MATHEMATICS OF COMPUTATION
Volume 85, Number 302, November 2016, Pages 3029–3050
http://dx.doi.org/10.1090/mcom/3076
Article electronically published on January 14, 2016

COMPUTATION OF INVARIANTS OF FINITE ABELIAN GROUPS

EVELYNE HUBERT AND GEORGE LABAHN

ABSTRACT. We investigate the computation and applications of rational invariants of the linear action of a finite abelian group in the nonmodular case. By diagonalization, such a group action can be described by integer matrices of orders and exponents. We make use of integer linear algebra to compute a minimal generating set of invariants along with the substitution needed to rewrite any invariant in terms of this generating set. In addition, we show how to construct a minimal generating set that consists only of polynomial invariants. As an application, we provide a symmetry reduction scheme for polynomial systems whose solution set is invariant by a finite abelian group action. Finally, we also provide an algorithm to find such symmetries given a polynomial system.

1. INTRODUCTION

Recently Faugère and Svartz [10] demonstrated how to reduce the complexity of Gröbner bases computations for ideals stable by the linear action of a finite abelian group in the nonmodular case. A typical example used is a cyclic group of permutations of the variables. Their strategy is based on the diagonalization of the group. It turns out that these diagonal actions have strong similarities with scalings that the present authors previously investigated in [21, 22]. 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 [21, 22]. 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.

The field of rational invariants of abelian groups has been thoroughly examined, in particular with respect to Noether's problem that questions the existence of an algebraically independent generating set [3, 4, 11, 12, 26, 39]. In this paper we first address the constructive aspect of this problem. In the light of the treatment of scalings we specify diagonal representations of finitely generated abelian groups with an exponent matrix. But now, when performing linear algebra operations on this exponent matrix, each row needs to be understood modulo the order of a group generator. This is elegantly handled by introducing those orders in a diagonal matrix. With this succinct presentation of the problem we establish analogous constructions : From a unimodular multiplier associated to the Hermite form of the

Received by the editor January 24, 2014 and, in revised form, September 4, 2014 and April 27, 2015.

2010 *Mathematics Subject Classification.* Primary 13A50, 15A72; Secondary 12Y05, 13P25, 13P15, 14L30.

Key words and phrases. Finite groups, rational invariants, matrix normal form, polynomial system reduction, constructive Noether's problem.

exponent and order matrices, we can compute a minimal set of generating rational invariants. The rationality of the field of invariants [11] is thus established as a byproduct of our direct and constructive proof. An additional important feature is that we can compute a minimal generating set of invariants that consists of monomials with nonnegative powers. Only the existence of such a set was previously established in [4]. Our minimal generating set comes with a triangular shape and provides generators for an algebra that is an explicit localization of the polynomial ring of invariants. They can be further exploited to compute the generators for the ring of polynomial invariants. Furthermore, for any generating set computed with our construction, any other invariant can be written in terms of these by an explicit substitution, one that is computed simultaneously.

As an application we show how one can reduce a system of polynomial equations whose solution set is invariant by the linear action of a finite abelian group to a reduced system of polynomial equations, with the invariants as new variables. The reduced system thus has the same number of variables, and to each of its solutions corresponds an orbit of solutions of the original system. The latter are retrieved as the solutions of a binomial triangular set. To compute the reduced system, we first adapt a concept of degree from [10] in order 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. A 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 polynomial system solving strategy contrasts with that of [10], where there is no change of variables. Instead, the invariance gives a block diagonal structure of the matrices arising in the F4, F5 and FGLM algorithms used to compute the Gröbner basis [6–8]. Both approaches start from the knowledge of the symmetry of the solution set. Although it is sometimes intrinsically known, we also provide a way to determine this symmetry. We had previously solved the analogous problem for scaling symmetry in [22] through the computation of a Hermite form. The problem in the present case 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 exponent differences of the terms in the polynomials. We show that the order matrix is read from the Smith normal form itself, while the exponent matrix is read from the left unimodular multiplier. Additionally, a generating set of invariants for the symmetry group defined in this way is also obtained directly from the left unimodular multiplier. The Smith normal form and its unimodular multipliers thus provide all the ingredients for a symmetry reduction scheme.

The computational efforts for invariant theory have focused on the ring of polynomial invariants [5, 38]. 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 problems that come in many guises. Furthermore, the class of rational invariants can address a wider class of

[1]For instance multi-homogeneous polynomial system solving in [21] and parameter reduction in dynamical models [22].

nonlinear actions, such as those central in differential geometry,[2] and algebraically characterize classical differential invariants [17,20]. General algorithms to compute rational invariants of a (rational) action of algebraic groups [18,19,23,25,29] rely on Gröbner bases computations. It is remarkable how much simpler and more effective the present approach is for use with finite abelian groups.

The remainder of the paper is organized as follows. Preliminary information about abelian group 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. 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 diagonal representation of a finite abelian group that provides a symmetry for the solution set of a given system of polynomial equations. Finally, we present a conclusion along with topics for future research.

2. Preliminaries

In this section we introduce our notation for finite groups of diagonal matrices and their linear actions. In addition we will present the various notions from integer linear algebra used later in this work. We shall use the matrix notation that was already introduced in [21,22].

2.1. **Matrix notation 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 s 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.

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 then easy to prove [21] 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]For example, conformal transformations or prolonged actions to the jet spaces.

2.2. **Finite groups of diagonal matrices.** Consider the group $\mathcal{Z} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$. Throughout this paper we assume that the characteristic of $\mathbb{K}$ does not divide $p = \operatorname{lcm}(p_1, \ldots, p_s)$ and that $\mathbb{K}$ contains a pth primitive root of unity ξ. Then $\mathbb{K}$ also 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 $B \in \mathbb{Z}^{s\times n}$ defines an n-dimensional diagonal representation of the group $\mathcal{Z}$ given as

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

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* $B \in \mathbb{Z}^{s\times n}$ 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 $\mathcal{Z} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$ is isomorphic to the group $\mathcal{U} = \mathbb{U}_{p_1} \times \cdots \times \mathbb{U}_{p_s}$, with 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 matrix $B \in \mathbb{Z}^{s\times n}$ is also the image of the representation

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

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

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

We shall alternatively use the two representations for convenience of notation. With the latter, one draws a clear analogy with [21, 22], where we dealt with the group $(\mathbb{K}^*)^r$ rather than $\mathcal{U}$. But now the ith row of B is to be understood modulo p_i.

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 then the (diagonal matrix) group specified by the exponent matrix $B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ and 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

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

Any finite abelian group is isomorphic to $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$ where $p_1 | p_2 | \ldots | p_s$. However, 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 in Section 6.

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* [34]. 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 $\hat{B} \in \mathbb{Z}^{s\times(n+s)}$ there exists a unimodular matrix $V \in \mathbb{Z}^{(n+s)\times(n+s)}$ such that $\hat{B}\,V$ 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 $\hat{B}\,V$ is in Hermite normal form will be referred to as a *Hermite multiplier* for $\hat{B}$.

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

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

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

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

and

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

Furthermore,

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

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 [21, 22]. 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 2.2. Let $B \in \mathbb{Z}^{2\times 3}$ 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

$[B\ \ -P]$ 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. For example in this case a second set of unimodular multipliers satisfying $[B\ \ -P]\,V = [I_2\ 0]$ and $W = V^{-1}$ are given by

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

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

The fact that Hermite multipliers are not unique is not surprising. 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 2.3. *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* $[B\ \ -P]$ *such that*

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

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

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 2.4. *Let* V *be the normalized Hermite multiplier for* $[B\ \ -P]$ *with Hermite form* $[H\ 0]$. *Then* $V_{\mathfrak{n}}$ *is nonsingular and* $p_1 \cdot p_2 \cdots p_s = \det(H) \cdot \det(V_{\mathfrak{n}})$.

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 involve only $V_{\mathfrak{i}}$ and $V_{\mathfrak{n}}$ and does not say anything about $P_{\mathfrak{i}}$ or $P_{\mathfrak{n}}$, it is the additional fact that V is a Hermite multiplier that ensures uniqueness.

Lemma 2.3 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 (cf. [35, 36]). 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 to have a formula for the inverse of $V_{\mathfrak{n}}$.

Lemma 2.5. *With V and W partitioned as* (1) *and* (2) *we have that*

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

Proof. We show first that $(W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B) V_{\mathfrak{n}} = I_n$. From $W\,V = I_{n+s}$ we deduce $W_{\mathfrak{d}} V_{\mathfrak{n}} + P_{\mathfrak{d}} P_{\mathfrak{n}} = I_n$, while from $\begin{bmatrix} B & -P \end{bmatrix} V = \begin{bmatrix} H & 0 \end{bmatrix}$ we deduce $B V_{\mathfrak{n}} = P\,P_{\mathfrak{n}}$. Hence $(W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B) V_{\mathfrak{n}} = I_n$.

Consider now the equality $\begin{bmatrix} B & -P \end{bmatrix} = \begin{bmatrix} H & 0 \end{bmatrix} W$. This implies $B = H\,W_{\mathfrak{u}}$ and $P = -H\,P_{\mathfrak{u}}$. Since H is nonsingular, so is $P_{\mathfrak{u}}$. Hence $B = -P P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}$ so that $P^{-1} B = -P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}}$. □

Since we can compute V and its inverse W simultaneously, the formula in Lemma 2.5 for the inverse of $V_{\mathfrak{n}}$ has the advantage that it requires only the inversion of the $s \times s$ diagonal matrix P. As a side remark, note that the equality

$$(4) \qquad \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix} \begin{bmatrix} I & 0 \\ -P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} & P_{\mathfrak{u}}^{-1} \end{bmatrix} = \begin{bmatrix} 0 & I \\ W_{\mathfrak{d}} - P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} W_{\mathfrak{u}} & P_{\mathfrak{d}} P_{\mathfrak{u}}^{-1} \end{bmatrix}$$

implies that the inverse of $V_{\mathfrak{n}}$ is in fact the Schur complement of the block $P_{\mathfrak{u}}$ in the matrix W written as in (2). 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

Let $B \in \mathbb{Z}^{s \times n}$ and $P = \operatorname{diag}(p_1, \ldots, p_s)$ where $p_i \in \mathbb{N}$, $p_i \neq 0$, and $\mathbb{K}$ is 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 (B, P) thus defines a finite group $\mathcal{D}$ of diagonal matrices that can be seen as an n-dimensional representation of $\mathcal{U} = \mathbb{U}_{p_1} \times \cdots \times \mathbb{U}_{p_s}$, where $\mathbb{U}_{p_i}$ is the group of p_ith roots of unity. With the matrix notation introduced in Section 2, the induced linear action is given as

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

A *rational invariant* is an element f of $\mathbb{K}(z)$ such that $f(\lambda^B \star z) = f(z)$ 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 $[B\ -P]$ provides a complete description of the field of rational invariants. Indeed we show that the matrix V along with its inverse W provides 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 notation for the Hermite form introduced in the previous section : $\begin{bmatrix} B & -P \end{bmatrix} V = \begin{bmatrix} H & 0 \end{bmatrix}$ 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 $(\lambda^B \star z)^v = z^v$ for any $\lambda \in \mathcal{U}$. This amounts to $\lambda^{Bv} = 1$, for all $\lambda \in \mathcal{U}$. When we considered in [21, 22] the action of $(\mathbb{K}^*)^r$ determined by $A \in \mathbb{Z}^{r\times n}$, z^v was invariant if and only if $Av = 0$. In the present case we have:

Lemma 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 $Bv = 0 \mod {}^t(p_1, \ldots, p_s)$; that is, there exists $k \in \mathbb{Z}^s$ such that $\begin{bmatrix} v \\ k \end{bmatrix} \in \ker_{\mathbb{Z}} \begin{bmatrix} B & -P \end{bmatrix} = \operatorname{colspan}_{\mathbb{Z}} \begin{bmatrix} V_{\mathfrak{n}} \\ P_{\mathfrak{n}} \end{bmatrix}$. 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 $BV_{\mathfrak{n}} = PP_{\mathfrak{n}}$ we have $Bv = Pk$ 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 [33]. 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*

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

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

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

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

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

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

For $p(\lambda^B \star z)$ to factor as $\chi(\lambda) p(z)$ we must have $\lambda^{Bw} = \lambda^{Bu}$ 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 Lemma 3.1 we have $w - u \in \operatorname{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ and $\chi(\lambda) = \lambda^{Bu}$. From the previous paragraph we have $\sum_{w \,\in\, \mathbb{Z}^n} b_w \lambda^{Bw} \, z^w = q(\lambda^B \star z) = \lambda^{Bu} q(z) = \lambda^{Bu} \sum_{w \,\in\, \mathbb{Z}^n} b_w \, z^w$. Thus $Bu = Bw$ and therefore there exists $v \in \operatorname{colspan}_{\mathbb{Z}} V_{\mathfrak{n}}$ such that $w = u + v$ for all w with b_w in the support of q. ☐

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

Theorem 3.3. *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*

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

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 observation that for $v \in \operatorname{colspan}_{\mathbb{Z}}(V_{\mathfrak{n}})$ we have $v = V_{\mathfrak{n}}\left(W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B\right) v$, which follows directly from Lemma 2.5. □

We therefore retrieve in a constructive way the fact that $\mathbb{K}(z)^{\mathcal{D}}$ is rational. The rationality of the field of invariants of a diagonal representation was established in [11] by observing that the monomial invariants formed a subgroup of the free abelian group of Laurent monomials. Monomial invariants thus form a free group. Rationality of the field of invariants was also proved for more general classes of actions [3, 24, 27], [33, Section 2.9].

Example 3.4. Consider the three polynomials in $\mathbb{K}[z_1, z_2, z_3]$ given by

$$f_1 = {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 - z_1\, z_2\, z_3 + 8,\; f_2 = {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 + 7,$$
$$f_3 = z_1^6 z_2^3 z_3^3 - 3 z_1^4 z_2^4 z_3 + z_1^6 + 32 z_1^3 + z_2^3.$$

They are invariants for the group of diagonal matrices defined by the exponent matrix and order matrix of Example 2.2. Thus a generating set of invariants is given by $g_1 = z_1^3$, $g_2 = z_2^3$, $g_3 = z_1 z_2 z_3$, and a set of rewrite rules is given by

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

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

$$f_1 = {g_3}^2 - g_2 - g_3 + 8,\ f_2 = {g_3}^2 - g_2 + 7,\ f_3 = g_1 {g_3}^3 - 3 g_1 g_2 g_3 + g_1^2 + 32 g_1 + g_2.$$

Note that the set of generators is polynomial and triangular. This is actually a general feature that is uncovered with the use of normalized Hermite multipliers.

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 3.5. *There is a minimal generating set of invariants that consists of a triangular set of monomials with nonnegative powers, that is, of the form*

(5)
$$\left\{\ z_1^{m_1},\ z_1^{v_{1,2}} z_2^{m_2},\ \ldots\ ,\ z_1^{v_{1,n}} \cdots z_{n-1}^{v_{n-1,n}} z_n^{m_n}\ \right\}, \quad \text{where } 0 \le v_{i,j} < m_i \text{ for all } i < j.$$

More specifically this set of generators is given by $z^{V_{\mathfrak{n}}}$ where $V_{\mathfrak{n}}$ is the right upper block in the normalized Hermite multiplier for $[B \;\; -P]$. Hence the exponents m_i satisfy

$$m_1 \ldots m_n = \frac{p_1 \cdots p_s}{\det H}\ . \tag{6}$$

Proof. From Lemma 2.3 there exists a normalized Hermite multiplier V for $[B \; -P]$. Equation (5), then follows since $V_{\mathfrak{n}}$ is in Hermite form. The second identity, equation (6) then follows from Corollary 2.4 since $p_1 \cdot p_2 \cdots p_s = \det(H) \cdot \prod_{i=1}^{n} m_i$. □

The existence of a minimal generating set consisting of polynomials was already known in [4]. There the existence proof proceeds recursively so that the triangular shape of such a generating set was already established also. The above approach provides a more direct proof with the great benefit of being constructive.

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 thus do not improve on Noether's bound. It is not difficult to find examples where this bound can be reached. As pointed out by a referee, this bound on the degree of the polynomial generators of the field of rational invariants also exists for the regular actions of any finite group, even in the modular case. For example, in [13, Section 2] one finds an elegantly simple construction for such a generating set of bounded degree. However the set is not minimal, is not a set of monomials as in the case of interest here, and finally does not come with rewrite rules.

Note that Theorem 3.3 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 invariant (Laurent) polynomial as a Laurent polynomial in the (polynomial) generators of $\mathbb{K}(z)^{\mathcal{D}}$ provided by Theorem 3.5.

If we wish to obtain generators for $\mathbb{K}[z]^{\mathcal{D}}$, there are several general algorithms [5,13,38]. We can also extend our construction by applying the results in [5, Section 4.2.1] since the rewrite rules contain the following additional information. 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 3.3 implies that the localization $\mathbb{K}[x]_h^{\mathcal{D}}$ is equal to $\mathbb{K}[h^{-1}, g_1, \ldots, g_n]$.

4. Invariants of finite abelian groups of matrices

In the nonmodular case, representations of finite abelian groups can be diagonalized so that we can apply the results described so far. In this section we illustrate such a diagonalization process and work out two 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

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

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 pth roots of unity. Since the elements of $\mathcal{G}$ commute, they are simultaneously diagonalizable [15] : 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 $\mathcal{G}$.*

As a consequence of Theorem 3.5, any 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. We can furthermore compute the polynomial generators explicitly, as well as the rewrite rules, by first diagonalizing the representation of the group.

Example 4.2. Let $\mathcal{G}$ be the subgroup of $\mathrm{GL}_n(\mathbb{K})$ generated by the single element

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

$\mathcal{G}$ is the natural linear representation of the cyclic group of permutations $(n, n-1, \dots, 1)$. M_σ is the companion matrix of the polynomial $\lambda^n - 1$, so its eigenvalues are the nth roots of unity. If ξ is a primitive nth root, then a matrix of eigenvectors is given by $\Xi(\xi) = \left(\xi^{ij}\right)_{1 \le i,j \le n}$. Hence

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

The group $\mathcal{D}$ is specified by the exponent matrix $B = \begin{bmatrix} 1 & 2 & 3 & \dots & n-1 & 0 \end{bmatrix}$ and the order matrix $P = \begin{bmatrix} n \end{bmatrix}$. The Hermite form, normal Hermite multiplier and inverse for $[B, -P]$ gives $H = [\ 1\ 0 \cdots 0]$,

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

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

This gives a set of generating invariants as

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

that is, $g_k = z_1^{n-k} z_k$ for $1 \le k \le n$, and associated rewrite rules

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

that is,

$$z_k \to \frac{g_k}{g_1^{\frac{n-k}{n}}}, \; 1 \leq k \leq n.$$

The following n polynomials then generate the field of rational invariants for $\mathcal{G}$:

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

where ξ is a primitive nth root of unity.

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

$$\begin{pmatrix} z_1 & z_2 & z_3 & \cdots & z_n \end{pmatrix}^t \to \Xi(\xi)^{-1} \left(g_1^{\frac{1}{n}}, g_2\, g_1^{\frac{2-n}{n}}, \dots, g_{n-1}\, g_1^{\frac{-1}{n}}, g_n\right)^t$$

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

Example 4.3. Let $\mathcal{G}$ be the subgroup of $\mathrm{GL}_n(\mathbb{K})$ generated by the matrices ξI_n and M_σ from the previous example, where ξ is a primitive nth root of unity. We consider its obvious linear action on $\mathbb{K}^n$. As in the previous example this group is diagonalized via the matrix $\Xi(\xi) = \left(\xi^{ij}\right)_{1\leq i,j\leq n}$ with the corresponding diagonal subgroup $\mathcal{D}$ of $\mathrm{GL}_n(\mathbb{K})$ generated by

$$\xi I_n \quad \text{and} \quad D_\xi = \mathrm{diag}\,(\xi, \xi^2, \dots, \xi^{n-1}, 1).$$

$\mathcal{D}$ is then specified by the exponent and order matrices $B = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 2 & 3 & \dots & n-1 & 0 \end{bmatrix}$ and $P = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$. Computing the Hermite form, normal Hermite multiplier and its inverse for $[B, -P]$ gives $[I_2, 0]$,

$$V = \left[\begin{array}{cc|ccccccc}
2 & -1 & n & 0 & 1 & 2 & \cdots & & n-2 \\
-1 & 1 & 0 & n & n-2 & n-3 & \cdots & 2 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & & 0 & \\
\vdots & \vdots & & & & & \ddots & \vdots & \vdots \\
\vdots & \vdots & & & & & & 1 & 0 \\
\vdots & \vdots & & & & & & & 1 \\
\hline
0 & 0 & 1 & 1 & 1 & \cdots & \cdots & 1 & 1 \\
0 & 0 & 1 & 2 & 2 & \cdots & \cdots & 2 & 1
\end{array}\right],$$

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

This gives a set of generating invariants as

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

with associated rewrite rules as

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

Thus the following n polynomials generate the field of rational invariants of $\mathcal{G}$:

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

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

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

5. Solving invariant systems of polynomials

We adopt the assumptions of Section 3 regarding $\mathbb{K}$, $\mathcal{U} = \mathbb{U}_{p_1} \times \cdots \times \mathbb{U}_{p_s}$, B 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 B. In other words we assume that if $z \in (\mathbb{K}^*)^n$ is such that $f(z) = 0$ for all $f \in F$, then $f(\lambda^B \star z) = 0$, 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 [10, 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.

Given that we have to partially restrict to toric solutions, it would be natural to consider methods that deal with Laurent polynomials [28, 32].

The proposed strategy 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 $B \in \mathbb{Z}^{s \times n}$ and the order matrix $P = \operatorname{diag}(p_1, \dots, p_s)$. In other words, if $z \in (\bar{\mathbb{K}}^*)^n$ is such that $f(z) = 0$, $\forall f \in F$, then $f(\lambda^B \star z) = 0$, $\forall f \in F$ and $\forall \lambda \in \mathcal{U} = \mathbb{U}_{p_1} \times \cdots \times \mathbb{U}_{p_s}$.

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

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

The following proposition shows that our simple definition of (B, P)-degree matches the notion of $\mathcal{Z}$-degree in [10, Section 3.1].

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

Proof. Consider a monomial z^u of (B, P)-degree d, that is, $Bu = d \mod (p_1, \dots, p_s)$. Then $\left(\lambda^B \star z\right)^u = \lambda^{Bu} z^u = \lambda^d z^u$.

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

A question raised in [10] is whether there are monomials of any given (B, P)-degree. If the Hermite normal form of $\begin{bmatrix} B & -P \end{bmatrix}$ is $\begin{bmatrix} I_s & 0 \end{bmatrix}$, then for any $d \in \mathcal{Z}$ we can find monomials of (B, 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 assumption as we assume the group representation given. Yet in Section 6 we show how to obtain a pair of exponent and order matrices (C, Q) that defines 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 $\begin{bmatrix} C & -Q \end{bmatrix}$.

The following proposition is a variation on [10, Theorem 4], from which we borrow the main idea of the proof.

Proposition 5.3. *Let $F \subset \mathbb{K}[z, z^{-1}]$ and $F^h = \{f_d \,|\, f \in F,\ d \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}\}$ 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 B, 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 $f(\lambda^B \star z) = \sum_d \lambda^d f_d(z)$ for all $\lambda \in \mathcal{U}$ we have a square linear system

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

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 $\lambda^B \star z$ is also a toric zero of F for any $\lambda \in \mathcal{U}$: for f in F and z a toric zero of F, $f(\lambda^B \star z) = 0$ 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 (B, 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 (B, P)-homogeneous of (B, 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 $\mathcal{U} = \mathbb{U}_{p_1} \times \cdots \times \mathbb{U}_{p_s}$ given by the exponent matrix $B \in \mathbb{Z}^{s \times n}$ and the order matrix $P = \operatorname{diag}(p_1, \dots, p_s)$.

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

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

Recall from Lemma 2.3 that $V_{\mathfrak{n}}$ is triangular with nonnegative entries. By Theorem 3.3, for each $f \in F$,

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

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

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

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 3.5. Furthermore, the product of the diagonal entries of $V_{\mathfrak{n}}$ equals $\prod_{i=1}^{s} p_i / \det H$ by Corollary 2.4. 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 3.4, we have that the symmetry reductions of $F = \{f_1, f_2, f_3\}$,

$$f_1 = {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 - z_1 z_2 z_3 + 8, \; f_2 = {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 + 7,$$
$$f_3 = z_1^6 z_2^3 z_3^3 - 3 z_1^4 z_2^4 z_3 + z_1^6 + 32 z_1^3 + z_2^3,$$

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

$$\mathfrak{f}_1 = {y_3}^2 - y_2 - y_3 + 8, \; \mathfrak{f}_2 = {y_3}^2 - y_2 + 7, \; \mathfrak{f}_3 = y_1 {y_3}^3 - 3 y_1 y_2 y_3 + y_1^2 + 32 y_1 + y_2.$$

The toric zeros of $\mathfrak{F}$ are the two points $(y_1, y_2, y_3) = (-8, 8, 1)$ and $(y_1, y_2, y_3) = (-1, 8, 1)$. Solving the triangular systems

$$z_1^3 = -8, \; z_2^3 = 8, \; z_1 z_2 z_3 = 1 \quad \text{and} \quad z_1^3 = -1, \; z_2^3 = 8, \; z_1 z_2 z_3 = 1$$

then gives eighteen toric zeros of F.

5.3. **Extension to nondiagonal representations - 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 any linear action of a finite abelian group. We illustrate this in an example.

Consider the following system of polynomial equations:

$$\begin{array}{rcl} 1 - cx_1 - x_1x_2^2 - x_1x_3^2 & = & 0 \\ 1 - cx_2 - x_2x_1^2 - x_2x_3^2 & = & 0 \\ 1 - cx_3 - x_3x_1^2 - x_3x_2^2 & = & 0 \end{array} \tag{7}$$

with c a parameter. This is a system describing a neural network model given in [31], and the solutions were given in Gatermann [14]. The strategy there was to use the symmetry to find a factorization of polynomials in the ideal and split the Gröbner basis computation accordingly. As a result, the twenty-one 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 orbit 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 is done via the matrix $\Xi(\xi) = \left(\xi^{ij}\right)_{1\leq i,j\leq 3}$ where ξ is a primitive cube root of unity. It implies the change of variable $x = \Xi(\xi)\, z$. The diagonal action of the group is determined by the exponent matrix $B = [1\ 2\ 0]$ and order matrix $P = [3]$ with invariants and rewrite rules then determined in Example 4.2.

Applying the change of variables to the polynomials in system (7) 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

$$\begin{array}{rcl} f_0 & = & 1 - cz_3 + z_1^3 + z_2^3 - 2z_3^3 \\ f_1 & = & cz_1 + 3z_1^2 z_2 - 3z_2^2 z_3 \\ f_2 & = & cz_2 + 3z_1 z_2^2 - 3z_1^2 z_3. \end{array} \tag{8}$$

Note that f_i is (B,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 localize 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

$$\mathfrak{f}_0 = 1 + y_1 - cy_3 - 2y_3^2 + \frac{y_2^3}{y_1}, \quad \mathfrak{f}_1 = c + 3y_2 - 3\frac{y_2^2 y_3}{y_1}, \quad \mathfrak{f}_2 = -3y_3 + c\frac{y_2}{y_1} + 3\frac{y_2^2}{y_1}.$$

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

$$y_3 = 0, \quad y_2 = \frac{c}{3}, \quad y_1^2 + y_1 - \frac{c^3}{27} = 0; \tag{9}$$

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

and

$$162\,c\,y_3^4 - 54\,y_3^3 + 81\,c^2\,y_3^2 - 108\,c\,y_3 + 4\,c^3 + 27 = 0,$$

$$(10)\quad y_2 = -\frac{81\,c}{49\,c^3-27}\,y_3^3 - \frac{14\,c^3}{49c^3-27}\,y_3^2 - \frac{93\,c^2}{2(49\,c^3-27)}\,y_3 - \frac{c\,(70\,c^3-243)}{6\,(49\,c^3-27)},$$

$$y_1 = y_3^3 + \frac{c}{2}\,y_3 - \frac{1}{2}.$$

Recall that the variable y_i stands for the generating invariants. The polynomial set (8) thus has six orbits of zeros, that is, eighteen 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 (9) or (10) are obtained by additionally solving the binomial triangular system given by the generating invariants:

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

By linear combinations $x = \Xi\,z$ we obtain eighteen solutions of the original system (7) organized in six orbits.

For completeness one should also examine the solutions of (8) for which $z_1 = 0$. Here, it is immediate to see that there are three solutions satisfying $z_1 = 0,\; z_2 = 0,\; 2\,z_3^3 + c\,z_3 - 1 = 0$. They each form an orbit. The corresponding solutions of the original system are then

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

6. Determining groups of homogeneity

In this section we consider the problem of finding the diagonal matrix 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 equations homogeneous for a grading by an abelian group. Indeed $f = a_0 x^{u_0} + a_1 x^{u_1} + \cdots + a_d x^{u_d}$, with $a_0 \neq 0$, is homogeneous if and only if $\tilde{f} = a_0 + a_1 x^{u_1-u_0} + \cdots + a_d x^{u_d-u_0}$ 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 means for enhancing the efficiency of Gröbner bases computations [9,10] or to propose symmetry reduction schemes as in [21, 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 and the rewrite rules. Also, the group obtained is given in its normalized form and its representation is faithful. The same construction 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 B and order matrix $P = \operatorname{diag}(p_1, \ldots, p_s)$ if $B\,K_f = 0 \bmod {}^t\begin{bmatrix} p_1 & \ldots & p_s \end{bmatrix}$.

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 [22, Section 5]. A related construction appears in [1] for initial ideals. 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

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

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 $a\,K = 0 \bmod p$, 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 $a\,K\,V = (a\,U^{-1})\,U\,K\,V = 0 \bmod p$. 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 $b_i\,s_i = 0 \bmod p$. 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. Suppose the Smith normal form of K is given by $U\,K\,V = \begin{bmatrix} S & 0 \end{bmatrix}$ where*

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

Consider the partitions

$$U = \begin{bmatrix} C \\ B \end{bmatrix} \quad \text{and} \quad U^{-1} = \begin{bmatrix} U_0 & U_1 \end{bmatrix} \text{ where } C \in \mathbb{Z}^{(n-s)\times n},\ B \in \mathbb{Z}^{s\times n}$$
$$\text{and } U_0 \in \mathbb{Z}^{n\times(n-s)},\ U_1 \in \mathbb{Z}^{n\times s}.$$

Then :

(i) *The elements of F are invariants for the diagonal representation determined by the order matrix $P = \operatorname{diag}(p_1, \ldots, p_s)$ and the exponent matrix B consisting of the last s rows of U.*

(ii) *The components of $[g_1, \ldots, g_n] = z^{\begin{bmatrix} U_0 & U_1 P \end{bmatrix}}$ form a minimal generating set of invariants for the diagonal representation defined by B and P.*

(iii) *For any invariant $f \in \mathbb{K}(z)$ of the diagonal representation defined by B and P,*

$$f(z) = f\left(g^{\begin{bmatrix} C \\ P^{-1}B \end{bmatrix}}\right).$$

Proof. Write $U\,K = \begin{bmatrix} S & 0 \end{bmatrix} V^{-1}$ and partition V^{-1} as

$$V^{-1} = \begin{bmatrix} V_0 \\ V_1 \\ V_2 \end{bmatrix}$$

where V_0 has $n-s$ rows and V_1 has s rows. Then $B\,K = PV_1$ and that proves (i).

For (ii) and (iii) we apply Theorem 3.3. The Hermite form and multiplier of $\begin{bmatrix} B & -P \end{bmatrix}$ is given by

$$\begin{bmatrix} B & -P \end{bmatrix} \begin{bmatrix} U_1 & U_0 & U_1 P \\ 0 & 0 & I_s \end{bmatrix} = \begin{bmatrix} I_s & 0 \end{bmatrix},$$

and the inverse of the above Hermite multiplier is determined via

$$\begin{bmatrix} B & -P \\ C & 0 \\ 0 & I_s \end{bmatrix} \begin{bmatrix} U_1 & U_0 & U_1 P \\ 0 & 0 & I_s \end{bmatrix} = I_{n+s}.$$

Thus $V_{\mathfrak{n}} = \begin{bmatrix} U_0 & U_1 P \end{bmatrix}$, $W_{\mathfrak{d}} = \begin{bmatrix} C \\ 0 \end{bmatrix}$, $P_{\mathfrak{d}} = \begin{bmatrix} 0 \\ I_s \end{bmatrix}$, so that $W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B = \begin{bmatrix} C \\ P^{-1}B \end{bmatrix}$. □

We remark that a similar proof shows that there exists a different Hermite multipler such that $V_{\mathfrak{n}} = K\,\hat{V}$, where $\hat{V}$ consists of the n first columns of V. This gives an alternative set of generating invariants.

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 the matrices defining respectively a generating set of invariants and the rewrite rules. The Smith form in Theorem 6.2 thus gives all the information needed for the symmetry reduction of the polynomial system defining K as described in Section 5.

Example 6.3. In order to find an exponent matrix B and order matrix P determining the symmetry for the equations in Example 3.4 the matrix of differences on the exponents of the terms is given by

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

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

$$S = \left[\begin{array}{ccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \quad \text{and} \quad U = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix}.$$

Taking the last two rows of U and S then gives the exponent and order matrices. They are equivalent to

$$B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

since $\xi^{-1} = \xi^2$ for any cubic root of unity. The underlying symmetry group is $\mathbb{Z}_3 \times \mathbb{Z}_3$. In this case

$$V_{\mathfrak{n}} = [\ U_0\ U_1 P\ ] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & -3 \\ 1 & 3 & 3 \end{bmatrix},$$

which, after normalization, is column equivalent to the $V_{\mathfrak{n}}$ given in Example 3.4.

7. Conclusion

In this paper we have investigated the computational aspects of rational invariants of the linear actions of finite abelian groups taking advantage of their diagonal representations. The close relation of such group actions to scalings previously studied by the authors [21, 22] 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 [30] by running the computation with different orderings 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 $\mathbb{K}(\xi)$ [4, 12]. A significant 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 [26, 39].

As for integer linear algebra, we are curious about the possible use of alternate unimodular multipliers. For example what does it mean in this context to normalize $V_{\mathfrak{n}}$ by LLL reduction rather than by Hermite computation. Similarly the Hermite form of $[B\ \ -P]$ is closely related (c.f. [2]) to the Howell form of the matrix B [16, 37], and a similar question can be asked here. 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.

Acknowledgements

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 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 of the program.

References

[1] D. Adrovic and J. Verschelde, *Computing Puiseux series for algebraic surfaces*, ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2012, pp. 20–27, DOI 10.1145/2442829.2442837. MR3206282

[2] A. Bockmayr and F. Eisenbrand, *Cutting planes and the elementary closure in fixed dimension*, Math. Oper. Res. **26** (2001), no. 2, 304–312, DOI 10.1287/moor.26.2.304.10555. MR1895830 (2003a:90032)

[3] H. E. A. Campbell and J. Chuai, *Invariant fields and localized invariant rings of p-groups*, Q. J. Math. **58** (2007), no. 2, 151–157, DOI 10.1093/qmath/ham011. MR2334859 (2008f:13007)

[4] A. Charnow, *On the fixed field of a linear abelian group*, J. London Math. Soc. (2) **1** (1969), 348–350. MR0246860 (40 #129)

[5] H. Derksen and G. Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I, Encyclopaedia of Mathematical Sciences, 130, Springer-Verlag, Berlin, 2002. MR1918599 (2003g:13004)

[6] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), Effective methods in algebraic geometry (Saint-Malo, 1998), J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, DOI 10.1016/S0022-4049(99)00005-5. MR1700538 (2000c:13038)

[7] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2002, pp. 75–83 (electronic), DOI 10.1145/780506.780516. MR2035234 (2005c:13033)

[8] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344, DOI 10.1006/jsco.1993.1051. MR1263871 (94k:68095)

[9] J.-C. Faugère, M. Safey El Din, and T. Verron, *On the complexity of computing Gröbner bases for quasi-homogeneous systems*, ISSAC 2013—Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2013, pp. 189–196, DOI 10.1145/2465506.2465943. MR3206357

[10] J.-C. Faugère and J. Svartz, *Gröbner bases of ideals invariant under a commutative group: the non-modular case*, ISSAC 2013—Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2013, pp. 347–354, DOI 10.1145/2465506.2465944. MR3206377

[11] E. Fischer, Die Isomorphie der Invariantenkörper der endlicher Abelschen Gruppen linearer Transformationen. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, 1915:77–80, 1915.

[12] E. Fischer, *Zur Theorie der endlichen Abelschen Gruppen* (German), Math. Ann. **77** (1915), no. 1, 81–88, DOI 10.1007/BF01456820. MR1511847

[13] P. Fleischmann, G. Kemper, and C. Woodcock, *Homomorphisms, localizations and a new algorithm to construct invariant rings of finite groups*, J. Algebra **309** (2007), no. 2, 497–517, DOI 10.1016/j.jalgebra.2005.06.038. MR2303190 (2008e:13003)

[14] K. Gatermann, Symbolic solution of polynomial equation systems with symmetry, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'90, pages 112–119, ACM, New York, 1990.

[15] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985. MR832183 (87e:15001)

[16] J. A. Howell, *Spans in the module* $(Z_m)^s$, Linear and Multilinear Algebra **19** (1986), no. 1, 67–77, DOI 10.1080/03081088608817705. MR835631 (88h:15031)

[17] E. Hubert, *Algebraic and differential invariants*, Foundations of computational mathematics, Budapest 2011, London Math. Soc. Lecture Note Ser., vol. 403, Cambridge Univ. Press, Cambridge, 2013, pp. 165–187. MR3137638

[18] 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*, 10pp., CEDRAM - Center for Diffusion of Academic Mathematical Journals, Marseille, France, 2013.

[19] E. Hubert and I. A. Kogan, *Rational invariants of a group action. Construction and rewriting*, J. Symbolic Comput. **42** (2007), no. 1-2, 203–217, DOI 10.1016/j.jsc.2006.03.005. MR2284293 (2007i:13009)

[20] E. Hubert and I. A. Kogan, *Smooth and algebraic invariants of a group action: local and global constructions*, Found. Comput. Math. **7** (2007), no. 4, 455–493, DOI 10.1007/s10208-006-0219-0. MR2352606 (2008m:22031)

[21] E. Hubert and G. Labahn, *Rational invariants of scalings from Hermite normal forms*, ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2012, pp. 219–226, DOI 10.1145/2442829.2442862. MR3206307

[22] E. Hubert and G. Labahn, *Scaling invariants and symmetry reduction of dynamical systems*, Found. Comput. Math. **13** (2013), no. 4, 479–516, DOI 10.1007/s10208-013-9165-9. MR3085676

[23] T. Kamke and G. Kemper, *Algorithmic invariant theory of nonreductive groups*, Qual. Theory Dyn. Syst. **11** (2012), no. 1, 79–110, DOI 10.1007/s12346-011-0059-4. MR2902726

[24] M.-c. Kang, *Fixed fields of triangular matrix groups*, J. Algebra **302** (2006), no. 2, 845–847, DOI 10.1016/j.jalgebra.2006.03.037. MR2293785 (2007m:13006)

[25] G. Kemper, *The computation of invariant fields and a constructive version of a theorem by Rosenlicht*, Transform. Groups **12** (2007), no. 4, 657–670, DOI 10.1007/s00031-007-0056-5. MR2365439 (2008m:13011)

[26] H. W. Lenstra Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325. MR0347788 (50 #289)

[27] T. Miyata, *Invariants of certain groups. I*, Nagoya Math. J. **41** (1971), 69–73. MR0272923 (42 #7804)

[28] B. Mourrain and P. Trébuchet, *Toric border basis*, ISSAC 2014—Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2014, pp. 343–350, DOI 10.1145/2608628.2608652. MR3239945

[29] J. Müller-Quade and T. Beth, *Calculating generators for invariant fields of linear algebraic groups*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 392–403, DOI 10.1007/3-540-46796-3_37. MR1846513 (2002f:13011)

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

[31] V. W. Noonburg, *A neural network modeled by an adaptive Lotka-Volterra system*, SIAM J. Appl. Math. **49** (1989), no. 6, 1779–1792, DOI 10.1137/0149109. MR1025961 (91c:92007)

[32] F. Pauer and A. Unterkircher, *Gröbner bases for ideals in Laurent polynomial rings and their application to systems of difference equations*, Appl. Algebra Engrg. Comm. Comput. **9** (1999), no. 4, 271–291, DOI 10.1007/s002000050108. MR1683300 (2000b:13039)

[33] È. B. Vinberg and V. L. Popov, *Invariant theory* (Russian), Algebraic geometry, 4 (Russian), Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, pp. 137–314, 315. MR1100485 (92d:14010)

[34] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Ltd., Chichester, 1986. MR874114 (88m:90090)

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

[36] A. Storjohann and G. Labahn, Asymptotically fast computation of Hermite normal forms of integer matrices, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC'96, pages 259–266, ACM, New York, 1996.

[37] A. Storjohann and T. Mulders, *Fast algorithms for linear algebra modulo N*, Algorithms—ESA '98 (Venice), Lecture Notes in Comput. Sci., vol. 1461, Springer, Berlin, 1998, pp. 139–150, DOI 10.1007/3-540-68530-8_12. MR1683348 (2000a:65056)

[38] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993. MR1255980 (94m:13004)

[39] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158. MR0244215 (39 #5532)

INRIA Méditerranée, 06902 Sophia Antipolis, France
E-mail address: `evelyne.hubert@inria.fr`

Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada N2L 3G1
E-mail address: `glabahn@uwaterloo.ca`