Czech Technical University in Prague
Faculty of Electrical Engineering
Department of Cybernetics

Bachelor Thesis

Using Symmetries in Solving Minimal Problems in Computer Vision

Viktor Korotynskiy

Supervisor: doc. Ing. Tomáš Pajdla, PhD.

Study Program: Cybernetics and Robotics, Bachelor

Field of Study: Robotics

May 24, 2018

CTU
CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

BACHELOR‘S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Korotynskiy Viktor** Personal ID number: **453214**

Faculty / Institute: **Faculty of Electrical Engineering**

Department / Institute: **Department of Cybernetics**

Study program: **Cybernetics and Robotics**

Branch of study: **Robotics**

II. Bachelor’s thesis details

Bachelor’s thesis title in English:

Using Symmetries in Solving Minimal Problems in Computer Vision

Bachelor’s thesis title in Czech:

Využití symetrií při řešení minimálních problémů v počítačovém vidění

Guidelines:

1) Study the approach to analyzing symmetries in polynomial systems from [1,2,3].
2) Suggest an approach to finding symmetries and demonstrate it on a relevant computer vision problem.
3) Implement the approach and evaluate it on real data.

Bibliography / sources:

[1] Viktor Larsson & Kalle Astrom. Uncovering symmetries in polynomial systems. ECCV 2016.
[2]Jean-Charles Faugére, Jules Svartz. Gröbner Bases of Ideals Invariant under a Commutative Group: the Non-Modular Case. The 38th International Symposium on Symbolic and Algebraic Computation, ISSAC '13, Jun 2013, Boston, United States. ACM, Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ISSAC '13, pp.347-354, 2013.
[3] Evelyne Hubert, George Labahn. Computing the Invariants of Finite Abelian Groups. Mathematics of Computation, American Mathematical Society, 2016, 85 (302), pp.3029-3050.

Name and workplace of bachelor’s thesis supervisor:

doc. Ing. Tomáš Pajdla, Ph.D., Applied Algebra and Geometry, CIIRC

Name and workplace of second bachelor’s thesis supervisor or consultant:

Date of bachelor’s thesis assignment: **11.01.2018** Deadline for bachelor thesis submission: **25.05.2018**

Assignment valid until: **30.09.2019**

doc. Ing. Tomáš Pajdla, Ph.D. Supervisor’s signature	doc. Ing. Tomáš Svoboda, Ph.D. Head of department’s signature	prof. Ing. Pavel Ripka, CSc. Dean’s signature

III. Assignment receipt

The student acknowledges that the bachelor’s thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the bachelor’s thesis, the author must state the names of consultants and include a list of references.

Date of assignment receipt	Student’s signature

Aknowledgements

I would like to thank my advisor Tomáš Pajdla for introducing me into the world of algebraic geometry and showing that algebraic geometry is no less interesting than other mathematical topics. In every talk with me, Tomáš Pajdla was very accurate while talking about mathematical concepts. This helped me in understanding the material very much.

Declaration

I declare that the presented work was developed independently and that I have listed all sources of information used within it in accordance with the methodical instructions for observing the ethical principles in the preparation of university theses.

Prague, date ....

signature

Abstract

Many problems in computer vision require solving a system of polynomial equations. Practical systems with a finite number of solutions may have a big number of solutions (greater than 100). The more the system has solutions, the more difficult it is to solve it. However, we can check if it is possible to get from one solution $\mathbf{v}_1$ another solution $\mathbf{v}_2$ (e.g. by multiplying $\mathbf{v}_1$ by some matrix). If there are such matrices, then we say that a polynomial system has symmetries. If we are able to find these symmetries, then there are two ways how to simplify the solution of the polynomial system. The first is to simplify the original polynomial system to get another (the reduced) polynomial system with a smaller number of solutions. Solving the reduced polynomial system, we can then obtain all the solutions of the original polynomial system as a matrix multiplication of the solutions of the reduced system. The second is to use an action matrix, which, after choosing specific monomials, becomes block-diagonal.

Keywords: computer vision, symmetries in polynomial systems, polynomial system reduction, ideals stable under matrices

Abstrakt

Mnoho problémů v počítačovém vidění vyžaduje vyřešení soustavy polynomiálních rovnic. Praktické systémy s konečným počtem řešení mohou mít velký počet řešení (více než 100). Čím více má soustava řešení, tím obtížnější je vyřešit ji. Můžeme však zkontrolovat, zda je možné získat z jednoho řešení $\mathbf{v}_1$ jiné řešení $\mathbf{v}_2$ (např. vynásobením $\mathbf{v}_1$ nějakou maticí). Pokud existují takové matice, říkáme, že polynomiální soustava má symetrie. Pokud budeme schopni tyto symetrie najít, pak jsou dva způsoby, jak zjednodušit řešení polynomiální soustavy. První způsob je zjednodušit původní polynomiální soustavu, abychom získali jinou (redukovanou) polynomiální soustavu s menším počtem řešení. Řešením redukované polynomiální soustavy pak můžeme získat všechna řešení původní polynomiální soustavy maticovým násobením řešení redukované soustavy. Druhý způsob je použit akční matici, která, po určitém výběru monomů, se stává blokově diagonální.

Klíčová slova: počítačové vidění, symetrie v polynomiálních soustavách, redukce polynomiální soustavy, idealy stabilní vůči maticím

Contents

1 Introduction

1.1 Motivation

Solving system of polynomial equations is a very common problem in computer vision. These systems usually consist of many polynomials of high degree in several variables. One of the state of the art methods for solving such systems is to construct an action matrix and find its eigenvalues (an eigenvalue method of solving). If the system has a huge number of solutions, then the action matrix is large. The larger the action matrix is, the more difficult it is to find its eigenvalues. However, there are some special polynomial systems called symmetric. This means that there exists some matrix $\mathbf{A}$ such that for any $\mathbf{v}$ from the solution set, $\mathbf{Av}$ also belongs to the solution set. Having found such matrices, we can either simplify the determination of the eigenvalues of the action matrix [3, 9], or obtain a simpler system of equations from the original one [8, 7].

1.2 State of The Art

There are several articles which describe how to use stability matrices. In [9] a connection was made between diagonal stability matrices and the block-diagonal structure of the action matrix. But it was not shown how to find diagonal stability matrices of a given polynomial system. The authors assumed that we know the stability matrices in advance. Another related work is [8, 7]. They made a connection between diagonal stability matrices and reduction of polynomial systems (i.e. obtaining some kind of a simpler system from the original one). Also, [8, 7] give a method how to find some diagonal stability matrices of a given polynomial system using linear algebra tools. There are also some related results in [6]. There it was described how to use stability matrices to speed up Groebner basis computations. In [3] a connection between stability matrices and the block-diagonal structure of the action matrix was made. However, in this thesis we concentrate on works [8, 7] and don't talk about action matrices. Summing up, [8, 7] proposed a method for finding only some diagonal stability matrices of a given polynomial system. In this thesis we propose a modified method from [8, 7] to find all diagonal stability matrices. To find them only linear algebra can be used. We also suggest a method for finding all in general non-diagonal stability matrices.

1.3 Contributions

In [8, 7] methods how to find only some diagonal stability matrices of a given polynomial system using linear algebra tools were proposed. To find such matrices, we can only look at the multidegrees of monomials in each polynomial and need not care about the coefficients. The first contribution of this work is the proposal of the method for finding all diagonal stability matrices. The main idea is to apply linear algebra on multidegrees of monomials in a reduced Groebner basis of an ideal generated by a given polynomial system. We also show that applying it on multidegrees of some other basis of the same ideal may not give us all diagonal stability matrices.

The second contribution is the proposal of the method for finding all in general non-diagonal stability matrices. However, to find them, it is no longer sufficient to use only linear algebra. Generally, we should solve another polynomial system, which can be more difficult than the original one.

2 Linear change of variables

Further we will use some well-known mathematical concepts taken from [1, 4]. These concpets are: ring [1, p. 346], field [1, p. 83], ring homomorphism [1, p. 353], polynomial ideal [4, p. 29], variety [4, p. 5], group [1, p. 42], subgroup [1, p. 44], group homomorphism [1, p. 51], isomorphic groups [1, p. 49], direct product of groups [1, p. 61].

Throughout this thesis we will work with an infinite number field k. For a matrix $\mathbf{A} \in k^{m\times n}$ we introduce a mapping

$$\begin{aligned} \varphi_{\mathbf{A}} \colon k[x_1, ..., x_m] &\to k[y_1, ..., y_n] \\ f(\mathbf{x}) &\mapsto f(\mathbf{Ay}) \end{aligned} \tag{2.1}$$

where

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

are the vectors of variables. The variables of the domain and image polynomial rings of $\varphi_{\mathbf{A}}$ are $x_1, ..., x_m$ and $y_1, ..., y_n$, respectively. Such a notation is made for simplicity because of a different number of variables in domain and image rings. But we will make an exception for a square matrix $\mathbf{A}$: instead of the image vector of variables $\mathbf{y}$ we will write the same $\mathbf{x}$ as for the domain polynomial ring. This is because $\mathbf{x}$ and $\mathbf{y}$ are vectors of the same length. We now give an Example 2.1, which shows how $\varphi_{\mathbf{A}}$ maps polynomials.

Example 2.1. *Suppose a number field $k = \mathbb{Q}$. Suppose a matrix*

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 3 & 1 \\ 4 & 7 & 3 & 0 \\ -1 & 5 & -2 & 1 \end{bmatrix} \in \mathbb{Q}^{3\times 4}.$$

Then the mapping $\varphi_{\mathbf{A}}$ is from $\mathbb{Q}[x_1, x_2, x_3]$ to $\mathbb{Q}[y_1, y_2, y_3, y_4]$. By definition (2.1) we have

$$\varphi_{\mathbf{A}}(f(\mathbf{x})) = f(\mathbf{Ay}) = f(y_1{+}3y_3{+}y_4, 4y_1{+}7y_2{+}3y_3, -y_1{+}5y_2{-}2y_3{+}y_4), \quad \forall f(\mathbf{x}) \in \mathbb{Q}[x_1, x_2, x_3].$$

Let's take $f(\mathbf{x}) = x_1 + x_2 + 2x_3$. Then

$$\varphi_{\mathbf{A}}(f(\mathbf{x})) = (y_1{+}3y_3{+}y_4){+}(4y_1{+}7y_2{+}3y_3){+}2(-y_1{+}5y_2{-}2y_3{+}y_4) = 3y_1{+}17y_2{+}2y_3{+}3y_4.$$

The following Section 3 will require from us to understand, how a mapping $\varphi_{\mathbf{A}}$ changes after removing some columns (or rows) from $\mathbf{A}$. We give the following Example 2.2.

Example 2.2. *Suppose a matrix* $\mathbf{A}$ *from Example 2.1. We can understand* $\mathbf{A}$ *in the following way:*

$$\mathbf{A} = \begin{array}{cccc|c} y_1 & y_2 & y_3 & y_4 & \\ \hline 1 & 0 & 3 & 1 & x_1 \\ 4 & 7 & 3 & 0 & x_2 \\ -1 & 5 & -2 & 1 & x_3 \end{array}$$

We will call the variable y_j *above the column* j *(resp.* x_j *to the right of row* j*) as* `labelled variable of the column` j *(resp.* `of the row` j*). Let's construct two matrices* $\mathbf{B}_1$ *(by replacing column* 3 *with a zero column) and* $\mathbf{B}_2$ *(by removing column* 3 *and its labelled variable) from* $\mathbf{A}$ *as*

$$\mathbf{B}_1 = \begin{array}{cccc|c} y_1 & y_2 & y_3 & y_4 & \\ \hline 1 & 0 & 0 & 1 & x_1 \\ 4 & 7 & 0 & 0 & x_2 \\ -1 & 5 & 0 & 1 & x_3 \end{array}, \quad \mathbf{B}_2 = \begin{array}{ccc|c} y_1 & y_2 & y_4 & \\ \hline 1 & 0 & 1 & x_1 \\ 4 & 7 & 0 & x_2 \\ -1 & 5 & 1 & x_3 \end{array}$$

Then we can easily see that

$$f(\mathbf{B}_1\mathbf{y}) = f(\mathbf{B}_2\mathbf{y}_r) = f(y_1 + y_4, 4y_1 + 7y_2, -y_1 + 5y_2 + y_4), \quad \mathbf{y}_r = \begin{bmatrix} y_1 \\ y_2 \\ y_4 \end{bmatrix}.$$

We generalize an Example 2.2 to the following Remark 2.1.

Remark 2.1. *Suppose a matrix* $\mathbf{A} \in k^{m\times n}$*. Construct two matrices* $\mathbf{B}_1$ *(by replacing column* j *with a zero column) and* $\mathbf{B}_2$ *(by removing the same column* j *and its labelled variable) from* $\mathbf{A}$ *as in Example 2.2. Then* $\varphi_{\mathbf{B}_1}\colon k[x_1, ..., x_m] \to k[y_1, ..., y_n]$ *and* $\varphi_{\mathbf{B}_2}\colon k[x_1, ..., x_m] \to k[y_1, ..., y_{j-1}, y_{j+1}, ..., y_n]$ *act on* $k[x_1, ..., x_m]$ *in the same way in the sense that*

$$\varphi_{\mathbf{B}_1}(f(\mathbf{x})) = \varphi_{\mathbf{B}_2}(f(\mathbf{x})) \quad \forall f(\mathbf{x}) \in k[x_1, ..., x_m].$$

As a corollary this means that $\ker(\varphi_{\mathbf{B}_1}) = \ker(\varphi_{\mathbf{B}_2})$*, which we will use later.*

We give a similar Remark 2.2 about removing rows from $\mathbf{A}$.

Remark 2.2. *Suppose we have a matrix* $\mathbf{A} \in k^{m\times n}$*. Construct two matrices* $\mathbf{B}_1$ *(by replacing row* j *with a zero row) and* $\mathbf{B}_2$ *(by removing the same row* j *and its labelled variable) from* $\mathbf{A}$*. Then* $\varphi_{\mathbf{B}_1}\colon k[x_1, ..., x_m] \to k[y_1, ..., y_n]$ *and* $\varphi_{\mathbf{B}_2}\colon k[x_1, ..., x_{j-1}, x_{j+1}, ..., x_m] \to k[y_1, ..., y_n]$ *act on* $k[x_1, ..., x_{j-1}, x_{j+1}, ..., x_m]$ *in the same way in the sense that*

$$\varphi_{\mathbf{B}_1}(f(\mathbf{x})) = \varphi_{\mathbf{B}_2}(f(\mathbf{x})) \quad \forall f(\mathbf{x}) \in k[x_1, ..., x_{j-1}, x_{j+1}, ..., x_m].$$

3 Polynomial ring after a linear change of variables

A matrix $\mathbf{A} \in k^{m \times n}$ is not necessarily a square matrix now. The following Lemma 3.1 shows that $\varphi_{\mathbf{A}}$ is a ring homomorphism from $k[x_1, ..., x_m]$ to $k[y_1, ..., y_n]$.

Lemma 3.1. *Suppose a matrix $\mathbf{A} \in k^{m \times n}$. Then the mapping $\varphi_{\mathbf{A}} \colon k[x_1, ..., x_m] \to k[y_1, ..., y_n]$ is a ring homomorphism.*

Proof. We can easily verify (it follows from definition (2.1) of $\varphi_{\mathbf{A}}$) that

$$\varphi_{\mathbf{A}}(f(\mathbf{x}) + g(\mathbf{x})) = f(\mathbf{Ay}) + g(\mathbf{Ay}) = \varphi_{\mathbf{A}}(f(\mathbf{x})) + \varphi_{\mathbf{A}}(g(\mathbf{x})),$$

$$\varphi_{\mathbf{A}}(f(\mathbf{x}) \cdot g(\mathbf{x})) = f(\mathbf{Ay}) \cdot g(\mathbf{Ay}) = \varphi_{\mathbf{A}}(f(\mathbf{x})) \cdot \varphi_{\mathbf{A}}(g(\mathbf{x})),$$

$$\varphi_{\mathbf{A}}(1) = 1,$$

which proves the lemma.

□

The following Lemma 3.2 shows a well-known fact about ring homomorphisms.

Lemma 3.2. *For any ring homomorphism $\varphi \colon R \to S$, where R and S are rings, the kernel of φ is an ideal in R.*

Proof. Statements $1) - 3)$ follows from the properties of ring homomorphism.
1) The zero polynomial lies in $\ker(\varphi)$, because $\varphi(0) = 0$.
2) For any two r_1 and r_2 from $\ker(\varphi)$ we have that

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = 0 + 0 = 0,$$

Then $r_1 + r_2 \in \ker(\varphi)$.
3) For any $x \in \ker(\varphi)$ and $r \in R$ we have

$$\varphi(r \cdot x) = \varphi(r) \cdot \varphi(x) = \varphi(r) \cdot 0 = 0,$$

$$\varphi(x \cdot r) = \varphi(x) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0,$$

Then $r \cdot x$ and $x \cdot r$ are in $\ker(\varphi)$. And we have the proof.

□

Lemma 3.2 tells us that the kernel of $\varphi_{\mathbf{A}}$ is an ideal in $k[x_1, ..., x_m]$. Now we will give Lemma 3.3, which will help to prove the following Lemmas in Sections 3.1 and 3.2.

Lemma 3.3. *Suppose a matrix* $\mathbf{A} \in k^{m\times n}$ *and a polynomial* $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{A}})$*. Then for any* $\mathbf{D} \in k^{n\times n}$ *we have* $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{AD}})$*.*

Proof. We have

$$\varphi_{\mathbf{AD}}(f(\mathbf{x})) = f(\mathbf{ADy}) \overset{(1)}{=} \varphi_{\mathbf{D}}(f(\mathbf{Ay})) = \varphi_{\mathbf{D}}(\varphi_{\mathbf{A}}(f(\mathbf{x}))) = \varphi_{\mathbf{D}}(0) = 0.$$

In the equality (1) we used an exception for a square matrix: not to relabel the vector of variables.

□

We want to note that $\varphi_{\mathbf{AD}}(f(\mathbf{x}))$ is equal to $\varphi_{\mathbf{D}}(\varphi_{\mathbf{A}}(f(\mathbf{x})))$, not to $\varphi_{\mathbf{A}}(\varphi_{\mathbf{D}}(f(\mathbf{x})))$. This is because $\varphi_{\mathbf{A}}(f(\mathbf{x}))$ means to change $\mathbf{x}$ to $\mathbf{Ax}$ and put it as a variable vector into $f(\mathbf{x})$. That's why, when we have $\varphi_{\mathbf{D}}(f(\mathbf{Ay}))$, this means that we change $\mathbf{y}$ to $\mathbf{Dy}$ and put it as a variable vector into $f(\mathbf{Ay})$ and get $f(\mathbf{ADy})$.

3.1 The case of a full row rank matrix

3.1.1 The case of a square matrix

The following Lemma 3.4 shows that for a square full row rank (invertible) $\mathbf{A} \in k^{n\times n}$ the mapping $\varphi_{\mathbf{A}}$ is a ring automorphism on $k[x_1, ..., x_n]$.

Lemma 3.4. *Suppose an invertible matrix* $\mathbf{A} \in k^{n\times n}$*. Then* $\varphi_{\mathbf{A}}$ *is a ring automorphism on* $k[x_1, ..., x_n]$*.*

Proof. To prove that $\varphi_{\mathbf{A}}$ is a ring automorphism, we only need to show that it is a bijection because we already know that it is a ring homomorphism. To show that it is bijective, we need to show that it is injective and surjective.
1) Injective. Suppose we have

$$f(\mathbf{Ax}) = g(\mathbf{Ax}),$$

then

$$\varphi_{\mathbf{A}^{-1}}(f(\mathbf{Ax})) = \varphi_{\mathbf{A}^{-1}}(g(\mathbf{Ax})),$$
$$f(\mathbf{AA}^{-1}\mathbf{x}) = g(\mathbf{AA}^{-1}\mathbf{x})$$

or

$$f(\mathbf{x}) = g(\mathbf{x}).$$

2) Surjective. We want to show that

$$\forall f(\mathbf{x}) \in k[x_1, ..., x_n] : \ \exists\, g(\mathbf{x}) \in k[x_1, ..., x_n] : \varphi_{\mathbf{A}}(g(\mathbf{x})) = f(\mathbf{x}).$$

We will choose $g(\mathbf{x}) = f(\mathbf{A}^{-1}\mathbf{x})$. It is obvious that $g(\mathbf{x}) \in k[x_1, ..., x_n]$ and

$$\varphi_{\mathbf{A}}(g(\mathbf{x})) = f(\mathbf{A}^{-1}\mathbf{Ax}) = f(\mathbf{x}).$$

□

Remark 3.1. *So, for an invertible* $\mathbf{A}$ *we can conclude from injectivity of* $\varphi_{\mathbf{A}}$ *that its kernel is the trivial ideal* $I = \{0\}$.

3.1.2 The case of a non-square matrix

Here we will just prove that for a full row rank non-square matrix $\mathbf{A} \in k^{m\times n}$ there holds $\ker(\varphi_{\mathbf{A}}) = \{0\}$ true.

Lemma 3.5. *Suppose a full row rank non-square matrix* $\mathbf{A} \in k^{m\times n}$ *(i.e.* $m \leq n$*). Then* $\ker(\varphi_{\mathbf{A}}) = \{0\}$.

Proof. From linear algebra we know that we can extract m linearly independent columns from $\mathbf{A}$. Let's denote by $\mathbf{B}_1 \in k^{m\times n}$ a matrix obtained from $\mathbf{A}$ in which we leave these m LI columns without changing and all the other columns replace by zero. Then, there exists a diagonal matrix $\mathbf{D} \in k^{n\times n}$ with 1 and 0 on its diagonal such that

$$\mathbf{B}_1 = \mathbf{AD}.$$

To get a contradiction suppose there is some nonzero polynomial $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{A}})$. By Lemma 3.3 we obtain that $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{B}_1})$. Denote by $\mathbf{B}_2 \in k^{m\times m}$ a matrix obtained from $\mathbf{B}_1$ by removing zero columns and their labelled variables. Then $\mathbf{B}_2$ is an invertible matrix. By Remark 2.1 we have that $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{B}_2})$. But by Remark 3.1 it is a contradiction. Then $\ker(\varphi_{\mathbf{A}}) = \{0\}$.

□

3.2 The case of not-full row rank matrix

Here we will show that for any matrix $\mathbf{A} \in k^{m\times n}$ not of full row rank, the kernel of $\varphi_{\mathbf{A}}$ cannot be the trivial ideal.

Suppose a matrix $\mathbf{A} \in k^{m\times n}$ not of full row rank. We can suppose that `the last` $q < m$ rows are linearly independent. Otherwise, to achieve this we can permute the rows of $\mathbf{A}$ together with and their labelled variables $x_1, ..., x_m$. We will denote the rows of $\mathbf{A}$ by $\mathbf{r}_1^T, ..., \mathbf{r}_m^T$. These are row vectors. Then for every $\mathbf{r}_j^T$, $j = 1, ..., m-q$ there exist (unique) numbers $c_{ij} \in k$, $i = m-q+1, ..., m$, such that

$$\mathbf{r}_j^T + \sum_{i=m-q+1}^{m} c_{ij}\mathbf{r}_i^T = \mathbf{0}^T. \tag{3.1}$$

The following Theorem 3.1 tells us what are the generators of $\ker(\varphi_{\mathbf{A}})$.

Theorem 3.1. *Suppose a matrix* $\mathbf{A} \in k^{m\times n}$ *not of full row rank and numbers* $c_{ij} \in k$, $m-q+1 \leq i \leq m$, $1 \leq j \leq m-q$ *from Equation* (3.1)*. Then*

$$\ker(\varphi_{\mathbf{A}}) = \left\langle \left\{ x_j + \sum_{i=m-q+1}^{m} c_{ij}x_i \right\}_{j=1}^{m-q} \right\rangle.$$

Proof. 1) We will denote $p_j(\mathbf{x}) = x_j + \sum_{i=m-q+1}^{m} c_{ij}x_i$. At first we can easily verify that linear polynomials $\left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q}$ lie in $\ker(\varphi_{\mathbf{A}})$. Applying $\varphi_{\mathbf{A}}$ on each of them we obtain

$$\varphi_{\mathbf{A}}\Big(x_j + \sum_{i=m-q+1}^{m} c_{ij}x_i\Big) = \mathbf{r}_j^T \cdot \mathbf{y} + \sum_{i=m-q+1}^{n} c_{ij}\mathbf{r}_i^T \cdot \mathbf{y} = \Big(\mathbf{r}_j^T + \sum_{i=m-q+1}^{m} c_{ij}\mathbf{r}_i^T\Big) \cdot \mathbf{y} = \mathbf{0}^T \cdot \mathbf{y} = 0.$$

And because $\varphi_{\mathbf{A}}$ is a ring homomorphism, then any polynomial combination of $\left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q}$ lies in $\ker(\varphi_{\mathbf{A}})$. Hence, we have now proved that

$$\ker(\varphi_{\mathbf{A}}) \supset \left\langle \left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q} \right\rangle.$$

2) Here we will prove the opposite inclusion. We will use the lex monomial ordering (grlex is also available) for variable ordering $x_1 > ... > x_n$. Take any $f(x_1, ..., x_m) \in \ker(\varphi_{\mathbf{A}})$ and apply the division algorithm [4, p. 59] on it by the set $\left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q}$. Then we obtain

$$f(\mathbf{x}) = \sum_{j=1}^{m-q} g_j(\mathbf{x}) \cdot p_j(\mathbf{x}) + r(\mathbf{x}).$$

Our task is to show that every $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{A}})$ is generated by $\left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q}$, which means that we have to show that $r(\mathbf{x}) = 0$. Because $f(\mathbf{x}) \in \ker(\varphi_{\mathbf{A}})$, $\left\{p_j(\mathbf{x})\right\}_{j=1}^{m-q} \subset \ker(\varphi_{\mathbf{A}})$ and $\ker(\varphi_{\mathbf{A}})$ is an ideal, then also $r(\mathbf{x}) \in \ker(\varphi_{\mathbf{A}})$. To get a contradiction suppose $r(\mathbf{x}) \neq 0$. From the properties of the division algorithm and because of using lex ordering $\Big(\mathrm{LT}(p_j(\mathbf{x})) = x_j, \quad 1 \leq j \leq m - q\Big)$ it follows that $r(\mathbf{x}) = r(x_{m-q+1}, ..., x_m)$, which means that r is a polynomial in only $x_{m-q+1}, ..., x_m$.
Now, because r is a polynomial in only $x_{m-q+1}, ..., x_m$, we conclude by Remark 2.2 that

$$\varphi_{\mathbf{A}}(r(x_{m-q+1}, ..., x_m)) = \varphi_{\mathbf{A}_{LI}}(r(x_{m-q+1}, ..., x_m)) = 0,$$

where $\mathbf{A}_{LI} \in k^{q \times n}$ is a matrix of q last linearly independent rows of $\mathbf{A}$. We can construct an invertible matrix $\mathbf{M} \in k^{q \times q}$ from $\mathbf{A}_{LI}$ by the same way as $\mathbf{B}_2$ was constructed from $\mathbf{A}$ in the proof of Lemma 3.5. Then by Lemma 3.3 and Remark 2.1 we have that $r(x_{m-q+1}, ..., x_m) \in \ker(\varphi_{\mathbf{M}})$. But by Remark 3.1 it is a contradiction. Then we must have that $r(x_{m-q+1}, ..., x_m)$ is the zero polynomial and we got the proof.

□

3.3 The general case

Here we will give the main theorem of this chapter. This theorem shows that $\varphi_{\mathbf{A}} : k[x_1, ..., x_m] \to k[y_1, ..., y_n]$ "reduces" $k[x_1, ..., x_m]$ to the polynomial ring isomorphic to $k[y_1, ..., y_q]$, where $q = \operatorname{rank} \mathbf{A}$.

Theorem 3.2. *Suppose a matrix* $\mathbf{A} = k^{m\times n}$ *such that* $\operatorname{rank}\mathbf{A} = q$. *Also suppose the mapping* $\varphi_{\mathbf{A}}\colon k[x_1, ..., x_m] \to k[y_1, ..., y_n]$. *Then there is a ring isomorphism*

$$\operatorname{im}(\varphi_{\mathbf{A}}) \cong k[y_1, ..., y_q].$$

In the case $q = 0$, *i.e.* $\mathbf{A} = \mathbf{O}$, *we have*

$$\operatorname{im}(\varphi_{\mathbf{A}}) \cong k.$$

Proof. It is sufficient to prove that

$$k[x_1, ..., x_m]/\ker(\varphi_{\mathbf{A}}) \cong k[y_1, ...y_q]$$

Then by the First Isomorphism Theorem [1, p. 68] we obtain $\operatorname{im}(\varphi_{\mathbf{A}}) \cong k[x_1, ..., x_m]/\ker(\varphi_{\mathbf{A}}) \cong k[y_1, ..., y_q]$.
The statement of the theorem is obvious for matrices $\mathbf{A}$ with full row rank. As mappings $\varphi_{\mathbf{A}}$ of such matrices have a trivial ideal as their kernel (by Remark 3.1 and Lemma 3.5), then

$$k[x_1, ..., x_m]/\ker(\varphi_{\mathbf{A}}) = k[x_1, ..., x_m]/\{0\} \cong k[x_1, ..., x_m].$$

Suppose now that $\mathbf{A}$ is of not full row rank. Then from [4, p. 229, Proposition 4], which states that $k[x_1, ..., x_n]/I \cong \operatorname{Span}\Big(\mathbf{x}^{\boldsymbol{\alpha}} : \mathbf{x}^{\boldsymbol{\alpha}} \notin \langle \operatorname{LT}(I)\rangle\Big)$, we obtain the desired result, because

$$S = \operatorname{Span}\Big(\mathbf{x}^{\boldsymbol{\alpha}} : \mathbf{x}^{\boldsymbol{\alpha}} \notin \langle \operatorname{LT}(\ker(\varphi_{\mathbf{A}}))\rangle\Big) = \operatorname{Span}\Big(\mathbf{x}^{\boldsymbol{\alpha}} : \mathbf{x}^{\boldsymbol{\alpha}} \notin \langle x_1, ..., x_{m-q}\rangle\Big) = k[x_{m-q+1}, ..., x_m].$$

If $\mathbf{A} = \mathbf{O}$, then it is obvious that the mapping $\varphi_{\mathbf{A}}\colon k[x_1, ..., x_m] \to k$ is surjective, from which the result follows.

□

4 Ideal after a linear change of variables

In all chapters further we will consider only the case of square matrix $\mathbf{A} \in k^{n \times n}$. If we will want to talk about invertible $\mathbf{A}$, then we will always note it at the beginnig of Lemma (or Definition). The following Lemma 4.1 describes a well-known fact about images by ring homomorphisms.

Lemma 4.1. *Suppose a ring homomorphism $\varphi \colon R \to S$, where R and S are rings. Then $\varphi(R)$ is a subring of S. Also if I is an ideal of R, then $\varphi(I)$ is an ideal of $\varphi(R)$.*

Corollary 1. *As a corollary of Lemma 4.1 we have that if $\mathbf{A}$ is invertible, then for any ideal I of $k[x_1, ..., x_n]$ there holds true that $\varphi_{\mathbf{A}}(I)$ is also an ideal of $k[x_1, ..., x_n]$.*

Proof. This follows from Lemma 3.4, which shows that

$$\varphi_{\mathbf{A}}(k[x_1, ..., x_n]) = k[x_1, ..., x_n].$$

□

We can ask a question: does there exist for an ideal I a matrix $\mathbf{A}$ such that $\varphi_{\mathbf{A}}$ maps I into itself? As we will see in the following sections, this could be very useful for computing the variety $\mathbf{V}(I)$. We give the following two definitions.

Definition 4.1. *A polynomial ideal $I \subset k[x_1, ..., x_n]$ is said to be* `stable under a matrix` *$\mathbf{A} \in k^{n \times n}$ if*

$$\varphi_{\mathbf{A}}(I) \subset I.$$

Such a matrix $\mathbf{A}$ we will call a `stability matrix of` *I.*

Definition 4.2. *A polynomial ideal $I \subset k[x_1, ..., x_n]$ is said to be* `invariant under a matrix` *$\mathbf{A} \in k^{n \times n}$ if*

$$\varphi_{\mathbf{A}}(I) = I.$$

The following Lemma 4.2 gives a necessary and sufficient condition for an ideal I to be stable under $\mathbf{A}$.

Lemma 4.2. *Suppose a polynomial ideal $I \subset k[x_1, ..., x_n]$ and let $G = \left\{ g_j(\mathbf{x}) \right\}_{j=1}^{m}$ be some set of generators of I. Then I is stable under $\mathbf{A} \in k^{n \times n}$ if and only if*

$$g_j(\mathbf{A}\mathbf{x}) \in I \quad \forall j = 1, ..., m.$$

Proof. It is trivial by Definition 4.1 that if I is stable under $\mathbf{A}$, then $g_j(\mathbf{Ax}) \in I \ \ \forall j = 1, ..., m$. Conversely, we want to prove the following implication:

$$g_j(\mathbf{Ax}) \in I \ \ \forall j = 1, ..., m \ \ \wedge \ \ f(\mathbf{x}) \in I \Rightarrow f(\mathbf{Ax}) \in I.$$

Any polynomial $f(\mathbf{x}) \in I$ we can write as

$$f(\mathbf{x}) = \sum_{j=1}^{m} h_j(\mathbf{x}) g_j(\mathbf{x}), \quad h_j(\mathbf{x}) \in k[x_1, ..., x_n] \ \ \forall j = 1, ..., m.$$

Then

$$f(\mathbf{Ax}) = \sum_{j=1}^{m} h_j(\mathbf{Ax}) g_j(\mathbf{Ax}).$$

Because $\Big\{h_j(\mathbf{Ax})\Big\}_{j=1}^{m} \subset k[x_1, ..., x_n]$ and by assumption $g_j(\mathbf{Ax}) \in I \ \ \forall j = 1, ..., m$, then also $f(\mathbf{Ax}) \in I$.

□

The following Remark 4.1 tells us more about an ideal I invariant under invertible matrix.

Remark 4.1. *Suppose an invertible matrix* $\mathbf{A} \in k^{n \times n}$. *Then*
1) An ideal I *is invariant under* $\mathbf{A}$ *if and only if* $\varphi_{\mathbf{A}} \colon I \to I$ *is a bijection.*
2) $\varphi_{\mathbf{A}} \colon I \to I$ *is a bijection if and only if* I *is stable under both* $\mathbf{A}$ *and* $\mathbf{A}^{-1}$.

Proof. 1) $\Rightarrow$) If $\mathbf{A}$ is invertible then we know from Lemma 3.4 that $\varphi_{\mathbf{A}} \colon k[x_1, ..., x_n] \to k[x_1, ..., x_n]$ is injective (and then also $\varphi_{\mathbf{A}} \colon I \to I$). Because I is invariant under $\mathbf{A}$, then $\varphi_{\mathbf{A}}(I) = I$, which shows that $\varphi_{\mathbf{A}} \colon I \to I$ is surjective.
1) $\Leftarrow$) $\varphi_{\mathbf{A}} \colon I \to I$ is a bijection, then it is surjective, from which the result follows.
2) $\Rightarrow$) It is obvious that $\varphi_{\mathbf{A}^{-1}} \colon I \to I$ is an inverse bijective map of $\varphi_{\mathbf{A}} \colon I \to I$, from which the result follows.
2) $\Leftarrow$) From Lemma 3.4 we know that $\varphi_{\mathbf{A}} \colon I \to I$ is injective. It remains to prove that it is surjective. Take any $f(\mathbf{x}) \in I$. We want to prove that there exist such $g(\mathbf{x}) \in I$ that $\varphi_{\mathbf{A}}(g(\mathbf{x})) = f(\mathbf{x})$. We will take $g(\mathbf{x}) = f(\mathbf{A}^{-1}\mathbf{x})$. Because I is stable under $\mathbf{A}^{-1}$, then $g(\mathbf{x}) \in I$. And also $\varphi_{\mathbf{A}}(g(\mathbf{x})) = \varphi_{\mathbf{A}}(f(\mathbf{A}^{-1}\mathbf{x})) = f(\mathbf{A}^{-1}\mathbf{Ax}) = f(\mathbf{x})$.

□

The following Lemma 4.3 gives the necessary and sufficient conditions for an ideal I to be invariant under $\mathbf{A}$. However to prove it generally we need to assume that $\mathbf{A}$ is invertible.

Lemma 4.3. *Suppose a polynomial ideal* $I \subset k[x_1, ..., x_n]$ *and let* $G = \Big\{g_j(\mathbf{x})\Big\}_{j=1}^{m}$ *be some set of generators of* I. *Let also* $\mathbf{A} \in k^{n \times n}$ *be an invertible matrix. Then* I *is invariant under* $\mathbf{A}$ *if and only if*

$$I = \left\langle \Big\{g_j(\mathbf{Ax})\Big\}_{j=1}^{m} \right\rangle.$$

Proof. $\Leftarrow$) Because $\left\{g_j(\mathbf{Ax})\right\}_{j=1}^m \subset I$, then by Lemma 4.2 we obtain that $\varphi_{\mathbf{A}}(I) \subset I$. To prove $I \subset \varphi_{\mathbf{A}}(I)$ we take any polynomial $f(\mathbf{x}) \in I$. Because $\left\{g_j(\mathbf{Ax})\right\}_{j=1}^m$ are the generators of I, then there exist polynomials $\left\{a_j(\mathbf{x})\right\}_{j=1}^m \subset k[x_1, ..., x_n]$ such that

$$f(\mathbf{x}) = \sum_{j=1}^{m} a_j(\mathbf{x}) g_j(\mathbf{Ax}).$$

Because (by Corollary 1) $\varphi_{\mathbf{A}}(I)$ is an ideal of $k[x_1, ..., x_n]$ and $\left\{g_j(\mathbf{Ax})\right\}_{j=1}^m \subset \varphi_{\mathbf{A}}(I)$, then $f(\mathbf{x}) \in \varphi_{\mathbf{A}}(I)$.

$\Rightarrow$) Because $\varphi_{\mathbf{A}}(I) \subset I$, then we conclude by Lemma 4.2 that $\left\{g_j(\mathbf{Ax})\right\}_{j=1}^m \subset I$. And because I is an ideal, then $\left\langle \left\{g_j(\mathbf{Ax})\right\}_{j=1}^m \right\rangle \subset I$. To prove an opposite inclusion, take any $f(\mathbf{x}) \in I$. By Remark 4.1 we have that $f(\mathbf{A}^{-1}\mathbf{x}) \in I$. Then there exist polynomials $\left\{b_j(\mathbf{x})\right\}_{j=1}^m \subset k[x_1, ..., x_n]$ such that

$$f(\mathbf{A}^{-1}\mathbf{x}) = \sum_{j=1}^{m} b_j(\mathbf{x}) g_j(\mathbf{x}).$$

Applying $\varphi_{\mathbf{A}}$ on both sides of the above equation we obtain

$$f(\mathbf{x}) = \sum_{j=1}^{m} b_j(\mathbf{Ax}) g_j(\mathbf{Ax}),$$

which proves the inclusion $I \subset \left\langle \left\{g_j(\mathbf{Ax})\right\}_{j=1}^m \right\rangle$.

□

We can ask a question: is it possible for an ideal I to be stable under an invertible $\mathbf{A}$, but not to be invariant under the same $\mathbf{A}$? It turns out that this case can not happen. But it can happen for a non-invertible $\mathbf{A}$. Here is an example.

Example 4.1. *Suppose an ideal $I = \langle x, y \rangle \subset \mathbb{Q}[x, y]$. Suppose a non-invertible matrix $\mathbf{A} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \in \mathbb{Q}^{2\times 2}$. Then $\varphi_{\mathbf{A}}(I)$ is a set*

$$\varphi_{\mathbf{A}}(I) = \left\{ h_1(x,y)\varphi_{\mathbf{A}}(x) + h_2(x,y)\varphi_{\mathbf{A}}(y) \;\;|\;\; h_1(x,y), h_2(x,y) \in \varphi_{\mathbf{A}}(\mathbb{Q}[x,y]) \right\} =$$

$$= \left\{ h(x,y)(x-y) \;\;|\;\; h(x,y) \in \varphi_{\mathbf{A}}(\mathbb{Q}[x,y]) \right\}.$$

Another words, $\varphi_{\mathbf{A}}(I)$ is an ideal of $\varphi_{\mathbf{A}}(\mathbb{Q}[x,y])$ generated by one polynomial $x - y$. We see from Lemma 4.2 that $\varphi_{\mathbf{A}}(I) \subset I$, because $\varphi_{\mathbf{A}}(x) = \varphi_{\mathbf{A}}(y) = x - y \in I$. We can also see that $x \in I$, but $x \notin \varphi_{\mathbf{A}}(I)$, because there doesn't exist such $h(x,y) \in \varphi_{\mathbf{A}}(\mathbb{Q}[x,y])$ that $x = h(x,y)(x-y)$. These then means that $\varphi_{\mathbf{A}}(I) \subsetneq I$.

We will next prove that Definitions 4.1 and 4.2 are equivalent for an invertible $\mathbf{A}$. For this we will prepare Lemmas 4.4 and 4.5. In Lemma 4.5 it will be shown that for an *upper triangular invertible matrix* $\mathbf{A}$ (under which I is stable) there exist generators $\Big\{g_j(\mathbf{x})\Big\}_{j=1}^{m}$ of I such that $\Big\{g_j(\mathbf{A}\mathbf{x})\Big\}_{j=1}^{m}$ are also generators of I. To prove Lemma 4.5, we will require the following Lemma 4.4, which tells us that a leading monomial (using lex ordering for variable ordering $x_1 > ... > x_n$) of a transformed monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ by an upper triangular invertible matrix $\mathbf{A}$ is the same monomial $\mathbf{x}^{\boldsymbol{\alpha}}$.

Lemma 4.4. *Suppose an upper triangular invertible matrix* $\mathbf{A} \in k^{n\times n}$. *Then*

$$\mathrm{LM}\Big((\mathbf{A}\mathbf{x})^{\boldsymbol{\alpha}}\Big) = \mathbf{x}^{\boldsymbol{\alpha}}, \quad \forall\, \boldsymbol{\alpha} = \begin{bmatrix}\alpha_1 & ... & \alpha_n\end{bmatrix} \in \mathbb{Z}^n_{\geq 0}.$$

with respect to the lex monomial ordering for variable ordering $x_1 > ... > x_n$.

Proof. We will prove it by induction on the number of variables n. It is obviously true for $n = 1$. Suppose it is true for $n = m-1$. Then we will prove it for $n = m$. We can decompose each monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ as

$$\mathbf{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1}\mathbf{x}_r^{\boldsymbol{\alpha}_r}, \quad \mathbf{x}_r = \begin{bmatrix}x_2\\ \vdots \\ x_m\end{bmatrix}, \quad \boldsymbol{\alpha}_r = \begin{bmatrix}\alpha_2 & ... & \alpha_m\end{bmatrix}.$$

We can also decompose matrix $\mathbf{A}$ as

$$\mathbf{A} = \begin{bmatrix}\mathbf{c}^T & \\ \mathbf{0} & \mathbf{B}\end{bmatrix},$$

where $\mathbf{c}^T \in k^{1\times m}$ and $\mathbf{B} \in k^{(m-1)\times(m-1)}$ is an invertible upper triangular matrix. It is also obvious that

$$(\mathbf{A}\mathbf{x})^{\boldsymbol{\alpha}} = (\mathbf{c}^T\mathbf{x})^{\alpha_1} \cdot (\begin{bmatrix}\mathbf{0} & \mathbf{B}\end{bmatrix}\mathbf{x})^{\boldsymbol{\alpha}_r} = (\mathbf{c}^T\mathbf{x})^{\alpha_1} \cdot (\mathbf{B}\mathbf{x}_r)^{\boldsymbol{\alpha}_r}.$$

By an inductive assumption we know that $\mathrm{LM}\Big((\mathbf{B}\mathbf{x}_r)^{\boldsymbol{\alpha}_r}\Big) = \mathbf{x}_r^{\boldsymbol{\alpha}_r}$. Because $\mathbf{A}$ is an upper triangular invertible matrix, then the first element of $\mathbf{c}$ is nonzero. Then, because of using the lex monomial ordering, we obtain

$$\mathrm{LM}\Big((\mathbf{c}^T\mathbf{x})^{\alpha_1}\Big) = x_1^{\alpha_1}.$$

Then by a well-known property $\mathrm{LM}\Big(f(\mathbf{x}) \cdot g(\mathbf{x})\Big) = \mathrm{LM}\Big(f(\mathbf{x})\Big) \cdot \mathrm{LM}\Big(g(\mathbf{x})\Big)$ for any $f(\mathbf{x})$ and $g(\mathbf{x})$ from $k[x_1, ..., x_n]$ we have

$$\mathrm{LM}\Big((\mathbf{A}\mathbf{x})^{\boldsymbol{\alpha}}\Big) = \mathrm{LM}\Big((\mathbf{c}^T\mathbf{x})^{\alpha_1} \cdot (\mathbf{B}\mathbf{x}_r)^{\boldsymbol{\alpha}_r}\Big) = \mathrm{LM}\Big((\mathbf{c}^T\mathbf{x})^{\alpha_1}\Big) \cdot \mathrm{LM}\Big((\mathbf{B}\mathbf{x}_r)^{\boldsymbol{\alpha}_r}\Big) = x_1^{\alpha_1} \cdot \mathbf{x}_r^{\boldsymbol{\alpha}_r} = \mathbf{x}^{\boldsymbol{\alpha}}.$$

□

Lemma 4.5. *Suppose an ideal* $I \subset k[x_1, ..., x_n]$ *stable under an upper triangular invertible matrix* $\mathbf{A} \in k^{n\times n}$. *Then for a Groebner basis* $\Big\{g_j(\mathbf{x})\Big\}_{j=1}^{m}$ *of* I *with respect to the lex monomial ordering for variable ordering* $x_1 > ... > x_n$, *there holds true that* $\Big\{g_j(\mathbf{A}\mathbf{x})\Big\}_{j=1}^{m}$ *are also generators of* I.

Proof. From Lemma 4.4 we have that

$$\mathrm{LM}\Big(g_j(\mathbf{x})\Big) = \mathrm{LM}\Big(g_j(\mathbf{Ax})\Big) \quad \forall j = 1, ..., m.$$

Then we have

$$\Big\langle \mathrm{LT}(I) \Big\rangle = \Big\langle \Big\{ \mathrm{LM}\Big(g_j(\mathbf{x})\Big) \Big\}_{j=1}^{m} \Big\rangle = \Big\langle \Big\{ \mathrm{LM}\Big(g_j(\mathbf{Ax})\Big) \Big\}_{j=1}^{m} \Big\rangle.$$

Because I is stable under $\mathbf{A}$, then $\Big\{g_j(\mathbf{Ax})\Big\}_{j=1}^{m} \subset I$. Because their leading monomials generate $\langle \mathrm{LT}(I) \rangle$, then we conclude that $\Big\{g_j(\mathbf{Ax})\Big\}_{j=1}^{m}$ is a Groebner basis of I with respect to the lex monomial ordering (and then they are the generators of I).

□

Corollary 2. *Suppose an ideal $I \subset k[x_1, ..., x_n]$ and an upper triangular invertible matrix $\mathbf{A} \in k^{n \times n}$. Then I is stable under $\mathbf{A}$ if and only if it is invariant under $\mathbf{A}$.*

Proof. $\Leftarrow$) This case is trivial.
$\Rightarrow$) Let's take some Groebner basis of I with respect to the lex monomial ordering for variable ordering $x_1 > ... > x_n$. From Lemma 4.5 we have that the images of these generators by $\varphi_{\mathbf{A}}$ also generate I. Then by Lemma 4.3 we obtain that I is invariant under $\mathbf{A}$.

□

Now we give the main Theorem 4.1 of this chapter. It states that for an invertible matrix $\mathbf{A}$ Definitions 4.1 and 4.2 are equivalent.

Theorem 4.1. *Suppose an ideal $I \subset k[x_1, ..., x_n]$ and an invertible matrix $\mathbf{A} \in k^{n \times n}$. Then I is stable under $\mathbf{A}$ if and only if I is invariant under $\mathbf{A}$.*

Proof. $\Leftarrow$) This case is trivial.
$\Rightarrow$) Let I' denote ideal $\varphi_{\mathbf{A}}(I)$. We know that any invertible matrix $\mathbf{A}$ can be decomposed into

$$\mathbf{A} = \mathbf{SDS}^{-1},$$

where $\mathbf{D}$ is a Jordan canonical form of $\mathbf{A}$, which means that $\mathbf{D}$ is upper triangular. And because $\mathbf{A}$ is invertible, then so is $\mathbf{D}$. Denote ideals $\varphi_{\mathbf{S}}(I)$ and $\varphi_{\mathbf{S}}(I')$ by $I_{\mathbf{S}}$ and $I'_{\mathbf{S}}$ respectively. It is obvious that

$$I'_{\mathbf{S}} = \varphi_{\mathbf{S}}(I') = \varphi_{\mathbf{S}}(\varphi_{\mathbf{A}}(I)) = \varphi_{\mathbf{AS}}(I) = \varphi_{\mathbf{SD}}(I) = \varphi_{\mathbf{D}}(\varphi_{\mathbf{S}}(I)) = \varphi_{\mathbf{D}}(I_{\mathbf{S}}) \tag{4.1}$$

And because $I' \subset I$ (I is stable under $\mathbf{A}$), then

$$I'_{\mathbf{S}} = \varphi_{\mathbf{S}}(I') \subset \varphi_{\mathbf{S}}(I) = I_{\mathbf{S}} \tag{4.2}$$

Then from $I'_{\mathbf{S}} = \varphi_{\mathbf{D}}(I_{\mathbf{S}})$ $\Big($ Equation (4.1) $\Big)$ and $I'_{\mathbf{S}} \subset I_{\mathbf{S}}$ $\Big($ Equation (4.2) $\Big)$ we conclude that $I_{\mathbf{S}}$ is stable under $\mathbf{D}$. Because $\mathbf{D}$ is upper triangular invertible matrix, then by Corollary 2 we obtain that

$$I'_{\mathbf{S}} = I_{\mathbf{S}}.$$

As $\varphi_{\mathbf{S}} \colon I \to I_{\mathbf{S}}$ and $\varphi_{\mathbf{S}} \colon I' \to I'_{\mathbf{S}}$ are bijections (they are injective because $\mathbf{S}$ is invertible, and surjective because by definition $I_{\mathbf{S}} = \varphi_{\mathbf{S}}(I)$ and $I'_{\mathbf{S}} = \varphi_{\mathbf{S}}(I')$), then it follows that

$$I' = \varphi_{\mathbf{S}^{-1}}(I'_{\mathbf{S}}) = \varphi_{\mathbf{S}^{-1}}(I_{\mathbf{S}}) = I.$$

And we have the proof.

□

5 Stability of an ideal's variety under a matrix multiplication

In the previous section we have described the stability of an ideal. Here we will describe the stability of an ideal's variety. Consider a (not necessarily invertible) matrix $\mathbf{A} \in k^{n\times n}$. We introduce a usual linear mapping

$$\begin{aligned} \sigma_{\mathbf{A}} \colon k^n &\to k^n \\ \mathbf{x} &\mapsto \mathbf{Ax} \end{aligned} \tag{5.1}$$

The following Definitions 5.1 and 5.2 are similar to the Definitions 4.1 and 4.2 from the previous section about ideals.

Definition 5.1. *A subset $V \subset k^n$ is said to be* ***stable under the matrix*** $\mathbf{A} \in k^{n\times n}$ *if*

$$\sigma_{\mathbf{A}}(V) \subset V.$$

Definition 5.2. *A subset $V \subset k^n$ is said to be* ***invariant under the matrix*** $\mathbf{A} \in k^{n\times n}$ *if*

$$\sigma_{\mathbf{A}}(V) = V.$$

Remark 5.1. *Suppose an invertible matrix $\mathbf{A}$. Then*
1) A subset $V \subset k^n$ is invariant under $\mathbf{A}$ if and only if $\sigma_{\mathbf{A}} \colon V \to V$ is a bijection.
2) Also $\sigma_{\mathbf{A}} \colon V \to V$ is a bijection if and only if V is stable under both $\mathbf{A}$ and $\mathbf{A}^{-1}$.

Proof. Proof can be made by a similar way as the proof of Remark 4.1.

□

We will define $\sigma_{\mathbf{A}}(\varnothing) = \varnothing$ for any matrix $\mathbf{A} \in k^{n\times n}$. Then by Definition 5.2 we conclude that an empty set is invariant under any matrix $\mathbf{A} \in k^{n\times n}$. The following Lemma 5.1 shows a connection between stability of an ideal and its variety.

Lemma 5.1. *Consider an ideal $I \subset k[x_1, ..., x_n]$. If I is stable under $\mathbf{A} \in k^{n\times n}$, then so is $\mathbf{V}(I)$.*

Proof. The statement of the Lemma is obvious for empty $\mathbf{V}(I)$. For a non-empty $\mathbf{V}(I)$ we need to show the following:

$$\mathbf{v} \in \mathbf{V}(I) \Rightarrow f(\mathbf{Av}) = 0 \;\; \forall f(\mathbf{x}) \in I.$$

Because I is stable under $\mathbf{A}$, then from Definition 4.1 we have:

$$p(\mathbf{x}) = f(\mathbf{A}\mathbf{x}) \in I \ \ \forall f(\mathbf{x}) \in I.$$

Because $p(\mathbf{x}) \in I$, then it vanishes on any $\mathbf{v} \in \mathbf{V}(I)$. Then this means that

$$\forall \mathbf{v} \in \mathbf{V}(I) \ \ \forall f(\mathbf{x}) \in I : f(\mathbf{A}\mathbf{v}) = p(\mathbf{v}) = 0.$$

□

Example 5.1. *Suppose an ideal $I \subset \mathbb{Q}[x]$ generated by $f(x) = x^4 - 1$. We can see that I is stable under $\mathbf{A} = -1 \in \mathbb{Q}^{1\times 1}$. The variety $\mathbf{V}(I)$ consists of two solutions ± 1 and is clearly stable under $\mathbf{A}$. Let's suppose an ideal $J \subset \mathbb{C}[x]$ generated by the same $f(x) = x^4 - 1$. We can see that J is also stable under $\mathbf{A} = -1 \in \mathbb{C}^{1\times 1}$. The variety $\mathbf{V}(J)$ consists of four solutions $\pm 1, \pm i$. We clearly see that $\mathbf{V}(J)$ is stable under $\mathbf{A}$. Notice that J and $\mathbf{V}(J)$ are also stable under $\mathbf{A} = \pm i$.*

Example 5.2. *Suppose an ideal $I = \langle x^3 - 1, xy - 1\rangle \subset \mathbb{C}[x, y]$. Denote $f_1(\mathbf{x}) = x^3 - 1$ and $f_2(\mathbf{x}) = xy - 1$. We can see that I is stable under*

$$\mathbf{A} = \begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{2}{3}} \end{bmatrix} \in \mathbb{C}^{2\times 2},$$

because

$$f_1(\mathbf{A}\mathbf{x}) = f_1(\mathbf{x}) \in I, \quad f_2(\mathbf{A}\mathbf{x}) = f_2(\mathbf{x}) \in I.$$

The variety of I is

$$\mathbf{V}(I) = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{1}{3}} \\ e^{2\pi i \frac{2}{3}} \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{2}{3}} \\ e^{2\pi i \frac{1}{3}} \end{bmatrix} \right\}.$$

And we clearly see that $\mathbf{V}(I)$ is also stable under $\mathbf{A}$.

We now give the following Corollary 3 of Lemma 5.1.

Corollary 3. *Suppose an ideal $I \subset k[x_1, ..., x_n]$ and an invertible matrix $\mathbf{A} \in k^{n\times n}$. If I is stable under $\mathbf{A}$, then $\mathbf{V}(I)$ is invariant under $\mathbf{A}$.*

Proof. From Lemma 5.1 it follows that $\mathbf{V}(I)$ is stable under $\mathbf{A}$. By Theorem 4.1 we obtain that I is invariant under $\mathbf{A}$, and then by Remark 4.1 also I is stable under $\mathbf{A}^{-1}$. Then by Lemma 5.1 $\mathbf{V}(I)$ is stable under $\mathbf{A}^{-1}$. By Remark 5.1 it follows that $\mathbf{V}(I)$ is invariant under $\mathbf{A}$.

□

We will next show that from stability of $\mathbf{V}(I)$ we can only talk about stability of a radical ideal of I.

Lemma 5.2. *Suppose an ideal $I \subset k[x_1, ..., x_n]$ and matrix $\mathbf{A} \in k^{n\times n}$. If $\mathbf{V}(I)$ is stable under $\mathbf{A}$, then so is $\mathbf{I}(\mathbf{V}(I))$.*

Proof. To prove that $\mathbf{I}(\mathbf{V}(I))$ is stable under $\mathbf{A}$ we need to show that

$$f(\mathbf{x}) \in \mathbf{I}(\mathbf{V}(I)) \Rightarrow f(\mathbf{Ax}) \in \mathbf{I}(\mathbf{V}(I)).$$

This is equivalent to the following:

$$\forall \mathbf{v} \in \mathbf{V}(I) \ \ \forall f(\mathbf{x}) : f(\mathbf{v}) = 0 \Rightarrow f(\mathbf{Av}) = 0.$$

Take any $\mathbf{v} \in \mathbf{V}(I)$. Because $\mathbf{V}(I)$ is stable under $\mathbf{A}$, then $\mathbf{Av} \in \mathbf{V}(I)$. But then it means that any polynomial $f(\mathbf{x}) \in \mathbf{I}(\mathbf{V}(I))$ vanishes on $\mathbf{Av}$ by the definition of $\mathbf{I}(\mathbf{V}(I))$.

□

Lemma 5.3. *Consider an ideal $I \subset k[x_1, ..., x_n]$ and an invertible matrix $\mathbf{A} \in k^{n\times n}$. Then the following statements are equivalent:*

(i) $\mathbf{V}(I)$ *is stable under* $\mathbf{A}$*,*

(ii) $\mathbf{I}(\mathbf{V}(I))$ *is stable under* $\mathbf{A}$*,*

(iii) $\mathbf{I}(\mathbf{V}(I))$ *is invariant under* $\mathbf{A}$*,*

(iv) $\mathbf{V}(I)$ *is invariant under* $\mathbf{A}$*.*

Proof. $(i) \Rightarrow (ii)$: follows from Lemma 5.2.
$(ii) \Rightarrow (iii)$: follows from Theorem 4.1.
$(iii) \Rightarrow (iv)$: follows from Corollary 3, where we will use the fact that $\mathbf{V}(\mathbf{I}(\mathbf{V}(I))) = \mathbf{V}(I)$.
$(iv) \Rightarrow (i)$: trivial.

□

Lemma 5.2 shows us that if the variety $\mathbf{V}(I)$ of a radical ideal I is stable under $\mathbf{A}$, then I is stable under $\mathbf{A}$. But it shouldn't be true for a non-radical ideal. We give the following Example 5.3, which shows it.

Example 5.3. *We will take a non-radical ideal $I = \langle x^2, y^2 \rangle \subset \mathbb{Q}[x, y]$. Its variety is*

$$\mathbf{V}(I) = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}.$$

This variety is stable under any matrix $\mathbf{A} \in \mathbb{Q}^{2\times 2}$. For example if we'll take

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

then by Definition 4.1 I isn't stable under $\mathbf{A}$, because for $f(\mathbf{x}) = x^2 \in I$ we have:

$$xy \notin I \Rightarrow f(\mathbf{Ax}) = (x + y)^2 = x^2 + 2xy + y^2 \notin I.$$

But if we take a radical ideal

$$J = \langle x, y \rangle \subset \mathbb{Q}[x, y]$$

with the same variety, then for its two generators $g_1(\mathbf{x}) = x$ and $g_2(\mathbf{x}) = y$ we have

$$g_1(\mathbf{Ax}) = x + y \in I, \quad g_2(\mathbf{Ax}) = y \in I.$$

Then, by Lemma 4.2, an ideal J is stable under $\mathbf{A}$.

As the last thing of this section we will say something about groups of stability matrices of an ideal I. The following Lemma 5.4 tells us that all invertible stability matrices of an ideal I form a group.

Lemma 5.4. *Suppose an ideal $I \subset k[x_1, ..., x_n]$. Then all its invertible stability matrices $\mathbf{A} \in k^{n \times n}$ form a group with respect to the operation of matrix multiplication.*

Proof. The set of all such matrices is obviously closed under matrix multiplication (it follows from Definition 4.1). Matrix multiplication is associative. Obviously, an identity matrix is one of stability matrices. And to every stability matrix $\mathbf{A}$ there exists an inverse $\mathbf{A}^{-1}$, which is by Theorem 4.1 also a stability matrix of I.

□

We will denote the group of all invertible stability matrices of I as G_I. In the next Chapter 6 we will use a notion of stability under a group of matrices. We give the following Definitions 5.3 and 5.4.

Definition 5.3. *A polynomial ideal $I \subset k[x_1, ..., x_n]$ is said to be* `stable under a group` *$G \subset \mathrm{GL}_n(k)$ if it is stable under any matrix from G.*

Definition 5.4. *A subset $V \subset k^n$ is said to be* `stable under a group` *$G \subset \mathrm{GL}_n(k)$ if it is stable under any matrix from G.*

6 Stability under a diagonal matrix of a special kind and a generalization of homogeneous polynomials

In this chapter we will see how homogeneous polynomials are connected with the stability of ideals under diagonal matrices of a "special kind". It even turns out that it is very easy to find all such stability diagonal matrices of a given ideal (we will describe the method in Section 8). By a "special kind" we understand the following kind of diagonal matrix:

$$D_\lambda^{\mathbf{c}} = \operatorname{diag}\left(\left\{\lambda^{c_j}\right\}_{j=1}^{n}\right) \in k^{n\times n}, c_j \in \mathbb{Z}, \lambda \in k^* \tag{6.1}$$

By k^* we denote $k\backslash\{0\}$. There is a reason why we suppose such a special kind of $D_\lambda^{\mathbf{c}}$. This matrix acts on a polynomial in a very nice way:

$$f(\mathbf{x}) = \sum_{j=1}^{s} a_j \mathbf{x}^{\boldsymbol{\alpha}_j} \Rightarrow \varphi_{D_\lambda^{\mathbf{c}}}(f(\mathbf{x})) = f(D_\lambda^{\mathbf{c}}\mathbf{x}) = \sum_{j=1}^{s} \lambda^{\mathbf{c}^T\boldsymbol{\alpha}_j} a_j \mathbf{x}^{\boldsymbol{\alpha}_j} = \sum_{j=1}^{s} \lambda^{q_j} a_j \mathbf{x}^{\boldsymbol{\alpha}_j}, \quad q_j = \mathbf{c}^T\boldsymbol{\alpha}_j \in \mathbb{Z}.$$

An interesting thing comes up when one of the following conditions holds true:

a) all q_j are equal to some $q \in \mathbb{Z}$.
b) there exists $p \in \mathbb{N}, p > 1$ such that all q_j are equal to some $q \in \mathbb{Z}_p$ modulo p.

We will discuss these two cases later. The main goal of this chapter is to give a necessary and sufficient condition for an ideal I to be stable under $D_\lambda^{\mathbf{c}}$. To understand the following material we should be familiar with the concept of a homogeneous polynomial. We recall that the total degree of monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ is defined as $\mathbf{1}^T\boldsymbol{\alpha}$.

Definition 6.1. *A polynomial $f(\mathbf{x}) \in k[x_1, ..., x_n]$ is said to be* **homogeneous** *if all monomials in $f(\mathbf{x})$ have the same total degree.*

Example 6.1. *A polynomial $f(\mathbf{x}) = x^3 + 2x^2y + y^3$ is homogeneous, because all monomials in $f(\mathbf{x})$ have the same total degree, which is equal to* 3.

We now give two similar Definitions 6.2 and 6.3 which relate to the conditions **a)** and **b)** above. By a **c**-weighted total degree of monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ we will mean a number $\mathbf{c}^T\boldsymbol{\alpha}$.

Definition 6.2. *A polynomial $f(\mathbf{x}) \in k[x_1, ..., x_n]$ is said to be* **c**-*weighted homogeneous for* $\mathbf{c} \in \mathbb{Z}^n$ *if all monomials in* $f(\mathbf{x})$ *have the same* **c**-*weighted total degree, i.e.*

$$f(\mathbf{x}) = \sum_{j=1}^{s} a_j \mathbf{x}^{\boldsymbol{\alpha}_j} \Rightarrow \mathbf{c}^T \boldsymbol{\alpha}_1 = \mathbf{c}^T \boldsymbol{\alpha}_2 = ... = \mathbf{c}^T \boldsymbol{\alpha}_s.$$

Definition 6.3. *A polynomial $f(\mathbf{x}) \in k[x_1, ..., x_n]$ is said to be* **c**-*weighted p-homogeneous for* $\mathbf{c} \in \mathbb{Z}^n$ *and $p \in \mathbb{N}$, $p > 1$ if all monomials in* $f(\mathbf{x})$ *have the same* **c**-*weighted total degree modulo p, i.e.*

$$f(\mathbf{x}) = \sum_{j=1}^{s} a_j \mathbf{x}^{\boldsymbol{\alpha}_j} \Rightarrow \mathbf{c}^T \boldsymbol{\alpha}_1 \equiv \mathbf{c}^T \boldsymbol{\alpha}_2 \equiv ... \equiv \mathbf{c}^T \boldsymbol{\alpha}_s \bmod p.$$

Notice that in Definition 6.3 we didn't exclude that $f(\mathbf{x})$ isn't a **c**-weighted homogeneous. It means that every **c**-weighted homogeneous polynomial is **c**-weighted p-homogeneous for every $p \in \mathbb{N}$, $p > 1$. Such a definition was made not to confuse the reader while giving Proposition 6.1. Also notice that Definition 6.2 is a small generalization of homogenity from Defintion 6.1 (which is for $\mathbf{c} = \mathbf{1}$). We give the following two Lemmas 6.1 and 6.2, which connect Definitions 6.2 and 6.3 with cases **a)** and **b)**, respectively.

Lemma 6.1. *Suppose a polynomial $f(\mathbf{x}) \in k[x_1, ..., x_n]$. Then $f(\mathbf{x})$ is* **c**-*weighted homogeneous if and only if*

$$f(D_\lambda^{\mathbf{c}} \mathbf{x}) = \lambda^q f(\mathbf{x}) \quad \forall \lambda \in k^*$$

for some $q \in \mathbb{Z}$.

Proof. $\Rightarrow$) Trivial.
$\Leftarrow$) We have

$$f(\mathbf{x}) = \sum_{j=1}^{s} b_j \mathbf{x}^{\boldsymbol{\alpha}_j} \Rightarrow \lambda^q f(\mathbf{x}) = f(D_\lambda^{\mathbf{c}} \mathbf{x}) = \sum_{j=1}^{s} \lambda^{q_j} \cdot b_j \mathbf{x}^{\boldsymbol{\alpha}_j} \quad \forall \lambda \in k^*,$$

or

$$h_\lambda(\mathbf{x}) = \sum_{j=1}^{s} (\lambda^q - \lambda^{q_j}) \cdot b_j \mathbf{x}^{\boldsymbol{\alpha}_j} = 0 \quad \forall \lambda \in k^* \tag{6.2}$$

Equation (6.2) means that $h_\lambda(\mathbf{x})$ is the zero polynomial for every $\lambda \in k^*$. Since $b_j \neq 0$ for $j = 1, ..., s$, it follows that

$$\lambda^q - \lambda^{q_j} = 0 \quad \forall \lambda \in k^*, \forall j = 1, ..., s \tag{6.3}$$

If $q_j = q \; \forall j = 1, ..., s$, then we are done. So, suppose that there exists $q_m \neq q$ for some $1 \leq m \leq s$. Notice that q and q_m can be negative integers. We take the least of q and q_m (call it t). Then $p(x) = x^{q-t} - x^{q_m - t}$ is a polynomial in $k[x]$. Equation (6.3) means that $p(\lambda) = 0 \; \forall \lambda \in k^*$. But we know that every nonzero polynomial in $k[x]$ of degree d has at most d roots in k. Since k is infinite, it follows that $p(x)$ has infinitely many roots. Hence $p(x)$ must be the zero polynomial, which means that $q - t = q_m - t$. And then $q = q_m$.

□

Lemma 6.2. *A polynomial $f(\mathbf{x}) \in \mathbb{C}[x_1, ..., x_n]$ is* $\mathbf{c}$*-weighted* p*-homogeneous if and only if*

$$f(D_\lambda^{\mathbf{c}}\mathbf{x}) = \lambda^q f(\mathbf{x}) \quad \forall \lambda \in \mathbb{U}_p$$

for some $q \in \mathbb{Z}$. By $\mathbb{U}_p$ we denote the finite group of p-th roots of unity.

Proof. By the same steps as in the proof of Lemma 6.1 we obtain

$$\lambda^q - \lambda^{q_j} = 0 \quad \forall \lambda \in \mathbb{U}_p, \forall j = 1, ..., s \tag{6.4}$$

If $q_j \equiv q \bmod p \ \forall j = 1, ..., s$, then we are done. So, suppose that there exists $q_m \not\equiv q \bmod p$ for some $1 \leq m \leq s$. Equation (6.4) means that

$$e^{2\pi i \frac{q}{p}} - e^{2\pi i \frac{q_m}{p}} = 0$$

for chosen $\lambda = e^{2\pi i \frac{1}{p}}$. Dividing this equation by $e^{2\pi i \frac{q_m}{p}}$ we obtain

$$e^{2\pi i \frac{q - q_m}{p}} = 1,$$

which is true if and only if $q - q_m \equiv 0 \bmod p$. Then $q \equiv q_m \bmod p$.

□

We will denote the infinite group of matrices $D_\lambda^{\mathbf{c}}$, $\lambda \in k^*$ for some fixed $\mathbf{c} \in \mathbb{Z}^n$ by $G_k^{\mathbf{c}}$. Similarly, by $G_p^{\mathbf{c}}$ we will denote the finite group of matrices $D_\lambda^{\mathbf{c}}$, $\lambda \in \mathbb{U}_p$ for some fixed $\mathbf{c} \in \mathbb{Z}^n$.

Next we give Proposition 6.1 which connects a homogenity of polynomials with an ideal's stability. At first, let's recall what is a reduced Groebner basis of a polynomial ideal. The following Definition 6.4 is taken directly from [4, p. 90, Definition 5].

Definition 6.4. *Fix an arbitrary monomial ordering. A* `reduced Groebner basis` *for a polynomial ideal I is a Groebner basis G for I such that:*

(i) $\mathrm{LC}(g) = 1$ *for all $g \in G$.*

(ii) For all $g \in G$, none of non-leading monomials of g lies in $\langle \mathrm{LT}(G) \rangle$.

Proposition 6.1. *Let $I \subset k[x_1, ..., x_n]$ (resp. $I \subset \mathbb{C}[x_1, ..., x_n]$) be a polynomial ideal. Then, I is stable under $G_k^{\mathbf{c}}$ (resp. $G_p^{\mathbf{c}}$) if and only if each polynomial in a reduced Groebner basis of I (with respect to any monomial ordering) consists of* $\mathbf{c}$*-weighted homogeneous (resp.* $\mathbf{c}$*-weighted p-homogeneous) polynomials.*

The following Lemmas 6.3 and 6.4 prove the ⇐ implication of the above Proposition 6.1.

Lemma 6.3. *Let $I \subset k[x_1, ..., x_n]$ be a polynomial ideal. Suppose some set $G = \left\{ g_j(\mathbf{x}) \right\}_{j=1}^m$ of generators of I. If each g_j, $j = 1, ..., m$ is* $\mathbf{c}$*-weighted homogeneous, then I is stable under $G_k^{\mathbf{c}}$.*

Proof. Let q_j be a $\mathbf{c}$-weighted total degree of each monomial in g_j. Take any matrix $D_\lambda^\mathbf{c}$ from $G_k^\mathbf{c}$. Then by Lemma 6.1 ($\Rightarrow$ implication) we have

$$g_j(D_\lambda^\mathbf{c}\mathbf{x}) = \lambda^{q_j} f(\mathbf{x}) \in I, \quad \forall j = 1, ..., m.$$

Then by Lemma 4.2 we obtain that I is stable under $D_\lambda^\mathbf{c}$ and this proves the Lemma.

□

Lemma 6.4. *Let $I \subset \mathbb{C}[x_1, ..., x_n]$ be a polynomial ideal. Suppose some set $G = \left\{g_j(\mathbf{x})\right\}_{j=1}^m$ of generators of I. If each g_j, $j = 1, ..., m$ is $\mathbf{c}$-weighted p-homogeneous, then I is stable under $G_p^\mathbf{c}$.*

Proof. This Lemma can be proved in a similar way as Lemma 6.3 (using Lemma 6.2 instead of Lemma 6.1).

□

Notice that the $\Leftarrow$ implication of Proposition 6.1 works for any basis of I (not only for a reduced Groebner basis), while the $\Rightarrow$ implication can fail for some basis of I. We give an Example 6.2.

Example 6.2. *Consider an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$, where*

$$f_1(\mathbf{x}) = x^2 + y^2, \quad f_2(\mathbf{x}) = x + y.$$

Then I is stable under

$$\mathbf{A} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in \mathbb{Q}^{2\times 2},$$

because

$$f_1(\mathbf{Ax}) = f_1(\mathbf{x}) \in I, \quad f_2(\mathbf{Ax}) = -f_2(\mathbf{x}) \in I.$$

We see that f_1 and f_2 are $\mathbf{1}$-weighted homogeneous of total degree 2 and 1 respectively. We can construct another basis of I:

$$I = \langle f_3, f_4 \rangle, \quad f_3(\mathbf{x}) = x^2 + y^2 + x + y, f_4(\mathbf{x}) = x + y.$$

We can see that f_3 is not $\mathbf{1}$-weighted homogeneous. However this cannot happen for a reduced Groebner basis of I.

Now, we are ready to prove a Proposition 6.1. We will split the proof into two Theorems 6.1 and 6.2 (for $G_k^\mathbf{c}$ and $G_p^\mathbf{c}$ respectively). We will prove only Theorem 6.1, because Theorem 6.2 can be proved in the same way.

Theorem 6.1. *Let $I \subset k[x_1, ..., x_n]$ be a polynomial ideal. Then I is stable under $G_k^\mathbf{c}$ if and only if its reduced Groebner basis $G = \left\{g_j(\mathbf{x})\right\}_{j=1}^m$ (with respect to any monomial ordering) consists of $\mathbf{c}$-weighted homogeneous polynomials.*

Proof. $\Leftarrow$) This case has been already proved by Lemma 6.3.
$\Rightarrow$) We will prove that if there exists a $g_t(\mathbf{x}) \in G$ that isn't $\mathbf{c}$-weighted homogeneous, then I isn't stable under $G_k^{\mathbf{c}}$. Our aim now is to find at least one $f(\mathbf{x})$ such that $f(D_\lambda^{\mathbf{c}}\mathbf{x}) \notin I$ for some $D_\lambda^{\mathbf{c}} \in G_k^{\mathbf{c}}$. Then, by Definition 5.3, we will get that I isn't stable under $G_k^{\mathbf{c}}$. We will show that such $f(\mathbf{x})$ is $g_t(\mathbf{x})$. The fact that $g_t(\mathbf{x})$ isn't $\mathbf{c}$-weighted homogeneous means (from Lemma 6.1) that there exists such $D_{\lambda_t}^{\mathbf{c}} \in G_k^{\mathbf{c}}$ that

$$g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) \neq \lambda^q g_t(\mathbf{x}) \quad \text{for any } q \in \mathbb{Z} \tag{6.5}$$

To get a contradiction, suppose $g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) \in I$. Let

$$g_t(\mathbf{x}) = \mathbf{x}^{\boldsymbol{\alpha}_1} + \sum_{j=2}^{s} a_j \mathbf{x}^{\boldsymbol{\alpha}_j}, \quad \mathrm{LT}(g_t) = \mathbf{x}^{\boldsymbol{\alpha}_1}.$$

Then

$$g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) = \lambda^{q_1}\mathbf{x}^{\boldsymbol{\alpha}_1} + \sum_{j=2}^{s} \lambda^{q_j} a_j \mathbf{x}^{\boldsymbol{\alpha}_j}.$$

Construct a polynomial

$$f(\mathbf{x}) = \lambda^{q_1} g_t(\mathbf{x}) - g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) = \sum_{j=2}^{s} \left(\lambda^{q_1} - \lambda^{q_j}\right) a_j \mathbf{x}^{\boldsymbol{\alpha}_j}.$$

The polynomial $f(\mathbf{x})$ is not the zero polynomial, which follows from Equation (6.5). Using assumption $g_t(\mathbf{x}) \in I$ and $g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) \in I$ we conclude that $f(\mathbf{x}) \in I$. Because G is a Groebner basis of I, then

$$\mathrm{LM}(f) \in \big\langle \mathrm{LT}(G) \big\rangle.$$

Notice that $\mathrm{LM}(f)$ is a non-leading monomial of g_t. Then by (ii) in Definition 6.4, it is a contradiction. So we must have that $g_t(D_{\lambda_t}^{\mathbf{c}}\mathbf{x}) \notin I$ and by Definition 5.3 we have that I isn't stable under $G_k^{\mathbf{c}}$.

□

Theorem 6.2. *Let $I \subset \mathbb{C}[x_1, ..., x_n]$ be a polynomial ideal. Then I is stable under $G_p^{\mathbf{c}}$ if and only if its reduced Groebner basis (with respect to any monomial ordering) consists of $\mathbf{c}$-weighted p-homogeneous polynomials.*

Proof. $\Leftarrow$) This case has been already proved by Lemma 6.4.
$\Rightarrow$) The proof can again be made in a similar way as the proof of Theorem 6.1 (using Lemma 6.2 instead of Lemma 6.1).

□

We want to note that Theorem 6.1 works generally only for infinite fields k, because the $\Leftarrow$ implication of Lemma 6.1 works generally only for infinite fields.

We refer to [4, p. 371, Definition 1 and Theorem 2]. At first we will explain what does the notion of homogeneous component mean. Suppose a polynomial f. Let f_j be the sum of all terms of $\mathbf{c}$-weighted total degree j. Then we call f_j the jth $\mathbf{c}$-weighted homogeneous component of f. We give the following Definition 6.5 and Theorem 6.3 (from [4, p. 371]).

Definition 6.5. *An ideal $I \subset k[x_1, ..., x_n]$ is said to be* $\mathbf{1}$*-weighted* `homogeneous` *if for each $f \in I$, the* $\mathbf{1}$*-weighted homogeneous components f_j of f are in I as well.*

Theorem 6.3. *Let $I \subset k[x_1, ..., x_n]$ be an ideal. Then the following are equivalent:*

(i) I is a $\mathbf{1}$*-weighted homogeneous ideal.*

(ii) $I = \langle f_1, ..., f_m \rangle$, where $f_1, ..., f_m$ are $\mathbf{1}$*-weighted homogeneous polynomials.*

(iii) A reduced Groebner basis of I (with respect to any monomial ordering) consists of $\mathbf{1}$*-weighted homogeneous polynomials.*

The above Theorem 6.3 can be generalized for $\mathbf{c}$-weighted homogenity and $\mathbf{c}$-weighted p-homogenity (we won't give the proof here). We can add one more statement to Theorem 6.3 about the stability of I and obtain the following Theorem 6.4.

Theorem 6.4. *Let $I \subset k[x_1, ..., x_n]$ (resp. $I \subset \mathbb{C}[x_1, ..., x_n]$) be an ideal. Then the following are equivalent:*

(i) I is a $\mathbf{c}$*-weighted homogeneous (resp.* $\mathbf{c}$*-weighted p-homogeneous) ideal.*

(ii) $I = \langle f_1, ..., f_m \rangle$, where $f_1, ..., f_m$ are $\mathbf{c}$*-weighted homogeneous (resp.* $\mathbf{c}$*-weighted p-homogeneous) polynomials.*

(iii) A reduced Groebner basis of I (with respect to any monomial ordering) consists of $\mathbf{c}$*-weighted homogeneous (resp.* $\mathbf{c}$*-weighted p-homogeneous) polynomials.*

(iv) I is stable under $G_k^{\mathbf{c}}$ (resp. $G_p^{\mathbf{c}}$).

We refer to some previous works [6, 7, 9]. In [6, Theorem 4], [7, Proposition 5.3] and [9, Theorem 1, Theorem 2 and Corollary 1] there is a proof of $(i) \iff (ii) \iff (iv)$ of the above Theorem 6.4 for $\mathbf{c}$-weighted p-homogenity using VanDerMonde matrix. However, in these papers there is no statement (iii) about reduced Groebner basis.

In Chapter 8 we will show how to apply Theorems 6.1 and 6.2 on finding groups $G_k^{\mathbf{c}}$ and $G_p^{\mathbf{c}}$ of stability matrices of a given ideal I. However, to understand Chapter 8, we should be familiar with the concepts of Hermite and Smith normal form of an integer matrix.

7 Remarks on Modules, Hermite and Smith Normal Forms

7.1 Modules

We cite [5, p. 179]: "Modules are to rings what vector spaces are to fields: elements of a given module over a ring can be added to one another an multiplies by elements of a ring. The axioms for a module are the same as for a vector space but instead of a field there is a commutative ring".

An R-module M is said to be ***finitely generated*** if there exist such $f_1, ..., f_m \in M$ such that for any $f \in M$ there exist such $r_1, ..., r_m \in R$ that $f = r_1 f_1 + ... + r_m f_m$. Such set of $f_1, ..., f_m$ is called a ***generating set of*** M. Linear dependence (resp. independence) is defined the same as for the vector spaces. What is different for modules (unlike for the vector spaces) is that a finitely generated M need not to have a linearly independent generating set (basis). The reason for this is that

$$a_1 f_1 + ... + a_m f_m = 0_M, \quad a_j \in R, f_j \in M, a_1 \neq 0_R$$

doesn't generally imply

$$\exists\, b_2, ..., b_m \in R : f_1 = b_2 f_2 + ... + b_m f_m.$$

However, there are modules which have a basis. These are called ***free*** modules. If every basis of a free finitely generated module M has the same number of elements, then we say that M is ***free of finite rank***.

We cite [2, p. 64]: "We can study most of linear algebra problems in the context of modules over a commutative ring instead of vector spaces over a field. If the ring R is an integral domain (no zero divisors), we can work over its field of fractions K. However, this is not completely satisfactory, since the answer that we want may be different. For example, to compute the kernel of a map defined between two free modules of finite rank (given as usual by a matrix), finding the kernel as a K-vector space is not sufficient, since we want it as an R-module. In fact, this kernel will usually not be a free module, hence cannot be represented by a matrix whose columns form a basis. One important special case where it will be free is when R is a principal ideal domain (an integral domain where every ideal is generated by one element). In this case all submodules of a free module of finite rank are free of finite rank. This happens when $R = \mathbb{Z}$ or $R = k[x]$ for a field k. In this case, asking for a basis of the kernel makes perfectly good sense".

7.2 The Hermite Normal Form

In Chapter 8 we will use the concepts Hermite and Smith normal form of an integer matrix. We give the following Definition 7.1 about the Hermite normal form.

Definition 7.1. *We will say that a matrix $M \in \mathbb{Z}^{m\times n}$, $M = m_{i,j}$ is in* `column Hermite normal form` *(abbreviated column HNF) if there exists $r \leq n$ and a strictly increasing map f from $[1, n-r]$ to $[1, m]$ satisfying the following properties:*

(i) For $1 \leq j \leq n-r$, $m_{f(j),j} \geq 1$, $m_{i,j} = 0$ if $i > f(j)$ and $0 \leq m_{f(k),j} < m_{f(k),k}$ if $k < j$.

(ii) The last r columns of M are zero.

Example 7.1. *Suppose the following matrix*

$$M = \begin{bmatrix} 1 & 0 & 5 \\ 4 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix} \in \mathbb{Z}^{5\times 3}.$$

We see that M has no zero columns, then $r = 0$. A strictly increasing map f from $[1, 3]$ (columns) to $[1, 5]$ (rows) can be defined as $f(1) = 2$ ($m_{2,1} = 4 \geq 1$), $f(2) = 4$ ($m_{4,2} = 1 \geq 1$), $f(3) = 5$ ($m_{5,3} = 2 \geq 1$). The statement $m_{i,j} = 0$ if $i > f(j)$ means that all elements in the column under each of pivots $m_{2,1}$, $m_{4,2}$ and $m_{5,3}$ are zero. The statement $0 \leq m_{f(k),j} < m_{f(k),k}$ if $k < j$ means that all elements in the rows to the right of pivots are non-negative and smaller than this pivot. Then we conclude that M is in column Hermite normal form.

Example 7.2. *For $m < n$ a matrix $M \in \mathbb{Z}^{m\times n}$ of full row rank in column Hermite normal form has the following shape:*

$$\begin{bmatrix} * & * & \dots & * & 0 & 0 & \dots & 0 \\ 0 & * & \dots & * & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & * & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Theorem 7.1. *Let $A \in \mathbb{Z}^{m\times n}$. Then there exists a unique $B \in \mathbb{Z}^{m\times n}$ in column HNF of the form $B = AU$ with $U \in \mathrm{GL}_n(\mathbb{Z})$, where $\mathrm{GL}_n(\mathbb{Z})$ is the group of matrices with integer coefficients which are invertible, i.e. whose determinant is equal to ±1.*

Proposition 7.1. *Let $A \in \mathbb{Z}^{m\times n}$, $B = AU$ its column HNF with $U \in \mathrm{GL}_n(\mathbb{Z})$, and let r be such that the last r columns of B are zero. Then a $\mathbb{Z}$-basis for the right integer kernel of A is given by the last r columns of U.*

The algorithmic proof of Theorem 7.1 can be found in [2, p. 68, Algorithm 2.4.4]. The proof of Proposition 7.1 can be found in [2, p. 73, Proposition 2.4.9].

By will also define a row Hermite normal form.

Definition 7.2. *We will say that a matrix $M \in \mathbb{Z}^{m\times n}$ is in* `row Hermite normal form` *(abbreviated row HNF) if M^T is in column Hermite normal form.*

Proposition 7.2. *Let $A \in \mathbb{Z}^{m\times n}$. Then there exists a unique $B \in \mathbb{Z}^{m\times n}$ in row HNF of the form $B = UA$ with $U \in \mathrm{GL}_m(\mathbb{Z})$.*

Proof. Suppose $B^T = A^T U^T$ is in column HNF, $U^T \in \mathrm{GL}_m(\mathbb{Z})$ (from Theorem 7.1 we know that such U^T exists). Then $B = UA$ is in row HNF and $U \in \mathrm{GL}_m(\mathbb{Z})$.

□

Proposition 7.3. *Let $A \in \mathbb{Z}^{m\times n}$, $B = UA$ its row HNF with $U \in \mathrm{GL}_m(\mathbb{Z})$, and let r be such that the last r rows of B are zero. Then a $\mathbb{Z}$-basis for the left integer kernel of A is given by the last r rows of U.*

Proof. The proof can be obtained similarly as the proof of Proposition 7.1 and using the fact that the left integer kernel of A is the right integer kernel of A^T.

□

7.3 The Smith Normal Form

The following Definition 7.3 explains what is the Smith normal form of an integer matrix. In the Definition 7.3 below we use a notation $a \mid b$ for integers a and b, which means that there exists $c \in \mathbb{Z}$ such that $b = ac$.

Definition 7.3. *We say that a full row rank matrix $B \in \mathbb{Z}^{m\times n}$ is in Smith normal form if B is a diagonal matrix with nonnegative integer coefficients such that $b_{i,i} \mid b_{i+1,i+1}$ for all $i < n$.*

Example 7.3. *The following matrix*

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{bmatrix}$$

is clearly in Smith normal form.

Theorem 7.2. *Let $A \in \mathbb{Z}^{m\times n}$ be a matrix of full row rank. Then there exists a unique matrix in Smith normal form B such that $B = VAU$ with U and V elements of $\mathrm{GL}_n(\mathbb{Z})$.*

The proof of Theorem 7.2 can be found in [2, p. 76, Theorem 2.4.12] for the case $m = n$.

8 Finding Scaling (Diagonal) Symmetries of a Given Polynomial System

In this chapter we will explain how to use linear algebra tools for finding all stability diagonal matrices of kind (6.1) of a given ideal. We refer to the previous works [8, Appendix A] (describes how to find $G_k^{\mathbf{c}}$) and [7, Section 6] (describes how to find $G_p^{\mathbf{c}}$). We will start with two examples (finding $G_k^{\mathbf{c}}$ in Example 8.1 and $G_p^{\mathbf{c}}$ in Example 8.2) and then give general methods. If an ideal $I \subset k[x_1, ..., x_n]$ has a group of stability matrices $G_k^{\mathbf{c}}$ (resp. $G_p^{\mathbf{c}}$), then we will say that I has infinite (resp. finite) symmetries.

Example 8.1. *Suppose an ideal*

$$I = \langle f_1, f_2\rangle \subset \mathbb{C}[z_1, z_2, z_3, z_4], \quad f_1 = z_2 z_4^2 - z_1 - z_4, f_2 = z_1 z_3 - z_2, F = \Big\{f_1, f_2\Big\}.$$

We will construct the so-called "matrix of exponent differences" K_F. From f_1 and f_2 we extract multidegrees of monomials for variable ordering $z_1 > z_2 > z_3 > z_4$:

$$f_1 \to \underbrace{\begin{bmatrix}0\\1\\0\\2\end{bmatrix}}_{d_{1_1}}, \underbrace{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}}_{d_{1_2}}, \underbrace{\begin{bmatrix}0\\0\\0\\1\end{bmatrix}}_{d_{1_3}} \quad f_2 \to \underbrace{\begin{bmatrix}1\\0\\1\\0\end{bmatrix}}_{d_{2_1}}, \underbrace{\begin{bmatrix}0\\1\\0\\0\end{bmatrix}}_{d_{2_2}}.$$

Then construct K_F as follows. Take the first multidegree d_{1_1} and d_{2_1} in f_1 and f_2 respectively and for the rest multidegrees $d_{1_j}, j > 1$ and $d_{2_j}, j > 1$ compute the differences $d_{1_j} - d_{1_1}$ and $d_{2_j} - d_{2_1}$ and put these differences as columns to the matrix K_F. We will obtain

$$K_F = \left[\begin{bmatrix}1\\0\\0\\0\end{bmatrix} - \begin{bmatrix}0\\1\\0\\2\end{bmatrix} \quad \begin{bmatrix}0\\0\\0\\1\end{bmatrix} - \begin{bmatrix}0\\1\\0\\2\end{bmatrix} \quad \begin{bmatrix}0\\1\\0\\0\end{bmatrix} - \begin{bmatrix}1\\0\\1\\0\end{bmatrix}\right] = \begin{bmatrix}1 & 0 & -1\\-1 & -1 & 1\\0 & 0 & -1\\-2 & -1 & 0\end{bmatrix}.$$

Compute a row Hermite normal form of K_F by some unimodular multiplier U:

$$\underbrace{\begin{bmatrix}1 & 0 & -1 & 0\\-1 & -1 & 0 & 0\\0 & 0 & -1 & 0\\1 & -1 & -2 & 1\end{bmatrix}}_{U}\underbrace{\begin{bmatrix}1 & 0 & -1\\-1 & -1 & 1\\0 & 0 & -1\\-2 & -1 & 0\end{bmatrix}}_{K_F} = \underbrace{\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\\0 & 0 & 0\end{bmatrix}}_{H}.$$

We see that the last row of H is zero. Then, by Proposition 7.3, the last row of U forms a basis for the integer lattice of the left kernel of K_F. Then we obtain the infinite group of stability matrices $G^{\mathbf{c}}_{\mathbb{C}}$, where $\mathbf{c} = \begin{bmatrix}1 & -1 & -2 & 1\end{bmatrix}$ is the last row of U.

To see that I is stable under $G^{\mathbf{c}}_{\mathbb{C}}$ suppose an arbitrary matrix

$$D^{\mathbf{c}}_{\lambda} = \begin{bmatrix}\lambda & & & \\ & \frac{1}{\lambda} & & \\ & & \frac{1}{\lambda^2} & \\ & & & \lambda\end{bmatrix}, \quad \lambda \in \mathbb{C}^*$$

from $G^{\mathbf{c}}_{\mathbb{C}}$. We will now show that $f_1(D^{\mathbf{c}}_{\lambda}\mathbf{z})$ and $f_2(D^{\mathbf{c}}_{\lambda}\mathbf{z})$ are in I, where $\mathbf{z} = \begin{bmatrix}z_1 & z_2 & z_3 & z_4\end{bmatrix}^T$. Then by Lemma 4.2 we get that I is stable under $D^{\mathbf{c}}_{\lambda}$. We obtain

$$f_1(D^{\mathbf{c}}_{\lambda}\mathbf{z}) = \Big(\frac{1}{\lambda}z_2\Big)\Big(\lambda z_4\Big)^2 - \lambda z_1 - \lambda z_4 = \lambda f_1(\mathbf{z}) \in I,$$

$$f_2(D^{\mathbf{c}}_{\lambda}\mathbf{z}) = \Big(\lambda z_1\Big)\Big(\frac{1}{\lambda^2}z_3\Big) - \frac{1}{\lambda}z_2 = \frac{1}{\lambda}f_2(\mathbf{z}) \in I.$$

Example 8.2. *Suppose an ideal*

$$I = \langle f_1, f_2\rangle \subset \mathbb{C}[x,y], \quad f_1 = x^3 - 1, f_2 = xy - 1, F = \Big\{f_1, f_2\Big\}.$$

Construct the matrix K_F by the same method as in Example 8.1 for variable ordering $x > y$:

$$K_F = \begin{bmatrix}-3 & -1\\ 0 & -1\end{bmatrix}.$$

We see that K_F has full row rank over $\mathbb{Z}$, and thus I has no infinite symmetries. Let us try to find finite symmetries. Unimodular multipliers U and V for Smith normal form of K_F are:

$$\underbrace{\begin{bmatrix}0 & -1\\ -1 & 1\end{bmatrix}}_{U}\underbrace{\begin{bmatrix}-3 & -1\\ 0 & -1\end{bmatrix}}_{K_F}\underbrace{\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}}_{V} = \underbrace{\begin{bmatrix}1 & 0\\ 0 & 3\end{bmatrix}}_{S}.$$

We look on the diagonal elements of S greater than 1. There is element $p = 3$ in the 2-nd row of S. Then vector $\mathbf{c}$ is represented by the 2-nd row of U. We obtain that I has finite symmetries $G^{\mathbf{c}}_{p}$, where $\mathbf{c} = \begin{bmatrix}-1 & 1\end{bmatrix}$ and $p = 3$, which means that

$$G^{\mathbf{c}}_{p} = \left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{1}{3}} & 0\\ 0 & e^{2\pi i\frac{2}{3}}\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{2}{3}} & 0\\ 0 & e^{2\pi i\frac{1}{3}}\end{bmatrix}\right\}.$$

8.1 Finding All Infinite Symmetries

Here we will give a method of how to find all infinite groups $G^{\mathbf{c}_j}_{k}, j = 1, ..., r$ of stability matrices of $I \subset k[x_1, ..., x_n]$. We will represent these groups by a matrix $A \in \mathbb{Z}^{r\times n}$, where the j-th row of A corresponds to $\mathbf{c}^T_j$ of $G^{\mathbf{c}_j}_{k}$ for $j = 1, ..., r$ (such a notation for A was used in [8]). We will use Theorem 6.1. To find all groups $G^{\mathbf{c}_j}_{k}$ of stability matrices of I, we should find all $\mathbf{c} \in \mathbb{Z}^n$ such that all polynomials in a reduced Groebner basis of I are $\mathbf{c}$-weighted homogeneous. We give the following Method 8.1.

Method 8.1. *Suppose a reduced Groebner basis of $I \subset k[x_1, ..., x_n]$:*

$$f_1(\mathbf{x}) = \sum_{j=1}^{s_1} a_{1j}\mathbf{x}^{\boldsymbol{\alpha}_{1j}}, \quad ..., \quad f_m(\mathbf{x}) = \sum_{j=1}^{s_m} a_{mj}\mathbf{x}^{\boldsymbol{\alpha}_{mj}}, \quad F = \Big\{f_1, ..., f_m\Big\}.$$

A **c***-weighted homogenity of f_j for $j = 1, ..., m$ means*

$$\mathbf{c}^T\boldsymbol{\alpha}_{11} = \mathbf{c}^T\boldsymbol{\alpha}_{12} = ... = \mathbf{c}^T\boldsymbol{\alpha}_{1s_1}, \quad ..., \quad \mathbf{c}^T\boldsymbol{\alpha}_{m1} = \mathbf{c}^T\boldsymbol{\alpha}_{m2} = ... = \mathbf{c}^T\boldsymbol{\alpha}_{ms_m}.$$

We can equivalently rewrite these equations as

$$\mathbf{c}^T\Big(\boldsymbol{\alpha}_{12} - \boldsymbol{\alpha}_{11}\Big) = \mathbf{c}^T\Big(\boldsymbol{\alpha}_{13} - \boldsymbol{\alpha}_{11}\Big) = ... = \mathbf{c}^T\Big(\boldsymbol{\alpha}_{1s_1} - \boldsymbol{\alpha}_{11}\Big) = \mathbf{c}^T\Big(\boldsymbol{\alpha}_{22} - \boldsymbol{\alpha}_{21}\Big) =$$

$$= ... = \mathbf{c}^T\Big(\boldsymbol{\alpha}_{2s_2} - \boldsymbol{\alpha}_{21}\Big) = ... = \mathbf{c}^T\Big(\boldsymbol{\alpha}_{ms_m} - \boldsymbol{\alpha}_{m1}\Big) = 0.$$

Or writing it in a matrix form gives

$$\mathbf{c}^T \underbrace{\begin{bmatrix}\boldsymbol{\alpha}_{12} - \boldsymbol{\alpha}_{11} & \boldsymbol{\alpha}_{13} - \boldsymbol{\alpha}_{11} & ... & \boldsymbol{\alpha}_{ms_m} - \boldsymbol{\alpha}_{m1}\end{bmatrix}}_{K_F} = \mathbf{0}^T.$$

$$\mathbf{c}^T K_F = \mathbf{0}^T.$$

The task of finding all **c***, for which polynomials $f_1, .., f_m$ are* **c***-weighted homogeneous, can be reformulated as finding a basis $C \subset \mathbb{Z}^n$ for the integer lattice of the left kernel of K_F. Then, every* **c** *satisfying the required property can be written as an integer combintation of vectors from C. Of course if K_F has full row rank over $\mathbb{Z}$, then C contains only zero vector. That's why we suppose that K_F hasn't full row rank over $\mathbb{Z}$. We can find a basis C using a row Hermite multiplier U of K_F:*

$$UK_F = H,$$

where the last r rows of H are zero. Then, by Proposition 7.3, the last r rows of U form a basis for the left kernel of K_F over $\mathbb{Z}$. And we let A be the last r rows of U.

We give the following Remark 8.1.

Remark 8.1. *An ideal I is stable under groups $G_k^{\mathbf{c}_j}$, $j = 1, ..., r$ if and only if I is stable under a group*

$$G_k^A = \Big\{M_1M_2 \;\mid\; M_1 \in G_k^{\mathbf{c}_{j_1}}, M_2 \in G_k^{\mathbf{c}_{j_2}}, \quad j_1, j_2 \in \Big\{1, ..., r\Big\}\Big\},$$

where $A = \begin{bmatrix}\mathbf{c}_1 & ... & \mathbf{c}_r\end{bmatrix}^T$.

That's why, instead of saying that an ideal I is stable under every group $G_k^{\mathbf{c}_j}$, $j = 1, ..., r$, where $\mathbf{c}_j^T$ is a row of A, we will just say that I is stable under G_k^A.

8.2 Finding All Finite Symmetries

Here we will give a method of how to find all finite groups $G_{p_j}^{\mathbf{c}_j}, j = 1, ..., r$ of stability matrices of $I \subset \mathbb{C}[x_1, ..., x_n]$. We will represent these groups by two matrices $B \in \mathbb{Z}^{r\times n}$ and $P = \operatorname{diag}(p_j) \in \mathbb{Z}^{r\times r}$, where the j-th row of B corresponds to $\mathbf{c}_j$ of $G_{p_j}^{\mathbf{c}_j}$ for $j = 1, ..., r$ (such a notation for B and P was used in [7]). We will use Theorem 6.2. To find all groups $G_{p_j}^{\mathbf{c}_j}$ of stability matrices of I, we should find all such $\mathbf{c} \in \mathbb{Z}^n$ and $p \in \mathbb{N}, p > 1$ that all polynomials in a reduced Groebner basis of I are $\mathbf{c}$-weighted p-homogeneous. We give the following Method 8.2.

Method 8.2. *Suppose a reduced Groebner basis of $I \subset \mathbb{C}[x_1, ..., x_n]$:*

$$f_1(\mathbf{x}) = \sum_{j=1}^{s_1} a_{1j}\mathbf{x}^{\boldsymbol{\alpha}_{1j}}, \quad ..., \quad f_m(\mathbf{x}) = \sum_{j=1}^{s_m} a_{mj}\mathbf{x}^{\boldsymbol{\alpha}_{mj}}, \quad F = \Big\{f_1, ..., f_m\Big\}.$$

Performing the same steps as in Method 8.1, we get a modular matrix equation

$$\mathbf{c}^T K_F \equiv \mathbf{0}^T \bmod p \tag{8.1}$$

Analogically as in [7, p. 20, paragraph 5], we assume that K_F has full row rank because not full row rank case was already described in Method 8.1. Let U and V be the unimodular multipliers such that

$$UK_FV = S$$

is in Smith normal form. Suppose that last r elements on the diagonal in S are > 1. We let B be the last r rows of U, and P be a diagonal matrix of the last r elements on the diagonal in S.

We give the following Remark 8.2.

Remark 8.2. *An ideal I is stable under groups $G_{p_j}^{\mathbf{c}_j}$, $j = 1, ..., r$ if and only if I is stable under a group*

$$G_P^B = \Big\{M_1M_2 \;\mid\; M_1 \in G_{p_{j_1}}^{\mathbf{c}_{j_1}}, M_2 \in G_{p_{j_2}}^{\mathbf{c}_{j_2}}, \quad j_1, j_2 \in \Big\{1, ..., r\Big\}\Big\},$$

where $B = \begin{bmatrix}\mathbf{c}_1 & ... & \mathbf{c}_r\end{bmatrix}^T$ and $P = \operatorname{diag}(p_1, ..., p_r)$.

That's why, instead of saying that an ideal I is stable under every group $G_{p_j}^{\mathbf{c}_j}, j = 1, ..., r$, where $\mathbf{c}_j^T$ is a row of B and p_j is a diagonal element of P, we will just say that I is stable under G_P^B.

Example 8.3. *Suppose that we obtained by Method 8.2 the following matrices*

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

Then making all possible products of matrices from $G_2^{\begin{bmatrix}0 & 1\end{bmatrix}^T}$ *and* $G_3^{\begin{bmatrix}1 & 1\end{bmatrix}^T}$ *we obtain the following group*

$$G_P^B = \left\{ \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{1}{3}} & 0\\0 & e^{2\pi i\frac{1}{3}}\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{2}{3}} & 0\\0 & e^{2\pi i\frac{2}{3}}\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{1}{3}} & 0\\0 & -e^{2\pi i\frac{1}{3}}\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{2}{3}} & 0\\0 & -e^{2\pi i\frac{2}{3}}\end{bmatrix} \right\}$$

of all diagonal stability matrices of I. We can notice that

$$G_P^B \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \cong G_6^{\begin{bmatrix}4 & 1\end{bmatrix}^T}.$$

Notice that in Example 8.1 (resp. 8.2) we didn't suppose a reduced Groebner basis of I, and that's why the method we used was incomplete (there could exist a group $G_k^{\mathbf{c}}$ (resp. $G_p^{\mathbf{c}}$), which it didn't find). We give the following Example 8.4, which shows that performing Method 8.2 on a basis of I (which is not a reduced Groebner basis) may not find finite symmetries, while they exist.

Example 8.4. *Suppose an ideal*

$$I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x,y], \quad f_1 = x^3 + x^2 - y - 1, f_2 = x^2 - y, F = \Big\{f_1, f_2\Big\}.$$

We note that F is not a reduced Groebner basis of I. Constructing matrix K_F we obtain

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

Smith normal of K_F is

$$S = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\end{bmatrix}.$$

But this doesn't mean that I has no finite symmetries. A reduced Groebner basis of I (using the grevlex monomial ordering for variable ordering $x > y$) is

$$I = \langle h_1, h_2, h_3 \rangle, \quad h_1 = y^2 - x, h_2 = xy - 1, h_3 = x^2 - y, H = \Big\{h_1, h_2, h_3\Big\}.$$

Constructing matrix K_H we obtain

$$K_H = \begin{bmatrix}1 & -1 & -2\\-2 & -1 & 1\end{bmatrix}.$$

Smith normal form of K_H is

$$\underbrace{\begin{bmatrix}1 & 0\\-1 & 1\end{bmatrix}}_{U}\underbrace{\begin{bmatrix}1 & -1 & -2\\-2 & -1 & 1\end{bmatrix}}_{K_H}\underbrace{\begin{bmatrix}0 & -1 & 1\\-1 & -1 & -1\\0 & 0 & 1\end{bmatrix}}_{V} = \underbrace{\begin{bmatrix}1 & 0 & 0\\0 & 3 & 0\end{bmatrix}}_{S}.$$

Then all finite symmetries of I we can describe by

$$B = \begin{bmatrix}-1 & 1\end{bmatrix}, \quad P = \begin{bmatrix}3\end{bmatrix}.$$

This gives us the finite group of all finite symmetries of I:

$$G_p^{\mathbf{c}} = \left\{ \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{1}{3}} & 0\\0 & e^{2\pi i\frac{2}{3}}\end{bmatrix}, \begin{bmatrix}e^{2\pi i\frac{2}{3}} & 0\\0 & e^{2\pi i\frac{1}{3}}\end{bmatrix} \right\}.$$

The main result of this section is that computing a matrix K_F of exponents differences of a reduced Groebner basis F of I can give us more symmetries than computing it from some another basis of I. However, the authors of [8] and [7] didn't use a reduced Groebner basis for finding symmetries. And we want to show that in [7, Example 3.5] there are more symmetries than the authors found.

Example 8.5. *Consider an ideal*

$$I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{C}[z_1, z_2, z_3],$$

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

The authors found only the symmetries

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

But we can compute a reduced Groebner basis of I with respect to the grevlex monomial ordering for variable ordering $z_1 > z_2 > z_3$:

$$I = \langle h_1, h_2, h_3, h_4 \rangle, \quad h_1 = z_3 - 1, h_2 = z_1z_2 + 4, h_3 = z_1^3 + z_2^3, h_4 = z_2^4 - 4z_1^2.$$

Then all finite symmetries are:

$$B = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix}, \quad P = \begin{bmatrix} 6 \end{bmatrix}.$$

9 Finding all stability matrices

In this section we give an algorithm of how to find all stability matrices of a given ideal I. At first we need the following Lemma 9.1. It shows that for any ideal $I \subset k[x_1, ..., x_n]$ two operators $\mod I$ and ψ (an evaluation on variables $y_1, ..., y_t$) are commutative on the ring $k[y_1, ..., y_t, x_1, ..., x_n]$ with respect to the operation of function composition.

Lemma 9.1. *Suppose an ideal $I \subset k[x_1, ..., x_n] \subset k[y_1, ..., y_t, x_1, ..., x_n]$. Also suppose an evaluation function*

$$\psi : k[y_1, ..., y_t, x_1, ..., x_n] \to k[x_1, ..., x_n]$$

$$f(y_1, ..., y_t, x_1, ..., x_n) \mapsto f(\alpha_1, ..., \alpha_t, x_1, ..., x_n),$$

where $\alpha_i \in k \ \ \forall i = 1, ..., t$. So ψ is an evaluation on variables $y_1, ..., y_t$. Then we have

$$\psi(f \mod I) = \psi(f) \mod I, \quad \forall f \in k[y_1, ..., y_t, x_1, ..., x_n].$$

Proof. Take any $f \in k[y_1, ..., y_t, x_1, ..., x_n]$. Let's denote

$$r_1 = \psi(f) \mod I, \quad r_2 = \psi(f \mod I).$$

It's obvious that r_1 and r_2 are from $k[x_1, ..., x_n]$. Suppose some Groebner basis $\Big\{g_j(x_1, ..., x_n)\Big\}_{j=1}^{m}$ of I. Then for r_1 there holds true

$$f(\alpha_1, ..., \alpha_t, x_1, ..., x_n) = \sum_{j=1}^{m} a_j(x_1, ..., x_n) \cdot g_j(x_1, ..., x_n) + r_1(x_1, ..., x_n) \tag{9.1}$$

For r_2 there holds true

$$f(y_1, ..., y_t, x_1, ..., x_n) = \sum_{j=1}^{m} b_j(y_1, ..., y_t, x_1, ..., x_n) \cdot g_j(x_1, ..., x_n) + R_2(y_1, ..., y_t, x_1, ..., x_n) \tag{9.2}$$

Applying ψ on both sides of (9.2) we obtain:

$$f(\alpha_1, ..., \alpha_t, x_1, ..., x_n) = \sum_{j=1}^{m} b_i(\alpha_1, ..., \alpha_t, x_1, ..., x_n) \cdot g_j(x_1, ..., x_n) + R_2(\alpha_1, ..., \alpha_t, x_1, ..., x_n),$$

$$r_2(x_1, ..., x_n) = R_2(\alpha_1, ..., \alpha_t, x_1, ..., x_n).$$

We conclude that $r_1 - r_2 \in I$, because

$$f(\alpha_1, ..., \alpha_t, x_1, ..., x_n) - f(\alpha_1, ..., \alpha_t, x_1, ..., x_n) =$$

$$= \sum_{j=1}^{m} \Big(a_j(x_1, ..., x_n) - b_j(\alpha_1, ..., \alpha_t, x_1, ..., x_n) \Big) \cdot g_j(x_1, ..., x_n) + \Big(r_1(x_1, ..., x_n) - r_2(x_1, ..., x_n) \Big) = 0.$$

To get a contradiction suppose $r_1 \neq r_2$ or that $r_1 - r_2 \neq 0$. Because $r_1 - r_2 \in I$, then $\mathrm{LT}(r_1 - r_2) \in \langle \mathrm{LT}(I) \rangle$. From the properties of the division algorithm it follows from (9.1) that

$$\mathrm{LT}(r_1) \notin \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

By the same reasoning it follows from (9.2) that none of monomials of $R_2(y_1, ..., y_t, x_1, ..., x_n)$ lies in $\langle \mathrm{LT}(I) \rangle$. It means that $\mathrm{LT}(r_2) \notin \langle \mathrm{LT}(I) \rangle$. This then means that $\mathrm{LT}(r_1 - r_2) \notin \langle \mathrm{LT}(I) \rangle$. It is a contradiction. Then $r_1 = r_2$ and we have the proof.

□

Now we are ready to give the following Theorem 9.1, which gives us an algorithm for finding all stability matrices of an ideal I.

Theorem 9.1. *Suppose an ideal $I = \langle f_1, ..., f_m \rangle \subset k[x_1, ..., x_n]$. Suppose also two $n \times n$ matrices: $\mathbf{S}$ with indeterminate elements $s_{11}, ..., s_{nn}$ and $\mathbf{A} \in k^{n \times n}$ with elements $a_{11}, ..., a_{nn}$ from k. Let*

$$r_j(s_{11}, ..., s_{nn}, x_1, ..., x_n) = f_j(\mathbf{Sx}) \bmod I, \quad j = 1, ..., m.$$

Then I is stable under $\mathbf{A}$ if and only if $r_j(a_{11}, ..., a_{nn}, x_1, ..., x_n) \in k[x_1, ..., x_n]$ is the zero polynomial for each $j = 1, ..., m$.

Proof. We see that $r_j \in k[s_{11}, ..., s_{nn}, x_1, ..., x_n]$, $j = 1, ..., m$. By Lemma 9.1 we have that

$$r_j(a_{11}, ..., a_{nn}, x_1, ..., x_n) = f_j(\mathbf{Ax}) \bmod I, \quad j = 1, ..., m.$$

Then by Lemma 4.2 we obtain the desired, because $f_j(\mathbf{Ax}) \in I$ if and only if $f_j(\mathbf{Ax}) \bmod I$ is the zero polynomial.

□

Definition 9.1. *We will say that a polynomial $f \in k[s_{11}, ..., s_{nn}, x_1, ..., x_n]$ is written in* **x***-monomial disjoint way if*

$$f = \sum_{j=1}^{q} h_j(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\alpha}_j},$$

where $h_j(s_{11}, ..., s_{nn}) \in k[s_{11}, ..., s_{nn}]$ and there don't exist $j_1 \neq j_2$ such that $\boldsymbol{\alpha}_{j_1} = \boldsymbol{\alpha}_{j_2}$.

Corollary 4. *Let each $r_j(s_{11}, ..., s_{nn}, x_1, ..., x_n)$ is written in* **x***-monomial disjoint way*

$$r_j(s_{11}, ..., s_{nn}, x_1, ..., x_n) = \sum_{i=1}^{q_j} h_{ji}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\beta}_{ji}}.$$

Then from definition of the zero polynomial it follows that $r_j(a_{11}, ..., a_{nn}, x_1, ..., x_n)$, $j = 1, ..., m$ are the zero polynomials if and only if

$$h_{ji}(a_{11}, ..., a_{nn}) = 0, \quad \forall j = 1, ..., m \quad \forall i = 1, ..., q_j.$$

Then to find all stability matrices all we need is just to solve a system of equations $h_{ji}(s_{11}, ..., s_{nn})$.

Remark 9.1. *Notice that Theorem 9.1 makes no restriction on invertibility of $\mathbf{A}$. Then solving system of equations h_{ji} can give us also non-invertible matrices $\mathbf{A}$. If we want only invertible, we can use an extra dimension and add another one equation*

$$h = w \cdot \det \mathbf{S} + 1,$$

where w is a new variable.

We will denote the ideal generated by equations $h_{ji}(s_{11}, ..., s_{nn})$ as

$$H_F = \left\langle \left\{ h_{ji} \right\} \right\rangle, \quad j = 1, ..., m, i = 1, ..., q_j,$$

where $F = \left\{ f_1, ..., f_m \right\}$ is a chosen basis of I to compute remainders r_j. It is obvious that $H_F \subset k[s_{11}, ..., s_{nn}]$. We will call H_F a ***matrix F-ideal of stability of I***. Now, we give an example of how to compute all stability matrices of a given ideal I.

Example 9.1. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x, y]$, where*

$$f_1(x, y) = x^3 - 1, \quad f_2(x, y) = xy - 1, \quad F = \left\{ f_1, f_2 \right\}.$$

Then we make polynomials:

$$f_1(\mathbf{Sx}) = s_{11}^3 x^3 + 3s_{11}^2 s_{12} x^2 y + 3s_{11} s_{12}^2 x y^2 + s_{12}^3 y^3 - 1,$$

$$f_2(\mathbf{Sx}) = s_{11} s_{21} x^2 + s_{11} s_{22} xy + s_{12} s_{21} xy + s_{12} s_{22} y^2 - 1.$$

Now compute the remainders of $f_1(\mathbf{Sx})$ and $f_2(\mathbf{Sx})$ modulo I

$$r_1 = f_1(\mathbf{Sx}) \bmod I = 3s_{11}^2 s_{12} x + 3s_{11} s_{12}^2 y + s_{11}^3 + s_{12}^3 - 1,$$

$$r_2 = f_2(\mathbf{Sx}) \bmod I = s_{12} s_{22} x + s_{11} s_{21} y + s_{11} s_{22} + s_{12} s_{21} - 1.$$

Extracting polynomials h_{ji} from r_1 and r_2 we obtain:

$$h_{11} = 3s_{11}^2 s_{12}, \quad h_{12} = 3s_{11} s_{12}^2, \quad h_{13} = s_{11}^3 + s_{12}^3 - 1,$$

$$h_{21} = s_{12} s_{22}, \quad h_{22} = s_{11} s_{21}, \quad h_{23} = s_{11} s_{22} + s_{12} s_{21} - 1.$$

Matrix F-ideal of stability of I is

$$H_F = \left\langle h_{11}, h_{12}, h_{13}, h_{21}, h_{22}, h_{23} \right\rangle.$$

The variety $\mathbf{V}(H_F)$ contains 6 solutions. We write them as a group G_I of 6 matrices:

$$G_I = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{2}{3}} \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{2}{3}} & 0 \\ 0 & e^{2\pi i \frac{1}{3}} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & e^{2\pi i \frac{1}{3}} \\ e^{2\pi i \frac{2}{3}} & 0 \end{bmatrix}, \begin{bmatrix} 0 & e^{2\pi i \frac{2}{3}} \\ e^{2\pi i \frac{1}{3}} & 0 \end{bmatrix} \right\}.$$

It is obvious by Theorem 9.1 that $\mathbf{V}(H_{F_1}) = \mathbf{V}(H_{F_2})$ for two different sets F_1 and F_2 of generators of I, because the set of all stability matrices of I is uniquely determined. But we can say even more: an ideal H_F doesn't depend on the choice of the set F of generators of I.

Lemma 9.2. *Suppose an ideal $I \subset k[x_1, ..., x_n]$. Let $F = \Big\{f_1, ..., f_m\Big\}$ and $G = \Big\{g_1, ..., g_r\Big\}$ be two different set of generators of I. Let H_F be a matrix F-stability ideal of I and H_G be a matrix G-stability ideal of I. Then $H_F = H_G$.*

Proof. 1) $H_F \supset H_G$. Let the remainders of $f_1, ..., f_m$ modulo I be written in an $\mathbf{x}$-monomial disjoint way:

$$\overline{f_i(\mathbf{Sx})}^I = \sum_{t=1}^{q_i} h_{it}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\alpha}_{it}}.$$

Then

$$H_F = \langle h_{it} \rangle, \quad i = 1, ..., m, t = 1, ..., q_i.$$

Because $f_1, ..., f_m$ are the generators of I then there exist $z_{ij} \subset k[x_1, ..., x_n]$ such that

$$g_j(\mathbf{x}) = \sum_{i=1}^{m} z_{ij}(\mathbf{x}) \cdot f_i(\mathbf{x}) \Rightarrow g_j(\mathbf{Sx}) = \sum_{i=1}^{m} z_{ij}(\mathbf{Sx}) \cdot f_i(\mathbf{Sx}), \quad \forall j = 1, ..., r.$$

Then $\forall j = 1, ..., r$ there exists $a_j(\mathbf{x}) \in I$ such that

$$\overline{g_j(\mathbf{Sx})}^I = \sum_{i=1}^{m} \overline{z_{ij}(\mathbf{Sx})}^I \cdot \overline{f_i(\mathbf{Sx})}^I + a_j(\mathbf{x}).$$

Then $\forall i = 1, ..., m$, $\forall j = 1, ..., r$ we write $\overline{z_{ij}(\mathbf{Sx})}^I \cdot \overline{f_i(\mathbf{Sx})}^I$ in $\mathbf{x}$-monomial disjoint way:

$$\overline{z_{ij}(\mathbf{Sx})}^I \cdot \overline{f_i(\mathbf{Sx})}^I = \sum_{t=1}^{c_{ij}} p_{ijt}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\beta}_{ijt}}.$$

It is obvious that p_{ijt} is a polynomial combination of $h_{i1}, ..., h_{iq_i}$. Let's now write $g_j(\mathbf{Sx})$ in the following way:

$$\overline{g_j(\mathbf{Sx})}^I = \sum_{i=1}^{m} \overline{z_{ij}(\mathbf{Sx})}^I \cdot \overline{f_i(\mathbf{Sx})}^I + a_j(\mathbf{x}) = \sum_{s=1}^{w_j} v_{sj}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\beta}_{sj}} + a_j(\mathbf{x}) \tag{9.3}$$

where $\sum_{s=1}^{w_j} v_{sj}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\beta}_{sj}}$ is written in $\mathbf{x}$-monomial disjoint way. We clearly see that v_{sj} is a linear combination of p_{ijt}. Then, applying mod I on Equation (9.3), we obtain

$$\overline{g_j(\mathbf{Sx})}^I = \overline{\overline{g_j(\mathbf{Sx})}^I}^I = \sum_{s=1}^{w_j} \overline{v_{sj}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\beta}_{sj}}}^I + \underbrace{\overline{a_j(\mathbf{x})}^I}_{=0} =$$

$$= \sum_{s=1}^{w_j} \overline{v_{sj}(s_{11}, ..., s_{nn})}^I \cdot \overline{\mathbf{x}^{\boldsymbol{\beta}_{sj}}}^I + b_j(\mathbf{x}) = \sum_{s=1}^{w_j} v_{sj}(s_{11}, ..., s_{nn}) \cdot \overline{\mathbf{x}^{\boldsymbol{\beta}_{sj}}}^I + b_j(\mathbf{x})$$

for some $b_j(\mathbf{x}) \in I$. Writing $\sum_{s=1}^{w_j} v_{sj}(s_{11}, ..., s_{nn}) \cdot \overline{\mathbf{x}^{\boldsymbol{\beta}_{sj}}}^{I}$ in an $\mathbf{x}$-monomial disjoint way we obtain

$$\overline{g_j(\mathbf{Sx})}^{I} = \overline{\overline{g_j(\mathbf{Sx})}}^{I} = \sum_{\zeta=1}^{c_j} u_{\zeta j}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\gamma}_{\zeta j}} + b_j(\mathbf{x}) \tag{9.4}$$

where $\mathbf{x}^{\boldsymbol{\gamma}_{sj}} \notin \langle \mathrm{LT}(I) \rangle$ and $u_{\zeta j}$ is a linear combination of v_{sj}. Applying $\mod I$ on Equation (9.4) we obtain

$$\overline{g_j(\mathbf{Sx})}^{I} = \overline{\overline{\overline{g_j(\mathbf{Sx})}}^{I}}^{I} = \sum_{\zeta=1}^{c_j} \overline{u_{\zeta j}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\gamma}_{\zeta j}}}^{I} + \underbrace{\overline{b_j(\mathbf{x})}^{I}}_{=0} = \sum_{\zeta=1}^{c_j} u_{\zeta j}(s_{11}, ..., s_{nn}) \cdot \mathbf{x}^{\boldsymbol{\gamma}_{\zeta j}}.$$

Notice that

$$H_G = \langle u_{\zeta j} \rangle, \quad j = 1, ..., r, \zeta = 1, ..., c_j.$$

Becuase $u_{\zeta j}(s_{11}, ..., s_{nn})$ is a polynomial combination of $h_{i1}, ..., h_{iq_i}$ then we proved that $H_F \supset H_G$.

2) $H_F \subset H_G$. Can be proved by a similar way.

□

Now, because matrix F-stability ideal of I doesn't depend on the choice of generators of I, then we can call it just ***matrix ideal of stability of*** I and denote as H_I.

10 Invariant Theory and Reduction of a Polynomial System Using Scaling Symmetries

10.1 Invariant Theory

Invariant theory is a very beautiful topic of mathematics. It studies objects invariant under some group G. Invariance means that these objects don't change after performing an action of this group. We will consider here polynomial invariant theory, which means that objects are polynomials. Denote by $k[x_1, ..., x_n]^G$ the set of all polynomials invariant under G. It can be proved that $k[x_1, ..., x_n]^G$ is a subring of $k[x_1, ..., x_n]$. Polynomial invariant theory gives an answer on three main questions:

1) Is $k[x_1, ..., x_n]^G$ a finitely generated algebra over k? We can reformulate this as follows: do there exist polynomials $w_1, ..., w_m \in k[x_1, ..., x_n]^G$ such that every polynomial $f \in k[x_1, ..., x_n]^G$ we can write as a polynomial in $w_1, ..., w_m$ with coefficients in k?

2) If such generators $w_1, ..., w_m$ exist, then how can we find them?

3) When we have found $w_1, ..., w_m$, then how to rewrite every polynomial $f \in k[x_1, ..., x_n]^G$ as a polynomial in $w_1, ..., w_m$?

In [4, Chapter 7 (Invariant Theory of Finite Groups)] there is an answer to all these questions assuming G is a finite matrix group (and action of this group on f is just a linear change of variables of f).

Assuming G is a matrix group (not necessarily finite) we define that a polynomial (or, more generally, rational function) f is *invariant under* G if there holds

$$f(\mathbf{A}\mathbf{x}) = f(\mathbf{x})$$

true for any matrix $\mathbf{A} \in G$.

10.2 Generating Set of Invariants of Scaling Symmetries and The Rewriting Rules

We want to start with a notation for monomials. Let $\mathbf{x}$ be a column vector of variables $x_1, ..., x_n$ and $\mathbf{M} \in \mathbb{Z}^{n \times s}$ be an integer matrix. Then by $\mathbf{x}^{\mathbf{M}}$ we will denote a column vector of s elements $\mathbf{x}^{\mathbf{M}_{\cdot,1}}, ..., \mathbf{x}^{\mathbf{M}_{\cdot,s}}$, where $\mathbf{M}_{\cdot,j}$ is the j-th column of $\mathbf{M}$.

Example 10.1. *Suppose a matrix*

$$\mathbf{M} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Then

$$\mathbf{x}^{\mathbf{M}} = \begin{bmatrix} x_1 x_2^3 & x_1^2 x_2^4 \end{bmatrix}^T.$$

10.2.1 Infinite Symmetries

We are now moving from a polynomial ring $k[x_1, ..., x_n]$ to a field of rational functions $k(x_1, ..., x_n)$. The reason of this will be described in Section 10.3. We recall (Section 8.1) that infinite scaling symmetries are represented by an integer matrix A. We will say that $f \in k(x_1, ..., x_n)$ is invariant under A, if f is invariant under a group G_k^A. Here we will describe shortly how to find a generating set of rational invariants under A and how to rewrite any rational invariant in terms of $w_1, ..., w_m$ (the so-called "rewriting rules"), as it was done in [8]. Finding this generating set means to find such invariants $w_1, ..., w_m \in k(x_1, ..., x_n)$ under A that any invariant $f \in k(x_1, ..., x_n)$ under A can be written as a rational function in $w_1, ..., w_m$ with coefficients in k.

A generating set of invariants is usually not unique. Invariants obtained in [8] are actually Laurent monomials (usual monomials only involving fractions). For example, $\frac{xy^2}{z^2}$ is a Laurent monomial from $k(x, y, z)$. To see the proof of how this generating set can be obtained and how to rewrite any rational invariant as a rational function in terms of this generating set the reader is refered to [8, Theorem 4.2]. We only give a method here. By $\mathbf{w}$ we will denote a column vector of $w_1, ..., w_m$.

Method 10.1. *Consider a field $k(x_1, ..., x_n)$ of rational functions. Suppose a matrix $A \in \mathbb{Z}^{r \times n}$ of full row rank over $\mathbb{Z}$ which defines infinite scaling symmetries. Suppose also a unimodular matrix $V \in \mathbb{Z}^{n \times n}$ such that AV is in column Hermite normal form. Denote by $V_{\mathfrak{n}}$ a submatrix of the last $n - r$ columns of V. Then the columns of $V_{\mathfrak{n}} \in \mathbb{Z}^{n \times (n-r)}$ are the multidegrees of Laurent monomials which form a generating set $\mathbf{w} = \begin{bmatrix} w_1 & ... & w_{n-r} \end{bmatrix}^T$ of rational invariants under A (this fact partially follows from Proposition 7.1). Suppose $W = V^{-1} \in \mathbb{Z}^{n \times n}$. Denote by $W_{\mathfrak{d}} \in \mathbb{Z}^{(n-r) \times n}$ a submatrix of the last $n - r$ rows of W. Then the rewriting rules are*

$$\mathbf{x} = \begin{bmatrix} x_1 & ... & x_n \end{bmatrix}^T \to \mathbf{w}^{W_{\mathfrak{d}}}.$$

Example 10.2. *Consider a field $k(x_1, x_2, x_3, x_4)$ of rational functions. Suppose infinite symmetries given by*

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

A unimodular column Hermite multiplier V of A is

$$V = \begin{bmatrix} 1 & 0 & 0 & 1 \\ -2 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad AV = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad V_{\mathfrak{n}} = \begin{bmatrix} 0 & 1 \\ 0 & -2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then we clearly see that the columns of $V_{\mathfrak{n}}$ lie in the right kernel of A. We construct Laurent monomials from the columns of $V_{\mathfrak{n}}$ as $w_1 = x_3$, $w_2 = \frac{x_1 x_4}{x_2^2}$. Then we see that w_1 and w_2 are invariant under groups $G_k^{\mathbf{a}_1}$ and $G_k^{\mathbf{a}_2}$, where $\mathbf{a}_1^T$ and $\mathbf{a}_2^T$ are rows of A. In addition, any rational invariant under A can be written as a rational function in w_1 and w_2. The inverse of V is

$$W = V^{-1} = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad W_{\mathfrak{d}} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then the rewriting rules are

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \end{bmatrix}^T \rightarrow \mathbf{w}^{W_{\mathfrak{d}}} = \begin{bmatrix} 1 & 1 & w_1 & w_2 \end{bmatrix}^T.$$

Suppose a rational invariant $f = \frac{x_1 x_3^2 x_4}{x_2^2} + \frac{x_2^4 x_3}{x_1^2 x_4^2}$ under A. Then we can rewrite it in terms of w_1 and w_2 as

$$f \rightarrow h = w_1^2 w_2 + \frac{w_1}{w_2^2}.$$

By Method 10.1 we can obtain different generating sets for a given A because unimodular column Hermite multiplier of A is not unique.

10.2.2 Finite Symmetries

10.2.2.1 Using Column Hermite Multiplier

Here we will also work with a field $k(x_1, ..., x_n)$ of rational functions. We recall (Section 8.2) that finite scaling symmetries are represented by matrices B and P. We will say that $f \in k(x_1, ..., x_n)$ is invariant under B and P, if f is invariant under a group G_P^B. Here we will describe shortly how to find a generating set $w_1, ..., w_m$ of rational invariants of scaling symmetries defined by B and P and how to rewrite any rational invariant as a rational function in $w_1, ..., w_m$ (as it was done in [7]). Invariants obtained in [7] are also Laurent monomials. To see the proof of how this generating set can be obtained and how to rewrite any rational invariant as a rational function in terms of this generating set the reader is refered to [7, Theorem 3.4]. We only give a method here.

Method 10.2. *Consider a field $k(x_1, ..., x_n)$ of rational functions. Suppose matrices $B \in \mathbb{Z}^{r \times n}$ and $P \in \mathbb{Z}^{r \times r}$ of full row rank over $\mathbb{Z}$ which define finite scaling symmetries. Suppose also a unimodular matrix $V \in \mathbb{Z}^{(n+r)\times(n+r)}$ such that $\begin{bmatrix} B & P \end{bmatrix} V$ is in column Hermite normal form. Denote by $V_{\mathfrak{n}}$ a submatrix of the first n elements of the last n columns of V. Then the columns of $V_{\mathfrak{n}}$ are the multidegrees of Laurent monomials which form a generating set of rational invariants under B and P. Suppose $W = V^{-1} \in \mathbb{Z}^{(n+r)\times(n+r)}$. Make a partition of W*

$$W = \begin{bmatrix} W_{\mathfrak{u}} & P_{\mathfrak{u}} \\ W_{\mathfrak{d}} & P_{\mathfrak{d}} \end{bmatrix}, \quad W_{\mathfrak{u}} \in \mathbb{Z}^{r \times n}, W_{\mathfrak{d}} \in \mathbb{Z}^{n \times n}, P_{\mathfrak{u}} \in \mathbb{Z}^{r \times r}, P_{\mathfrak{d}} \in \mathbb{Z}^{n \times r}.$$

Then the rewriting rules are

$$\mathbf{x} = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix}^T \rightarrow \mathbf{w}^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B}.$$

Example 10.3. *Consider a field $k(x, y)$ of rational functions. Suppose finite symmetries the same as in Example 8.4 given by*

$$B = \begin{bmatrix} 1 & 2 \end{bmatrix}, \quad P = \begin{bmatrix} 3 \end{bmatrix}.$$

A unimodular column Hermite multiplier V of $\begin{bmatrix} B & P \end{bmatrix}$ is

$$V = \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} B & P \end{bmatrix} V = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}, \quad V_{\mathfrak{n}} = \begin{bmatrix} -2 & -3 \\ 1 & 0 \end{bmatrix}.$$

Then we clearly see that the last 2 columns of V lie in the right kernel of $\begin{bmatrix} B & P \end{bmatrix}$. From the columns of $V_{\mathfrak{n}}$ we construct Laurent monomials $w_1 = \frac{y}{x^2}$, $w_2 = \frac{1}{x^3}$. Then we see that w_1 and w_2 are invariant under the finite group $G_p^{\mathbf{c}}$ with $\mathbf{c} = \begin{bmatrix} 1 & 2 \end{bmatrix}$ and $p = 3$. In addition, any rational invariant under B and P can be written as a rational function in w_1 and w_2. The inverse of V is

$$W = V^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad W_{\mathfrak{d}} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad P_{\mathfrak{d}} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Then the rewriting rules are

$$\begin{bmatrix} x & y \end{bmatrix}^T \to \mathbf{w}^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B} = \begin{bmatrix} \frac{1}{w_2^{1/3}} & \frac{w_1}{w_2^{2/3}} \end{bmatrix}^T.$$

Suppose a rational invariant $f = \frac{x^7 + y^3 x + y^2}{x^4 + y^2}$ under B and P. Then we can rewrite it in terms of w_1 and w_2 as

$$f \to h = \frac{\frac{1}{w_2^{7/3}} + \frac{w_1^3}{w_2^{4/3}} + \frac{w_1^2}{w_2^{4/3}}}{\frac{1}{w_2^{4/3}} + \frac{w_1^2}{w_2^{4/3}}} = \frac{\frac{1}{w_2} + w_1^3 + w_1^2}{1 + w_1^2} = \frac{w_1^3 w_2 + w_1^2 w_2 + 1}{w_2(1 + w_1^2)}.$$

By Method 10.2 we also can obtain different generating sets for given B and P because column Hermite multiplier of $\begin{bmatrix} B & P \end{bmatrix}$ is not unique.

It is also possible to compute with a Hermite multiplier of $\begin{bmatrix} B & -P \end{bmatrix}$ (which was used in [7]). We want to note that there is a typo in [7]. The rewriting rules using Hermite multiplier of $\begin{bmatrix} B & -P \end{bmatrix}$ should be

$$\mathbf{x} \to \mathbf{w}^{W_{\mathfrak{d}} + P_{\mathfrak{d}} P^{-1} B},$$

but in [7] was written

$$\mathbf{x} \to \mathbf{w}^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B},$$

which is for Hermite multiplier of $\begin{bmatrix} B & P \end{bmatrix}$. The reader can see how this typo firstly occurred in the proof of [7, Lemma 2.6]. But all the results in [7] are correct.

10.2.2.2 Using Reynolds Operator

Here we will work with a polynomial ring $k[x_1, ..., x_n]$. Suppose a finite matrix group G acting on a polynomial as a linear change of variables. Then the Reynolds Operator $R_G \colon k[x_1, ..., x_n] \to k[x_1, ..., x_n]$ is defined as

$$R_G(f)(\mathbf{x}) = \frac{1}{|G|} \sum_{\mathbf{A} \in G} f(\mathbf{A}\mathbf{x}).$$

If $f \in k[x_1, ..., x_n]$, then $R_G(f) \in k[x_1, ..., x_n]^G$. We can use the Reynolds Operator for finding a generating set $w_1, ..., w_m$ of the ring of invariants $k[x_1, ..., x_n]^G$, which means that every polynomial $f \in k[x_1, ..., x_n]$ we can rewrite as a polynomial in $w_1, .., w_m$ with coefficients in k. We refer to [4, Chapter 7, §3, Theorem 5], which tells us how to find a generating set. Also [4, Chapter 7, §3, Proposition 7] describes how to rewrite any invariant polynomial as a polynomial in these generators.

Example 10.4. *Consider a polynomial ring $k[x, y]$. Also suppose a finite matrix group as in Example 10.3*

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{1}{3}} & 0 \\ 0 & e^{2\pi i \frac{2}{3}} \end{bmatrix}, \begin{bmatrix} e^{2\pi i \frac{2}{3}} & 0 \\ 0 & e^{2\pi i \frac{1}{3}} \end{bmatrix} \right\}.$$

We can use [4, Chapter 7, §3, Theorem 5] to compute a generating set of $k[x, y]^G$. It consists of 3 monomials xy, x^3, y^3 and then

$$f \in k[x, y]^G \iff f \in k[xy, x^3, y^3].$$

10.3 Reduction of a Polynomial System

This section presents our current (partial) understanding of polynomial systems reduction. And it is still ongoing work. We will work here only with scaling symmetries.

We cite [8, Section 5, paragraph 1]: “if the solution set of a polynomial system of equation is invariant under a group action, then there is an equivalent system given in terms of invariants of this group action. The equivalent system written in terms of a generating set of invariants is the reduced system. However, for general symmetry reductions a futher problem is to recover the solutions of the original system from the solutions of the reduced system”.

We want to note that by a notion of “invariant set under a group” mathematicians usually mean our Definition 5.4 (which is for specific set $V \subset k^n$ and group $G \subset \mathrm{GL}_n(k)$). And a notion of stability in mathematical world means something different. That’s why, when in [8] the authors talk about an invariant solution set under a group G, we will understand it (according to our Definition 5.4) as a stable solution set under the same group G.

If a variety $\mathbf{V}(I) \subset k^n$ (resp. $\mathbf{V}(I) \subset \mathbb{C}^n$) has a group of stability matrices $G_k^{\mathbf{c}}$ (resp. $G_p^{\mathbf{c}}$), then we will say that $\mathbf{V}(I)$ has infinite (resp. finite) symmetries. To see how to construct the solutions of the original system from its reduced form the reader is refered to [8, Theorem 5.3] and [7, Theorem 5.5]. Here we will only describe how to obtain a reduced system.

10.3.1 Reduction of Infinite Symmetries

To understand in more details the reduction of infinite symmetries the reader is refered to [8, Proposition 5.2 and Theorem 5.3]. We only show some examples here.

Suppose a system P of polynomials $p_j(\mathbf{x}) = 0$, $j = 1, ..., q$. Polynomials p_j generate an ideal $I \subset k[x_1, ..., x_n]$. Our aim is to find all infinite symmetries of $\mathbf{V}(I)$. In [8, p. 7, paragraph after Definition 5.1] the authors wrote that "Appendix A provides a way of determining *some* of these symmetries". We, however, give a method of how to determine *all* infinite symmetries of $\mathbf{V}(I)$. We give the following Lemma 10.1.

Lemma 10.1. *Suppose an ideal $I \subset k[x_1, ..., x_n]$. Then its variety $\mathbf{V}(I)$ is stable under $G_k^{\mathbf{c}}$ if and only if a reduced Groebner basis of $\mathbf{I}(\mathbf{V}(I))$ (with respect to any monomial ordering) consists of $\mathbf{c}$-weighted homogeneous polynomials.*

Proof. The proof can be easily obtained from Lemma 5.3 ($(i) \iff (ii)$) and Theorem 6.1. □

Then applying Method 8.1 on a reduced Groebner basis of $\mathbf{I}(\mathbf{V}(I))$ gives us all infinite symmetries of $\mathbf{V}(I)$. These symmetries we represent by a matrix A. After obtaining these symmetries we want to find an equivalent system (possibly not of polynomials, but rational functions, we will see later) given in terms of invariants under A.

Suppose a reduced Groebner basis $GB = \left\{g_j(\mathbf{x})\right\}_{j=1}^{m}$ of $\mathbf{I}(\mathbf{V}(I))$ from which A was obtained. Then GB is an equivalent polynomial system to a polynomial system P, because $\mathbf{V}(\mathbf{I}(\mathbf{V}(I))) = \mathbf{V}(I)$. There can happen two cases.

Case 10.1. *All polynomials in GB are invariant under A, which means that $A\boldsymbol{\alpha} = \mathbf{0}$ for every monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ from GB.*

Case 10.2. *There exists a polynomial g_t in GB which is not invariant under A, which means that $A\boldsymbol{\alpha}_i = A\boldsymbol{\alpha}_j \neq \mathbf{0}$ for every two monomials $\mathbf{x}^{\boldsymbol{\alpha}_i}$ and $\mathbf{x}^{\boldsymbol{\alpha}_j}$ in g_t. The equality $A\boldsymbol{\alpha}_i = A\boldsymbol{\alpha}_j$ holds true because g_t is $\mathbf{c}$-weighted homogeneous for every row $\mathbf{c}$ of A. Then to obtain a rational invariant under A from g_t we just divide g_t by its some (for example, last) monomial. We will do this for every polynomial in GB which is not invariant under A. To be able to do such dividing, we suppose that variables in the dividing monomials cannot be zero. That's why we obtain an equivalent system to the original one, where we discount all the solutions for which there is a zero component in variables involving the division.*

After obtaining an equivalent (or almost equivalent as in Case 10.2) system of invariants under A (call it F) we can rewrite these invariants as rational functions in terms of a generating set (obtained by Method 10.1) and obtain a new reduced system of equations (call it H) in new variables. After obtaining the solutions of H we need somehow to construct from them the solutions of F. (We think that we can recover only the solutions of F which don't have a zero component in a variable which lies in a denominator of some Laurent monomial from generating set.)

The authors in [8, Proposition 5.2 and Theorem 5.3] (possibly, for simplification) just discount `all` the solutions of the original system for which there is a zero component and say that every of the rest solutions of the original system can be obtained from the solutions of H.

We give the following Example 10.5 taken from [8, Example 5.4].

Example 10.5. *Consider an ideal*

$$I = \langle g_1, g_2 \rangle \subset \mathbb{Q}[z_1, z_2, z_3, z_4], \quad g_1 = z_2 z_4^2 - z_1, \quad g_2 = z_1 z_3 - z_2.$$

This ideal is radical and g_1, g_2 is already a reduced Groebner basis of I. All infinite symmetries of $\mathbf{V}(I)$ (obtained by Method 8.1) are given by matrix

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

We see that we are dealing with the Case 10.2, because g_1 and g_2 are not invariant under A. Then we make from them the following rational invariants under A:

$$f_1 = \frac{z_2 z_4^2}{z_1} - 1, \quad f_2 = \frac{z_1 z_3}{z_2} - 1.$$

A unimodular column Hermite multiplier V for A (obtained in [8]) is

$$V = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}, V_{\mathfrak{n}} = \begin{bmatrix} 1 & -1 \\ -1 & 1 \\ 1 & 0 \\ 0 & 2 \end{bmatrix}, \quad W = V^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{bmatrix}.$$

Then a generating set of invariants is formed by monomials $w_1 = \frac{z_1 z_3}{z_2}$ and $w_2 = \frac{z_2 z_4^2}{z_1}$. The rewriting rules are

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 \end{bmatrix}^T \rightarrow \mathbf{w}^{W_{\mathfrak{d}}} = \begin{bmatrix} 1 & \frac{1}{w_2} & \frac{w_1}{w_2} & w_2 \end{bmatrix}.$$

Then we rewrite f_1 and f_2 in terms of a generating set as

$$f_1 \rightarrow h_1 = \frac{1}{w_2} w_2^2 - 1 = w_2 - 1, \quad f_2 \rightarrow h_2 = \frac{\frac{w_1}{w_2}}{\frac{1}{w_2}} - 1 = w_1 - 1.$$

Obtained system of h_1 and h_2 is the reduced system.

As the last thing, we want to note that reduction of infinite symmetries is closely connected to dimensional analysis and the Buckingham's π-Theorem (as was mentioned in [8, Section 4, paragraph 2]).

10.3.2 Reduction of Finite Symmetries

To understand in more details the reduction of finite symmetries the reader is refered to [8, Theorem 5.5]. We only show some examples here.

The steps here to obtain a reduced system are the same as in the case of reduction of finite symmetries. We give the following Lemma 10.2 for obtaining all finite symmetries of $\mathbf{V}(I)$.

Lemma 10.2. *Suppose an ideal $I \subset \mathbb{C}[x_1, ..., x_n]$. Then its variety $\mathbf{V}(I)$ is stable under $G_p^{\mathbf{c}}$ if and only if a reduced Groebner basis of $\mathbf{I}(\mathbf{V}(I))$ (with respect to any monomial ordering) consists of $\mathbf{c}$-weighted p-homogeneous polynomials.*

Proof. The proof can be easily obtained from Lemma 5.3 ($(i) \iff (ii)$) and Theorem 6.2. □

Then applying Method 8.2 on a reduced Groebner basis of $\mathbf{I}(\mathbf{V}(I))$ gives us all finite symmetries of $\mathbf{V}(I)$. These symmetries we represent by matrices B and P. We give the following Example 10.6.

Example 10.6. *Consider an ideal*

$$I = \langle g_1, g_2 \rangle \subset \mathbb{C}[x, y], \quad g_1 = x^3 - 1, \quad g_2 = xy - 1.$$

This ideal is a radical. Its reduced Groebner basis (with respect to the grevlex monomial ordering for variable ordering $x > y$) is

$$g_3 = y^2 - x, \quad g_4 = xy - 1, \quad g_5 = x^2 - y.$$

All finite symmetries of $\mathbf{V}(I)$ (obtained by Method 8.2) are given by matrices

$$B = \begin{bmatrix} -1 & 1 \end{bmatrix}, \quad P = \begin{bmatrix} 3 \end{bmatrix}.$$

Taking g_3, g_4, g_5 we see that we are dealing with the Case 10.2, because g_3 and g_5 are not invariant under B and P. Then we make from them the following rational invariants under B and P:

$$f_3 = \frac{y^2}{x} - 1, \quad f_4 = xy - 1, \quad f_5 = \frac{x^2}{y} - 1, \quad F_1 = \Big\{ f_3, f_4, f_5 \Big\}.$$

Let's try to take also g_1, g_2. We see that we are dealing with the Case 10.1, because g_1 and g_2 are invariant under B and P. Then we let

$$f_1 = x^3 - 1, \quad f_2 = xy - 1, \quad F_2 = \Big\{ f_1, f_2 \Big\}.$$

A unimodular column Hermite multiplier V for $\begin{bmatrix} B & P \end{bmatrix}$ is

$$V = \begin{bmatrix} -1 & 1 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, V_{\mathfrak{n}} = \begin{bmatrix} 1 & 3 \\ 1 & 0 \end{bmatrix}, \quad W = V^{-1} = \begin{bmatrix} -1 & 1 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Then a generating set of invariants is formed by monomials $w_1 = xy$ and $w_2 = x^3$. The rewriting rules are

$$\begin{bmatrix} x & y \end{bmatrix}^T \to \mathbf{w}^{W_{\mathfrak{d}} - P_{\mathfrak{d}} P^{-1} B} = \begin{bmatrix} w_2^{1/3} & \frac{w_1}{w_2^{1/3}} \end{bmatrix}^T.$$

Rewriting F_1 in terms of a generating set we obtain

$$f_3 \to h_3 = \frac{\frac{w_1^2}{w_2^{2/3}}}{w_2^{1/3}} - 1 = \frac{w_1^2}{w_2} - 1, \quad f_4 \to h_4 = w_2^{1/3} \frac{w_1}{w_2^{1/3}} - 1 = w_1 - 1, \quad f_5 \to h_5 = \frac{w_2^{2/3}}{\frac{w_1}{w_2^{1/3}}} - 1 = \frac{w_2}{w_1} - 1.$$

Rewriting F_2 in terms of a generating set we obtain

$$f_1 \to h_1 = w_2 - 1, \quad f_2 \to h_2 = w_2^{1/3}\frac{w_1}{w_2^{1/3}} - 1 = w_1 - 1.$$

We see that the system F_2 was rewritten to simpler equations in w_1 and w_2 that the system F_1.

Further examples on reduction of finite symmetries can be found in [7, Examples 3.5 and 3.7]. The following Example 10.7 shows how to use invariants obtained using the Reynolds operator to reduce the system.

Example 10.7. *Consider the same ideal as in Example 10.6*

$$I = \langle g_1, g_2 \rangle \subset \mathbb{C}[x,y], \quad g_1 = x^3 - 1, \quad g_2 = xy - 1.$$

All finite symmetries of $\mathbf{V}(I)$ are given by a finite matrix group

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e^{2\pi i\frac{1}{3}} & 0 \\ 0 & e^{2\pi i\frac{2}{3}} \end{bmatrix}, \begin{bmatrix} e^{2\pi i\frac{2}{3}} & 0 \\ 0 & e^{2\pi i\frac{1}{3}} \end{bmatrix} \right\}.$$

In Example 10.4 we saw that $w_1 = x^3$, $w_2 = y^3$ and $w_3 = xy$ form a generating set of $\mathbb{C}[x,y]^G$, and then

$$f \in \mathbb{C}[x,y]^G \iff f \in \mathbb{C}[x^3, y^3, xy].$$

Notice that the above equivalence is dealing only with polynomials invariant under G (not rational functions). We see that g_1 and g_2 are invariant under G. We use [4, Chapter 7, §3, Proposition 7] to rewrite g_1 and g_2 in terms of x^3, y^3 and xy:

$$g_1 = w_1 - 1, \quad g_2 = w_2 - 1.$$

But, if we take another generators of I:

$$g_1 = x^3 - 1, \quad g_3 = x^2 - y,$$

then we see that g_3 is not invariant and we cannot use [4, Chapter 7, §3, Proposition 7] (while in the case of reduction using column Hermite multiplier it wasn't a problem).

The reason why we moved from a polynomial ring to a field of rational functions (Subsection 10.2.1, the 1st sentence) is that computing with a column Hermite multiplier V and its inverse W there can arise negative integers.

As the last thing of this section we want to note that in [8] and [7] there are two different methods of recovering solutions of the original system from its reduced form. In [8] the solutions of the original are obtained from the reduced one by simple multiplying and rising to powers the solutions of the reduced system (see [8, Theorem 5.3 and Example 5.4]). While in [7], after obtaining the solutions of the reduced system, we then should solve another (monomial) system M (see [7, Theorem 5.5 and Example 5.6]). We also want to note that in [7] the so-called "normalized" unimodular column Hermite multiplier of $\begin{bmatrix} B & -P \end{bmatrix}$ was used. For such a multiplier, the matrix $V_\mathfrak{n}$ becomes upper triangular. This then means that a monomial system M becomes an upper triangular and, as a corollary, not so hard to solve.

10.4 Note On a Homogeneous Ideal

Suppose a $\mathbf{1}$-homogeneous ideal $I \subset k[x_1, ..., x_n]$ generated by $\mathbf{1}$-weighted homogeneous polynomials $g_1, ..., g_m$. Then $\mathbf{V}(I)$ has infinite symmetries given by $A = \mathbf{1} \in \mathbb{Z}^{1\times n}$. One of unimodular column Hermite multipliers V of A is

$$V = \begin{bmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ... & 1 \\ -1 & -1 & -1 & ... & -1 \end{bmatrix} \in \mathbb{Z}^{n\times n}, \quad W = V^{-1} = \begin{bmatrix} -1 & -1 & ... & -1 & -1 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \end{bmatrix}.$$

Then $w_1 = \frac{x_1}{x_n}$, $w_2 = \frac{x_2}{x_n}$, ..., $w_{n-1} = \frac{x_{n-1}}{x_n}$ form a generating set of rational invariants under A. We clearly see that $g_1, ..., g_m$ cannot be invariant under A, because $\mathbf{1}$-weighted total degree of a monomial in any polynomial cannot be less than one (and as a consequence cannot be equal to zero). But each of $g_1, ..., g_m$ we can devide by $x_n^{r_j}$, where r_j is $\mathbf{1}$-weighted total degree of each monomial in g_j. After such division, we obtain a set $F = \left\{f_1, ..., f_m\right\}$ of rational functions invariant under A. We can see the rewriting rules in terms of $w_1, ..., w_{n-1}$ from the last $n-1$ rows of W , which are

$$\begin{bmatrix} x_1 & ... & x_n \end{bmatrix}^T \to \begin{bmatrix} w_1 & ... & w_{n-1} & 1 \end{bmatrix}^T.$$

And we note that after rewriting we obtain ***polynomials*** in $w_1, ..., w_{n-1}$ from $f_1, ..., f_m$.

11 Permutation Representations

In this chapter we will explain how stability matrices of I act on a variety $\mathbf{V}(I)$. We will consider here only ideals I with a finite non-empty variety $\mathbf{V}(I)$. By Corollary 3 we can claim that $\mathbf{V}(I)$ is a G_I-set (see [1, p. 176]). Suppose $\mathbf{V}(I)$ has m elements. Then we can construct a group homomorphism

$$\varphi\colon G_I \to S_m,$$

(where S_m is the symmetric group on m elements) in a usual way. Suppose $g \in G_I$ permorfs the following permutation σ_g of the elements of $\mathbf{V}(I)$:

$$\sigma_g = \begin{pmatrix} 1 & 2 & \dots & m \\ i_1 & i_2 & \dots & i_m \end{pmatrix}.$$

Then we set $\varphi(g) = \sigma_g$. We can easily verify (see [1, p.182, Proposition 8.2]) that so defined φ is a group homomorphism. The First Isomorphism Theorem tells us that $\mathrm{im}(\varphi)$ is a subgroup of S_m. In examples below we will show that φ shouldn't be surjective nor injective.

Example 11.1. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x, y]$, where*

$$f_1(x, y) = x^2 + y^2 - 1, \quad f_2(x, y) = x + y - 1, \quad \mathbf{V}(I) = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

A group of all stability matrices G_I is:

$$G_I = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Let's look on how these matrices permute the elements of $\mathbf{V}(I)$. Let's denote $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Then

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_2 & \mathbf{v}_1 \end{bmatrix}.$$

Then we construct φ as follows:

$$\varphi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) = (\ ), \quad \varphi\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) = (1\ \ 2).$$

Here $(\ \ )$ means the identity permutation, $(1\ \ 2)$ means permutation of 2 elements. Obviously, homomorphism φ here is surjective and injective (φ is an isomorphism), and then

$$G_I \cong S_2.$$

Example 11.2. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{R}[x, y]$, where*

$$f_1(x,y) = x^2 + y^2 - 1, \quad f_2(x,y) = x + y, \quad \mathbf{V}(I) = \left\{ \begin{bmatrix} -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{bmatrix}, \begin{bmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{bmatrix} \right\}.$$

A group G_I is:

$$G_I = \Bigg\{ \underbrace{\begin{bmatrix} -s_{22} + 1 + w & -s_{22} + w \\ s_{22} - 1 & s_{22} \end{bmatrix}}_{\text{set } M_1}, \underbrace{\begin{bmatrix} -s_{22} - 1 - w & -s_{22} - w \\ s_{22} + 1 & s_{22} \end{bmatrix}}_{\text{set } M_2} \Bigg\}, \quad s_{22} \in \mathbb{R}, w \in \mathbb{R}^*.$$

Let's denote $\mathbf{v}_1 = \begin{bmatrix} -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{bmatrix}$. Then we can verify that $\forall s_{22} \in \mathbb{R}, w \in \mathbb{R}^*$ there holds true

$$\begin{bmatrix} -s_{22} + 1 + w & -s_{22} + w \\ s_{22} - 1 & s_{22} \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix},$$

$$\begin{bmatrix} -s_{22} - 1 - w & -s_{22} - w \\ s_{22} + 1 & s_{22} \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_2 & \mathbf{v}_1 \end{bmatrix}.$$

Hence, after constructing a homomorphism φ, we conclude by The First Isomorphism Theorem that the set M_1 is a normal subgroup of G_I and

$$G_I / M_1 \cong S_2.$$

We also could suppose here a field $\mathbb{C}$ instead of $\mathbb{R}$. Then $\mathbf{V}(I)$ is the same. Also group G_I is the same, only $s_{22} \in \mathbb{C}$ and $w \in \mathbb{C}^*$.

Example 11.3. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x, y]$, where*

$$f_1(x,y) = x^4 - 1, \quad f_2(x,y) = xy - 1, \quad \mathbf{V}(I) = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \end{bmatrix}, \begin{bmatrix} i \\ -i \end{bmatrix}, \begin{bmatrix} -i \\ i \end{bmatrix} \right\}.$$

Then a group of all stability matrices of I is:

$$G_I = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \right\}.$$

We can easily verify which permutation of $\mathbf{V}(I)$ performs each matrix of G_I and then conclude that

$$G_I \cong D_4,$$

where D_4 is a dihedral group (group of symmetries of a regular 4-polygon).

Example 11.4. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x, y]$, where*

$$f_1(x,y) = y^3 + x^2 + x + 1, \quad f_2(x,y) = xy + y - 1, \quad |\mathbf{V}(I)| = 5.$$

A group of all stability matrices of I is:

$$G_I = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Example 11.5. *Suppose an ideal $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x, y]$, where*

$$f_1(x, y) = -xz + y^2 + 1, \quad f_2(x, y) = xyz + y - 1, \quad f_3(x, y) = z^2 + y + 1, \quad |\mathbf{V}(I)| = 6.$$

A group of all stability matrices of I is:

$$G_I = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\} \cong S_2.$$

You may have already noticed that Examples 11.3 and 9.1 are similar and differ only by an exponent of the first monomial in f_1. In Example 9.1 we can in the same way (by observing which permutation of $\mathbf{V}(I)$ performs each matrix from G_I) conclude that

$$G_I \cong D_3 \cong S_3.$$

This observation can be made for all such ideals with generators $f_1(x, y)_q = x^q - 1$, $q \geq 3$ and $f_2(x, y) = xy - 1$. We want to note that the solutions of $I_q = \langle f_1(x, y)_q, f_2(x, y) \rangle$ "form a regular q-polygon". We give Definition 11.2, which explains what does than mean.

Definition 11.1. *Suppose a vector $\mathbf{x} = \begin{bmatrix} a + bi & c + di \end{bmatrix} \in \mathbb{C}^2$. We will say that $\mathbf{y}$ is an* ***extension of*** $\mathbf{x}$ ***to*** $\mathbb{R}^4$ *if $\mathbf{y} = \begin{bmatrix} a & b & c & d \end{bmatrix}$.*

Definition 11.2. *Suppose a subset $V_1 \subset \mathbb{C}^2$ with m elements. Make an extension of each vector in V_1 to obtain a new subset $V_2 \subset \mathbb{R}^4$. We will say that V_1* ***forms a regular*** m***-polygon*** *if $\forall\, \mathbf{v}_1, \mathbf{v}_2 \in V_2$:*

(i) $\|\mathbf{v}_1\|_2 = \|\mathbf{v}_2\|_2$.

(ii) $\angle(\mathbf{v}_1, \mathbf{v}_2) = r\frac{2\pi}{m}$ *for some integer r, $0 \leq r \leq m - 1$.*

Let's take a look on Example 11.3. We extend variety from this example to $\mathbb{R}^4$ and obtain

$$V = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

We can easily verify that V forms a regular 4-polygon by Definition 11.2. And because $I = \langle x^4 - 1, xy - 1 \rangle \subset \mathbb{C}[x, y]$ is radical, then we see that Conjecture 11.1 holds true. The same it is for Example 9.1.

We saw in examples above that in some cases G_I is finite, in some not. Proposition 11.1 gives a sufficient condition for G_I to be finite. In the proof of Proposition 11.1 we will use the following Lemma 11.1.

Lemma 11.1. *Suppose an ideal $I \subset k[x_1, ..., x_n]$. Then G_I is a subgroup of $G_{\mathbf{I}(\mathbf{V}(I))}$.*

Proof. Take any $g \in G_I$. By Corollary 3, $\mathbf{V}(I)$ is invariant under g. Then by Lemma 5.3 $(ii \iff iv)$, $\mathbf{I}(\mathbf{V}(I))$ is stable under g.

□

Proposition 11.1. *Suppose an ideal $I \subset k[x_1, ..., x_n]$. If $\mathbf{V}(I)$ is finite and* $\operatorname{Span}_k(\mathbf{V}(I)) = k^n$*, then G_I is finite.*

Proof. We know from Lemma 5.3 that $\mathbf{A}$ is from $G_{\mathbf{I}(\mathbf{V}(I))}$ if and only if $\mathbf{A}$ permutes elements of $\mathbf{V}(I)$. Because $\operatorname{Span}_k(\mathbf{V}(I)) = k^n$, then we can extract a basis $\mathbf{v}_1, ..., \mathbf{v}_n$ for k^n from $\mathbf{V}(I)$. Take any permutation σ on m elements. We want to find all matrices $\mathbf{A}_\sigma$ which perform this permutation on $\mathbf{V}(I)$. Notice that $\mathbf{A}_\sigma$ should also perform some permutation τ of $\mathbf{v}_1, ..., \mathbf{v}_n$:

$$\mathbf{A}_\sigma \begin{bmatrix} \mathbf{v}_1 & ... & \mathbf{v}_n \end{bmatrix} = \begin{bmatrix} \mathbf{v}_{i_1} & ... & \mathbf{v}_{i_n} \end{bmatrix}, \quad \tau = \begin{pmatrix} 1 & ... & n \\ i_1 & ... & i_n \end{pmatrix}.$$

Then

$$\mathbf{A}_\sigma = \begin{bmatrix} \mathbf{v}_{i_1} & ... & \mathbf{v}_{i_n} \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & ... & \mathbf{v}_n \end{bmatrix}^{-1} \tag{11.1}$$

Now, we know that $\mathbf{A}_\sigma$ defined in Equation (11.1) performs a permutation τ of $\mathbf{v}_1, ..., \mathbf{v}_n$. But we should check if $\mathbf{A}_\sigma$ performs a permutation σ on all elements in $\mathbf{V}(I)$. If it is true, then $\mathbf{A}_\sigma$ belongs to $G_{\mathbf{I}(\mathbf{V}(I))}$ (and from Equation (11.1) it follows that there doesn't exist another matrix $\mathbf{B}_\sigma$ which performs the same permutation σ of $\mathbf{V}(I)$). Because there is only a finite number of permutations on m elements (namely $m!$), then we conclude that $G_{\mathbf{I}(\mathbf{V}(I))}$ has cardinality at most $m!$. Because G_I is a subgroup of $G_{\mathbf{I}(\mathbf{V}(I))}$, then it follows that G_I also has cardinality at most $m!$ and, as a corollary, is finite.

□

We give the following conjecture about how big can be a group of stability matrices of an ideal I with a specific finite variety.

Conjecture 11.1. *Let k be a subfield of $\mathbb{C}$. Suppose an ideal $I \subset k[x, y]$ with a finite variety $\mathbf{V}(I)$, $\left|\mathbf{V}(I)\right| = m$, $m \geq 3$. Suppose also that* $\operatorname{Span}_k(\mathbf{V}(I)) = k^2$*. Then G_I is isomorphic to some subgroup of dihedral group D_m. For a radical ideal I, G_I is isomorphic to D_m if and only if $\mathbf{V}(I)$ forms a regular m-polygon.*

In the statement of the above conjecture we made a restriction $\operatorname{Span}_k(\mathbf{V}(I)) = k^2$ to make a group G_I finite by Proposition 11.1. We also want $m \geq 3$, because for $m = 2$ a variety $\mathbf{V}(I)$ with the property $\operatorname{Span}_k(\mathbf{V}(I)) = k^2$ cannot form a regular 2-polygon. We suppose k is a subfield of $\mathbb{C}$, because a notion of forming a regular polygon (Definition 11.2) is defined for subsets of $\mathbb{C}^2$.

Also, for a variety $\mathbf{V}(I)$ with 2 elements with the property $\operatorname{Span}_{\mathbb{C}}(\mathbf{V}(I)) = \mathbb{C}^2$ (from Proposition 11.1) we obtain that G_I can be a trivial one or isomorphic to S_2.

12 Finding All Symmetries of a Weak Perspective-n-Points Problem

We refer to [9, Section 5]. The problem of estimating the pose of a weak perspective camera can be reduced to

$$\min_{s,R} \left\| R \operatorname{diag}(a_1, a_2, a_3) - \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \right\|_F^2 \quad \text{s.t. } RR^T = s^2 I_2,$$

where $a_1 \geq a_2 \geq a_3 \geq 0$. We can use a quaternion parametrization of 2×3 rotation R:

$$R(\mathbf{q}) = \begin{bmatrix} q_1^2 + q_2^2 - q_3^2 - q_4^2 & 2(q_2q_3 - q_1q_4) & 2(q_1q_3 + q_2q_4) \\ 2(q_1q_4 + q_2q_3) & q_1^2 - q_2^2 + q_3^2 - q_4^2 & 2(q_3q_4 - q_1q_2) \end{bmatrix},$$

where $\mathbf{q} = \begin{bmatrix} q_1 & q_2 & q_3 & q_4 \end{bmatrix}$ and $\|q\|_2 = s$. Then constructing a cost function we obtain

$$f(\mathbf{q}) = \|R(\mathbf{q})A - B\|_F^2, \quad A = \operatorname{diag}(a_1, a_2, a_3), \quad B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix}.$$

Minimising $f(\mathbf{q})$ means finding the solutions of $\mathbf{q}$ for

$$\mathbf{g}(\mathbf{q}) = \nabla_{\mathbf{q}} f(\mathbf{q}) = \mathbf{0}.$$

Because $\mathbf{q}$ is of length 4, then we should solve the system of 4 polynomial equations.

Example 12.1. *Choosing*

$$A = \operatorname{diag}(2, 3, 5) \quad B = \begin{bmatrix} -8 & -11 & 13 \\ 9 & 8 & 11 \end{bmatrix}$$

we obtain the following equations $\mathbf{g}(\mathbf{q}) = \mathbf{0}$*:*

$$g_1(\mathbf{q}) = 52q_1^3 + 180q_1q_2^2 + 220q_1q_3^2 + 52q_1q_4^2 - 40q_2q_3q_4 - 32q_1 + 220q_2 - 260q_3 - 204q_4,$$

$$g_2(\mathbf{q}) = 180q_1^2q_2 - 40q_1q_3q_4 + 52q_2^3 + 52q_2q_3^2 + 220q_2q_4^2 + 220q_1 + 160q_2 + 60q_3 - 260q_4,$$

$$g_3(\mathbf{q}) = 220q_1^2q_3 - 40q_1q_2q_4 + 52q_2^2q_3 + 52q_3^3 + 180q_3q_4^2 - 260q_1 + 60q_2 - 160q_3 - 220q_4,$$

$$g_4(\mathbf{q}) = 52q_1^2q_4 - 40q_1q_2q_3 + 220q_2^2q_4 + 180q_3^2q_4 + 52q_4^3 - 204q_1 - 260q_2 - 220q_3 + 32q_4.$$

All stability matrices of $I = \langle g_1, g_2, g_3, g_4\rangle \subset \mathbb{C}[q_1, q_2, q_3, q_4]$ *are*

$$G_I = \left\{ \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} & & & i \\ & & i & \\ & -i & & \\ -i & & & \end{bmatrix}, \begin{bmatrix} & & & -i \\ & & -i & \\ & i & & \\ i & & & \end{bmatrix} \right\}.$$

We can easily see that

$$G_I \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

And because $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *is abelian, then we can diagonalize* G_I *to obtain an isomophic group of diagonal matrices. It was done in [9, p. 10, Section 5.2]. One of matrices* $\mathbf{S} \in \mathrm{GL}_4(\mathbb{C})$ *which diagonalizes* G_I *is*

$$\mathbf{S} = \begin{bmatrix} -i & 0 & i & 0 \\ 0 & -i & 0 & i \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Then

$$G_J = \mathbf{S}^{-1} G_I \mathbf{S} =$$

$$= \left\{ \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix} \right\}.$$

We can represent this group by matrices B *and* P *as follows:*

$$B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad P = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

Applying a linear change of variables on g_1, g_2, g_3, g_4 *by matrix* $\mathbf{S}$ *we obtain a new ideal* $J = \langle g_1(\mathbf{Sx}), g_2(\mathbf{Sx}), g_3(\mathbf{Sx}), g_4(\mathbf{Sx})\rangle = \varphi_{\mathbf{S}}(I)$ *which is stable under* G_J *(as was shown in the proof of Theorem 4.1).*

13 Conclusion

In this thesis we have shown how to find stability matrices of a given ideal and how to use them for reduction of polynomial systems.

We explained that to obtain all infinite scaling symmetries of a given ideal I we need to find a $\mathbb{Z}$-basis of the left integer kernel of matrix of exponents differences K_F obtained from a reduced Groebner basis F of I. To obtain all finite symmetries we need to compute the Smith normal form of K_F. In Chapter 10 we have shown how to reduce a polynomial system to obtain another polynomial system with a smaller number of solutions [8, 7].

In Chapter 9 we proposed a method for finding all stability matrices of a given ideal. We saw that this leads to solving another polynomial system, usually more difficult than the original one.

In Chapter 4 we have shown that an ideal I is stable under an ivertible matrix $\mathbf{A}$ if and only if it is invariant under $\mathbf{A}$. We used this fact to show that $\mathbf{A}$ acts as a bijection on $\mathbf{V}(I)$. In the case of finite variety, $\mathbf{A}$ permutes elements of $\mathbf{V}(I)$. This allows us to construct a group homomorphism from G_I to the symmetric group S_m (m is the number of elements in $\mathbf{V}(I)$), which was described in Chapter 11. We gave a conjecture that for a finite variety $\mathbf{V}(I) \subset k^2$ (k is a subfield of $\mathbb{C}$, $m \geq 3$) such that $\mathrm{Span}_k(\mathbf{V}(I)) = k^2$, a group G_I cannot be bigger than a dihedral group D_m.

In the last Chapter 12 we found all stability matrices of the weak perspective-n-points problem. We have shown that in generic situation there are only 4 stability matrices, which form an abelian group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Bibliography

[1] M. Artin. *Algebra*. Prentice Hall, 1991.

[2] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, Third Corrected Printing, 1996.

[3] R. M. Corless, K. Gatermann, and I. S. Kotsireas. "Using symmetries in the eigenvalue method for polynomial systems". In: *Journal of Symbolic Computation* (2009), pp. 1536–1550. DOI: 10.1016/j.jsc.2008.11.009.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer, Second Edition, 1998.

[5] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, 1998.

[6] J.-C. Faugère and J. Svartz. "Gröbner bases of ideals invariant under a commutative group: the non-modular case". In: *ISAAC'13, Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*. Boston, USA: ACM, 2013, pp. 347–354. DOI: 10.1145/2465506.2465944.

[7] E. Hubert and G. Labahn. "Computing the invariants of finite abelian groups". In: *Mathematics of Computation, American Mathematical Society* (2016), pp. 3029–3050. DOI: 10.1090/mcom/3076.

[8] E. Hubert and G. Labahn. "Rational invariants of scalings from Hermite normal forms". In: *ISAAC'12, Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. Grenoble, France: ACM, 2012, pp. 219–226. DOI: 10.1145/2442829.2442862.

[9] V. Larsson and K. Åström. "Uncovering symmetries in polynomial systems". In: *ECCV 2016, Proceedings of the 14th European Conference on Computer Vision*. Amsterdam, The Netherlands: Springer Verlag, 2016, pp. 252–267. DOI: 10.1007/978-3-319-46487-9_16.

Appendix A. Contents of the attached CD

```
/
├── FindingSymmetries ............... folder with code for finding symmetries
│   ├── TPLibrary ..................... folder with imported library
│   │   ├── TPMapleLibrary.mla ....... library archive file
│   │   └── TPMapleLibrary.mw ......... implementation of library functions
│   └── FindingSymmetries.mw ........ the implemented approach to finding symmetries
├── Bachelor_Thesis.pdf ............ digital copy of this thesis
└── README.txt
```