Rational Invariants of Finite Abelian Groups

Evelyne Hubert, George Labahn

Rational Invariants of Finite Abelian Groups

Evelyne Hubert * George Labahn †

December 22, 2013

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.

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

1 Introduction

Recently Faugère and Svartz [4] 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. We observe that these diagonal actions have strong similarities with scalings that we had previously investigated in [10, 11]. Scalings are diagonal representations of the torus and can be defined by a matrix of exponents. In [10, 11] integer linear algebra was applied to compute the invariants of scalings and develop their applications. It was shown that the Hermite form of the exponent matrix, together with an associated unimodular multiplier, provide the exponents of monomials that describe a 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 rewriting rules. From a unimodular multiplier associated to a 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 great feature we exhibit is that we can choose the generating set of invariants to consist of monomials with non negative powers. Such a set comes with a triangular shape. Furthermore it provides generators for an algebra that is the localisation of the polynomial ring. This latter can therefore be obtained with subsequent computations.

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 the original system and its the number of variables is the same. The complete set of solutions of the original

*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

system is obtained from the solutions of the reduced system by solving a binomial triangular set. To compute the reduced system, we first adapt a concept of degree from [4] to split the polynomials in the system into invariants. We then use our special set of polynomial invariants and the associated rewrite rules to obtain the reduced system. Obtaining our reduced system is efficient as our main cost 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 results generalize to linear representation 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 we have an explicit substitution to rewrite any invariants in terms of these. 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 [21, 3]. Yet some applications can be approached with rational invariants[1]. Indeed a generating set of rational invariants separates generic orbits. The class of rational invariants can furthermore address a wider class of nonlinear actions, such as the those central in differential geometry[2] and algebraically characterize classical differential invariants [9, 7]. General algorithms to compute rational invariants of (rational) action of algebraic groups [8, 12, 13, 14] 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 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. Section 4 gives the details of the symmetry reduction scheme for polynomial systems. Section 5 deals with the case of arbitrary finite abelian group actions including examples illustrating our methods. Finally, we present topics for future research in the conclusion.

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 [10, 11]. 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 $a = [a_1, \ldots, a_s]^T$ 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 indeterminates, 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.

[1] For instance multi-homogeneous polynomial system solving in [10] and parameter reduction in dynamical models [11].
[2] Like conformal transformations or prolonged actions to the jet spaces.

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:

$$x \star y = [x_1 y_1, \ldots, x_n y_n]$$

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 [10] that

(a) $\lambda^{A+B} = \lambda^A \star \lambda^B$

(b) $\lambda^{AC} = (\lambda^A)^c$,

(c) $(y \star z)^A = y^A \star z^A$.

(d) 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 $\mathcal{Z} = \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$. All along the paper we assume that the characteristic of $\mathbb{K}$ does not divide $p = \mathrm{lcm}(p_1, \ldots, p_s)$. We asssume furthermore 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:

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

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 and *order matrix* $P = \mathrm{diag}\,(p_1, \ldots, p_s) \in \mathbb{Z}^{s \times s}$.

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 being given explicitely 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 $P = \mathrm{diag}\,(p_1, \ldots, p_s)$ is also the image of the representation

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

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

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

One then draws a clear analogy with [10, 11] 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 $\xi^2 + \xi + 1 = 0$, i.e. ξ is a primitive 3^{rd} 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 $p_1 | p_2 | \ldots | p_s$ [18]. In this article we do not enforce this canonical divisibility condition.

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* [17]. In the case of full rank matrices the Hermite form is an upper triangular matrix with positive non-zero 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 A there exists a unimodular matrix V such that AV 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 multiplier V where $A \cdot V$ is in Hermite form will be referred to as a *Hermite multiplier*.

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 $A \in \mathbb{Z}^{s \times n}$. Consider the Hermite normal form

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

with a Hermite multiplier V partitioned as

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

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

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

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

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

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 [10, 11]. 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 $P = \mathit{diag}(3,3)$ be the exponent and order matrices that defined the group of diagonal matrices in Example 2.1. In this case $[A \;\; -P]$ has Hermite form $[I_2 \;\; 0]$ 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. In this case a second set of unimodular multipliers satisfying $[A \;\; -P] \cdot V = [I_2 \;\; 0]$ 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 repect to the columns of V_n.

Lemma 2.4 *We can always choose a Hermite multiplier*

$$V = \begin{bmatrix} V_i & V_n \\ P_i & P_n \end{bmatrix}$$

for $[A \;\; -P]$ such that

$$\begin{bmatrix} 0 & I_n \\ -P & A \end{bmatrix} \cdot \begin{bmatrix} P_n & P_i \\ V_n & V_i \end{bmatrix} = \begin{bmatrix} V_n & V_i \\ 0 & H \end{bmatrix} \tag{1}$$

is in column Hermite form. Then V is the normalized Hermite multiplier.

The uniqueness of $V_{\mathfrak{n}}$ in the normalized Hermite multiplier is guaranteed by the uniqueness of the Hermite form. While the notion of normalized Hermite multiplier appears to only involve $V_{\mathfrak{n}}$ and $V_{\mathfrak{i}}$ 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.

Finding a normalized Hermite form costs $O((n+s)^4 d)$ where d is the size of the largest p_i (c.f. [19, 20]). Furthermore, since V is produced from column operations the W matrix can be computed simultaneously with minimal cost by the inverse column operations.

Taking determinants on both sides of Equation (1) 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*

$$p_1 \cdot p_2 \cdots p_s = \det(H) \cdot \det(V_{\mathfrak{n}}). \tag{2}$$

3 Invariants of finite groups of diagonal matrices

We consider $A \in \mathbb{Z}^{s\times n}$ a full row rank matrix, $P = \operatorname{diag}(p_1, \ldots, p_s)$, where $p_i \in \mathbb{N}$, and $\mathbb{K}$ a field whose characteristic does not divide $p = \operatorname{lcm}(p_1, \ldots, p_s)$. 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 the 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 us with 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 non negative powers for which we can bound the degrees. This leads us to 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 [10, 11] then z^v is 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 $v \in \operatorname{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$.*

PROOF: Assume z^v is invariant. Then $Av = 0 \mod {}^t(p_1, \ldots, p_s)$, that is, there exists k such that $\begin{bmatrix} v \\ k \end{bmatrix} \in \ker_{\mathbb{Z}} \begin{bmatrix} A & -P \end{bmatrix} = \mathrm{colspan}_{\mathbb{Z}} \begin{bmatrix} V_{\mathfrak{n}} \\ P_{\mathfrak{n}} \end{bmatrix}$. Hence $v \in \mathrm{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$. Conversely if $v \in \mathrm{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ 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.

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*

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

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

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 $w - u \in \mathrm{colspan}_{\mathbb{Z}}\, V_{\mathfrak{n}}$ 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 $v \in \mathrm{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ such that $w = u + v$ for all w with b_w in the support of q. □

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

PROOF: Note first that $-P = HP_{\mathfrak{u}}$ so that $P_{\mathfrak{u}}$ is invertible. By hypothesis, there is $u \in \mathbb{Z}^n$ such that $v = V_{\mathfrak{n}} u$. Then $W_{\mathfrak{u}} v = W_{\mathfrak{u}} V_{\mathfrak{n}} u = -P_{\mathfrak{u}} P_{\mathfrak{n}} u$ and thus $P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} v = -P_{\mathfrak{n}} u$. Multiplying both sides on the left by $P_{\mathfrak{d}}$ we obtain $P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} v = -P_{\mathfrak{d}} P_{\mathfrak{n}} u = (W_{\mathfrak{d}} V_{\mathfrak{n}} - I)\, u$ so that $u = (W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}})\, v$. Finally, multiplying both sides by $V_{\mathfrak{n}}$ we obtain the desired result. □

Remark 3.4 *Note 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*

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

Here $P_{\mathfrak{u}}$ is nonsingular since $H \cdot P_{\mathfrak{u}} = -P$ and H is nonsingular. The Schur complement in this case describes the column operations that eliminate the top left matrix in W. That is,

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

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

Theorem 3.5 *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 [16, Section 2.9].

Example 3.6 *Consider the 3 polynomials in $\mathbb{K}[z_1, z_2, z_3]$ given by*

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

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

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

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

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

□

3.2 Polynomial generators

Just as the Hermite multiplier, the set of generating rational invariants is not canonical. For each order of the variables $(x_1, \ldots, x_n)$ there is nonetheless a generating set with desirable features. This leads us to discuss polynomial invariants.

Theorem 3.7 *There is a minimal generating set of invariants that consists of a triangular set of monomials with non-negative 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. 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 giving part (i). Part (ii) follows from Corollary 2.5 since

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

Part (iii) follows from the fact that $V_{\mathfrak{n}}$ is in column Hermite form. □

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 3.11.

Example 3.8 *For the integer matrices* $A \in \mathbb{Z}^{1\times 3}$ *and* $P = [3]$ *from Example 3.6 we can also determine that the normalized Hermite multiplier is*

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

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

$$g_1 \ = \ z_1^3, \quad g_2 \ = \ z_1 z_2, \quad g_3 \ = \ z_3$$

and a set of rewrite rules is given by

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

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 3.5 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 3.7.

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 $\ker[A \ -P] \cap \mathbb{N}^n$ [21, 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 Reynold operator can be omitted. Here, in one round of linear algebra, we nonetheless have 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 [21, 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 3.5 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 3.9 *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 3.11, the output can be combinatorially large.

Example 3.10 *Continuing with Example 3.8, we can obtain the generators for $\mathbb{K}[z]^{\mathcal{D}}$ as follows. Consider the Gröbner basis $\tilde{Q}$ for*

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

according to a term order that eliminates 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

$$\tilde{Q} = \left\{z_3 - x_3, z_1\,z_2 - x_1\,x_2, z_2\,x_1^2 - x_2\,z_1^2, z_2^2\,x_1 - x_2^2\,z_1, z_2^3 - x_2^3, z_1^3 - x_1^3, -1 + x_1^3\,w, x_1\,x_2\,w\,z_1^2 - z_2, x_1^2\,x_2^2\,z_1\,w - z_2^2\right\}.$$

Take $Q = \tilde{Q} \cap \mathbb{K}[z,x]$ and subsitute x_1, x_2, x_3 by 0. The non zero elements are the monomials $\left\{z_3, z_1\,z_2, z_2^3, z_1^3\right\}$. They form a generating set for $\mathbb{K}[z]^{\mathcal{D}}$.

3.3 Additional examples

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

$$\xi I_n = \begin{bmatrix} \xi & & \\ & \ddots & \\ & & \xi \end{bmatrix}, \tag{3}$$

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

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

Hence

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

The generating invariants of Theorem 3.5 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

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

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

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

Though simple, this example is interesting as it shows the sharpness of Noether's bound for the generators of polynomial invariant rings [21, 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 3.12 *Consider the subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element*

$$D_\xi = \begin{bmatrix} \xi & & & & \\ & \xi^2 & & & \\ & & \ddots & & \\ & & & \xi^{n-1} & \\ & & & & 1 \end{bmatrix} \tag{4}$$

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 a group of cyclic permutations that we will examine in Example 5.3.

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 3.5, 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 3.5, the set of rewrite rules is given by

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

Example 3.13 *Consider the subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$ generated by*

$$\xi I_n = \begin{bmatrix} \xi & & & & \\ & \xi & & & \\ & & \ddots & & \\ & & & \xi & \\ & & & & \xi \end{bmatrix} \quad \text{and} \quad D_\xi = \begin{bmatrix} \xi & & & & \\ & \xi^2 & & & \\ & & \ddots & & \\ & & & \xi^{n-1} & \\ & & & & 1 \end{bmatrix} \tag{5}$$

where ξ is a nth root of unity. The group $\mathcal{D}$ is specified by the exponent matrix $A = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 2 & 3 & \ldots & n-1 & 0 \end{bmatrix}$ and the order matrix $P = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$. The Hermite form of $[A, -P]$ is $[A, -P] \cdot V = [I_2, 0]$ and its normalized Hermite multiplier 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 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 [4, 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.

4.1 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 by the linear (diagonal) action of $\mathcal{U}$ defined by the exponent matrix $A \in \mathbb{Z}^{s \times n}$, that is, if $z \in (\bar{\mathbb{K}}^*)^n$ is such that $f(z) = 0$, $\forall f \in F$ then $f(\lambda^A \star z) = 0$, $\forall \lambda \in \mathcal{U}$ and $\forall f \in F$.

Definition 4.1 *The A-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* $A\,u \mod (p_1, \ldots, p_s)$.

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

The following proposition shows that our simple definition of A-degree matches the notion of $\mathcal{Z}$-degree in [4, Section 3.1].

Proposition 4.2 *If* $f \in \mathbb{K}[z, z^{-1}]$ *is A-homogeneous of A-degree d then* $f\left(\lambda^A \star z\right) = \lambda^d f$ *for all* $\lambda \in \mathcal{U}$.

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

A question raised in [4] is whether there are monomials of any given A-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-degree d. These are the $z^{u+V_{\mathfrak{n}} v}$ where $u = V_{\mathfrak{i}}\, d$ and $v \in \mathbb{Z}^n$.

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

Proposition 4.3 *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

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

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 $\left(\xi_i^{(k-1)(l-1)}\right)_{1 \le k,l \le p_i}$, for $1 \le i \le s$ 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. $\square$

Proposition 4.4 *If $f \in \mathbb{K}[z, z^{-1}]$ is A-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-homogeneous of A-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 $(\bar{\mathbb{K}}^*)^n$.

4.2 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 that $V_{\mathfrak{n}}$ is triangular. By Theorem 3.5, 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 the substitution. The polynomial $\mathfrak{f}$ is the *symmetry reduction of f*.

Theorem 4.5 *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 3.7. 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 $\prod_{i=1}^s p_i / \det H$ 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 4.6 *Continuing with Example 3.6, 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

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

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 cube root of 1.

5 Invariants of finite abelian groups of matrices

Representations of finite abelian groups can be diagonalized. As such that 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

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

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 [6] : 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 $D_i = \Xi^{-1} \cdot G_i \cdot \Xi$, $1 \le i \le s$.

Proposition 5.1 *Take $f, g \in \mathbb{K}(z_1, \ldots, z_n)$ with $f(z) = g(\Xi z) \Leftrightarrow f(z) = g(\Xi^{-1} z)$. Then g is invariant for $\mathcal{D}$ if and only if f is an invariant for $\mathcal{G}$.*

Theorem 5.2 *Consider an abelian group $\mathcal{G}$ of order p, $\mathbb{K}$ of characteristic not dividing p 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 5.1, this is actually a corollary to Theorem 3.7. 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 and show how the symmetry reduction scheme of Section 4 extends to this situation.

Example 5.3 *Let $\mathcal{G}$ be the subgroup of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element:*

$$M_\sigma = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{bmatrix}. \tag{6}$$

We consider its obvious linear action on $\mathbb{K}^n$. 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. Furthermore, any rational invariants of $\mathcal{G}$ can be written in terms of $(g_1, \ldots, g_n)$ with the following substitution.

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

where

$$\Xi(\xi) = \left(\xi^{ij}\right)_{1 \leq i,j \leq n} = \begin{bmatrix} \xi & \xi^2 & \ldots & \xi^{n-1} & 1 \\ \xi^2 & \xi^4 & \ldots & \xi^{2(n-1)} & 1 \\ \vdots & & & & \\ \vdots & & & \vdots & \vdots \\ \xi^{n-1} & \xi^{2(n-1)} & \ldots & \xi^{(n-1)(n-1)} & 1 \\ 1 & 1 & \ldots & 1 & 1 \end{bmatrix} \tag{7}$$

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

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

The underlying group of diagonal matrices is the group examined in Example 3.12.

Example 5.4 *Let $\mathcal{G}$ be the subgroup of $\mathrm{GL}_n(\mathbb{K})$ generated by the matrices*

$$\xi I_n = \begin{bmatrix} \xi & & & & \\ & \xi & & & \\ & & \ddots & & \\ & & & \xi & \\ & & & & \xi \end{bmatrix} \quad \text{and} \quad M_\sigma = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix} \tag{8}$$

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

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

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

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

where $\Xi(\xi)$ is as in Example 5.3.

Indeed, the group $\mathcal{D} = \Xi^{-1}\,\mathcal{G}\,\Xi$ is generated by the diagonal matrices $\mathrm{diag}(\xi, \xi, \dots, \xi)$ and $\mathrm{diag}(\xi, \dots, \xi^{n-1}, 1)$ and it was considered in Example 3.13.

6 Conclusion

In this paper we investigated invariants of linear action of commutative finite groups taking advantage of their diagonal representations. The close relation of such group actions to scalings previously studied by the authors [10, 11] prompted us to make use of integer linear algebra to compute invariants and rewrite rules. The primary tool used was the Hermite normal forms and their unimodular multipliers of a matrix derived from both the exponents of the diagonal actions and the orders of the generators in order to 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 have showed how to compute a generating set for the ring of polynomial invariants based on the knowledge of the localisation provided by our contruction. Our construction could also be applied to compute the separating set described in [15] by running the computation with different ordering of the variables.

In the present approach of 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 $\mathbb{K}(\xi)$ [5, 2]. The real 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 [22].

We are in the process of extending the concept of symmetry reductions to the case where the finite group is not abelian. In this case we mention finite solvable groups where one can recursively use our symmetry reductions to obtain invariants.

Finally, 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 $V_{\mathtt{n}}$. Similarly the Hermite form of $[A \ -P]$ seems to be closely related [1] to the Howell form of a matrix [19] and so we wish to learn if using such a form will be an advantage. Finally, in some applications the matrix of exponents is sparse and hence there is the need for 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 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.

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

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

[7] 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. Cambrige University Press, 2012.

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

[9] 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.

[10] 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.

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

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

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

[14] 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.

[15] M. D. Neusel and M. Sezer. Separating invariants for modular p-groups and groups acting diagonally. *Math. Res. Lett.*, 16(6):1029–1036, 2009.

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

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

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

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

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

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

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