Rational Invariants of Finite Abelian Groups

Evelyne Hubert [*] George Labahn [†]

January 20, 2014

Abstract

We investigate the field of rational invariants of the linear action of a finite abelian group in the non modular case. By diagonalization, the group is accurately described by an integer matrix of exponents. We make use of linear algebra to compute a minimal generating set of invariants and the substitution to rewrite any invariant in terms of this generating set. We show that the generating set can be chosen to consist of polynomial invariants. As an application, we provide a symmetry reduction scheme for polynomial systems the solution set of which are invariant by the group action. We furthermore provide an algorithm to find such symmetries given a polynomial system.

Keywords: Finite groups, Rational invariants, Matrix normal form, Polynomial system reduction.

1 Introduction

Recently Faugère and Svartz [5] demonstrated how to reduce the complexity of Gröbner bases computations for ideals stable by the linear action of a finite abelian group. Their strategy is based on the diagonalization of the group. It turns out that these diagonal actions have strong similarities with scalings which the present authors previously investigated in [14, 15]. Scalings are diagonal representations of tori and can be defined by a matrix of exponents. Integer linear algebra was used to compute the invariants of scalings and develop their applications in [14, 15]. It was shown that the unimodular multipliers associated to the Hermite form of the exponent matrix provide the exponents of monomials that describe a minimal generating set of invariants and rewrite rules.

In this article we specify diagonal representations of finitely generated abelian groups with a similar exponent matrix. When the group is finite, an order matrix is also needed. We show that analogous, though slightly more complex, results can then be established for determining generating sets of invariants and rewrite rules. From a unimodular multiplier associated to the Hermite form of the exponent and order matrices, we can compute a minimal set of generating rational invariants. This provides a direct constructive proof of the rationality of the field of invariants. More remarkable is the fact that any other invariant can be written in terms of these by an explicit substitution. An additional important feature is that we can choose the generating set of invariants to consist of monomials with nonnegative powers. Such a set comes with a triangular shape and provides generators for an algebra that is an explicit localization of the polynomial ring of invariants.

As an application we show how one can reduce a system of polynomial equations, whose solution set is invariant by the linear action of an abelian group, into a reduced system of polynomial equations, with the invariants as new variables. The reduced system has the order of the group times less solutions than

[*] INRIA Méditerranée, 06902 Sophia Antipolis, France evelyne.hubert@inria.fr

[†] Cheriton School of Computer Science, University of Waterloo, Waterloo ON, Canada N2L 3G1 glabahn@uwaterloo.ca

the original system while keeping the number of variables the same. Each of its solution correspond to an orbit of solutions of the original system and these are retrieved as the solutions of a binomial triangular set. To compute the reduced system, we first adapt a concept of degree from [5] to split the polynomials in the system into invariants. We then use our special set of polynomial invariants along with the associated rewrite rules to obtain the reduced system. The main cost of the reduction is a Hermite form computation, which in our case is $O((n+s)^4 d)$ where n is the number of variables in the polynomial system, s is the number of generators of the finite group and d is the log of the order of the group. The distinctive feature of our approach is that it organizes the solutions of the original system in orbits of solutions. They can thus be presented qualitatively, in particular when ultimately dealing with groups of permutations.

The above strategy, and alternatively [5], for polynomial system solving, start from the knowledge of the symmetry of the solution set. Though it is often intrinsically known, we provide a way to determine those. In [15] we determined the scaling symmetry, by determining its exponent matrix through the computation of the Hermite form of the matrix of exponents of the terms in the polynomials. The problem here is to determine both the exponent matrix and the orders of the group. This is solved by computing the Smith normal form of the matrix of exponents of the terms in the polynomials. We show that the order matrix is read on the Smith normal form itself, while the exponent matrix is read on the left unimodular multiplier. Additionally, a generating set of invariants for the diagonal group hence defined is obtained directly from the right unimodular multiplier. The Smith normal form and its unimodular multipliers thus provide all the ingredients for a symmetry reduction scheme.

The results generalize to linear representations of finite abelian groups. In the non-modular case, the action can be diagonalized, possibly over an extension of the base field. As a result, the field of rational invariants for an n-dimensional representation of an abelian group is generated by n polynomial invariants and any invariant can be to written in terms of these generators by an explicit substitution. This result on the field of rational invariants is to be contrasted to the situation for the ring of polynomial invariants. There the minimal number of algebra generators can be combinatorially high, even in the basic case of cyclic groups.

The computational efforts for invariant theory have focused on the ring of polynomial invariants [29, 3]. Yet some applications can be approached with rational invariants[1]. Indeed a generating set of rational invariants separates generic orbits. It is therefore applicable to the equivalence problem that come in many guises. The class of rational invariants can furthermore address a wider class of nonlinear actions, such as those central in differential geometry[2] and algebraically characterize classical differential invariants [13, 10]. General algorithms to compute rational invariants of (rational) action of algebraic groups [11, 12, 16, 17, 19] rely on Gröbner bases computations. It is remarkable how much simpler and more effective the present approach is for use with abelian groups.

The remainder of the paper is organized as follows. Preliminary information about diagonal actions, their defining exponent and order matrices, as well as integer linear algebra are to be found in the next section. Section 3 shows the use of integer linear algebra to determine invariants of the diagonal action of finite groups, giving the details of invariant generation and rewrite rules. We discuss there polynomial invariants as well. Section 4 deals with the case of arbitrary finite abelian group actions including examples illustrating our methods. Section 5 gives the details of the symmetry reduction scheme for polynomial systems, including an example of solving a polynomial system coming from neural networks. Section 6 considers the problem of finding a representation of a finite abelian group that provides a symmetry for the solution set of a given set of polynomials equations. Finally, we present a conclusion along with topics for future research.

Acknowledgement: Part of this research was conducted when both authors were hosted by the Institute of Mathematical Sciences in the National University of Singapore during the amazing program *Inverse Moment Problems: the Crossroads of Analysis, Algebra, Discrete Geometry and Combinatorics.* Many thanks to Dimitrii Pasechnik and Sinai Robins, Nanyang Technological University, the organizers.

[1] For instance multi-homogeneous polynomial system solving in [14] and parameter reduction in dynamical models [15].

[2] For example, conformal transformations or prolonged actions to the jet spaces.

2 Preliminaries

In this section we introduce our notations for finite groups of diagonal matrices and their linear actions. We shall use the matrix notations that were already introduced in [14, 15]. In addition we will present the various notions from integer linear algebra used later in this work.

2.1 Matrix notations for monomial maps

Let $\mathbb{K}$ be a field and denote $\mathbb{K} \setminus \{0\}$ by $\mathbb{K}^*$. If $a = {}^t[a_1, \ldots, a_s]$ is a column vector of integers and $\lambda = [\lambda_1, \ldots, \lambda_s]$ is a row vector with entries in $\mathbb{K}^*$, then λ^a denotes the scalar

$$\lambda^a = \lambda_1^{a_1} \cdots \lambda_s^{a_s}.$$

If $\lambda = [\lambda_1, \ldots, \lambda_s]$ is a row vector of r indeterminants, then λ^a can be understood as a monomial in the Laurent polynomial ring $\mathbb{K}[\lambda, \lambda^{-1}]$, a domain isomorphic to $\mathbb{K}[\lambda, \mu]/(\lambda_1\mu_1 - 1, \ldots, \lambda_s\mu_s - 1)$. We extend this notation to matrices. If A is an $s \times n$ matrix with entries in $\mathbb{Z}$ then λ^A is the row vector

$$\lambda^A = [\lambda^{A_{\cdot,1}}, \cdots, \lambda^{A_{\cdot,n}}]$$

where $A_{\cdot,1}, \ldots, A_{\cdot,n}$ are the n columns of A.

If $x = [x_1, \ldots, x_n]$ and $y = [y_1, \ldots, y_n]$ are two row vectors, we write $x \star y$ for the row vector obtained by component wise multiplication:

$$x \star y = [x_1y_1, \ldots, x_ny_n]$$

Assume A and B are integer matrices of size $s \times n$ and C of size $n \times r$; λ, x and y are row vectors with s components. It is easy to prove [14] that

$$\lambda^{A+B} = \lambda^A \star \lambda^B, \quad \lambda^{AC} = (\lambda^A)^C, \quad (y \star z)^A = y^A \star z^A.$$

Furthermore if $A = [A_1, A_2]$ is a partition of the columns of A, then $\lambda^A = [\lambda^{A_1}, \lambda^{A_2}]$.

2.2 Finite groups of diagonal matrices

Consider the group $\mathcal{Z} = \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$. Throughout this paper we assume that the characteristic of $\mathbb{K}$ does not divide $p = \operatorname{lcm}(p_1, \ldots, p_s)$. Furthermore we assume that $\mathbb{K}$ contains a pth primitive root of unity ξ. Then $\mathbb{K}$ contains a p_ith primitive root of unity, which can be taken as $\xi_i = \xi^{\frac{p}{p_i}}$, for all $1 \leq i \leq s$.

An integer matrix $A \in \mathbb{Z}^{s\times n}$ defines an n-dimensional diagonal representation of this group given as

$$\begin{array}{ccc} \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s} & \to & \mathrm{GL}_n(\mathbb{K}) \\ (m_1, \ldots, m_s) & \mapsto & \operatorname{diag}\left((\xi_1^{m_1}, \ldots \xi_s^{m_s})^A\right). \end{array}$$

The image of the group morphism above is a subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$. We shall speak of $\mathcal{D}$ as the finite group of diagonal matrices defined by the *exponent matrix* $A \in \mathbb{Z}^{s\times n}$ and *order matrix* $P = \operatorname{diag}(p_1, \ldots, p_s) \in \mathbb{Z}^{s\times s}$.

Let $\mathbb{U}_{p_i}$ be the group of the p_ith roots of unity. The group $\mathcal{Z} = \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$ is isomorphic to the group $\mathcal{U} = \mathbb{U}_{p_1} \times \ldots \times \mathbb{U}_{p_s}$, an isomorphism given explicitly by $(m_1, \ldots, m_s) \mapsto (\xi_1^{m_1}, \ldots, \xi_s^{m_s})$. The group $\mathcal{D}$ of diagonal matrices defined by an exponent and order matrix $A \in \mathbb{Z}^{s\times n}$ and $P = \operatorname{diag}(p_1, \ldots, p_s)$ is also the image of the representation

$$\begin{array}{ccc} \mathcal{U} & \to & \mathrm{GL}_n(\mathbb{K}) \\ \lambda & \mapsto & \operatorname{diag}(\lambda^A). \end{array}$$

The induced linear action of $\mathcal{U}$ on $\mathbb{K}^n$ is then conveniently noted

$$\begin{array}{ccc} \mathcal{U}\times\mathbb{K}^n & \rightarrow & \mathbb{K}^n \\ (\lambda, z) & \mapsto & \lambda^A \star z. \end{array}$$

One then draws a clear analogy with [14, 15] where we dealt with the group $(\mathbb{K}^*)^r$ instead of $\mathcal{U}$. We shall alternatively use the two representations for convenience of notations.

Example 2.1 *Let $\mathcal{D}$ be the subgroup of $\mathrm{GL}_3(\mathbb{K})$ generated by*

$$I_\xi = \begin{bmatrix} \xi & & \\ & \xi & \\ & & \xi \end{bmatrix} \text{ and } M_\xi = \begin{bmatrix} \xi & & \\ & \xi^2 & \\ & & 1 \end{bmatrix}.$$

where $\xi^2+\xi+1=0$, that is, ξ is a primitive 3rd root of unity. $\mathcal{D}$ is the (diagonal matrix) group specified by $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ with order matrix $P = \begin{bmatrix} 3 & \\ & 3 \end{bmatrix}$. In other words $\mathcal{D}$ is the image of the representation of $\mathbb{Z}_3 \times \mathbb{Z}_3$ explicitly given by

$$(m,n) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \mapsto \begin{bmatrix} \xi^m\xi^n & & \\ & \xi^m\xi^{2\,n} & \\ & & \xi^m \end{bmatrix} \in \mathcal{D}.$$

Example 2.2 *Let $\mathcal{D}$ be the subgroup of $\mathrm{GL}_3(\mathbb{K})$ generated by*

$$I_\zeta = \begin{bmatrix} \zeta & & \\ & \zeta & \\ & & \zeta \end{bmatrix} \text{ and } M_\xi = \begin{bmatrix} \xi & & \\ & \xi^2 & \\ & & 1 \end{bmatrix}.$$

where $\zeta+1=0$ and $\xi^2+\xi+1=0$. $\mathcal{D}$ is the (diagonal matrix) group specified by $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ with order matrix $P = \begin{bmatrix} 2 & \\ & 3 \end{bmatrix}$. In other words $\mathcal{D}$ is the image of the representation of $\mathbb{Z}_2 \times \mathbb{Z}_3$ explicitly given by

$$(m,n) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \mapsto \begin{bmatrix} \zeta^m\xi^n & & \\ & \zeta^m\xi^{2\,n} & \\ & & \zeta^m \end{bmatrix} \in \mathcal{D}.$$

Obviously $\mathbb{Z}_2 \times Z_3$ is isomorphic to $\mathbb{Z}_6$ and $\mathcal{D}$ is also obtained as the image of the representation

$$k \in \mathbb{Z}_6 \mapsto \begin{bmatrix} \eta^k & & \\ & \eta^{-k} & \\ & & \eta^{3k} \end{bmatrix} \in \mathcal{D}$$

where $\eta = \zeta\xi$ is a primitive 6^{th} root of unity. Thus $\mathcal{D}$ is also specified by $A = \begin{bmatrix} 1 & -1 & 3 \end{bmatrix}$ with order matrix $P = \begin{bmatrix} 6 \end{bmatrix}$.

Just as in the example above, any finite abelian group is isomorphic to $\mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$ where $p_1|p_2|\ldots|p_s$ [25]. In this article we do not enforce this canonical divisibility condition. It nonetheless appears naturally when we look for the group of homogeneity of a set of rational functions is computed in Section 6. We shall then see how to *normalize* the group and actually find an equivalent faithful representation.

2.3 Integer linear algebra

Every $s \times (n+s)$ integer matrix can be transformed via integer column operations to obtain a unique *column Hermite form* [24]. In the case of a full rank matrix the Hermite normal form is an upper triangular matrix with positive nonzero entries on the diagonal, nonnegative entries in the rest of the first s columns and zeros in the last n columns. Furthermore the diagonal entries are bigger than the corresponding entries in each row.

The column operations for constructing a Hermite normal form are encoded in unimodular matrices, that is, invertible integer matrices whose inverses are also integer matrices. Thus for each $\hat{A} \in \mathbb{Z}^{s\times(n+s)}$ there exists a unimodular matrix $V \in \mathbb{Z}^{(n+s)\times(n+s)}$ such that $\hat{A}\,V$ is in Hermite normal form. In this paper the unimodular multiplier plays a bigger role than the Hermite form itself. For ease of presentation a unimodular matrix V such that $\hat{A}\,V$ is in Hermite normal form will be referred to as a *Hermite multiplier* for $\hat{A}$.

We consider the group $\mathcal{D}$ of diagonal matrices determined by the exponent matrix $A \in \mathbb{Z}^{s\times n}$ and the order matrix $P \in \mathbb{Z}^{s\times s}$. Consider the Hermite normal form

$$\begin{bmatrix} A & -P \end{bmatrix} V = \begin{bmatrix} H & 0 \end{bmatrix}$$

with $H \in \mathbb{Z}^{s\times s}$ and a Hermite multiplier V partitioned as

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} \tag{1}$$

with $V_{\mathfrak{i}} \in \mathbb{Z}^{n\times s}$, $V_{\mathfrak{n}} \in \mathbb{Z}^{n\times n}$, $P_{\mathfrak{i}} \in \mathbb{Z}^{s\times s}$, $P_{\mathfrak{n}} \in \mathbb{Z}^{s\times n}$. Breaking the inverse of V into the following blocks

$$V^{-1} = W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} \tag{2}$$

where $W_{\mathfrak{u}} \in \mathbb{Z}^{s\times n}$, $W_{\mathfrak{d}} \in \mathbb{Z}^{n\times n}$, $P_{\mathfrak{u}} \in \mathbb{Z}^{s\times s}$, $P_{\mathfrak{d}} \in \mathbb{Z}^{n\times s}$ we then have the identities

$$V_{\mathfrak{i}}W_{\mathfrak{u}} + V_{\mathfrak{n}}W_{\mathfrak{d}} = I_n, \quad V_{\mathfrak{i}}P_{\mathfrak{u}} + V_{\mathfrak{n}}P_{\mathfrak{d}} = 0, \quad P_{\mathfrak{i}}W_{\mathfrak{u}} + P_{\mathfrak{n}}W_{\mathfrak{d}} = 0, \quad P_{\mathfrak{i}}P_{\mathfrak{u}} + P_{\mathfrak{n}}P_{\mathfrak{d}} = 0$$

and

$$W_{\mathfrak{u}}V_{\mathfrak{i}} + P_{\mathfrak{u}}P_{\mathfrak{i}} = I, \quad W_{\mathfrak{u}}V_{\mathfrak{n}} + P_{\mathfrak{n}}P_{\mathfrak{d}} = 0, \quad W_{\mathfrak{d}}V_{\mathfrak{i}} + P_{\mathfrak{d}}P_{\mathfrak{i}} = 0, \quad W_{\mathfrak{d}}V_{\mathfrak{n}} + P_{\mathfrak{d}}P_{\mathfrak{n}} = I.$$

Furthermore

$$AV_{\mathfrak{i}} - PP_{\mathfrak{i}} = H, \quad AV_{\mathfrak{n}} - PP_{\mathfrak{n}} = 0, \quad A = HW_{\mathfrak{u}} \quad \text{and} \quad P = -HP_{\mathfrak{u}}.$$

From the last equality we see that $P_{\mathfrak{u}}$ is upper triangular and the ith diagonal entry of H divides p_i.

The indices were chosen in analogy to [14, 15]. The index $\mathfrak{i}$ and $\mathfrak{n}$ stand respectively for *image* and *nullspace*, while $\mathfrak{u}$ and $\mathfrak{d}$ stand respectively for *up* and *down*.

Example 2.3 *Let $A \in \mathbb{Z}^{2\times 3}$ and $P =$ diag$(3,3)$ be the exponent and order matrices that defined the group of diagonal matrices in Example 2.1. In this case $[A \quad -P]$ has Hermite form $[I_2 \quad 0]$ with Hermite multiplier*

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} = \left[\begin{array}{cc|ccc} 0 & 1 & 1 & 2 & -2 \\ 0 & 3 & -2 & 2 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & -1 & 2 & 0 \end{array}\right] \text{ and inverse } W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} = \left[\begin{array}{ccc|cc} 1 & 1 & 1 & -3 & 0 \\ 1 & 2 & 0 & 0 & -3 \\ \hline 0 & 0 & 0 & 2 & -1 \\ -1 & -2 & 0 & 1 & 3 \\ -1 & -1 & 0 & 2 & 1 \end{array}\right].$$

The Hermite multiplier is not unique. For example in this case a second set of unimodular multipliers satisfying $[A \quad -P]\,V = [I_2 \quad 0]$ and $W = V^{-1}$ are given by

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} = \left[\begin{array}{cc|ccc} 2 & -1 & 3 & 0 & 1 \\ 1 & 1 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 \end{array}\right], \quad W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} = \left[\begin{array}{ccc|cc} 1 & 1 & 1 & -3 & 0 \\ 0 & 1 & 2 & 0 & -3 \\ \hline 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right].$$

As noted in Example 2.3, Hermite multipliers are not unique. Indeed any column operations on the last n columns leaves the Hermite form intact. Similarly one can use any of the last n columns to eliminate entries in the first s columns without affecting the Hermite form. We say V is a *normalized Hermite multiplier* if it is a Hermite multiplier where V_n is also in Hermite form and where V_i is reduced with respect to the columns of V_n.

Lemma 2.4 *We can always choose a Hermite multiplier*

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix}$$

for $[A \quad -P]$ *such that*

$$\begin{bmatrix} 0 & I_n \\ -P & A \end{bmatrix} \cdot \begin{bmatrix} P_{\mathfrak{n}} & P_{\mathfrak{i}} \\ V_{\mathfrak{n}} & V_{\mathfrak{i}} \end{bmatrix} = \begin{bmatrix} V_{\mathfrak{n}} & V_{\mathfrak{i}} \\ 0 & H \end{bmatrix} \tag{3}$$

is in column Hermite form. Then V *is the normalized Hermite multiplier for* $[A \quad -P]$.

Taking determinants on both sides of Equation (3) combined with the fact that diagonal entries of a Hermite form are positive gives the following corollary.

Corollary 2.5 *Let* V *be the normalized Hermite multiplier for* $[A \quad -P]$ *with Hermite form* $[H \quad 0]$*. Then* $V_{\mathfrak{n}}$ *is nonsingular and*

$$p_1 \cdot p_2 \cdots p_s = \ det\ (H) \cdot \ det\ (V_{\mathfrak{n}}). \tag{4}$$

The uniqueness of $V_{\mathfrak{n}}$ in the normalized Hermite multiplier is guaranteed by the uniqueness of the Hermite form for full rank square matrices. While the notion of normalized Hermite multiplier appears to only involve $V_{\mathfrak{i}}$ and $V_{\mathfrak{n}}$ and does not say anything about $P_{\mathfrak{i}}$ nor $P_{\mathfrak{n}}$ it is the additional fact that V is a Hermite multiplier that ensures uniqueness.

Lemma 2.4 also tells us about the cost of finding a normalized Hermite form. Indeed the cost is $O((n+s)^4 d)$ where d is the size of the largest p_i (c.f. [26, 27]). Furthermore, since V is produced from column operations the W matrix can be computed simultaneously with minimal cost by the inverse column operations.

It will also be useful later on to have a formula for the inverse of $V_{\mathfrak{n}}$.

Lemma 2.6 *With* V *and* W *partitioned as (1) and (2) we have that*

$$V_{\mathfrak{n}}^{-1} = W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}.$$

PROOF: Note first that $P_{\mathfrak{u}}$ is nonsingular since $H \cdot P_{\mathfrak{u}} = -P$ and H is nonsingular. The result follows $V \cdot W = I$ along with

$$\begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} \begin{bmatrix} I & 0 \\ -P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} & P_{\mathfrak{u}}^{-1} \end{bmatrix} = \begin{bmatrix} 0 & I \\ W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} & P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} \end{bmatrix}. \tag{5}$$

since these two imply that $V_{\mathfrak{n}} \cdot (W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}) = I_n$. □

Since we can compute V and its inverse W simultaneously, the formula in Lemma 2.6 for the inverse of $V_{\mathfrak{n}}$ has the advantage that it requires the inversion of a smaller $s \times s$ triangular matrix $P_{\mathfrak{u}}$. Furthermore the proof of Lemma 2.6 using equation (5) implies that $(W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}})$ is the Schur complement of $P_{\mathfrak{u}}$ in the matrix

$$W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix}.$$

The Schur complement in this case describes the column operations that eliminate the top left matrix in W.

3 Invariants of finite groups of diagonal matrices

We consider $A \in \mathbb{Z}^{s\times n}$ a full row rank matrix, $P = \operatorname{diag}(p_1,\dots,p_s)$, where $p_i \in \mathbb{N}$, and $\mathbb{K}$ a field whose characteristic does not divide $p = \operatorname{lcm}(p_1,\dots,p_s)$. In addition we assume that $\mathbb{K}$ contains a pth primitive root of unity. The pair (A, P) thus defines a finite group $\mathcal{D}$ of diagonal matrices that can be seen as a n-dimensional representation of $\mathcal{U} = \mathbb{U}_{p_1} \times \ldots \times \mathbb{U}_{p_s}$, where $\mathbb{U}_{p_i}$ is the group of p_ith roots of unity. With the matrix notations introduced in Section 2, the induced linear action is given as

$$\begin{array}{ccc} \mathcal{U}\times\mathbb{K}^n & \to & \mathbb{K}^n \\ (\lambda, z) & \mapsto & \lambda^A \star z. \end{array}$$

A *rational invariant* is an element f of $\mathbb{K}(z)$ such that $f(\lambda^A \star z) = f(z)$ for all $\lambda \in \mathcal{U}$. Rational invariants form a subfield $\mathbb{K}(z)^{\mathcal{D}}$ of $\mathbb{K}(z)$. In this section we show how a Hermite multiplier V of $[A \quad -P]$ provides a complete description of the field of rational invariants. Indeed we will show that the matrix V along with its inverse W provide both a generating set of rational invariants and a simple rewriting of any invariant in terms of this generating set. In a second stage we exhibit a generating set that consists of a triangular set of monomials with nonnegative powers for which we can bound the degrees. This leads us to also discuss the invariant polynomial ring.

3.1 Generating invariants and rewriting

We recall our notations for the Hermite form introduced in the previous section :

$$\begin{bmatrix} A & -P \end{bmatrix} V = \begin{bmatrix} H & 0 \end{bmatrix}$$

with a Hermite multiplier V and its inverse W partitioned as

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix}, \quad W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix}.$$

A Laurent monomial z^v, $v \in \mathbb{Z}^n$, is invariant if $(\lambda^A \star z)^v = z^v$ for any $\lambda \in \mathcal{U}$. This amounts to $\lambda^{Av} = 1$, for all $\lambda \in \mathcal{U}$. When we considered the action of $(\mathbb{K}^*)^r$ in [14, 15] then z^v was invariant if and only if $Av = 0$. In the present case we have:

Proposition 3.1 *For $v \in \mathbb{Z}^n$, the Laurent monomial z^v is invariant if and only if $v \in colspan_{\mathbb{Z}} V_{\mathfrak{n}}$.*

PROOF: Assume z^v is invariant. Then $Av = 0 \mod {}^t(p_1,\dots,p_s)$, that is, there exists $k \in \mathbb{Z}^s$ such that $\begin{bmatrix} v \\ k \end{bmatrix} \in \ker_{\mathbb{Z}} \begin{bmatrix} A & -P \end{bmatrix} = \operatorname{colspan}_{\mathbb{Z}} \begin{bmatrix} V_{\mathfrak{n}} \\ P_{\mathfrak{n}} \end{bmatrix}$. Hence $v \in \operatorname{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$. Conversely if $v \in \operatorname{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ there exists $u \in \mathbb{Z}^n$ such that $v = V_{\mathfrak{n}} u$. Since $AV_{\mathfrak{n}} = PP_{\mathfrak{n}}$ we have $Av = Pk$ for $k = P_{\mathfrak{n}} u \in \mathbb{Z}^s$. Thus z^v is invariant. □

The following lemma shows that rational invariants of a diagonal action can be written as a rational function of invariant Laurent monomials. This can be proved by specializing more general results on generating sets of rational invariants and the multiplicative groups of monomials [23]. We choose to present this simple and direct proof as it guides us when building a group of symmetry for a set of polynomials of rational functions in Section 6.

Lemma 3.2 *Suppose $\frac{p}{q} \in \mathbb{K}(z)^{\mathcal{D}}$, with $p, q \in \mathbb{K}[z]$ relatively prime. Then there exists $u \in \mathbb{Z}^n$ such that*

$$p(z) \quad = \sum_{v \,\in\, colspan_{\mathbb{Z}} V_{\mathfrak{n}}} a_v \, z^{u+v} \quad \text{and} \quad q(z) \quad = \sum_{v \,\in\, colspan_{\mathbb{Z}} V_{\mathfrak{n}}} b_v \, z^{u+v}$$

where the families of coefficients, $(a_v)_v$ and $(b_v)_v$, have finite support.[3]

[3] In particular $a_v = 0$ (respectively $b_v = 0$) when $u + v \notin \mathbb{N}^n$.

PROOF: We take advantage of the more general fact that rational invariants of a linear action on $\mathbb{K}^n$ are quotients of semi-invariants. Indeed, if p/q is a rational invariant, then

$$p(z)\, q(\lambda^A \star z) = p(\lambda^A \star z)\, q(z)$$

in $\mathbb{K}(\lambda)[z]$. As p and q are relatively prime, $p(z)$ divides $p(\lambda^A \star z)$ and, since these two polynomials have the same degree, there exists $\chi(\lambda) \in \mathbb{K}$ such that $p(\lambda^A \star z) = \chi(\lambda)\, p(z)$. It then also follows that $q(\lambda^A \star z) = \chi(\lambda)\, q(z)$.

Let us now look at the specific case of a diagonal action. Then

$$p(z) = \sum_{w \,\in\, \mathbb{Z}^n} a_w\, z^w \quad \Rightarrow \quad p(\lambda^A \star z) = \sum_{w \,\in\, \mathbb{Z}^n} a_w \lambda^{Aw}\, z^w.$$

For $p(\lambda^A \star z)$ to factor as $\chi(\lambda) p(z)$ we must have $\lambda^{Aw} = \lambda^{Au}$ for any two vectors $u, w \in \mathbb{Z}^n$ with a_v and a_u in the support of p. Let us fix u. Then using the same argument as in Theorem 3.1 we have $w - u \in \text{colspan}_{\mathbb{Z}}\, V_{\mathfrak{n}}$ and $\chi(\lambda) = \lambda^{Au}$. From the previous paragraph we have $\sum_{w \,\in\, \mathbb{Z}^n} b_w \lambda^{Aw}\, z^w = q(\lambda^A \star z) = \lambda^{Au} q(z) = \lambda^{Au} \sum_{w \,\in\, \mathbb{Z}^n} b_w\, z^w$. Thus $Au = Aw$ and therefore there exists $v \in \text{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ such that $w = u + v$ for all w with b_w in the support of q. □

Lemma 3.3 *For $v \in \text{colspan}_{\mathbb{Z}}(V_{\mathfrak{n}})$ we have $v = V_{\mathfrak{n}} \left(W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} \right) v$.*

PROOF: The result follows directly from Lemma 2.6. □

Theorem 3.4 *The n components of $g = z^{V_{\mathfrak{n}}}$ form a minimal generating set of invariants. Furthermore, if $f \in \mathbb{K}(z_1, \ldots, z_n)$ is a rational invariant then*

$$f(z) = f\left(g^{\left(W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} \right)} \right)$$

can be reorganized as a rational function of $(g_1, \ldots, g_n)$ - meaning that the fractional powers disappear.

PROOF: The result follows directly from the representation of the rational invariants in Lemma 3.2 combined with the identity given in Lemma 3.3. □

We therefore retrieve in a constructive way the fact that $\mathbb{K}(z)^{\mathcal{D}}$ is rational, a situation that happens for more general classes of actions [23, Section 2.9].

Example 3.5 *Consider the 3 polynomials in $\mathbb{K}[z_1, z_2, z_3]$ given by*

$$f_1 \;=\; 3z_1z_2 + 3z_3 - 3z_3^2 \;+\; 12, \qquad f_2 \;=\; -\,3z_1z_2 \;+\; 3z_3^2 \;-\; 15, \qquad f_3 \;=\; z_1^3 + z_2^3 + z_3^3 - 3z_1z_2z_3 \;-\; 13.$$

They are invariants for the group of diagonal matrices defined by the exponent matrix $A = [1\ 2\ 0]$ and order matrix $P = [3]$. We then obtain

$$[A \;\; -P] \cdot \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} = [1\ 0\ 0\ 0]$$

with

$$\begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} = \left[\begin{array}{c|ccc} 1 & 2 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & -1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 \end{array}\right] \text{ and inverse } \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} = \left[\begin{array}{ccc|c} 1 & 2 & 0 & -3 \\ \hline 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & -2 \end{array}\right].$$

Thus a generating set of rational invariants is given by

$$g_1 \;=\; \frac{z_1^2}{z_2 z_3}, \quad g_2 \;=\; z_1 z_2, \quad g_3 \;=\; z_3$$

and a set of rewrite rules is given by

$$(z_1,\ z_2,\ z_3) \rightarrow (\ g_1^{1/3} {g_2}^{1/3} {g_3}^{1/3},\ \ \frac{{g_2}^{2/3}}{g_1^{1/3} g_3^{1/3}},\ \ g_3).$$

In this case one can rewrite the polynomials f_1, f_2 and f_3 in terms of the three generating invariants as

$$f_1 \ = \ 3g_2 \ + \ 3g_3 \ - \ 3g_3^2 \ + \ 12, \ \ f_2 \ = \ -3g_2 \ + \ 3{g_3}^2 \ - \ 15, \quad f_3 \ = \ g_1g_2g_3 + \frac{g_2^2}{g_1g_3} + {g_3}^3 - 3g_2g_3 \ - \ 13.$$

3.2 Polynomial generators

Just as a Hermite multiplier is not unique, the set of generating rational invariants is not canonical. For each order of the variables $(z_1, \ldots, z_n)$ there is nonetheless a generating set with desirable features. This leads us to discuss polynomial invariants.

Theorem 3.6 *There is a minimal generating set of invariants that consists of a triangular set of monomials with nonnegative powers. More specifically this set of generators is given by $z^{V_\mathfrak{n}}$ where $V_\mathfrak{n}$ is the normalized Hermite multiplier for $[A \ \ -P]$. Therefore:*

(iii) The triangular set of generating invariants monomials is given as $(z_1^{m_1}, {z_1}^{v_{1,2}} z_2^{m_2}, \ldots, {z_1}^{v_{1,n}} \ldots {z_{n-1}}^{v_{n-1,n}} {z_n}^{m_n})$, where $0 \leq v_{i,j} < m_i$ for all $i < j$.

(ii) The diagonal entries m_i of $V_\mathfrak{n}$ satisfy $m_1 \ldots m_n = \frac{p_1 \ldots p_s}{\det H}$

PROOF: From Lemma 2.4 there exists a normalized Hermite multiplier V for $[A \ \ -P]$. For such a normalized multiplier V_n is in column Hermite form and hence $V_n \in \mathbb{N}^{n \times n}$ has nonnegative entries and is upper triangular. Therefore $g = z^{V_\mathfrak{n}}$ gives the required polynomial generating invariants with the triangular structure coming from $V_\mathfrak{n}$ being in Hermite form. This gives part (i). Part (ii) follows from Corollary 2.5 since

$$p_1 \cdot p_2 \cdots p_s = \ \det \ (H) \cdot \prod_{i=1}^{n} m_i \ .$$

□

The total degree of the jth monomial is at most $\sum_{j=1}^{n}(m_j - j + 1) \leq \frac{\prod_{i=1}^{s} p_i}{\det H}$. When $\det H = 1$ we can thus reach Noether's bound, as in Example 3.10.

Example 3.7 *For the integer matrices $A \in \mathbb{Z}^{1\times 3}$ and $P = [3]$ from Example 3.5 we determine the normalized Hermite multiplier as*

$$\begin{bmatrix} V_\mathfrak{i} & V_\mathfrak{n} \\ P_\mathfrak{i} & P_\mathfrak{n} \end{bmatrix} = \left[\begin{array}{c|ccc} 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 \end{array}\right] \text{ and inverse } \begin{bmatrix} W_\mathfrak{u} & P_\mathfrak{u} \\ W_\mathfrak{d} & P_\mathfrak{d} \end{bmatrix} = \left[\begin{array}{ccc|c} 1 & 2 & 0 & -3 \\ \hline 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right].$$

Thus a generating set of polynomial invariants is given by the triangular set

$$g_1 \ = \ z_1^3, \quad g_2 \ = \ z_1z_2, \quad g_3 \ = \ z_3$$

and a set of rewrite rules is given by

$$(z_1,\ z_2,\ z_3) \rightarrow (\ g_1^{1/3}, \frac{g_2}{g_1^{1/3}},\ \ g_3).$$

In this case one can rewrite the polynomials f_1, f_2 and f_3 in terms of the three generating invariants as

$$f_1 \;=\; 3g_2 \;+\; 3g_3 - \;3{g_3}^2 \;+\; 12, \quad f_2 \;=\; -\,3g_2 \;+\; 3{g_3}^2 \;-\; 15, \quad f_3 \;=\; g_1 + \frac{g_2^3}{g_1} + {g_3}^3 - 3g_2g_3 \;-\; 13.$$

Note that Theorem 3.4 does not imply that we have a generating set for the ring of polynomial invariants $\mathbb{K}[z]^{\mathcal{D}}$. It only implies that we can rewrite any polynomial invariant as a Laurent polynomial in the (polynomial) generators of $\mathbb{K}(z)^{\mathcal{D}}$ provided by Theorem 3.6.

If we wish to obtain generators for $\mathbb{K}[z]^{\mathcal{D}}$, there are several algorithms, but, to our knowledge, none that would provide simultaneously rewrite rules. First, the computation of a generating set of polynomial invariants in the present situation can be directly obtained from a simply described Hilbert basis for $\ker[A \quad -P] \cap \mathbb{N}^n$ [29, Corollary 2.7.4]). We can also apply the general algorithm for reductive groups [3, Algorithm 4.1.9]. The ideal involved is, in this case, binomial and the step that involves the Reynold operator can be omitted.

In one round of linear algebra, we obtain here an algebraically independent set of polynomial invariants. They are unfortunately not primary but they can serve as input for the very general algorithm based on Molien's series for completion into a fundamental set for $\mathbb{K}[z]^{\mathcal{D}}$ (see for instance [29, Algorithm 2.2.5] or [3, Algorithm 2.6.1]). We also have additional information from the rewrite rules so that the following strategy should prove more efficient, as well as easy to implement. Let $h \in \mathbb{K}[x]^{\mathcal{D}}$ be the product of the generators g_i that appear with a negative power in the rewrite rules. Then Theorem 3.4 implies that the localization $\mathbb{K}[x]^{\mathcal{D}}_h$ is equal to $\mathbb{K}[h^{-1}, g_1, \ldots, g_n]$. We can thus straightforwardly apply [3, Section 4.2.1] to obtain the following result.

Theorem 3.8 *Let $h = \prod_{i \in I} g_i \in \mathbb{K}[x]^{\mathcal{D}}$, where I is the set of indices of the rows of $W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}$ that contain a negative entry. If Q is a set of generators for the ideal $(g_1(z) - g_1(x), \ldots, g_n(z) - g_n(x)) : h(z)^\infty \subset \mathbb{K}[z, x]$ then $\{q(z, 0) \,|\, q \in Q\}$ is a fundamental set for $\mathbb{K}[z]^G$.*

The set Q can be obtained by computing a Gröbner basis for $(h(z)\,w - 1, g_1(z) - g_1(x), g_n(z) - g_n(x))$ with a term order that eliminates w. This ideal is binomial, a case where Gröbner basis computations are rather efficient. Yet, as we shall see in Example 3.10, the output can be combinatorially large.

Example 3.9 *Continuing with Example 3.7, we can obtain generators for $\mathbb{K}[z]^{\mathcal{D}}$ as follows. The set of generators for $\mathbb{K}(z)^{\mathcal{D}}$ is $\left\{z_1^3,\, z_1, z_2,\, z_3\right\}$ and the denominators in the rewrite rules only involve powers of z_1. We shall thus consider the Gröbner basis $\tilde{Q}$ for*

$$\left(z_1^3 - x_1^3, z_1z_2 - x_1x_2, z_3 - x_3, z_1^3 w - 1\right) \cap \mathbb{K}[z, x, w].$$

For instance if we take the default graded reverse lexicographic order with $z_1 > z_2 > z_3 > x_1 > x_2 > x_3$ we obtain

$$\tilde{Q} = \left\{z_3 - x_3, z_1\, z_2 - x_1\, x_2, z_2\, x_1^2 - x_2\, z_1^2, z_2^2\, x_1 - x_2^2\, z_1, z_2^3 - x_2^3, z_1^3 - x_1^3\right\}.$$

Subsituting x_1, x_2, x_3 by 0, the remaining nonzero elements are the monomials $\left\{z_1^3,\, z_1\, z_2,\, z_3,\, z_2^3\right\}$. They form a generating set for $\mathbb{K}[z]^{\mathcal{D}}$.

3.3 Additional examples

Example 3.10 *Consider the subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element*

$$\xi I_n = \begin{bmatrix} \xi & & \\ & \ddots & \\ & & \xi \end{bmatrix}, \tag{6}$$

where ξ is a primitive pth root of unity. $\mathcal{D}$ is defined by the exponent matrix $A = \begin{bmatrix} 1 & \dots & 1 \end{bmatrix} \in \mathbb{Z}^{1\times n}$ and order matrix $P = \begin{bmatrix} p \end{bmatrix}$. The normalized Hermite multiplier of $[A \quad -P]$ is

$$V = \begin{bmatrix} 1 & p & p-1 & \dots & p-1 \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 0 & 1 & 1 & \dots & 1 \end{bmatrix} \quad \textit{with inverse} \quad W = \begin{bmatrix} 1 & 1 & \dots & 1 & -p \\ 0 & -1 & \dots & -1 & 1 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{bmatrix}.$$

Hence

$$W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} = \begin{bmatrix} \frac{1}{p} & -\frac{p-1}{p} & \dots & -\frac{p-1}{p} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

The generating invariants of Theorem 3.4 are thus

$$g_1 = z_1^p, \text{ and } g_k = z_1^{p-1} z_k, \; 2 \le k \le n,$$

and the rewrite rules are

$$z_1 \to g_1^{\frac{1}{p}}, \text{ and } z_k \to \frac{g_k}{g_1^{\frac{p-1}{p}}}, \; 2 \le k \le n.$$

All the monomials of degree p are actually invariant. We can use those to demonstrate how the apparent fractional powers disappear under substitution. For $u \in \mathbb{N}^n$ such that $\sum_{i=1}^n u_i = p$, the rewrite rules imply

$$z_1^{u_1} z_2^{u_2} \dots z_n^{u_n} = g_1^{\frac{u_1}{p} - \frac{u_2(p-1)}{p} - \dots - \frac{u_n(p-1)}{p}} g_2^{u_1} \dots g_n^{u_n} = \frac{g_1 g_2^{u_1} \cdots g_n^{u_n}}{g_1^{u_2+\dots+u_n}}.$$

Though simple, this example is interesting as it shows the sharpness of Noether's bound for the generators of polynomial invariant rings [29, Proposition 2.15]. A minimal generating set of invariants for the algebra $\mathbb{K}[z]^{\mathcal{D}}$ consists of all monomials of degree p. This minimal generating set thus has $\begin{pmatrix} n+p-1 \\ n-1 \end{pmatrix}$ elements. This is in contrast with the set of n polynomial invariants g_i above that generate $\mathbb{K}(z)^{\mathcal{D}}$. From the rewrite rules we can furthermore infer that $\mathbb{K}[z]^{\mathcal{D}}_{g_1} = \mathbb{K}[g_1^{-1}, g_1, \dots, g_n]$.

Example 3.11 *Consider the subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element*

$$D_\xi = \begin{bmatrix} \xi & & & & \\ & \xi^2 & & & \\ & & \ddots & & \\ & & & \xi^{n-1} & \\ & & & & 1 \end{bmatrix} \tag{7}$$

where ξ is a primitive nth root of unity. $\mathcal{D}$ is defined by the exponent matrix $A = \begin{bmatrix} 1 & 2 & \dots & n-1 & 0 \end{bmatrix}$ with the order matrix $P = \begin{bmatrix} n \end{bmatrix}$. This group is the diagonalization of the representation of the cyclic group of permutations examined in Example 4.3.

In order to obtain polynomial generators, we compute the normalized Hermite multiplier for $\begin{bmatrix} A & -P \end{bmatrix}$ *:*

$$V = \left[\begin{array}{c|c} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ \hline P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{array}\right] = \left[\begin{array}{c|cccccc} 1 & n & n-2 & \cdots & \cdots & 1 & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \ddots & 0 \\ \vdots & 0 & 0 & \cdots & \cdots & 0 & 1 \\ \hline 0 & 1 & 1 & \dots & \dots & 1 & 0 \end{array}\right].$$

By Theorem 3.4, a set of generating invariants of the diagonal action are thus $\left\{ z_1^{n-k} z_k \,|\, 1 \leq k \leq n \right\}$*. In order to obtain the rewrite rules one notices that the inverse of* V *is given by*

$$W = \left[\begin{array}{cccccc|c} 1 & 2 & 3 & \cdots & n-1 & 0 & -n \\ \hline 0 & -1 & -1 & \cdots & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & 1 & 0 & \vdots \\ 0 & \dots & \dots & \dots & 0 & 1 & 0 \end{array}\right]$$

and so

$$W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} = \begin{bmatrix} \frac{1}{n} & -\frac{n-2}{n} & \cdots & -\frac{1}{n} & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

By Theorem 3.4, the set of rewrite rules is given by

$$z \to g^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}} = \left(g_1^{\frac{1}{n}},\ \frac{g_2}{g_1^{\frac{n-2}{n}}},\ \dots \frac{g_{n-1}}{g_1^{\frac{1}{n}}},\ g_n \right), \qquad \text{that is,} \qquad z_k \to \frac{g_k}{g_1^{\frac{n-k}{n}}},\ 1 \leq k \leq n.$$

Example 3.12 *Consider the subgroup* $\mathcal{D}$ *of* $\mathrm{GL}_n(\mathbb{K})$ *generated by*

$$\xi I_n = \begin{bmatrix} \xi & & & & \\ & \xi & & & \\ & & \ddots & & \\ & & & \xi & \\ & & & & \xi \end{bmatrix} \quad \text{and} \quad D_\xi = \begin{bmatrix} \xi & & & & \\ & \xi^2 & & & \\ & & \ddots & & \\ & & & \xi^{n-1} & \\ & & & & 1 \end{bmatrix} \tag{8}$$

where ξ *is a* n*th root of unity. The group* $\mathcal{D}$ *is specified by the exponent matrix* $A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 2 & 3 & \dots & n-1 & 0 \end{bmatrix}$ *and the order matrix* $P = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$*. The Hermite form of* $[A, -P]$ *is* $[I_2, 0]$ *and its normalized Hermite mul-*

tiplier is

$$V = \left[\begin{array}{c|c} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ \hline P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{array}\right] = \left[\begin{array}{cc|cccccccc}
2 & -1 & n & 0 & 1 & 2 & \cdots & \cdots & n-3 & n-2 \\
-1 & 1 & 0 & n & n-2 & n-3 & \cdots & \cdots & 2 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & \cdots & & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & & & 0 & \\
\vdots & \vdots & & & & & \ddots & & \vdots & \vdots \\
 & & & & & & & \ddots & \vdots & \vdots \\
\vdots & \vdots & & & & & & & 1 & 0 \\
\vdots & \vdots & & & & & & & & 1 \\
\hline
0 & 0 & 1 & 1 & 1 & \cdots & \cdots & & 1 & 1 \\
0 & 0 & 1 & 2 & 2 & \cdots & \cdots & & 2 & 1
\end{array}\right]$$

with inverse

$$W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} = \left[\begin{array}{cccccc|cc}
1 & 1 & 1 & \cdots & 1 & 1 & -n & 0 \\
1 & 2 & 3 & \cdots & n-1 & 0 & 0 & -n \\
\hline
0 & 0 & 0 & \cdots & 0 & -1 & 2 & -1 \\
0 & 0 & -1 & \cdots & -1 & -1 & -1 & 1 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & & 1 & & & \vdots & \vdots \\
\vdots & \vdots & & & \ddots & \vdots & \vdots & \\
0 & 0 & & & & 1 & 0 & 0
\end{array}\right].$$

This gives a set of generating invariants as

$$g = z^{V_{\mathfrak{n}}} = \left(z_1^n,\ z_2^n,\ z_1 z_2^{n-2} z_3,\ z_1^2 z_2^{n-3} z_4,\ \ldots\ ,\ z_1^{n-3} z_2^2 z_{n-1},\ z_1^{n-2} z_n\right)\ ,$$

that is, $g_1 = z_1^n$ and $g_k = z_1^{k-2} z_2^{n-k+1} z_k$ for $2 \leq k \leq n$. Since

$$W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} = \begin{bmatrix}
\frac{1}{n} & 0 & \frac{-1}{n} & \cdots & \frac{-(n-3)}{n} & \frac{-(n-2)}{n} \\
0 & \frac{1}{n} & \frac{2-n}{n} & \cdots & \frac{-2}{n} & \frac{-1}{n} \\
0 & 0 & 1 & \cdots & 0 & 0 \\
 & & & \ddots & & \vdots \\
 & & & & \ddots & \vdots \\
 & & & & & 1
\end{bmatrix},$$

the rewrite rules are

$$z \to g^{W_{\mathfrak{d}} - P_{\mathfrak{d}} \cdot P_{\mathfrak{u}}^{-1} \cdot W_{\mathfrak{u}}} = \left(g_1^{\frac{1}{n}},\ g_2^{\frac{1}{n}}, \frac{g_3}{g_1^{\frac{1}{n}} g_2^{\frac{n-2}{n}}},\ \ldots,\ \frac{g_{n-1}}{g_1^{\frac{n-3}{n}} g_2^{\frac{2}{n}}},\ \frac{g_n}{g_1^{\frac{n-2}{n}} g_2^{\frac{1}{n}}}\right).$$

That is, $z_1 \to g_1^{\frac{1}{n}}$, $z_k \to \frac{g_k}{g_1^{\frac{k-2}{n}} g_2^{\frac{n-k+1}{n}}}$ for $2 \leq k \leq n-1$ and $z_n \to \frac{g_1^{\frac{2}{n}} g_n}{g_2^{\frac{n+1}{n}}}$.

4 Invariants of finite abelian groups of matrices

Representations of finite abelian groups can be diagonalized. As such the results about invariants of diagonal representations of finite groups can be generalized to abelian groups. In this section we illustrate such a diagonalization process and work out some relevant examples.

Consider $\mathcal{G}$ a finite abelian subgroup of $\mathrm{GL}_n(\mathbb{K})$ of order p. Assume that the characteristic of $\mathbb{K}$ does not divide p and that $\mathbb{K}$ contains a primitive pth root of unity. Let $G_1, \ldots, G_s \in \mathrm{GL}_n(\mathbb{K})$ be a set of generators for $\mathcal{G}$ whose respective orders are $p_1, \ldots, p_s$. Then $\mathcal{G}$ is the image of the representation

$$\begin{array}{ccc} \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s} & \rightarrow & \mathrm{GL}_n(\mathbb{K}) \\ (m_1, \ldots, m_s) & \mapsto & G_1^{m_1} \cdots G_s^{m_s} \end{array}.$$

For any element G of $\mathcal{G}$ we have $G^p = I_n$. The minimal polynomial of G thus has only simple factors. Therefore G is diagonalizable and the eigenvalues of G are p-th roots of unity. Since the elements of $\mathcal{G}$ commute, they are simultaneously diagonalizable [8] : there exists an invertible matrix Ξ with entries in $\mathbb{K}$ such that $\Xi^{-1} \cdot G \cdot \Xi$ is diagonal for all $G \in \mathcal{G}$. We introduce $\mathcal{D} = \Xi^{-1} \cdot \mathcal{G} \cdot \Xi$ the finite subgroup of diagonal matrices in $\mathrm{GL}_n(\mathbb{K})$ generated by $D_i = \Xi^{-1} \cdot G_i \cdot \Xi$, $1 \leq i \leq s$.

Proposition 4.1 *Take $f, g \in \mathbb{K}(z_1, \ldots, z_n)$ with $f(\Xi z) = g(z) \Leftrightarrow f(z) = g(\Xi^{-1} z)$. Then g is invariant for $\mathcal{D}$ if and only if f is an invariant for $\mathcal{G}$.*

Theorem 4.2 *Consider an abelian group $\mathcal{G}$ of order p, $\mathbb{K}$ of characteristic not dividing p and containing a primitive p-th root of unity. A n-dimensional representation of $\mathcal{G}$ over $\mathbb{K}$ admits a set of n polynomials in $\mathbb{K}[z]^{\mathcal{G}}$ as generators of the field $\mathbb{K}(z)^{\mathcal{G}}$ of rational invariants.*

In view of Proposition 4.1, this is actually a corollary to Theorem 3.6. We can thus compute the polynomial generators explicitly, as well as the rewrite rules, by first diagonalizing the representation of the group. We work out a sample of relevant examples.

Example 4.3 *Let $\mathcal{G}$ be the subgroup of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element:*

$$M_\sigma = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{bmatrix}. \tag{9}$$

$\mathcal{G}$ is the natural linear representation of the cyclic group of permutations $(n, n-1, \ldots, 1)$.

The following n polynomials generate the field of rational invariants:

$$g_k = \left(\sum_{i=1}^{n} \frac{z_i}{\xi^i} \right)^{n-k} \left(\sum_{i=1}^{n} \frac{z_i}{\xi^{ki}} \right), \quad 1 \leq k \leq n$$

where ξ is a primitive n^{th} root of unity. In the case of $n = 3$, for instance, these invariants are

$$\begin{aligned} g_1 &= z_1^3 + z_2^3 + z_3^3 - 3\,(z_1^2\, z_2 + z_2^2\, z_3 + z_3^2\, z_1) + 6\, z_1\, z_2\, z_3 + 3\,\xi\,(z_1 - z_2)\,(z_2 - z_3)\,(z_3 - z_1), \\ g_2 &= z_1^2 + z_2^2 + z_3^2 - z_1\, z_2 - z_2\, z_3 - z_3\, z_1, \\ g_3 &= z_1 + z_2 + z_3 \end{aligned}$$

Furthermore, any rational invariants of $\mathcal{G}$ can be written in terms of $(g_1, \ldots, g_n)$ with the following substitution.

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ \vdots \\ z_n \end{pmatrix} \rightarrow \Xi(\xi)^{-1} \begin{pmatrix} g_1^{\frac{1}{n}} \\ g_2\, g_1^{\frac{2-n}{n}} \\ \vdots \\ g_{n-1}\, g_1^{\frac{-1}{n}} \\ g_n \end{pmatrix}$$

where

$$\Xi(\xi) = \left(\xi^{ij}\right)_{1\leq i,j\leq n} = \begin{bmatrix} \xi & \xi^2 & \dots & \xi^{n-1} & 1 \\ \xi^2 & \xi^4 & \dots & \xi^{2(n-1)} & 1 \\ \vdots & & & & \\ \vdots & & & \vdots & \vdots \\ \xi^{n-1} & \xi^{2(n-1)} & \dots & \xi^{(n-1)(n-1)} & 1 \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix} \tag{10}$$

and $\Xi(\xi)^{-1} = \frac{1}{n}\,\Xi\left(\xi^{-1}\right)$.

Indeed M_σ *is the companion matrix of the polynomial* $\lambda^n - 1$. *Therefore the eigenvalues of* M_σ *are the* n*-th roots of unity. If* ξ *is a primitive* n*-th root then a matrix of eigenvectors is given by* $\Xi(\xi)$ *above. Hence*

$$\mathcal{G} = \left\{ \Xi\, diag\left(\xi, \dots, \xi^{n-1}, 1\right)^\ell\, \Xi^{-1}, \ell = 0, \dots, n-1 \right\}.$$

The underlying group of diagonal matrices was examined in Example 3.11.

Example 4.4 *Let* $\mathcal{G}$ *be the subgroup of* $\mathrm{GL}_n(\mathbb{K})$ *generated by the matrices*

$$\xi I_n = \begin{bmatrix} \xi & & & & \\ & \xi & & & \\ & & \ddots & & \\ & & & \xi & \\ & & & & \xi \end{bmatrix} \quad \text{and} \quad M_\sigma = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix} \tag{11}$$

where ξ *is a primitive* n*th root of unity. We consider its obvious linear action on* $\mathbb{K}^n$. *The following* n *polynomials generate the field of rational invariants:*

$$g_1 = \left(\sum_{i=1}^{n} \frac{z_i}{\xi^i}\right)^n \text{ and } g_k = \left(\sum_{i=1}^{n} \frac{z_i}{\xi^i}\right)^{k-2} \left(\sum_{i=1}^{n} \frac{z_i}{\xi^{2i}}\right)^{n-k+1} \left(\sum_{i=1}^{n} \frac{z_i}{\xi^{ki}}\right), \quad 2 \leq k \leq n.$$

Furthermore, any rational invariants of $\mathcal{G}$ *can be written in terms of* $(g_1, \dots, g_n)$ *with the following substitution.*

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ \vdots \\ z_n \end{pmatrix} \to \Xi(\xi)^{-1} \begin{pmatrix} g_1^{\frac{1}{n}} \\ g_2^{\frac{1}{n}} \\ \frac{g_3}{g_1^{\frac{1}{n}}\, g_2^{\frac{n-2}{n}}}, \\ \vdots \\ \frac{g_{n-1}}{g_1^{\frac{n-3}{n}}\, g_2^{\frac{2}{n}}} \\ \frac{g_n}{g_1^{\frac{n-2}{n}}\, g_2^{\frac{1}{n}}} \end{pmatrix}$$

where $\Xi(\xi)$ *is as in Example 4.3.*

Indeed, the group $\mathcal{D} = \Xi^{-1}\,\mathcal{G}\,\Xi$ *is generated by the diagonal matrices* $diag(\xi, \xi, \dots, \xi)$ *and* $diag(\xi, \dots, \xi^{n-1}, 1)$ *and was considered in Example 3.12.*

5 Solving invariant systems of polynomials

We adopt the assumptions of Section 3 regarding $\mathbb{K}$, $\mathcal{U} = \mathbb{U}_{p_1} \times \ldots \times \mathbb{U}_{p_s}$, A and P. In addition let $\bar{\mathbb{K}}$ be an algebraically closed field extension of $\mathbb{K}$.

We consider a set of Laurent polynomials $F \subset \mathbb{K}[z, z^{-1}]$ and assume that its set of toric zeros is invariant by the linear (diagonal) action of $\mathcal{U}$ defined by A. In other words we assume that if $z \in (\mathbb{K}^*)^n$ is such that $f(z) = 0$ for all $f \in F$ then $f(\lambda^A \star z) = 0$, for all $\lambda \in \mathcal{U}$ and $f \in F$.

We first show how to obtain an equivalent system of invariant Laurent polynomials. The strategy here partly follows [5, Section 3]. We then show how to find the toric zeros of a system of invariant Laurent polynomials through a *reduced* system of polynomials and a triangular set of binomials. Each solution of the reduced system determines an orbit of solutions of the original system. Each orbit is determined by values for the rational invariants. The elements in each orbit of solutions is then obtained by solving the binomial triangular set.

The question of an optimal method to solve the reduced system is not addressed in this paper. Given that we have to partially restrict to toric solutions, it would be natural to consider methods that deal with Laurent polynomials [22, 18].

The proposed strategy nonetheless extends to systems of polynomial equations whose solution set is invariant under a finite abelian group, as for instance cyclic permutations. We illustrate this with a relevant example.

5.1 Invariant systems of polynomials

We consider a set of Laurent polynomials $F \subset \mathbb{K}[z, z^{-1}]$ and assume that its set of toric zeros is invariant under the n-dimensional diagonal representation defined by the exponent matrix $A \in \mathbb{Z}^{s\times n}$, and the order matrix $P = \operatorname{diag}(p_1, \ldots, p_s)$. In other words, if $z \in (\bar{\mathbb{K}}^*)^n$ is such that $f(z) = 0$, $\forall f \in F$, then $f(\lambda^A \star z) = 0$, $\forall f \in F$ and $\forall \lambda \in \mathcal{U} = \mathbb{U}_{p_1} \times \ldots \times \mathbb{U}_{p_s}$.

Definition 5.1 *The (A, P)-degree of a monomial $z^u = z_1^{u_1} \ldots z_n^{u_n}$ defined by $u \in \mathbb{Z}^n$ is the element of $\mathcal{Z} = \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$ given by $A\,u \mod {}^t(p_1, \ldots, p_s)$.*

A Laurent polynomial $f \in \mathbb{K}[z, z^{-1}]$ is (A, P)-homogeneous of (A, P)-degree $d \in \mathcal{Z}$ if all the monomials of its support are of (A, P)-degree d.

A Laurent polynomial $f \in \mathbb{K}[z, z^{-1}]$ can be written as the sum $f = \sum_{d\in\mathcal{Z}} f_d$ where f_d is (A, P)-homogeneous of (A, P)-degree d. The Laurent polynomials f_d are the (A, P)-homogeneous components of f.

The following proposition shows that our simple definition of (A, P)-degree matches the notion of $\mathcal{Z}$-degree in [5, Section 3.1].

Proposition 5.2 *$f \in \mathbb{K}[z, z^{-1}]$ is (A, P)-homogeneous of (A, P)-degree d if and only if $f\left(\lambda^A \star z\right) = \lambda^d f$ for all $\lambda \in \mathcal{U}$.*

PROOF: Consider a monomial z^u of (A, P)-degree d, that is, $Au = d \mod (p_1, \ldots, p_s)$. Then $\left(\lambda^A \star z\right)^u = \lambda^{Au} z^u = \lambda^d z^u$.

Conversely $f\left(\lambda^A \star z\right)^u = \lambda^d f$ implies that all the monomials z^u in f are such that $\left(\lambda^A \star z\right)^u = \lambda^d z^u$. Hence $A\,u = d \mod {}^t(p_1, \ldots, p_s)$. □

A question raised in [5] is whether there are monomials of any given (A, P)-degree. If the Hermite normal form of $\begin{bmatrix} A & -P \end{bmatrix}$ is $\begin{bmatrix} I_s & 0 \end{bmatrix}$ then for any $d \in \mathcal{Z}$ we can find monomials of (A, P)-degree d. These are the $z^{u+V_\mathfrak{n} v}$ where $u = V_\mathfrak{i}\, d$ and $v \in \mathbb{Z}^n$. In this section we do not make this asumption as we assume the group representation given. Yet in Section 6 we show how to obtain a pair of matrices of exponents and orders (B, Q) that define the same group of diagonal $n \times n$ matrices and for which $\begin{bmatrix} I_s & 0 \end{bmatrix}$ is the Hermite normal form of $\begin{bmatrix} B & -Q \end{bmatrix}$.

The following proposition is a variation on [5, Theorem 4] of which we borrow the main idea of the proof.

Proposition 5.3 *Let $F \subset \mathbb{K}[z, z^{-1}]$ and $F^h = \{f_d \,|\, f \in F,\ d \in \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}\}$ be the set of the homogeneous components of the elements of F. If the set of toric zeros of F is invariant by the diagonal action of $\mathcal{U}$ defined by A then it is equal to the set of toric zeros of F^h.*

PROOF: Obviously we have the ideal inclusion $(F) \subset (F^h)$ and thus the zeros of F^h are included in the set of zeros of F.

Conversely, since $f(\lambda^A \star z) = \sum_d \lambda^d f_d(z)$ for all $\lambda \in \mathcal{U}$ we have a square linear system

$$\left(f(\lambda^A \star z)\right)_{\lambda \in \mathcal{U}} = \left(\lambda^d\right)_{\lambda \in \mathcal{U}, d \in \mathcal{Z}} (f_d)_{d \in \mathcal{Z}}.$$

With an appropriate ordering of the elements of $\mathcal{U}$ and $\mathcal{Z}$ the square matrix $\left(\lambda^d\right)_{\lambda \in \mathcal{U}, d \in \mathcal{Z}}$ is the Kronecker product of the Vandermonde matrices $\left(\xi_i^{(k-1)(l-1)}\right)_{1 \leq k,l \leq p_i}$, for $1 \leq i \leq s$ and ξ_i a primitive p_ith root of unity. It is therefore invertible.

By hypothesis, if z is a toric zero of F, then $\lambda^A \star z$ is also a toric zero of F for any $\lambda \in \mathcal{U}$: for f in F and z a toric zero of F, $f(\lambda^A \star z) = 0$ for all $\lambda \in \mathcal{U}$. It follows that $f_d(z) = 0$, for all d. The set of toric zeros of F is thus included in the set of toric zeros of F^h. □

Proposition 5.4 *If $f \in \mathbb{K}[z, z^{-1}]$ is (A, P)-homogeneous then there is a $u \in \mathbb{Z}^n$ such that $f = z^u \bar{f}$ where $\bar{f} \in \mathbb{K}[z, z^{-1}]$ is (A, P)-homogeneous of (A, P)-degree 0, that is, is invariant.*

Starting from a set F of (Laurent) polynomials we can thus deduce a set $\bar{F}$ of invariant Laurent polynomials that admit the same set of zeros in $(\bar{\mathbb{K}}^*)^n$.

5.2 Systems of invariant polynomials

We consider now a set F of invariant Laurent polynomials for the diagonal action of $\mathcal{U} = \mathbb{U}_{p_1} \times \ldots \mathbb{U}_{p_s}$ given by the exponent matrix $A \in \mathbb{Z}^{s \times n}$ and the order matrix $P = \operatorname{diag}(p_1, \ldots, p_s)$.

Consider the normalized Hermite multiplier for $\begin{bmatrix} A & -P \end{bmatrix}$

$$V = \begin{bmatrix} V_{\mathfrak{i}} & V_{\mathfrak{n}} \\ P_{\mathfrak{i}} & P_{\mathfrak{n}} \end{bmatrix} \quad \text{with inverse} \quad W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix}.$$

Recall from Lemma 2.4 that $V_{\mathfrak{n}}$ is triangular with non negative entries. By Theorem 3.4, for each $f \in F$

$$f(z_1, \ldots, z_n) = f\left((g_1(z), \ldots, g_n(z))^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}}\right)$$

so there exists a Laurent polynomial $\mathfrak{f} \in \mathbb{K}[y_1, \ldots, y_n, y_1^{-1}, \ldots, y_n^{-1}]$ such that $f(z_1, \ldots, z_n) = \mathfrak{f}(g_1(z), \ldots, g_n(z))$. This polynomial is given *symbolically* by

$$\mathfrak{f}(y_1, \ldots, y_n) = f\left((y_1, \ldots, y_n)^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}}\right),$$

meaning that the fractional powers disappear upon substitution. The polynomial $\mathfrak{f}$ is the *symmetry reduction of f*.

Theorem 5.5 *Let F be a set of invariant Laurent polynomials in $\mathbb{K}[z, z^{-1}]$ and consider the set $\mathfrak{F} \subset \mathbb{K}[y, y^{-1}]$ of their symmetry reductions.*

If $z \in (\bar{\mathbb{K}}^*)^n$ is a zero of F then $z^{V_{\mathfrak{n}}}$ is a solution of $\mathfrak{F}$. Conversely, if $y \in (\bar{\mathbb{K}}^*)^n$ is a zero of $\mathfrak{F}$ then there exists $\frac{p_1 \cdots p_s}{\det H}$ zeros of F in $(\bar{\mathbb{K}}^*)^n$ that are the solutions of the triangular system $z^{V_{\mathfrak{n}}} = y$.

PROOF: The first part comes from the definition of the symmetry reduction: $f(z) = \mathfrak{f}\left(z^{V_\mathfrak{n}}\right)$.

The fact that $z^{V_\mathfrak{n}}$ is triangular follows from Theorem 3.6. Furthermore the product of the diagonal entries of $V_\mathfrak{n}$ equals $\prod_{i=1}^{s} p_i / \det H$ by Corollary 2.5. Hence, for any $y \in (\bar{\mathbb{K}}^*)^n$, the system $z^{V_\mathfrak{n}} = y$ has the announced number of solutions in $(\bar{\mathbb{K}}^*)^n$.

For $y \in (\bar{\mathbb{K}}^*)^n$ a zero of $\mathfrak{F}$ and $z \in (\bar{\mathbb{K}}^*)^n$ a solution of $z^{V_\mathfrak{n}} = y$ we have $f(z) = \mathfrak{f}(z^{V_\mathfrak{n}}) = \mathfrak{f}(y) = 0$. □

Example 5.6 *Continuing with Example 3.5, we have that the symmetry reductions of* $F = \{f_1,\ f_2, f_3\}$

$$f_1 \;=\; 3z_1z_2 + 3z_3 - 3z_3^2 \;+\; 12, \quad f_2 \;=\; -\,3z_1z_2 \;+\; 3z_3^2 \;-\; 15, \quad f_3 \;=\; z_1^3 + z_2^3 + z_3^3 - 3z_1z_2z_3 \;-\; 13$$

are given by $\mathfrak{F} = \{\mathfrak{f}_1, \mathfrak{f}_2, \mathfrak{f}_3\}$ *where*

$$\mathfrak{f}_1 \;=\; 3y_2 \;+\; 3y_3 -\; 3{y_3}^2 \;+\; 12, \quad \mathfrak{f}_2 \;=\; -\,3y_2 \;+\; 3{y_3}^2 \;-\; 15, \quad \mathfrak{f}_3 \;=\; y_1 + \frac{y_2^3}{y_1} + {y_3}^3 - 3y_2y_3 \;-\; 13.$$

The toric zeros of $\mathfrak{F}$ *are easily determined as the two points*

$$(y_1,\ y_2,\ y_3) = (8,\ -4,\ 1) \quad \textit{and} \quad (y_1,\ y_2,\ y_3) = (\ -8,\ -4,\ 1).$$

Solving the triangular system:

$$z_1^3 = \ \pm\ 8,\ z_1z_2 = -4,\ z_3 = 1$$

we obtain six toric zeros of F *as:*

$$(2,\ -2, 1),\ \ (-2,\ 2,\ 1),\ \ (2\xi,\ -2\xi^2, 1),\ \ (-2\xi,\ 2\xi^2,\ 1),\ \ (2\xi^2,\ -2\xi, 1),\ \ (-2\xi^2,\ 2\xi,\ 1),$$

where ξ *is a primitive cube root of* 1.

5.3 Extension to finite abelian groups - an example

In view of Section 4 it is obvious that we can extend our scheme to solve polynomial systems to the case where the zeros are invariant under the linear action of a finite abelian group. We illustrate this on an example.

Consider the following system of polynomial equations

$$\begin{aligned} 1 - cx_1 - x_1x_2^2 - x_1x_3^2 &= 0 \\ 1 - cx_2 - x_2x_1^2 - x_2x_3^2 &= 0 \\ 1 - cx_3 - x_3x_1^2 - x_3x_2^2 &= 0 \end{aligned} \tag{12}$$

with c a parameter. This is a system describing a neural network model given in [21] and the solutions were given in Gatermann [7]. The strategy there is to use the symmetry to find factorization of polynomials in the ideal and split the Gröbner basis computation accordingly. As a result, the 21 solutions of the system are given by five triangular sets. We use this system to illustrate our alternate scheme.

Our approach is a symmetry reduction scheme. It first characterizes the orbits of solutions by computing the values of the rational invariants on the solutions. The elements of each orbits of solutions are then retrieved through a triangular system.

The set of zeros of this neural network system are easily seen to be invariant under the cyclic group generated by the permutation $\sigma = (321)$. Diagonalizing this linear group action was done in Example 4.3. It implies the change of variable $x = \Xi(\xi)\, z$ with ξ a cubic root of unity. The diagonal action of the group is determined by the exponent matrix $A = [1\ 2\ 0]$ and order matrix $P = [3]$.

Applying the change of variables to the polynomials in System (12) we obtain polynomials $f_0 - \xi f_1 - \xi^2 f_2$, $f_0 - \xi^2 f_1 - \xi f_2$, and $f_0 - f_1 - f_2$, where

$$\begin{array}{rcl} f_0 & = & 1 - c z_3 + z_1^3 + z_2^3 - 2 z_3^3 \\ f_1 & = & c z_1 + 3 z_1^2 z_2 - 3 z_2^2 z_3 \\ f_2 & = & c z_2 + 3 z_1 z_2^2 - 3 z_1^2 z_3. \end{array} \tag{13}$$

Note that f_i is (A, P)-homogeneous of degree i, for $0 \leq i \leq 2$. By Proposition 5.3 the original system is thus equivalent to the system given by f_0, f_1 and f_2.

The statement in Theorem 5.5 is made for toric zeros, but one can refine this statement by tracking the denominators involved in the rewriting rules. Here, one can refine to the statement for the solutions $(z_1, z_2, z_3) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$ and localise at z_1 only (i.e. allow ourselves to divide by z_1 only). The reduced system corresponding to the set of invariants $\left\{ f_0, \frac{f_1}{z_1}, \frac{f_2}{z_1^2} \right\}$ is given by

$$\mathfrak{f}_0 = 1 + y_1 - c y_3 - 2 y_3^2 + \frac{y_2^3}{y_1}, \quad \mathfrak{f}_1 = c + 3 y_2 - 3 \frac{y_2^2 y_3}{y_1}, \quad \mathfrak{f}_2 = -3 y_3 + c \frac{y_2}{y_1} + 3 \frac{y_2^2}{y_1}.$$

This system has $6 = 2 + 4$ zeros. They are given as the union of the solutions of the two triangular sets[4]

$$y_3 = 0, \quad y_2 = \frac{c}{3}, \quad y_1^2 + y_1 - \frac{c^3}{27} = 0; \tag{14}$$

and

$$\begin{gathered} 162\, c\, y_3^4 - 54\, y_3^3 + 81\, c^2\, y_3^2 - 108\, c\, y_3 + 4\, c^3 + 27 = 0, \\ y_2 = -\frac{81\, c}{49\, c^3 - 27}\, y_3^3 - \frac{14\, c^3}{49 c^3 - 27}\, y_3^2 - \frac{93\, c^2}{2 (49\, c^3 - 27)}\, y_3 - \frac{c\, (70\, c^3 - 243)}{6\, (49\, c^3 - 27)} \\ y_1 = y_3^3 + \frac{c}{2}\, y_3 - \frac{1}{2}. \end{gathered} \tag{15}$$

Recall that the variable y_i stands for the generating invariants g_i. The polynomial set (13) has thus 6 orbits of zeros, that is 18 solutions, where $\frac{x_1}{\xi} + \frac{x_2}{\xi^2} + x_3 \neq 0$. The elements of an orbit determined by a solution (y_1, y_2, y_3) of either (14) or (15) are obtained by additionnally solving the binomial triangular system given by the generating invariants:

$$z_1^3 \;=\; y_1, \quad z_1 z_2 \;=\; y_2, \quad z_3 \;=\; y_3.$$

By linear combinations $x = \Xi\, z$ we obtain 18 solutions of the original system (12) organized in 6 orbits.

For completeness one should also examine the solutions of (13) for which $z_1 = 0$. Here, it is immediate to see that there are three solutions satisfying

$$z_1 = 0, \quad z_2 = 0, \quad 2\, z_3^3 + c\, z_3 - 1 = 0.$$

They each form an orbit. The corresponding solutions of the original system are indeed

$$x_1 = x_2 = x_3 = \eta, \text{ for } 2\, \eta^3 + c\, \eta - 1 = 0.$$

[4] These were quickly computed with Gröbner bases and factorisation.

6 Determining groups of homogeneity

In this section we consider the problem of finding the diagonal groups that leave a finite set of rational functions invariant. This can be used to determine weights and orders that make a system of (Laurent) polynomial equation homogeneous for a grading by an abelian group. Indeed $f = a_0x^{u_0}+a_1x^{u_1}+\ldots+a_dx^{u_d}$, with $a_0 \neq 0$, is homogeneous if and only if $\tilde{f} = a_0 + a_1x^{u_1-u_0} + \ldots + a_dx^{u_d-u_0}$ is invariant for the diagonal representations considered.

This is somehow the inverse problem to Section 3. For the symmetry reduction scheme offered in Section 5, the group action was assumed to be known. On one hand, indeed, permutation groups naturally arise in the formulation of some problems and it is reasonable to assume that some symmetries of the solution set are known. This is the case of the system presented in Section 5.3. On the other hand, different concepts of homogeneity come as a practical mean for enhancing the efficiency of Gröbner bases computations [4, 5] or to propose symmetry reduction schemes as [14, Section 5] and Section 5 above. Given the simplicity of the algorithm we give here to determine the weights of homogeneity, it is worth going through this preliminary step before attempting to solve a polynomial system.

A remarkable feature is that we determine simultaneously a generating set of invariants for the underlying representation. The rewrite rules are then obtained by inverting the matrix of exponents of this generating set. Also, the group obtained is given in its normalized form and its representation is faithful. The same contruction provides a canonical representation for a given finite group of diagonal matrices.

Consider $f = \frac{p}{q} \in \mathbb{K}(z)$, where $p, q \in \mathbb{K}[z]$ are relatively prime, and pick w in the support of p or q. Let K_f be the matrix whose columns consist of the vectors $v - w$ for all v in the support of p and q (with $v \neq w$). By Lemma 3.2, f is invariant for the diagonal group action determined by the exponent matrix A and order matrix $P = \operatorname{diag}(p_1, \ldots, p_s)$ if $A\,K_f = 0 \bmod {}^t\begin{bmatrix}p_1 & \ldots & p_s\end{bmatrix}$.

In the case of a finite set F of rational functions we can associate a matrix K_f to each element $f \in F$ as previously described and define the block matrix $K = [K_f | f \in F]$. If K does not have full row rank then there exists a diagonal action of some $(\mathbb{K}^*)^r$, *i.e.* a scaling, that leaves the rational functions $f \in F$ invariants. This situation is dealt with in [15, Section 5]. Hence, for the rest of this section, we assume that K has full row rank and we look for the diagonal representations of finite abelian groups that leave each element of F invariant.

For $K \in \mathbb{Z}^{n\times m}$ a full row rank matrix of integers, there exist unimodular matrices $U \in \mathbb{Z}^{n\times n}, V \in \mathbb{Z}^{m\times m}$ such that $U\,K\,V$ is in Smith normal form, *i.e.* $U\,K\,V = \begin{bmatrix}S & 0\end{bmatrix}$ where either $S = I_n$ or there exists $s \leq n$ such that

$$S = \operatorname{diag}(1, \ldots, 1, p_1, \ldots, p_s) \quad \text{with } p_i \neq 1 \quad \text{and} \quad p_i \mid p_{i+1} \text{ for } i = 1 \ldots s-1.$$

The former case cannot happen when there is a group of diagonal matrices for which F is invariant.

Proposition 6.1 *If there exists $a = [a_1, \ldots, a_n] \in \mathbb{Z}^{1\times n}$ and $p \in \mathbb{N}$ such that $\gcd(a_1, \ldots, a_n, p) = 1$ and $a\,K = 0 \mod p$ then the Smith normal form of K has a diagonal entry different from 1.*

PROOF: Let U and V be the unimodular multipliers for the Smith normal form, *i.e.* $U\,K\,V = [S \;\; 0]$ where $S = \operatorname{diag}(s_1, \ldots, s_n)$. Then $a\,K\,V = (a\,U^{-1})\,U\,K\,V = 0 \mod p$. Since U is unimodular, $\gcd(b_1, \ldots, b_n, p) = 1$ where $[b_1, \ldots, b_n] = a\,U^{-1}$. Therefore at least one b_i is not a multiple of p. Yet we have $b_i\,s_i = 0 \mod p$. Therefore s_i cannot be equal to 1. □

Theorem 6.2 *Consider F a set of rational functions in $\mathbb{K}(z_1, \ldots, z_n)$ such that an associated matrix K for the exponents in F is of full row rank. If the Smith normal form of K is given by $U\,K\,V = \begin{bmatrix}S & 0\end{bmatrix}$ where*

$$S = \operatorname{diag}(1, \ldots, 1, p_1, \ldots, p_s) \quad \text{with} \quad p_i \neq 1 \quad \text{and} \quad p_i \mid p_{i+1} \text{ for } i = 1 \ldots s-1$$

then

(i) the elements of F are invariants for the diagonal representation determined by the order matrix $P = \mathrm{diag}\,(p_1, \dots, p_s)$ and the exponent matrix A consisting of the last s rows of U,

(ii) the columns of $K\,V_1$, where V_1 consists of the n first columns of V, are the exponents of a generating set of invariants for the diagonal representation given by (A, P). More precisely, there is a matrix $M \in \mathbb{Z}^{n\times s}$ such that

$$\Omega = \left[\begin{array}{c|cc} M & \multicolumn{2}{c}{K V_1} \\ \hline 0 & 0 & \multicolumn{1}{|c}{I_s} \end{array}\right]$$

is a Hermite multiplier for $[A \quad -P]$ and the Hermite normal form is $[A \quad -P]\,\Omega = [I_s \quad 0]$

(iii) the Hermite normal form of $K\,V_1$ is the matrix $V_\mathfrak{n}$ of Theorem 3.6.

PROOF: Let A be the matrix made of the last s rows of U. As a submatrix of a unimodular matrix, A is of full row rank. Furthermore, writing $U\,K = S\,V^{-1}$ we see that $A\,K = 0 \mod {}^t\!\begin{bmatrix} p_1 & \dots & p_s \end{bmatrix}$. This proves statement (i).

To see point (ii), let us split further V_1 into $[\hat{V}_1, \check{V}_1]$ where $\hat{V}_1 \in \mathbb{Z}^{n\times(n-s)}$ and $\check{V}_1 \in \mathbb{Z}^{n\times s}$. Noting that $A\,K\,V_1 = P\,[0 \quad I_s]$ we deduce that the columns of the $(n+s)\times n$ matrix

$$\begin{bmatrix} K\,\hat{V}_1 & K\check{V}_1 \\ 0 & I_s \end{bmatrix}$$

are in the right kernel of $[A \quad -P]$.

Consider $\begin{bmatrix} L & M \end{bmatrix}$ the inverse of U, with $L \in \mathbb{Z}^{n\times(n-s)}$ and $M \in \mathbb{Z}^{n\times s}$. Then $A\,[M \quad L] = [I_s \quad 0]$. Let

$$\Omega = \begin{bmatrix} M & L & K\check{V}_1 \\ 0 & 0 & I_s \end{bmatrix}.$$

Note that Ω is unimodular since $[L \quad M]$ is unimodular. Then $[A \quad -P]\,\Omega = [I_s \quad 0]$ is in Hermite normal form. The final result comes from the fact that $L = K\,\hat{V}_1$ since $K\,V_1 = U^{-1}S = [L \quad M]\,S$. □

Theorem 6.2 thus allows one to construct the matrices defining a diagonal representation of a finite group of symmetry while at the same time constructing a matrix $V_\mathfrak{n} = KV_1$ defining a generating set of invariants. The inverse of this matrix defines the rewrite rule (Lemma 2.6 and Theorem 3.4). Thus, in the case of a polynomial system the Smith form in Theorem 6.2 gives all the information needed for a symmetry reduction according to Section 5.

Example 6.3 *In order to find an exponent matrix A and order matrix P determining the symmetry for the equations in Example 3.5 the matrix of differences on the exponents of the terms of the polynomials is given by*

$$K = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 3 & 0 & 1 \\ 0 & 1 & 2 & 0 & 2 & 0 & 0 & 3 & 1 \end{bmatrix}.$$

The Smith normal form S of K along with its left unimodular multiplier U are

$$S = \left[\begin{array}{ccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \quad \text{and} \quad U = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix}.$$

Taking the last row of U and S then gives the exponent and order matrices as

$$A = [\,1 \ -1\ 0\,] \quad \text{and} \quad P = [\,3\,]$$

which is equivalent to

$$A = [\ 1\ 2\ 0\ ] \quad \textit{and} \quad P = [\ 3\ ]$$

since $\xi^{-1} = \xi^2$ *for any cubic root of unity. The underlying symmetry group is* $\mathbb{Z}_3$*. In this case the matrix* $V_{\mathfrak{n}}$ *is given in Example 3.7.*

Example 6.4 *Consider the system of polynomial equations given by*

$$\begin{array}{rcl} x_3x_4^7x_5 - x_1^4x_2^2x_5 + 3x_2x_3^3x_4^9x_5 + 4x_1^3x_3^7x_4^7x_5^4 & = & 0 \\ x_1x_3^6x_4^3x_5 + 12x_1x_4^3x_5 - 9x_1^4x_3^9x_5^4 & = & 0 \\ 1 + x_2x_3^2x_4^8 & = & 0. \end{array}$$

In this case the matrix of exponent differences is given by

$$K = \begin{bmatrix} 4 & 0 & 3 & 0 & 3 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \\ -1 & 2 & 6 & -6 & 3 & 2 \\ -7 & 2 & 0 & 0 & -3 & 8 \\ 0 & 0 & 3 & 0 & 3 & 0 \end{bmatrix}.$$

The Smith normal form S *along with a left unimodular matrix* U *for* K *are given by*

$$S = \left[\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 12 & 0 \end{array}\right] \quad \textit{and} \quad U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -10 & -2 & 0 & 1 & 1 \\ -9 & 0 & -1 & 1 & 1 \\ -9 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

There is thus a 5-dimensional diagonal representation of the group $\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}$ *that leave those polynomials invariant. Its exponent and order matrices are given by*

$$A = \begin{bmatrix} -10 & -2 & 0 & 1 & 1 \\ -9 & 0 & -1 & 1 & 1 \\ -9 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \textit{and} \quad P = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{bmatrix}.$$

In this case V *the right unimodular multiplier of* K *is given by*

$$V = \begin{bmatrix} -2 & 0 & 0 & 0 & -3 & 0 \\ 4 & 1 & 0 & 0 & 6 & -1 \\ -4 & 0 & 1 & 0 & -11 & -2 \\ 1 & 0 & 0 & 1 & -1 & -1 \\ 7 & 0 & -1 & 0 & 15 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

with the column Hermite form of K multiplied by the first 5 columns of V given by

$$V_{\mathfrak{n}} = \begin{bmatrix} 12 & 4 & 0 & 4 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 6 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}.$$

We can also apply Theorem 6.2 to *normalize* the group and find an equivalent faithful representation. Similar ideas underly the classical proofs that any finite abelian group is isomorphic to some $\mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$. We give the explicit construction here and show some examples

Consider the n-dimensional diagonal representation defined by a matrix of exponents $B \in \mathbb{Z}^{s \times n}$ and an order matrix $Q = \operatorname{diag}(q_1, \ldots, q_s)$. Let $V_{\mathfrak{n}}$ be a matrix of exponents for a set of generating invariants as found in Theorem 3.4. Applying the construction of Theorem 6.2 to $K = V_{\mathfrak{n}}$ we obtain a faithful representation given by the exponent matrix A and order matrix P. The group is then given in its normalized form, with a divisibility condition on the orders of the generators.

Example 6.5 *Recall Example 2.2 where the diagonal subgroup of* $\mathrm{GL}_3(\mathbb{K})$ *was initially given by the exponent matrix* $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ *with order matrix* $P = \begin{bmatrix} 2 & \\ & 3 \end{bmatrix}$. *The Hermite normal form of* $[A \quad -P]$ *is* $[I_2 \quad 0]$ *and a Hermite multiplier is*

$$V = \left[\begin{array}{cc|ccc} 2 & -1 & 6 & 1 & 3 \\ -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 3 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 \end{array}\right].$$

The top right 3×3 *block* $V_{\mathfrak{n}}$ *provide the exponents of a generating set of invariants for the diagonal representation defined by the pair of matrices* (A, P). *Let us apply Theorem 6.2 to* $K = V_{\mathfrak{n}}$. *The Smith normal form of* $V_{\mathfrak{n}}$ *is given by*

$$\left[\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & -1 & -3 \end{array}\right] V_{\mathfrak{n}} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 6 \end{array}\right].$$

So the same diagonal subgroup of $\mathrm{GL}_3(\mathbb{K})$ *is defined by the exponent matrix* $A = \begin{bmatrix} 1 & -1 & -3 \end{bmatrix}$ *and order matrix* $P = \begin{bmatrix} 6 \end{bmatrix}$.

Example 6.6 *Assume a diagonal subgroup of* $\mathrm{GL}_2(\mathbb{K})$ *is given as a representation of* $\mathbb{Z}_4 \times \mathbb{Z}_2$ *by the following the exponent matrix*

$$A = \begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix}.$$

The order matrix is $P = \operatorname{diag}(4, 2)$ *and the Hermite normal form of* $[A \quad -P]$ *is given by*

$$[A \quad -P] \left[\begin{array}{cc|cc} 0 & 1 & 4 & 2 \\ 1 & -1 & 0 & 1 \\ \hline 0 & 0 & 3 & 2 \\ 0 & 0 & 2 & 1 \end{array}\right] = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

The top right 2×2 *block* $V_{\mathfrak{n}}$ *of the Hermite multiplier in the above equality provides the exponents of a generating set of invariants for the diagonal group of matrices under consideration. The Smith normal form* *of $V_{\mathfrak{n}}$ is given by*

$$\left[\begin{array}{cc} 0 & 1 \\ \hline 1 & -2 \end{array}\right] V_{\mathfrak{n}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & 4 \end{array}\right].$$

Hence the same diagonal subgroup of $\mathrm{GL}_3(\mathbb{K})$ *is defined as a faithful representation of* $\mathbb{Z}_4$ *by the exponent matrix* $A = \begin{bmatrix} 1 & -2 \end{bmatrix}$ *and order matrix* $P = \begin{bmatrix} 4 \end{bmatrix}$.

7 Conclusion

In this paper we have investigated invariants of linear action of abelian finite groups taking advantage of their diagonal representations. The close relation of such group actions to scalings previously studied by the authors [14, 15] prompted us to make use of integer linear algebra to compute invariants and rewrite rules. The primary tool used is the Hermite normal form of a matrix derived from both the exponents of the diagonal representations and the orders of the generators of the group. The unimodular multipliers determine both invariants and rewrite rules. As an application of our methods we showed how to reduce a system of polynomial equations to a new system of polynomial equations in the invariants.

We provided a minimal set of generators for the field of rational invariants of the linear action of a finite abelian group in terms of polynomials and discussed how to extend it to a set of generators for the ring of polynomial invariants. Our construction could also be applied to compute the separating set described in [20] by running the computation with different ordering of the variables.

In the present approach for abelian groups, we obtained a minimal set of generating invariants by introducing a root ξ of unity. This gives a direct constructive proof of the rationality of the field of invariants over $\mathbb{K}(\xi)$ [6, 2]. A great benefit of our approach is that it provides a simple mechanism to rewrite any rational invariants in terms of the exhibited generators. The question we might address is to determine a generating set of invariants over $\mathbb{K}$, in which case the field of invariants no longer needs to be rational [30].

We are interested in extending the concept of symmetry reductions to dynamical systems and to the case where the finite group is not abelian. We expect that our methods can be generalized to finite solvable groups and hence include all finite groups of odd order. The polynomial system of subsection 5.3 describes both situations : it is actually symmetric under the solvable dihedral group D_3 and describes the equilibrium states of a dynamical system modelling a neural network.

With respect to our use of integer linear algebra, future research will also include the use of alternate unimodular multipliers, for example one normalized not via Hermite computation but rather using LLL reduction for $V_{\mathfrak{n}}$. Similarly the Hermite form of $[A \ \ -P]$ is closely related (c.f. [1]) to the Howell form of the matrix A [9, 28]. We wish to learn if using such a form is an advantage. Finally, in some applications the matrix of exponents is sparse and hence there is a need to make use of normalized Hermite forms for sparse matrices.

References

[1] A. Bockmayr and F. Eisenbrand. Cutting planes and the elementary closure in fixed dimension. *Mathematics of Operations Research*, 26(2):304–312, 2001.

[2] A. Charnow. On the fixed field of a linear abelian group. *Journal of the London Mathematical Society*, 1(2):348–350, 1969.

[3] H. Derksen and G. Kemper. *Computational Invariant Theory.* Invariant Theory and Algebraic Transformation Groups I. Springer-Verlag, 2002.

[4] J.-C. Faugere, M. Safey El Din, and Verron T. On the complexity of computing gröbner bases for quasi-homogeneous systems. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13, pages 189–196, New York, NY, USA, 2013. ACM.

[5] J.-C. Faugere and J. Svartz. Gröbner bases of ideals invariant under a commutative group : the non-modular case. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, pages 347–354, New York, NY, USA, 2013. ACM.

[6] E. Fischer. Zur Theorie der Endlichen Abelschen Gruppen. *Mathematische Annalen*, 77(1):81–88, 1915.

[7] K. Gatermann. Symbolic solution of polynomial equation systems with symmetry. In *Proceedings of ISSAC 1990*, pages 112–119. ACM press, 1990.

[8] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, 1985.

[9] J.A. Howell. Spans in the module $(Z_m)^s$. *Linear and Multilinear Algebra*, 19:67–77, 1986.

[10] E. Hubert. Algebraic and differential invariants. In F. Cucker, T. Krick, A. Pinkus, and A. Szanto, editors, *Foundations of computational mathematics, Budapest 2011*, number 403 in London Mathematical Society Lecture Note Series. Cambridge University Press, 2012.

[11] E. Hubert. Rational Invariants of a Group Action. In P. Boito, G. Chèze, C. Pernet, and M. Safey El Din, editors, *Journees Nationales de Calcul Formel*, volume 3 of *Les cours du CIRM*, page 10p, Marseille, France, 2013. CEDRAM - Center for Diffusion of Academic Mathematical Journals.

[12] E. Hubert and I. Kogan. Rational invariants of a group action. Construction and rewriting. *Journal of Symbolic Computation*, 42(1-2):203–217, 2007.

[13] E. Hubert and I. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4):455–493, 2007.

[14] E. Hubert and G. Labahn. Rational invariants of scalings from Hermite normal forms. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'12, pages 219–226, 2012.

[15] E. Hubert and G. Labahn. Scaling invariants and symmetry reduction of dynamical systems. *Foundations of Computational Mathematics*, 13(4):479–516, 2013.

[16] T. Kamke and G. Kemper. Algorithmic invariant theory of nonreductive group. *Qualitative Theory of Dynamical Systems*, 11:79–110, 2012.

[17] G. Kemper. The computation of invariant fields and a new proof of a theorem by Rosenlicht. *Transformation Groups*, 12:657–670, 2007.

[18] B. Mourrain and P. Trebuchet. Toric border bases. in preparation, 2014.

[19] J. Müller-Quade and T. Beth. Calculating generators for invariant fields of linear algebraic groups. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 1719 of *LNCS*. Springer, 1999.

[20] M. D. Neusel and M. Sezer. Characterizing separating invariants. `http://hopf.math.purdue.edu/Neusel-Sezer/separating.pdf`, 2010.

[21] V.W. Noonburg. A neural network modeled by an adaptive Lotka-Volterra system. *SIAM Journal of Applied Mathematics*, 6:1779–1792, 1989.

[22] F. Pauer and A. Unterkircher. Gröbner bases for ideals in Laurent polynomial rings and their application to systems of difference equations. *Applicable Algebra in Engineering, Communication and Computing*, 9(4):271–291, 2 1999.

[23] V. L. Popov and E. B. Vinberg. Invariant Theory. In *Algebraic geometry. IV*, Encyclopedia of Mathematical Sciences. Springer-Verlag, 1994.

[24] A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.

[25] J-P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics.* Springer, 1996.

[26] A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology—ETH, 2000.

[27] A. Storjohann and G. Labahn. Asymptotically fast computation of Hermite Normal Forms of integer matrices. In *Proceedings of ISSAC 1996*, pages 259–266, 1996.

[28] A. Storjohann and T. Mulders. Fast algorithms for linear algebra modulo n. algorithms. In *ESA'98*, volume 1461 of *Lecture Notes in Computer Science*, pages 139–150, 1998.

[29] B. Sturmfels. *Algorithms in Invariant Theory.* Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.

[30] R. Swan. Invariant rational functions and a problem of Steenrod. *Inventiones mathematicae*, 7(2):148–158, 1969.