of order q. We can now show that, having fixed these combinatorial invariants, the cardinality of the orbit of x is a polynomial in q whose coefficients are integers which do not depend on R. Also, the number of elements of M having these combinatorial invariants is a polynomial in q whose coefficients are integers which do not depend on R. Using these observations, we will be able to conclude that the number of orbits of pairs in M is a polynomial in q whose coefficients are integers which do not depend on R.

Let λ'/I denote the partition corresponding to the isomorphism class of $M'/R\gamma(I)$. The partition λ'/I is completely determined by the partition λ' and the ideal $I \in \mathcal{J}(\mathbf{P})_{\lambda'}$, and is independent of R (see Lemma 6.2).

Theorem 5.2. *Fix $J \in \mathcal{J}(\mathbf{P})_{\lambda'/I}$ and $K \in \mathcal{J}(\mathbf{P})_{\lambda''}$. Then the cardinality of the G_I-orbit of any element $x = (x', x'')$ such that $I(\bar{x}') = J$*

and $I(x'') = K$ is given by

$$|M'_{J\cup K}|\left(\sum_{K'\subset J\cup K,\, \max K'\supset \max K - J} |M''^{*}_{K'}|\right). \tag{5.3}$$

Proof. This is a direct consequence of Theorems 3.5 and 5.1. □

Applying Theorem 2.10 and (2.11) to Theorem 5.2, we obtain the following result.

Theorem 5.4. *For every $\lambda \in \Lambda_0$, $I \in \mathcal{J}(\mathbf{P})_\lambda$, $J \in \mathcal{J}(\mathbf{P})_{\lambda'/I}$, and $K \in \mathcal{J}(\mathbf{P})_{\lambda''}$, there exists a monic polynomial $\alpha_{I,J,K}(t) \in \mathbf{Z}[t]$ of degree $[J \cup K]_\lambda$ such that, for any discrete valuation ring R with residue field of order q, if M is the R-module defined by (1.2), then the cardinality of the G_I-orbit of $x \in M$ is of the form $\alpha_{I,J,K}(q)$, where $J = I(\bar{x}')$ and $K = I(x'')$.*

If the sets

$$X_{I,J,K} = \{(x', x'') \in M \mid I(\bar{x}') = J \text{ and } I(x'') = K\}$$

were G_I-stable, we could have concluded that $X_{I,J,K}$ consists of

$$\frac{|X_{I,J,K}|}{\alpha_{I,J,K}(q)}$$

many orbits, each of cardinality $\alpha_{I,J,K}(q)$. However, $X_{I,J,K}$ is not, in general, G_I-stable (this can be seen by viewing the condition (5.1.2) in the context of Theorem 3.5). The following lemma gives us a way to work around this problem.

Lemma 5.5. *Let S be a finite set with a partition $S = \coprod_{i=1}^N S_i$ (for the application we have in mind, these will be the G_I-orbits in M). Suppose that S has another partition $S = \coprod_{j=1}^Q T_j$, such that there exist positive integers $n_1, n_2, \dots, n_Q$ for which, if $x \in T_j \cap S_i$, then $|S_i| = n_j$ (in our case, the T_j's will be the sets $X_{I,J,K}$). Then the number of $i \in \{1, \dots, N\}$ such that $|S_i| = n$ is given by*

$$\frac{1}{n} \sum_{\{j \mid n_j = n\}} |T_j|.$$

Proof. Note that

$$\coprod_{\{j \mid n_j = n\}} |T_j|$$

is the union of all the S_i's for which $|S_i| = n$. □

By Theorem 2.10 and (2.11), we also know that there exists a polynomial $\chi_{I,J,K}(t) \in \mathbf{Z}[t]$ such that, whenever R is a discrete valuation ring with residue field of order q, $|X_{I,J,K}| = \chi_{I,J,K}(q)$.

Taking S to be the set M, the S_i's to be the G_I-orbits in M, and the T_j's to be the sets $X_{I,J,K}$ in Lemma 5.5, we obtain the following result.

Theorem 5.6. *Let $\alpha(t) \in Z[t]$ be a monic polynomial. Consider the rational function*

$$N_\alpha(t) = \frac{1}{\alpha(t)} \sum_{\{(I,J,K) | \alpha_{I,J,K}(t) = \alpha(t)\}} \chi_{I,J,K}(t).$$

Then, whenever R is a discrete valuation ring with residue field of order q, the number of G_I-orbits in M with cardinality $\alpha(q)$ is $N_\alpha(q)$.

The following lemma shows that it is in fact a polynomial in q with integer coefficients.

Lemma 5.7. *Let $r(q)$ and $s(q)$ be polynomials in q with integer coefficients. Suppose that $r(q)/s(q)$ takes integer values for infinitely many values of q. Then $r(q)/s(q)$ is a polynomial in q with rational coefficients. If, in addition $s(q)$ is monic, then this polynomial has integer coefficients.*

The proof, being fairly straightforward, is omitted.

Example 5.8. Consider an arbitrary $\lambda \in \Lambda$, and take I to be the maximal ideal in $\mathcal{J}(\mathbf{P})_\lambda$ (this is the ideal in $\mathbf{P}$ generated by $\mathbf{P}_\lambda$). Then, in the notation of (1.1),

$$\lambda' = (\lambda_1), \quad \lambda'' = (\lambda_1^{m_1-1}, \lambda_2^{m_2}, \dots, \lambda_l^{m_l}).$$

The element $\gamma(I)$ is a generator of M', and so $M'/R\gamma(I) = 0$. It follows that the only possibility for the ideal $J \in \mathcal{J}(\mathbf{P})_{\lambda'/I}$ is $J = \emptyset$. As a result, the only combinatorial invariant of a G_I-orbits in M is $K \in \mathcal{J}(\mathbf{P})_{\lambda''}$. We have

$$\alpha_{I,\emptyset,K}(q) = |M'_K||M''^*_K|.$$

On the other hand,

$$|X_{I,\emptyset,K}| = q^{\lambda_1}|M''^*_K|.$$

Therefore, given a polynomial $\alpha(q)$, the number of G_I-orbits of cardinality $\alpha(q)$ is

$$\sum_{\{K \in \mathcal{J}(\mathbf{P})_{\lambda''} | \alpha_{I,\emptyset,K} = \alpha(q)\}} \frac{q^{\lambda_1}}{|M'_K|}.$$

Cardinality	Number of Orbits
1	q^3
$(q-1)q^7$	$(q-1)q$
$(q-1)q^{12}$	$(q-1)$
q^4	$(q-1)q^2$
$(q-1)^2q^{11}$	1
$(q-1)^2q^8$	q
$(q-1)^2q^{10}$	1
$(q-1)q^2$	q^2
$(q-1)^2q^6$	q
$(q-1)^2q^3$	q^2
$(q-1)^2q^5$	q
$(q-1)$	q^3
$(q-1)q^{15}$	1
$(q-1)q^5$	q
q^9	$(q-1)q$
$(q-1)q^8$	q
$(q-1)q^{14}$	1
$(q-1)q^{11}$	$(q-1)$
$(q-1)q^6$	q^2
$(q-1)q^4$	$(q-1)q^2$
$(q-1)q^3$	$2q^2$
$(q-1)q^9$	q^2
$(q-1)q^{10}$	q

TABLE 2. Cardinalities and numbers of G_I-orbits

Since $K=\emptyset$ is the only ideal in $\mathcal{J}(\mathbf{P})_{\lambda''}$ for which $|M'_K|=1$, it turns out that the total number of G_I-orbits in $M_I\times M$ is a monic polynomial in q of degree λ_1.

For example, if $\lambda=(2,1^{m_2})$ and I is the maximal ideal in $\mathcal{J}(\mathbf{P})_\lambda$, then the number of G_I-orbits in M is q^2+q, and, if $\lambda=(2^{m_1},1^{m_2})$ with $m_1>1$, then the number of G_I-orbits in λ is q^2+2q+1.

Example 5.9. Now consider the case where $\lambda=(5,4,4,2,1)$ and I is the ideal of Figure 2. Then the first column of Table 5.9 gives all the possible cardinalities for G_I-orbits in M. The corresponding entry of the second column is the number of orbits with that cardinality. The total number of G_I-orbits in M is given by the polynomial

$$4q^3+6q^2+6q+2.$$

These data were generated using a computer program written in Sage. In general the total number of G_I-orbits in M need not be a polynomial with positive integer coefficients, for example, take $\lambda = (2)$ (so $M = R/P^2R$) and I the ideal generated by $(1, 2)$ (the corresponding orbit in M contains π). Then the number of G_I-orbits in M is $2q - 1$.

The above results can be summarized to give the following theorem.

Theorem 5.10. *Fix $\lambda \in \Lambda_0$ and an order ideal $I \in \mathcal{J}(\mathbf{P})_\lambda$. There exist polynomials $\alpha_1(t), \ldots, \alpha_N(t)$, $\beta_1(t), \ldots, \beta_N(t)$ with integer coefficients such that, for every discrete valuation ring R with finite residue field of order q, if $M = M_\lambda$ is as in* (1.2) *and G is the group of R-module automorphisms of M, then the decomposition of $M_I^* \times M$ into G-orbits consists of a disjoint union over $i \in \{1, \ldots, N\}$ of $\beta_i(q)$ orbits of cardinality $\alpha_i(q)$.*

For the total number of orbits in $M \times M$, we have the following result.

Theorem 5.11. *For every $\lambda \in \Lambda$, there exists a monic polynomial $n_\lambda(t) \in \mathbf{Z}[t]$ of degree λ_1 such that, for any discrete valuation ring R with finite residue field of order q, if M is the R-module defined in* (1.2) *and $G = \mathrm{Aut}_R(M)$, then*

$$|G\backslash(M \times M)| = n_\lambda(q).$$

Proof. The only thing that remains to be proved is the assertion about the degree of $n_\lambda(q)$. By Theorem 5.6, we have

$$\deg n_\lambda(q) = \max_{I,J,K}(\deg |X_{I,J,K}| - \deg \alpha_{I,J,K}(q)).$$

Recalling the definitions of $X_{I,J,K}$ and $\alpha_{I,J,K}(q)$, we find that we need to show that

$$[J \cup K]_{\lambda'/I} + \log_q |R\gamma(I)| + [K]_{\lambda''} \leq \lambda_1 + [J \cup K]_\lambda.$$

Observe that $[J \cup K]_\lambda = [J \cup K]_{\lambda'} + [J \cup K]_{\lambda''}$, and $[K]_{\lambda''} \leq [J \cup K]_{\lambda''}$. Moreover, it turns out that $[J \cup K]_{\lambda'/I} \leq [J \cup K]_{\lambda'}$ (see Lemma 5.12 below). Therefore, the inequality to be proved reduces to $\log_q |R\gamma(I)| \leq \lambda_1$, which is obviously true. Furthermore, if equality holds, then $\log_q |R\gamma(I)| = \lambda_1$, which is only possible if I is the maximal ideal in $\mathcal{J}(\mathbf{P})_\lambda$, which was considered in Example 5.8, where a monic polynomial of degree λ_1 was obtained. ☐

Lemma 5.12. *For any ideal $J \in \mathcal{J}(\mathbf{P})_{\lambda'/I}$, we have*

$$[J]_{\lambda'/I} \leq [J]_{\lambda'}.$$

Proof. The partition λ'/I is described in Lemma 6.2. Observe that

$$k_1 \geq v_1 + k_2 - v_2 \geq k_2 \geq v_2 + k_3 - v_2 \geq \cdots \geq v_{s-1} + k_s - v_s \geq v_s.$$

In other words, the parts of λ'/I alternate with the parts of λ'. For each ideal $J \in \mathcal{J}(\mathbf{P})_{\lambda'/I}$, the contribution of J to $[J]_{\lambda'/I}$ in a given chain $(*, v_i + k_{i+1} - v_{i+1}) \subset \mathbf{P}_{\lambda'/I}$ (or $(*, v_s) \subset \mathbf{P}_{\lambda'/I}$) is equal to its contribution to $[J]_{\lambda'}$ in the chain $(*, k_i) \subset \mathbf{P}_{\lambda'}$ (respectively $(*, k_s) \subset \mathbf{P}_{\lambda'}$). It follows that $[J]_{\lambda'/I} \leq [J]_{\lambda'}$. □

6. Orbits in $M_I^* \times M_L^*$

In order to refine Theorem 5.10 to the enumeration of G-orbits in $M_I^* \times M_L^*$ for a pair of order ideals $(I, L) \in \mathcal{J}(\mathbf{P})_\lambda^2$, we need to repeat the calculations in Section 5 with $X_{I,J,K}$ replaced by its subset

$$X_{I,J,K,L} = \{x \in X_{I,J,K} \mid x \in M_L^*\}.$$

Thus our goal is to show that $|X_{I,J,K,L}|$ is a polynomial in q whose coefficients are integers which do not depend on R. By using Möbius inversion on the lattice $\mathcal{J}(\mathbf{P})_\lambda$, it suffices to show that

$$Y_{I,J,K,L} = \{x \in X_{I,J,K} \mid x \in M_L\}$$

has a cardinality given by a polynomial in q whose coefficients are integers which do not depend on R. This is easier, because $x = (x', x'') \in M_L$ if and only if $x' \in M'_L$ and $x'' \in M''_L$. If $(x', x'') \in Y_{I,J,K,L}$, we also have that $x'' \in {M''_K}^*$. Thus $Y_{I,J,K,L} = \emptyset$ unless $K \subset L$. But, if $K \subset L$, then

$$|Y_{I,J,K,L}| = |\{x' \in M'_L \mid I(\bar{x}') = J\}||{M''_K}^*|.$$

Therefore, it suffices to prove the following lemma.

Lemma 6.1. *The cardinality of the set*

$$\{x' \in M' \mid x' \in M'_L \text{ and } I(\bar{x}') = J\}$$

is a polynomial in q whose coefficients are integers which do not depend on R.

Proof. Let $\bar{M}'$ denote the quotient $M'/R\gamma(I)$ (so $\bar{M}'$ is isomorphic to $M_{\lambda'/I}$ in the notation of Section 5). Suppose that $\max I = \{(v_1, k_1), \ldots, (v_s, k_s)\}$. Then

$$M' = R/P^{k_1} \oplus \cdots \oplus R/P^{k_s}.$$

Lemma 6.2. *Let λ'/I denote the partition given by*

$$\lambda'/I = (v_1 + k_2 - v_2, v_2 + k_3 - v_3, \ldots, v_{s-1} + k_s - v_s, v_s),$$

and let $M_{\lambda'/I}$ be the corresponding R-module as given by (1.2)*. If Q is the matrix*

$$Q = \begin{pmatrix} 1 & -\pi^{v_1-v_2} & 0 & \cdots & 0 & 0 \\ 0 & 1 & -\pi^{v_2-v_3} & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\pi^{v_{s-1}-v_s} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

then the isomorphism $R^s \to R^s$ whose matrix is Q descends to a homomorphism $\bar{Q} : M' \to M_{\lambda'/I}$ such that $\ker \bar{Q} \supset R\gamma(I)$. The induced homomorphism $M'/R\gamma(I) \to M_{\lambda'/I}$ is an isomorphism of R-modules.

Proof. Let $e_1, \ldots, e_s$ denote the generators of M', and $f_1, \ldots, f_s$ denote the generators of $M_{\lambda'/I}$. Then

$$Q\tilde{e}_j = \begin{cases} \tilde{f}_1, & \text{for } j = 1, \\ -\pi^{v_{j-1}-v_j}\tilde{f}_{j-1} + \tilde{f}_j, & \text{for } 1 < j \leq n. \end{cases}$$

Here $\tilde{e}_j$ (or $\tilde{f}_i$) denotes the standard lift of e_i (or f_j) to R^s. By using the inequalities $k_j > v_j + k_{j+1} - v_{j+1}$ for $1 \leq j < s$ and $k_s \geq v_s$, one easily verifies that $Q(\pi^{k_j}\tilde{e}_j)$ is 0 in $M_{\lambda'/I}$. Therefore Q induces a well-defined R-module homomorphism $\bar{Q} : M' \to M_{\lambda'/I}$. Now, we have

$$\begin{aligned} \bar{Q}(\gamma(I)) &= \bar{Q}\left(\sum \pi^{v_j} e_j\right) \\ &= \pi^{v_1} f_1 + (-\pi^{v_2+v_1-v_2} f_1 + \pi^{v_2} f_2) + (-\pi^{v_3+v_2-v_3} f_2 + \pi^{v_3} f_2) \\ &\qquad + \cdots + (-\pi^{v_s+v_{s-1}-v_s} f_{s-1} + \pi^{v_s} f_s) \\ &= 0. \end{aligned}$$

Therefore $\bar{Q}$ induces a homomorphism $M'/R\gamma(I) \to M_{\lambda'/I}$. Because $Q \in SL_s(R)$, $\bar{Q}$ is onto. When the residue field of R is finite, one easily verifies that $|R\gamma(I)||M_{\lambda'/I}| = |M'|$, whereby $\bar{Q}$ is an isomorphism. Indeed, $|R\gamma(I)| = q^{k_1-v_1}$, $|M'| = q^{|\lambda'|}$, and $|M_{\lambda'/I}| = q^{|\lambda'/I|} = q^{v_1+k_2+\cdots+k_s}$. In general, this argument using cardinalities can be easily replaced by an argument using the lengths of modules of R. □

We now return to the proof of Lemma 6.1. Using Möbius inversion on the lattice $\mathcal{J}(\mathbf{P}_{\lambda'/I})$, in order to prove Lemma 6.1, it suffices to show that the cardinality of the set

$$S = \{x' \in M' \mid x' \in M'_L \text{ and } \bar{x}' \in (M_{\lambda/I})_J\}$$

is a polynomial in q whose coefficients are integers which do not depend on R. Write $x' \in M'$ as $x'_1 e_1 + \cdots + x'_s e_s$, and $y \in M_{\lambda/I}$ as $y_1 f_1 + \cdots +$

$y_s f_s$. By (2.7) and Lemma 6.2, S consists of elements $m' \in M'$ such that

$$\begin{aligned} v(x_i') &\geq \partial_{k_i} L && \text{for } i = 1, \dots, s, \\ v(\bar{Q}(x')_i) &\geq \partial_{v_i + k_{i+1} - v_{i+1}} J && \text{for } i = 1, \dots, s-1, \text{ and} \\ v(\bar{Q}(x')_s) &\geq \partial_{v_s} J, \end{aligned}$$

which can be rewritten as

$$\begin{aligned} v(x_i') &\geq \partial_{k_i} L && \text{for } i = 1, \dots, s, \\ v(x_i' - \pi^{v_i - v_{i+1}} x_{i+1}') &\geq \partial_{v_i + k_{i+1} - v_{i+1}} J && \text{for } i = 1, \dots, s-1, \text{ and} \\ v(x_s') &\geq \partial_{v_s} J. \end{aligned}$$

Therefore we are free to choose for x_s any element of $R/P^{k_s}R$ which satisfies

$$v(x_s') \geq \max(\partial_{k_s} L, \partial_{v_s} J).$$

Thus the number of possible choices of x_s' of any given valuation is a polynomial in q with coefficients that are integers which do not depend on R. Having fixed x_s', we are free to choose x_{s-1}' satisfying

$$\begin{aligned} v(x_{s-1}') &\geq \partial_{k_{s-1}} L \\ v(x_{s-1}' + \pi^{v_{s-1} - v_s} m_s') &\geq \partial_{v_{s-1} + k_s - v_s} J. \end{aligned}$$

Note that, for any $z, w \in R/P^k R$ and non-negative integers u, v, the cardinality of the set

$$\{z \mid v(z + w) \geq v \text{ and } v(z) = u\}$$

is a polynomial in q with coefficients that are integers which do not depend on R. This shows that, for each fixed valuation of x_s', the number of possible choices for x_{s-1}' of a fixed valuation is again a polynomial in q whose coefficients are integers that do not depend on R. Continuing in this manner, we find that the cardinality of S is a polynomial in q whose coefficients are integers which do not depend on R. $\square$

Proceeding exactly as in the proof of Theorem 5.10, we obtain the following refinement.

Theorem 6.3 (Main theorem)**.** *Let R be a discrete valuation ring with finite residue field of order q. Fix $\lambda \in \Lambda_0$ and take M as in* (1.2)*. Let G denote the group of R-module automorphisms of M. Fix order ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$ (and hence G-orbits M_I^* and M_J^* in M). There exist polynomials $\alpha_1(t), \dots, \alpha_N(t)$, $\beta_1(t), \dots, \beta_N(t)$ with integer coefficients such that, for every discrete valuation ring R with finite residue field of order q, if $M = M_\lambda$ is as in* (1.2) *and G is the group of R-module* *automorphisms of M, then the decomposition of $M_I^* \times M_J^*$ into G-orbits consists of a disjoint union over $i \in \{1, \ldots, N\}$ of $\beta_i(q)$ orbits of cardinality $\alpha_i(q)$.*

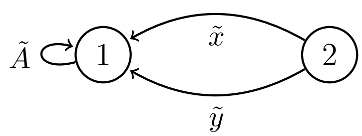
If we are only interested in the number of orbits (and not the number of orbits of a given cardinality), Corollary 4.5 allows us to reduce any $\lambda \in \Lambda$ to $\lambda_2 \in \Lambda_0$.

Theorem 6.4. *For every $\lambda \in \Lambda$ and for all order ideals $I, J \in \mathcal{J}(\mathbf{P})_\lambda$, there exists a polynomial $n_{\lambda,I,J}(t) \in \mathbf{Z}[t]$ such that, whenever R is a discrete valuation ring with finite residue field of order q, M is the R-module given by* (1.2) *and $G = \mathrm{Aut}_R(M)$, we have*

$$|G\backslash(M_I^* \times M_J^*)| = n_{\lambda,I,J}(q).$$

7. Relation to representations of quivers

Consider the quiver Q represented by



To an $n \times n$ matrix A and two n-vectors x and y (all with coordinates in a finite field $\mathbf{F}_q$ of order q), we may associate a representation of this quiver with dimension vector $(n, 1)$ by taking $V_1 = \mathbf{F}_q^n$, $V_2 = \mathbf{F}_q$, the linear map corresponding to the arrow $\tilde{A}$ given by A, the linear maps corresponding to the arrows $\tilde{x}$ and $\tilde{y}$ being those which take the unit in $V_2 = \mathbf{F}_q$ to the vectors x and y, respectively. The representations corresponding to triples (A, x, y) and (A, x', y') are isomorphic if and only if there exists an element $g \in GL_n(\mathbf{F}_q)$ such that

$$gAg^{-1} = A, \; gx = x', \; gy = y'.$$

Thus, the isomorphism classes of representations of Q are in bijective correspondence with triples (A, x, y) consisting of an $n \times n$ matrix and two n-vectors up to a simultaneous change of basis.

If we view $\mathbf{F}_q^n$ as an $\mathbf{F}_q[t]$-module M^A where t acts via the matrix A, then the number of isomorphism classes of representations of the form (A, x, y) with A fixed may be interpreted as the number of $G^A = \mathrm{Aut}_{k[t]} M$-orbits in $M^A \times M^A$. The total number of isomorphism classes of representations of Q with dimension vector $(n, 1)$ is given by

$$R_{n,1}(q) = \sum_A |G^A\backslash(M^A \times M^A)|, \tag{7.1}$$

where A runs over a set of representatives for the similarity classes in $M_n(k)$. This polynomial was introduced by Kac in [8], where he asserted that, for any quiver, the number of isomorphism classes of representations with a fixed dimension vector is a polynomial in q with integer coefficients. He conjectured the non-negativity of a related polynomial (which counts the number of isomorphism classes of absolutely indecomposable representations) from which the non-negativity of coefficients of $R_{n,1}(q)$ follows (see Hua [7]). Kac's conjecture was proved by Hausel, Letellier and Rodriguez-Villegas [6] recently.

We now explain how the results of this paper (together with Green's theory of types of matrices [5]) enable us to compute the right-hand side of (7.1). Let $\mathrm{Irr}\,\mathbf{F}_q[t]$ denote the set of irreducible monic polynomials in $\mathbf{F}_q[t]$. Let Λ_0 denote the subset of Λ consisting of elements λ of type (1.1) for which all the cardinals m_i are finite (this is just the set of all partitions). For $\lambda \in \Lambda_0$ as in (1.1), let $|\lambda| = \sum m_i\lambda_i$. Recall that similarity classes of $n\times n$ matrices with entries in $\mathbf{F}_q$ are parametrized by functions

$$c : \mathrm{Irr}\,\mathbf{F}_q[t] \to \Lambda_0$$

such that

$$\sum_{f\in \mathrm{Irr}\,\mathbf{F}_q[t]} (\deg f)|c(f)| = n.$$

The above condition imposes the constraint that $c(f)$ is the empty partition $\emptyset$ with $|\emptyset| = 0$ for all but finitely many $f \in \mathrm{Irr}\,\mathbf{F}_q[t]$. The similarity classes parametrized by c and c' are said to be of the same type if there exists a degree-preserving bijection $\sigma : \mathrm{Irr}\,\mathbf{F}_q[t] \to \mathrm{Irr}\,\mathbf{F}_q[t]$ such that $c' = c\circ\sigma$.

Given a function $c : \mathrm{Irr}\,\mathbf{F}_q[t] \to \Lambda_0$ parametrizing a similarity class of $n\times n$ matrices, let τ_c denote the multiset of pairs $(c(f), \deg f)$ as f ranges over the set of irreducible polynomials in $\mathbf{F}_q[t]$ for which $c(f) \neq \emptyset$. Then c and c' are of the same type if and only if $\tau_c = \tau_{c'}$. Thus, the set of types of $n\times n$ matrices with entries in $\mathbf{F}_q$ is parametrized by multisets of the form

$$\tau = \{(\lambda^{(1)}, d_1)^{a_1}, (\lambda^{(2)}, d_2)^{a_2}, \dots\} \tag{7.2}$$

such that

$$\sum_i a_i d_i |\lambda^{(i)}| = n. \tag{7.3}$$

Let $T(n)$ denote the set of multisets of pairs in $\Lambda_0 \times \mathbf{Z}_{>0}$ satisfying (7.3). For example, $T(2)$ has four elements given by:

- $\{((1,1),1)\}$ (central type);
- $\{((2),1)\}$ (non-semisimple type);

- $\{((1), 2)\}$ (irreducible type);
- $\{((1), 1)^2\}$ (split regular semisimple type).

If A is an $n \times n$ matrix of type τ as in (7.2), then, by primary decomposition,

$$n_\tau(q) = |G^A \backslash M^A \times M^A| = \prod_i n_{\lambda^{(i)}}(q^{d_i}),$$

where $n_\lambda(q)$ denotes the cardinality of $|G_\lambda \backslash (M_\lambda \times M_\lambda)|$ when the residue field of R has cardinality q. It is also easy to enumerate the number of similarity classes of a given type τ: for each positive integer d, let m_d denote the number of times a pair of the form (λ, d) occurs in τ (counted with multiplicity). Let $\Phi_d(q)$ denote the number of irreducible polynomials in $\mathbf{F}_q[t]$ of degree d in $\mathbf{F}_q[t]$. This is a polynomial in q with rational coefficients,

$$\Phi_d(q) = \frac{1}{d} \sum_{e|d} \mu(d/e) q^e,$$

where μ is the classical Möbius function. The number of similarity classes of type τ is

$$c_\tau(q) = \frac{1}{\prod_i a_i!} \prod_d \Phi_d(q)(\Phi_d(q) - 1) \cdots (\Phi_d(q) - m_d + 1).$$

We obtain a formula for $R_{n,1}(q)$,

$$R_{n,1}(q) = \sum_{\tau \in T(n)} c_\tau(q) n_\tau(q), \tag{7.4}$$

which can also be expressed as a product expansion for the generating function of $R_{n,1}(q)$ in the spirit of Kung [10] and Stong [13]:

$$\sum_{n=0}^{\infty} R_{n,1}(q) x^n = \prod_{d=1}^{\infty} \left(\sum_{\lambda \in \Lambda_0} n_\lambda(q^d) x^{d|\lambda|} \right)^{\Phi_d(q)}. \tag{7.5}$$

There is an alternative method for computing $R_{n,1}(q)$, namely the Kac–Stanley formula [8, p. 90], which is based on Burnside's lemma and a theory of types adapted to quivers (this formula is a way to compute the number of isomorphism classes of representations of a quiver with any dimension vector). A comparison of the values obtained for $R_{n,1}(q)$ using these two substantially different methods verifies the validity of our results. This has been carried out by computer for values of n up to 18 (the code for this can be found at `http://www.imsc.res.in/~amri/pairs/`).

Acknowledgment

We thank Kunal Dutta, who went through the paper carefully and pointed out several corrections. We also thank an anonymous referee whose suggestions have significantly improved our exposition.

References

[1] G. Birkhoff. Subgroups of Abelian groups. *Proc. London Math. Soc. (2)*, 38(1):385–401, 1935.

[2] W. Calvert, K. Dutta, and A. Prasad. Degeneration and orbits of tuples and subgroups in an abelian group. *J. Group Theory*, 16(2):221–233, 2013.

[3] U. V. Dubey, A. Prasad, and P. Singla. The Cartan matrix of a centraliser algebra. *Proc. Indian Acad. Sci. Math. Sci.*, 122(1):67–73, 2012.

[4] K. Dutta and A. Prasad. Degenerations and orbits in finite abelian groups. *J. Combin. Theory Ser. A*, 118(6):1685–1694, 2011.

[5] J. A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, 80:402–447, 1955.

[6] T. Hausel, E. Letellier, and F. Rodriguez-Villegas. Positivity of Kac polynomials and DT-invariants for quivers. *Ann. of Math. (2)*, 177:1147–1186, 2013.

[7] J. Hua. *Representations of quivers over finite fields*. Ph.D. thesis, University of New South Wales, 1998.

[8] V. G. Kac. Root systems, representations of quivers and invariant theory. In: *Invariant theory*, pp. 74–108. Springer, 1983.

[9] B. L. Kerby and E. Rode. Characteristic subgroups of finite abelian groups. *Commun. Algebra*, 39(4):1315–1343, 2011.

[10] J. P. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra Appl.*, 36:141–155, 1981.

[11] G. A. Miller. Determination of all the characteristic subgroups of any abelian group. *Amer. J. Math.*, 27(1):15–24, 1905.

[12] M. Schwachhöfer and M. Stroppel. Finding representatives for the orbits under the automorphism group of a bounded abelian group. *J. Algebra*, 211(1):225–239, 1999.

[13] R. Stong. Some asymptotic results on finite vector spaces. *Adv. Appl. Math.*, 9(2):167–199, 1988.

The Institute of Mathematical Sciences, Chennai.