COMPUTING GENERATORS FOR RINGS OF MULTIPLICATIVE INVARIANTS

A Dissertation
Submitted to
the Temple University Graduate Board

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

by
Marc Stetson Renault
August, 2002

ABSTRACT

COMPUTING GENERATORS FOR RINGS OF MULTIPLICATIVE INVARIANTS

Marc Stetson Renault
DOCTOR OF PHILOSOPHY

Temple University, August, 2002

Dr. Martin Lorenz, Chair

The study of the relationship between a ring R and its subring of invariants R^G under the action of a group G, *invariant theory* for short, is a classical algebraic theme permeating virtually all areas of pure mathematics, some areas of applied mathematics, notably coding theory, and certain parts of theoretical physics as well.

Although the field of invariant theory is over a century old, one particular branch, *multiplicative invariant theory*, has emerged and attracted much attention in the last 35 years. In multiplicative invariant theory one considers a free abelian group A of finite rank n ($A \cong \mathbb{Z}^n$) on which a group G acts by automorphisms ($G \to \mathrm{GL}_n(\mathbb{Z})$). The G-action on A extends uniquely to an action on the group algebra $R = k[A]$ ($R \cong k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$).

The motivating problem of this dissertation can be summed up as follows:

> *Let A be a free abelian group of finite rank, let k be any commutative ring, and let G be a finite group acting multiplicatively on the group algebra $k[A]$. Construct and implement an efficient algorithm for computing generators for $k[A]^G$, the subalgebra of multiplicative invariants.*

Finding explicit generators for invariants has always been at the heart of classical invariant theory; in recent years powerful algorithms have been developed for the computation of invariants in the classical setting. However, very little has been done for the computation of multiplicative invariants (exceptions include [Lor01] and [Rei02]).

In Chapter 3 we provide algorithms for computing generators for $k[A]^G$ when G is a reflection group (§3.3), and in chapter 4 we compute generators for $k[A]^G$ when G is a subgroup of a reflection group (§4.2). The algorithms have been implemented in the computer algebra system *Magma*, and the program source code along with sample output can be found in the appendices.

ACKNOWLEDGMENTS

First and foremost, I owe a huge debt of gratitude to my advisor Martin Lorenz for introducing me to the field of invariant theory and guiding me through the dissertation research and writing process. The amount of time he spent analyzing and dissecting this thesis is truly remarkable. His rigorous approach and high standards provided a constant incentive to dig deeper. Vielen Dank.

Secondly, many thanks go to my good friends in the Temple mathematics department, Matthias Beck, Ibrahim Al-Rasasi, Jay Pathak, and Mohammed Tesemma. Our discussions over the years have been invaluable and certainly influenced and assisted my research.

Finally, thanks go to my wife Tara who has steadfastly supported me during my education and the dissertation writing process. Her faith in me has been a great comfort and motivation.

TABLE OF CONTENTS

LIST OF ALGORITHMS

LIST OF FIGURES

CONVENTIONS AND NOTATION

The following conventions and notation will be used throughout, unless explicitly stated otherwise. For items with more complete definitions given in the text, we include the section number where information can be found.

Notation	Description	See
k	a commutative ring	
$\mathbb{R}_+$	the nonnegative real numbers	
$\mathbb{Q}_+$	the nonnegative rational numbers	
$\mathbb{N}$	the nonnegative integers (note $0 \in \mathbb{N}$)	
$\mathbb{R}_+S$, $\mathbb{N}S$	for S a subset of a real vector space, $\mathbb{R}_+S := \sum_{s\in S} z_s s$ with $z_s \in \mathbb{R}_+$ almost all zero; similar for $\mathbb{N}S$	2.4.6
$S + T$	$\{\, s + t \;:\; s \in S,\; t \in T \,\}$, for S, T subsets of a commutative monoid	
$\mathrm{tr}_G(r)$	for a ring R, a finite group $G \subseteq \mathrm{Aut}(R)$, and $r \in R$, this is the G-trace of r, namely, $\sum_{g\in G} r^g$	2.2.2
A	a free abelian group of finite rank n; note $A \cong \mathbb{Z}^n$	2.2.1
$k[A]$	the group ring of A over k; note $k[A] \cong k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$	2.2.1
a, b, c, d	elements of A, called monomials or lattice points	
f, p, q	elements of $k[A]$, called Laurent polynomials	

a^*	the canonical image of $a \in A$ in $k[A]$; a typical $f \in k[A]$ can be uniquely written as $f = \sum_{a \in A} k_a a^*$ with the $k_a \in k$ almost all zero	2.3.1
G, H	finite subgroups of $\mathrm{GL}(A)$	
V	the $\mathbb{R}$-vector space $A \otimes_{\mathbb{Z}} \mathbb{R}$ of dimension n; we consider $A \subseteq V$ and $\mathrm{GL}(A) \subseteq \mathrm{GL}(V)$	2.4.3
v^g	the image of $v \in V$ under the automorphism $g \in G \subseteq \mathrm{GL}(A) \subseteq \mathrm{GL}(V)$	2.4.1
v^G	$\{\, v^g \ : \ g \in G \,\}$, the orbit of v under G	3.2.1
$\sigma_G(a)$	$\sum_{b \in a^G} b^* \in k[A]^G$, the (monomial) orbit sum of a	2.3.2
$(\ ,\ )$	a positive-definite, symmetric, bilinear, G-invariant inner product on V	2.4.3
π	the orthogonal projection $V \twoheadrightarrow (V^G)^\perp$	2.4.3
r	$\dim \pi(V)$	2.4.3
ρ	$\mathrm{Id} - \pi$, the orthogonal projection $V \twoheadrightarrow V^G$	2.4.3
E	the r-dimensional $\mathbb{R}$-vector space $\pi(V)$	2.4.3
H_g	the hyperplane in V that is fixed by a reflection $g \in \mathrm{GL}(A) \subseteq \mathrm{GL}(V)$	2.4.1
A_g	the infinite cyclic group $H_g^\perp \cap A$	2.4.3
$\pm a_g$	the two generators for A_g	2.4.3
Φ	$\{\, \pm a_g \ : \ g \in G \text{ is a reflection} \,\}$, a crystallographic root system for E; note $\Phi \subseteq A \cap E$	2.4.2
Δ	a base of Φ	2.4.2
δ	an element of Δ, called a simple root	
Λ	$\{\, v \in E \ : \ v - v^g \in A \ \forall\, g \in G \,\}$, the weight lattice; note $\mathbb{Z}\Phi \subseteq \Lambda \subseteq E$	2.4.4
Λ_+, $\Lambda_+(\Delta)$	$\{\, \lambda \in \Lambda \ : \ (\lambda, \delta) \geq 0 \ \forall\, \delta \in \Delta \,\}$, the set of dominant weights relative to Δ	2.4.4
$\lambda_1, \ldots, \lambda_r$	the fundamental dominant weights	2.4.4

$\mathcal{C},\ \mathcal{C}(\Delta)$	$\{\, v \in V \ :\ (v,\delta) > 0 \ \forall\, \delta \in \Delta \,\}$, the Weyl chamber relative to Δ	
$\overline{\mathcal{C}},\ \overline{\mathcal{C}}(\Delta)$	$\{\, v \in V \ :\ (v,\delta) \geq 0 \ \forall\, \delta \in \Delta \,\}$, the closure of $\mathcal{C}(\Delta)$ in V	2.4.6
$\bar{v}$	the unique element in the set $v^G \cap \overline{\mathcal{C}}$	3.2.1
D	$A \cap \overline{\mathcal{C}}$; note $\pi(D) \subseteq \Lambda_+ \subseteq \frac{1}{m}\pi(D)$ for some $0 \neq m \in \mathbb{N}$	2.4.6
DCC	the *descending chain condition*; an ordered set with DCC has no infinite sequence $a_1 > a_2 > \cdots$	3.2.1
$\sim$	for $v, w \in V$, write $v \sim w$ if $0 = \pi(\bar{w} - \bar{v}) \in \mathbb{R}_+\Delta$	3.2.1
$<$	for $v, w \in V$, write $v < w$ if $0 \neq \pi(\bar{w} - \bar{v}) \in \mathbb{R}_+\Delta$	3.2.1
$<$	for $p, q \in k[A]$, write $p < q$ if for each $x \in \mathrm{HM}(p)$ there exists some $y \in \mathrm{HM}(q)$ such that $x < y$	3.2.1
m_i	$n_i\lambda_i$ where $0 \neq n_i \in \mathbb{N}$ is minimal such that $n_i\lambda_i \in \pi(A)$	3.4
K_M	the zonotope $\sum_{i=1}^{r} [0, m_i] \subseteq E$	3.4
Z	$\pi(A) \cap K_M \setminus \{\, 0 \,\}$, note Z generates D	3.4
$X{\uparrow}^T$	$\bigcup_{t \in T} X^t$, where $X \subseteq V$ and $T \subseteq H$, a reflection group	4.2
$\overline{D_i}$	D^{h_i}, where $\{\, \mathrm{Id} = h_1, h_2, \ldots, h_u \,\}$ is a left transversal for G in H, a finite reflection group	4.2
D_i	$D_1 := D,\ \ D_i := \overline{D_i} \setminus \bigcup_{j<i} \overline{D_j}{\uparrow}^G$ for $2 \leq i \leq u$	4.2
Ω_i	a minimal set such that $D_i = \Omega_i + \overline{D_i}$	4.2
H_ω	the isotropy (stabilizer) subgroup of H for ω	4.2
$\prec$	Given $p, f \in k[A]$ write $p \prec f$ if $p < f$ or if $p \not> f$ and $\min\{\, i \ :\ \mathrm{HM}(p) \cap D_i \neq \varnothing \,\} > \min\{\, i \ :\ \mathrm{HM}(f) \cap D_i \neq \varnothing \,\}$.	4.2

CHAPTER 1

INTRODUCTION

1.1 For the Non-mathematician

Invariant theory is part of abstract algebra, a discipline that is largely concerned with the study of “algebraic structures”. For example, one has the sense that the integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are somehow structurally different from the real numbers (all the numbers on the number line) which are somehow different than the complex numbers (the set of all numbers of the form $a + bi$ where a and b are real numbers and $i = \sqrt{-1}$), and so forth. The algebraist describes, exactly and mathematically, structures such as these.

Within abstract algebra, the invariant theorist studies the set of polynomials (objects like $5x^3 + 2y - 1$, or $x^2y + 3z$, for example), which is a type of structure called a *ring.* This means, essentially, that one can add, subtract, and multiply polynomials together to get other polynomials. One can *act upon* the ring of polynomials, modifying all polynomials according to a fixed rule. For instance, we can interchange x and y in all the polynomials. Remarkably, when this happens, some polynomials will remain unchanged ($x^2 + y^2 = y^2 + x^2$), while others are changed ($2x - y \neq 2y - x$). Those polynomials that remain unchanged are said to be *invariant* and in fact the set of all the invariant polynomials forms a ring called the *ring of invariants* (check: if you add together two invariant polynomials or if you multiply two invariant polynomials, the result is always an invariant polynomial). Acting on the ring of polynomials in different ways, i.e., using different rules for how to modify polynomials, creates different rings of invariants. Invariant theory is the study of these rings of invariants.

It always happens that a ring of invariants contains infinitely many elements, and yet often all these elements can be described by just a few "generators", which are in some sense the building blocks for the entire ring: every element in the ring is a sum of products of generators. The idea is that if we can find the generators, then we can describe the entire ring. A helpful analogy may be to consider the English language. Although infinitely many sentences are possible, every sentence is composed of words which in turn are composed of different combinations of just 26 letters. The words correspond to elements of the ring of invariants, and the letters correspond to the generators of that ring.

Finally, it needs to be noted that invariant theory takes essentially two different forms: "linear" and "multiplicative". Traditionally, invariant theory has focused on the linear case. However, within the last 30 years or so, the study of multiplicative invariant theory has grown and attracted some keen interest.

History

Historically, great importance has been placed on finding generators. From its inception, finding explicit generators for rings of invariants has been at the core of invariant theory.

Isaac Newton noticed a curious thing about the polynomial $x^2+y^2+z^2$. No matter how one permutes the variables, the polynomial remains unchanged. However, this is not true for a polynomial such as $2x + y + z$. Polynomials that remain unchanged in this way are said to be "invariant under permutation". In fact, the set of all polynomials in three variables that are invariant under permutation can be described using just three generating polynomials, $x + y + z$, $xy + xz + yz$, and xyz, in that every invariant is a sum of products of these three polynomials. Waring generalized this result to polynomials with arbitrarily many variables [Van85, p.77].

The father of modern invariant theory, David Hilbert (1862 – 1943), put invariant theory into a much more abstract setting, giving it a broader scope and more application. The theory he developed is still valuable to modern theoretical physics, and has been applied to coding theory as well. As Waring found generators for the ring of invariants under permutation, so Hilbert sought generators in the more abstract setting. Although rings of invariants have infinitely many elements, Hilbert proved that a great number of them have only finitely many generators. However, his results did not provide a way to actually construct the generators.

Emmy Noether (1882 – 1935), improved Hilbert's results by showing that a much larger class of invariant rings, in fact "almost all" invariant rings, have finitely many generators. Moreover, she created an algorithm that could actually find generators. However, from a computational point of view, her algorithm is unsatisfactory because it is extremely inefficient and it creates far more generators than are actually required.

Current Research

Just a few years ago an 80-year-old open question based on Noether's work concerning the degrees of the generators was resolved independently by Fleischmann and Fogarty [DK02, §3.7]. Without a doubt, invariant theory is an active area of research; invariant theory conferences are held and exciting results continue to be published.

Recent developments in invariant theory include an algorithm, implemented by Gregor Kemper, that efficiently computes generators for some rings of invariants under linear actions. Although much progress has been made in computational linear invariant theory, there is almost no literature on the computational aspects of multiplicative invariant theory (exceptions include [Lor01] and [Rei02]). The aim of this work is to start filling that gap by presenting algorithms for computing generators of rings of invariants under multiplicative actions.

1.2 A More Mathematical Introduction

The study of the relationship between a ring R and its subring of invariants R^G under the action of a group G, *invariant theory* for short, is a classical algebraic theme permeating virtually all areas of pure mathematics, some areas of applied mathematics, notably coding theory (e.g., [Slo77] and the references therein), and certain parts of theoretical physics as well.

In the most traditional setting, the ring R is a polynomial algebra $k[x_1, \ldots, x_n]$ over a field k and G acts on R via linear transformations of the space of variables $V = \sum_{i=1}^{n} kx_i$. This type of action is commonly called a *linear action*; the resulting algebra of invariants R^G is often referred to as an algebra of *polynomial invariants*. The ring theoretic properties of R^G have been rather thoroughly explored, especially for finite groups G. Early work of Hilbert [Hil90, Hil93] and of E. Noether [Noe16, Noe26] established that R^G is an integrally closed affine domain over k and R is a finitely generated R^G-module. More precise structural information is available when the characteristic of the base field k does not divide the order of G (the *nonmodular case*). The invariant algebra R^G is then known to be Cohen-Macaulay (Hochster and Eagon [HE71]). Furthermore, by the Shephard-Todd-Chevalley theorem [ST54], [Che55], R^G is a polynomial algebra over k precisely if G acts as a pseudoreflection group on V.

More recently, another type of action, usually called a *multiplicative action*, has attracted much attention. This action arises from *G-lattices*, that is, from free abelian groups A of finite rank n on which the group G acts by automorphisms. The G-action on A extends uniquely to an action on the group algebra $R = k[A]$. In explicit terms, after choosing a $\mathbb{Z}$-basis, A can be viewed as $\mathbb{Z}^n$, the G-action on A is given by a homomorphism $G \to \mathrm{GL}_n(\mathbb{Z})$, and the group algebra $R = k[A]$ becomes the Laurent polynomial algebra $k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$.

Multiplicative actions are technically more demanding than their linear counterpart, mainly due to the lack of a suitable grading on $k[A]$ preserved by the G-action. In addition, since the action is represented by integer matrices, the subject has an arithmetic aspect not present in the linear case. Multiplicative actions occur naturally in a variety of contexts including centers and prime ideals of group algebras (cf. [Ros78]), representation rings of Lie algebras (see [Bou68]), and Noether's rationality problem (e.g., [Sal87]).

The motivating problem of this dissertation can be summed up as follows:

Let A be a free abelian group of finite rank, let k be any commutative

> *ring, and let G be a finite group acting multiplicatively on the group algebra $k[A]$. Construct and implement an efficient algorithm for computing generators for $k[A]^G$, the subalgebra of multiplicative invariants.*

Finding explicit generators for invariants is at the core of classical invariant theory. In principle, Noether's method from [Noe16] (described in Theorem 2.3) can be adapted to deal with multiplicative (or other) invariants; it is, however, extremely inefficient. Existing algorithms for linear invariants, implemented in the computer algebra systems *Maple* and *Magma*, take advantage of the grading present in the linear case. One can then use Poincaré series as a powerful tool for a priori calculation of the number of independent invariants in each degree (Molien's formula). Since $k[A]$ admits no suitable G-grading under the multiplicative action, new methods must be developed.

In Chapter 3 we provide algorithms for computing generators when G is a reflection group (§3.3) and more generally, when G is a subgroup of a reflection group (Section 4.2). Furthermore, these methods result in an algorithm that rewrites any invariant as a polynomial in these generators. In the case where G is the symmetric group, this latter algorithm becomes the classical algorithm for rewriting symmetric polynomials as polynomials in elementary symmetric polynomials. The algorithms have been implemented using the computer algebra system *Magma*, and the program source code and some sample output can be found in the appendices.

CHAPTER 2

PRELIMINARIES

2.1 Overview

In §2.2 we will compare linear and multiplicative invariant theory, and examine some fundamental theorems giving us insight into the structure of invariant rings in general. Section 2.3 discusses the particulars of the multiplicative setting, describing some of the main results, and how they motivate the results of Chapter 3. Finally, §2.4 is more technical in nature, laying down some of the details of reflection groups and root systems, powerful tools for the computation of generators.

2.2 Invariant Theory

2.2.1 Linear and Multiplicative Invariants

In its most general form, invariant theory considers a ring R, a group $G \subseteq \mathrm{Aut}(R)$, and it studies the structure of the subring of invariants

$$R^G := \{\, r \in R \;:\; r^g = r \;\forall\; g \in G \,\}$$

where the r^g denotes the image of r under g.

A major area of study within invariant theory is the study of *polynomial invariants*, or *linear invariant theory*. Consider a free k-module V of finite rank and a group

$G \subseteq \mathrm{GL}(V)$. The action of G on V extends uniquely to k-algebra automorphisms of $\mathrm{Sym}(V)$, the symmetric algebra of V.

$$\mathrm{Sym}(V) = k \oplus V \oplus \mathrm{Sym}^2(V) \oplus \mathrm{Sym}^3(V) \oplus \cdots$$

Here $\mathrm{Sym}^m(V)$ denotes the m-th symmetric power of V, which consists of the homogeneous elements of degree m. The action of G on $\mathrm{Sym}(V)$ is called a linear action. Once a basis $\{ x_1, \ldots, x_n \}$ for V is fixed, $\mathrm{Sym}(V)$ can be viewed as the polynomial ring $\mathrm{Sym}(V) \cong k[x_1, \ldots, x_n]$, and $\mathrm{Sym}^m(V)$ as the set of homogeneous polynomials of degree m.

Since G stabilizes V and the action of G is a k-algebra automorphism, G also stabilizes $\mathrm{Sym}^m(V)$, thus providing a G-invariant grading of $\mathrm{Sym}(V)$. Consequently we know the ring of invariants is graded, and tools such as Molien's theorem allow one to quickly compute the ring of invariants [Smi95, p.86].

Within the last 35 years or so, a new type of group action on a ring, the *multiplicative action* (also called exponential, lattice, or monomial action), as started gaining interest. Consider now a free abelian group A of finite rank, and a group $G \subseteq \mathrm{GL}(A)$. The action of G on A extends uniquely to k-algebra automorphisms of the group ring $k[A]$. If we fix a generating set $\{ x_1, \ldots, x_n \}$ for A, then we can view $k[A]$ as the Laurent polynomial ring $k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Multiplicative actions stabilize a finite rank generating group of units, whereas linear actions stabilize a finite rank generating k-subspace. In the general multiplicative setting no connected G-invariant grading of $k[A]$ is present (i.e., no G-invariant grading whose degree 0 component is k).

2.2.2 Basic Theorems of Invariant Theory

We present two theorems that give us insight into the structure of invariant rings. Both theorems are true for invariant theory in general, so they can be applied to both the linear and the multiplicative settings. The first theorem is due to Noether [Noe26]. A proof can be found in [Smi95, p. 26]. Recall that a k-algebra R is called *affine* if R is finitely generated, or equivalently, if R is the homomorphic image of some polynomial algebra in finitely many variables over k. Also, recall that a commutative ring is called *noetherian* if every ideal is finitely generated. More generally, a module is called noetherian if every submodule is finitely generated.

Theorem 2.1 (Noether's Finiteness Theorem). *Let R be a commutative, affine k-algebra, where k is any commutative ring. If $G \subseteq \mathrm{Aut}_{k\text{-}alg}(R)$ is a finite group, then R is a finitely generated R^G-module. If additionally k is noetherian, then R^G is an affine k-algebra as well.*

The following consequence is used as we explore subgroups of reflection groups in §4.2. We recall that by Hilbert's basis theorem, any affine algebra over a noetherian ring will itself be noetherian. Additionally, a module over a noetherian ring is a noetherian module if and only if it is finitely generated

Corollary 2.2. *If k is noetherian and $G \subsetneq H$ are finite groups contained in $\mathrm{Aut}_{k\text{-}alg}(R)$, then R^G is a finitely generated R^H-module.*

Proof. By the theorem, R is finite over R^H. Since k is noetherian, R^H is an affine algebra over k, and by Hilbert's basis theorem this implies that R^H is noetherian. Thus R is a noetherian R^H-module. Submodules of noetherian modules are finitely generated, so R^G is a finitely generated R^H-module. □

Beyond simply knowing that the ring of invariants is finitely generated, we can often exhibit an explicit finite set of generators for R^G. The following theorem has its origin in [Noe16], while its current form is due, independently, to Fleischmann [Fle00] and Fogarty [Fog01], with simplification of the proof due to Benson. The most recent statement and proof of the theorem can be found in [DK02, Cor. 3.7.4]. If G acts on R we define the *G-trace* of $r \in R$ as

$$\mathrm{tr}_G(r) := \sum_{g \in G} r^g.$$

Theorem 2.3 (Noether's Method for Computing Invariant Generators). *Let R be a commutative, affine k-algebra, where k is any commutative ring, and let $G \subseteq \mathrm{Aut}_{k\text{-}alg}(R)$ be a finite group such that $|G|$ is invertible in k. If $r_1, \ldots, r_m$ are* *algebra generators for R such that the k-submodule $\sum_{i=1}^{m} kr_i$ of R is G-stable, then R^G is generated by the elements $\operatorname{tr}_G(r_1^{d_1} \cdots r_m^{d_m})$ where $(d_1, \ldots, d_m)$ varies over all m-tuples of nonnegative integers such that $d_1 + \cdots + d_m \leq |G|$.*

Remark. The elements $r_1, \ldots, r_m$ as in the above theorem can always be found, for if X is any finite set of algebra generators of R, then we may assign

$$\{ r_1, \ldots, r_m \} := \bigcup_{g \in G} X^g.$$

While this theorem does indeed provide an algorithm for computing generators of an invariant ring, it is generally extremely inefficient. For example, suppose R is the polynomial algebra $k\,[x_1, \ldots, x_n]$ and S_n acts on R by permuting the variables. It is a classical result that R^{S_n} is generated by the n elementary symmetric polynomials $e_1, \ldots, e_n$ defined by

$$e_t := \sum_{1 \leq i_1 < i_2 < \cdots < i_t \leq n} x_{i_1} x_{i_2} \cdots x_{i_t}. \tag{2.1}$$

However, were we to use Noether's method to find generators for R^{S_n}, we would have to compute $\operatorname{tr}_{S_n}(x_1^{d_1} \cdots x_n^{d_n})$ for all possible sums of nonnegative integers $d_1 + \cdots + d_n \leq n!$ When $n = 10$ this amounts to $\binom{10!+10}{10} \approx 1.09 \times 10^{59}$ trace calculations, despite the fact that only the 10 elementary symmetric polynomials suffice to generate $R^{S_{10}}$.

2.3 Multiplicative Invariants

2.3.1 Set-Up

We start with a free abelian group of finite rank, $(A, +)$, on which a finite group, $G \subseteq \mathrm{GL}(A)$ acts. The G-action on A extends uniquely to an action on the group algebra $k[A]$, where k is any commutative ring. The operation of addition in A becomes multiplication in $k[A]$, and we will write a^* for the canonical image of a in $k[A]$. Observe, for instance, that $(m - a)^* = m^*(a^*)^{-1}$. Thus, a typical element $f \in k[A]$ can be uniquely written $f = \sum_{a \in A} k_a a^*$ with the $k_a \in k$ almost all zero.

Definition 2.4. Write $f \in k[A]$ as $\sum_{a \in A} k_a a^*$ with the $k_a \in k$ almost all zero. The set

$$\operatorname{Supp}(f) := \{\, a \in A \ : \ k_a \neq 0 \,\}$$

is called the *support of f*.

If we choose a $\mathbb{Z}$-basis $\{\, x_1, \ldots, x_n \,\}$ for A, then A can be viewed as $\mathbb{Z}^n$, the G-action on A is given by an embedding $G \hookrightarrow \mathrm{GL}_n(\mathbb{Z})$, and the group algebra $k[A]$ becomes the Laurent polynomial algebra $k[(x_1^*)^{\pm 1}, \cdots, (x_n^*)^{\pm 1}]$. We will call the elements of A either lattice points (when we wish to emphasize the lattice structure of A) or monomials (to emphasize the role of A in $k[A]$). We will call the elements of $k[A]$ Laurent polynomials.

Example 2.5. Suppose that $A \cong \mathbb{Z}^2$ with ordered basis $\{\, x, y \,\}$. For ease of notation let $\mathbf{x} = x^*$ and $\mathbf{y} = y^*$. so that $k[A] = k[\mathbf{x}^{\pm 1}, \mathbf{y}^{\pm 1}]$, and $g \in \mathrm{GL}_2(\mathbb{Z})$ is the matrix $\left(\begin{smallmatrix} 1 & -3 \\ 1 & -2 \end{smallmatrix}\right)$. As an automorphism of A, g (acting from the right on row vectors) sends x to $x - 3y$ and y to $x - 2y$. As an automorphism of $k[A]$, g sends $\mathbf{x}$ to $\mathbf{x}\mathbf{y}^{-3}$ and $\mathbf{y}$ to $\mathbf{x}\mathbf{y}^{-2}$. Thus, for $k_1, k_2 \in k$,

$$\begin{aligned}(k_1\mathbf{x}\mathbf{y}^5 + k_2\mathbf{x}^{-2}\mathbf{y})^g &= k_1(\mathbf{x}\mathbf{y}^{-3})(\mathbf{x}\mathbf{y}^{-2})^5 + k_2(\mathbf{x}\mathbf{y}^{-3})^{-2}(\mathbf{x}\mathbf{y}^{-2}) \\ &= k_1\mathbf{x}^6\mathbf{y}^{-13} + k_2\mathbf{x}^{-1}\mathbf{y}^4\end{aligned}$$

2.3.2 Orbit Sums

Perhaps the most basic way to create an element of $k[A]^G$ is to construct a *monomial orbit sum*,

$$\sigma_G(a) := \sum_{b \in a^G} b^*,$$

where $a \in A$. One can take the orbit sum of any element of $k[A]$, but our focus shall rest exclusively on monomial orbit sums and we will simply write “orbit sum” to mean a monomial orbit sum. Furthermore, when the context is clear, we will suppress the subscript G.

Theorem 2.6. *The set of orbit sums $\{\,\sigma(a)\ :\ a \in A\,\}$ forms a k-basis for $k[A]^G$. That is, if A/G denotes a transversal for the G-orbits in A, then*

$$k[A]^G = \bigoplus_{a \in A/G} k\sigma(a).$$

Proof. Clearly $\sigma(a) \in k[A]^G$. The $\sigma(a)$ are linearly independent since their supports are disjoint. If $f = \sum k_a a^* \in k[A]^G$, and $g \in G$, then $f = f^g = \sum k_a (a^*)^g = \sum k_a (a^g)^*$. Comparing the coefficients of a^g on both sides we obtain $k_{a^g} = k_a$. In other words, the coefficients k_b have the same constant value k_{a^G} for all $b \in a^G$. It follows that $f = \sum k_{a^G}\sigma(a)$ and thus the $\sigma(a)$ span $k[A]^G$ as a k-module. □

Corollary 2.7. *$k[A]^G$ is an affine k-algebra. Furthermore, if $H \subseteq \mathrm{GL}(A)$ is finite and $G \subseteq H$, then $k[A]^G$ is a finitely generated $k[A]^H$-module.*

Proof. The structure constants for the orbit sum basis belong to the subring k' of k that is generated by 1_k. Thus, as a k-algebra, $k[A]$ is defined over k':

$$k[A]^G = k \otimes_{k'} R' \quad \text{where} \quad R' = \bigoplus_{a \in A/G} k'\sigma(a) = k'[A]^G. \tag{2.2}$$

Clearly k' is a noetherian ring, so by Noether's finiteness theorem 2.1, R' is affine over the noetherian ring k', and hence $k[A]^G$ is an affine k-algebra.

By Corollary 2.2, $k'[A]^G$ is a finitely generated $k'[A]^H$-module. Again from equation (2.2) it is clear that $k[A]^G$ is a finitely generated $k[A]^H$-module. □

Remark. The orbit sums $\sigma(a)$ $(a \in A)$ only involve the coefficients 0 and 1 from k, hence each $\sigma(a)$ can be viewed as the image of a corresponding orbit sum in $\mathbb{Z}[A]$. Consequently,

$$k[A]^G = k \otimes_{\mathbb{Z}} \mathbb{Z}[A]^G.$$

Thus, if $k \to k'$ is any ring homomorphism, then

$$k'[A]^G = k' \otimes_k k[A]^G. \tag{2.3}$$

In particular, we may work, whenever convenient, over $k = \mathbb{Z}$, or at the very least with $\mathrm{char}(k) = 0$.

Finally, while the set of *all* orbit sums generates $k[A]^G$ as a k-module, one can always find a finite set of orbit sums that generates $k[A]^G$ as an algebra. Indeed, by Corollary 2.7 above, there are finitely many algebra generators for $k[A]^G$, and each of these generators is a finite linear combination of orbit sums. Clearly then the (finitely many) orbit sums occurring in these linear combinations are contained in $k[A]^G$ and generate $k[A]^G$.

Example 2.8. Recall definition (2.1) and let $e_1, \ldots, e_n$ denote the n elementary symmetric polynomials in $k[x_1, \ldots, x_n]$. Now $k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] = k[x_1, \ldots, x_n][e_n^{-1}]$ and so

$$\begin{aligned} k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]^{S_n} &= k[x_1, \ldots, x_n]^{S_n}[e_n^{-1}] \\ &= k[e_1, \ldots, e_n, e_n^{-1}] \end{aligned}$$

Now observe that e_i is exactly $\sigma_{S_n}(x_1 x_2 \cdots x_i)$, and $e_n^{-1} = \sigma_{S_n}((x_1 \cdots x_n)^{-1})$, so we have found algebra generators for the ring of invariants that are orbit sums.

In Theorem 3.11 we will see how to use orbit sums to generalize this fact to reflection groups.

2.3.3 Basic Results

We record here some basic results about the structure of rings of multiplicative invariants to motivate the findings in Chapter 3. The articles [Far84, Far85] are recommended as a good introduction to multiplicative invariant theory.

One of the most celebrated results of linear invariant theory is the so called Shephard-Todd-Chevalley theorem [ST54, Che55]; many of the theorems in multiplicative invariant theory are the result of finding analogies to the Shephard-Todd-Chevalley theorem in the multiplicative setting. It should be mentioned that Serre [Ser67] was also a significant contributor to the Shephard-Todd-Chevalley theorem. Recall that in the linear setting V is a free k-module of finite rank, and $G \subseteq \mathrm{GL}(V)$. The group G is called a *pseudoreflection group* if it is generated by pseudoreflections, that is, elements $g \in G$ such that $\mathrm{Id} - g$ has rank 1. Recall that for a k-module V of finite rank, $\mathrm{Sym}(V)$ can be realized as a polynomial algebra.

Theorem 2.9 (Shephard-Todd, Chevalley, Serre). *Assume $G \subseteq \mathrm{GL}(V)$ is finite and that k is a field with char$(k) \nmid |G|$. Then:* $\mathrm{Sym}(V)^G$ *is a polynomial algebra over k if and only if G is a pseudoreflection group.*

In the multiplicative setting, the first analogous question one might ask is, when is $k[A]^G$ a group algebra? The following proof is found in [Lor01].

Proposition 2.10. *$k[A]^G$ is a group algebra if and only if G acts trivially on A.*

Proof. Of course "only if" is the only interesting direction. We may assume k to be a field by fixing a map $k \to K$ into a field K and using equation (2.3). The group of units of $k[A]$ is given by $\mathrm{U}(k[A]) = \mathrm{U}(k) \times A$. [This follows from the fact that A is an ordered group (c.f. [Pas71, pp. 112 – 114]). Alternatively, viewing $k[A]$ as the Laurent polynomial algebra in n indeterminates, one can argue by induction on n using a degree argument.] Since group algebras are generated, as k-algebras, by units, and $\mathrm{U}(k[A]^G) = \mathrm{U}(k[A])^G = \mathrm{U}(k) \times A^G$, our hypothesis implies that $k[A]^G = k[A^G]$. By Noether's Finiteness Theorem $k[A]$ is integral over $k[A]^G$, but on the other hand, A/A^G is torsion-free. Thus we must have $A = A^G$, as desired. □

At the other extreme, the following theorem, proved independently in [Ste75] and [Far84], addresses the circumstances under which $k[A]^G$ is a polynomial ring. Note that a group G is called a *reflection group* if it is generated by reflections, that is, pseudoreflections $g \in G$ such that $g^2 = \mathrm{Id}$.

Theorem 2.11. *$k[A]^G$ is a polynomial ring if and only if G is a reflection group and A can be realized as a weight lattice whose Weyl group is G.*

We shall make a more thorough examination of reflection groups, weight lattices, etc. in the next section. The above theorem is actually a special case of the next one [Ste75, Far86].

Theorem 2.12. *Let $G \subseteq \mathrm{GL}(A)$ be a finite group. Then $k[A]^G$ is the tensor product of a polynomial ring and a group algebra if and only if G acts as a reflection group on A/A^G and A/A^G can be realized as a weight lattice whose Weyl group is induced by G.*

In fact, we can push the generality even further. The following is implicit in [Far85] and made explicit in [Lor01].

Theorem 2.13. *Let $G \subseteq \mathrm{GL}(A)$ be a finite reflection group. Then $k[A]^G = k[M]$ for some monoid M that can be embedded into $\mathbb{Z}^n$ for some n.*

In [Lor01] Lorenz indicates how to compute a finite set of monoid generators for such an M, thus producing algebra generators for $k[A]^G$. The converse of the above theorem is currently an open problem.

In §3.3 we will derive a slightly different set of algebra generators which, while not generating $k[A]^G$ as a monoid algebra, do lend themselves nicely to computation. Continuing the theme of generalizing the above theorems, §4.2 addresses the issue of computing algebra generators for $k[A]^G$ when G is a subgroup of a reflection group.

The next theorem, due to Z. Reichstein [Rei02] makes use of the recent notion of a SAGBI basis to create another analog to the Shephard-Todd-Chevalley theorem. The term SAGBI stands for "Subalgebra Analog to Gröbner Bases for Ideals", and was introduced by Robbiano and Sweedler in [RS90]. Such bases are characterized by the existence of the *subduction algorithm*, a particularly "nice" algorithm making it possible to express any element in the subalgebra as a polynomial in the basis elements.

Theorem 2.14. *$k[A]^G$ has a finite SAGBI basis if and only if G is a reflection group.*

Note that not all subalgebras have SAGBI bases, and even though a finite SAGBI basis may not exist, there may still exist a finite generating set and an algorithm capable of expressing subalgebra elements in terms of the generators. This will be the case when we treat invariants under subgroups of reflection groups.

2.4 Reflection Groups, Root Systems, and Weight Lattices

We follow the basic notions and notation laid out by Humphries [Hum72, Hum90].

2.4.1 Reflections

Start with E, a real finite dimensional vector space with a positive definite symmetric bilinear form (α, β).

Definition 2.15. A *reflection* is a linear operator g on E which sends some nonzero vector α to $-\alpha$ (written exponentially, $\alpha^g = -\alpha$) and fixes pointwise the hyperplane H_g that is orthogonal to α. Equivalently, a reflection is a linear operator g on E with $\operatorname{rank}(g - \mathrm{Id}) = 1$ such that $g^2 = \mathrm{Id}$.

Indeed, since $E = \mathbb{R}\alpha \oplus H_g$, the matrix of a reflection g with respect to a basis of E obtained by completing α by a basis of H_g is the diagonal matrix $\operatorname{diag}(-1, 1, \ldots, 1)$. Thus $g^2 = \mathrm{Id}$ and $\operatorname{rank}(g - \mathrm{Id}) = 1$. Conversely, suppose $g \in \mathrm{GL}(E)$ satisfies $g^2 = \mathrm{Id}$ and $\operatorname{rank}(g - \mathrm{Id}) = 1$. Putting $L := \operatorname{Im}(g - \mathrm{Id})$ and $H := \operatorname{Ker}(g - \mathrm{Id})$ we have $\dim L = 1$ and $\dim H + \dim L = \dim E$. Thus L is a line on which g acts as -1 (since $g^2 = \mathrm{Id}$), and H is a hyperplane on which g acts trivially. Thus $E = L \oplus H$ and by the G-invariance of $(\ ,\ )$, we must have $H \subseteq L^\perp$ and so $H = L^\perp$.

We label the reflection that takes α to $-\alpha$ by g_α and note that $g_\alpha = g_{c\alpha}$ for any $c \in \mathbb{R}$.

Definition 2.16. A group $G \subseteq \mathrm{GL}(E)$ is called a *reflection group* if it is generated by reflections.

Not every element of a reflection group is a reflection, and reflection groups may contain more reflections than are needed to generate the group.

If g_α is a reflection and $\beta \in E$, then we observe

$$\beta^{g_\alpha} = \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha. \tag{2.4}$$

The scalar $2(\beta, \alpha)/(\alpha, \alpha)$ occurs often enough to warrant an abbreviation, $\langle \beta, \alpha \rangle$.

2.4.2 Root Systems

A subset Φ of E is called a *crystallographic root system* in E if the following conditions are satisfied:

1. Φ is finite, spans E, and does not contain 0.

2. If $\alpha \in \Phi$ then $\pm\alpha \in \Phi$, but no other scalar multiples of α are in Φ.

3. If $\alpha \in \Phi$, then the reflection g_α stabilizes Φ.

4. If $\alpha, \beta \in \Phi$ then $\langle \beta, \alpha \rangle \in \mathbb{Z}$.

Because of condition (2), Φ is often called a *reduced* root system (e.g. [Bou68]). Condition (4) is often called the *crystallographic condition.*

The lattice $\mathbb{Z}\Phi \subseteq E$ is called the *root lattice.* Given a crystallographic root system Φ in E, the group $\mathcal{W}$ generated by the reflections g_α ($\alpha \in \Phi$) is called the *Weyl group* for Φ.

Every root system Φ contains a subset Δ, called a *base* of Φ such that

1. Δ is a basis for E,

2. $\Phi \subseteq \mathbb{N}\Delta \cup -\mathbb{N}\Delta$.

By the notation $\mathbb{N}\Delta$, we mean the set of all finite sums $\left\{ \sum_{\delta \in \Delta} n_\delta \delta \ : \ n_\delta \in \mathbb{N} \right\}$. The elements $\delta \in \Delta$ are called *simple roots*, and the corresponding reflections g_δ in $\mathcal{W}$ are called *simple reflections.* As a consequence of (2), if $\delta_1, \delta_2 \in \Delta$ are distinct simple roots then the angle between them is obtuse, that is, $(\delta_1, \delta_2) \leq 0$; see [Hum90, p. 9].

2.4.3 Applications to Multiplicative Invariant Theory

To see how these ideas arise in multiplicative invariant theory, embed $A \cong \mathbb{Z}^n$ into the n-dimensional $\mathbb{R}$-vector space

$$V := A \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^n$$

and view $G \subseteq \mathrm{GL}(A)$ as a subgroup of $\mathrm{GL}(V)$. We can always construct a G-invariant inner product on V by taking an arbitrary inner product and "averaging" it over the group. That is, if $[\ ,\ ]$ denotes an arbitrary inner product on V, we define a new inner product $(\ ,\ )$ by

$$(\alpha, \beta) := \frac{1}{|G|} \sum_{g \in G} [\alpha^g, \beta^g].$$

Then, for any $h \in G$,

$$(\alpha^h, \beta^h) = \frac{1}{|G|} \sum_{g \in G} [\alpha^{hg}, \beta^{hg}] = (\alpha, \beta).$$

Thus each member of G becomes an orthogonal transformation with respect to this inner product.

For the remainder of this chapter we assume that

$$G \subseteq \mathrm{GL}(A) \text{ is a reflection group.}$$

Observe that V^G is exactly the vector space formed by taking the intersection of the hyperplanes $H_g = V^{\langle g \rangle}$ for all the generating reflections $g \in G$. Define π to be the orthogonal projection of V onto $(V^G)^\perp$, and let $\rho := \mathrm{Id} - \pi$. Assign

$$E := \pi(V) = (V^G)^\perp \quad \text{and} \quad r := \dim E.$$

It is worth noting that ρ is the usual *Reynolds operator*,

$$\rho(v) = \frac{1}{|G|} \sum_{g \in G} v^g. \tag{2.5}$$

(In particular, ρ and $\pi = \mathrm{Id} - \rho$ do not depend on the choice of inner product.) To see the above equality, denote the right hand side above by $\rho'(v)$ for now and observe that $\rho'(v) \in V^G$. Then $\rho' \mid_{V^G} = \mathrm{Id}_{V^G}$, while for $v \in E = (V^G)^\perp$ one calculates

$$\begin{aligned}
(\rho'(v), \rho'(v)) &= \frac{1}{|G|} \sum_{g \in G} (v^g, \rho'(v)) \\
&= \frac{1}{|G|} \sum_{g \in G} (v^g, \rho'(v)^g) \\
&= (v, \rho'(v)) \\
&= 0
\end{aligned}$$

Thus $\rho' \mid_E = 0$, and hence ρ' is the orthogonal projection of V to V^G, that is, $\rho' = \rho$.

Two helpful observations can be made by considering equation (2.5):

$$v - v^g \in E \text{ for all } v \in V \tag{2.6}$$

and

$$\pi(v^g) = \pi(v)^g \text{ for all } v \in V. \tag{2.7}$$

By (2.5), $\rho(v - v^g) = 0$, and so $v - v^g = \pi(v - v^g) \in \pi(V) = E$, giving us (2.6). Additionally, $\rho(v - v^g) = 0$ implies $\rho(v)^g = \rho(v) = \rho(v^g)$. Substituting $Id - \pi = \rho$ gives us (2.7).

We proceed now to construct a crystallographic root system $\Phi \subseteq A$ for the space $E = \pi(V)$. Note that the construction of Φ that follows depends on the group G. The following construction is also presented in Algorithm 1.

If g is a reflection in G, the one-dimensional vector space $(H_g)^\perp = \ker(g + \mathrm{Id})$ meets A to form an infinite cyclic group, denoted A_g. Let a_g denote one of the two possible generators for A_g and define

$$\Phi := \{\, \pm a_g \ : \ g \text{ is a reflection in } G \,\}. \tag{2.8}$$

Observe that $\Phi \subseteq E$. Furthermore, by construction, we have an inclusion of lattices $\mathbb{Z}\Phi \subseteq A$.

Algorithm 1 Constructing a root system from a reflection group

```
Input: a finite reflection group, $G$
Let $X := \{\, g \in G \ : \ g \text{ is a reflection} \,\}$
Let $R := \bigcup_{g \in X} \{\, \text{a generator of } \operatorname{Ker}(g + \mathrm{Id}) \,\}$
Let $\Phi := \{\, \pm a \ : \ a \in R \,\}$
Output: $\Phi$
```

The following lemma is part of the "folklore" of finite reflection groups and its straightforward proof appears in [Far86].

Lemma 2.17. *Φ is a crystallographic root system for E.*

Certainly Φ is not the only root system for E, but it is a "maximal" one contained in A. It is clear that G restricted to E is the Weyl group for Φ.

Constructing a base Δ for Φ is a simple matter. Note that $E \neq \bigcup_g H_g$ where g runs over the (finitely many) reflections in G, so there exists a vector $\gamma \in E$ not fixed by any reflection in G. Let $\Phi_+(\gamma)$ denote the set of those roots $\alpha \in \Phi$ such that $(\alpha, \gamma) \geq 0$. A root in $\Phi_+(\gamma)$ is called *indecomposable* if it cannot be written as the sum of two roots also in $\Phi_+(\gamma)$. Then the set of indecomposable roots, $\Delta(\gamma)$, forms a base for Φ. See [Hum72, Thm. 10.1] for the proof of this fact. Algorithm 2 summarizes these ideas.

Algorithm 2 Compute a base for a root system

```
Input: A root system, $\Phi \subseteq E$
repeat
    Choose a random $\gamma \in V$
until $(\gamma, a) \neq 0$ for all $a \in \Phi$
Let $\Phi_+ := \{ a \in \Phi \ : \ (\gamma, a) > 0 \}$
Let $\Delta := \Phi_+ \setminus \{ a + b \ : \ a, b \in \Phi_+ \}$
Output: $\Delta$
```

Example 2.18. Consider the group $G = \left\langle g_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), g_2 = \left(\begin{smallmatrix} -1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \right\rangle \cong S_3$, acting (by right multiplication) on $A = \mathbb{Z}^2$. The elements g_1 and g_2 are reflections, so G is a reflection group, and there exists a third reflection in G, namely $g_3 = \left(\begin{smallmatrix} 1 & -1 \\ 0 & -1 \end{smallmatrix}\right)$. The other elements of G are the identity and two elements of order 3. While g_2 and g_3 are not orthogonal reflections with respect to the standard inner product, all reflections are orthogonal with respect to the inner product induced by the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Figure 2.1 shows lattice $A = \mathbb{Z}^2 \subseteq E = V = \mathbb{R}^2$ and the hyperplanes H_i (intersecting at the origin) fixed by the reflections g_i $(i = 1, 2, 3)$. The points $\pm a_i$ are then the generators of the infinite cyclic group $H_i^\perp \cap A$, and so $\{ \pm a_i \ : \ i = 1, 2, 3 \}$ forms a root system in $E = V = \mathbb{R}^2$. Finally, a base $\Delta(\gamma)$ is constructed using, for instance, $\gamma = (1, 2)$. In fact, any γ in the open region bounded on the right by H_1 and bounded on the left by H_2 will produce the same base.

2.4.4 The Weight Lattice

The root system Φ gives rise to the *weight lattice* $\Lambda \subseteq E$, defined:

$$\Lambda := \{ v \in E = \pi(V) \ : \ v - v^g \in A_g \ \forall \ \text{ reflections } g \in G \}. \tag{2.9}$$

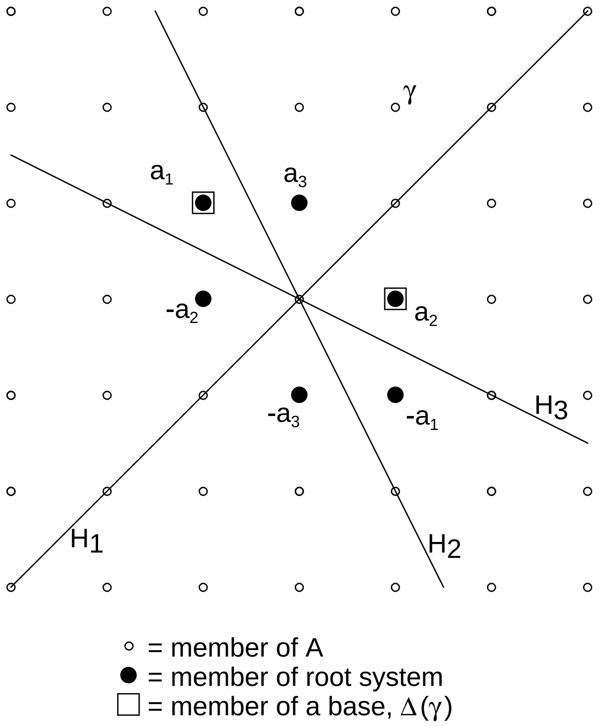

Figure 2.1: The root system and base described in Example 2.18.

Equivalently, by (2.4),

$$\Lambda = \{\, v \in E = \pi(V) \ : \ \langle v, a_g \rangle \in \mathbb{Z} \ \forall \ a_g \in \Phi \,\}\,. \tag{2.10}$$

Thirdly, we remark that Λ can be described directly, without reference to Φ as follows:

$$\Lambda = \{\, v \in E = \pi(V) \ : \ v - v^g \in A \ \forall \ g \in G \,\}\,. \tag{2.11}$$

Indeed, since $a_g \in A$, the condition $v - v^g \in A_g$ for all reflections $g \in G$ certainly implies $v - v^g \in A$ for all reflections $g \in G$, and since G is generated by reflections, $v - v^g \in A$ actually holds for *all* $g \in G$. Conversely, if $v - v^g \in A$ holds for all $g \in G$, the for all reflections $g \in G$ we have $v - v^g \in \operatorname{Ker}(\operatorname{Id} + g) \cap A = A_g$.

Finally, we remark that in the foregoing it suffices to check the conditions for all *simple* reflections $g \in G$ or all $a_g \in \Delta$. See [Hum72, p. 67].

By the above definitions for Λ it is clear that

$$\mathbb{Z}\Phi \subseteq \Lambda \subseteq E.$$

Perhaps one of the most useful lemmas for our purposes is the following, again found in [Far86].

Lemma 2.19. $\pi(A) \subseteq \Lambda$.

Proof. Recalling (2.6), we know $a - a^g \in \pi(V) \cap A$ for any $a \in A$. Thus, using (2.7), $\pi(a) - \pi(a)^g = \pi(a - a^g) = a - a^g \in A$. By equation (2.11) it now follows that $\pi(A) \subseteq \Lambda$. □

Fix a base $\Delta = \{\, \delta_1, \ldots, \delta_r \,\}$, and let g_i denote the simple reflection corresponding to δ_i (so $\delta_i = a_{g_i}$, and $\delta_i^{g_i} = -\delta_i$). The *fundamental dominant weights (relative to* Δ*)* are the weights $\lambda_1, \ldots, \lambda_r \in \Lambda$ defined by

$$\lambda_i - \lambda_i^{g_j} = \begin{cases} \delta_i \text{ if } i = j \\ 0 \text{ if } i \neq j. \end{cases} \tag{2.12}$$

Recalling equation (2.4), $\lambda_i^{g_j} = \lambda_i - 2(\lambda_i, \delta_j)\delta_j/(\delta_j, \delta_j)$, and hence

$$\frac{2(\lambda_i, \delta_j)}{(\delta_j, \delta_j)} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j. \end{cases} \tag{2.13}$$

Thus $\{\, \lambda_1, \ldots, \lambda_r \,\}$ is exactly the basis of E that is dual to $\left\{ \frac{2}{(\delta_1,\delta_1)}\delta_1, \ldots, \frac{2}{(\delta_r,\delta_r)}\delta_r \right\}$.

The fundamental dominant weights form a $\mathbb{Z}$-basis for the weight lattice Λ:

$$\Lambda = \bigoplus_{i=1}^{r} \mathbb{Z}\lambda_i.$$

The monoid $\Lambda_+ = \Lambda_+(\Delta)$ of *dominant weights* for Δ is defined

$$\Lambda_+ := \bigoplus_{i=1}^{r} \mathbb{N}\lambda_i. \tag{2.14}$$

Now it is straightforward to show that

$$\Lambda_+ = \{\, \lambda \in \Lambda \;:\; (\lambda, \delta) \geq 0 \;\forall\; \delta \in \Delta \,\}. \tag{2.15}$$

Figure 2.2 depicts the dominant weights for a base, continuing example 2.18.

2.4.5 Computing Fundamental Dominant Weights

In expression (2.12) we knew that λ_i was in E to begin with. However, any $v \in V$ satisfying

$$\pi(v) - v^{g_j} = \begin{cases} \delta_i \text{ if } i = j \\ 0 \text{ if } i \neq j. \end{cases} \tag{2.16}$$

must be contained in E since $0, \delta_i, \pi(v) \in E$. Consequently such a v would be a fundamental dominant weight. Identify A with $\mathbb{Z}^n$, and let $[\pi]$ and $[g_i]$ denote the matrices of the linear transformations π and g_i, with respect to the standard basis. Then we have

$$\pi(v) - v^{g_j} = v([\pi] - [g_i]).$$

Thus

$$\begin{bmatrix} \text{---}\ \lambda_1\ \text{---} \\ \vdots \\ \text{---}\ \lambda_r\ \text{---} \end{bmatrix} ([\pi] - [g_i]) = \begin{bmatrix} \text{---}\ 0\ \text{---} \\ \vdots \\ \text{---}\ \delta_i\ \text{---} \\ \vdots \\ \text{---}\ 0\ \text{---} \end{bmatrix}$$

and so

$$\begin{bmatrix} \text{---}\ \lambda_1\ \text{---} \\ \vdots \\ \text{---}\ \lambda_r\ \text{---} \end{bmatrix} \sum_{i=1}^{r}([\pi] - [g_i]) = \begin{bmatrix} \text{---}\ \delta_1\ \text{---} \\ \vdots \\ \text{---}\ \delta_r\ \text{---} \end{bmatrix}.$$

Assign $M := \sum_{i=1}^{r}([\pi] - [g_i])$. Then

$$\begin{bmatrix} \text{---}\ \lambda_1\ \text{---} \\ \vdots \\ \text{---}\ \lambda_r\ \text{---} \end{bmatrix} = \begin{bmatrix} \text{---}\ \delta_1\ \text{---} \\ \vdots \\ \text{---}\ \delta_r\ \text{---} \end{bmatrix} M^{-1}. \tag{2.17}$$

One can see from the above equation that $\lambda_i \in \mathbb{Q}^n$ for all i, since the entries of M are rational and each simple root is an element of $A = \mathbb{Z}^n$. Consequently,

$$\Lambda \subseteq \mathbb{Q} \otimes A. \tag{2.18}$$

Remark. The matrix M above is indeed invertible: with respect to a basis of V of the form $\mathcal{B} \cup \{\, \delta_1, \ldots, \delta_r \,\}$ where $\mathcal{B}$ is any basis of $\rho(V) = V^G$, the matrix of $M = r[\pi] - \sum_{i=1}^{r}[g_i] \in \mathrm{End}_{\mathbb{R}}(V)$ is

$$\left[\begin{array}{c|c} -r\,\mathrm{Id}_{s\times s} & \\ \hline & \left(2\frac{(\delta_i,\delta_j)}{(\delta_j,\delta_j)}\right)_{i,j=1,\ldots,r} \end{array}\right]_{n\times n}$$

where $s = n - r$. Here the matrix in the lower right hand corner is called the *Cartan matrix* of Φ. This matrix is nonsingular [Hum72, p. 55], and hence M is nonsingular.

2.4.6 Weyl Chambers

The hyperplanes $H_g = V^{\langle g \rangle}$ (g a reflection) partition V into finitely many regions.

Definition 2.20. Let $G \subseteq \mathrm{GL}(A)$ be a finite reflection group. The connected components of $V \setminus \cup \{\, H_g : g \text{ is a reflection} \,\}$ are open sets called *Weyl chambers.* Let $\mathcal{C}$ denote a Weyl chamber, and we will call its closure, $\overline{\mathcal{C}}$ a *closed Weyl chamber.*

Equivalently, suppose $\Phi = \{\, \pm a_g \;:\; g \text{ a reflection} \,\} \subseteq V$ is a root system for $E = \pi(V)$ (recall (2.8)), let $\gamma \in V$ be a vector that is not fixed by any reflection $g \in G$, and define the closed half-space

$$H_g^+(\gamma) := \begin{cases} \{\, v \in V \;:\; (v, a_g) \geq 0 \,\} & \text{if } (\gamma, a_g) > 0 \\ \{\, v \in V \;:\; (v, a_g) \leq 0 \,\} & \text{if } (\gamma, a_g) < 0. \end{cases} \tag{2.19}$$

Then the intersection of the closed half-spaces $H_g^+(\gamma)$ for all the reflections $g \in G$ is a closed Weyl chamber.

The following lemma can be synthesized from the material in [Hum72, §10.1].

Lemma 2.21. *There is a 1-1 correspondence between closed Weyl chambers and bases of Φ: Given a closed Weyl chamber $\overline{\mathcal{C}}$, the set*

$$\{\, a \in \Phi \;:\; (\gamma, a) \geq 0 \;\forall\, \gamma \in \overline{\mathcal{C}} \,\} \bigcap \{\, a \in \Phi \;:\; (\gamma, a) = 0 \textit{ for some } 0 \neq \gamma \in \overline{\mathcal{C}} \,\}$$

forms a base for Φ; given a base Δ, the set

$$\overline{\mathcal{C}}(\Delta) = \{\, v \in V \;:\; (\delta, v) \geq 0 \;\forall\, \delta \in \Delta \,\} \tag{2.20}$$

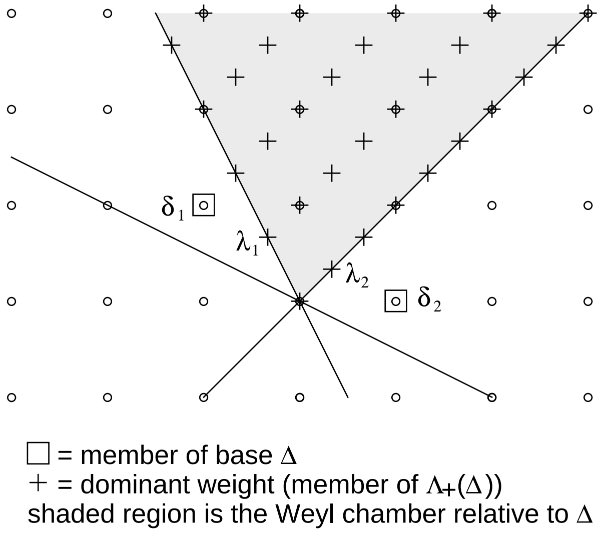
δ1
λ1
λ2
δ2
□ = member of base Δ
+ = dominant weight (member of Λ+(Δ))
shaded region is the Weyl chamber relative to Δ

Figure 2.2: Dominant weights and a Weyl chamber for a given base.

forms a closed Weyl chamber.

The set $\overline{\mathcal{C}}(\Delta)$ is called the *fundamental closed Weyl chamber relative to* Δ.

A *cone* is a nonempty subset of an $\mathbb{R}$-vector space V that is closed under linear combinations with coefficients in $\mathbb{R}_+$. If $S \subseteq V$, then

$$\mathbb{R}_+S = \left\{ \sum_{s \in S} z_s s \text{ with } z_s \in \mathbb{R}_+ \text{ almost all zero} \right\}$$

is the *cone generated by* S, and is the smallest cone in V containing S. A cone is called *finitely generated* if it can be generated as above by a finite set. A cone is *rational* if it has a generating set consisting of vectors in some $\mathbb{Q}$-vector subspace U of V with $\dim U = \dim V$. For example, we will often wish to consider the rational finitely generated cone $\mathbb{R}_+\Delta$. A *rational half-space* is a set of the form

$$H^+ = \{ v \in V \ : \ (a, v) \geq \beta \}$$

for some $0 \neq a \in U$, and $\beta \in \mathbb{Q}$. If C is a cone in V, then its *dual cone* is the set

$$C^\vee := \{ v \in V \ : \ (v, w) \geq 0 \ \forall \ w \in C \} \, .$$

It is well-known that if C is a finitely generated cone, then $(C^\vee)^\vee = C$.

Lemma 2.22. *Fix a base Δ and let $\overline{\mathcal{C}} = \overline{\mathcal{C}}(\Delta)$.*

(a) $\overline{\mathcal{C}}$ is a finitely generated rational cone in V.

(b) The dual cone of $\overline{\mathcal{C}}$ is $\mathbb{R}_+\Delta$.

Proof. (a) It is known [BH93, p. 247] that a cone is finitely generated and rational if and only if it is the intersection of finitely many rational half-spaces. In our setting, $V = \mathbb{R} \otimes_{\mathbb{Z}} A \cong \mathbb{R}^n$ is a $\mathbb{R}$-vector space and $U = \mathbb{Q} \otimes_{\mathbb{Z}} A \cong \mathbb{Q}^n$ is a $\mathbb{Q}$-vector subspace of V with $\dim U = \dim V$. The half-spaces $H_g^+(\gamma)$ where g is a reflection (2.19) are thus rational half-spaces, since $a_g \in A \subseteq U$. Part (b) follows from Lemma 2.21. □

We will often want to refer specifically to those elements of a closed Weyl chamber that belong to A, and so we define

$$D := A \cap \overline{\mathcal{C}}(\Delta) = \{\, a \in A \;:\; (a, \delta) \geq 0 \;\forall\; \delta \in \Delta \,\}$$

The following lemma is well-known.

Lemma 2.23 (Gordan's Lemma). *D is a finitely generated monoid.*

Proof. Let C denote the cone $\mathbb{R}_+\Delta$. Then C is a rational convex polyhedral cone in V and $D = C^\vee \cap A$. The assertion now follows from [Ful93, Prop. 1, p. 12] □

The next two theorems and many related results can be found in [Hum90, §1.8] and [Hum90, §1.12] respectively. We will use these results extensively.

Theorem 2.24. *Let $G \subseteq \mathrm{GL}(A) \subseteq \mathrm{GL}(V)$ be a finite reflection group. Then G acts simply transitively on the closed Weyl chambers of V.*

Theorem 2.25. *Let $G \subseteq \mathrm{GL}(A) \subseteq \mathrm{GL}(V)$ be a finite reflection group and let $\overline{\mathcal{C}} \subseteq V$ be a closed Weyl chamber. Then $\overline{\mathcal{C}}$ is a fundamental domain for the action of G on V, i.e., every G-orbit in D intersects $\overline{\mathcal{C}}$ at exactly one point. Consequently, D is a fundamental domain for the action of G on A.*

Applying Theorems 2.6 and 2.25, we see that any $f \in k[A]^G$ can be written as $f = k_0 + k_1\sigma(d_1) + k_2\sigma(d_2) + \cdots + k_t\sigma(d_t)$ for some t where each $k_i \in k$ and $1 \neq d_i \in D$.

Furthermore, $\mathrm{Supp}(\sigma(d_i)) \cap D = \{ d_i \}$, so d_i is the unique orbit sum representative in D. Thus, once D is fixed, we have a canonical way of representing orbit sums.

Since $\overline{\mathcal{C}}$ is the intersection of closed half-spaces, it is a submonoid of $(\mathbb{R}^n, +)$. The following lemma describes the role of V^G in this monoid.

Lemma 2.26.

(a) $V^G = \cap H_g$ *over all reflections* $g \in G$.

(b) V^G *is precisely the set of invertible elements in* $\overline{\mathcal{C}}$.

Proof. For (a), $v^g = v \ \forall \ g \in G \iff v^g = v \ \forall$ reflections $g \iff v \in H_g \ \forall$ reflections.

To prove (b), first suppose that $v \in V^G$. Of course $-v \in V^G$ also, and by Theorem 2.25, v and $-v$ must be contained in every closed Weyl chamber. Conversely, suppose $v, -v \in \overline{\mathcal{C}}$. Let H_g^+ denote the closed half-space containing $\overline{\mathcal{C}}$ and bounded by H_g, so by definition, $\overline{\mathcal{C}} = \cap H_g^+$ for all reflections $g \in G$. Since $v, -v \in \overline{\mathcal{C}}$, we must have $v, -v \in H_g^+$ for all reflections $g \in G$. Of course $v, -v \in H_g^+$ implies $v, -v \in H_g$. By (a) it now follows that $v, -v \in V^G$. □

Corollary 2.27. $\pi(\overline{\mathcal{C}}) \subseteq \overline{\mathcal{C}}$.

Proof. Let $v \in \overline{\mathcal{C}}$. Then $\pi(v) = v + w$ for some $w \in V^G$. Since $v, w \in \overline{\mathcal{C}}$, so is $\pi(v)$. □

From the above lemma it is clear that the monoids $\pi(\overline{\mathcal{C}})$ and $\pi(D)$ have no non-trivial invertible elements. Note $A^G = V^G \cap A \subseteq D$.

Lemma 2.28. *Fix a base* Δ. *Put* $\Lambda_+ = \Lambda_+(\Delta)$ *and* $\overline{\mathcal{C}} = \overline{\mathcal{C}}(\Delta)$.

(a) $\Lambda_+ = \overline{\mathcal{C}} \cap \Lambda$

(b) $\pi(D) \subseteq \Lambda_+ \subseteq \frac{1}{m}\pi(D)$ *for some* $0 \neq m \in \mathbb{N}$.

Proof. Statement (a) is an immediate consequence of equations (2.15) and (2.20). To show (b), first notice that by Corollary 2.27 we know $\pi(D) \subseteq \overline{\mathcal{C}}$. Also, by Lemma 2.19 we know $\pi(D) \subseteq \Lambda$. Thus, by part (a) above, $\pi(D) \subseteq \Lambda_+$.

For $\Lambda_+ \subseteq \frac{1}{m}\pi(D)$ it suffices to show that $m\lambda_i \in \pi(D)$ $(1 \leq i \leq r)$, since $\Lambda_+ = \bigoplus_{i=1}^r \mathbb{N}\lambda_i$ (2.14). Of course $\lambda_i \in \mathbb{Q} \otimes A$ by (2.18), so $m\lambda_i \in A$ for some $0 < m \in \mathbb{N}$. Now $m\lambda_i \in \overline{\mathcal{C}}$ by part (a), and $m\lambda_i \in E$, thus $m\lambda_i = \pi(m\lambda_i) \in \pi(D)$. □

Definition 2.29. A set $F \subseteq \overline{\mathcal{C}}$ is called a *face* of $\overline{\mathcal{C}}$, if there exists some $v = v_F \in \mathbb{R}_+\Delta$ such that $(v, w) = 0$ for all $w \in F$, and $(v, w) > 0$ for all $w \in \overline{\mathcal{C}} \setminus F$.

Remark. V^G is contained in every face of $\overline{\mathcal{C}}$.

Lemma 2.30.

(a) $\pi(\overline{\mathcal{C}}) \subseteq E$ is a finitely generated rational cone.

(b) If F is a face of $\overline{\mathcal{C}}$ then $\pi(F)$ is a face of $\pi(\overline{\mathcal{C}})$. Furthermore, in the notation from Definition 2.29, we may choose $v_{\pi(F)} = v_F$.

(c) If F is a face of $\overline{\mathcal{C}}$ then $\pi(\overline{\mathcal{C}} \setminus F) = \pi(\overline{\mathcal{C}}) \setminus \pi(F)$.

Proof. (a) We simply remark without elaboration that $\pi(\overline{\mathcal{C}})$ is finitely generated as a rational cone by the fundamental dominant weights $\lambda_1, \dots, \lambda_r$.

(b) Let F be a face of $\overline{\mathcal{C}}$ and choose $v = v_F \in \mathbb{R}_+\Delta$ as in Definition 2.29. Let $w \in \pi(F)$, so $w + \gamma \in F$ for some $\gamma \in V^G$. Then $(v, w) = (v, w) + (v, \gamma) = (v, w + \gamma) = 0$.

If $w \in \pi(\overline{\mathcal{C}}) \setminus \pi(F)$ then $w \in \pi(\overline{\mathcal{C}})$, so by Corollary 2.27, $w \in \overline{\mathcal{C}}$, and by Lemma 2.26, $w + \gamma \in \overline{\mathcal{C}}$ for all $\gamma \in V^G$. Furthermore, $w \notin \pi(F)$, so $w + \gamma \notin F$ for all $\gamma \in V^G$. Thus $w + \gamma \in \overline{\mathcal{C}} \setminus F$ for all $\gamma \in V^G$. It now follows that $(v, w) = (v, w) + (v, \gamma) = (v, w + \gamma) > 0$. Furthermore, it is clear that we can choose $v_{\pi(F)} = v = v_F$.

(c) First suppose that $w \in \pi(\overline{\mathcal{C}} \setminus F)$, and so $w \in \pi(\overline{\mathcal{C}})$. Now $w + \gamma \in \overline{\mathcal{C}} \setminus F$ for some $\gamma \in V^G$ and so $(v, w) = (v, w) + (v, \gamma) = (v, w + \gamma) > 0$. Since $\pi(F)$ is a face of $\pi(\overline{\mathcal{C}})$, this implies $w \notin \pi(F)$. Hence $w \in \pi(\overline{\mathcal{C}}) \setminus \pi(F)$.

If $w \in \pi(\overline{\mathcal{C}}) \setminus \pi(F)$, then of course $w \in \overline{\mathcal{C}}$ by Corollary 2.27. Since $\pi(F)$ is a face of $\pi(\overline{\mathcal{C}})$, we must have $(v, w) > 0$ and thus $w \notin F$. Now $w \in \overline{\mathcal{C}} \setminus F$, and so $w = \pi(w) \in \pi(\overline{\mathcal{C}} \setminus F)$. □

2.5 The Hilbert of a Monoid

We prove here a lemma about commutative monoids that will be useful to us in §3.4. There we will apply these results to the monoid $\pi(D)$. This lemma is well-known, but we provide a proof for lack of a suitable reference.

Let $(M, +)$ be a commutative monoid. An element $0 \neq m \in M$ is called *indecomposable* if $m = a + b$ $(a, b \in M) \implies a = 0$ or $b = 0$.

Lemma 2.31. *Let $(M, +)$ be a commutative monoid that is*

> *finitely generated,*
> *cancellative ($a + c = a + b \Longrightarrow a = b$ for $a, b, c \in M$),*
> *torsion-free ($na = nb \Longrightarrow a = b$ for $a, b \in M$ and $0 \neq n \in \mathbb{N}$), and*
> *positive ($a + b = 0$, $a, b \in M \Longrightarrow a = b = 0$).*

Then

(a) There is a monoid homomorphism $\varphi : M \to \mathbb{N}$ satisfying $\varphi(m) > 0$ for all $0 \neq m \in M$.

(b) M has finitely many indecomposable elements, say $m_1, \ldots, m_s$. These elements generate M, and every generating set for M contains $\{ m_1, \ldots, m_s \}$.

Proof. (a) See, e.g., [Swa92, Thm. 4.5].

(b) Clearly, all indecomposable elements must be contained in every generating set of M. Thus, it suffices to show that the indecomposable elements of M do indeed generate M.

Now consider an element $0 \neq m \in M$. If m is not indecomposable, then write $m = a + b$ with $0 \neq a, b \in M$. Using part (a), $\varphi(a), \varphi(b) < \varphi(m)$. By induction we know that a and b can be written as a sum of indecomposable elements of M, and hence so can m. □

The set $\{ m_1, \ldots, m_s \}$ is the unique smallest generating set of M, and it is called the *Hilbert basis* of M. An algorithm for computing the Hilbert basis for any finitely generated, cancellative, torsion-free, positive monoid can be found in [Stu96, Alg. 13.2].

CHAPTER 3

MULTIPLICATIVE INVARIANTS UNDER FINITE REFLECTION GROUPS

3.1 Overview

In this chapter we will describe methods for computing algebra generators for the ring of multiplicative invariants, $k[A]^G$, where G is a reflection group. We obtain a result of Farkas [Far86] using an algorithmic approach. In the next chapter we will extend our methods to obtain generators when G is a subgroup of a reflection group.

3.2 Preliminaries

We will establish a partial order on $k[A]$ that satisfies the descending chain condition (DCC), and describe orbital polynomials, two tools that will be of major use in the remaining sections of this chapter. First, however, we recall and fix some notation (see Section 2.4 for definitions):

$G \subseteq \mathrm{GL}(A)$ is a finite reflection group;
V is the $\mathbb{R}$-vector space $A \otimes_{\mathbb{Z}} \mathbb{R}$ of dimension n;
$(\, , \,)$ is a G-invariant inner product on V;

π is the orthogonal projection $V \to (V^G)^\perp = E$, and $r := \dim E$;

$\Phi \subseteq A$ is the crystallographic root system constructed from G, for $E = \pi(V)$, see (2.8);

Δ is a fixed base of Φ;

Λ is the weight lattice, Λ_+ is the set of dominant weights w.r.t. Δ, and $\{\, \lambda_1, \dots, \lambda_r \,\}$ are the fundamental dominant weights;

$\overline{\mathcal{C}} := \overline{\mathcal{C}}(\Delta) = \{\, v \in V \;:\; (v, \delta) \geq 0 \;\forall\; \delta \in \Delta \,\}$ is the closed Weyl chamber relative to Δ;

$D := A \cap \overline{\mathcal{C}} = \{\, a \in A \;:\; (a, \delta) \geq 0 \;\forall\; \delta \in \Delta \,\}$. D is a fundamental domain for the action of G on A. Recall $A^G \subseteq D$.

3.2.1 A Partial Order

The base Δ gives rise to a partial order on V. By Theorem 2.25 we know that for any $v \in V$, the set $v^G \cap \overline{\mathcal{C}}$ consists of a single element. Denote this element by $\bar{v}$.

$$\{\, \bar{v} \,\} := v^G \cap \overline{\mathcal{C}} \tag{3.1}$$

Definition 3.1 (A partial order on V). We write $v \sim w$ if $\pi(\bar{w} - \bar{v}) = 0$, and we write $v < w$ if $0 \neq \pi(\bar{w} - \bar{v}) \in \mathbb{R}_+\Delta$. We write $v \leq w$ to mean $v < w$ or $v = w$, and we write $v \lesssim w$ to mean $v < w$ or $v \sim w$. In particular, $v \lesssim w$ if and only if $\pi(\bar{w} - \bar{v}) \in \mathbb{R}_+\Delta$.

Obviously, if $v < w$ then $v^g < w^h$ for any $g, h \in G$. Now $\leq$ is a partial order on V: reflexivity is clear, and transitivity follows from the fact that $\mathbb{R}_+\Delta$ is a positive monoid (the sum of any two nonzero elements in $\mathbb{R}_+\Delta$ must be nonzero since Δ is a linearly independent set). This last fact also implies the antisymmetry of $\leq$, i.e., $v < w$ and $w < v$ is impossible.

The definition of this partial order is similar to, but slightly broader than that given in [Hum72, p. 47], due to the possibility that $V^G \neq 0$ in our setting. Of course, the partial order $\leq$ when restricted to A is a partial order on A.

Lemma 3.2. *The set A has the descending chain condition (DCC) with respect to $\leq$. That is, there exists no infinite sequence $a_1 > a_2 > a_3 > \cdots$ with all $a_i \in A$.*

Proof. We prove the above lemma in two steps: (1) For all $a, b \in A$ we have $a < b \iff \pi(\bar{a}) < \pi(\bar{b})$, and (2) The set $(\Lambda_+, \leq)$ has DCC. By Lemma 2.28, $\pi(\bar{a}), \pi(\bar{b}) \in \Lambda_+$, so these two conditions imply DCC on A.

(1) Observe

$$\pi\left(\overline{\pi(\bar{b})} - \overline{\pi(\bar{a})}\right) = \pi\left(\pi(\bar{b}) - \pi(\bar{a})\right) = \pi(\bar{b}) - \pi(\bar{a}) = \pi(\bar{b} - \bar{a})$$

The first equality holds since $\pi(\overline{\mathcal{C}}) \subseteq \overline{\mathcal{C}}$ (Corollary 2.27) and hence $\overline{\pi(\bar{v})} = \pi(\bar{v})$. The second equality comes from the fact that π is idempotent. Now clearly $\pi(\bar{b} - \bar{a}) \in \mathbb{R}_+\Delta \iff \pi\left(\overline{\pi(\bar{b})} - \overline{\pi(\bar{a})}\right) \in \mathbb{R}_+\Delta$, that is, $a < b \iff \pi(\bar{a}) < \pi(\bar{b})$.

(2) Let $\mu \in \Lambda_+$ be given. We will show that there exist only finitely many $\lambda \in \Lambda_+$ such that $\lambda \leq \mu$. Since Λ_+ is a monoid (see, e.g. (2.15)), $\mu + \lambda \in \Lambda_+$.

By Lemma 2.28 and Definition (2.9), $\Lambda_+ = \Lambda \cap \overline{\mathcal{C}} \subseteq E$, so clearly $\mu = \bar{\mu}$, $\lambda = \bar{\lambda}$, $\pi(\mu) = \mu$, and $\pi(\lambda) = \lambda$. By definition $\lambda \leq \mu \implies \pi(\mu - \lambda) \in \mathbb{R}_+\Delta$, and so we must have $\mu - \lambda \in \mathbb{R}_+\Delta$. In particular, $\mu - \lambda$ can be written as an $\mathbb{R}_+$-linear combination of simple roots $\delta \in \Delta$.

By equation (2.15), we see that $0 \leq (\mu + \lambda, \mu - \lambda) = (\mu, \mu) - (\lambda, \lambda)$. Thus λ is in the compact set $\{\, v \in E \;:\; (v, v) \leq (\mu, \mu) \,\}$. Of course λ is also in the discrete set Λ_+. The intersection of a compact set with a discrete one is necessarily finite, thus only finitely many $\lambda \in \Lambda_+$ can satisfy $\lambda \leq \mu$. This proves DCC on Λ_+. □

Let $\mathcal{F}(V)$ denote the set of all finite subsets of V. For $X, Y \in \mathcal{F}(V)$, define $X > Y$ if for each $y \in Y$ there exists some $x \in X$ such that $x > y$. Note that $\varnothing < X$ for all $\varnothing \neq X \in \mathcal{F}(V)$ The following lemma can be found in [Die00].

Lemma 3.3 (König's Infinity Lemma). *$\mathcal{F}(A)$ with the above ordering satisfies the descending chain condition.*

Proof. Suppose for a contradiction that $X_0 > X_1 > X_2 > \cdots$ is an infinite chain of elements in $\mathcal{F}(A)$. Let $\mathcal{P}$ be the set of all chains of the form $y_0 > y_1 > y_2 > \cdots > y_n$ where $y_i \in X_i$. Clearly $\mathcal{P}$ is an infinite set. Since X_0 is finite, there must exist some $x_0 \in X_0$ such that infinitely many chains start at x_0. Let $\mathcal{P}_0$ denote the set of chains containing x_0, and observe that since X_1 is finite there must exist some $x_1 \in X_1$

such that infinitely many chains in $\mathcal{P}_0$ contain x_1. Let $\mathcal{P}_1 \subseteq \mathcal{P}_0$ denote the set of chains containing x_1 and determine x_2 in the same fashion. The set $\mathcal{P}_n$ is infinite for any n, and so x_{n+1} gets defined for all $n \in \mathbb{N}$, thus creating an infinite chain $x_0 > x_1 > x_2 > \cdots$ of elements in A, and providing the contradiction we seek. □

The above definitions and lemma allow us to construct a partial order with DCC on all of $k[A]$. Let $p \in k[A]$ be written as the finite sum $p = \sum k_a a^*$ where $k_a \in k$ and $a \in A$. Recall Definition 2.4, that the support of p is $\mathrm{Supp}(p) = \{\, a \in A \;:\; k_a \neq 0 \,\}$. We define the set of *highest monomials* of p as

$$\mathrm{HM}(p) = \{\, a \in \mathrm{Supp}(p) \;:\; a \not< b \text{ for all } b \in \mathrm{Supp}(p) \,\}$$

For example, if $f = k_1\sigma(a_1) + k_2\sigma(a_2)$ for elements $a_1, a_2 \in A$ with $a_1 > a_2$, then $\mathrm{HM}(f) = \mathrm{Supp}(\sigma(a_1)) = a_1^G$, the orbit of a_1 under the action of G.

Definition 3.4. For Laurent polynomials $p, q \in k[A]$ define $p < q$ if and only if for each $x \in \mathrm{HM}(p)$ there exists some $y \in \mathrm{HM}(q)$ such that $x < y$. We write $p \leq q$ to mean $p < q$ or $p = q$.

Lemma 3.5. *This ordering of Definition 3.4 on $k[A]$ satisfies the descending chain condition.*

Proof. This follows immediately from Lemma 3.3. Note that $\mathrm{HM}(p) = \mathrm{Supp}(p) = \varnothing$ for $p = 0$. □

We finish this section with a technical lemma, a similar version of which can be found in [Hum90, Lemma 1.12].

Lemma 3.6. *If $v \gtrsim w$, then $\pi(\bar{v} - w) \in \mathbb{R}_+\Delta$.*

Proof. By hypothesis $\pi(\bar{v} - \bar{w}) \in \mathbb{R}_+\Delta$. Assume for the moment the following claim: $\bar{v} - v \in \mathbb{R}_+\Delta$ for all $v \in V$. If the claim is true, then $\pi(\bar{w} - w) \in \mathbb{R}_+\Delta$. Since $\mathbb{R}_+\Delta$ is a monoid, we get $\pi(\bar{v} - \bar{w}) + \pi(\bar{w} - w) = \pi(\bar{v} - w) \in \mathbb{R}_+\Delta$. Thus it only remains to prove the claim.

Observe first that indeed $\bar{v} - v \in E$ since for any $g \in G$ and $\gamma \in V^G$ we get $(v^g - v, \gamma) = (v^g, \gamma) - (v, \gamma) = (v, \gamma) - (v, \gamma) = 0$. Hence $\bar{v} - v$ must be some $\mathbb{R}$-linear combination of Δ.

Define a new partial order (used only in this proof) on V: write $v \preceq w$ if and only if $w - v \in \mathbb{R}_+\Delta$. It is easy to verify that this satisfies the partial order axioms. Consider the set $L = \{ v^g \ : \ g \in G, \ v^g \succeq v \}$. Certainly $v \in L$ and L is finite, so there exists a maximal (w.r.t. $\prec$) element $w \in L$. If $\delta_1, \ldots, \delta_r$ are the simple roots we can write $w = \gamma + z_1\delta_1 + z_2\delta_2 + \cdots + z_r\delta_r$ for some $\gamma \in V^G$ and $z_i \in \mathbb{R}$. Letting g_i be the simple reflection corresponding to δ_i and recalling equation (2.4), we see $w^{g_i} - w = -(2(w, \delta_i)/(\delta_i, \delta_i))\delta_i$. Of course $w^{g_i} = v^g$ for some g, so by the maximality of w in L we know that $w^{g_i} - w \notin \mathbb{R}_+\Delta \setminus \{ 0 \}$ (otherwise $w^{g_i} \succ w$ and $w^{g_i} \succ v$, contradicting the maximality of w in L), and hence $(w, \delta_i) \geq 0$. This must be true for all δ_i, thus proving that $w \in \overline{\mathcal{C}}$ and hence $w = \bar{v}$. Since $\bar{v} \succeq v$ it finally follows that $\bar{v} - v \in \mathbb{R}_+\Delta$. □

The fact from the above proof that $\bar{v} - v \in \mathbb{R}_+\Delta$ for all $v \in V$ can be used for the following result.

Lemma 3.7. *Let $v, w \in V$ and suppose that $v, w \in \overline{\mathcal{C}}^g$, and $(v + w)^\ell \in \overline{\mathcal{C}}^h$ for some $g, h, \ell \in G$. Then $v^\ell, w^\ell \in \overline{\mathcal{C}}^h$.*

Proof. Certainly $(v + w)^{\ell h^{-1}} \in \overline{\mathcal{C}}$, and also $v^{g^{-1}}, w^{g^{-1}} \in \overline{\mathcal{C}}$, so $(v + w)^{g^{-1}} \in \overline{\mathcal{C}}$. We know from Theorem 2.25 that the G-orbit of $(v + w)$ intersects $\overline{\mathcal{C}}$ in exactly one point, so we have

$$v^{\ell h^{-1}} + w^{\ell h^{-1}} = (v + w)^{\ell h^{-1}} = (v + w)^{g^{-1}} = v^{g^{-1}} + w^{g^{-1}}.$$

Thus,

$$w^{\ell h^{-1}} - w^{g^{-1}} = v^{g^{-1}} - v^{\ell h^{-1}}. \tag{3.2}$$

Of course $v^{g^{-1}} = \bar{v}$ and $w^{g^{-1}} = \bar{w}$, so (using the remark preceding this lemma) the right-hand side of (3.2) belongs to $\mathbb{R}_+\Delta$, while the left-hand side of (3.2) belongs to $-\mathbb{R}_+\Delta$. Thus they both must equal 0. That is, $v^\ell = v^{g^{-1}h} \in \overline{\mathcal{C}}^h$ and $w^\ell = w^{g^{-1}h} \in \overline{\mathcal{C}}^h$. □

3.2.2 Orbital Laurent Polynomials

Definition 3.8. For a finite reflection group $G \subseteq \mathrm{GL}(A)$, we say that $p \in k[A]^G$ is *G-orbital through a* if $p = p' + \sigma_G(a)$ and $x < a$ for all $x \in \mathrm{Supp}(p')$. (We will omit the G when the context is clear). For a subgroup $H \subseteq G$, we say that $p \subseteq k[A]^H$ is H-orbital through a if $p = p' + \sigma_H(a)$ and $x < a$ for all $x \in \mathrm{Supp}(p')$, where the order, $<$, is determined by G as in Definition 3.1.

Of course orbit sums are orbital. Additionally, if p is orbital through a, then $\mathrm{HM}(p) = a^G$, the orbit of a under G. Furthermore, if $f \in k[A]^G$ and $\mathrm{HM}(f) = a^G$ for some $a \in A$, then f is orbital *only if* the coefficient on a in f is 1_k.

The following technical lemma is not very interesting on its own, but it will be of use to us in several proofs to come.

Lemma 3.9. *Let H_1, H_2 be subgroups of a reflection group $G \subseteq \mathrm{GL}(A)$. Suppose $p \in k[A]^{H_1}$ is H_1-orbital through a, and $q \in k[A]^{H_2}$ is H_2-orbital through b. Let $x \in \mathrm{Supp}(p)$ and $y \in \mathrm{Supp}(q)$. If $\pi(\bar{a} + \bar{b}) = \pi(x^{g_1} + y^{g_2})$ for some $g_1, g_2 \in G$, then $x^{g_1} = \bar{a}$ and $y^{g_2} = \bar{b}$.*

Before we present the proof note that $\bar{a}$ need not be in the H_1-orbit of a, and x^{g_1} need not be in $\mathrm{Supp}(p)$.

Proof. Since $\pi(\bar{a} + \bar{b}) = \pi(x^{g_1} + y^{g_2})$, we can write

$$\pi(\bar{a} - x^{g_1}) = \pi(y^{g_2} - \bar{b}).$$

Using Lemma 3.6 we know that the left-hand side above belongs to $\mathbb{R}_+\Delta$, while the right-hand side belongs to $-\mathbb{R}_+\Delta$. Hence,

$$\pi(\bar{a} - x^{g_1}) = \pi(y^{g_2} - \bar{b}) = 0.$$

Since $\pi(\bar{a} - x^{g_1}) = 0$ we can write $x^{g_1} = \bar{a} + w$ for some $w \in V^G = \mathrm{Ker}(\pi)$. Since $\bar{a} \in \overline{\mathcal{C}}$ and $w \in \overline{\mathcal{C}}$ (Lemma 2.26(b)), x^{g_1} must also be in $\overline{\mathcal{C}}$. Thus $x^{g_1} = \overline{x^{g_1}} = \bar{x}$ and we can write $\pi(\bar{a} - \bar{x}) = 0$. By Definition 3.1, this says that $a \sim x$. Since p is H_1-orbital through a, we must have $x \in \mathrm{Supp}(\sigma_{H_1}(a)) = a^{H_1}$. That is, $x = a^h$ for some $h \in H_1$. Now $x^{g_1} = \bar{x} = \overline{a^h} = \bar{a}$. Similarly, we must have $y^{g_2} = \bar{b}$. □

Lemma 3.10. *If $p \in k[A]^G$ is orbital through a and $q \in k[A]^G$ is orbital through b, then pq is orbital through $\bar{a} + \bar{b}$. In particular,* $\mathrm{HM}(pq) = (\bar{a} + \bar{b})^G$.

Proof. Write $p = p' + \sigma_G(a)$ and $q = q' + \sigma_G(b)$, with $a > x$ for all $x \in \mathrm{Supp}(p')$ and $b > y$ for all $y \in \mathrm{Supp}(q')$. Note that

$$\mathrm{Supp}(pq) \subseteq \mathrm{Supp}(p) + \mathrm{Supp}(q). \tag{3.3}$$

We first show that $\bar{a} + \bar{b}$ actually is in the support of pq, with coefficient 1_k. This is immediate from the following claim.

Claim: $x + y = \bar{a} + \bar{b}$ ($x \in \mathrm{Supp}(p)$, $y \in \mathrm{Supp}(q)$) $\Longrightarrow x = \bar{a}$ and $y = \bar{b}$.

Proof of claim: If $x + y = \bar{a} + \bar{b}$, then certainly $\pi(x + y) = \pi(\bar{a} + \bar{b})$. By Lemma 3.9 we conclude $x = \bar{a}$ and $y = \bar{b}$, and the claim is proved.

Since $\bar{a} + \bar{b} \in \mathrm{Supp}(pq)$, and pq is G-invariant, we must be able to write $pq = r' + \sigma(\bar{a} + \bar{b})$ for some $r' \in k[A]^G$. We must now show that for all $z \in \mathrm{Supp}(r')$, $z < \bar{a} + \bar{b}$. Actually, we will show that if $x + y \notin (\bar{a} + \bar{b})^G$, ($x \in \mathrm{Supp}(p)$, $y \in \mathrm{Supp}(q)$) then $x + y < \bar{a} + \bar{b}$, and by (3.3) this implies our desired result. The proof consists of our demonstrating two facts: (1) $x + y \lesssim \bar{a} + \bar{b}$, and (2) if $x + y \sim \bar{a} + \bar{b}$, then $x + y \in (\bar{a} + \bar{b})^G$. The proofs of these facts follow below.

(1) We know that $x \lesssim \bar{a}$ and so $x^g \lesssim \bar{a}$ for all $g \in G$. Thus by Lemma 3.6, for all $g \in G$,

$$\pi(\bar{a} - x^g) \in \mathbb{R}_+\Delta. \tag{3.4}$$

Similarly,

$$\pi(\bar{b} - y^h) \in \mathbb{R}_+\Delta \tag{3.5}$$

for all $h \in G$. Now there must exist some $\ell \in G$ such that $\overline{x + y} = (x + y)^\ell = x^\ell + y^\ell$. Setting $g = h = \ell$ and adding equations (3.4) and (3.5) together yield

$$\pi(\bar{a} + \bar{b} - (x^\ell + y^\ell)) = \pi(\bar{a} + \bar{b} - \overline{x + y}) \in \mathbb{R}_+\Delta.$$

By definition, (noting that $\bar{a} + \bar{b} \in \overline{\mathcal{C}}$) this implies $x + y \lesssim \bar{a} + \bar{b}$.

(2) If we assume that $x + y \sim \bar{a} + \bar{b}$ then by Definition 3.1 we get

$$\pi(\overline{\bar{a} + \bar{b}} - \overline{x + y}) = 0. \tag{3.6}$$

We note that $\overline{\bar{a}+\bar{b}} = \bar{a}+\bar{b}$, and $\overline{x+y} = (x+y)^g = x^g + y^g$ for some $g \in G$. Thus equation (3.6) is equivalent to

$$\pi(\bar{a}+\bar{b}) = \pi(x^g + y^g). \tag{3.7}$$

Applying Lemma 3.9 we conclude $x^g = \bar{a}$ and $y^g = \bar{b}$. Thus $(x+y)^g = x^g + y^g = \bar{a}+\bar{b}$ and we have $x+y \in (\bar{a}+\bar{b})^G$, as desired.

Finally, we remark that by points (1) and (2) above, if $x+y \notin (\bar{a}+\bar{b})^G$, then $x+y < \bar{a}+\bar{b}$, and we conclude that pq is orbital through $\bar{a}+\bar{b}$. □

Remark. We record two straightforward observations:

1. If $q \in k[A]^G$ is orbital through a, then $q - \sigma(a) \in k[A]^G$, and $q - \sigma(a) < \sigma(a)$.

2. If $f, p \in k[A]^G$ such that $f = \sum k_i \sigma(a_i)$ and $p < \sigma(a_i)$ for some a_i, then $p < f$.

3.3 Generators for Invariants Under a Reflection Group

The following result can be found in [Far86], though we supply a new algorithmic proof. Recall that D is a finitely generated monoid (Lemma 2.23).

Theorem 3.11. *Let $\{ a_1, \ldots, a_s \} \subseteq D$ be a generating set for the monoid D, and let $p_1, \ldots, p_s$ be orbital elements in $k[A]^G$ such that p_i is orbital through a_i. Then $k[A]^G = k[p_1, \ldots, p_s]$.*

In particular, if we know that $\{ a_1, \ldots, a_s \}$ is a generating set for D, then we can always choose $p_i = \sigma(a_i)$. Section 3.4 addresses the issue of computing an explicit minimal generating set for D.

The above theorem is proved via Algorithm 3, which rewrites any element of $k[A]^G$ as a polynomial in $p_1, \ldots, p_s$.

Concerning Algorithm 3, the fact that we can express f as in line 5 is given following Theorem 2.25. Line 7 uses the fact that $a_1, \ldots, a_s$ generate D as a monoid. Since the p_i are orbital through a_i, Lemma 3.10 implies q (line 8) is orbital through d_i.

Algorithm 3 Rewrite $f \in k[A]^G$ as polynomial in algebra generators

```
1:  Input: $f \in k[A]^G$
2:  if $f \in k$ then
3:      Output: $f$.
4:  end if
5:  $f = k_0 + k_1\sigma(d_1) + k_2\sigma(d_2) + \cdots + k_t\sigma(d_t)$ where $k_i \in k$ and $0 \neq d_i \in D$.
6:  for $i$ from 1 to $t$ do
7:      Write $d_i = n_1a_1 + n_2a_2 + \cdots + n_sa_s \quad (n_i \in \mathbb{N})$.
8:      Let $q := p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}$.
9:      Let $r_i := q - $ Rewrite$(q - \sigma(d_i))$.
10: end for
11: Output: $k_0 + k_1r_1 + k_2r_2 + \cdots + k_tr_t$.
```

In line 9, observe first that $r_i = \sigma(d_i)$ since rewriting an expression does not change its value. Thus the value returned in line 11 is the same as the input, as expressed in line 5.

The crux of Algorithm 3 now occurs as the algorithm calls itself recursively. By the remark following Lemma 3.10, we know that (1) the new argument $q - \sigma(d_i)$ is strictly less than $\sigma(d_i)$, and hence (2) it is strictly less than f. Since the ordering of $k[A]$ satisfies DCC (Lemma 3.5), we are assured that the algorithm terminates. This proves Theorem 3.11.

3.4 Constructing a Minimal Generating Set for the Monoid D.

By Theorem 3.11, we know that once we have monoid generators for D, we can create algebra generators for $k[A]^G$. We turn now to the task of constructing a minimal set of generators for D. Actual computer code for accomplishing this task, written for the computer algebra system *Magma*, can be found in Appendix A.

In this section, Lemma 3.14 demonstrates how to lift any generating set for the monoid $\pi(D)$ to a generating set for the monoid D, Lemma 3.15 indicates that $\pi(D)$ has a Hilbert basis (i.e., a minimal generating set), Lemma 3.16 shows that this Hilbert basis lifted to D is a minimal generating set for D, and then finally, Algorithm 4 provides a method for computing the Hilbert basis for $\pi(D)$.

Let B be a basis for A^G, recall that $\rho := id - \pi : V \twoheadrightarrow V^G$, and consider the following region contained in $\rho(V)$,

$$K_B := \sum_{b \in B} [0, b) = \left\{ \sum_{b \in B} t_b b \ : \ 0 \leq t_b < 1 \right\}. \tag{3.8}$$

Lemma 3.12. *For each $y \in \pi(D)$ there exists a unique $d \in D$ such that $\pi(d) = y$ and $\rho(d) \in K_B$.*

Proof. First note that by the construction of K_B, for any $v \in V^G$ there exists a unique $c \in A^G$ such that $v - c \in K_B$. To see this, fix $v \in V^G = A^G \otimes_{\mathbb{Z}} \mathbb{R}$, and write $v = \sum_{b \in B} z_b b$ where each $z_b \in \mathbb{R}$. For any $c \in A^G$ we can write $c = \sum_{b \in B} n_b b$ where each $n_b \in \mathbb{Z}$. Now if $v - c \in K_B$, then it must be true that $0 \leq z_b - n_b < 1$ for each $b \in B$. This uniquely determines each $n_b = \lfloor z_b \rfloor$ and hence c is uniquely determined.

To show existence in the lemma, let $y \in \pi(D)$ be given and choose any $d' \in D$ such that $\pi(d') = y$. By the previous paragraph, there must exist (a unique) $c \in A^G$ such that $\rho(d') - c \in K_B$. Let $d := d' - c$. Then $\pi(d) = \pi(d') = y$, and $\rho(d) = \rho(d') - c \in K_B$.

For uniqueness, suppose $d_1, d_2 \in D$ such that $\pi(d_1) = \pi(d_2)$ and $\rho(d_1), \rho(d_2) \in K_B$. If $c \in A^G$ is the unique element such that $\rho(d_1) - c \in K_B$, then clearly $c = 0$ since $\rho(d_1) \in K_B$. However, $d_1 - d_2 \in A^G$ and $\rho(d_1) - (d_1 - d_2) = \rho(d_1 - (d_1 - d_2)) = \rho(d_2) \in K_B$. Thus $d_1 = d_2$. □

Corollary 3.13. *Let $X \subseteq \pi(D)$ and let $X' := A \cap (X + K_B) \subseteq D$. Then π yields a bijection $X' \to X$.*

Remark. To actually compute the set X' in the above corollary, we first compute the finite set $K_B \cap \rho(A)$ by applying ρ to a basis of A and using some basic linear algebra. Then $A \cap (X + K_B) = A \cap (X + (K_B \cap \rho(A)))$ and, if X finite, the latter expression can be determined with finitely many calculations.

Lemma 3.14. *Suppose $W \subseteq \pi(D)$ is given such that W generates $\pi(D)$, and let $W' := A \cap (W + K_B)$. Then $W' \cup \{\, \pm b \;:\; b \in B \,\}$ generates the monoid D.*

Proof. Let $d \in D$. By hypothesis, $\pi(d) = \sum_{w \in W} n_w w$ where $n_w \in \mathbb{N}$. By Corollary 3.13, we know that for each $w \in W$ there exists a unique w' in W' such that $\pi(w') = w$. Thus $\pi(d) = \sum_{w \in W} n_w \pi(w')$. Since π is a homomorphism of A with $\operatorname{Ker}_A(\pi) = A^G$, we get $d = \sum_{w \in W} n_w w' + c$ for some $c \in A^G$. Clearly A^G is generated by B, and the lemma is proved. □

Lemma 3.15. *$\pi(D)$ has a Hilbert basis.*

Proof. Lemma 2.23 tells us that the monoid D is finitely generated, and so the monoid $\pi(D)$ must be finitely generated as well. The fact that $\pi(D)$ is cancellative and torsion-free follows immediately from the fact that $\pi(D)$ sits in a real vector space, namely $E = \pi(V)$. Finally, Lemma 2.26(b) assures us that $\pi(D)$ is positive. Thus all the hypotheses of Lemma 2.31 are satisfied and $\pi(D)$ must have a Hilbert basis. □

Lemma 3.16. *Let W be a Hilbert basis for $\pi(D)$, let B be a basis for A^G, and let $W' := A \cap (W + K_B)$. Then $W' \cup \{\, \pm b \;:\; b \in B \,\}$ is a minimal generating set, with respect to containment, for D.*

Proof. By Lemma 2.31(b), W is the unique smallest generating set for $\pi(D)$, and by Lemma 3.14, $W' \cup \{\, \pm b \;:\; b \in B \,\}$ generates D. For contradiction, assume $X \subsetneq W' \cup \{\, \pm b \;:\; b \in B \,\}$ generates D. Then $\pi(X)$ generates $\pi(D)$, and so $\pi(X) \supseteq W$, by Lemma 2.31(b). Corollary 3.13 now implies that $X \supseteq W'$, and thus $X \cap A^G \subsetneq \{\, \pm b \;:\; b \in B \,\}$. By Lemma 2.26(b), the group of invertible elements of D is A^G, and so $X \cap A^G$ must generate A^G as a monoid. However, $X \cap A^G \subsetneq \{\, \pm b \;:\; b \in B \,\}$, and clearly no proper subset of $\{\, \pm b \;:\; b \in B \,\}$ generates A^G as a monoid, giving us our desired contradiction. □

Finally, it only remains to compute the Hilbert basis of $\pi(D)$. Following [Lor01], we employ properties of the weight lattice to accomplish this task. Algorithm 4 summarizes the calculations required, assuming $A = \mathbb{Z}^n$.

As noted in Lemma 2.28(b), $\pi(D) \subseteq \Lambda_+ = \oplus_{i=1}^{r} \mathbb{N}\lambda_i \subseteq \frac{1}{m}\pi(D)$ where $\lambda_1, \ldots, \lambda_r$ are the fundamental dominant weights and $0 \neq m \in \mathbb{N}$. Hence there exist $0 \neq n_i \in \mathbb{N}$

such that $n_i\lambda_i \in \pi(D)$. Choose such n_i minimal, and let $m_i := n_i\lambda_i$. Consider the zonotope contained in V,

$$K_M := \sum_{i=1}^{r}[0, m_i] = \left\{ \sum_{i=1}^{r} t_i m_i \ : \ 0 \leq t_i \leq 1 \right\}. \tag{3.9}$$

The set

$$Z := \pi(A) \cap K_M \setminus \{ 0 \} \tag{3.10}$$

is finite and generates $\pi(D)$.

The Hilbert basis of $\pi(D)$ then is just the set of indecomposable lattice points in Z, that is, those $z \in Z$ that cannot be written $z = x_1 + x_2$ with $0 \neq x_1, x_2 \in Z$. The Hilbert basis can thus be computed as $Z \setminus (Z + Z)$.

Algorithm 4 Compute a Hilbert basis for $\pi(D)$

```
Input: a finite reflection group $G \subseteq \mathrm{GL}_n(\mathbb{Z})$
Construct the root system $\Phi$ from $G$ (Algorithm 1)
Construct a base $\Delta \subseteq \Phi$ for $E = \pi(V)$ (Algorithm 2)
Compute the fundamental dominant weights $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}^n$ from equation (2.17)
for i = 1 to r do
    Find the least $0 \neq n_i \in \mathbb{N}$ such that $n_i\lambda_i \in \pi(\mathbb{Z}^n)$
end for
Let $Y := \{ \sum_{i=1}^{r} n_i'\lambda_i \ : \ n_i' \in \mathbb{N},\ 0 \leq n_i' \leq n_i \}$
Let $Z := (\pi(\mathbb{Z}^n) \cap Y) \setminus \{ 0 \}$
Let HB := $Z \setminus \{ z_1 + z_2 \ : \ z_1, z_2 \in Z \}$
Output: HB.
```

CHAPTER 4

MULTIPLICATIVE INVARIANTS UNDER SUBGROUPS OF REFLECTION GROUPS

4.1 Overview

In this chapter we will assume that G is a *subgroup* of a reflection group $H \subseteq \mathrm{GL}(A)$. Our goal is to produce generators for the ring of invariants $k[A]^G$. By Corollary 2.7 we know that $k[A]^G$ is a finitely generated $k[A]^H$-module. We provide algorithms that will (1) produce the module generators (Algorithm 6, §4.3), and (2) rewrite any G-invariant as a $k[A]^H$-linear combination of these module generators (Algorithm 5, §4.2).

Much of the work in this chapter was inspired by [Göb95] in which Göbel examines classical invariants under subgroups of the symmetric group.

All the notation of the previous chapter remains valid, now with the reflection group H in place of G. In particular, recall that for $a \in A$ we denote the orbit sum of a under G as $\sigma_G(a)$, and we denote the orbit sum of a under H as $\sigma_H(a)$. Let $\Delta \subseteq A$ be a set of simple roots for $E = \pi(V)$ as constructed in §2.4, from the reflection group

H. As before $D = \{\, a \in A \ : \ (a, \delta) \geq 0 \ \forall \ \delta \in \Delta \,\}$ is a fundamental domain for the action of H on A.

4.2 Generators for Invariants Under a Subgroup of a Reflection Group

Let $\{\, \mathrm{Id} = h_1, h_2, \ldots, h_u \,\}$ be a left transversal for G in H, so $H = \bigcup_{i=1}^{u} h_i G$, a disjoint union. Theorem 2.24 tells us that H acts simply transitively on closed Weyl chambers, so there are $|H|$ closed Weyl chambers, and each of them can be expressed as $\overline{\mathcal{C}}^{h_i g}$ for some $i \in \{\, 1, \ldots, u \,\}$ and $g \in G$.

We introduce the following new notation: for a set $X \subseteq V$ and a subset $T \subseteq H$, define

$$X{\uparrow}^{T} := \bigcup_{t \in T} X^{t}$$

where $X^t = \{\, x^t \ : \ x \in X \,\}$.

For the following definitions and lemma it may be helpful to refer to Figure 4.1. Let $\overline{\mathcal{C}}_i := \overline{\mathcal{C}}^{h_i}$ and let $\overline{D_i} := D^{h_i}$, so of course $\overline{D_i} = A \cap \overline{\mathcal{C}}_i$. Let $D_1 := \overline{D_1} = D$, and define

$$D_i := \overline{D_i} \setminus \bigcup_{j<i} \overline{D_j}{\uparrow}^{G} \quad \text{for } i = 2, ..., u \tag{4.1}$$

Example 4.1. Consider again the finite reflection group from Example 2.18, $H = \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \right\rangle \cong S_3$, acting (by right multiplication) on $A = \mathbb{Z}^2$. Let $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and consider the subgroup $G = \langle g \rangle$. The set $\left\{\, h_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), h_2 = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), h_3 = \left(\begin{smallmatrix} -1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \,\right\}$ forms a left transversal for G in H. The sets D_i $(i = 1, 2, 3)$ are depicted in Figure 4.1. Note that $\overline{D_i}$ always contains the points of A lying on the boundary of $\overline{\mathcal{C}}_i$, whereas D_i may not.

By Theorem 2.24, the simply transitive action of H on closed Weyl chambers, we know that for any $h \in H$ the set D^h can be expressed as $D^{h_i g} = \overline{D_i}^{g}$ for some $i \in \{\, 1, \ldots, u \,\}$ and $g \in G$.

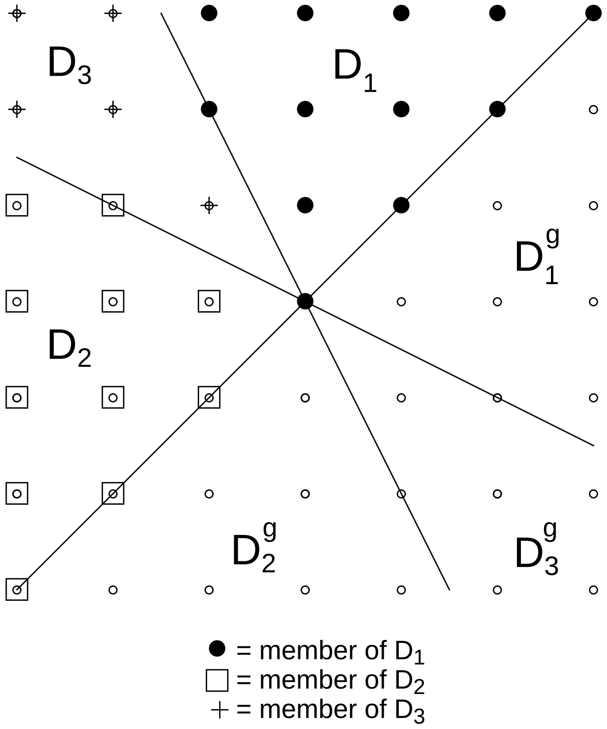

Figure 4.1: The sets D_i $(i = 1, 2, 3)$ described in Example 4.1.

Lemma 4.2.

(a) If $D_i{\uparrow}^G \cap \overline{D_j}{\uparrow}^G \neq \varnothing$ *then* $i \leq j$.

(b) A *is the disjoint union of the* $D_i{\uparrow}^G$ *for* $i = 1, ..., u$.

(c) $D_i = \overline{D_i} \setminus F$, *where* F *denotes some union of faces of* $\overline{\mathcal{C}}_i$.

(d) $\bigcup_{i=1}^{u} D_i$ *is a fundamental domain for the action of* G *on* A.

Proof. (a) If $j < i$ then by (4.1), $D_i \cap \overline{D_j}{\uparrow}^G = \varnothing$. This is exactly the contrapositive of the statement we wish to prove.

(b) If $j < i$ then by (4.1), $D_i \cap \overline{D_j}{\uparrow}^G = \varnothing$, as in part (a). Thus $D_i{\uparrow}^G \cap \overline{D_j}{\uparrow}^G = \varnothing$, and hence $D_i{\uparrow}^G \cap D_j{\uparrow}^G = \varnothing$. Now given $a \in A$, let i be minimal so that $a \in \overline{D_i}{\uparrow}^G$ (note that $\bigcup_i \overline{D_i}{\uparrow}^G = \bigcup_{h \in H} D^h = A$). Then $a^g \in \overline{D_i}$ for some g and $a^g \notin \overline{D_j}{\uparrow}^G$ for $j < i$. Thus $a^g \in \overline{D_i} \setminus \bigcup_{j<i} \overline{D_j}{\uparrow}^G = D_i$. Therefore by (4.1), $a \in D_i{\uparrow}^G$.

(c) Unraveling expression (4.1), we see

$$\begin{aligned} D_i &= \overline{D_i} \setminus \bigcup_{j<i} \left(\overline{D_i} \cap \overline{D_j}{\uparrow}^G\right) \\ &= \overline{D_i} \setminus \bigcup_{j<i} \left(\bigcup_{g \in G} \left(\overline{D_i} \cap \overline{D_j}^g\right) \right) \end{aligned}$$

Now $\overline{D_i} \cap \overline{D_j}^g = (A \cap \overline{\mathcal{C}}_i) \cap (A \cap \overline{\mathcal{C}}_j^g) = A \cap (\overline{\mathcal{C}}_i \cap \overline{\mathcal{C}}_j^g)$. Note that $\overline{\mathcal{C}}_i$ and $\overline{\mathcal{C}}_j^g$ are two closed Weyl chambers, and so their intersection must be a mutual face. Specifically, it is a face of $\overline{\mathcal{C}}_i$ and this proves part (c).

(d) By part (b) we know that the sets $D_i{\uparrow}^G$ $(1 \leq i \leq u)$ partition A. If $a \in D_i{\uparrow}^G$, then $a^G \cap D_i \neq \varnothing$. Since, by Theorem 2.25, $\overline{D_i}$ is a fundamental domain for the action of H on A, we know that the set $a^G \cap D_i$ contains exactly one element. Conversely, $a \notin D_i{\uparrow}^G$ implies $a^G \cap D_i = \varnothing$. Thus, given any $a \in A$, the set $a^G \cap \bigcup_{i=1}^u D_i$ always contains exactly one element, making it a fundamental domain for the action of G on A. □

If $\Omega_i \subseteq A$ is given such that $D_i = \Omega_i + \overline{D_i}$, then it must be true that $\Omega_i \subseteq D_i$ since $0 \in \overline{D_i}$. In §4.3, Algorithm 6 we construct finite sets Ω_i of minimal cardinality such that $D_i = \Omega_i + \overline{D_i}$. For instance, observe $D_1 = \{0\} + \overline{D_1}$ and so it suffices for Ω_1 to be $\{0\}$. Furthermore, if $\Omega_1 = \{0\}$ then it must be true that $0 \notin \Omega_i$ for $i > 1$ since the D_i's are disjoint (Lemma 4.2(b)) and $\Omega_i \subseteq D_i$.

Just as the generators for the monoid D yield algebra generators of $k[A]^H$, we will find that the elements of the Ω_i's yield generators of $k[A]^G$ as a module over $k[A]^H$. Recall from Definition 3.8 what it means for $q \in k[A]^G$ to be G-orbital where G is a subgroup of a reflection group.

Theorem 4.3. *Fix $\Omega_1, \ldots, \Omega_u \subseteq A$ such that $D_i = \Omega_i + \overline{D_i}$, and let $\Omega = \bigcup_{i=1}^u \Omega_i$. To each $\omega \in \Omega$ associate an element $q_\omega \in k[A]^G$ that is G-orbital through ω (for instance, $q_\omega = \sigma_G(\omega)$), and let $Q = \{ q_\omega \, : \, \omega \in \Omega \}$. Then Q generates $k[A]^G$ as a module over $k[A]^H$.*

The proof of this theorem is given by Algorithm 5 below which takes an arbitrary $f \in k[A]^G$ and rewrites it as a Q-linear combination of elements of $k[A]^H$.

Algorithm 5 Rewrite $f \in k[A]^G$ as a Q-linear combination of H-invariants

```
1:  **Input**: $f \in k[A]^G$.
2:  **if** $f \in k$ **then**
3:      **Output:** $f$.
4:  **end if**
5:  Let $B_f := \mathrm{Supp}(f) \cap (\bigcup_{i=1}^{u} D_i)$.
6:  Write $f = \sum_{b \in B_f} k_b \sigma_G(b)$, with $k_b \in k$.
7:  **for** $b \in B_f$ **do**
8:      Determine $i$ such that $b \in D_i$.
9:      Find $\omega \in \Omega_i$ and $a \in \overline{D_i}$ such that $b = \omega + a$.
10:     Let $s_b := q_\omega \sigma_H(a) - \mathbf{Rewrite}(q_\omega \sigma_H(a) - \sigma_G(b))$.
11: **end for**
12: **Output**: $\sum_{b \in B_f} k_b s_b$.
```

In line 5, notice that by Lemma 4.2(d), $\bigcup_{i=1}^{u} D_i$ is a fundamental domain for the action of G on A. Thus, every G-orbit sum in f contains exactly one representative in B_f, and this is expressed in line 6. In line 9, the fact that there exists such an a and ω comes from our hypothesis that $D_i = \Omega_i + \overline{D_i}$.

In line 10, the algorithm calls itself recursively. Note first that $s_b = \sigma_G(b)$ since the algorithm only rewrites an invariant; it does not change its value. Secondly, note that indeed the new argument, $q_\omega \sigma_H(a) - \sigma_G(b)$, is an element of $k[A]^G$. Thirdly, note that s_b is a Q-linear combination of elements of $k[A]^H$: the first term, $q_\omega \sigma_H(a)$ is an element of Q times an element of $k[A]^H$, and the second term, by recursion, must also be in the desired form. Finally, the output in line 12 must be a Q-linear combination of H-invariants since each s_b is.

The remainder of this section works toward Corollary 4.8 in which we prove that the algorithm terminates by showing that $\sigma_H(a) q_\omega - \sigma_G(b)$ (line 10) is "strictly less than" f with respect to the following partial order with DCC.

Definition 4.4. Given $p, f \in k[A]$ we write $p \prec f$ if $p < f$ or if $p \not> f$ and $\min \{ i \ : \ \mathrm{HM}(p) \cap D_i \neq \varnothing \} > \min \{ i \ : \ \mathrm{HM}(f) \cap D_i \neq \varnothing \}$.

Here, the partial order $<$ on V and the sets $\mathrm{HM}(\cdot)$ of highest monomials are defined as in Section 3.2.1 using the base Δ for the reflection group H. The relation $\prec$ satisfies DCC on $k[A]^G$ since $<$ has DCC on $k[A]$ and there are only finitely many D_i.

When we multiply an H-orbital and a G-orbital element together, the HM set of their product has a form that is easy to describe. The following generalizes Lemma 3.10.

Lemma 4.5. *Consider $p \in k[A]^H$, and $q \in k[A]^G$ such that p is H-orbital through $a \in \overline{D_i}$ for some i, and q is G-orbital through $\omega \in D_i$. Then $\mathrm{HM}(pq) = (a+\omega)^{H_\omega G}$ where H_ω is the isotropy subgroup in H for ω. Furthermore, for any $z \in \mathrm{HM}(pq)$, the coefficient on z^* in the expansion of pq is 1_k.*

Proof. We prove the lemma in three steps. We will keep the notation $x \in \mathrm{Supp}(p)$ and $y \in \mathrm{Supp}(q)$, and observe that if $z \in \mathrm{Supp}(pq)$, then $z = x + y$ for some $x \in \mathrm{Supp}(p)$ and $y \in \mathrm{Supp}(q)$. Furthermore, observe that $\overline{D_i}$ is a monoid and $D_i \subseteq \overline{D_i}$, thus a, ω, and $a + \omega$ are all in $\overline{D_i}$. Letting h_i be a member of the left transversal for G in H we get

$$\overline{a+\omega} = (a+\omega)^{h_i^{-1}} = a^{h_i^{-1}} + \omega^{h_i^{-1}} = \bar{a} + \bar{\omega}. \tag{4.2}$$

(1) *$(a+\omega)^\ell \in \mathrm{Supp}(pq)$ for all $\ell \in H_\omega G$. Furthermore, if $z = (a+\omega)^\ell$ then the coefficient on z^* in the expansion of pq is 1_k.*

Suppose that $x + y = (a+\omega)^\ell$ for some $\ell \in H_\omega G$. Our claim will be proved by showing that $x = a^\ell$ and $y = \omega^\ell$.

Putting $h := \ell^{-1} h_i^{-1}$ and using (4.2) we get $x^h + y^h = (a+\omega)^{\ell h} = \bar{a} + \bar{\omega}$. Certainly then $\pi(x^h + y^h) = \pi(\bar{a} + \bar{\omega})$ and by Lemma 3.9, this implies $x^h = \bar{a}$ and $y^h = \bar{b}$. Thus $x = a^\ell$ and $y = b^\ell$ as desired.

(2) *If $z \in \mathrm{Supp}(pq)$, then $z \lesssim a + \omega$.*

Write $z = x + y$. By the transitive action of H on the Weyl chambers (Theorem 2.24), there exists $h \in H$ such that $(x+y)^h = \overline{x+y} \in D$. Thus

$$\pi(\overline{a+\omega} - \overline{x+y}) = \pi(\bar{a} + \bar{\omega} - (x^h + y^h)) = \pi(\bar{a} - x^h) + \pi(\bar{\omega} - y^h). \tag{4.3}$$

By Lemma 3.6, each of the two terms on the right hand side above is in $\mathbb{R}_+\Delta$, and hence $\pi(\overline{a+\omega}-\overline{x+y}) \in \mathbb{R}_+\Delta$. By Definition 3.1 this means exactly that $x+y \lesssim a+\omega$.

(3) *If* $z \in \operatorname{Supp}(pq)$ *and* $z \sim a+\omega$, *then* $z \in (a+\omega)^{H_\omega G}$.

Write z as $x+y$. If $x+y \sim a+\omega$ then, by definition,

$$\pi(\overline{a+\omega} - \overline{x+y}) = 0.$$

We can write $\overline{a+\omega} = \bar{a} + \bar{b}$ and $\overline{x+y} = (x+y)^h$ for some $h \in H$, and so the above equation can be rewritten as

$$\pi(\bar{a} + \bar{\omega}) = \pi(x^h + y^h).$$

Applying Lemma 3.9 and expression (4.2), we get $x^h = \bar{a} = a^{h_i^{-1}}$ and $y^h = \bar{\omega} = \omega^{h_i^{-1}}$. Setting $\ell = h^{-1}h_i^{-1}$, this gives us

$$x = a^\ell \quad \text{and} \quad y = \omega^\ell \tag{4.4}$$

and so

$$z = x + y = (a+\omega)^\ell. \tag{4.5}$$

From (4.4) it is clear that $y \sim \omega$. Since q is G-orbital through ω, and $y \in \operatorname{Supp}(q)$, it must happen that $y = \omega^g$ for some $g \in G$. Thus $\omega^g = \omega^\ell$ implying $\omega = \omega^{\ell g^{-1}}$, and so $\ell g^{-1} \in H_\omega$. Finally, we can conclude

$$\ell \in H_\omega G. \tag{4.6}$$

Equations (4.5) and (4.6) together prove step (3). □

Lemma 4.6. *Suppose* $a \in \overline{D_i}$ *and* $\omega \in D_i$. *Then either*

1) $(a+\omega)^{H_\omega G} \setminus (a+\omega)^G = \varnothing$, *or*

2) $(a+\omega)^{H_\omega G} \setminus (a+\omega)^G \subseteq \bigcup_{j>i} D_j{\uparrow}^G$.

Proof. Clearly $(a+\omega)^{H_\omega G} \supseteq (a+\omega)^G$, and so if $(a+\omega)^{H_\omega G} = (a+\omega)^G$ then case (1) above occurs.

Suppose that $(a+\omega)^{H_\omega G} \supsetneq (a+\omega)^G$, and so there exists some $\ell \in H_\omega G$ such that

$$(a+\omega)^\ell \notin (a+\omega)^G. \tag{4.7}$$

By Lemma 4.2(b), there exists a unique j such that $(a+\omega)^\ell \in D_j{\uparrow}^G$. If $j = i$, then $(a+\omega)^\ell \in D_i^g \subseteq \overline{\mathcal{C}}_i^g$ for some $g \in G$. But of course, since $a+\omega \in \overline{D_i}$, we know that $(a+\omega)^g \in D_i^g \subseteq \overline{\mathcal{C}}_i^g$. By Theorem 2.25, the orbit $(a+\omega)^H$ intersects $\overline{\mathcal{C}}_i^g$ in exactly one point, and thus $(a+\omega)^\ell = (a+\omega)^g$. But this contradicts expression (4.7). Thus

$$(a+\omega)^\ell \in D_j{\uparrow}^G \text{ for some } j \neq i.$$

We will now prove that in fact $j > i$ by showing $\omega \in D_i{\uparrow}^G \cap \overline{D_j}{\uparrow}^G$ and appealing to Lemma 4.2(a). By hypothesis, we know that $\omega \in D_i \subseteq D_i{\uparrow}^G$. Claim: $\omega \in \overline{D_j}{\uparrow}^G$. Once the claim is proved, the proof of the lemma will be complete.

We know that $a, \omega \in \overline{D_i}$ and $(a+\omega)^\ell \in \overline{D_j}^g$ for some $g \in G$. By Lemma 3.7 this implies $a^\ell, \omega^\ell \in \overline{D_j}^g$. Write $\ell = hg'$ for some $h \in H_\omega$ and $g' \in G$. Then

$$\omega^{g'} = \omega^{hg'} = \omega^\ell \in \overline{D_j}^g.$$

Consequently, $\omega \in \overline{D_j}{\uparrow}^G$ as needed, and the claim and the proof are complete. □

Lemma 4.7. *Let notation be given as in Algorithm 5. Then* $q_\omega \sigma_H(a) - \sigma_G(b) \prec f$.

Proof. Recall that $a \in \overline{D_i}$, $\omega \in D_i$, and $b = a+\omega \in D_i$. We know that $\mathrm{HM}(\sigma_G(a+\omega)) = (a+\omega)^G$ and that the coefficient of any element in $\mathrm{HM}(\sigma_G(a+\omega))$ is 1_k. By Lemma 4.5 we know that $\mathrm{HM}(q_\omega\sigma_H(a)) = (a+\omega)^{H_\omega G}$ and that the coefficient of any element in $\mathrm{HM}(q_\omega\sigma_H(a))$ is 1_k.

Claim: if $b \notin \mathrm{HM}(f)$, then for any $x \in \mathrm{HM}(q_\omega\sigma_H(a) - \sigma_G(a+\omega))$ there exists some $y \in \mathrm{HM}(f)$ such that $x < y$. To see this, note first that $b \notin \mathrm{HM}(f)$ implies there exists $y \in \mathrm{HM}(f)$ such that $b < y$. Next, $x \in \mathrm{HM}(q_\omega\sigma_H(a) - \sigma_G(a+\omega))$ implies $x \lesssim a+\omega = b$. By the transitivity of the partial order, $x < y$. Now the claim is proved. By Definition 3.4, $q_\omega\sigma_H(a) - \sigma_G(a+\omega) < f$, and consequently, Definition 4.4 tells us that $q_\omega\sigma_H(a) - \sigma_G(a+\omega) \prec f$.

For the remainder of the proof we may assume $a+\omega \in \mathrm{HM}(f)$. Since f is G-invariant, this implies $(a+\omega)^G \subseteq \mathrm{HM}(f)$. Consider now the two possibilities in Lemma 4.6 for the form of $(a+\omega)^{H_\omega G} \setminus (a+\omega)^G$.

CASE 1: $(a+\omega)^{H_\omega G} \setminus (a+\omega)^G = \varnothing$. Then

$$\begin{aligned}
&x \in \mathrm{HM}(q_\omega \sigma_H(a) - \sigma_G(a+\omega)) \\
\Longrightarrow\ & x \in \mathrm{Supp}(q_\omega \sigma_H(a) - \sigma_G(a+\omega)) \subseteq \mathrm{HM}(f) \\
\Longrightarrow\ & x < y \text{ for all } y \in \mathrm{Supp}(\sigma_G(a+\omega)) \\
\Longrightarrow\ & \exists\ y \in \mathrm{HM}(f) \text{ such that } x < y.
\end{aligned}$$

Thus, by Definition 3.4, $q_\omega \sigma_H(a) - \sigma_G(a+\omega) < f$. Consequently, Definition 4.4 tells us $q_\omega \sigma_H(a) - \sigma_G(a+\omega) \prec f$.

CASE 2: $(a+\omega)^{H_\omega G} \setminus (a+\omega)^G \subseteq \bigcup_{j>i} D_j{\uparrow}^G$. Now

$$\begin{aligned}
&x \in \mathrm{HM}(q_\omega \sigma_H(a) - \sigma_G(a+\omega)) \ \cap\ \bigcup_{j=1}^{u} D_j \\
\Longrightarrow\ & x \in (a+\omega)^{H_\omega G} \setminus (a+\omega)^G \ \cap\ \bigcup_{j>i} D_j \\
\Longrightarrow\ & \min\{\, j \ :\ x \in D_j \,\} > i = \min\{\, j \ :\ \mathrm{HM}(\sigma_G(a+\omega)) \cap D_j \neq \varnothing \,\} \\
& \qquad\qquad\qquad\qquad \geq \min\{\, j \ :\ \mathrm{HM}(f) \cap D_j \neq \varnothing \,\}\,.
\end{aligned}$$

The last inequality above uses the fact that $\mathrm{HM}(\sigma_G(a+\omega)) = (a+\omega)^G \subseteq \mathrm{HM}(f)$. We finally need to show that in fact $q_\omega \sigma_H(a) - \sigma_G(a+\omega) \not\succ f$. One sees this since for all $x \in \mathrm{HM}(q_\omega \sigma_H(a))$ and all $y \in \mathrm{HM}(\sigma_G(a+\omega))$, we have $x \sim y$, and so $q_\omega \sigma_H(a) - \sigma_G(a+\omega) \lesssim \sigma_G(a+\omega)$. Certainly $\sigma_G(a+\omega) \not\succ f$ since $\mathrm{Supp}(\sigma_G(a+\omega)) \subseteq \mathrm{Supp}(f)$. Thus we must have $q_\omega \sigma_H(a) - \sigma_G(a+\omega) \prec f$ □

Corollary 4.8. *Algorithm 5 eventually terminates.*

Proof. The order $\prec$ satisfies DCC on $k[A]^G$, and every time Algorithm 5 calls itself in line 10, Lemma 4.7 assures us that the new argument is strictly less than (with respect to $\prec$) the argument it received. The base case is handled when $f \in k$, in which case the algorithm immediately returns f itself. □

4.3 Constructing Ω_i

We begin by defining what we mean by the notation Ω_i.

Definition 4.9. Ω_i is a minimal set (with respect to containment) satisfying

$$D_i = \Omega_i + \overline{D_i}$$

Note that D_i may not be uniquely determined. The aim of this section is to construct minimal sets Ω_i for $(i = 1, \ldots, u)$. Let $\{ F_j \}_{j \in J}$ be some collection of faces of $\overline{\mathcal{C}}$, and let $F = \bigcup_{j \in J} F_j$. It is evident that $\overline{D_i}$ is H-isomorphic to D, and considering Lemma 4.2(c), D_i is H-isomorphic to $D \setminus F$ for some collection of faces. We will find a finite set $Y \subseteq D$ such that $D \setminus F = Y + D$, and then modify Y to obtain a minimal set Ω such that $D \setminus F = \Omega + D$.

Recall from Definition 2.29 that if F_j is a face of $\overline{\mathcal{C}}$, then there exists some $v_j \in \mathbb{R}_+\Delta$ such that $(v_j, w) = 0$ for all $w \in F_j$, and $(v_j, w) > 0$ for all $w \in \overline{\mathcal{C}} \setminus F_j$. Also, recall the definition of K_B (3.8), and the fact that there is a bijection between any set $X \subseteq \pi(A)$ and the set $A \cap (X + K_B)$ by Corollary 3.13.

Lemma 4.10. *Let F be some union of faces of $\overline{\mathcal{C}}$, and suppose that there exists a set $Y \subseteq \pi(D)$ such that $\pi(D \setminus F) = Y + \pi(D)$. Then putting $Y' := A \cap (Y + K_B)$, we get $D \setminus F = Y' + D$.*

Proof. We first show that $D \setminus F \supseteq Y' + D$. Recall from Corollary 3.13 that $Y' \subseteq D$; so certainly $Y' + D \subseteq D$ Write $F = \bigcup_{j \in J} F_j$ for faces F_j of $\overline{\mathcal{C}}$, and let $\{ v_j \}_{j \in J} \subseteq \mathbb{R}_+\Delta$ be chosen so that $(v_j, w) = 0$ for all $w \in F_j$ and $(v_j, w) > 0$ for all $w \in D \setminus F_j$. Let $y' \in Y'$, let $d \in D$. By construction, $\pi(y') \in Y$, so our hypothesis $\pi(D \setminus F) = Y + \pi(D)$ implies $\pi(y' + d) := x \in \pi(D \setminus F)$. Thus there exists some $x' \in D \setminus F$ so that $\pi(x') = x$, and it follows that $y' + d = x' + c$ for some $c \in \mathrm{Ker}_A(\pi) = A^G \subseteq D$. For any $j \in J$, we get $(v_j, x') > 0$ and $(v_j, c) \geq 0$, and hence

$$(v_j, y' + d) = (v_j, x' + c) = (v_j, x') + (v_j, c) > 0.$$

That is, $y' + d \notin F_j$ for any j, and so $y' + d \notin F$. This proves the inclusion $Y' + D \subseteq D \setminus F$.

To show $D \setminus F \subseteq Y' + D$, take any $x \in D \setminus F$. Then $\pi(x) \in \pi(D \setminus F)$ and by hypothesis, $\pi(x) = y + \pi(d)$ for some $y \in Y$ and $d \in D$. By construction of Y'

and Corollary 3.13, there exists a (unique) $y' \in Y'$ such that $\pi(y') = y$, and hence $\pi(x) = \pi(y' + d)$. This implies that $x = y' + d + c$ for some $c \in A^G = \operatorname{Ker}_A(\pi)$. Now $A^G \subseteq D$, so $d + c \in D$, and containment is shown. □

From the above lemma, our problem of finding a set $Y \subseteq D$ such that $D \setminus F = Y + D$ reduces to the problem of finding $Y \subseteq \pi(D)$ such that $\pi(D \setminus F) = Y + \pi(D)$.

Recall from §3.4 that $m_i := n_i\lambda_i$ where λ_i is a fundamental dominant weight and $0 \neq n_i \in \mathbb{N}$ is minimal such that $n_i\lambda_i \in \pi(D)$. Recall (3.9),

$$K_M := \sum_{i=1}^{r} [0, m_i] = \left\{ \sum_{i=1}^{r} t_i m_i \;:\; 0 \leq t_i \leq 1 \right\}.$$

and recall from (3.10) that the finite set

$$Z := \pi(A) \cap K_M \setminus \{ 0 \}$$

generates the monoid $\pi(D)$. Note that K_M and Z are both contained in $E = \pi(V)$. Put

$$Y := Z \setminus F \subseteq \pi(D).$$

Lemma 4.11. $\pi(D \setminus F) = Y + \pi(D)$.

Proof. First observe, by Lemma 2.30, that $\pi(F)$ is a union of faces for $\pi(\overline{\mathcal{C}})$, and $\pi(D \setminus F) = \pi(D) \setminus \pi(F)$.

The containment $\pi(D \setminus F) \supseteq Y + \pi(D)$ is not difficult to see: for any $j \in J$ it happens that $(v_j, y) > 0$ for all $y \in Y$, and also $(v_j, d) \geq 0$ for all $d \in \pi(D)$. Thus for all $j \in J$ we have $(v_j, y + d) = (v_j, y) + (v_j, d) > 0$ implying $y + d \in \pi(D \setminus F)$.

For the other containment, suppose that $x \in \pi(D \setminus F) = \pi(D) \setminus \pi(F)$. By Lemma 2.28(b) and formula (2.14)

$$\pi(D) \subseteq \Lambda_+ = \bigoplus_{i=1}^{r} \mathbb{N}\lambda_i$$

and, clearly,

$$\bigoplus_{i=1}^{r} \mathbb{N}\lambda_i \subseteq \bigoplus_{i=1}^{r} \mathbb{Q}_+\lambda_i = \bigoplus_{i=1}^{r} \mathbb{Q}_+ m_i.$$

Thus, since $x \in \pi(D)$, we can write

$$x = \sum_{i=1}^{r} q_i m_i \tag{4.8}$$

for some $q_i \in \mathbb{Q}_+$. Let $I := \{\, i \ : \ 1 \leq i \leq r,\ q_i \neq 0 \,\}$, and for $i \in I$ define

$$t_i := \begin{cases} 1 & \text{if } q_i \in \mathbb{N} \\ q_i - \lfloor q_i \rfloor & \text{otherwise} \end{cases}$$

where $\lfloor\ \rfloor$ is the greatest integer function. Let

$$m := \sum_{i \in I} t_i m_i$$

and thus

$$x = m + \sum_{i \in I} (q_i - t_i) m_i. \tag{4.9}$$

Since $q_i - t_i \in \mathbb{N}$, clearly $\sum_{i \in I} (q_i - t_i) m_i \in \pi(D)$, and so the lemma will be proved by showing that $m \in Y$.

Since $x \in \pi(A)$ and $\sum_{i \in I} (q_i - t_i) m_i \in \pi(A)$ it follows from (4.9) that $m \in \pi(A)$. Furthermore, since $0 < t_i \leq 1$, we know $m \in K_M \setminus \{\, 0 \,\}$. Thus $m \in \pi(A) \cap K_M \setminus \{\, 0 \,\} = Z$.

Since $Y = Z \setminus F$, it only remains to show that $m \notin F$. If there is any $j \in J$ such that $\{\, m_i \,\}_{i \in I} \subseteq F_j$, then we see from (4.8) that $x \in F_j$, and so $x = \pi(x) \in \pi(F)$ contradicting our hypothesis. Thus, for each $j \in J$ there exists some $i \in I$ such that $(v_j, m_i) > 0$. Consequently, for each $j \in J$,

$$(v_j, m) = (v_j, \sum_{i \in I} t_i m_i) = \sum_{i \in I} t_i (v_j, m_i) > 0.$$

Hence, $m \notin F_j$ for any j, and so $m \notin F$. We have now shown that $m \in Y$.

Thus, equation (4.9) expresses x as the sum of an element in Y and an element in $\pi(D)$. □

We now use the set $Y = Z \setminus F$ to create a minimal subset Ω such that $\pi(D \setminus F) = \Omega + \pi(D)$. If $F = \varnothing$ then clearly $\Omega = \{\, 0 \,\}$ suffices. For $F \neq \varnothing$ consider the set

$$\Omega := Y \setminus (Y + Z). \tag{4.10}$$

Figure 4.2: The sets described in Example 4.12. Note that $0 \in \Omega_1$.

Lemmas 4.13 and 4.14 prove that Ω is indeed the set we seek. Recalling Definition 4.9, the definition of Ω_i, the following example illustrates how we find the Ω_i.

Example 4.12. Recall the groups H, G, and the transversal from Example 4.1, and consider Figure 4.2. The set Z consists of those lattice points, excluding 0, in the dashed parallelogram (K_M) shown in $D_1 = D$. Let Z_2 denote the image of Z in $\overline{D_2}$ and let Z_3 denote the image of Z in $\overline{D_3}$. Then

$$\begin{aligned} Y_1 &= Z \\ Y_2 &= Z_2 \setminus \{\text{the boundary points in } \overline{D_1}{\uparrow}^G\} = Z_2 \\ Y_3 &= Z_3 \setminus \{\text{the boundary points in } \overline{D_1}{\uparrow}^G \text{ and } \overline{D_2}{\uparrow}^G\}. \end{aligned}$$

The cross at the origin represents the set $\Omega_1 = \{\, 0 \,\}$, the three crosses in D_2 are the elements of Ω_2, and the single cross in D_3 is the only element of Ω_3.

Lemma 4.13. *Given $y \in Y$, we can write $y = \omega + d$ for some $\omega \in \Omega$ and $d \in \pi(D)$.*

Proof. From (4.10) it is clear that for any $y \in Y$, either $y \in \Omega$, or $y = y' + z$ for some $y' \in Y$ and $z \in Z \subseteq \pi(D)$. By Lemma 2.31(a), that there is a monoid homomorphism $\varphi : \pi(D) \to \mathbb{N}$ satisfying $\varphi(d) > 0$ for all $0 \neq d \in \pi(D)$. Since $Y \subseteq \pi(D)$, we know that if $y = y' + z$, then $\varphi(y') < \varphi(y)$; by induction we must have $y' = \omega + d$ for some $\omega \in \Omega$ and $d \in \pi(D)$. Thus $y = \omega + d + z$. Since $d + z \in \pi(D)$, this proves the lemma. □

Lemma 4.14. *Let Ω be constructed as in (4.10). Then $\pi(D \setminus F) = \Omega + \pi(D)$. Furthermore, for any set $\Omega_0 \subsetneq \Omega$, we have $\pi(D \setminus F) \neq \Omega_0 + \pi(D)$.*

Proof. The fact that $\pi(D \setminus F) = \Omega + \pi(D)$ is an immediate consequence of Lemmas 4.11 and 4.13.

To prove minimality, let $\omega \in \Omega \setminus \Omega_0$. Now $\omega \in \Omega \subseteq Y \subseteq \pi(D \setminus F)$, so assume we can write

$$\omega = \omega_0 + d \tag{4.11}$$

for some $\omega_0 \in \Omega_0$ and $d \in \pi(D)$. By choice of ω we know $d \neq 0$. By the construction of Ω, we know that for any $y \in Y$, either $y \in \Omega$, or $y = y' + z$ for some $y' \in Y$ and $z \in Z \subseteq \pi(D)$, but not both statements can be true. Since $\omega_0 \in Y$ and $\omega \in \Omega$ we conclude from equation (4.11) that we must have $d \notin Z$.

Claim: If $0 \neq d \in \pi(D) \setminus Z$ and $d' \in \pi(D)$ then $d + d' \notin Z$. Assuming the claim true for now, we must equation (4.11) implies that $\omega \notin Z$ since $\omega_0 \in \pi(D)$. However, this contradicts the fact that $\omega \in \Omega \subseteq Y \subseteq Z$, and so expression (4.11) is not possible. It only remains to prove the claim.

Proof of claim: If $d' \in \pi(D)$, then $d' = s_1 m_1 + \cdots + s_r m_r$ for $s_i \in \mathbb{Q}_+$; see (4.8). If $0 \neq d \in \pi(D) \setminus Z$, then $d = t_1 m_1 + \cdots + t_r m_r$ with all $t_i \in \mathbb{Q}_+$, and some $t_i > 1$. Thus $t_i + s_i > 1$ for some i, and $d + d' \notin Z$. □

Finally, we collect several of the preceding ideas together in Algorithm 6 and outline those steps required to actually compute the sets Ω_i for $1 \leq i \leq u$.

Algorithm 6 Computing Ω_i

```
**Input:** A finite reflection group $H \subseteq \mathrm{GL}(A)$ and a subgroup $G \subseteq H$.
Using $H$, compute the set $Z \subseteq \pi(D)$ as was done in Algorithm 4
Compute a left transversal $\{\, \mathrm{Id} = h_1, h_2, \ldots, h_u \,\}$ for $G$ in $H$
**for** $i$ from 1 to $u$ **do**
    Define $Z_i := Z^{h_i}$
**end for**
$X := \varnothing$
$\Omega_1 := 0$
**for** $i$ from 2 to $u$ **do**
    $X := X \cup Z_{i-1}\!\uparrow^G$
    $Y := Z_i \setminus X$
    $\Omega_i := Y \setminus (Y + Z_i)$
**end for**
**if** $\pi \neq \mathrm{Id}$ **then**
    **for** $i$ from 1 to $u$ **do**
        $\Omega_i := A \cap (\Omega_i + K_B)$
    **end for**
**end if**
**Output:** $\bigcup_{i=1}^{u} \Omega_i$
```

REFERENCES

[Bou68] N. Bourbaki, *Groupes et Algèbre de Lie, IV, V, VI*, Hermann, Paris, 1968.

[BH93] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge, New York, 1993.

[Che55] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **67** (1955), 778–782.

[Die00] R. Diestel, *Graph Theory*, Springer-Verlag, New York, 2000.

[DK02] H. Derksen and G. Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[Far84] D. R. Farkas, *Multiplicative Invariants*, Enseign. Math. **30** (1984), 141–157.

[Far85] D. R. Farkas, *Toward Multiplicative Invariant Theory*, In S. Montgomery (ed.) Group Actions on Rings, Contemp. Math. **43** (1985), Amer. Math. Soc., Providence, RI, 69–80.

[Far86] D. R. Farkas, *Reflection Groups and Multiplicative Invariants*, Rocky Mountain J. of Math. **16** (1986), 215–222.

[Fle00] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **156** (2000), 23 –32.

[Fog01] J. Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7.

[Ful93] W. Fulton, *Introduction to Toric Varieties*, Annals of Math. Studies **131**, Princeton University Press, Princeton, 1993.

[Göb95] M. Göbel, *Computing Bases for Rings of Permutation-invariant Polynomials*, J. Symbolic Computation **19** (1995), 285–291.

[Hil90] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.

[Hil93] D. Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–373.

[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.

[Hum72] J. E. Humphries, *Introduction to Lie Algebras and Representation Theory*, Grad. Texts in Math **9** (1972), Springer-Verlag, New York.

[Hum90] J. E. Humphries, *Reflection Groups and Coxeter Groups*, Cambridge studies in advanced mathematics **29** (1990), Cambridge University Press, Cambridge.

[Lor01] M. Lorenz, *Multiplicative Invariants and Semigroup Algebras*, Algebra and Representation Theory **4** (2001), 293–304.

[Noe16] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.

[Noe26] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28–35; reprinted in *Collected Papers*, pp. 485–492, Springer-Verlag, New York, 1983.

[Pas71] D. Passman, *Infinite Group Rings*, Marcel Dekker, New York, 1971.

[Rei02] Z. Reichstein, *SAGBI bases in rings of multiplicative invariants*, Preprint, available from `www.math.ubc.ca/~reichst/pub.html`.

[RS90] L. Robbiano and M. Sweedler, *Subalgebra bases*, Springer Lecture Notes in Mathematics **1430** (1990), 61–87.

[Ros78] J. E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc. **36** (1978), 385–447;

[Sal87] D. J. Saltman, *Multiplicative field invariants*, J. Algebra **106** (1987), 221–238.

[Ser67] J.-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, In Colloque d'algèbre ENSFJ, Paris 1967, Secrétariat mathématique, 1968.

[ST54] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6**(1954), 274–304.

[Slo77] N. J. A. Sloane, *Error correcting codes and invariant theory: New applications of a nineteenth-century technique*, Amer. Math. Monthly **84** (1977), 82–107.

[Smi95] L. Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Massachusetts, 1996.

[Ste75] R. Steinberg, *On a Theorem of Pittie*, Topology **14** (1975), 173–177.

[Stu96] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8** (1996), Amer. Math. Soc., Providence, RI.

[Swa92] R. Swan, *Gubeladze's proof of Anderson's conjecture*, Contemp. Math. **124** (1992), Amer. Math. Soc., Providence, RI, 215–250.

[Van85] B. L. Van Der Waerden, *A History of Algebra*, Springer-Verlag, Berlin, New York, 1985.

APPENDIX A

THE PROGRAM SOURCE CODE

The following code, written for the Computer Algebra System *Magma*, contains many functions for using integer matrix reflection groups to compute root systems, fundamental dominant weights, etc. The two main functions are “HB” and “ModuleGens”, outlined in Sections 3.4 and 4.3 respectively. Commands which are predefined in *Magma* are shown in boldface.

```
//  The following functions/procedures are defined in this file.

// CheckGroup(~G : CheckReflectionGroup := true)
// FundamentalDominantWeights(A, G)
// FDW(A, G)
// HB(G)
// IsReflectionGroup(G)
// LatticeOfGroup(G)
// LiftToA(X, A, G)
// ModuleGens(G, H : ShowMore := false)
// Proj(V, A, B)
// reflection(v, a)
// ReflectionsOfGroup(G)
// RootSys(A, G)
// SeqProduct(SS)
// SimpleRoots(A, G)
// SpaceDecomp(A, G)
// Ztope(A, G : ComputeBoundary := false)
// Create a lattice with standard basis and
// G-invariant inner product
LatticeOfGroup := function(G)
  pdf := ChangeRing(PositiveDefiniteForm(G), BaseRing(G));
  return Lattice(G!1, pdf);
end function;


// Given a group G, return the set of reflections in that group
ReflectionsOfGroup := function(G)
  Mat := MatrixRing(Integers(), Degree(G));
  return {g : g in G | Rank(Mat!g - Mat!1) eq 1};
end function;


IsReflectionGroup := function(G)
  return G eq MatrixGroup<Degree(G),BaseRing(G)|ReflectionsOfGroup(G)>;
end function;


CheckGroup := procedure(~G : CheckReflectionGroup := true)
  Mat := MatrixRing(Integers(), Degree(G));
  if exists{g : g in Generators(G) | not IsCoercible(Mat,g)} then
    error "Error: Your group contains matrices with noninteger entries
        .";
  end if;

  if CheckReflectionGroup and not IsReflectionGroup(G) then
    error "Error: The group you entered is not a reflection group.";
  end if;

  //Finally, we make sure that the base ring of the matrix group
  //is the rationals (modifying the base ring if necessary).
  //This allows the group to act on rational lattice points,
  //not just integral ones.
  if BaseRing(G) ne Rationals() then
    G := ChangeRing(G, Rationals());
  end if;
end procedure;


// Input: a lattice, A, and a group G that acts on A
// Output: three vector spaces,
//        1) the ambient space of A
//          2) the space on which G acts effectively
//          3) the space that is pointwise fixed by G
SpaceDecomp := function(A, G)
  V := AmbientSpace(A);
  Mat := MatrixRing(Integers(), Degree(G));
  gens := Generators(G);

  fixmat := &+{Mat!g : g in gens} - #gens*Mat!1;
  fixbase := Basis(Kernel(fixmat));  //lives in A
  Fixed := sub< V | [V!f : f in fixbase] >;

  Espan := { V!(b - b^g) : b in Basis(A), g in Generators(G) };
  Effective := sub<V | Espan>;

  return V, Effective, Fixed, fixbase;
end function;


// Input: a vector space V and two subspaces A and B such that V = A ⊕ B
// Output: two projection maps and a matrix:
//      1) the projection of V onto A with kernel B
//      2) the projection of V onto B with kernel A
//      3) the matrix of the first projection (acting from right on rows)
Proj := function(V,A,B)
  n := Dimension(V);
  dimA := Dimension(A);
  dimB := Dimension(B);
  U := VerticalJoin( BasisMatrix(A), BasisMatrix(B) );
  diag := [1:i in [1..dimA]] cat [0:i in [1..dimB]];
  Pr := DiagonalMatrix(Rationals(), n, diag); // proj wrt given basis
  P := U^-1 * Pr * U;    // proj wrt standard basis
  pi  := map<V -> A | v :-> v*P >;     // proj onto A along B
  rho := map<V -> B | v :-> v - v*P>; // proj onto B along A
  return pi,rho,P;
end function;


RootSys := function(A,G)
  Mat := MatrixRing(Integers(), Degree(G));
  RS := &join{Generators(Kernel(Mat!ref + Mat!1)) : ref in
      ReflectionsOfGroup(G)};
  return  &join{{A!r, -1*(A!r)} : r in RS};
end function;


SimpleRoots := function(A,G)
  dim := Degree(G);
  RS := RootSys(A,G);  //these are points in A
  gamma := A![ i+9 : i in [1..dim] ];

  goodgamma := false;
  while goodgamma eq false do
    RootSysPlus := {r : r in RS | InnerProduct(gamma, r) gt 0};
    if RS eq RootSysPlus join {-1*r : r in RootSysPlus} then
      goodgamma := true;
    else
      gamma := gamma + A![1 : i in [1..dim]];
    end if;
  end while;

  SR := RootSysPlus diff {r+s : r,s in RootSysPlus};
  return [ sr : sr in SR ];
end function;
```

```
reflection := function(v,a)  // elements of a common inner product space
  return v - ((2*(v,a))/(a,a))*a;
end function;



FundamentalDominantWeights := function(A,G)
  SR := SimpleRoots(A,G);  //a sequence of lattice points
  V,E,F := SpaceDecomp(A,G);
  n := Dimension(V);
  r := Dimension(E); // = number of simple roots
  SRelts := [ Eltseq(SR[i]) : i in [1..r] ];
  SRmat := Matrix(Rationals(), r,n, SRelts);

  // create the simple reflections in G corresponding
  // to the simple roots
  e := Basis(A);    // standard basis e_1,...,e_n
  Refl := [];
  for j in [1..r] do
    seq := [ Eltseq(reflection(e[i],SR[j])) : i in [1..n] ];
    Refl[j] := Matrix(Rationals(), n,n, seq);
  end for;

  _, _, P := Proj(V, E, F); // P is the matrix of the projection
                            // onto E with kernel F.
  PGmat := r*P - &+Refl;
  DWmat := SRmat * PGmat^-1;
  return [ V!DWmat[i] : i in [1..r] ];
end function;

// Short-hand for the above function
FDW := FundamentalDominantWeights;
```

```
// Return the "Cartesian Product" of a sequence of sequences
// There ought to be a built-in function for this...
SeqProduct := function( SS )  // SS is a sequence of sequences
  S := [ s : s in SS | s ne [] ];
  r := #S;
  P := []; //final product
  Od := [ 1 : i in [1..r] ];  //Odometer

  go := true;
  while go do
    p := [ S[i,Od[i]] : i in [1..r] ];
    Append(~P, p);

    i := r;
    while i gt 0 and Od[i] eq #S[i] do i -:= 1; end while;
    if i gt 0 then
      Od[i] +:= 1;
      for j in [i+1..r] do Od[j] := 1; end for;
    else
      go := false;
    end if;
  end while;

  return P;
end function;




//IN:  a set X of elements in π(A)
//OUT: a set X' of elements in A such that π(X′) = X
//       X' is the set  A ∩ [X + (ρ(A) ∩ K_B)]
LiftToA := function(X, A, G)

  V,E,F,Fbasis := SpaceDecomp(A,G);
  pi, rho := Proj(V,E,F);
  AGbasis := [ A!fb : fb in Fbasis ];
  AG := sub<A | AGbasis>; //the G-fixed sublattice of A
  rhoA := ext<AG | rho(Basis(A))>;
  Q, psi := quo<rhoA | AG>; //this is finite
  WFmat := Matrix( [ F!(q @@ psi) : q in Q ] ); //WF = "weights fixed"
  //we now modify WFmat into WFrepsmat
  Bmat := Matrix( [ F!b : b in AGbasis ] );
  Xmat := Solution(Bmat, WFmat);
  for i in [1..NumberOfRows(Xmat)] do
    for j in [1..NumberOfColumns(Xmat)] do
      Xmat[i,j] := Xmat[i,j] - Floor(Xmat[i,j]);
    end for;
  end for;
  WFrepsmat := Xmat * Bmat;
  WFreps := { WFrepsmat[i] : i in [1..NumberOfRows(WFrepsmat)] };
  // WFreps = $\rho(A) \cap K_B$

  return { A!(x+w) : x in X, w in WFreps | IsCoercible(A, x+w) };
end function;



//IN:  Lattice A, and an integral matrix reflection group G
//     that acts on A
//OUT: 1) the set $(\pi(A) \cap K_M)$ $A!0$
//     2) the indexed set of "primary" monoid generators $m_1, ..., m_r$
Ztope := function(A, G : ComputeBoundary := false)
  V,E,F,Fbasis := SpaceDecomp(A,G); //Fbasis could be empty
  n := Dimension(V);
  r := Dimension(E);
  fdw := FDW(A,G); // note that #fdw = r

  if n eq r then
    // A = pi(A)
    Lat := A;
    stretchers := [ LCM([Denominator(f) : f in Eltseq(fdw[i])]) : i in
        [1..r] ];
  else
    // A != pi(A)
    pi, rho := Proj(V,E,F);
    AE := sub<A | SimpleRoots(A,G)>;  // AE = A ∩ E
    piA := ext<AE | pi(Basis(A))>;
    Lat := piA;
    stretchers := [];
    for i in [1..r] do
      j := 1;
      while not j*fdw[i] in piA do j +:= 1; end while;
      stretchers[i] := j;
    end for;
  end if;

  M := { stretchers[i]*fdw[i] : i in [1..r] };

  coeffs := SeqProduct( [ [0..stretchers[i]] : i in [1..r]] );
  Wgts := { &+{c[i]*fdw[i] : i in [1..r]} : c in coeffs };
  ZLatPts := { Lat!w : w in Wgts | IsCoercible(Lat,w) };
  Z := ZLatPts diff {Lat!0};

  if ComputeBoundary then
    BdryWgts := { &+{c[i]*fdw[i] : i in [1..r]} : c in coeffs | 0 in c
          };
    BdryLatPts := { Lat!w : w in BdryWgts | IsCoercible(Lat,w) };
    return Z, M, BdryLatPts;
  else
    return Z, M;
  end if;

end function;




//    A Main Algorithm
//
//IN:  A matrix reflection group G of rank n.
//OUT: A set of lattice points in A = ℤ^n whose G-orbit sums
//          generate the invariant ring k[A]^G
```

```
HB := function(G)
  CheckGroup(~G);
  A := LatticeOfGroup(G);

  V,E,F,Fbasis := SpaceDecomp(A,G);  //Fbasis could be empty
  n := Dimension(V);
  r := Dimension(E);

  Z, M := Ztope(A,G);  //note: $Z \subseteq \pi(A)$, and $0 \notin Z$.
  HilBase := Z diff {z1 + z2 : z1,z2 in Z};
  if n eq r then
    //make sure elements in M are listed first
    return SetToIndexedSet(M) join SetToIndexedSet(HilBase);
  else
    M := SetToIndexedSet(LiftToA(M, A, G));
    HilBase := SetToIndexedSet(LiftToA(HilBase, A, G));
    AGbasis := { A!fb : fb in Fbasis };
    B := &join{ {@ b,-b @} : b in AGbasis };
    return M join HilBase join B;
  end if;
end function;

//   A Main Algorithm
//
//IN: integral matrix groups G,H, with G in H, and H a
//     reflection group.  Rank(G) = n.
//OUT: a sequence of sets of lattice points in $A = \mathbb{Z}^n$ whose
//      G-orbit sums serve as module generators for $k[A]^G$ over $k[A]^H$
ModuleGens := function(G, H : ShowMore := false)
  CheckGroup(~H);
  CheckGroup(~G : CheckReflectionGroup := false);
  if G notsubset H then
    error "Error: Arg 1 must be a subgroup of Arg 2";
  end if;

  A := LatticeOfGroup(H);
  V,E := SpaceDecomp(A,H);
  n := Dimension(V);
  r := Dimension(E);
  T := RightTransversal(H,G);  // transversal for H over G
                                //   T[1] = identity matrix
  T := {@ t^-1 : t in T @};  // Now T is a LEFT trans. for H over G
  Zt,M,BdryPts := Ztope(A,H : ComputeBoundary := true);
                   //note: Zt ⊆ π(A) , and 0 ∉ Zt

  Z := [];
  B := [];
  Z[1] := Zt;
  B[1] := BdryPts;
  for i in [2..#T] do
    Z[i] := Zt^T[i];
    B[i] := BdryPts^T[i];
  end for;

  Used := {};
  Y := Z[1];
  ModGens := [{V!0}];   //lattice points for the module generators
  for i in [2..#T] do
    Used join:= &join{ (Y meet B[i-1])^g : g in G };
    Y := Z[i] diff Used;   //remove some faces of Z[i]
    Yirreducibles := Y diff { y+z : y in Y, z in Z[i] };
    Append(~ModGens, Yirreducibles);
  end for;

  if n gt r then
    ModGens := [ LiftToA(Yirred, A, H): Yirred in ModGens ];
  end if;

  if not ShowMore then
    ModGens := &join{ Yirred : Yirred in ModGens };
  end if;

  return ModGens;
end function;
```

APPENDIX B

SOME SAMPLE OUTPUT

```
> // The following file contains definitions for 7 integer
> // matrix groups.

> load "MultInvarExamples.m";
Loading "MultInvarExamples.m"

Example groups now loaded:
    Reflection groups:     G1, G2, G3, G4
    Other matrix groups:  H3, H4

    Containment: G2 in G1,    H3 in G3,    H4 in G4

> // The following file is printed in Appendix A, and
> // contains functions for working with reflection
> // groups and multiplicative invariants.

> load "refinv.m";
Loading "refinv.m"

> G1;
MatrixGroup(2, Rational Field)
Generators:
    [0 1]
    [1 0]
```

```
      [ 1  -1]
      [ 0  -1]


> Order(G1);
6

> IsReflectionGroup(G1);
true

> ReflectionsOfGroup(G1);
{
      [-1   0]
      [-1   1],

      [0  1]
      [1  0],

      [ 1  -1]
      [ 0  -1]
}

> // G1 is a finite reflection group of rank 2, acting
> // naturally on A = $\mathbb{Z}^2$. A submonoid, D, of A
> // can be found, as described in Chapter 2.  The command
> // HB(G) finds a minimal generating set for D; when
> // $\pi(A) = A$, this generating set is the
> // Hilbert basis for D.

> HB(G1);
{@
      (-1   2),
      (1  1),
      (0  1)
@}
```

```
> // Create the lattice that G naturally acts on,
> // with G-invariant inner product.

> A1 := LatticeOfGroup(G1); A1;
Standard Lattice of rank 2 and degree 2
Inner Product Matrix:
[2 1]
[1 2]

> RootSys(A1, G1);
{
    (0 1),
    ( 1 -1),
    (-1  0),
    (-1  1),
    (1 0),
    ( 0 -1)
}

> // Find a base for the above root system.

> SimpleRoots(A1, G1);
[
    (-1  1),
    (1 0)
]

> // Since A1 has rank 2 and there are 2 simple roots,
> // we must have A1^G1 = {0}.

> // Find the fundamental dominant weights
> // relative to the base above.

> FDW(A1, G1);
[
    (-1/3  2/3),
    (1/3 1/3)
]


> //----------------------------------------------


> G2;
MatrixGroup(2, Rational Field)
Generators:
    [0 1]
    [1 0]

> IsReflectionGroup(G2);
true

> HB(G2);
{@
    (0 1),
    (1 1),
    (-1 -1)
@}

> A2 := LatticeOfGroup(G2);

> A2;
Standard Lattice of rank 2 and degree 2

> // The next command finds the (rational) ambient space
> // of A2, the ``effective'' space, and the space that
> // is fixed under the action of G2.  V = E ⊕ F.

> V, E, F := SpaceDecomp(A2, G2);

> E;
Vector space of degree 2, dimension 1 over Rational Field
Generators:
(-1  1)
```

```
( 1 -1)
Echelonized basis:
( 1 -1)
Inner Product Matrix:
[1 0]
[0 1]

> // The fixed space for G2:

> F;
Vector space of degree 2, dimension 1 over Rational Field
Generators:
(1 1)
Echelonized basis:
(1 1)
Inner Product Matrix:
[1 0]
[0 1]

> G2 subset G1;
true

> // G2 is a subgroup of G1. We now find the module
> // generators for $k[A2]^{G2}$ as a module over
> // $k[A2]^{G1}$, as described in Chapter 4.

> ModuleGens(G2, G1);
{
    (-1  1),
    (-1  0),
    (-1 -1),
    (-2  1),
    (0 0)
}

> // We can explicitly list the sets $\Omega_1, \Omega_2, \Omega_3$.
> ModuleGens(G2, G1 : ShowMore);
[
    {
        (0 0)
    },
    {
        (-1  0),
        (-1 -1),
        (-2  1)
    },
    {
        (-1  1)
    }
]

//------------------------------------------------------------


> G3;
MatrixGroup(3, Rational Field)
Generators:
    [0 1 0]
    [1 0 0]
    [0 0 1]

    [0 0 1]
    [1 0 0]
    [0 1 0]

> Order(G3);
6

> IsReflectionGroup(G3);
true

> ReflectionsOfGroup(G3);
{
    [0 0 1]
    [0 1 0]
    [1 0 0],

    [0 1 0]
    [1 0 0]
    [0 0 1],

    [1 0 0]
    [0 0 1]
    [0 1 0]
}

> // The elements of HB(G) are listed so that any points
> // in A^G are listed last. These points always occur
> // in ±b pairs.

> HB(G3);
{@
    (0 0 1),
    (0 1 1),
    (1 1 1),
    (-1 -1 -1)
@}

> A3 := LatticeOfGroup(G3);

> SimpleRoots(A3, G3);
[
    (-1  1  0),
    ( 0 -1  1)
]


//-------------------------------------------------------------
```

```
> G4;
MatrixGroup(3, Rational Field)
Generators:
    [ 1  0 -1]
    [ 0  1 -1]
    [ 0  0 -1]

    [0 1 0]
    [1 0 0]
    [0 0 1]

    [0 0 1]
    [0 1 0]
    [1 0 0]

> Order(G4);
24

> #ReflectionsOfGroup(G4);
6

> HB(G4);
{@
    (1 1 1),
    (-1 -1  3),
    (-1  1  1),
    (0 0 1),
    (-1  0  2),
    (0 1 1)
@}

> A4 := LatticeOfGroup(G4);

> #SimpleRoots(A4, G4);
3
```

```
//----------------------------------------------------------------


> H3;
MatrixGroup(3, Rational Field)
Generators:
    [0 0 1]
    [1 0 0]
    [0 1 0]

> IsReflectionGroup(H3);
false

> H3 subset G3;
true

> ModuleGens(H3, G3);
{
    (0 0 0),
    (-1  1  0)
}


//----------------------------------------------------------------


> H4;
MatrixGroup(3, Rational Field)
Generators:
    [-1  1  0]
    [-1  0  1]
    [-1  0  0]

> IsReflectionGroup(H4);  Order(H4);
false
4
```

```
> H4 subset G4;
true

> ModuleGens(H4, G4);
{
    (1 0 1),
    (1 0 0),
    ( 2 -1  0),
    (-2  2  1),
    (-2  0 -1),
    (-3  1  0),
    (0 0 0),
    (-3  1  2),
    (-2  0  3),
    (-1  2  0),
    ( 1 -1  1),
    (-2  1  1),
    (-2  1 -1),
    (-2  1  2),
    (0 1 0)
}

> ModuleGens(H4, G4 : ShowMore);
[
    {
        (0 0 0)
    },
    {
        ( 2 -1  0),
        ( 1 -1  1),
        (1 0 1),
        (1 0 0)
    },
    {
        (-3  1  0),
        (-2  1 -1),
        (-2  0 -1)
    },
    {
        (−2  1  1),
        (−1  2  0),
        (−2  2  1)
    },
    {
        (0 1 0)
    },
    {
        (−2  1  2),
        (−3  1  2),
        (−2  0  3)
    }
]
```