

**REFLECTION GROUPS AND SEMIGROUP ALGEBRAS IN  
MULTIPLICATIVE INVARIANT THEORY**

---

A Dissertation  
Submitted to  
the Temple University Graduate Board

---

in Partial Fulfillment  
of the Requirements for the Degree of  
DOCTOR OF PHILOSOPHY

---

by  
Mohammed S. Tesemma  
August, 2004

©

by

Mohammed S. Tesemma

August, 2004

All Rights Reserved

# ABSTRACT

## REFLECTION GROUPS AND SEMIGROUP ALGEBRAS IN MULTIPLICATIVE INVARIANT THEORY

Mohammed S. Tesemma

DOCTOR OF PHILOSOPHY

Temple University, August, 2004

Professor Martin Lorenz, Chair

In classical invariant theory one considers the situation where a group  $\mathcal{G}$  of  $n \times n$  matrices over a field  $\mathbf{K}$  acts on the polynomial algebra  $\mathbf{K}[x_1, \dots, x_n]$  by linear substitutions of the variables  $x_i$ . The subalgebra of all polynomials fixed (invariant) under the action of  $\mathcal{G}$  is called the algebra of polynomial  $\mathcal{G}$ -invariants, usually denoted by  $\mathbf{K}[x_1, \dots, x_n]^{\mathcal{G}}$ . One of the most celebrated results on polynomial invariants is the Shephard-Todd-Chevalley Theorem:

*Assume that  $\mathcal{G}$  is finite of order not divisible by the characteristic of  $\mathbf{K}$ . Then the invariant algebra  $\mathbf{K}[x_1, \dots, x_n]^{\mathcal{G}}$  is again a polynomial algebra if and only if  $\mathcal{G}$  acts as a pseudo-reflection group on the vector space  $V = \bigoplus_{i=1}^n \mathbf{K}x_i$ .*

Here an element  $g \in \mathcal{G}$  is called a pseudo-reflection on  $V$  if  $\mathcal{G}$  acts trivially on a hyperplane in  $V$  or, equivalently, if the  $n \times n$  matrix  $g - 1_V$  has rank one. The group  $\mathcal{G}$  is said to act as a pseudo-reflection group on  $V$  if  $\mathcal{G}$  is generated by elements that are pseudo-reflections on  $V$ .

A different kind of group action, on Laurent polynomial algebras instead of polynomial algebras, is defined as follows. Let  $\mathcal{G}$  be a finite group acting by automorphism on a lattice  $\mathbf{A} \cong \mathbb{Z}^n$ , and hence on the group algebra  $\mathbf{K}[\mathbf{A}]$  over a field  $\mathbf{K}$ . Fixing an isomorphism  $\mathbf{A} \cong \mathbb{Z}^n$ , we may think of the  $\mathcal{G}$ -action on  $\mathbf{A}$  as given by a homomorphism  $\mathcal{G} \rightarrow \mathrm{GL}_n(\mathbb{Z})$ , the group of invertible  $n \times n$ -matrices

over  $\mathbb{Z}$ , and the group algebra  $\mathbb{K}[A]$  can be identified with the Laurent polynomial algebra  $\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ . The subalgebra  $\mathbb{K}[A]^{\mathcal{G}}$  of  $\mathcal{G}$ -invariant Laurent polynomials in  $\mathbb{K}[A]$  is called an *algebra of multiplicative invariants*. A result of Lorenz ([Lo01]) states that if  $\mathcal{G}$  acts as a pseudo-reflection group on the  $\mathbb{Q}$ -vector space  $A \otimes \mathbb{Q}$  then  $\mathbb{K}[A]^{\mathcal{G}}$  is a semigroup algebra over  $\mathbb{K}$ . This is a multiplicative analogue of the “if”-part of Shephard-Todd-Chevalley theorem for polynomial invariants. However, the converse of Lorenz’s theorem is open. In this thesis we will state and prove an extended version of this theorem which does indeed have a converse. Moreover, we take a different approach than [Lo01] inasmuch as our arguments are based on the geometry of simplicial cones rather than root systems.

# ACKNOWLEDGEMENTS

First I would like to take this opportunity to express my sincere appreciation and gratitude to my supervisor Professor Martin Lorenz for his endless support and expert guidance throughout my studies at Temple. What I learned from his mathematical maturity and rigor is beyond words. He also devoted enormous amount of time reading my thesis with patience and gave life to the scratch work by organizing it and adding a finishing touch.

Secondly my thanks go to Professor Edward Letzter whose ideas and approach to problems in algebra inspired all of us who learned from him.

I would like to thank Professors Boris Datskovsky, Georgia Triantafyllou, Marvin Knopp, Shiferaw Berhanu, Orin Chein, Cristian Gutierrez, Sinai Robins and others from whom I learned mathematics at Temple. I also want to thank Professors John Schiller and David Zitarelli for their hospitality and help.

To my classmates Melanie Butler, Jay Pathak and Mark Renault. We shared ideas and learned a lot from each other in several topics courses. I am happy to know you all and to have been influenced by your talents in one way or another.

To Omer Yayenie, whose assistance with Maple programming has its own place in my thesis.

Last but not least, to my wife and best friend Almaz, the most patient and warm-hearted individual. Without your comfort and faith in me this work would never have reached its conclusion. Our beautiful daughter, Faven, also paid a big sacrifice missing parents for such a long time. After all, time is now approaching for a big family reunion!

# DEDICATION

For my parents Belinesh Ali and Seid Tesemma with all  
my love and gratitude.

# TABLE OF CONTENTS

<b>ABSTRACT</b>	<b>iv</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vi</b>
<b>DEDICATION</b>	<b>vii</b>
<b>LIST OF FIGURES</b>	<b>x</b>
<b>NOTATION</b>	<b>xi</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 Classical Invariant Theory . . . . .	2
1.3 Linear Actions . . . . .	3
1.3.1 The Setting . . . . .	3
1.3.2 Basic Problems of Invariant Theory . . . . .	3
1.3.3 Open Problems for Finite Groups . . . . .	7
1.4 Multiplicative Actions . . . . .	8
1.5 Some Results on Multiplicative Invariants . . . . .	10
1.5.1 Problem (“Semigroup Algebra Problem”) . . . . .	12
1.5.2 Our Contribution . . . . .	12
<b>2 PRELIMINARIES</b>	<b>14</b>
2.1 Overview . . . . .	14
2.2 Monoids . . . . .	14
2.3 Semigroup Algebras . . . . .	16
2.4 Group Actions . . . . .	17
2.5 Basics on Polyhedral Cones . . . . .	19
2.6 Multiplicative Actions, Again . . . . .	21
2.7 Fundamental Domains . . . . .	24

2.7.1	Term Orders . . . . .	24
2.7.2	SAGBI Bases . . . . .	28
<b>3</b>	<b>REFLECTION GROUPS</b>	<b>31</b>
3.1	Basic Concepts . . . . .	31
3.2	Reflection Groups from Polyhedral Cones . . . . .	33
<b>4</b>	<b>THE THEOREM OF LORENZ USING SAGBI BASES</b>	<b>43</b>
4.1	Overview . . . . .	43
4.2	Proof of Theorem 4.1.2 . . . . .	44
4.3	The Converse . . . . .	48
4.4	Examples . . . . .	48
<b>A</b>	<b>MAPLE PROGRAM</b>	<b>55</b>
	<b>REFERENCES</b>	<b>58</b>



# LIST OF FIGURES

4.1	$A^\gamma$ for the reflection group in Example 4.4.1 . . . . .	50
4.2	$A^\gamma$ for the non-reflection group in Example 4.4.2 . . . . .	54

# NOTATION

$K$	an arbitrary field.
$\mathbb{A}$	an arbitrary $K$ -algebra.
$S(V)$	the symmetric algebra of a $K$ -vector space $V$ .
$\mathbb{Z}_+, \mathbb{Q}_+, \mathbb{R}_+$	the non-negative integers, rationals, and reals respectively.
$A := x^{\mathbb{Z}^n}$	a free abelian group of rank $n$ in multiplicative notation
$K[A]$	the group algebra of $A$ over $K$
$S := K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$	the Laurent polynomial algebra in $n$ variables.
$\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$	a group of automorphisms of $\mathbb{Z}^n$ or $K^n$ .
$R = S^{\mathcal{G}}$	the invariant algebra.
$\sum_{fin}$	sum of a finite collection.
$\langle \{\dots\} \rangle_{mon}$	the submonoid generated by a given set $\{\dots\}$ .
$\langle \{\dots\} \rangle_{gp}$	the group generated by the given set $\{\dots\}$ .
$\vartheta$	orbit sum.
$C^\vee$	the dual of a cone $C$ .
$\mathrm{Supp}(f)$	the support of $f$ .
$\mathcal{H}$	a family of hyperplanes.
$\mathcal{I}$	the initial map.
$\mathcal{F}$	face of a cone.
$M$	a multiplicative monoid.

# CHAPTER 1

## INTRODUCTION

### 1.1 Overview

In algebraic terms, invariant theory is concerned with the study of group actions, their fixed points, and their orbits. The actions are usually on algebras of various sorts, the fixed points are subalgebras and the closed orbits form an algebraic variety. More generally, if a group acts by automorphisms on a ring then the object of investigation is the subring consisting of all elements that are invariant (fixed) under the group action. One would like to determine which ring theoretic properties of the ring are inherited by the subring of invariants.

In this Introduction we will start with a discussion of invariant theory from a historical point of view. In §1.3 we will describe linear actions on polynomial algebras, the type of group action studied in classical invariant theory. Following the general outline of [NS02] we will state various important problems of invariant theory and discuss some known results. Some of these problems will provide the motivation for the questions considered in detail later in this thesis. In §1.4 we set the stage for a relatively new type of group actions on Laurent polynomials called *multiplicative actions*. In §1.5 we will state some known results in multiplicative invariant theory that are related

to classical results on polynomial invariants. Finally we will state the main problem to which this thesis is devoted and describe our contribution towards its solution.

## 1.2 Classical Invariant Theory

Classical invariant theory is the study of the geometrical properties of algebraic group actions on affine space  $\mathbb{A}^n = \mathbb{K}^n$  ( $\mathbb{K}$  is some algebraically closed field, traditionally the complex numbers). Such a group action yields an action on the algebra of polynomial functions on  $\mathbb{A}^n$ , that is, the ordinary polynomial algebra  $\mathbb{K}[x_1, \dots, x_n]$ . This fascinating field was brought to life at the beginning of the 19<sup>th</sup> century just as the theory of solutions of polynomial equations was given its present form by Galois. The fundamental problem of invariant theory was to find or at least prove the existence of a finite system of generators for the algebra of polynomial invariants. David Hilbert solved the existence problem in a spectacular series of papers from 1888 - 1893 that propelled him into the position of the most renowned mathematician of his time. The fact that the central problem was solved in combination with a new abstract approach which entirely displaced the computational in pure mathematics caused invariant theory to sink into relative obscurity. But the indirect influence of invariant theory continued to be felt in group theory and representation theory, while in abstract algebra the three most famous of Hilbert's general theorems, *the Basis Theorem*, *the Syzygy Theorem* and *the Nullstellensatz*, were all born as Lemmas (Hilfsätze) in his invariant theory papers. Recent years have witnessed a dramatic resurgence of this subject with new applications ranging from topology and geometry to physics, continuum mechanics, and computer vision.

As a result of its historical roots, the subject holds a particular fascination for any mathematician with a desire to understand the culture, sociology, and history of mathematics. (Part of the contents of the above section on classical invariant theory is taken from [O199].)

## 1.3 Linear Actions

### 1.3.1 The Setting

In the most traditional setting of invariant theory, the ring under consideration is the polynomial algebra  $\mathbb{K}[x_1, \dots, x_n]$  and the group  $\mathcal{G}$  acts on  $\mathbb{K}[x_1, \dots, x_n]$  by sending the space of variables  $\bigoplus_{i=1}^n \mathbb{K}x_i$  to itself. In a modern base free description this can be rephrased as follows. Let  $V$  be an  $n$ -dimensional vector space over  $\mathbb{K}$  and let  $\mathcal{G} \rightarrow GL(V)$  be a representation of  $\mathcal{G}$  on  $V$ . Thus  $\mathcal{G}$  acts on  $V$  by automorphism and this action can be uniquely extended to the symmetric algebra

$$\mathcal{S}(V) := \bigoplus_{j=0}^{\infty} V^{\otimes j} / \langle \{a \otimes b - b \otimes a; a, b \in V\} \rangle.$$

A choice of basis for  $V$  gives us an explicit isomorphism  $\mathcal{S}(V) \cong \mathbb{K}[x_1, \dots, x_n]$  with  $V$  corresponding to the space of variables  $\bigoplus_{i=1}^n \mathbb{K}x_i$ . The action of  $\mathcal{G}$  on  $V$  becomes an action by linear substitutions of the variables, i.e., for each  $g \in \mathcal{G}$  we have  $g \cdot x_i = \sum_{j=1}^n a_{ij}x_j$  for some  $a_{ij} \in \mathbb{K}$  that are determined by  $g$ . This justifies the name *linear action*. The resulting invariant algebra  $\mathcal{S}(V)^{\mathcal{G}}$  is often referred to as an algebra of *polynomial invariants*.

**Example 1.3.1.** Let  $\mathcal{G} = \mathcal{S}_n$  be the symmetric group of all permutations on the set  $\{1, \dots, n\}$  acting on  $\mathbb{K}[x_1, \dots, x_n]$  by  $g \cdot x_i = x_{g(i)}$ , for  $g \in \mathcal{G}$ . The resulting invariant algebra is  $\mathbb{K}[\sigma_1, \dots, \sigma_n]$ , where

$$\sigma_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} x_{i_1} \cdots x_{i_r}, \quad r = 1, \dots, n$$

is the  $r^{\text{th}}$  elementary symmetric polynomial.

### 1.3.2 Basic Problems of Invariant Theory

In the setting of §1.3.1, it is certainly of great significance to know whether or not the invariant algebra,  $\mathcal{S}(V)^{\mathcal{G}}$ , has a certain finite description. Below are several interpretations of finiteness.

## 1. Algebraic Finiteness

We know that  $\mathcal{S}(V) \cong \mathbb{K}[x_1, \dots, x_n]$  is  $\mathbb{K}$ -affine, i.e., finitely generated as an algebra over  $\mathbb{K}$ . Now the problem on algebraic finiteness asks:

Is  $\mathcal{S}(V)^{\mathcal{G}}$  also finitely generated as algebra over  $\mathbb{K}$ ?

The answer is positive, even in a more general setting:

**Theorem 1.3.2 (E. Noether [No16]).** *Suppose  $\mathcal{G}$  is a finite group acting by automorphism of a finitely generated commutative  $\mathbb{K}$ -algebra  $\mathbb{A}$ . Then  $\mathbb{A}^{\mathcal{G}}$  is also a finitely generated commutative  $\mathbb{K}$ -algebra and  $\mathbb{A}$  is finitely generated as a module over  $\mathbb{A}^{\mathcal{G}}$ .*

There exists versions of Theorem 1.3.2 for actions of certain infinite groups, but the theorem is not valid in general if  $\mathcal{G}$  is an infinite group. In fact, this question for an arbitrary group acting linearly on  $\mathbb{K}[x_1, \dots, x_n]$  is Hilbert's famous 14<sup>th</sup> problem. In 1959 Nagata gave a counterexample showing that the invariant subring of certain “exotic” matrix groups are not finitely generated.

The next result tells us where to look for actual generators of algebras of polynomial invariants.

**Theorem 1.3.3 (P. Fleischmann [Fl], J. Fogarty [Fo]).** *Suppose  $\rho : \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{K})$  is a representation of a finite group  $\mathcal{G}$  such that  $\mathrm{char}(\mathbb{K})$  does not divide the order of  $\mathcal{G}$ . Then the algebra of polynomial invariants  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  is generated by  $\mathcal{G}$ -invariant polynomials of degree at most  $|\mathcal{G}|$ .*

The bound  $|\mathcal{G}|$  provided by the theorem is known as Noether's degree bound. Indeed the result was first proved by E. Noether in characteristic zero [No16], and her proof remains valid as long as the characteristic of  $\mathbb{K}$  is bigger than  $|\mathcal{G}|$ . For a long time it was an open question as to whether it is in fact sufficient to require only that  $\mathrm{char}(\mathbb{K})$  does not divide  $|\mathcal{G}|$ . This case is usually referred to as the “non-modular case”.

Returning to the general setting of Theorem 1.3.2, the condition that  $\mathbb{A}^{\mathcal{G}}$  is affine allows us to apply another fundamental result of Noether:

**Theorem 1.3.4 (Noether Normalization Lemma).** *Let  $\mathbb{A}$  be an affine commutative  $\mathbb{K}$ -algebra. Then there exists  $y_1, \dots, y_n \in \mathbb{A}$  which are algebraically independent over  $\mathbb{K}$  and such that  $\mathbb{A}$  is a finite module over the polynomial subalgebra  $\mathbb{K}[y_1, \dots, y_n]$  of  $\mathbb{A}$ .*

In view of this result, we may find invariants  $y_1, \dots, y_n \in \mathbb{A}^{\mathcal{G}}$  which are algebraically independent over  $\mathbb{K}$  and such that the invariant algebra  $\mathbb{A}^{\mathcal{G}}$  is a finite module over the subalgebra  $\mathbb{K}[y_1, \dots, y_n]$ . The invariants  $y_1, \dots, y_n$  are called “primary invariants”; they are by no means uniquely determined.

## 2. Homological Finiteness

If  $\mathcal{S}(V)^{\mathcal{G}} = \mathbb{K}[f_1, \dots, f_m]$  is finitely generated, we may define an epimorphism

$$\rho : \mathbb{K}[t_1, \dots, t_m] \twoheadrightarrow \mathcal{S}(V)^{\mathcal{G}} : t_i \mapsto f_i$$

from the polynomial algebra  $\mathbb{K}[t_1, \dots, t_m]$  with  $m$ -variables to the invariant algebra. The kernel of  $\rho$  is called the “first Syzygy module” denoted  $Syz_1$ . Suppose  $Syz_1, \dots, Syz_\ell$  have already been defined. Choose a generating set of minimal size for  $Syz_\ell$  as  $\mathbb{K}[t_1, \dots, t_m]$ -module, and let  $L_{\ell+1}$  be a free  $\mathbb{K}[x_1, \dots, x_m]$ -module with basis in bijective correspondence with this generating set. Thus we have a canonical epimorphism  $L_{\ell+1} \twoheadrightarrow Syz_\ell$ . The kernel of this epimorphism is the next syzygy module,  $Syz_{\ell+1}$ . Now the problem of homological finiteness is the following:

Are the syzygy modules of  $\mathcal{S}(V)^{\mathcal{G}}$  finitely generated? Is the syzygy chain finite? That is, does one have  $Syz_\ell = 0$  for some  $\ell$ ?

These questions are answered in the positive by two fundamental results of Hilbert:

**Theorem 1.3.5 (Hilbert’s Basis Theorem).** *Every submodule of a finitely generated  $\mathbb{K}[x_1, \dots, x_n]$ -module is finitely generated.*

**Theorem 1.3.6 (Hilbert's Syzygy Theorem).** *Any module  $\mathcal{M}$  over the polynomial algebra  $\mathbb{K}[x_1, \dots, x_n]$  has a finite free resolution of length at most  $n$ , i.e., there is a chain of  $\mathbb{K}[x_1, \dots, x_n]$ -module homomorphism*

$$0 \longrightarrow F_s \xrightarrow{\varphi_s} \dots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} \mathcal{M} \longrightarrow 0$$

*with  $\text{im}(\varphi_i) = \ker(\varphi_{i-1})$ ,  $i \leq n$  and such that all  $F_i$  are free modules. If  $\mathcal{M}$  is finitely generated then  $F_0, \dots, F_s$  may be chosen finitely generated as well.*

### 3. Combinatorial Finiteness

A  $\mathbb{K}$ -algebra  $\mathbb{A}$  is *graded* (by  $\mathbb{Z}_+$ ) if  $\mathbb{A} = \bigoplus_{j=0}^{\infty} \mathbb{A}_j$ , where each  $\mathbb{A}_j$  is a  $\mathbb{K}$ -vector space and multiplication is compatible with the decomposition, i.e.,  $\mathbb{A}_i \cdot \mathbb{A}_j \subseteq \mathbb{A}_{i+j}$ .

For example, if  $\mathbb{A}$  is the polynomial algebra  $\mathbb{K}[x_1, \dots, x_n]$  then we may define  $\mathbb{A}_j$  to be the vector space of homogeneous polynomials of total degree  $j$ .

In general, if  $\mathbb{A}$  is affine and connected (i.e.  $\mathbb{A}_0 = \mathbb{K}$ ) then it is easy to see that all  $\mathbb{A}_j$  are finite dimensional over  $\mathbb{K}$ . The *Poincaré series* of such a graded algebra is defined to be the generating function

$$P_t(\mathbb{A}) = \sum_{j=0}^{\infty} (\dim_{\mathbb{K}} \mathbb{A}_j) t^j \in \mathbb{Z}[[t]]$$

**Example 1.3.7.** *The Poincaré series for the polynomial algebra  $\mathbb{K}[x]$  is*

$$P_t(\mathbb{K}[x]) = 1 + t + t^2 + \dots = \frac{1}{1-t}$$

*More generally,*

$$P_t(\mathbb{K}[x_1, \dots, x_n]) = \left(\frac{1}{1-t}\right)^n$$

All this applies to algebras of polynomial invariants  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  for finite group  $\mathcal{G}$ , since they are affine and connected. Therefore the combinatorial finiteness question is:

Does there exist a simple formula for the Poincaré series of the ring of invariants?



In characteristic 0, the answer is provided by the following result which is extensively used in algorithms for finding generators for the invariant algebra  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$ .

**Theorem 1.3.8 (T. Molien [Mo]).** *Let  $\rho : \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{K})$  be a representation of a finite group  $\mathcal{G}$  over a field  $\mathbb{K}$  of characteristic zero. Then the Poincaré series for the ring of invariants is given by*

$$P_t(\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \frac{1}{\det(1 - gt)}$$

One important observation from the above theorems is that they all assume finiteness of the acting group  $\mathcal{G}$ . We will concentrate on finite groups from now on and turn to some open questions concerning their invariant algebras next.

### 1.3.3 Open Problems for Finite Groups

**1. Cohen-Macaulay Problem:** Let  $\rho : \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{K})$  be a representation of a finite group over the field  $\mathbb{K}$  and let  $y_1, \dots, y_n \in \mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  be a set of primary invariants; so  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  is a finitely generated module over  $\mathbb{K}[y_1, \dots, y_n]$ . Can one say more about this module structure? In the non-modular case, the answer is provided by the following result.

**Theorem 1.3.9 (Hochster and Eagon [HE71]).** *If  $\rho : \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{K})$  is a representation of finite group and  $\mathrm{char}(\mathbb{K})$  does not divide  $|\mathcal{G}|$  then  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  is free over  $\mathbb{K}[y_1, \dots, y_n]$ .*

In the language of commutative algebra, the conclusion of the theorem states that  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{G}}$  is a Cohen-Macaulay ring. In the modular case (i.e., when  $\mathrm{char}(\mathbb{K})$  divides  $|\mathcal{G}|$ ), the result is no longer valid. It is one of the most important open problems on polynomial invariants to determine exactly when they are Cohen-Macaulay.

**2. Polynomial Algebra Problem:** We know that the rings we started with, the polynomial algebras, are particularly nice in that they are generated

by a system of  $n$  parameters which is exactly equal to its Krull dimension. This is not always the case for the invariant algebra. Therefore the following question arises:

For which finite groups  $\mathcal{G} \hookrightarrow GL_n(\mathbf{K})$  and which fields  $\mathbf{K}$  is  $\mathbf{K}[x_1, \dots, x_n]^{\mathcal{G}}$  again a polynomial algebra?

The answer to this classical problem in invariant theory, in the non-modular case, is due to Shephard, Todd and Chevalley.

**Theorem 1.3.10 (Shephard-Todd-Chevalley Theorem [ST54, Ch55]).**

*Suppose that the finite group  $\mathcal{G}$  acts linearly on the symmetric algebra  $\mathcal{S}(V)$  of the finite dimensional  $\mathbf{K}$ -vector space  $V$  and that the characteristic of  $\mathbf{K}$  does not divide the order of  $\mathcal{G}$ . Then the following are equivalent*

(i) *The invariant algebra  $\mathcal{S}(V)^{\mathcal{G}}$  is a polynomial algebra over  $\mathbf{K}$ .*

(ii)  *$\mathcal{G}$  acts as a pseudoreflection group on  $V$ .*

Here, an element  $g \in \mathcal{G}$  is called a pseudoreflection on  $V$  if the linear transformation  $\text{Id}_V - g$  of  $V$  has rank 1. A group is called a pseudoreflection group on  $V$  if  $\mathcal{G}$  can be generated by pseudo-reflections on  $V$ . We will present a detailed study of reflection groups in Chapter 3. It was observed by Serre [Se67] that the implication (i)  $\Rightarrow$  (ii) in the Shephard-Todd-Chevalley Theorem works in any characteristic. This is however not true of (ii)  $\Rightarrow$  (i): there are reflection groups whose polynomial invariants in the modular case are not even Cohen-Macaulay, let alone polynomial algebras; see [Nak80]. It is an open problem at present to determine exactly when modular polynomial invariants of reflection groups are polynomial algebras.

## 1.4 Multiplicative Actions

During the past 20 years another branch of invariant theory, known as *multiplicative invariant theory*, has established itself as an independent branch

of invariant theory in its own right, beginning with the work of D. Farkas in the 80's [Fa84, Fa85]. Prior to Farkas, only a few isolated results on multiplicative invariants, also called “exponential invariants” or “monomial invariants”, were known, notably in the work of Bourbaki [Bo68], Steinberg [Ste75] and Richardson [Ri82].

Multiplicative invariants arise from lattices, that is, from free abelian groups of finite rank, and their group algebras. Traditionally, a lattice  $\mathbf{A}$  of rank  $n$  is identified with  $\mathbb{Z}^n$  by choosing a basis. Hence the usual notation for lattices is additive. However, when viewed inside its group algebra, the lattice has to be thought of as a multiplicative subgroup. We indicate this passage from the additive to the multiplicative setting by adopting a formal exponential notation. In detail, the group algebra  $\mathbf{K}[\mathbf{A}]$  has a  $\mathbf{K}$ -basis  $\mathbf{A} = \{\mathbf{x}^a \mid a \in \mathbb{Z}^n\}$  labelled by the elements of  $\mathbb{Z}^n$ . Multiplication in  $\mathbf{K}[\mathbf{A}]$  is defined by  $\mathbf{K}$ -linear extension of the rule

$$\mathbf{x}^a \mathbf{x}^b = \mathbf{x}^{a+b}.$$

Thus,  $\mathbf{A}$  is a subgroup of the group of (multiplicative) units of the algebra  $\mathbf{K}[\mathbf{A}]$ . The group algebra  $\mathbf{K}[\mathbf{A}]$  can be thought of as a Laurent polynomial algebra:

$$\mathbf{K}[\mathbf{A}] \cong \mathbf{K}[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}]$$

via the group isomorphism

$$\mathbf{A} \cong \langle x_1^{\pm 1}, \dots, x_n^{\pm 1} \rangle_{\text{mon}} : \mathbf{x}^a \mapsto x_1^{a_1} \cdots x_n^{a_n}, \quad \text{where } a = (a_1, \dots, a_n) \in \mathbb{Z}^n$$

Thus the subgroup  $\mathbf{A} = \{\mathbf{x}^a : a \in \mathbb{Z}^n\}$  corresponds to the group of “monomials” in the Laurent polynomial algebra  $\mathbf{K}[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}]$ .

Now let  $\mathcal{G}$  be a group with representation  $\mathcal{G} \rightarrow \text{GL}(\mathbf{A}) \cong \text{GL}_n(\mathbb{Z})$ , the homomorphism induces an action on  $\mathbf{A}$  which can be uniquely extended to an action by  $\mathbf{K}$ -algebra automorphisms on  $\mathbf{K}[\mathbf{A}]$ . Explicitly, the action of  $\mathcal{G}$  on  $\mathbf{K}[\mathbf{A}]$  is given by

$$g \cdot \mathbf{x}^a = \mathbf{x}^{g \cdot a} \in \mathbf{A}, \quad (g \in \mathcal{G}, \mathbf{x}^a \in \mathbf{A})$$

This action stabilizes the multiplicative group of monomial units  $A$ . Hence the name “multiplicative” or “monomial” action. One notable feature of multiplicative actions is the fact that the degree of Laurent polynomials (i.e. the grading of the algebra) is not preserved under the action. This is in sharp contrast with the case of linear actions and causes a great deal of added difficulty in the investigation of multiplicative invariants.

## 1.5 Some Results on Multiplicative Invariants

Below we give a brief survey of some results in multiplicative invariant theory. Most of the results we list here are related to the polynomial algebra problem for linear actions. In the multiplicative case, the analogous problem would ask when the invariant algebra  $K[A]^{\mathcal{G}}$  is again a Laurent polynomial algebra or, equivalently, a group algebra. However, a simple argument (see [Lo01]) shows that, this happens only when  $\mathcal{G}$  acts trivially. On the other hand, there are several interesting results in the literature that are in the spirit of the Shephard-Todd-Chevalley Theorem.

For all the theorems below we keep the following notations:  $A$  is a free abelian group of rank  $n$ ,  $\mathcal{G} \leq GL A \cong GL_n(\mathbb{Z})$  a finite group,  $K[A]$  the group algebra and  $K[A]^{\mathcal{G}}$  is the algebra of multiplicative invariants.

**Farkas [Fa84, Fa86]:** The invariant algebra  $\mathbb{C}[A]^{\mathcal{G}}$  is a polynomial algebra over  $\mathbb{C}$  iff  $A$  is isomorphic as a  $\mathcal{G}$ -module to the weight lattice of some root system with Weyl group  $\mathcal{G}$ .

**Lorenz [Lo96]:** If  $\text{char}(K) \nmid |\mathcal{G}|$ , then the following are equivalent:

- (i) The algebra of invariants  $K[A]^{\mathcal{G}}$  is regular.
- (ii)  $K[A]$  is free as  $K[A]^{\mathcal{G}}$ -module.
- (iii)  $K[A]^{\mathcal{G}}$  is a mixed Laurent polynomial algebra, i.e.

$\mathbb{K}[\mathbf{A}]^{\mathcal{G}} \cong \mathbb{K}[x_1^{\pm 1}, \dots, x_r^{\pm 1}, x_{r+1}, \dots, x_d]$ . Here, necessarily,  $r = \text{rank } \mathbf{A}^{\mathcal{G}}$  and  $d = \text{rank } \mathbf{A}$ .

(iv)  $\mathcal{G}$  is a reflection group and  $H^1(\mathcal{G}, \mathbf{A}^D) = 0$ , where  $D \leq \mathcal{G}$  is generated by the reflections that are diagonalizable over  $\mathbb{Z}$  and  $\mathbf{A}^D$  denotes the  $D$ -invariants in  $\mathbf{A}$ .

**Lorenz [Lo01]:** If  $\mathcal{G}$  acts as a reflection group on  $\mathbf{A}$  then the invariant algebra  $\mathbb{K}[\mathbf{A}]^{\mathcal{G}}$  is a semigroup algebra  $\mathbb{K}[\mathbf{M}]$ , where the structure of the monoid  $\mathbf{M}$  is known.

Here, semigroup algebras  $\mathbb{K}[\mathbf{M}]$  are defined exactly as ordinary group algebras (see §1.4), except that  $\mathbf{M}$  is merely required to be a semigroup and hence does not necessarily consist of units in  $\mathbb{K}[\mathbf{M}]$ .

**Reichstein [Re03]:** The following are equivalent:

- (i)  $\mathbb{K}[\mathbf{A}]^{\mathcal{G}}$  has a finite SAGBI<sup>1</sup> bases.
- (ii)  $\mathcal{G}$  is a reflection group on  $\mathbf{A}$ .

My focus is on the last of Lorenz's results: *multiplicative invariants of finite reflection groups are affine normal semigroup algebras*. I will refer to this result throughout as *Lorenz's Theorem*.

Here we want to emphasize that affine normal semigroup algebras are an interesting class of algebras:

(i) They are common generalizations of polynomial and Laurent polynomial algebras.

(ii) Their fields of fractions are rational over the base field. This answers the so-called "rationality problem" when  $\mathcal{G}$  is a reflection group. In general,

---

<sup>1</sup>The term SAGBI from computational algebra stands for *Subalgebra Analogue to Gröbner Bases for Ideals*. We will give a detailed definition later.

Hajja and Kang [Ha87, HK92, HK94] established rationality of multiplicative invariant fields of ranks 2 and 3, except for one case in rank 3 which is still undecided. The approach of Hajja and Kang is computational case by case investigating each of the (finitely many) possible groups.

(iii) Projective modules over affine normal semigroup algebras are free, (Gubeladze’s theorem [Gu92]). In view of (i) this a far reaching generalization of the celebrated Quillen-Suslin Theorem for polynomial rings.

### 1.5.1 Problem (“Semigroup Algebra Problem”)

In view of the already mentioned facts concerning semigroup algebras Lorenz’s theorem, along with the envisioned converse, would be a powerful analogue to the Shephard-Todd-Chevalley theorem of linear actions. But the converse of Lorenz’s theorem is an open, although Lorenz has a significant result in that direction obtained by using geometric methods.

Thus we formulate the following problem:

*If the invariant algebra  $K[A]^{\mathcal{G}}$  is a semigroup algebra over  $K$ , must  $\mathcal{G}$  act as a reflection group on  $A$ ?*

### 1.5.2 Our Contribution

We will answer the above question from a little different perspective. In Chapter 4 we will rework the proof of Lorenz’s theorem using *SAGBI bases* and *simplicial cones* following Reichstein’s work [Re03]. The core idea used in Lorenz’s original proof can be rephrased in the language of simplicial cones which results in a conceptually simpler proof avoiding the machinery of root systems that was used in [Lo01]. We restrict ourselves to the case where  $\mathcal{G}$  acts *effectively* on  $\mathbb{Z}^n$ , that is,  $(\mathbb{Z}^n)^{\mathcal{G}} = \{0\}$ .

In detail, consider a total ordering,  $\succeq$ , on the lattice  $A \cong \mathbb{Z}^n$  that is compatible with the addition operation, i.e.  $a \succeq b \Rightarrow a + c \succeq b + c$ ;  $(a, b, c \in \mathbb{Z}^n)$ . We will discuss such orderings in §2.7.1 in detail and in particular exhibit a

simple example.

For each nonzero Laurent polynomial

$$f = \sum_i k_i x^{a_i} \in \mathbb{K}[A] \cong \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$$

define

$$\mathcal{I}(f) := \max_i \{a_i \mid k_i \neq 0\} \in \mathbb{Z}^n$$

This gives a monoid homomorphism

$$\mathcal{I}: (\mathbb{K}[A] \setminus \{0\}, \cdot) \longrightarrow (\mathbb{Z}^n, +)$$

called the *initial map*. In Chapter 4, we will prove that, when  $\mathcal{G}$  acts as a reflection group on  $A$ , then  $\mathbb{K}[A]^{\mathcal{G}}$  is a semigroup algebra  $\mathbb{K}[M]$  for some submonoid  $M \subseteq (\mathbb{K}[A] \setminus \{0\}, \cdot)$  such that the restriction of the initial map to  $M$  is injective. Moreover the converse of this statement is also true. Hence we have the following result which summarizes our contribution to the semigroup algebra problem.

**Theorem 1.5.1.** *Assume that  $\mathcal{G}$  acts effectively on  $\mathbb{Z}^n$ . Then the following are equivalent:*

- (i)  $\mathcal{G}$  acts as a reflection group on  $\mathbb{Z}^n$ .
- (ii) There exists a monoid  $M \subseteq (\mathbb{K}[A]^{\mathcal{G}}, \cdot)$  such that  $\mathbb{K}[A]^{\mathcal{G}} = \mathbb{K}[M]$  is a semigroup algebra and the initial map  $\mathcal{I}$  is injective on  $M$ .

# CHAPTER 2

## PRELIMINARIES

### 2.1 Overview

We will start by providing the basic definitions and facts concerning monoids, semigroup algebras, and group actions. In particular, we will prove Maschke's theorem for further application. We proceed by introducing polyhedral cones which will play a crucial role in the proof of our main result, Theorem 1.5.1. Next, returning to multiplicative actions, we will illustrate the definitions given in the Introduction with some explicit examples. The chapter concludes with a section on fundamental domains for multiplicative actions.

### 2.2 Monoids

A monoid is a set  $M$  with an associative operation  $\mu: M \times M \rightarrow M$  and identity element. The monoid  $M$  is called *commutative* if  $\mu(a, b) = \mu(b, a)$  holds for all  $a, b \in M$ . Some examples of commutative monoids are  $\mathbb{Z}$  with multiplication (identity element 1) and  $\mathbb{Z}^r \oplus \mathbb{Z}_+^s$  with addition (identity element  $(0, \dots, 0)$ ). We will only be concerned with commutative monoids in this thesis and therefore usually use additive notation for the operation of  $M$ ; so



$\mu(a, b) = a + b$  for  $a, b \in M$ ,  $na = a + \cdots + a$  ( $n$  summands) for  $a \in M$ ,  $n \in \mathbb{N}$ , and  $0$  denotes the identity element of  $M$ . However, in the setting of semigroup algebras, we will consider multiplicative monoids. We will use the notation  $\mathbf{M}$  to emphasize this fact; see §2.3 below.

Submonoids and monoid homomorphisms are defined as usual. The intersection of any family of submonoids of a given monoid  $M$  is again a submonoid of  $M$ . In particular, for any subset  $S \subseteq M$ , there is a unique smallest submonoid of  $M$  which contains  $S$ ; it will be denoted by  $\langle S \rangle_{mon}$ . Using the above additive notation, the elements of  $\langle S \rangle_{mon}$  can be thought of as the finite  $\mathbb{Z}_+$ -linear combinations of elements of  $S$ . The monoid  $M$  is called *finitely generated* if  $M = \langle S \rangle_{mon}$  for some finite subset  $S \subseteq M$ .

**Definition 2.2.1.** *A commutative monoid  $(M, +)$  is called*

*cancellative* if  $a + c = b + c \Rightarrow a = b$  for all  $a, b, c \in M$

*torsion-free* if  $na = nb \Rightarrow a = b$ , for  $a, b \in M$  and  $n \in \mathbb{N}$

Every commutative monoid  $M$  has a *group of fractions*, denoted  $M_{gp}$ ; it can be constructed as

$$M_{gp} = M \times M / \sim$$

with componentwise operation. Here,  $\sim$  is an equivalence relation on  $M \times M$  given by

$$(a, b) \sim (c, d) \Leftrightarrow \exists m_1, m_2 \in M : m_1 + a = m_2 + c \ \& \ m_1 + b = m_2 + d$$

The map

$$\nu : M \longrightarrow M_{gp} \cong M \times M / \sim : \quad a \mapsto (a, 0) / \sim$$

is a monoid homomorphism, called the “canonical” homomorphism.

**Lemma 2.2.2.** *Let  $(M, +)$  be a finitely generated commutative monoid. Then  $M$  is isomorphic to a submonoid of  $\mathbb{Z}^r$  (with  $+$ ) for some  $r \in \mathbb{N}$  if and only if  $M$  is both cancellative and torsion free.*

*Proof.* The implication  $\Rightarrow$  is trivial, since  $\mathbb{Z}^r$  is cancellative and torsion free and these properties are inherited by all submonoids.

For  $\Leftarrow$ , we use the canonical homomorphism  $\nu: M \rightarrow M_{gp}$ . Note first that since  $M$  is finitely generated it follows that  $M_{gp}$  is a finitely generated abelian group. Therefore, it will suffice to prove the following two facts:

(i)  $\nu$  is injective.

(ii) the group  $M_{gp}$  is torsion-free (and hence  $M_{gp} \cong \mathbb{Z}^r$  for some  $r \in \mathbb{N}$ , by the fundamental theorem of finitely generated abelian groups [DF99, Thm.5.2.3]).

Proof for (i): Let  $\nu(a) = \nu(b)$ , that is  $(a, 0) \sim (b, 0)$ . Then there exists  $m_1, m_2 \in M$  such that  $m_1 + a = m_2 + b$  and  $m_1 + 0 = m_2 + 0$ . The latter equality implies  $m_1 = m_2$ . Hence from the first equality and the fact that  $M$  is cancellative, we get  $a = b$ . This proves (i).

Proof for (ii): Let  $(a, b) \in M_{gp}$  be a torsion element. That is  $n(a, b) = (na, nb) \sim (0, 0)$  for some  $n \in \mathbb{N}$ . Thus there exists  $m_1, m_2 \in M$  such that  $m_1 + na = m_2 + 0$  and  $m_1 + nb = m_2 + 0$ . It follows that  $m_1 + na = m_2 = m_1 + nb$ . Since  $M$  is cancellative, we deduce that  $na = nb$ , and since  $M$  is torsion free, we obtain that  $a = b$ . Finally, one can easily see that  $(a, a) \sim (0, 0)$ . Therefore  $M_{gp}$  has no non-trivial torsion element, proving (ii). Hence the lemma is proved.  $\square$

## 2.3 Semigroup Algebras

In this section,  $\mathbb{K}$  denotes an arbitrary base field.

**Definition 2.3.1.** A  $\mathbb{K}$ -algebra  $\mathbb{A}$  is called a semigroup algebra if there exists a submonoid  $\mathbb{M} \subseteq (\mathbb{A}, \cdot)$  such that the elements of  $\mathbb{M}$  form a  $\mathbb{K}$ -basis of  $\mathbb{A}$ .

**Example 2.3.2.** 1. The polynomial algebra  $\mathbb{K}[x_1, \dots, x_n]$  and Laurent polynomial algebra  $\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$  are both semigroup algebras. The monoids  $\mathbb{M}$

in question are given by  $\mathbf{M} = \langle x_1, \dots, x_n \rangle_{\text{mon}} \cong (\mathbb{Z}_+^n, +)$  in the first case and  $\mathbf{M} = \langle x_1^{\pm 1}, \dots, x_n^{\pm 1} \rangle_{\text{mon}} \cong (\mathbb{Z}^n, +)$  in the second.

2. The algebra  $\mathbb{K}[x^2, xy, y^2]$  is a semigroup algebra since elements of the monoid  $\mathbf{M} = \langle x^2, xy, y^2 \rangle_{\text{mon}}$  form a  $\mathbb{K}$ -basis of  $\mathbb{K}[x^2, xy, y^2]$ . One can show that the monoid  $\mathbf{M}$  is not isomorphic to a monoid of the form  $\mathbb{Z}^r \oplus \mathbb{Z}_+^s$ .

**Proposition 2.3.3.** *Let  $\mathbb{K}[\mathbf{M}]$  be a semigroup algebra. Then;*

(i)  $\mathbb{K}[\mathbf{M}]$  is a finitely generated (affine)  $\mathbb{K}$ -algebra if and only if  $\mathbf{M}$  is a finitely generated monoid.

(ii)  $\mathbb{K}[\mathbf{M}]$  is a domain if and only if  $\mathbf{M}$  is cancellative and torsion-free.

*Proof.* (i). The implication  $\Leftarrow$  is trivial. For  $\Rightarrow$ , assume the  $\mathbb{K}$ -algebra  $\mathbb{K}[\mathbf{M}]$  is generated by  $f_1, \dots, f_r$  say. Each  $f_i$  can be written in terms of the basis  $\mathbf{M}$  of  $\mathbb{K}[\mathbf{M}]$ ; this requires finitely many elements  $m_1, \dots, m_s \in \mathbf{M}$ . We claim that  $\mathbf{M} = \langle m_1, \dots, m_s \rangle_{\text{mon}}$ . For this, let  $a \in \mathbf{M}$  be arbitrary. Then  $a = P(f_1, \dots, f_r) = Q(m_1, \dots, m_s)$  for suitable polynomials  $P$  and  $Q$  with coefficients in  $\mathbb{K}$ . Note that  $Q(m_1, \dots, m_s)$  is a  $\mathbb{K}$ -linear combination of monomials in the  $m'_i$ 's; these are elements of  $\mathbf{M}$ . By  $\mathbb{K}$ -independence of  $\mathbf{M}$ , we conclude that  $a$  is a monomial in the  $m_i$ . In other words,  $a \in \langle m_1, \dots, m_s \rangle_{\text{mon}}$ . Hence,  $\mathbf{M}$  is generated by  $m_1, \dots, m_s$ .

(ii). The implication  $\Leftarrow$  follows from Lemma 2.2.2. Indeed, our hypotheses on  $\mathbf{M}$  imply that  $\mathbf{M}$  embeds into  $\mathbb{Z}^r$  for some  $r$ , and hence  $\mathbb{K}[\mathbf{M}]$  embeds into  $\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ . Since  $\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$  is a domain, so is  $\mathbb{K}[\mathbf{M}]$ . For the converse (which is not difficult), see [Gi84, Theorem 8.1].  $\square$

## 2.4 Group Actions

**Definition 2.4.1.** *An action of a group  $\mathcal{G}$  on a set  $E$  is a map*

$$\mathcal{G} \times E \longrightarrow E : (g, a) \mapsto g \cdot a, \quad (g \in \mathcal{G}, a \in E)$$

*such that  $1 \cdot a = a$  and  $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$  holds for each  $a \in E$  and  $g_1, g_2 \in \mathcal{G}$ . Here,  $1$  denotes the identity element of  $\mathcal{G}$ .*

Equivalently, an action of a group  $\mathcal{G}$  on  $E$  amounts to a group homomorphism

$$\rho : \mathcal{G} \longrightarrow \text{perm}(E)$$

where  $\text{perm}(E)$  is the group of all permutations of  $E$ .

If  $V$  is a vectorspace over a field  $\mathbf{K}$  and the action of  $\mathcal{G}$  on  $V$  also satisfies

$$g \cdot (v_1 + v_2) = (g \cdot v_1) + (g \cdot v_2) \quad \text{and} \quad g \cdot (kv) = k(g \cdot v)$$

for all  $v, v_i \in V$  and  $k \in \mathbf{K}$  then we say that  $\mathcal{G}$  acts on  $V$  by  $\mathbf{K}$ -*automorphism*.

This amounts to having a group homomorphism, called a *representation*,

$$\rho : \mathcal{G} \longrightarrow \text{GL}(V)$$

where  $\text{GL}(V)$  is the group of all invertible  $\mathbf{K}$ -linear transformations of  $V$ . A vector space  $V$  admitting a  $\mathcal{G}$ -action is called  $\mathbf{K}[\mathcal{G}]$ -module.

Given a  $\mathbf{K}[\mathcal{G}]$ -module  $V$ , a subspace  $V' \subset V$  is called *stable* under  $\mathcal{G}$  if  $g(V') \subset V'$  for all  $g \in \mathcal{G}$ , i.e.  $V'$  is itself a  $\mathbf{K}[\mathcal{G}]$ -module. A representation  $\rho : \mathcal{G} \longrightarrow \text{GL}(V)$  is said to be *completely reducible* if, given a  $\mathcal{G}$ -stable subspace  $V' \subset V$ , there exists a  $\mathcal{G}$ -stable subspace  $V'' \subset V$  such that  $V = V' \oplus V''$ .

**Theorem 2.4.2 (Maschke's Theorem).** *If  $V$  is a vector space over a field  $\mathbf{K}$  and  $\text{char}(\mathbf{K})$  does not divide  $|\mathcal{G}|$ , then every representation*

$$\rho : \mathcal{G} \longrightarrow \text{GL}(V)$$

*is completely reducible.*

*Proof.* Suppose  $V' \subset V$  is stable under  $\mathcal{G}$ . Let  $p : V \longrightarrow V$  be any  $\mathbf{K}$ -linear projection with  $\text{Im}(p) = V'$ . Define a map  $\hat{p} : V \longrightarrow V$  by

$$\hat{p}(v) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} g^{-1} \cdot p(g \cdot v)$$

One can easily verify that

$$(i) \quad \hat{p}(\sigma \cdot x) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} g^{-1} p(g\sigma \cdot x) = \sigma \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} (g\sigma)^{-1} p((g\sigma) \cdot x)$$

$$= \sigma \hat{p}(x), \forall \sigma \in \mathcal{G}, x \in V.$$

$$(ii) \quad \text{Im}(\hat{p}) = V' \quad \text{and} \quad \hat{p}|_{V'} = \text{Id}_{V'}.$$

These properties imply that  $\ker(\hat{p})$  is a complement of  $V'$  which is  $\mathcal{G}$ -stable.  $\square$

**Definition 2.4.3.** Let  $\mathcal{G}$  be a group acting on  $E$  and  $a \in E$  we define the orbit of  $a$  to be the set  $\mathcal{O}_a := \{g \cdot a : g \in \mathcal{G}\}$ .

The distinct  $\mathcal{G}$ -orbits form a partition of  $E$ . Any subset of  $E$  containing exactly one representative from each orbit is called a *fundamental domain* for the action of  $\mathcal{G}$  on  $E$ . We will study fundamental domains of multiplicative actions later in detail as they play an important role in multiplicative invariant theory. It will turn out that certain fundamental domains will be geometric objects in  $\mathbb{R}^n$  known as polyhedral cones. Therefore, we study polyhedral cones in the next section.

## 2.5 Basics on Polyhedral Cones

A subset  $C$  of  $\mathbb{R}^n$  is called a *cone* if  $\sum_{i=1}^m r_i c_i \in C$  holds for all  $c_i \in C$  and  $r_i \in \mathbb{R}_+$ . Clearly, intersections of cones are cones. The smallest cone in  $\mathbb{R}^n$  containing a given subset  $X$  of  $\mathbb{R}^n$  is

$$C = \text{Pos}(X) = \left\{ \sum_{x \in X} r_x x : x \in X, r_x \in \mathbb{R}_+ \text{ almost all zero} \right\};$$

it is called the cone *generated by*  $X$ . If  $X \subseteq \mathbb{Z}^n$  we call  $C$  an *integral cone*, and if  $X$  is finite the cone  $C$  will be called a *polyhedral cone*. Clearly, integral polyhedral cones are exactly those cones that can be generated by finite subsets  $X \subseteq \mathbb{Z}^n$ .

Let  $(\mathbb{R}^n)^* = \text{Hom}(\mathbb{R}^n, \mathbb{R}) \cong \mathbb{R}^n$  be the dual of  $\mathbb{R}^n$ , with dual pairing  $\langle, \rangle$ . For any cone  $C$  in  $\mathbb{R}^n$  we define the dual cone,  $C^\vee$ , by

$$C^\vee = \{f \in (\mathbb{R}^n)^* : \langle f, c \rangle \geq 0 \ \forall c \in C\}$$

It follows from the definition that  $C^\vee$  is also a cone. Moreover, if  $C$  is an integral polyhedral cone then so is  $C^\vee$ ; see [Ew96, Theorem V.2.10].

**Definition 2.5.1.** Given a cone  $C \subseteq \mathbb{R}^n$ , we define

(i) a **face**  $\mathcal{F}$  of  $C$  to be a subset of the form

$$\mathcal{F} := C \cap f^\perp = \{c \in C : \langle f, c \rangle = 0\} \text{ for some } f \in C^\vee.$$

Each face is again a cone in  $\mathbb{R}^n$ .

(ii) the **dimension** of  $C$  to be the dimension of the subspace generated by  $C$ .

(iii) the **facets** of  $C$  to be the faces  $\mathcal{F}$  of  $C$  with  $\dim \mathcal{F} = \dim C - 1$ . Faces of dimension one are called **edges** of the cone.

We state below some basic facts about polyhedral cones for future use.

**Lemma 2.5.2.** *A polyhedral cone is a closed subset of  $\mathbb{R}^n$ .*

*Proof.* Let  $C \subseteq \mathbb{R}^n$  be a polyhedral cone; so  $C = \text{Pos}(v_1, \dots, v_k) = \sum_{i=1}^k \mathbb{R}_+ v_i$  for suitable  $v_i \in \mathbb{R}^n$ . Clearly, the rays  $\mathbb{R}_+ v_i$  are all closed subsets of  $\mathbb{R}^n$ . Moreover, for any two closed subsets  $A$  and  $B$  of  $\mathbb{R}^n$ , the ‘‘Minkowski sum’’  $A + B = \{a + b \mid a \in A, b \in B\}$  is again a closed subset of  $\mathbb{R}^n$ ; see, e.g., [Ew96, p. 103/4]. The assertion now follows by induction, because  $C$  is the Minkowski sum of the rays  $\mathbb{R}_+ v_i$  for  $i = 1, \dots, k$ .  $\square$

Note that any cone  $C \subseteq \mathbb{R}^n$  is in particular a submonoid of  $(\mathbb{R}^n, +)$ , and hence so is  $C \cap \mathbb{Z}^n$ .

**Lemma 2.5.3 (Gordan’s Lemma).** *Let  $C$  be an integral polyhedral cone in  $\mathbb{R}^n$ , then, the monoid  $C \cap \mathbb{Z}^n$  is finitely generated.*

*Proof.* Write  $C = \text{Pos}\{v_1, \dots, v_k\}$  with  $v_i \in \mathbb{Z}^n$ . Consider the set

$$F := \left\{ \sum_{i=1}^k \lambda_i v_i \mid 0 \leq \lambda_i \leq 1 \right\},$$

a compact subset of  $\mathbb{R}^n$ . Since  $F \cap C \cap \mathbb{Z}^n$  is a discrete subset of  $F$ , it must be finite. Now we claim that  $F \cap C \cap \mathbb{Z}^n$  generates  $C \cap \mathbb{Z}^n$ . For this, let  $v \in C \cap \mathbb{Z}^n$  and write  $v = \sum_{i=1}^k r_i v_i$  with  $r_i \in \mathbb{R}_+$ . Now write each  $r_i = [r_i] + \{r_i\}$  where  $[r_i]$  and  $\{r_i\}$  are the integer and fractional parts of  $r_i$  respectively. Hence

$v = \sum_{i=1}^k [r_i]v_i + \sum_{i=1}^k \{r_i\}v_i$ . But  $\sum_{i=1}^k \{r_i\}v_i = v - \sum_{i=1}^k [r_i]v_i \in C \cap \mathbb{Z}^n$ . Since  $0 \leq \{r_i\} < 1$ , it follows that  $\sum_{i=1}^k \{r_i\}v_i \in F \cap C \cap \mathbb{Z}^n$ . This proves the lemma.  $\square$

Let us close this section by proving two standard facts for future use.

**Lemma 2.5.4.** (i) *Any finite dimensional vector space over an infinite field cannot be expressed as a finite union of proper subspaces.*

(ii) *If a cone  $C$  in  $\mathbb{R}^n$  satisfies  $C \subseteq \bigcup_1^m W_i$  for subspaces  $W_i \subseteq \mathbb{R}^n$  then  $C \subseteq W_i$  for some  $i$ . In particular, the subspace generated by  $C$  is contained in  $W_i$ .*

*Proof.* (i). Assume to the contrary that  $V$  is a finite dimensional vector space over an infinite field  $\mathbb{K}$  so that  $V = \bigcup_{i=1}^m W_i$ , where  $W_i \subsetneq V$ . We can assume  $m$  minimal; so  $\bigcup_{j \neq i} W_j \subsetneq V$ . This allows us to pick  $w_i \in W_i \setminus \bigcup_{j \neq i} W_j$ . Since clearly  $m \geq 2$ , let's consider the infinite subset  $\{w_1 + kw_2 : k \in \mathbb{K}\}$  of  $V$ . At least two distinct elements, say  $w_1 + k_1w_2$  and  $w_1 + k_2w_2$ , belong to same subspace, say  $W_j$ , for some  $j$ . Hence  $w_2 = \frac{1}{k_1 - k_2}[(w_1 + k_1w_2) - (w_1 + k_2w_2)] \in W_j$ . Since  $w_2$  belongs only to  $W_2$ , we must have  $j = 2$ . But then  $w_1 + k_1w_2 \in W_j = W_2$ , whence  $w_1 \in W_2$ . This contradicts the choice of  $w_i$ , thereby proving part (i).

(ii). The above argument works with only minor modifications. Indeed, assume that  $C \subseteq \bigcup_1^m W_i$  and that  $m$  is minimal; so  $C$  is not contained in  $\bigcup_{j \neq i} W_j$  for any  $i$ . Our goal is to show that  $m = 1$ . Suppose that  $m \geq 2$ . Pick  $w_i \in C \setminus \bigcup_{j \neq i} W_j$ ; so  $w_i \in W_i$ . Consider the infinite subset  $\{w_1 + rw_2 : r \in \mathbb{R}_+\}$  of  $C$  and argue exactly as above to reach a contradiction.  $\square$

## 2.6 Multiplicative Actions, Again

We review the setting of multiplicative actions as introduced in §1.4 and illustrate it by discussing some examples.

Let  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  be a finite integral matrix group. Then  $\mathcal{G}$  acts on column vectors ( $n \times 1$  matrices) from  $\mathbb{Z}^n$ ,  $\mathbb{Q}^n$  or  $\mathbb{R}^n$  by ordinary matrix multiplication. Recall that every element of the group algebra  $\mathbb{K}[\mathbf{A}]$  of the lattice  $\mathbb{Z}^n$  can be uniquely written in the form

$$\sum_{a \in \mathbb{Z}^n} k_a \mathbf{x}^a \quad \text{with } k_a \in \mathbb{K} \text{ almost all zero.}$$

Here,  $\mathbf{A} = \{\mathbf{x}^a \mid a \in \mathbb{Z}^n\}$  is the canonical  $\mathbb{K}$ -basis of  $\mathbb{K}[\mathbf{A}]$ . Putting

$$x_i = \mathbf{x}^{e_i} ,$$

where  $e_i \in \mathbb{Z}^n$  is the basis element of  $\mathbb{Z}^n$  with 1 in the  $i^{\text{th}}$  component and 0s elsewhere, the group algebra  $\mathbb{K}[\mathbf{A}]$  becomes the Laurent polynomial algebra in the variables  $x_i$ :

$$\mathbb{K}[\mathbf{A}] = \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] .$$

The  $\mathcal{G}$ -action on  $\mathbb{Z}^n$  gives rise to an action by  $\mathbb{K}$ -algebra automorphism on  $\mathbb{K}[\mathbf{A}]$  as follows:

$$\mathcal{G} \times \mathbb{K}[\mathbf{A}] \longrightarrow \mathbb{K}[\mathbf{A}] : (g, \sum_{a \in \mathbb{Z}^n} k_a \mathbf{x}^a) \mapsto \sum_{a \in \mathbb{Z}^n} k_a \mathbf{x}^{g \cdot a} .$$

We will use the notation  $g(f)$  or  $g \cdot f$  for the image of  $f \in \mathbb{K}[\mathbf{A}]$  under  $g \in \mathcal{G}$ . The following example illustrates this action.

**Example 2.6.1.**  $\mathbf{S} = \mathbb{K}[x^{\pm 1}, y^{\pm 1}]$ . Note here that  $\mathbb{Z}^2 \cong \langle x^{\pm 1}, y^{\pm 1} \rangle_{\text{mon}}$  via  $(1, 0) \mapsto x$ ,  $(0, 1) \mapsto y$ . In general,  $(a, b) \mapsto x^a y^b$ . Now let  $g = \begin{pmatrix} 2 & -5 \\ -3 & 8 \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ . We calculate the images of  $x$ ,  $y$ , and  $5x^2y^{-3} + 7xy^4 - 12$  under the action of  $g$ :

$$g(x) \leftrightarrow g((1, 0)) = (2, -3) \leftrightarrow x^2y^{-3}$$

$$g(y) \leftrightarrow g((0, 1)) = (-5, 8) \leftrightarrow x^{-5}y^8$$

$$\begin{aligned} g(5x^2y^{-3} + 7xy^4 - 12) &= 5g(x^2)g(y^{-3}) + 7g(x)g(y^4) - 12 \\ &= 5g(x)^2g(y)^{-3} + 7g(x)g(y)^4 - 12 \\ &= 5(x^2y^{-3})^2(x^{-5}y^8)^{-3} + 7(x^2y^{-3})(x^{-5}y^8)^4 - 12 \\ &= 5x^{19}y^{-30} + 7x^{-18}y^{29} - 12 \end{aligned}$$



**Notation:** The following notations will be used henceforth. The group algebra  $\mathbb{K}[A]$  (or Laurent polynomial algebra) will be denoted by  $\mathbb{S}$ ; so

$$\mathbb{S} = \mathbb{K}[A] = \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] .$$

Throughout,  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  will be a finite group acting multiplicatively on  $\mathbb{S}$ . The subalgebra of all Laurent polynomials that are invariant under the  $\mathcal{G}$ -action is known as *algebra of multiplicative invariants*; it will be denoted by

$$\mathbb{R} := \mathbb{S}^{\mathcal{G}} .$$

There is a standard method of producing invariant elements as follows. Given  $f \in \mathbb{S}$  we define the *orbit sum*,  $\vartheta(f)$ , of  $f$  to be the Laurent polynomial

$$\vartheta(f) = \sum_{f' \in \mathcal{O}_f} f' ,$$

where  $\mathcal{O}_f := \{g \cdot f : g \in \mathcal{G}\}$  is the  $\mathcal{G}$ -orbit of  $f$ ; see Definition 2.4.3. Observe that  $\vartheta(f)$  is certainly a  $\mathcal{G}$ -invariant element. The most important orbit sums are those where  $f = \mathbf{x}^a \in \mathbb{A}$  is a monomial. In this case, we will usually write  $\vartheta(a)$  instead of  $\vartheta(\mathbf{x}^a)$ . It is easily seen that

$$\mathbb{R} = \bigoplus_{a \in \mathcal{G} \backslash \mathbb{A}} \mathbb{K} \vartheta(a) ,$$

where  $\mathcal{G} \backslash \mathbb{A}$  denotes any transversal for the  $\mathcal{G}$ -orbits in  $\mathbb{A}$ .

**Example 2.6.2.** Let  $\mathcal{S}_n$  be the symmetric group of all permutations on the set  $\{1, \dots, n\}$ , let  $\{e_i\}_1^n$  denote the standard basis of  $\mathbb{Z}^n$  and put  $x_i = \mathbf{x}^{e_i} \in \mathbb{S} = \mathbb{K}[A]$ , as above. Then  $\mathcal{S}_n$  acts on  $\mathbb{Z}^n$  via  $s(e_i) = e_{s(i)}$  ( $s \in \mathcal{S}_n$ ) and this action gives rise to the following action on  $\mathbb{S}$ :

$$s(x_i) = x_{s(i)} \quad (s \in \mathcal{S}_n) .$$

The orbit sum of the monomial  $\mathbf{x}^{e_1 + \dots + e_i} = x_1 x_2 \dots x_i \in \mathbb{S}$  is the  $i^{\text{th}}$  elementary symmetric function

$$\sigma_i = \sum_{j_1 < \dots < j_i} x_{j_1} x_{j_2} \dots x_{j_i} ;$$

see Example 1.3.1. In particular,  $\sigma_n = x_1 x_2 \dots x_n$ . But observe that

$$S = \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] = \mathbb{K}[x_1, \dots, x_n][\sigma_n^{-1}] .$$

By Example 1.3.1,  $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{S}_n} = \mathbb{K}[\sigma_1, \dots, \sigma_n]$ . Therefore,

$$R = S^{\mathcal{S}_n} = \mathbb{K}[\sigma_1, \dots, \sigma_{n-1}, \sigma_n^{\pm 1}] ,$$

a mixed Laurent polynomial algebra in  $n$  variables, with 1 variable inverted.

## 2.7 Fundamental Domains

We recall the notion of a fundamental domain; it was already briefly mentioned in §2.4.

**Definition 2.7.1.** *Suppose a group  $\mathcal{G}$  acts on a set  $E$ . We call a subset  $F \subseteq E$  a fundamental domain for the action if each  $\mathcal{G}$ -orbit in  $E$  intersects  $F$  in exactly one point. This is equivalent to the following two conditions:*

- (a) *For every  $v \in E$ , there exists  $g \in \mathcal{G}$  such that  $g \cdot v \in F$ , and*
- (b) *If some  $v_1, v_2 \in F$  and  $g \in \mathcal{G}$  satisfy  $v_1 = g \cdot v_2$  then  $v_1 = v_2$ .*

**Lemma 2.7.2.** *let  $\mathcal{G}$  be a finite group acting by automorphisms on a finite dimensional vector space  $V$  and let  $F$  be a fundamental domain for the  $\mathcal{G}$ -action. Then  $\dim(F) = \dim(V)$ , where  $\dim(F)$  denotes the dimension of the subspace of  $V$  that is generated by  $F$ .*

*Proof.* Assume to the contrary that  $\dim(F) < \dim(V)$ . Then, since  $V = \bigcup_{g \in \mathcal{G}} g(F)$  and  $\dim(F) = \dim(g(F))$ , it follows that  $V$  is a finite union of proper subspaces, contradicting Lemma 2.5.4.  $\square$

### 2.7.1 Term Orders

A partial ordering on a set  $S$  is a relation, denoted by  $\geq$ , satisfying:

- (i)  $a \geq a$  for all  $a \in S$  (reflexive property)
- (ii) If  $a \geq b$  and  $b \geq a$  then  $a = b$  (antisymmetric property)
- (iii) If  $a \geq b$  and  $b \geq c$  then  $a \geq c$  (transitive property)

If, in addition, the partial ordering satisfies the additional property;

- (iv) For any  $a, b \in S$  either  $a \geq b$  or  $b \geq a$

then we call the partial order a linear ordering (or total ordering). We will be primarily interested in certain linear orderings on  $\mathbb{R}^n$  that are compatible with addition and scalar multiplication. Explicitly, we will assume that our ordering of  $\mathbb{R}^n$  also satisfies the following conditions:

- (v)  $a \geq b \Rightarrow a + c \geq b + c$  for all  $c \in \mathbb{R}^n$ ;
- (vi)  $a \geq b \Rightarrow ra \geq rb$  for all  $r \in \mathbb{R}_+$ .

Such a linear order of  $\mathbb{R}^n$  will be called a *term order*. There are several term orderings on  $\mathbb{R}^n$ ; here is a particularly simple and well-known example:

**Lexicographic Ordering:** Let  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{R}^n$ . The lexicographic (dictionary) order on  $\mathbb{R}^n$ , denoted  $\succeq_{lex}$ , is defined by  $(a_1, \dots, a_n) \succeq_{lex} (b_1, \dots, b_n)$  if and only if the first non zero entry of  $(a_1, \dots, a_n) - (b_1, \dots, b_n) = (a_1 - b_1, \dots, a_n - b_n)$  is positive. For example, if  $\alpha = (-1, 7, 50)$  and  $\beta = (-1, 8, 0)$  then  $\beta - \alpha = (0, 1, -50)$ . Hence,  $\beta \succeq_{lex} \alpha$ . One can easily see that  $\succeq_{lex}$  is indeed a term order on  $\mathbb{R}^n$ .

**Notation:** In the following  $\succeq$  will denote an arbitrary term ordering of  $\mathbb{R}^n$ .

**Definition 2.7.3.** Given a finite subgroup  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  acting on  $\mathbb{Z}^n$  and  $\mathbb{R}^n$  by matrix multiplication, as before, we define:

- (i)  $A^\succ(\mathcal{G}) := \{a \in \mathbb{Z}^n : a \succeq g \cdot a \ \forall g \in \mathcal{G}\}$ ,
- (ii)  $X^\succ(\mathcal{G}) := \{v \in \mathbb{R}^n : v \succeq g \cdot v \ \forall g \in \mathcal{G}\}$

If no confusion arises we will suppress the  $\mathcal{G}$  and simply write  $A^\succ$  or  $X^\succ$  respectively.

**Definition 2.7.4.** *A submonoid  $S$  of  $\mathbb{Z}^n$  is said to be saturated if  $ma \in S$  for  $a \in \mathbb{Z}^n$  and  $m \in \mathbb{N}$  implies that  $a \in S$ .*

**Lemma 2.7.5.** *(i)  $\mathbb{Z}^n \cap X^\succ = A^\succ$ . The sets  $A^\succ$  and  $X^\succ$  are fundamental domains for the  $\mathcal{G}$ -action on  $\mathbb{Z}^n$  and  $\mathbb{R}^n$  respectively. Moreover,  $A^\succ$  is a saturated submonoid of  $\mathbb{Z}^n$ .*

*(ii)  $\mathbb{Q}_+A^\succ$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{Q}^n$ . Furthermore  $\mathbb{Q}^n \cap \text{Pos}(A^\succ) \subseteq \mathbb{Q}^n \cap X^\succ = \mathbb{Q}_+A^\succ$ ; (recall that  $\text{Pos}(A^\succ) := \mathbb{R}_+A^\succ$ ).*

*(iii)  $\text{Pos}(A^\succ)$  is a polyhedral cone if and only if  $A^\succ$  is a finitely generated semigroup. In this case it is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$ .*

*Proof.* (i). The equality  $\mathbb{Z}^n \cap X^\succ = A^\succ$  is immediate from the definition since the set  $\mathbb{Z}^n \cap X^\succ = \{a \in \mathbb{Z}^n : a \succeq g \cdot a, \forall g \in \mathcal{G}\} = A^\succ$ . Next the fact that  $A^\succ$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{Z}^n$  is also clear from the definition of  $A^\succ$ : every  $\mathcal{G}$ -orbit in  $\mathbb{Z}^n$  has a unique largest element with respect to  $\succeq$ , and these largest elements form the set  $A^\succ$ . Similar argument proves that  $X^\succ$  is a fundamental domain for the  $\mathcal{G}$  action on  $\mathbb{R}^n$ .

To complete (i) we also show  $A^\succ$  is a saturated submonoid of  $\mathbb{Z}^n$ : Let  $a, b \in A^\succ$  and  $g \in \mathcal{G}$  then  $a + b \succeq g \cdot a + g \cdot b = g \cdot (a + b)$ . Therefore,  $a + b \in A^\succ$ . Since, clearly,  $0 \in A^\succ$ , this shows that  $A^\succ$  is a submonoid of  $\mathbb{Z}^n$ . In order to show that  $A^\succ$  is saturated, note that for any  $v, w \in \mathbb{R}^n$  and  $m \in \mathbb{N}$ , we have  $v \succeq w \Leftrightarrow mv \succeq mw$ . Thus, if  $a \in \mathbb{Z}^n$  satisfies  $ma \in A^\succ$  then  $ma \succeq g \cdot (ma) = m(g \cdot a)$  for all  $g \in \mathcal{G}$ , and hence  $a \succeq g(a)$ . Therefore,  $a \in A^\succ$ , proving that  $A^\succ$  is saturated.

(ii). We check conditions (a) and (b) in Definition 2.7.1 for  $\mathbb{Q}_+A^\succ$ . For (a), let  $\alpha \in \mathbb{Q}^n$  and choose  $m \in \mathbb{N}$  such that  $m\alpha \in \mathbb{Z}^n$ . By (i), there exists  $g \in \mathcal{G}$  such that  $g \cdot (m\alpha) \in A^\succ$ . Hence,  $g \cdot \alpha = \frac{1}{m}g \cdot (m\alpha) \in \mathbb{Q}_+A^\succ$ , which proves (a).

To check (b), let  $\alpha, \beta \in \mathbb{Q}_+ A^\succ$  such that  $\alpha = g\beta$  for some  $g \in \mathcal{G}$ . Then choose an  $m \in \mathbb{N}$  such that  $m\alpha, m\beta \in A^\succ$ . Now,  $g \cdot m\beta = m(g \cdot \beta) = m\alpha \in A^\succ$ . Therefore,  $m\beta = m\alpha$ , since  $A^\succ$  is a fundamental domain. This in turn implies that  $\alpha = \beta$ , as required. This shows that  $\mathbb{Q}_+ A^\succ$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{Q}^n$ .

Now we show  $\mathbb{Q}^n \cap \mathbb{R}_+ A^\succ \subseteq \mathbb{Q}^n \cap X^\succ = \mathbb{Q}_+ A^\succ$ : From the definition of  $\succeq$  it is clear that  $\mathbb{R}_+ A^\succ \subseteq X^\succ$  and hence the inclusion  $\mathbb{Q}^n \cap \mathbb{R}_+ A^\succ \subseteq \mathbb{Q}^n \cap X^\succ$ . It is also evident that  $\mathbb{Q}_+ A^\succ \subseteq X^\succ$ , but since  $\mathbb{Q}_+ A^\succ \subseteq \mathbb{Q}^n$  then we have the inclusion  $\mathbb{Q}_+ A^\succ \subseteq \mathbb{Q}^n \cap X^\succ$ . Conversely the set  $\mathbb{Q}^n \cap X^\succ = \{v \in \mathbb{Q}^n : v \succeq g \cdot v, \forall g \in \mathcal{G}\}$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{Q}^n$ . But since we also proved that  $\mathbb{Q}_+ A^\succ$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{Q}^n$  we have inclusion of fundamental domains  $\mathbb{Q}_+ A^\succ \subseteq \mathbb{Q}^n \cap X^\succ$ . This forces the equality  $\mathbb{Q}_+ A^\succ = \mathbb{Q}^n \cap X^\succ$  completing the proof of (ii).

(iii). First lets start with  $A^\succ$  is finitely generated semigroup then it trivially follows that  $Pos(A^\succ)$  is a polyhedral cone. Conversely, if  $Pos(A^\succ)$  is polyhedral (and hence integral polyhedral) then the semigroup  $Pos(A^\succ) \cap \mathbb{Z}^n$  is finitely generated by Gordan's Lemma (Lemma 2.5.3). Furthermore by (i) above and the fact that  $Pos(A^\succ) \subseteq X^\succ$  we have,

$$X^\succ \cap \mathbb{Z}^n = A^\succ \subseteq Pos(A^\succ) \cap \mathbb{Z}^n \subseteq X^\succ \cap \mathbb{Z}^n$$

Hence we have equality  $Pos(A^\succ) \cap \mathbb{Z}^n = A^\succ$ . Hence  $A^\succ$  is finitely generated.

Continuing with our assumption that  $Pos(A^\succ)$  is polyhedral, we check conditions (a) and (b) in Definition 2.7.1. To prove (a), let  $v \in \mathbb{R}^n$  and let  $\{v_m\}_{m=1}^\infty$  be a sequence in  $\mathbb{Q}^n$  converging to  $v$ . By (ii) we know that, for each  $m$ , there exist  $g_m \in \mathcal{G}$  such that  $g_m \cdot v_m \in \mathbb{Q}_+ A^\succ$ . But since  $\mathcal{G}$  is finite, there is a subsequence  $\{m_j\}_{j=1}^\infty$  such that  $\{g_{m_j}\}_{j=1}^\infty$  is fixed element of  $\mathcal{G}$ , say  $g_0$ . Thus,  $g_0 \cdot v_{m_j} \in Pos(A^\succ)$  and  $\lim_{j \rightarrow \infty} (g_0 \cdot v_{m_j}) = g_0 \cdot (\lim_{j \rightarrow \infty} v_{m_j}) = g_0 \cdot v$ . Since  $Pos(A^\succ)$  is closed, by Lemma 2.5.2, we conclude that  $g_0 \cdot v \in Pos(A^\succ)$ . Thus, condition (a) is proved.

For (b), suppose that  $v_1 = g \cdot v_2$  for some  $v_1, v_2 \in Pos(A^\succ)$  and  $g \in \mathcal{G}$ . Thus,  $v_1 \in Pos(A^\succ) \cap g[Pos(A^\succ)]$ . By part (ii), every rational point in

$Pos(A^\succ) \cap g[Pos(A^\succ)]$  is fixed by  $g$ . Moreover,  $Pos(A^\succ) \cap g[Pos(A^\succ)]$  is an integral cone (see, e.g., [Re03, Lemma 2.1(a)]), and so the rational points in  $Pos(A^\succ) \cap g[Pos(A^\succ)]$  are dense in  $Pos(A^\succ) \cap g[Pos(A^\succ)]$ . Since  $g$  is continuous, we conclude that every point of  $Pos(A^\succ) \cap g[Pos(A^\succ)]$  is fixed by  $g$ . In particular,  $v_1 = g \cdot v_1 = v_2$ .  $\square$

Some portions of (i) and (iii) are also proved, in a slightly different way, in [Re03, Lemmas 2.6 and 2.8].

## 2.7.2 SAGBI Bases

In the polynomial algebra  $\mathbb{K}[x]$  of one variable, the degree of a polynomial  $f \in \mathbb{K}[x]$  is the maximum exponent  $m \in \mathbb{Z}_+$  of monomials in  $f$ . This idea can be generalized to Laurent polynomial algebras in  $n$ -variables as follows. Recall that  $\succeq$  denotes a fixed term order on  $\mathbb{R}^n$  (and hence on  $\mathbb{Z}^n$ ).

**Definition 2.7.6.** *Given  $0 \neq f = \sum_{a \in \mathbb{Z}^n} k_a x^a \in \mathbb{S} := \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ , we define the initial degree of  $f$ , denoted  $\mathcal{I}(f)$ , to be the largest exponent  $a \in \mathbb{Z}^n$  (with respect to  $\succeq$ ) such that  $k_a \neq 0$ .*

For any subset  $T \subseteq \mathbb{S}$  we put

$$\mathcal{I}(T) = \{\mathcal{I}(f) : 0 \neq f \in T\}.$$

**Remark 2.7.7.** *It is easy to see that  $\mathcal{I}(1) = 0$  and*

$$\mathcal{I}(f_1 \cdot f_2) = \mathcal{I}(f_1) + \mathcal{I}(f_2)$$

for all  $0 \neq f_1, f_2 \in \mathbb{S}$ . In other words,

$$\mathcal{I} : (\mathbb{S} \setminus \{0\}, \cdot) \longrightarrow (\mathbb{Z}^n, +)$$

is a monoid homomorphism. In particular, if  $T$  is a subalgebra (with 1) of  $\mathbb{S}$  then  $\mathcal{I}(T)$  is a submonoid of  $\mathbb{Z}^n$ .

We can extend the above definitions verbatim to the group algebra  $S_{\mathbb{R}} = \mathbb{K}[A_{\mathbb{R}}]$ , where we have put  $A_{\mathbb{R}} = \{\mathbf{x}^v : v \in \mathbb{R}^n\}$ ; the only difference is that initial degrees no longer need to belong to  $\mathbb{Z}^n$  but to  $\mathbb{R}^n$ .

**Proposition 2.7.8.** *Let  $T$  be a subalgebra of  $S$  and let  $\{f_{\lambda}\}_{\lambda \in \Lambda}$  be a family of elements of  $T$  such that the monoid  $\mathcal{S}(T)$  is generated by  $\{\mathcal{S}(f_{\lambda})\}_{\lambda \in \Lambda}$ . If  $\mathcal{S}(T)$  is well ordered under  $\succ$  then  $T$  is generated by  $\{f_{\lambda}\}_{\lambda \in \Lambda}$ , that is,  $T = \mathbb{K}[f_{\lambda} : \lambda \in \Lambda]$ .*

*Proof.* Let  $0 \neq \tau_1 \in T$ . Our goal is to write  $\tau_1$  as a polynomial in  $\{f_{\lambda}\}_{\lambda \in \Lambda}$ . Start by writing

$$\mathcal{S}(\tau_1) = d_1 \mathcal{S}(f_{\lambda_1}) + \dots + d_r \mathcal{S}(f_{\lambda_r}); \quad d_i \in \mathbb{N}$$

Let  $k \in \mathbb{K}$  be such that the leading term of  $k\tau_1$  equals the leading term of  $\prod_{i=1}^r (f_{\lambda_i})^{d_i}$  and put  $\tau_2 = k\tau_1 - \prod_{i=1}^r (f_{\lambda_i})^{d_i} \in T$ . Then either  $\tau_2 = 0$ , in which case we are done, or  $\mathcal{S}(\tau_1) \succ \mathcal{S}(\tau_2)$ . In the later case, we replace  $\tau_1$  by  $\tau_2$  and proceed inductively to construct a decreasing sequence  $\mathcal{S}(\tau_1) \succ \mathcal{S}(\tau_2) \succ \dots$  with  $\tau_i \in T$ . Since  $\mathcal{S}(T)$  is well ordered the above sequence terminates and hence the process must stop, proving our claim.  $\square$

The above proof yields an algorithm for writing an element of  $T$  in terms of  $\{f_{\lambda}\}_{\lambda \in \Lambda}$ , called *subduction algorithm*. It is analogous to expressing an element of an ideal in terms of Gröbner bases. For this reason, the set  $\{f_{\lambda} : \lambda \in \Lambda\}$  is called a “SAGBI” bases of  $T$ . The term SAGBI stands for “*Subalgebra Analogue to Gröbner Bases for Ideals*”. Both terms, SAGBI bases and subduction algorithm were introduced by Robbiano and Sweedler in [RS90]. If  $\Lambda$  is finite, i.e.,  $\mathcal{S}(T)$  is finitely generated, then we say that  $T$  has a *finite SAGBI basis*.

We finish this chapter by determining the monoid  $\mathcal{S}(R)$  for multiplicative invariant algebras  $R = \mathbb{K}[A]^{\mathcal{G}}$ . Recall the definition of  $A^{\succ}$  from Definition 2.7.3. This following Lemma is identical with [Re03, Lemma 2.6(a)].

**Lemma 2.7.9.** *Let  $\mathbb{K}[A]^{\mathcal{G}}$  denote the algebra of  $\mathcal{G}$ -invariants of  $\mathbb{K}[A]$ . Then*

$$\mathcal{S}(\mathbb{K}[A]^{\mathcal{G}}) = A^{\succ} .$$

*Proof.* Let  $a \in \mathcal{I}(\mathbb{K}[\mathbf{A}]^{\mathcal{G}})$ ; so  $a = \mathcal{I}(f)$  for some  $0 \neq f \in \mathbb{K}[\mathbf{A}]^{\mathcal{G}}$ . Then  $a \in \text{Supp}(f)$  and hence  $g \cdot a \in \text{Supp}(f)$  for each  $g \in \mathcal{G}$ . But since  $a = \mathcal{I}(f)$  we have  $a \succeq g \cdot a$  for all  $g \in \mathcal{G}$ . Therefore  $a \in A^{\succ}$ . Conversely let  $a \in A^{\succ}$  then the orbit sum  $\vartheta(a)$  is a nonzero element of  $\mathbb{K}[\mathbf{A}]^{\mathcal{G}}$  and  $\mathcal{I}(\vartheta(a)) = a$ . Hence  $a \in \mathcal{I}(\mathbb{K}[\mathbf{A}]^{\mathcal{G}})$ . This proves the Lemma.  $\square$



# CHAPTER 3

## REFLECTION GROUPS

In this chapter, we focus on multiplicative actions of reflection groups. The basic definitions and concepts pertaining to reflections and reflection groups are recalled in §3.2. In §3.3, we will show that any finite group  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{R})$  must be a reflection group if its natural action on  $\mathbb{R}^n$  has a fundamental domain that is a polyhedral cone. In particular, if  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  and the cone  $X^\succ$  in Definition 2.7.3 is polyhedral then  $\mathcal{G}$  is a reflection group. The converse also holds and is proved in §3.4: for any finite reflection group  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$ , the cone  $X^\succ$  is polyhedral. Finally, in §3.5, we consider finite reflection groups  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  that act effectively on  $\mathbb{Z}^n$ , that is,  $(\mathbb{Z}^n)^\mathcal{G} = \{0\}$ . We show that, in this case, the cone  $X^\succ$  is actually simplicial. We will also prove a number of technicalities on reflections for later use.

Except for the result on simplicial cones, the main results in this chapter are all due to Reichstein [Re03].

### 3.1 Basic Concepts

**Definition 3.1.1.** *A automorphism  $\phi$  of a finite dimensional vector space  $V$  is called a pseudo-reflection if  $\mathrm{Id}_V - \phi$  has rank 1, that is,  $\{v - \phi(v) : v \in V\}$  is*

a 1-dimensional subspace of  $V$ . If further  $\phi^2 = \text{Id}_V$ , we call  $\phi$  a reflection. A group of automorphisms of  $V$  is said to be a reflection group if it is generated by reflections.

Geometrically, a reflection is an invertible linear transformation leaving some hyperplane pointwise fixed and sending any vector orthogonal to that hyperplane to its negative. In general, there are pseudo-reflections that are not reflections. For example,  $\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{C})$  is a pseudo-reflection but not a reflection. In our study, we consider finite groups  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  acting on the lattice  $\mathbf{A} \cong \mathbb{Z}^n$ . But trivially this action is extendable to an action on the vector spaces  $\mathbb{Q}^n$  or  $\mathbb{R}^n$ . Therefore we say  $g \in \text{GL}_n(\mathbb{Z})$  is a reflection or pseudo-reflection on the lattice  $\mathbf{A}$  depending on whether it is reflection or pseudo-reflection on  $\mathbb{R}^n$  or, equivalently, on  $\mathbb{Q}^n$ . The following Proposition shows that reflections and pseudo-reflections in  $\mathcal{G}$  are the same.

**Proposition 3.1.2.** *Pseudo-reflections of finite order on  $\mathbb{R}^n$  are reflections.*

*Proof.* Let  $\sigma$  be a pseudo-reflection on  $V = \mathbb{R}^n$  and put  $\mathcal{G} = \langle \sigma \rangle_{gp}$ . Then  $\mathcal{G}$  acts on  $V$  and the hyperplane

$$\mathcal{H}_\sigma = \ker(\sigma - \text{Id}_V)$$

is stable under the  $\mathcal{G}$ -action. Since  $\mathbb{R}$  has characteristic zero, we can apply Maschke's theorem: there exists a complement  $V''$  of  $V'$  stable under  $\mathcal{G}$ . But  $V''$  is 1-dimensional; so  $V'' = \mathbb{R}v$  for some  $v \in V$  with  $\sigma(v) = \lambda v$  ( $\lambda \in \mathbb{R}$ ). Hence the matrix of  $\sigma$  corresponding to a basis of  $V$  that consists of a basis of  $V'$  together with  $v$  is given by

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda \end{pmatrix}$$

But since  $\sigma$  is of finite order,  $\lambda$  must be of finite order. as well, and since  $\sigma$  is not identity then the only possibility for  $\lambda$  is  $-1$ . Thus,  $\sigma^2 = \text{Id}_V$  and so  $\sigma$  is a reflection.  $\square$



is a polyhedral cone. In particular, by Lemma 2.7.2, we have  $\dim X = n$ . Let  $\mathcal{F}_1, \dots, \mathcal{F}_m$  denote the facets of  $X$  and write  $\mathcal{F}_i = X \cap v_i^\perp$  for suitable  $v_i \in X^\vee$ . We identify the dual  $(\mathbb{R}^n)^*$  with  $\mathbb{R}^n$  by means of a fixed a symmetric,  $\mathcal{G}$ -invariant, positive definite bilinear form  $\langle \cdot, \cdot \rangle$  on  $\mathbb{R}^n$ , as in equation (3.1). So  $X^\vee \subseteq \mathbb{R}^n$ . Now define a reflection,  $\sigma_i$ , to be the orthogonal transformation of  $\mathbb{R}^n$  sending  $v_i \mapsto -v_i$  and fixing the hyperplane  $\mathcal{H}_i := v_i^\perp$  orthogonal to  $v_i$ . Note also that  $\mathcal{F}_i \subseteq \mathcal{H}_i$ , and so  $\mathcal{H}_i$  is the space generated by  $\mathcal{F}_i$ , since  $\dim(\mathcal{F}_i) = n - 1$ .

The following Theorem is identical with [Re03, Proposition 4.1].

**Theorem 3.2.1 (Reichstein [Re03]).** *Let  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{R})$  be a finite group such that there is a fundamental domain,  $X$ , for the natural  $\mathcal{G}$ -action on  $\mathbb{R}^n$  which is a polyhedral cone. Then  $\mathcal{G}$  is a reflection group. Specifically, using the above notations, the reflections  $\sigma_1, \dots, \sigma_m$  generate  $\mathcal{G}$ .*

*Proof.* We begin by proving the following claim which holds for any fundamental domain for the action of  $\mathcal{G}$ :

*Claim 1:* The boundary  $\partial X$  of  $X$  is contained in  $Y := \bigcup_{g(X) \neq X} g(X)$ .

Suppose to the contrary that there is an  $x \in \partial X \setminus Y$ . Since  $X$  is closed, by Lemma 2.5.2(ii), each set  $g(X)$  is also closed, and hence so is  $Y$ . Therefore, there exists a neighborhood  $B$  of  $x$  such that  $B \cap Y = \emptyset$ . On the other hand, since  $x \in \partial X$ , there exists  $b \in B \setminus X$ . Hence  $b \notin Y \cup X$ . But this is a contradiction since  $X$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$ , and hence  $Y \cup X = \mathbb{R}^n$ . This proves Claim 1.

Next, using the notations introduced above, we prove

*Claim 2:* The reflections  $\sigma_1, \dots, \sigma_m$  all belong to  $\mathcal{G}$ .

To prove this, pick a point  $p$  in some facet  $\mathcal{F}_i$  of  $X$ ; so  $p \in \partial X$ . By Claim 1, there exists some  $1 \neq g \in \mathcal{G}$  such that  $p \in g(X)$ . Therefore,  $p \in X$  and  $g^{-1}(p) \in X$ . But as  $X$  is a fundamental domain, this is possible only if

$g^{-1}(p) = p$ . Since  $p \in \mathcal{F}_i$  was arbitrarily chosen we have proved that

$$\mathcal{F}_i \subseteq \bigcup_{1 \neq g \in \mathcal{G}} \ker(g - 1) .$$

By Lemma 2.5.4(ii), it follows that  $\mathcal{H}_i \subseteq \ker(g_i - 1)$  for some  $1 \neq g_i \in \mathcal{G}$ . Thus,  $g_i$  is a non-identity orthogonal transformation of  $\mathbb{R}^n$  that fixes  $\mathcal{H}_i$  point-wise. Consequently,  $g_i$  maps  $\mathcal{H}_i^\perp = \mathbb{R}v_i$  to itself. Since  $g_i$  has finite order  $\neq 1$ , the only possibility for  $g_i(v_i)$  is  $-v_i$ . Therefore  $g_i = \sigma_i$ , whence  $\sigma_i \in \mathcal{G}$ . Thus, Claim 2 is proved.

Now let  $\mathcal{G}_0$  be the subgroup of  $\mathcal{G}$  generated by  $\{\sigma_1, \dots, \sigma_m\}$ . Since  $X$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$ , Lemma 2.5.4(i) implies that

$$X \not\subseteq \bigcup_{1 \neq g \in \mathcal{G}} \ker(g - 1) .$$

Hence, there exists a point  $p \in X$  such that  $g(p) \neq p$  for all  $1 \neq g \in \mathcal{G}$ . In particular,  $p \notin g_0(\mathcal{H}_i)$  for any  $g_0 \in \mathcal{G}_0$  and  $i = 1, \dots, m$ . Indeed, if  $p = g_0(h_i)$  for some  $h_i \in \mathcal{H}_i$  then  $g_0\sigma_i g_0^{-1}(p) = p$  which is a contradiction since  $g_0\sigma_i g_0^{-1}$  is not the identity. Now consider the closed chamber

$$\mathcal{C} = \bigcap_{g_0, i} g_0(\mathcal{H}_i)^+ ,$$

where  $g_0$  runs over all elements of  $\mathcal{G}_0$ ,  $i \in \{1, \dots, m\}$ , and  $g_0(\mathcal{H}_i)^+$  denotes the closed half space bounded by  $g_0(\mathcal{H}_i)$  which contains the point  $p$ . We have  $\mathcal{C} \subseteq X$ , since  $X = \bigcap_{i=1}^m \mathcal{H}_i^+$ . By [Bo68, Theorem V.3.3.2],  $\mathcal{C}$  is a fundamental domain for the action of  $\mathcal{G}_0$  on  $\mathbb{R}^n$ . Hence, for any  $g \in \mathcal{G}$ , there exists  $g_0 \in \mathcal{G}_0$  and  $c \in \mathcal{C}$  such that  $g(p) = g_0(c)$ . Thus,  $g_0^{-1}g(p) = c \in X$  and  $p \in X$ . This forces  $g_0^{-1}g(p) = p$  and so  $g = g_0 \in \mathcal{G}_0$ . Since this statement is true for arbitrary  $g \in \mathcal{G}$ , it follows that  $\mathcal{G} = \mathcal{G}_0$ . This completes the proof of the Theorem.  $\square$

Recall the definition of the cone  $X^\succ$  from Definition 2.7.3.

**Corollary 3.2.2.** *Let  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  be finite and assume that the cone  $X^\succ$  is polyhedral. Then  $\mathcal{G}$  is a reflection group.*

*Proof.* By Lemma 2.7.5(iii), our hypothesis on  $X^\succ$  implies that  $X^\succ$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$ .  $\square$

In this section, let  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  be a finite group. Our goal is to prove the converse to Corollary 3.2.2: if  $\mathcal{G}$  is a reflection group then the cone  $X^\succ$  is polyhedral.

Let  $\sigma \in \mathcal{G}$  be a reflection. Then  $\ker_{\mathbb{Z}^n}(\sigma + \mathrm{Id}) = \{a \in \mathbb{Z}^n : \sigma(a) = -a\}$  is of rank 1, and so it has two possible generators which differ by a  $\pm$ -sign. We let  $e_\sigma$  denote the generator of  $\ker_{\mathbb{Z}^n}(\sigma + \mathrm{Id})$  satisfying  $e_\sigma \succ (0, \dots, 0)$ . Thus,

$$\sigma(e_\sigma) = -e_\sigma . \quad (3.2)$$

The linear form on  $\mathbb{R}^n$  that is associated with  $e_\sigma$  will be denoted by  $l_\sigma$ ; so

$$l_\sigma : \mathbb{R}^n \rightarrow \mathbb{R} , \quad l_\sigma(v) = \langle v, e_\sigma \rangle . \quad (3.3)$$

Note that  $l_\sigma$  is  $\mathbb{Z}$ -valued on  $\mathbb{Z}^n$ , since the bilinear form  $\langle , \rangle$  in (3.1) is  $\mathbb{Z}$ -valued on  $\mathbb{Z}^n \times \mathbb{Z}^n$ . As in the proof of Proposition 3.1.2, we let

$$\mathcal{H}_\sigma = \ker(\sigma - \mathrm{Id}_V)$$

denote the hyperplane of  $\mathbb{R}^n$  that is fixed by  $\sigma$ . The following (standard) Lemma further explains the connections between  $\sigma$ ,  $l_\sigma$  and  $\mathcal{H}_\sigma$

**Lemma 3.2.3.** (i)  $\mathcal{H}_\sigma = \ker(l_\sigma) = \{v \in \mathbb{R}^n : \langle v, e_\sigma \rangle = 0\}$ ;

(ii) For all  $v \in \mathbb{R}^n$ ,  $\sigma(v) = v - 2 \frac{l_\sigma(v)}{\langle e_\sigma, e_\sigma \rangle} e_\sigma$ .

*Proof.* (i). The second equality in (i) is obvious. To prove the first equality, let  $v \in \mathcal{H}_\sigma$ . Then

$$l_\sigma(v) = \langle v, e_\sigma \rangle = \langle \sigma(v), \sigma(e_\sigma) \rangle = \langle v, -e_\sigma \rangle = - \langle v, e_\sigma \rangle .$$

Therefore,  $l_\sigma(v) = \langle v, e_\sigma \rangle = 0$  and so  $\mathcal{H}_\sigma \subseteq \ker(l_\sigma)$ . But  $\dim \mathcal{H}_\sigma = n - 1$  and, since  $l_\sigma$  is a nonzero linear form,  $\dim(\ker(l_\sigma)) = n - 1$ . Therefore, we must have  $\mathcal{H}_\sigma = \ker(l_\sigma)$ .

(ii). Both sides of the asserted formula are linear transformations of  $\mathbb{R}^n = \mathcal{H}_\sigma \oplus \mathbb{R}e_\sigma$ , and both are the identity on  $\mathcal{H}_\sigma$  (use part (i) for the right hand side) and send  $e_\sigma$  to  $-e_\sigma$ . Thus, the two transformations are the same.  $\square$

Recall the definition of  $X^\succ$  from Definition 2.7.3. The following result is an elaboration of [Re03, Proposition 3.1].

**Proposition 3.2.4 (Reichstein [Re03]).** *Let  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  be a finite reflection group. Then*

$$\begin{aligned} X^\succ &= \{v \in \mathbb{R}^n : v \succeq g(v) \text{ for all } g \in \mathcal{G}\} \\ &= \{v \in \mathbb{R}^n : v \succeq \sigma(v) \text{ for all reflections } \sigma \in \mathcal{G}\} \\ &= \{v \in \mathbb{R}^n : l_\sigma(v) \geq 0 \text{ for all reflections } \sigma \in \mathcal{G}\}. \end{aligned}$$

*Proof.* Clearly  $X^\succ = \{v \in \mathbb{R}^n : v \succeq g(v) \text{ for all } g \in \mathcal{G}\}$  is the definition of  $X^\succ$  and equality of  $\{v \in \mathbb{R}^n : v \succeq \sigma(v) \text{ for all reflections } \sigma \in \mathcal{G}\} = \{v \in \mathbb{R}^n : l_\sigma(v) \geq 0 \text{ for all reflections } \sigma \in \mathcal{G}\}$  follows from Lemma 3.2.3(ii) that  $v \succeq \sigma(v)$  is equivalent to  $l_\sigma(v) \geq 0$  for all reflections  $\sigma \in \mathcal{G}$ .

Moreover the inclusion  $\{v \in \mathbb{R}^n : v \succeq g(v) \text{ for all } g \in \mathcal{G}\} \subseteq \{v \in \mathbb{R}^n : v \succeq \sigma(v) \text{ for all reflections } \sigma \in \mathcal{G}\}$  is trivial. So it only remains to verify the reverse inclusion of above. For this put

$$\mathcal{H}_\sigma^+ = \{v \in \mathbb{R}^n : l_\sigma(v) \geq 0\} \quad \text{and} \quad C = \bigcap_{\sigma} \mathcal{H}_\sigma^+,$$

where  $\sigma$  runs over the reflections in  $\mathcal{G}$ . Thus,  $C$  is a cone in  $\mathbb{R}^n$  which is integral polyhedral, because the  $l_\sigma$  are finitely many linear forms that are  $\mathbb{Z}$ -valued on  $\mathbb{Z}^n$ ; see [Ew96, Theorem V.2.10(a)]. By Lemma 2.7.5(i)  $X^\succ$  is a fundamental domain for the  $\mathcal{G}$  action on  $\mathbb{R}^n$  hence  $\dim(X^\succ) = n$ . Now applying Lemma 2.5.4 it follows that  $X^\succ$  is not contained in a finite union of hyperplanes of  $\mathbb{R}^n$ . Since  $X^\succ \subseteq C$ , neither is  $C$ . Thus,

$$C_0 = \bigcap_{\sigma} \{v \in \mathbb{R}^n : l_\sigma(v) > 0\} \tag{3.4}$$

is nonempty and is a chamber for the collection of hyperplanes  $\mathcal{H}_\sigma$  of  $\mathbb{R}^n$ ; see [Bo68, V.3.1]. Consequently,  $C = \overline{C_0}$  (see [Bo68, V.1.3 formula (6)]) and  $C$  is a fundamental domain for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$ , by [Bo68, V.3.3, Theorem 2]. But since  $X^\succ$  is also a fundamental domain for the  $\mathcal{G}$ -action on

$\mathbb{R}^n$ , (Lemma 2.7.5), we have the following inclusion of fundamental domains,  $X^\succ \subseteq C = \bigcap_\sigma \mathcal{H}_\sigma^+$ . Hence they must be equal.  $\square$

**Corollary 3.2.5.** *If  $\mathcal{G}$  is a finite reflection group then  $X^\succ = \text{Pos}(A^\succ)$ .*

*Proof.* From the above Theorem we know that  $X^\succ = C$ , but since  $C$  is an integral polyhedral cone we have,  $C = \text{Pos}(x_1, \dots, x_s)$  for some  $x_i \in \mathbb{Z}^n$ ,  $i = 1, \dots, s$ . Now since  $x_i$  are clearly in  $A^\succ$  then  $C = \text{Pos}(\{x_1, \dots, x_s\}) \subseteq \text{Pos}(A^\succ)$ . But since  $\text{Pos}(A^\succ) \subseteq X^\succ$  we have the equality as desired.  $\square$

To summarize, we combine Theorem 3.2.4, Corollary 3.2.2 and Lemma 2.7.5(iii) into the following theorem.

**Theorem 3.2.6 (Reichstein [Re03]).** *Let  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  be a finite group. Then the following are equivalent:*

- (i)  $\mathcal{G}$  is a reflection group;
- (ii) the monoid  $A^\succ = \{a \in \mathbb{Z}^n : a \succeq g \cdot a \ \forall g \in \mathcal{G}\}$  is finitely generated;
- (iii) the cone  $X^\succ = \text{Pos}(A^\succ)$  is polyhedral.

We continue to assume that  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  is a finite reflection group. We will now focus on the case where  $\mathcal{G}$  acts *effectively* on  $\mathbb{Z}^n$ , i.e.,  $(\mathbb{Z}^n)^\mathcal{G} = 0$ . Our goal will be to show that, in this case, the cone  $X^\succ$  is actually a simplicial cone in the sense of the following definition.

**Definition 3.2.7.** *A polyhedral cone  $C \subseteq \mathbb{R}^n$  is called simplicial if it can be generated by linearly independent vectors in  $\mathbb{R}^n$ .*

**Lemma 3.2.8.** *Let  $C = \text{Pos}\{v_1, \dots, v_m\}$  be a simplicial cone in  $\mathbb{R}^n$ , where  $v_1, \dots, v_m$  are linearly independent. Then  $C$  has exactly  $m$  facets and  $m$  edges. In fact, the rays  $\mathbb{R}_+v_i$ ,  $i = 1, \dots, m$  are precisely the edges of  $C$ , and they also are the intersections of all different collections of  $m - 1$  facets.*

*If  $C$  is also an integral cone then we may choose all  $v_i \in \mathbb{Z}^n$ .*



*Proof.* Working inside the vector space that is generated by  $C$ , we may assume that  $m = n$ . Thus, by hypothesis,  $\{v_i\}_{i=1}^n$  is a basis of  $\mathbb{R}^n$ . Let  $\{f_i\}_{i=1}^n \in (\mathbb{R}^n)^*$  be the dual basis; so  $\langle f_i, v_j \rangle = \delta_{ij}$ . Then the dual cone  $C^\vee = \{f \in (\mathbb{R}^n)^* : \langle f, c \rangle \geq 0 \ \forall c \in C\}$  is given by  $C^\vee = \sum_1^n \mathbb{R}_+ f_i$ . Indeed, any  $f \in (\mathbb{R}^n)^*$  can be written as  $f = \sum_{i=1}^n r_i f_i$  with  $r_i \in \mathbb{R}$ , and  $f \in C^\vee$  if and only  $r_i = \langle f, v_i \rangle \geq 0$  for all  $i$ .

Recall that, by definition, the faces  $\mathcal{F}$  of  $C$  are the subsets of the form  $\mathcal{F} = C \cap f^\perp$  for some  $f \in C^\vee$ . Writing  $f = \sum r_i f_i$ , as above, one obtains that  $C \cap f^\perp = \sum_{i:r_i=0} \mathbb{R}_+ v_i$ . Therefore, the faces of  $C$  are determined as follows

$$\mathcal{F}_I = \sum_{i \in I} \mathbb{R}_+ v_i : I \subseteq \{1, 2, \dots, n\},$$

and  $\dim(\mathcal{F}_I) = |I|$ , the cardinality of  $I$ .

Hence the edges of  $C$  are exactly the rays  $\mathcal{E}_i = \mathbb{R}_+ v_i$  and the facets are  $\mathcal{F}_i := \sum_{j \neq i} \mathbb{R}_+ v_j$ . One can easily see that each edge is the intersection  $n - 1$  of the facets.

Finally, if  $C$  is integral then so are all its faces; see [Oda, Proposition 1.3]. In particular, the edges  $\mathbb{R}_+ v_i$  are integral; so we may take  $v_i \in \mathbb{Z}^n$ . This completes the proof of the lemma.  $\square$

We now turn to finite reflection groups  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$ . Our first goal is to give some equivalent conditions for  $\mathcal{G}$  to act effectively on  $\mathbb{Z}^n$ . To this end, recall from Proposition 3.2.4 that

$$X^\succ = \{v \in \mathbb{R}^n : v \succeq \sigma(v) \text{ for all reflections } \sigma \in \mathcal{G}\} = \bigcap_{\sigma} \mathcal{H}_\sigma^+,$$

where  $\sigma$  runs over the reflections in  $\mathcal{G}$ ,  $\mathcal{H}_\sigma^+ = \{v \in \mathbb{R}^n : l_\sigma(v) \geq 0\}$  is as in the proof of Proposition 3.2.4, and  $l_\sigma \in (\mathbb{R}^n)^*$  is the linear form of (3.3). Let  $\sigma_i$  ( $i = 1, \dots, t$ ) be a minimal collection of reflections in  $\mathcal{G}$  so that

$$X^\succ = \bigcap_{i=1}^t \mathcal{H}_i^+, \tag{3.5}$$

where we have put

$$\mathcal{H}_i^+ = \mathcal{H}_{\sigma_i}^+ = \{v \in \mathbb{R}^n : l_{\sigma_i}(v) \geq 0\}.$$

For simplicity, we will also write  $l_i$  for the linear form  $l_{\sigma_i}$ , and  $e_i$  for the element  $e_{\sigma_i} \in \mathbb{Z}^n$  in (3.2); so  $l_i = \langle \cdot, e_i \rangle$ . By Lemma 3.2.3, we have

$$\mathcal{H}_i := \ker(l_i) = \{v \in \mathbb{R}^n : \langle v, e_i \rangle = 0\} . \quad (3.6)$$

**Lemma 3.2.9.** *With the above notations, we have:*

(i)  $\langle e_i, e_j \rangle \leq 0$  for distinct  $i, j \in \{1, \dots, t\}$ .

(ii) The vectors  $e_1, \dots, e_t$  are linearly independent over  $\mathbb{R}$ .

*Proof.* For (i), see [Re03, Lemma 5.1] (which in turn relies on [Bo68, Proposition V.3.4.3(iii)]).

For (ii), suppose that  $\sum_{i=1}^t r_i e_i = 0$  for suitable  $r_i \in \mathbb{R}$ . After possibly rearranging and collecting the positive and negative scalars  $r_i$  separately we may write

$$\sum r_\alpha e_\alpha = \sum r_\beta e_\beta =: a$$

where  $r_\alpha, r_\beta \in \mathbb{R}_+$  and the  $e_\alpha, e_\beta$  are distinct. By part (i),

$$\langle a, a \rangle = \sum_{\alpha, \beta} r_\alpha r_\beta \langle e_\alpha, e_\beta \rangle \leq 0$$

and hence  $a = 0$ , since  $\langle \cdot, \cdot \rangle$  is positive definite. Now choose  $v_0 \in C_0$ , where  $C_0$  is as in (3.4). Then  $\langle e_\alpha, v_0 \rangle > 0$  but

$$0 = \langle a, v_0 \rangle = \langle \sum r_\alpha e_\alpha, v_0 \rangle = \sum r_\alpha \langle e_\alpha, v_0 \rangle .$$

It follows that  $r_\alpha = 0$  for all  $\alpha$ . Similarly can show  $r_\beta = 0$ . Therefore,  $r_i = 0$  for all  $i = 1, \dots, t$  and hence the  $e_i$  are linearly independent.  $\square$

The following lemma gives the promised equivalent conditions for effectiveness of the  $\mathcal{G}$ -action.

**Lemma 3.2.10.** *The following are equivalent:*

(i)  $(\mathbb{Z}^n)^{\mathcal{G}} = 0$ .

(ii)  $\{e_1, \dots, e_t\}$  span  $\mathbb{R}^n$

(iii)  $X^\succ$  contains no nonzero linear subspace.

*Proof.* (i)  $\Leftrightarrow$  (ii) : Note that

$$\begin{aligned} v \in (\mathbb{Z}^n)^\mathcal{G} &\Leftrightarrow -v \in (\mathbb{Z}^n)^\mathcal{G} \Leftrightarrow v \succeq g(v) \text{ and } -v \succeq g(-v), \forall g \in \mathcal{G} \\ &\Leftrightarrow v, -v \in A^\succ \Leftrightarrow l_i(v) \geq 0 \text{ and } l_i(-v) \geq 0, \forall i = 1, \dots, t, \\ &\Leftrightarrow l_i(v) = 0, \forall i = 1, \dots, t \Leftrightarrow v \in \{e_1, \dots, e_t\}^\perp, \end{aligned}$$

where the second equivalence follows from equation (3.5) and the fact that  $A^\succ \subseteq X^\succ$ . Hence,  $(\mathbb{Z}^n)^\mathcal{G} = 0 \Leftrightarrow \{e_1, \dots, e_t\}^\perp = 0 \Leftrightarrow \{e_1, \dots, e_t\}$  span  $\mathbb{R}^n$

(i)  $\Leftrightarrow$  (iii) : This is implicitly shown in the equivalence (i)  $\Leftrightarrow$  (ii) above.

Note also that  $(\mathbb{R}^n)^\mathcal{G} = \mathbb{R} \otimes_{\mathbb{Z}} (\mathbb{Z}^n)^\mathcal{G}$ .  $\square$

It is now a simple matter to prove the main result of this section.

**Theorem 3.2.11.** *Let  $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$  be a finite reflection group that acts effectively on  $\mathbb{Z}^n$ . Then the cone  $\text{Pos}(A^\succ) = X^\succ$  (see Theorem 3.2.6) is a simplicial cone of dimension  $n$ .*

*Proof.* From Lemma 3.2.10 we know that the vectors  $e_1, \dots, e_t$  generate  $\mathbb{R}^n$  and, by Lemma 3.2.9, they are linearly independent. Hence,  $t = n$  and  $e_1, \dots, e_t$  is a basis of  $\mathbb{R}^n$ . Identifying the dual  $(\mathbb{R}^n)^*$  with  $\mathbb{R}^n$  by means of the bilinear form  $\langle, \rangle$ , as usual, let  $w_i, \dots, w_n$  be the dual basis of  $\mathbb{R}^n$ ; so  $\langle w_i, e_j \rangle = \delta_{i,j}$ .

Recall from equation (3.5) that

$$X^\succ = \bigcap_{i=1}^t \mathcal{H}_i^+.$$

Thus, all  $w_i$  belong to  $X^\succ$ , and hence  $\text{Pos}(w_1, \dots, w_t) \subseteq X^\succ$ . Conversely, let  $x \in X^\succ$  and write  $x = \sum r_i w_i$  with  $r_i \in \mathbb{R}$ . Then, for all  $j$ ,

$$0 \leq \langle x, e_j \rangle = \left\langle \sum_i r_i w_i, e_j \right\rangle = \sum_i r_i \langle w_i, e_j \rangle = r_j$$

This shows that  $x \in \text{Pos}(w_1, \dots, w_t)$ . Therefore,  $X^\succ = \text{Pos}(w_1, \dots, w_t)$  is a simplicial cone of dimension  $n$ .  $\square$

**Remark 3.2.12.** *The converse of Theorem 3.2.11 also holds: if  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  is any finite group such that the cone  $\mathrm{Pos}(A^\succ)$  is simplicial then  $\mathcal{G}$  is a reflection group which acts effectively on  $\mathbb{Z}^n$ . Indeed, simplicial cones are polyhedral and contain no nonzero linear subspaces. Thus, Theorem 3.2.6 implies that  $\mathcal{G}$  is a reflection group and Lemma 3.2.10 yields that  $\mathcal{G}$  acts effectively.*

We finish this section by noting the following group theoretical consequence of Theorem 3.2.11 (which is known and can also be proved by using root systems).

**Corollary 3.2.13.** *If  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  is a finite reflection group that acts effectively on  $\mathbb{Z}^n$  then  $\mathcal{G}$  can be generated by at most  $n$  reflections.*

*Proof.* By Theorem 3.2.11, the fundamental domain  $X^\succ$  for the  $\mathcal{G}$ -action on  $\mathbb{R}^n$  (see Theorem 3.2.6) is a simplicial cone of dimension  $n$ . Thus, by Lemma 3.2.8,  $X^\succ$  has exactly  $n$  facets. Finally, Theorem 3.2.1 yields that the wall reflections across the facets generate  $\mathcal{G}$ . □

# CHAPTER 4

## THE THEOREM OF LORENZ USING SAGBI BASES

### 4.1 Overview

Throughout this chapter, we assume  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  to be a finite group. Furthermore, as in previous chapters,  $\mathbb{S} := \mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] \cong \mathbb{K}[\mathbb{A}]$  will be the group algebra, with the multiplicative action of  $\mathcal{G}$ , and  $\mathbb{R} := \mathbb{K}[\mathbb{A}]^{\mathcal{G}}$  will denote the multiplicative invariant algebra.

In this chapter, we prove the main results of this thesis. In particular, we will prove Theorem 1.5.1 that was stated in the Introduction. In doing so, we will give a new proof of the following result which is one of the variants of the Shephard-Todd-Chevalley Theorem in multiplicative invariant theory.

**Theorem 4.1.1 (Lorenz [Lo01]).** *If  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  is a finite reflection group acting effectively on the lattice  $\mathbb{Z}^n$ , then the multiplicative invariant algebra  $\mathbb{R} = \mathbb{K}[\mathbb{A}]^{\mathcal{G}}$  is a semigroup algebra.*

Theorem 4.1.1 actually holds for any finite reflection group, even if the action on  $\mathbb{Z}^n$  is not effective; see [Lo01]. Moreover, the structure of the monoid

$\mathbf{M}$  so that  $\mathbf{R} \cong \mathbf{K}[\mathbf{M}]$  is known; [Lo01] gives a description in terms of the weight lattice of a suitable root system.

Our approach is different from the one taken in [Lo01]. Using SAGBI bases, simplicial cones, and results developed in the previous chapters we will prove the following result. As before, we assume that an arbitrary term ordering  $\succeq$  of  $\mathbb{R}^n$  has been chosen.

**Theorem 4.1.2.** *Let  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  be a finite group such that the cone  $\mathrm{Pos}(A^\succ)$  is simplicial. Then the multiplicative invariant algebra  $\mathbf{R} = \mathbf{K}[A]^\mathcal{G}$  is a semi-group algebra  $\mathbf{K}[\mathbf{M}]$  such that the initial map gives an isomorphism  $\mathcal{I} : \mathbf{M} \cong A^\succ$ .*

Recall that, by Theorem 3.2.11 and Remark 3.2.12, our hypothesis on  $\mathrm{Pos}(A^\succ)$  above is equivalent to  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  being a finite reflection group that acts effectively on  $\mathbb{Z}^n$ . Therefore, Theorem 4.1.2 implies Theorem 4.1.1. Note also that the implication (i)  $\Rightarrow$  (ii) of Theorem 1.5.1, stated in the Introduction, is covered by Theorem 4.1.2. The reverse implication, (ii)  $\Rightarrow$  (i), is a rather straightforward consequence of Theorem 3.2.6; see Proposition 4.3.1 below.

Finally, in §4.4 we will apply the techniques used in the proof of Theorem 4.1.2 to calculate the invariant algebra  $\mathbf{R}$  for a particular example.

## 4.2 Proof of Theorem 4.1.2

We assume that the cone  $X^\succ = \mathrm{Pos}(A^\succ)$  is simplicial. As was pointed out above, this forces  $\mathcal{G}$  to be a finite reflection group that acts effectively on  $\mathbb{Z}^n$ . In particular, by Proposition 3.2.4, we know that

$$X^\succ = \{v \in \mathbb{R}^n : v \succeq g(v) \text{ for all } g \in \mathcal{G}\} \quad (4.1)$$

and  $X^\succ$  is a fundamental domain for the action of  $\mathcal{G}$  on  $\mathbb{R}^n$ . The latter implies that  $\dim X^\succ = n$ ; see Lemma 2.7.2. Thus, since  $X^\succ$  is a simplicial cone, we may write  $X^\succ = \mathrm{Pos}(v_1, \dots, v_n)$ , where the  $v_i$  form a basis of  $\mathbb{R}^n$ . By Lemma 3.2.8, we may choose  $v_i \in \mathbb{Z}^n$  and so  $v_i \in \mathbb{Z}^n \cap X^\succ = A^\succ$ .

**Lemma 4.2.1.** *Suppose  $X^\succ$  is a simplicial cone, say  $X^\succ = \text{Pos}(v_1, \dots, v_n)$  with linearly independent  $v_i \in A^\succ$ , as above. There exist  $p_i \in \mathbb{N}$  such that the lattice*

$$L := \mathbb{Z} \frac{1}{p_1} v_1 + \dots + \mathbb{Z} \frac{1}{p_n} v_n \subseteq \mathbb{R}^n$$

has the following properties:

(i)  $\mathbb{Z}^n \subseteq L$  and  $A^\succ = \mathbb{Z}^n \cap L_+$ , where  $L_+ := \mathbb{Z}_+ \frac{1}{p_1} v_1 + \dots + \mathbb{Z}_+ \frac{1}{p_n} v_n$ ;

(ii)  $L$  is  $\mathcal{G}$ -stable and  $\mathcal{G}$  acts trivially on  $L/\mathbb{Z}^n$ .

Moreover  $A^\succ = \mathbb{Z}^n \cap L_+$ , where  $L_+ := \mathbb{Z}_+ \frac{1}{p_1} v_1 + \dots + \mathbb{Z}_+ \frac{1}{p_n} v_n$  and  $A^\succ$  is a well ordered set with respect to  $\succ$ .

*Proof.* By Lemma 3.2.8, the facets of  $X^\succ$  are given by

$$\mathcal{F}_i := \sum_{j \neq i} \mathbb{R}_+ v_j \quad (i = 1, \dots, n).$$

Let  $\lambda_i \in \mathcal{F}_i^\perp \cap \mathbb{Z}^n$  be a generator of the 1-dimensional lattice  $\mathcal{F}_i^\perp \cap \mathbb{Z}^n$ . Observe that  $\langle \lambda_i, v_i \rangle \neq 0$ , for otherwise  $\lambda_i \in \{v_1, \dots, v_n\}^\perp = 0$ , a contradiction. Replacing  $\lambda_i$  by  $-\lambda_i$  if necessary we may assume that  $\langle \lambda_i, v_i \rangle >> 0$ . The linear transformations

$$\sigma_i : \mathbb{R}^n \longrightarrow \mathbb{R}^n : v \mapsto v - \frac{2 \langle v, \lambda_i \rangle}{\langle \lambda_i, \lambda_i \rangle} \lambda_i$$

are reflections across the hyperplane  $\mathbb{R}\mathcal{F}_i$ . In fact, by Theorem 3.2.1, the  $\sigma_i$  belong to  $\mathcal{G}$  and generate  $\mathcal{G}$ . Hence,  $\sigma_i(\mathbb{Z}^n) \subseteq \mathbb{Z}^n$ . It follows that  $2 \frac{\langle a, \lambda_i \rangle}{\langle \lambda_i, \lambda_i \rangle} \lambda_i = a - \sigma_i(a) \in \mathbb{Z}^n$  for all  $a \in \mathbb{Z}^n$ . Therefore,  $2 \frac{\langle a, \lambda_i \rangle}{\langle \lambda_i, \lambda_i \rangle} \lambda_i \in \mathbb{Z}^n \cap \mathcal{F}_i^\perp = \mathbb{Z}\lambda_i$ , and hence

$$2 \frac{\langle a, \lambda_i \rangle}{\langle \lambda_i, \lambda_i \rangle} \in \mathbb{Z} \quad \text{for all } a \in \mathbb{Z}^n. \quad (4.2)$$

In particular, since  $\langle v_i, \lambda_i \rangle >> 0$  it follows that

$$p_i := 2 \frac{\langle v_i, \lambda_i \rangle}{\langle \lambda_i, \lambda_i \rangle} \in \mathbb{N}. \quad (4.3)$$

We claim that the numbers  $p_i$  satisfy properties (i) and (ii) of the lemma. For simplicity put

$$v'_i := \frac{v_i}{p_i};$$

so  $X^\succ = \text{Pos}(v'_1, \dots, v'_n)$ .

For (i), let  $a \in \mathbb{Z}^n$  and write  $a = \sum_i r_i v'_i$  for suitable  $r_i \in \mathbb{R}$ . Then, by (4.2),

$$2 \frac{\langle a, \lambda_j \rangle}{\langle \lambda_j, \lambda_j \rangle} = 2 \frac{\langle \sum_{i=1}^n r_i v'_i, \lambda_j \rangle}{\langle \lambda_j, \lambda_j \rangle} = 2 \frac{r_j \langle v_j, \lambda_j \rangle}{p_j \langle \lambda_j, \lambda_j \rangle} = r_j \in \mathbb{Z}.$$

This proves the inclusion  $\mathbb{Z}^n \subseteq L$ , and hence (i) is proved.

Property (ii) says that

$$g(v'_i) - v'_i \in \mathbb{Z}^n$$

holds for all  $g \in \mathcal{G}$  and  $i = 1, \dots, n$ . Since  $\sigma_1, \dots, \sigma_n$  are generators of  $\mathcal{G}$ , by Theorem 3.2.1, it suffices to show this for  $g = \sigma_j$   $j \in \{1, \dots, n\}$ . But

$$\begin{aligned} \sigma_j(v'_i) - v'_i &= v'_i - 2 \frac{\langle v'_i, \lambda_j \rangle}{\langle \lambda_j, \lambda_j \rangle} \lambda_j - v'_i = -2 \frac{\langle v'_i, \lambda_j \rangle}{\langle \lambda_j, \lambda_j \rangle} \lambda_j \\ &= -\frac{1}{p_i} 2 \frac{\langle v_i, \lambda_j \rangle}{\langle \lambda_j, \lambda_j \rangle} \lambda_j = -\delta_{ij} \lambda_j \in \mathbb{Z}^n, \end{aligned}$$

where  $\delta_{ij}$  is the Kronecker delta. This proves (ii).

Now consider  $A^\succ$ . Note that  $L_+ = L \cap X^\succ$ . Thus, by (i),  $A^\succ = \mathbb{Z}^n \cap X^\succ \subseteq L \cap X^\succ = L_+$  and hence  $A^\succ \subseteq \mathbb{Z}^n \cap L_+$ . On the other hand, putting  $p = \prod_1^n p_i$ , we have  $pL_+ \subseteq A^\succ$  because  $v_i \in A^\succ$ . Since  $A^\succ$  is a saturated submonoid of  $\mathbb{Z}^n$ , by Lemma 2.7.5(i), we conclude that  $A^\succ = \mathbb{Z}^n \cap L_+$ , as asserted. Finally, by Lemma 3.2.10(ii) the set  $\{\lambda_1, \dots, \lambda_n\}$  spans the whole  $\mathbb{R}^n$ . Hence, by [Re03, Prop 5.5],  $A^\succ \cap \mathbb{R}\lambda_1 + \dots + \mathbb{R}\lambda_n = A^\succ$  is well ordered.  $\square$

We are now ready to give the proof of Theorem 4.1.2.

*Proof of Theorem 4.1.2.* Write  $X^\succ = \text{Pos}(v_1, \dots, v_n)$  with linearly independent  $v_i \in A^\succ$  and put  $v'_i = \frac{v_i}{p_i}$  and  $L_+ = \mathbb{Z}_+ v'_1 + \dots + \mathbb{Z}_+ v'_n$  with  $p_i \in \mathbb{N}$ , as in Lemma 4.2.1. Consider an element  $w \in A^\succ = \mathbb{Z}^n \cap L_+$ ; so

$$w = \sum_{i=1}^n z_i v'_i \tag{4.4}$$

with uniquely determined  $z_i = z_i(w) \in \mathbb{Z}_+$ . As in §2.7.2, we view the group algebra  $S = K[A]$  as being contained in the larger group algebra  $S_{\mathbb{R}} = K[A_{\mathbb{R}}]$ ,



where  $A_{\mathbb{R}} = \{x^v : v \in \mathbb{R}^n\}$ . In  $S_{\mathbb{R}}$ , form the invariant

$$f_w := \prod_{i=1}^n \vartheta(x^{v'_i})^{z_i}. \quad (4.5)$$

We claim that  $f_w$  actually belongs to  $S$ , and hence to  $R = S^{\mathcal{G}}$ . To show this, recall that

$$\vartheta(x^{v'_i}) = \sum_{g \in \mathcal{G}/\mathcal{G}_{v'_i}} x^{g \cdot v'_i},$$

where  $\mathcal{G}_{v'_i}$  denotes the stabilizer of  $v'_i$  in  $\mathcal{G}$ . Expanding the product  $f_w = \prod_{i=1}^n \vartheta(x^{v'_i})^{z_i}$ , we see that  $f_w$  is a  $K$ -linear combination of terms of the form  $x^v$  with  $v = \sum_{i=1}^n \sum_{k=1}^{z_i} g_{i,k} \cdot v'_i$  for suitable  $g_{1,1}, \dots, g_{n,z_n} \in \mathcal{G}$ . By Lemma 4.2.1(ii),

$$v - w = \sum_{i=1}^n \sum_{k=1}^{z_i} (g_{i,k} \cdot v'_i - v'_i) \in \mathbb{Z}^n.$$

Since  $w \in \mathbb{Z}^n$ , it follows that  $v \in \mathbb{Z}^n$ . Hence, all  $v$  in the support of  $f_w$  belong to  $\mathbb{Z}^n$  and so  $f_w \in S$ , as we have claimed. Moreover, by (4.1) and Remark 2.7.7, the initial term of  $f_w$  is given by

$$\mathcal{I}(f_w) = \sum_{i=1}^n z_i \mathcal{I}(\vartheta(x^{v'_i})) = \sum_{i=1}^n z_i v'_i = w. \quad (4.6)$$

Observe that  $f_{w+w'} = f_w f_{w'}$  holds for  $w, w' \in A^{\succ}$ . Thus, the collection

$$M := \{f_w : w \in A^{\succ}\}$$

is a submonoid of  $(R, \cdot)$  and the map  $A^{\succ} \rightarrow M$ ,  $w \mapsto f_w$ , is a monoid isomorphism with inverse the initial map  $\mathcal{I}$ . Formula (4.6) also implies that the elements of  $M$  are linearly independent over  $K$ . Indeed, any finite linear combination  $f = \sum_1^t \lambda_j f_{w_j} = 0$  with  $0 \neq \lambda_j \in K$  and  $w_j \in A^{\succ}$  satisfies  $\mathcal{I}(f) = \max_j \{w_j\}$ .

To complete the proof of Theorem 4.1.2, it suffices to show that  $M$  generates the  $K$ -algebra  $R$ . But, by Lemma 2.7.9, we have  $\mathcal{I}(R) = A^{\succ} = \{\mathcal{I}(f) : f \in M\}$  and  $A^{\succ}$  is well ordered, by Lemma 4.2.1. Therefore, Proposition 2.7.8 implies that  $R$  is indeed generated by  $M$ . This completes the proof.  $\square$

**Remark 4.2.2.** *By Lemma 2.7.5(iii), the semigroup  $A^\succ$  is finitely generated. If  $w_1, \dots, w_r$  is any collection of generators for  $A^\succ$  then the above proof shows that the monoid  $M$  is generated by the elements  $f_{w_i}$ , and these elements form a finite SAGBI basis of the multiplicative invariant algebra  $R$ .*

### 4.3 The Converse

In this section, we establish the other implication, (ii)  $\Rightarrow$  (i) of Theorem 1.5.1 stated in the Introduction. We do not assume that  $\mathcal{G}$  acts effectively here.

**Proposition 4.3.1.** *Assume that the multiplicative invariant algebra  $R = K[A]^\mathcal{G}$  is a semigroup algebra  $K[M]$  for some submonoid  $M$  of  $(R, \cdot)$  such that the initial map  $\mathcal{I}$  is injective on  $M$ . Then  $\mathcal{G}$  acts as a reflection group on  $\mathbb{Z}^n$ .*

*Proof.* By Noether's Theorem 1.3.2,  $R$  is an affine  $K$ -algebra. Hence, by Proposition 2.3.3, the monoid  $M$  is finitely generated, say  $M = \langle \{f_1, \dots, f_s\} \rangle_{mon}$ .

We next show that  $\mathcal{I}(R) = \langle \{\mathcal{I}(f_1), \dots, \mathcal{I}(f_s)\} \rangle_{mon}$ . Here, the inclusion  $\supseteq$  is trivial. Conversely, let  $f \in R$  be given. Write  $f$  as a finite sum  $f = \sum_i k_i m_i$  with  $k_i \in K$  and distinct  $m_i \in M$ . By hypothesis on  $\mathcal{I}$ , all  $\mathcal{I}(m_i)$  are distinct. Hence,

$$\mathcal{I}(f) = \max_i \{\mathcal{I}(m_i)\} \in \mathcal{I}(M) .$$

Since  $M = \langle \{f_1, \dots, f_s\} \rangle_{mon}$  and  $\mathcal{I}$  is a monoid map, we have  $\mathcal{I}(M) = \langle \{\mathcal{I}(f_1), \dots, \mathcal{I}(f_s)\} \rangle_{mon}$ . This proves the reverse inclusion,  $\subseteq$ .

Finally, by Lemma 2.7.9, we have  $\mathcal{I}(R) = A^\succ$ ; so we have shown that  $A^\succ$  is a finitely generated monoid. By Theorem 3.2.6, we conclude that  $\mathcal{G}$  is a reflection group.  $\square$

### 4.4 Examples

Our first example describes the action of a reflection group on  $\mathbb{Z}^2$ . We will determine the monoid  $A^\succ$  for this example, using the lexicographical order

on  $\mathbb{Z}^2$ , and explicitly carry out the construction of a monoid basis  $\mathbf{M}$  for the multiplicative invariant algebra  $\mathbf{R}$  by following the main steps in the proof of Theorem 4.1.2. This example will also illustrate that not just any finite SAGBI basis will lead to a suitable monoid  $\mathbf{M} \subseteq (\mathbf{R}, \cdot)$  so that  $\mathbf{R} = \mathbf{K}[\mathbf{M}]$ .

**Example 4.4.1.** Recall from Example 3.1.3 that symmetric group  $\mathcal{S}_{n+1}$  act on  $\mathbb{Z}^{n+1}$  by  $s(e_i) = e_{s(i)}$  ( $s \in \mathcal{S}_{n+1}$ ), where  $\{e_i\}_1^{n+1}$  is the standard basis of  $\mathbb{Z}^{n+1}$ , and all transpositions act as reflections. The sublattice of  $\mathbb{Z}^{n+1}$  that is spanned by the elements  $a_i = e_i - e_{i+1}$  ( $i = 1, \dots, n$ ) is easily seen to be stable under  $\mathcal{S}_{n+1}$ ; so  $\mathcal{S}_{n+1}$  acts as a reflection group on this lattice, which is known as the root lattice  $A_n$ . We will consider the case  $n = 2$  in detail here.

Thus,  $\mathcal{G} = \mathcal{S}_3$  acts on  $A_2 = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2 \cong \mathbb{Z}^2$ . For example, the transposition  $(1, 2) \in \mathcal{G}$  sends  $a_1 \mapsto -a_1$  and  $a_2 \mapsto a_1 + a_2$ ; so  $(1, 2)$  acts via the matrix  $t = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ . Similarly, the 3-cycle  $(1, 2, 3) \in \mathcal{G}$  acts via the matrix  $u = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ . The complete list of all matrices for the elements of  $\mathcal{G}$  is as follows:

$$\begin{aligned} I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & r &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, & s &= \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \\ t &= \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, & u &= \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, & v &= \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

Observe that  $r, s$ , and  $t$  are the reflections in  $\mathcal{G}$ . We will identify  $A_2$  with  $\mathbb{Z}^2$ , as above, and use the lexicographical order  $\succeq = \succeq_{lex}$  on  $\mathbb{Z}^2$ ; see §2.7.1.

We first determine  $A^\succ$ . By Proposition 3.2.4, we have

$$A^\succ = \mathbb{Z}^2 \cap X^\succ = \{v \in \mathbb{Z}^2 : v \succeq \sigma \cdot v \text{ for } \sigma = r, s, t\}$$

For  $(a, b) \in \mathbb{Z}^2$ , we have

$$\begin{aligned} (a, b) \succeq r \cdot (a, b) = (-b, -a) & \Leftrightarrow a \geq -b \\ (a, b) \succeq s \cdot (a, b) = (a, a - b) & \Leftrightarrow 2b \geq a \\ (a, b) \succeq t \cdot (a, b) = (b - a, b) & \Leftrightarrow 2a \geq b \end{aligned}$$

Intersecting the sets we get that:

$$A^\succ = \{(a, b) \in \mathbb{Z}^2 : 2a \geq b \geq a/2\}.$$

This submonoid of  $\mathbb{Z}^2$  is generated by three points:

$$w_1 = (2, 1), w_2 = (1, 2), w_3 = (1, 1)$$

In the Appendix, we give a Maple program that will solve the simultaneous inequalities and give a quick graphical description of the set  $A^\succ$ . See Figure 4.1 below, for the example under consideration.

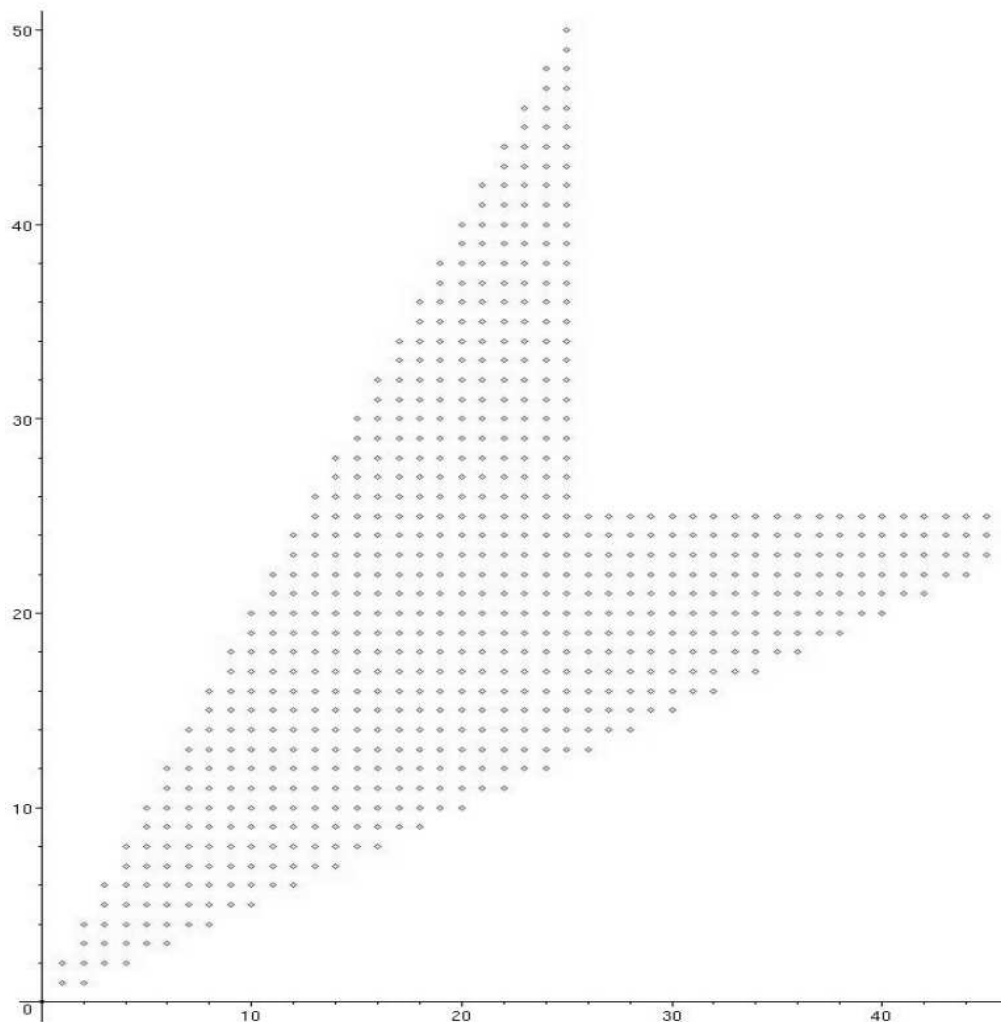


Figure 4.1:  $A^\succ$  for the reflection group in Example 4.4.1

Visibly,  $A^\succ$  is well ordered (as it should be, since  $\mathcal{G}$  acts effectively on  $\mathbb{Z}^2$ ; see Lemma 4.2.1).

In the group algebra  $\mathbf{S} = \mathbf{K}[A]$ , write  $x = \mathbf{x}^{(1,0)}$  and  $y = \mathbf{x}^{(0,1)}$ . Then the orbit sums of  $w_1, w_2, w_3$  are:

$$\begin{aligned} f_1 &= \vartheta(\mathbf{x}^{w_1}) = x^2y + x^{-1}y^{-2} + x^{-1}y \\ f_2 &= \vartheta(\mathbf{x}^{w_2}) = xy^2 + x^{-2}y^{-1} + x^1y^{-1} \\ f_3 &= \vartheta(\mathbf{x}^{w_3}) = xy + x^{-1}y^{-1} + x + y + x^{-1} + y^{-1} \end{aligned}$$

By Proposition 2.7.8,  $\{f_1, f_2, f_3\}$  is a SAGBI basis of  $\mathbf{R} = \mathbf{K}[x^{\pm 1}, y^{\pm 1}]^{\mathcal{G}}$ . However, the submonoid of  $(\mathbf{R}, \cdot)$  that is generated by  $\{f_1, f_2, f_3\}$  does not form a  $\mathbf{K}$ -basis for  $\mathbf{R}$ . Indeed, the  $f_i$  satisfy the relation

$$f_1f_2 - f_3^3 + 3f_1f_3 + 3f_2f_3 + 6f_1 + 6f_2 + 9f_3 + 9 = 0 .$$

On the other hand, we know that  $\mathbf{R}$  is a semigroup algebra. Let us a semigroup basis  $\mathbf{M}$  of  $\mathbf{R}$  for this example by tracking the proof of Theorem 4.1.2. We start with the monoid  $A^\succ = \mathbb{Z}_+(2, 1) + \mathbb{Z}_+(1, 1) + \mathbb{Z}_+(1, 2)$  that was determined above. Thus, in the notation of Lemma 4.2.1, we have  $X^\succ = \text{Pos}(A^\succ) = \text{Pos}(v_1, v_2)$  with  $v_1 = w_1 = (2, 1), v_2 = w_2 = (1, 2)$ . Let  $p = p_1, \frac{1}{q} = p_2$  be as in Lemma 4.2.1. These could be determined by formula (4.3), but this would require calculating the bilinear form  $\langle \cdot, \cdot \rangle$  in (3.1). Instead, we note that, by Lemma 4.2.1(ii), we must have

$$\begin{aligned} r\left(\frac{1}{p}v_1\right) - \frac{1}{p}v_1 &= \left(\frac{-1}{p}, \frac{-2}{p}\right) - \left(\frac{2}{p}, \frac{1}{p}\right) = \left(\frac{-3}{p}, \frac{-3}{p}\right) \in \mathbb{Z}^n \\ r\left(\frac{1}{q}v_2\right) - \frac{1}{q}v_2 &= \left(\frac{-2}{q}, \frac{-1}{q}\right) - \left(\frac{1}{q}, \frac{2}{q}\right) = \left(\frac{-3}{q}, \frac{-3}{q}\right) \in \mathbb{Z}^n \\ s\left(\frac{1}{p}v_1\right) - \frac{1}{p}v_1 &= \left(\frac{2}{p}, \frac{1}{p}\right) - \left(\frac{2}{p}, \frac{1}{p}\right) = (0, 0) \in \mathbb{Z}^n \\ s\left(\frac{1}{q}v_2\right) - \frac{1}{q}v_2 &= \left(\frac{1}{q}, \frac{-1}{q}\right) - \left(\frac{1}{q}, \frac{2}{q}\right) = \left(0, \frac{-3}{q}\right) \in \mathbb{Z}^n \end{aligned}$$

Hence  $p = 1$  or  $3$  and  $q = 1$  or  $3$ . But by Lemma 4.2.1(i), we must have  $\mathbb{Z}^2 \subseteq L = \mathbb{Z}_p^1 v_1 + \mathbb{Z}_q^1 v_2$  which is impossible if either  $p$  or  $q$  equals  $1$ . Therefore,

$$p = q = 3 .$$

Thus, putting  $v'_1 = \frac{1}{p}v_1$  and  $v'_2 = \frac{1}{q}v_2$  as in the proof of Theorem 4.1.2, we have

$$w_1 = 3v'_1, w_2 = 3v'_2 \quad \text{and} \quad w_3 = v'_1 + v'_2 .$$

Therefore by formulas (4.4) and (4.5), we obtain the following generators for the invariant algebra  $\mathbb{R}$ :

$$\begin{aligned} f_1 = f_{w_1} = \vartheta(v'_1)^3 &= (x^{2/3}y^{1/3} + x^{-1/3}y^{-2/3} + x^{-1/3}y^{1/3})^3 \\ &= \left[ \frac{xy + y + 1}{x^{1/3}y^{2/3}} \right]^3 = x^{-1}y^{-2}(xy + y + 1)^3 \end{aligned}$$

$$\begin{aligned} f_2 = f_{w_2} = \vartheta(v'_2)^3 &= (x^{1/3}y^{2/3} + x^{-2/3}y^{-1/3} + x^{1/3}y^{-1/3})^3 \\ &= \left[ \frac{(xy + x + 1)}{x^{2/3}y^{1/3}} \right]^3 = x^{-2}y^{-1}(xy + x + 1)^3 \end{aligned}$$

$$\begin{aligned} f_3 = f_{w_3} = \vartheta(v'_1)\vartheta(v'_2) &= \\ &= (x^{2/3}y^{1/3} + x^{-1/3}y^{-2/3} + x^{-1/3}y^{1/3})(x^{1/3}y^{2/3} + x^{-2/3}y^{-1/3} + x^{1/3}y^{-1/3}) \\ &= x^{-1}y^{-1}(xy + y + 1)(xy + x + 1) \end{aligned}$$

By the proof of Theorem 4.1.2, the monoid

$$\mathbf{M} = \langle \vartheta(v'_1)^3, \vartheta(v'_2)^3, \vartheta(v'_1)\vartheta(v'_2) \rangle_{\text{mon}}$$

is indeed a  $\mathbb{K}$ -basis for the invariant algebra  $\mathbb{R}$ ; so  $\mathbb{R} = \mathbb{K}[\mathbf{M}]$ .

In the next example, the group  $\mathcal{G}$  is not a reflection group. We will demonstrate via the graph of  $A^\wedge(\mathcal{G})$  that it is not a finitely generated semigroup. This will serve to illustrate the implication (ii)  $\Rightarrow$  (i) in Theorem 3.2.6. Again, this example is in rank 2 and we use the lexicographic ordering on  $\mathbb{R}^2$ .

**Example 4.4.2.** Let  $\mathcal{G} \leq \text{GL}_2(\mathbb{Z})$  by the cyclic group generated by the matrix  $t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ . The transformation of  $\mathbb{R}^2$  given by  $t$  is counterclockwise rotation by the angle  $\pi/2$ ; so  $\mathcal{G}$  has order 4. The elements of  $\mathcal{G}$  are:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, r = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, s = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

For  $(a, b) \in \mathbb{Z}^2$ , we have

$$\begin{aligned} (a, b) \succ r(a, b) = (b, -a) & \Leftrightarrow a > b \cup [a = b \cap b \geq 0] \\ (a, b) \succ s(a, b) = (-a, -b) & \Leftrightarrow a > 0 \cup [a = 0 \cap b \geq 0] \\ (a, b) \succ t(a, b) = (-b, a) & \Leftrightarrow a > -b \cup [a = -b \cap b \geq 0] \end{aligned}$$

Combining all the inequalities we get that;

$$A^\succ = \{(a, b) \in \mathbb{Z}^2 : a \geq 0 \cap -a < b \leq a\} .$$

Observe that a generation by any finite collection of points in  $A^\succ$  will exclude points of  $A^\succ$  on the boundary  $\{(a, b) : -a + 1 = b\}$  of  $A^\succ$ , as the figure below clearly demonstrates. Therefore  $A^\succ$  can not be finitely generated.

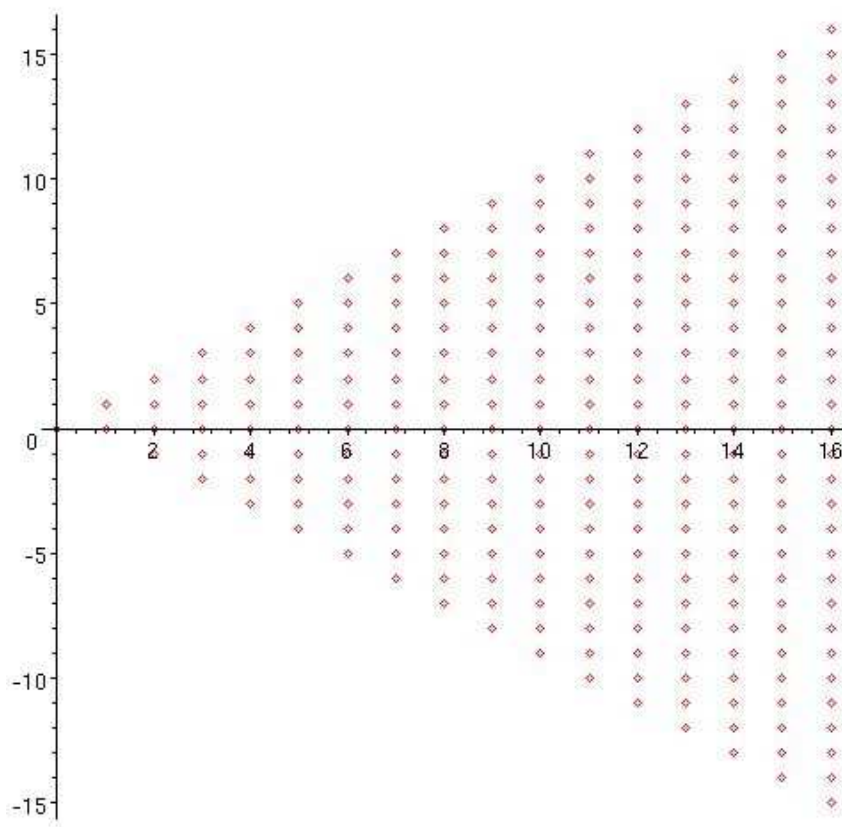


Figure 4.2:  $A^\sim$  for the non-reflection group in Example 4.4.2



# APPENDIX A

## MAPLE PROGRAM

Below we give a maple program that will calculate and graph  $A^\lambda$  on a given interval

```

Greater:=proc()
local integer:m,k,l,p;
with(linalg):
VEC1:=args[1];
VEC2:=args[2]; tempo:=matadd(VEC1,VEC2,1,-1);
TRUTH:=false;
if tempo[1] > 0 then
TRUTH:=true;
elif tempo[1]=0 and tempo[2] > 0 then
TRUTH:=true;
# elif tempo[1]=0 and tempo[2]=0 and tempo[3] > 0 then
# TRUTH:=true
fi;
RETURN(TRUTH);
end;LEXICOG:=proc()
local

```

```
integer:j,m,k,l,n,p;
LISTT:=args[1]; p:=nops(LISTT);Tempo:=LISTT[1];# print(p,LISTT,Tempo);
# for m from 1 to p do
for j from 1 to p do
T_ value:= Greater(Tempo,LISTT[j]);
if T_ value = false then
Tempo:=LISTT[j];# print(Tempo);
fi;
od;
#od;
RETURN(Tempo);
end;
```

For particular example one need to add the following to the above program,  
 Example: To calculate  $A^\wedge$  for the group,

$$G_6 = \{I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, r = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, s = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, t = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \\ u = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, v = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\}$$

```

> with(linalg): > MAT[1]:=linalg[matrix](2,2,[1,0,0,1]);
> MAT[2]:=linalg[matrix](2,2,[0,-1,-1,0]);
> MAT[3]:=linalg[matrix](2,2,[1,0,1,-1]);
> MAT[4]:=linalg[matrix](2,2,[-1,1,0,1]);
> MAT[5]:=linalg[matrix](2,2,[0,-1,1,-1]);
> MAT[6]:=linalg[matrix](2,2,[-1,1,-1,0]);
> SETT:=[];
> for a1 from -25 to 15 do
> for a2 from -25 to 15 do
> VEC:=linalg[vector](2,[a1,a2]);
> Temp_List:=[];
> for m from 1 to 6 do
> Temp_List:=[op(Temp_List), multiply(MAT[m],VEC)];
> od; # print(Temp_List);
> T_P:=LEXICOG(Temp_List);
T_T := [T_P[1], T_P[2]]; #print(T_P);
> SETT:=[op(SETT),T_T];
> # print(SETT);
> od;
> od; #print(SETT);
> with(plots):
> points:=op(SETT):pointplot(points,color=red);

```

## REFERENCES

- [Bo68] N. Bourbaki, *Groupes et Algèbres de Lie*, chap. 4–6, Hermann, Paris, 1968.
- [Ch55] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.
- [DF99] D.S. Dummit and R.M. Foote, *Abstract Algebra*, John Wiley & Sons Inc. New York, 1999.
- [Ew96] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, GTM 168, Springer-Verlag, New York, 1996.
- [Fa84] D. Farkas, *Multiplicative invariants*, L'Enseignement Mathématique, t.**30** (1984), 141 - 157.
- [Fa85] D. Farkas, *Towards multiplicative invariant theory*, in: “Group actions on Rings” (S. Montgomery, ed.), Amer. Math. Soc., Providence, RI, Contemporary Math. **43** (1985), 69-80.
- [Fa86] D. Farkas, *Reflection groups and multiplicative invariants*, Rocky Mt. J. **16** (1986), 215 - 222.
- [Fl] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **156** (2000), 23 - 32.
- [Fo] J. Fogarty, *On Noether's bound for polynomial invariants of finite groups*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5 - 7.

- [Fu93] W. Fulton, *Introduction to Toric Varieties*, Annals of Mathematics Studies; vol. **131**, Princeton University Press, Princeton NJ, 1993.
- [Gi84] R. Gilmer, *Commutative Semigroup Rings*, Chicago Lectures in Mathematics Series, 1984.
- [Gu92] J. Gubeladze, *The elementary action on unimodular rows over a monoid ring*, J. Algebra **148** (1992), 135 -161.
- [Ha87] M. Hajja, *Rationality of finite groups of monomial automorphisms of  $K(x, y)$* , J. of Algebra **109** (1987), 46 - 51.
- [HK92] M. Hajja and M.C. Kang, *Finite group actions on rational function fields*, J. of Algebra **149** (1992), 139 - 154.
- [HK94] M. Hajja and M.C. Kang, *Three-dimensional purely monomial group actions*, J. of Algebra **170** (1994), 805 - 860.
- [HE71] M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020–1058.
- [Hu72] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag New York, 1972.
- [Ka01] R. Kane, *Reflection Groups and Invariant Theory*, Canadian Mathematical Society, Springer New York, 2001.
- [Lo96] M. Lorenz, *Regularity of multiplicative invariants*, Communications in Algebra **24(3)**, 1996 1051 - 1055.
- [Lo01] M. Lorenz, *Multiplicative invariants and semigroup algebras*, Alg. and Rep. Theory **4** (2001), 293-304.
- [Lo03] M. Lorenz, *Multiplicative Invariant Theory*, to appear in the series “Invariant Theory and Algebraic Transformation Groups” of the Springer Encyclopaedia of Mathematical Sciences.

- [Mo] T. Molien, *Über die Invarianten der Linearen Substitutionsgruppen*, Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152 - 1156.
- [Nak80] H. Nakajima, *Invariants of finite abelian groups generated by transvections*, Tokyo J. Math. **3** (1980), 201–214.
- [NS02] M.D. Neusel and L. Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs **94**, AMS 2002.
- [Ne72] M. Newman, *Integral Matrices*, Pure and applied mathematics; a series of monographs and textbooks, **v. 45**, New York, Academic Press, 1972.
- [No16] E. Noether, *Der Endlichkeitssatz der Invarianten Endlicher Gruppen*, Math. Ann. **77** (1916), 89–92; reprinted in *Collected Papers*, pp. 181–184, Springer-Verlag, New York, 1983.
- [Oda] T. Oda, *Convex Bodies and Algebraic Geometry*, Springer-Verlag, Berlin, 1988.
- [Ol99] P.J. Oliver, *Classical Invariant Theory*, London Mathematical Society Student Text **44**, Cambridge University Press 1999.
- [Re03] Z. Reichstein, *SAGBI basis in rings of multiplicative invariants*, Commentarii Math. Helvetici **78(1)** (2003), 185 - 202.
- [Ri82] R.W. Richardson, *Orbits, invariants and representations associated to involutions of reductive groups*, Invent. Math. **66** (1982), 287 - 312.
- [RS90] L. Robbiano, M. Sweedler, *Subalgebra Bases*, Commutative Algebra (Salvador,1988), Lecture Notes in Math., 1430 (1990), Springer, Berlin, 1990, 61 - 87.

- [Se67] J.P. Serre, *Groups finis d'automorphismes d'anneaux locaux réguliers*, Colloq. d'Alg. École Norm. de Jeunes Filles, Paris (1976), 1 -11.
- [ST54] G.C. Shephard and J.A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.
- [Ste75] R. Steinberg, *On a theorem of Pittie*, Topology **14** (1975), 173–177.
- [Stu93] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Wien, 1993.
- [Zi95] G. Ziegler, *Lectures on Polytopes*, GTM 152, Springer-Verlag, New York, 1995.