Multiplicative Invariants of Root Lattices

A Dissertation
Submitted to
the Temple University Graduate Board

---

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

---

by
Jessica A. Hamm
August, 2014

Examining Committee Members:

Marin Lorenz, Advisory Chair, Mathematics
David Futer, Mathematics
Edward Letzter, Mathematics
Ellen Kirkman, Wake Forest University, Mathematics

ABSTRACT

Multiplicative Invariants of Root Lattices

Jessica A. Hamm
DOCTOR OF PHILOSOPHY

Temple University, August, 2014

Dr. Martin Lorenz, Chair

Classical invariant theory is a field of study within abstract algebra that has been around for well over a century. However, the field of *multiplicative* invariant theory is rather new, having only been studied formally for the past 35 years. Multiplicative invariants arise naturally in a variety of settings, notably as representation rings of Lie algebras, centers of group algebras, and actions on algebraic tori.

Here we start with a group G and a *G-lattice* $L \cong \mathbb{Z}^n$ on which G acts via automorphisms. We choose any (commutative) base ring $\Bbbk$ and form the group algebra $\Bbbk[L] \cong \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Our group action extends uniquely to a multiplicative action on $\Bbbk[L]$ and we wish to describe the invariants under this action as well as study nice properties of the invariant algebra.

Multiplicative actions have some strikingly different features than their linear counterpart. One nice feature of multiplicative actions is the reduction to finite groups. This fact along with a theorem of Jordan says that there are a finite number of multiplicative invariant algebras (up to $\cong$) for any rank n. It is feasible then to create a database of multiplicative invariants in low ranks. This has been done for $n = 2$ in [16]. However, the number of invariant algebras to consider grows considerably with n. For example, when $n = 4$ there are 710 multiplicative invariant algebras. Because creating such a database is quite a daunting task we have focused on calculating invariants for special lattices in the thesis.

In the thesis we calculate the invariants for lattices associated to irreducible root systems under the actions of their Weyl groups. The multiplicative invariants for an

arbitrary root lattice under its Weyl group can be written as a tensor product of invariant algebras for the irreducible root lattices. Hence, by calculating the invariants for these irreducible root lattices we have actually given a description of multiplicative invariants for an arbitrary root lattice, giving a significant contribution to the desired database and to the field of multiplicative invariant theory.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere thanks to several people. First and foremost I want to thank God for His faithfulness in bringing me to this goal. Apart from Him I can do nothing so all the glory and honor goes to Him.

I would like to give the deepest and most sincere gratitude possible to my advisor Dr. Martin Lorenz. Dr. Lorenz has been one of the best teachers I have ever had and I have learned so much from him in and out of the classroom. As an advisor he has been extremely patient and more helpful than I can describe. I am thankful that he has introduced me to so many topics in math but particularly to the field of multiplicative invariant theory. His expert teaching in the classroom along with his guidance and encouragement throughout research has been vital to my success as a graduate student and I am truly grateful.

I would also like to thank all the Temple math faculty who I have encountered in some way or another. My knowledge of mathematics has grown so much in the past five years and I owe that to the professors of the many classes I have taken as a graduate student at Temple. In particular, I would like to thank my thesis committee; Dr. Dave Futer, Dr. Ed Letzter, and Dr. Ellen Kirkman. I am so pleased that you were all able to be involved in such a big moment of my life. I would also like to thank Dr. Irina Mitrea and Dr. Maria Lorenz. Irina and Maria have both given me numerous wonderful opportunities to be involved in math outreach and the success I had on the job market is due largely to these experiences that set me apart. Maria has also taught me so much about how to be a good teacher and I appreciate everything she has done. Maria, you are a role model to me!

I would like to thank my fellow graduate students who have helped me survive these past 5 years. In particular, I would like to thank Beca for her constant encouragement (and all the flowers from Owen). I would also like to thank Brian and Christian who have worked with me on countless homework problems throughout the years. I also want to give a huge thank you to Austin Daughton. Austin not only taught me a lot of math but he also helped guide me through the process of

applying for jobs and writing a thesis. He has been an invalualable resource to me and I am so glad to have him as my friend! Thanks for your patience and humble attitude Austin.

I want to thank three people who the math department and, in particular, graduate students could not live without: Kathleen Paul, Alexis Cogan, and Sherrie King-Woods. Thank you all for everything you do each day! Your hard work does not go unnoticed and I really appreciate all the help you have given me as a graduate student.

Lastly, I would like to thank my friends and family. To my wonderful, supportive husband Arran: without you I would not be finishing this degree. Thank you for always talking about math with me. You are the most selfless person I know and I can't put into words how much all you've done means to me. You are truly my better half and I'm so excited for our future together! To my sister Smeggers: you are my very best friend! Thank you for always being thoughtful and encouraging! To my niece Paisley: you can't talk yet but all your sweet smiles make everything better. You are such a joy in my life and I can't wait to teach you math when you get older. Thanks to my dad and grandma for their endless support and love as well! Thanks to Ron Taylor and Jason Parsley for encouraging me in mathematics and believing in me when I didn't believe in myself. I also owe a huge debt of gratitude to my Beth Zion mishpocha. Beth Zion has truly become my family and I love each and everyone of you! Thanks for all your prayers and encouragement throughout these 5 years. I feel so blessed to have so many special people in my life who have helped me in this journey. Thank you so much everyone!!!

TABLE OF CONTENTS

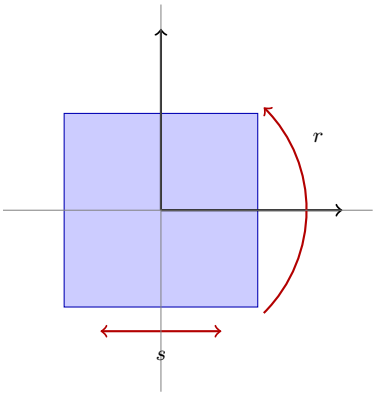
CHAPTER 1

Introduction

1.1 For the Non-Mathematician

"The theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head." –Hermann Weyl [27]

Invariant theory is a field of study within abstract algebra that has been around for well over a century. To get a feel for invariant theory let's start by discussing symmetries. Imagine that you have an object in front of you. You close your eyes and I transform the object in some way (i.e. by turning it around, flipping it over, etc.). Now when you open your eyes it appears that nothing has happened. This transformation is an example of a *symmetry*. There are several examples of symmetries that you are probably quite familiar with already. First of all, you may remember even and odd functions from high school algebra. An even function is symmetric about the y-axis, meaning if we reflect the graph of our function about the line $x = 0$, the graph stays the same.



You may also be aware of symmetries of geometric objects, such as a square. For example, we can rotate a square 90° and leave it unchanged as a geometric figure. A square also has reflectional symmetries. The collection of all 8 symmetries of a square form D_8, a mathematical object called a *group*. More generally, for any regular n-gon we may form the group of $2n$ symmetries of this object, called the *dihedral group*, D_{2n}. The collection of symmetries of a Rubik's cube form a group called the Rubik's Cube Group. Within this group, we have rotations of the faces of the Rubik's cube. Now you may be thinking that when we rotate a face of a Rubik's cube it doesn't look the same as before. This is somewhat true–the geometric object is the same but the "labels" have now been rearranged. This is where invariant theory comes into play.

Invariant theory has two major players: a *group* and an *object* on which that group acts. In our examples above, the groups were collections of symmetries and the objects the groups were acting on were the geometric figures–the graph, the square, and the Rubik's cube. If we label our geometric objects and let the symmetries "act" on them we now have a way of noticing the changes incurred by the symmetry. The elements left *invariant* under a particular symmetry are those in which the labels are left unchanged. Though symmetries are just one type of example, hopefully I have given you an idea of the flavor of group actions and invariants.

A bit more abstractly, classical invariant theory deals with polynomials and groups acting on them. For instance, consider the ring $\mathbb{Z}[x, y]$, polynomials in x and y with coefficients in $\mathbb{Z}$, and the group action described by switching x and y. Here the polynomial $x + y$ is left invariant under the group action since $x + y \mapsto y + x$. However, $x - y \mapsto y - x \neq x - y$, so this element is not invariant. It turns out that the invariants under this action can be described as a *subring* of $\mathbb{Z}[x, y]$, and in particular the invariants are given by $\mathbb{Z}[x + y, xy]$. More generally, the set of

invariants inherits a nice structure from the original object being acted on. The field of invariant theory is concerned with calculating and studying this structure. We want to find a nice way of describing our invariants and to then investigate what properties they may have.

Multiplicative invariant theory is a relatively new field within invariant theory. Here we consider actions on *Laurent* polynomial rings, for example, $\mathbb{Z}[x, x^{-1}]$. Though this is similar to the setting of above, there are many stark contrasts, some which make things easier and others that make it more difficult. Other than a few isolated results, the study of this branch of mathematics began in the 1980s in the work of Daniel Farkas, who also coined the name "multiplicative invariant theory". Being newer means there are still many things unknown which leaves a lot of exciting questions open for a brave mathematician to explore.

1.2 For the Mathematician

Invariant theory is a classical algebraic/geometric theme permeating virtually all areas of pure mathematics, some areas of applied mathematics, notably coding theory (see, e.g., [23] and the references therein), and certain parts of theoretical physics as well. In algebraic terms, the theory is concerned with study of the relationship between a ring S and its subring of invariants, $R = S^G$, under the action of a group G.

The most traditional setting of invariant theory arises from a linear action of G on an n-dimensional vector space V over a field $\Bbbk$. This action can be extended to the symmetric algebra $S(V)$; a choice of basis for V yields an explicit isomorphism $S(V) \cong \Bbbk[x_1, \ldots, x_n]$. This type of action is commonly called a *linear action*; the resulting algebra of invariants $R = S(V)^G$ is often referred to as an algebra of *polynomial invariants*. The ring theoretic properties of polynomial invariants have been thoroughly explored, especially for *finite groups* G to which we will restrict ourselves in this dissertation. Early work of Hilbert [11, 12] and of E. Noether [18, 17] established that R is an integrally closed affine domain over $\Bbbk$ and $S(V)$

is a finitely generated R-module. One of the most celebrated results on polynomial invariants is the following.

Shephard-Todd-Chevalley Theorem ([22], [6]). *Suppose that the finite group G acts linearly on the symmetric algebra $S(V)$ of the $\Bbbk$-vector space V and that the characteristic of $\Bbbk$ does not divide the order of G. Then the invariant algebra $S(V)^G$ is a polynomial algebra over $\Bbbk$ precisely if G acts as a pseudoreflection group on V.*

Here, an element $g \in G$ is called a pseudoreflection on V if the linear transformation of V that is afforded by $1-g$ has rank 1; the group G is called a pseudoreflection group on V if G can be generated by pseudoreflections on V.

As indicated in the title, this thesis will be focusing on a different branch of invariant theory known as *multiplicative invariant theory*. This theory has emerged relatively recently and has only been studied systematically during the past 30 years, beginning with the work of D. Farkas in the 80's [8, 9]. Prior to Farkas, only a few isolated results on multiplicative invariants, also known as "exponential invariants" or "monomial invariants", were known, notably in the work of Bourbaki [2] and Steinberg [24]. Multiplicative invariants arise from lattices, that is, from free abelian groups of finite rank, $L \cong \mathbb{Z}^n$. An action of a finite group G on L is given by an integral representation $G \to \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$. Any such action can be uniquely extended to a G-action on the group algebra $\Bbbk[L] \cong \Bbbk[x_1^{\pm 1}, x_2^{\pm 1}, ..., x_n^{\pm 1}]$ over any (commutative) base ring $\Bbbk$. Within the Laurent polynomial algebra $\Bbbk[x_1^{\pm 1}, x_2^{\pm 1}, ..., x_n^{\pm 1}]$, the lattice L becomes the multiplicative group of units that is generated by the "variables" x_i and their inverses; so L is the group of monomials in the Laurent polynomial algebra. The action of G stabilizes L and hence maps monomials to monomials; this explains the terms "multiplicative" or "monomial" actions. Despite some obvious formal similarities in the basic setup, multiplicative invariant theory and its linear counterpart exhibit many strikingly different features. For one, other than the theory of polynomial invariants, multiplicative invariant theory is only concerned with *finite* group actions: when studying the

invariants of a multiplicative action under an arbitrary group, one can gather all information by reducing to a suitable finite group. This tells us in particular that multiplicative invariant algebras $\Bbbk[L]^G$ are always affine $\Bbbk$-algebras. Another notable feature of multiplicative actions is the fact that the degree of Laurent polynomials is not preserved under the action. This is again in sharp contrast with the classical case of linear actions and causes a great deal of added difficulty when investigating multiplicative invariants. Finally, due to the fact that multiplicative actions arise from integral representations, the subject has a strong arithmetic component. The foregoing will be explained in more detail in Section 2.2.2.

1.2.1 My Research

As mentioned above, when dealing with multiplicative invariants one may reduce to finite groups. By a classical theorem of Jordan [15], for each given rank n, there are only finitely many finite subgroups $G \subseteq \mathrm{GL}_n(\mathbb{Z})$ up to conjugacy, and hence there are only finitely many possible multiplicative invariant algebras $\Bbbk[x_1^{\pm 1}, x_2^{\pm 1}, ..., x_n^{\pm 1}]^G$ up to isomorphism. Thus, a complete database of multiplicative invariants is possible in principle, at least for small n. However, the number of cases to consider increases rather sharply with n, and hence the envisioned database is unrealistic for now. Instead, for my thesis I have calculated the multiplicative invariants for certain especially important lattices of arbitrarily large rank, specifically the so-called *root lattices* arising in Lie theory. In this section we describe the problems worked on in the thesis and state a sample result.

Root systems and their associated Weyl groups have their origins in in the theory of semisimple Lie algebras. Without going into the details of this connection – it will not be needed for our work – let us just remark that the root system of a semisimple Lie algebra characterizes the Lie algebra up to isomorphism. In Section 2.3, we will review the basics of root systems. Each root system naturally leads to two lattices on which the Weyl group acts, the root lattice and the weight lattice. The multiplicative invariant algebras of weight lattices under the Weyl group action are known by a theorem of Bourbaki: they are always polynomial algebras [2,

Théorème VI.3.1]. Root lattices, on the other hand, generally have more complicated multiplicative invariants. However, since Weyl groups are reflection groups, it is known that the invariant algebras in question are affine normal monoid algebras [16, Theorem 6.1.1], but the structure of the monoid in question is a priori unclear.

The multiplicative invariant algebra of the root lattice $L = L(\Phi)$ of an arbitrary root system Φ is just the tensor product of the multiplicative invariant algebras of the root lattices of the irreducible components of Φ; see Section 2.3.2. Thus we may focus solely on finding the multiplicative invariants of these irreducible components. All irreducible root systems have been classified and must be one of the following types: the four classical types, A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), and D_n ($n \geq 4$) or the exceptional types, $\mathsf{E}_6, \mathsf{E}_7, \mathsf{E}_8, \mathsf{F}_4$, and G_2 [2, Théorème VI.4.3]. The invariants for root lattices of type A_n and B_n have been calculated in [16] though, in addition, we explicitly give primary invariants and some computational methods related to A_n in this thesis. For completeness, we include the earlier calculations along with our contributions, followed by the calculations for the two remaining classical types, C_n and D_n, and for the exceptional types, all of which is new. In each case, we have computed a system of fundamental invariants and have determined some interesting features of the multiplicative invariant algebra $\mathbb{Z}[L]^{\mathcal{W}}$ such as its class group and, in some cases, a presentation of the algebra.

As a sample, we state the result for the root system $\Phi = \mathsf{C}_n$. Explicitly, Φ is the following subset of Euclidean space $\mathbb{R}^n$:

$$\Phi = \{\pm 2\varepsilon_i \mid 1 \leq i \leq n\} \cup \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq n\}$$

where $\{\varepsilon_i\}_1^n$ denotes the standard basis of $\mathbb{R}^n$. The Weyl group of Φ is given by

$$\mathcal{W} = \{\pm 1\}^n \rtimes \mathcal{S}_n$$

where the subgroup $\{\pm 1\}^n$ acts diagonally on the basis $\{\varepsilon_i\}_1^n$ and $\mathcal{S}_n$ permutes this basis in the obvious way. The root lattice $L(\mathsf{C}_n)$, by definition, is just the $\mathbb{Z}$-linear span of Φ in $\mathbb{R}^n$. We shall denote this lattice by C_n; it is a sublattice of index 2 in the standard lattice $\bigoplus_{i=1}^n \mathbb{Z}\varepsilon_i = \mathbb{Z}^n \subseteq \mathbb{R}^n$. Writing x_i for the element of the group ring $\mathbb{Z}[\mathbb{Z}^n]$ that corresponds to ε_i, we let σ_k denote the k^{th} elementary symmetric

function in the variables $x_i + x_i^{-1}$ $(i = 1, \ldots, n)$:

$$\sigma_k = \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=k}} \prod_{i \in I} (x_i + x_i^{-1})$$

With these notations, we can now state our result for $\Phi = \mathsf{C}_n$.

Theorem 1.2.1. (a) ***Algebra structure:*** *$\mathbb{Z}[C_n]^{\mathcal{W}}$ is isomorphic to the monoid algebra $\mathbb{Z}[M_n]$ with*

$$M_n = \Big\{ (l_1, l_2, \ldots, l_n) \in \mathbb{Z}_+^n \mid \sum_{i=1}^{n} i l_i \equiv 0 \bmod 2 \Big\}$$

The isomorphism is given by

$$\begin{array}{ccc} \mathbb{Z}[M_n] & \xrightarrow{\sim} & \mathbb{Z}[C_n]^{\mathcal{W}} \\ \cup & & \cup \\ (l_1, l_2, \ldots, l_n) & \longmapsto & \sigma_1^{l_1} \sigma_2^{l_2} \cdots \sigma_n^{l_n} \end{array}$$

The monoid M_n decomposes as $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor} \oplus V$ with

$$V = \Big\{ (k_1, k_2, \ldots, k_{\lceil \frac{n}{2} \rceil}) \in \mathbb{Z}_+^{\lceil \frac{n}{2} \rceil} \mid \sum_i k_i \equiv 0 \bmod 2 \Big\}$$

Thus, $\mathbb{Z}[C_n]^{\mathcal{W}}$ is a polynomial algebra in $\lfloor \frac{n}{2} \rfloor$ variables over the second Veronese subring of a polynomial algebra in $\lceil \frac{n}{2} \rceil$ variables over $\mathbb{Z}$.

(b) ***Fundamental invariants:*** *The algebra $\mathbb{Z}[C_n]^{\mathcal{W}}$ is generated by the following $n + \binom{\lceil \frac{n}{2} \rceil}{2}$ invariants:*

$$\pi_i = \begin{cases} \sigma_i & \text{for } i \text{ even} \\ \sigma_i^2 & \text{for } i \text{ odd} \end{cases}$$

$$\gamma_{i,j} = \sigma_i \sigma_j \quad (1 \le i < j \le n \text{ and } i, j \text{ both odd})$$

The π_i are primary invariants and the $\gamma_{i,j}$ are secondary: $\mathbb{Z}[\pi_1, \ldots, \pi_n]$ is a polynomial algebra over $\mathbb{Z}$ and $\mathbb{Z}[C_n]^{\mathcal{W}}$ is a finite module over $\mathbb{Z}[\pi_1, \ldots, \pi_n]$.

(c) ***Hironaka decomposition:***

$$\mathbb{Z}[C_n]^{\mathcal{W}} = \bigoplus_{\substack{1 \le i_1 < j_1 < i_2 < \cdots < i_t < j_t \le n \\ \text{all odd}}} \gamma_{i_1,j_1}\gamma_{i_2,j_2}\cdots\gamma_{i_t,j_t}\,\mathbb{Z}[\pi_1,\ldots,\pi_n]$$

(Here, we allow $t = 0$, the corresponding summand being $\mathbb{Z}[\pi_1,\ldots,\pi_n]$.)

(d) ***Defining relations:*** *The $\binom{\lceil \frac{n}{2} \rceil}{2}$ relations*

$$\pi_i\pi_j = \gamma_{i,j}^2 \qquad (1 \le i < j \le n \text{ and } i,j \text{ both odd})$$

are defining relations for $\mathbb{Z}[C_n]^{\mathcal{W}}$.

In addition to the above theorem, we find similar results for the remaining classical root lattices as well as calculate the invariant algebras for the exceptional lattices. With the exceptional lattices we are able to give an algebra presentation and in all cases we calculate the class group of our resulting invariant algebra.

CHAPTER 2

Preliminaries

2.1 Overview

This chapter serves to introduce notation to be used throughout this thesis and to deploy the background material and technical tools necessary for our work in later chapters. We will start by describing the general set-up and the special features of multiplicative invariant theory in some more detail than given in the Introduction. Then we will list some important theorems regarding invariants that we will need. Finally, we will review some general definitions and facts concerning root systems, class groups and Veronese algebras.

2.2 The Basics of Multiplicative Invariant Theory

2.2.1 Set-up

We start with a *lattice* L, that is, a free abelian group of finite rank. So $L \cong \mathbb{Z}^n$ for some n. For a group G, we say that L is a *G-lattice* if G acts on L by means of a homomorphism $G \to \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$, i.e. an integral representation. In the classical setting of *polynomial invariants* one would form the symmetric algebra, $S(L)$, and let G act via linear substitution of the variables. In multiplicative invariant theory, however, we form the group algebra $\Bbbk[L]$ over a commutative base

ring $\Bbbk$ of our choice and extend our action in a particular way.

In detail, the group algebra is the free $\Bbbk$-module with L as basis and with multiplication provided by the $\Bbbk$-linear extension of addition in L. In order to distinguish the addition of L from the one in $\Bbbk[L]$, we will represent the $\Bbbk$-basis L of $\Bbbk[L]$ by the formal exponential expressions $\{\mathbf{x}^m \mid m \in L\}$. With this, addition in L becomes multiplication in $\Bbbk[L]$:

$$\mathbf{x}^0 = 1, \quad \mathbf{x}^m\mathbf{x}^{m'} = \mathbf{x}^{m+m'} \quad \text{and} \quad \mathbf{x}^{-m} = (\mathbf{x}^m)^{-1}$$

Hence $\{\mathbf{x}^m \mid m \in L\}$ is a subgroup of the (multiplicative) group of units of $\Bbbk[L]$, and

$$\Bbbk[L] = \bigoplus_{m \in L} \Bbbk\mathbf{x}^m$$

After fixing a $\mathbb{Z}$-basis for $L \cong \mathbb{Z}^n$, say $a_1, \ldots, a_n$, and writing $x_i = \mathbf{x}^{a_i}$, we can think of the group algebra as the Laurent polynomial algebra over $\Bbbk$ in n variables. Explicitly, writing a given $m \in L$ as $m = z_1a_1 + \cdots + z_na_n$ for unique $z_i \in \mathbb{Z}$, we have

$$\begin{array}{ccc} \Bbbk[L] & \xrightarrow{\sim} & \Bbbk[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \\ \cup & & \cup \\ \mathbf{x}^m & \longmapsto & x_1^{z_1} \cdots x_n^{z_n} \end{array}$$

Under the above map the image of $L \cong \{\mathbf{x}^m \mid m \in L\}$ consists of all monomials in the variables x_i and their inverses.

If L is a G-lattice, then the G-action on L extends uniquely to an action of G on $\Bbbk[L]$ by $\Bbbk$-linearity. In detail, since each element $f \in \Bbbk[L]$ can be written uniquely as a finite sum $f = \sum_{m \in L} k_m\mathbf{x}^m$, with $k_m \in \Bbbk$ almost all zero, we may define

$$g(f) \underset{\text{def}}{=} \sum_{m \in L} k_m\mathbf{x}^{g(m)}$$

for $g \in G$. This yields an action of G by $\Bbbk$-algebra automorphisms on $\Bbbk[L]$. Multiplicative invariant theory aims to calculate the subalgebra

$$\boxed{\Bbbk[L]^G = \{f \in \Bbbk[L] \mid g(f) = f \quad \forall\, g \in G\}}$$

and study its main algebraic features. The algebra $\Bbbk[L]^G$ is called the *multiplicative invariant algebra* that is associated to the G-lattice L.

Example 2.2.1. Let $L = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$ and $G = \mathcal{S}_3$, the symmetric group on $\{1, 2, 3\}$. Define the group action on L by the following matrices:

$$g = (12) \qquad \longmapsto \quad \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$h = (123) \qquad \longmapsto \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

So $g(a_1) = -a_1$, $g(a_2) = a_1 + a_2$, $h(a_1) = a_2$, and $h(a_2) = -a_1 - a_2$. Now to get a multiplicative action we form the group algebra, $\Bbbk[L] \cong \Bbbk[x_1^{\pm 1}, x_2^{\pm 1}]$ and our action becomes $g(x_1) = x_1^{-1}$, $g(x_2) = x_1x_2$, $h(x_1) = x_2$, and $h(x_2) = x_1^{-1}x_2^{-1}$. So if we let $\Bbbk = \mathbb{Z}$ and take the Laurent polynomial $f(x) = 2x_1^2 - 3x_1x_2 + x_1^{-1}x_2$ then

$$g(f) = 2x_1^{-2} - 3x_2 + x_1^2x_2$$
$$h(f) = 2x_2^2 - 3x_1^{-1} + x_1^{-1}x_2^{-2}$$

As we will see later, L is actually an example of a root lattice with its corresponding Weyl group acting. Specifically, L is the 2-dimensional root lattice associated to root system A_2, with Weyl group $\mathcal{W}(\mathsf{A}_2) = \mathcal{S}_3$.

You may notice that in the example above the multiplicative action did not preserve the degree of a particular monomial. This is true of most multiplicative actions, a feature of multiplicative invariant theory that is in stark contrast with that of polynomial invariants, which have a natural grading by "total degree in the variables". Thus, the technique of grading, which is very useful for polynomial invariants, is generally not available for multiplicative invariants. In Figure 2.1, we have visually rendered the invariant algebras that arise from the multiplicative and linear inversion actions of the cyclic group $C_2 = \langle g \mid g^2 = 1 \rangle$ in dimension 2. In more detail, C_2 acts multiplicatively on the Laurent polynomial algebra $\Bbbk[x_1^{\pm 1}, x_2^{\pm 1}]$ via $g(x_i) = x_i^{-1}$. The resulting multiplicative invariant algebra has the presentation $\Bbbk[x_1^{\pm 1}, x_2^{\pm 1}]^{C_2} \cong \Bbbk[x, y, z]/(xyz - x^2 - y^2 - z^2 + 4)$, which results in the orange

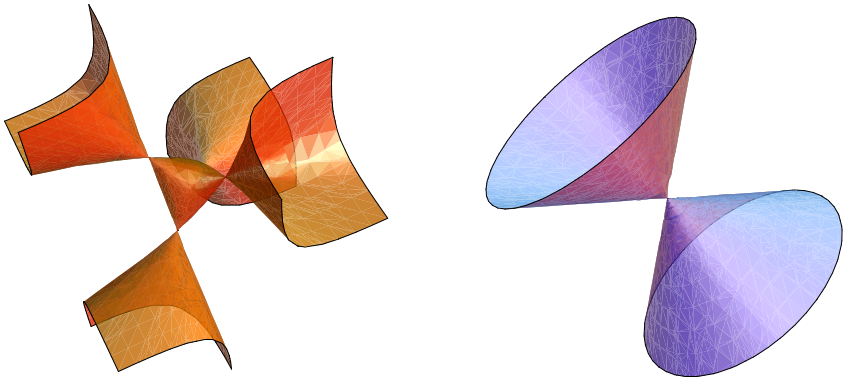


Figure 2.1: Multiplicative vs. linear inversion in rank 2

picture in Figure 2.1. By way of comparison, we have also included the picture of the polynomial invariant algebra $\Bbbk[x_1, x_2]^{C_2}$ that results form the linear inversion action $g(x_i) = -x_i$; this invariant algebra has the much simpler presentation $\Bbbk[x_1, x_2]^{C_2} \cong \Bbbk[x, y, z]/(z^2 - xy)$ resulting in the blue picture. For the detailed verification of the above presentations, we refer to [16]. Visibly, the multiplicative case is the more complicated one.

On the other hand, multiplicative invariants do have several desirable features not found in the theory of polynomial invariants. We will discuss those below.

2.2.2 Some Nice Features

Let L be a G-lattice as above. Recall that $\{\mathbf{x}^m \mid m \in L\}$ forms a $\Bbbk$-basis for the group algebra $\Bbbk[L]$ and notice that G simply permutes this basis. Thus, the multiplicative action of G on $\Bbbk[L]$ is a permutation action. This allows us to easily describe the $\Bbbk$-linear structure of the multiplicative invariant algebra $\Bbbk[L]^G$. In this section, we will describe this structure in detail, thereby revealing two very nice features of multiplicative invariants.

To start, we need some definitions. For a given $f = \sum_{m \in L} k_m \mathbf{x}^m \in \Bbbk[L]$, we define $\mathrm{Supp}(f) := \{m \in L \mid k_m \neq 0\}$; this is a finite subset of L called the

support of f. Notice that if $f \in \Bbbk[L]^G$, then the support $\mathrm{Supp}(f)$ is G-stable and, consequently, $\mathrm{Supp}(f)$ is contained in the following subset of L, which is actually easily seen to be a sublattice of L:

$$L_{\text{fin}} = \{m \in L \mid |G(m)| < \infty\} = \{m \in L \mid |G : G_m| < \infty\}$$

Here $G(m)$ denotes the G-orbit of m and G_m the stabilizer of m in G, also called the isotropy group of m. We define the *orbit sum* of m by

$$\mathsf{orb}(m) \underset{\text{def}}{=} \sum_{m' \in G(m)} \mathbf{x}^{m'} = \sum_{g \in G/G_m} \mathbf{x}^{g(m)}$$

It then follows that f must be a $\Bbbk$-linear combination of the orbit sums $\mathsf{orb}(m)$ for $m \in \mathrm{Supp}(f)$, and all these m belong to L_{fin}. Moreover, all orbit sums clearly belong to $\Bbbk[L]^G$, and different orbit sums are $\Bbbk$-linearly independent, since they have disjoint supports. This shows that the different orbits sums form a $\Bbbk$-basis of the invariant algebra $\Bbbk[L]^G$, and hence we obtain the $\Bbbk$-linear structure of $\Bbbk[L]^G$:

$$\boxed{\Bbbk[L]^G = \bigoplus_{m \in G\backslash L_{\text{fin}}} \Bbbk\, \mathsf{orb}(m)}$$

where $G\backslash L_{\text{fin}}$ denotes a transversal for the finite G-orbits in L.

Also note that each orbit sum $\mathsf{orb}(m)$ above has coefficients 0 or 1 in $\Bbbk$. Since $\Bbbk[L] = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]$ each orbit sum can actually be thought of as an orbit sum in $\mathbb{Z}[L]$. Hence, the invariant algebra $\Bbbk[L]^G$ is defined over $\mathbb{Z}$:

$$\Bbbk[L]^G = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G$$

This has some nice consequences. In particular, we may choose to replace a general coefficient ring $\Bbbk$ with $\mathbb{Z}$ and work in this more familiar (but often more difficult!) setting. Many of the features of $\mathbb{Z}[L]^G$ will naturally extend to $\Bbbk[L]^G$.

Another remarkable property of multiplicative invariants is the fact that, even though we may start with a G-lattice L for an arbitrary group G, we can quickly reduce to a suitable finite group. To see this, consider the kernel of the action of G on L,

$$\mathrm{Ker}_G(L) := \{g \in G \mid g(m) = m \quad \forall\, m \in L\} = \bigcap_{m \in L} G_m$$

Note that the lattice L_{fin} is finitely generated, being a sublattice of $L \cong \mathbb{Z}^n$. Say L_{fin} has generators $m_1, \ldots, m_r$. Since each $m_i \in L_{\text{fin}}$, we know the isotropy group G_{m_i} is a finite index subgroup of G. But $\operatorname{Ker}_G(L_{\text{fin}}) = \bigcap_{i=1}^{r} G_{m_i}$ and so it too has finite index in G. Lastly, note that $\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^G$ by our analysis of the $\Bbbk$-linear structure of $\Bbbk[L]^G$. It follows that

$$\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^{\mathcal{G}}$$

where $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$, a finite group. We summarize our observations in the following proposition.

Proposition 2.2.2. *Let L be a G-lattice for an arbitrary group G and let $\Bbbk$ be any commutative ring. Then with notation as above:*

(a) $\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^{\mathcal{G}}$

(b) $\Bbbk[L]^G = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G$

2.2.3 Some Useful Classical Theorems

Now that we have a better understanding of multiplicative actions and the resulting invariant algebras, we will list some theorems that will be useful as we proceed. As just discussed, it suffices to consider finite groups when calculating multiplicative invariants. This allows us to use the following important theorem of Jordan [15].

Theorem 2.2.3 (Jordan (1880))**.** *For each given n, the general linear group $\mathrm{GL}_n(\mathbb{Z})$ has only finitely many finite subgroups up to conjugacy.*

This implies that, for a particular n, there are only finitely many multiplicative invariant algebras $\Bbbk[L]^G$ with $\operatorname{rank} L = n$, up to isomorphism. In principle, it is conceivable, then, to create a database of all such invariant algebras. However, the number of groups, and hence the number of invariant algebras to consider, grows rather quickly with n as is illustrated in Table 2.1. It is for this reason that trying

n	# fin. $G \leq \mathrm{GL}_n(\mathbb{Z})$ (up to conj.)	# max'l G (up to conj.)
1	2	1
2	13	2
3	73	4
4	710	9
5	6079	17
6	85311	39

Table 2.1: Numbers of finite subgroups

to classify all multiplicative invariant algebras for a given rank n becomes quite a daunting task. So far, this has only been carried out for $n \leq 2$; see [16].

The reduction to finite groups and to $\mathbb{Z}$ as coefficient ring, as stated in Proposition 2.2.2, also implies that every multiplicative invariant algebra $\Bbbk[L]^G$ is an affine $\Bbbk$-algebra, that is, $\Bbbk[L]^G$ is generated by finitely many elements as a $\Bbbk$-algebra. This is a consequence of the following classical result.

Theorem 2.2.4 (Noether's Finiteness Theorem)**.** *Let R be a commutative affine $\Bbbk$-algebra, where $\Bbbk$ is any commutative ring. If $G \subseteq \mathrm{Aut}_{\Bbbk-alg}(R)$ is a finite group, then R is a finitely generated R^G module. If $\Bbbk$ is Noetherian, then R^G is an affine $\Bbbk$-algebra as well.*

To see how this implies that $\Bbbk[L]^G$ is affine over $\Bbbk$, recall that we may assume that G is finite. Thus, Noether's Finiteness Theorem implies that $\mathbb{Z}[L]^G$ is affine over $\mathbb{Z}$. Since $\Bbbk[L]^G \cong \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G$ by Proposition 2.2.2, it follows that $\Bbbk[L]^G$ is affine over $\Bbbk$ as well.

Any finite generating set of the algebra $\Bbbk[L]^G$, or any other invariant algebra R^G that is known to be affine, is called a system of *fundamental invariants*. One often distinguishes between *primary* and *secondary* invariants; these are defined as

follows.

Definition. Let R be a commutative $\Bbbk$-algebra and let G be a finite group acting by automorphisms on R such that the invariant algebra R^G is affine. Elements $f_1, \ldots, f_n \in R^G$ are called *primary invariants* if the f_i are algebraically independent and R^G is finitely generated as a module over the subalgebra $P = \Bbbk[f_1, \ldots, f_n]$, say $R^G = \sum_{i=1}^{m} g_i P$. In this case, the g_i are called *secondary invariants.*

When working over a base *field* $\Bbbk$, we always know that such invariants exist for $\Bbbk[L]^G$ by Noether's Normalization Lemma.

Theorem 2.2.5 (Noether's Normalization Lemma)**.** *Let A be an affine commutative $\Bbbk$-algebra, where $\Bbbk$ is a field. Then there exists elements $x_1, \ldots, x_n \in A$ which are algebraically independent over $\Bbbk$ and such that A is a finite module over the polynomial ring $\Bbbk[x_1, \ldots, x_n]$.*

Although we are not aware of a version of Noether's Normalization Lemma that holds for $\mathbb{Z}$ rather than a field, we will see that, for the invariant algebras considered in this thesis, we can in fact find explicit primary and secondary invariants for $\mathbb{Z}[L]^G$. Though primary invariants for $\mathbb{Z}[L]^G$ are in no way unique, the number of such invariants is determined: it is equal to the rank of the lattice L. This follows easily from Krull dimension considerations. If L is a root lattice and G is the associated Weyl group, we will see that the resulting invariant algebra $\mathbb{Z}[L]^G$ is in fact a *free* module over the subalgebra $P = \mathbb{Z}[f_1, \ldots, f_n]$ that is generated by the primary invariants – this ultimately follows from the fact that G acts as a reflection group on L in this case; see Propostion 2.3.5 below. Thus, we have a decomposition

$$\mathbb{Z}[L]^G = \bigoplus_{i=1}^{m} g_i P$$

Such a decomposition is often called a *Hironaka decomposition* in invariant theory; the operative ring theoretic property behind the existence of a Hironaka decomposition is the *Cohen-Macaulay* property, to which we will return below.

2.3 Root Systems and Weyl Groups

In this section, we will review the basic definitions and facts concerning root systems and their Weyl groups. We will define root lattices and discuss what is known about multiplicative invariants of such lattices. Our background references for root systems are Bourbaki [2] and Humphreys [13].

Let $\mathbb{E} \cong \mathbb{R}^n$ denote a Euclidean space with inner product $(\,.\,,\,.\,)$. For $v, w \in \mathbb{E}$, $w \neq 0$, put

$$\langle v, w \rangle := \frac{2(v,w)}{(w,w)}$$

The map $s_w \colon \mathbb{E} \to \mathbb{E}$ that is defined by

$$s_w(v) = v - \langle v, w \rangle w \qquad (v \in \mathbb{E})$$

is obviously linear; it sends w to $-w$; and it is the identity on the hyperplane $w^\perp = \{v \in \mathbb{E} \mid (v,w) = 0\}$. Moreover, it is straightforward to see that s_w is an orthogonal transformation, that is, s_w preserves the inner product of $\mathbb{E}$. The map s_w is called the *reflection* of $\mathbb{E}$ that is associated with w.

A subset $\Phi \subseteq \mathbb{E}$ is called a *root system* if the following conditions are satisfied:

(R1) Φ is a finite subset of $\mathbb{E} \setminus 0$ that spans the $\mathbb{R}$-vector space $\mathbb{E}$.

(R2) If $\alpha \in \Phi$, then $\mathbb{R}\alpha \cap \Phi = \{\pm\alpha\}$.

(R3) If $\alpha, \beta \in \Phi$, then $s_\alpha(\beta) \in \Phi$.

(R4) If $\alpha, \beta \in \Phi$, then $\langle \beta, \alpha \rangle \in \mathbb{Z}$.

The dimension $n = \dim_{\mathbb{R}} \mathbb{E}$ is called *rank* of Φ. The *Weyl group* of Φ is the subgroup of $\mathrm{GL}(\mathbb{E}) \cong \mathrm{GL}_n(\mathbb{R})$ that is generated by the reflections s_α with $\alpha \in \Phi$:

$$\mathcal{W} = \mathcal{W}(\Phi) := \langle s_\alpha \mid \alpha \in \Phi \rangle$$

It follows from **(R3)** that each s_α, when restricted to Φ, yields a permutation of Φ. Therefore, we have a well-defined restriction homomorphism $\mathcal{W} \to \mathcal{S}_\Phi = \{\text{permutations of } \Phi\}$. This is in fact a monomorphism of groups by **(R1)**. Therefore, $\mathcal{W}$ is always a finite reflection group. We also note that the $\mathcal{W}$-invariants $\mathbb{E}^{\mathcal{W}} = \{v \in \mathbb{E} \mid s(v) = v \; \forall s \in \mathcal{W}\}$ are trivial:

Lemma 2.3.1. $\mathbb{E}^{\mathcal{W}} = \{0\}$.

Proof. Let $v \in \mathbb{E}^{\mathcal{W}}$. Then for all $\alpha \in \Phi$, we must have $s_\alpha(v) = v$. Now,

$$s_\alpha(v) = v \iff v - \langle v, \alpha \rangle \alpha = v \iff (v, \alpha) = 0$$

This shows that $v \in \bigcap_{\alpha \in \Phi} \alpha^\perp$. Axiom **(R1)** implies that $\bigcap_{\alpha \in \Phi} \alpha^\perp = \mathbb{E}^\perp = \{0\}$ and so $v = 0$ as desired. □

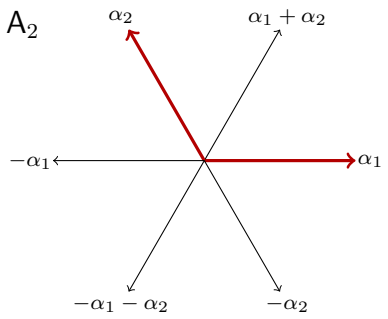
Finally, we recall the notion of a *base* of a root system Φ: this is a subset $\Delta \subseteq \Phi$ satisfying the following conditions.

(B1) Δ is an $\mathbb{R}$-basis of $\mathbb{E}$, and

(B2) Each $\beta \in \Phi$ has the form $\beta = \sum_{\alpha \in \Delta} z_\alpha \alpha$ with all $z_\alpha \in \mathbb{Z}_+$ or all $z_\alpha \in -\mathbb{Z}_+$.

For the proof that each root system does in fact have a base, we refer to the aforementioned standard references.

We conclude this subsection with the picture of the root system Φ of type A_2 in $\mathbb{E} \cong \mathbb{R}^2$. The vectors α_1 and α_2 form a base of this root system. We will discuss the root systems of type A_n $(n \geq 2)$ in more detail later in this thesis.



(2.1)

2.3.1 Lattices Associated to a Root System

Let Φ be a root system in Euclidean space $\mathbb{E} \cong \mathbb{R}^n$. The *root lattice* of Φ is defined by

$$L = L(\Phi) \underset{\text{def}}{=} \mathbb{Z}\Phi \subseteq \mathbb{E}$$

where $\mathbb{Z}\Phi = \sum_{\alpha\in\Phi} \mathbb{Z}\alpha$. If $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ is a fixed base of Φ, then

$$L = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i \cong \mathbb{Z}^n$$

So L is indeed a lattice. By axioms **(R3)** and **(R1)**, the Weyl group $\mathcal{W} = \mathcal{W}(\Phi)$ acts faithfully on L. By **(R4)**, the root lattice L is contained in the so-called *weight lattice* of Φ, which is defined by

$$\begin{aligned}\Lambda = \Lambda(\Phi) &\underset{\text{def}}{=} \{v \in \mathbb{E} \mid \langle v, \alpha\rangle \in \mathbb{Z} \text{ for all } \alpha \in \Phi\} \\ &= \{v \in \mathbb{E} \mid \langle v, \alpha\rangle \in \mathbb{Z} \text{ for all } \alpha \in \Delta\}\end{aligned}$$

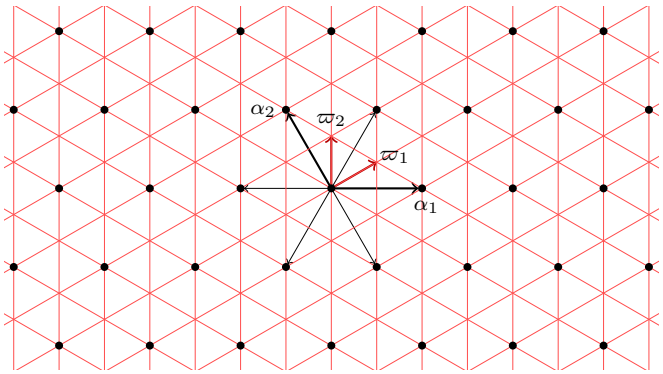
For the last equality above, see [13, p. 67]. It follows from axiom **(R3)** and the fact that $\mathcal{W}$ preserves the bracket $\langle\,.\,,\,.\,\rangle$ that $\mathcal{W}$ stabilizes Λ as well. In view of **(B1)**, the base Δ yields an $\mathbb{R}$-linear isomorphism

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\sim} & \mathbb{R}^n \\ \cup & & \cup \\ v & \longmapsto & (\langle v, \alpha_i\rangle)_1^n \end{array}$$

Under this isomorphism, $\Lambda \subseteq \mathbb{E}$ corresponds to $\mathbb{Z}^n \subseteq \mathbb{R}^n$; so Λ is also a lattice. The preimages $\varpi_i \in \Lambda$ of the standard $\mathbb{Z}$-basis vectors of $\varepsilon_i \in \mathbb{Z}^n$ are called the *fundamental weights* with respect to Δ; they form an $\mathbb{R}$-basis of $\mathbb{E}$. Thus

$$\langle \varpi_i, \alpha_j\rangle = \delta_{i,j} \qquad \text{and} \qquad \Lambda = \bigoplus_{i=1}^{n} \mathbb{Z}\varpi_i \cong \mathbb{Z}^n$$

The picture below shows the root lattice L and the weight lattice Λ for the root system Φ of type A_2 from (2.1). The root lattice L is indicated by black dots and the weight lattice Λ as the intersections of the red lines.



(2.2)

For our calculations of class groups later in this thesis, we will need the following fact from group cohomology; see [16].

Lemma 2.3.2. *With the above notation,* $H^1(\mathcal{W}, L) = \Lambda/L$.

Proof. The exact sequence of $\mathcal{W}$-modules

$$0 \longrightarrow L = L \otimes \mathbb{Z} \longrightarrow L \otimes \mathbb{Q} \longrightarrow L \otimes (\mathbb{Q}/\mathbb{Z}) \longrightarrow 0$$

gives rise to a long cohomology sequence which starts as follows:

$$0 \longrightarrow L^{\mathcal{W}} \longrightarrow (L \otimes \mathbb{Q})^{\mathcal{W}} \longrightarrow (L \otimes (\mathbb{Q}/\mathbb{Z}))^{\mathcal{W}} \longrightarrow H^1(\mathcal{W}, L) \longrightarrow H^1(\mathcal{W}, L \otimes \mathbb{Q})$$

Since $L \otimes \mathbb{Q}$ embeds into $\mathbb{E}$, Lemma 2.3.1 implies that $(L \otimes \mathbb{Q})^{\mathcal{W}} = 0$. Moreover, by a standard fact about the cohomology of finite groups over fields of characteristic 0, we also have $H^1(\mathcal{W}, L \otimes \mathbb{Q}) = 0$. Therefore, the above exact sequences yield the isomorphisms

$$H^1(\mathcal{W}, L) \cong (L \otimes (\mathbb{Q}/\mathbb{Z}))^{\mathcal{W}} \cong ((L \otimes \mathbb{Q})/L)^{\mathcal{W}}$$

It remains to show that

$$((L \otimes \mathbb{Q})/L)^{\mathcal{W}} = \Lambda/L \tag{2.3}$$

To prove this equality, recall that $L \subseteq \Lambda$ and both lattices have rank n; so Λ/L is finite. Therefore, $L \subseteq \Lambda \subseteq L \otimes \mathbb{Q} \subseteq \mathbb{E}$ and it suffices to show that $\Lambda/L = (\mathbb{E}/L)^{\mathcal{W}}$. The inclusion $\subseteq$ states that $v - s_\alpha(v) \in L$ holds for all $\alpha \in \Phi$ and $v \in \Lambda$, because the reflections s_α generate $\mathcal{W}$. But $v - s_\alpha(v) = \langle v, \alpha \rangle \alpha \in \mathbb{Z}\alpha \subseteq L$ as desired. Conversely, let $v \in \mathbb{E}$ be such that $v - s(v) \in L$ for all $s \in \mathcal{W}$. Specializing to $s = s_\alpha$ with $\alpha \in \Delta$, this says that $\langle v, \alpha \rangle \alpha \in L$, and since $L = \bigoplus_{\alpha \in \Delta} \mathbb{Z}\alpha$, we must have $\langle v, \alpha \rangle \in \mathbb{Z}$. Since $\alpha \in \Delta$ was arbitrary, it follows that $v \in \Lambda$. This proves $\supseteq$, thereby completing the proof of the lemma. □

2.3.2 Multiplicative Invariants: Reduction to Irreducible Root Systems

Let Φ be a root system and let $\mathcal{W} = \mathcal{W}(\Phi)$ be the associated Weyl group. As was mentioned earlier, the multiplicative invariant algebra $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ of the $\mathcal{W}$-action

on the weight lattice $\Lambda = \Lambda(\Phi)$ is a polynomial algebra over $\mathbb{Z}$. A convenient set of variables is provided by the orbit sums

$$\mathsf{orb}(\varpi_i) = \sum_{w \in \mathcal{W}/\mathcal{W}_{\varpi_i}} \mathbf{x}^{w(\varpi_i)}$$

of the fundamental weights ϖ_i. See [2, Théorème VI.3.1] or [16, Theorem 3.6.1] for a proof of this result. Thus, in the following, we will concentrate on the multiplicative invariant algebra $\mathbb{Z}[L]^{\mathcal{W}}$ of the root lattice $L = L(\Phi)$. Our goal in this section is to justify the claim made in the Introduction that it suffices to consider the case of an irreducible root system Φ.

A root system Φ is called *irreducible* if it is not possible to write Φ as a disjoint union $\Phi = \Phi_1 \sqcup \Phi_2$ with nonempty Φ_1 and Φ_2 that are elementwise orthogonal to each other. A general root system Φ uniquely decomposes as a disjoint union $\Phi = \bigsqcup_{i=1}^{r} \Phi_i$ of irreducible root systems Φ_i that are elementwise orthogonal to each other; these are called the irreducible components of Φ. The Weyl group $\mathcal{W} = \mathcal{W}(\Phi)$ is then the direct product of the Weyl groups $\mathcal{W}_i = \mathcal{W}(\Phi_i)$, with $\mathcal{W}_i$ acting trivially on all Φ_j with $j \neq i$. See [2, Section VI.1.2] for all this. It follows that $L = \bigoplus_{i=1}^{r} L_i$ with $L_i = L(\Phi_i) = \mathbb{Z}\Phi_i$ and so $\mathbb{Z}[L] \cong \mathbb{Z}[L_1] \otimes_{\mathbb{Z}} \mathbb{Z}[L_2] \otimes \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[L_r]$. This description of $\mathbb{Z}[L]$ and the above description of $\mathcal{W}$ easily imply that

$$\mathbb{Z}[L]^{\mathcal{W}} \cong \mathbb{Z}[L_1]^{\mathcal{W}_1} \otimes_{\mathbb{Z}} \mathbb{Z}[L_2]^{\mathcal{W}_2} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[L_r]^{\mathcal{W}_r}$$

Therefore, it suffices to describe the factors $\mathbb{Z}[L_i]^{\mathcal{W}_i}$, and so we may assume that Φ is irreducible.

2.3.3 Multiplicative Invariants: Monoid Algebra Structure

Again, let Φ be a root system and let $\mathcal{W} = \mathcal{W}(\Phi)$ be the associated Weyl group. As was remarked in the previous section, the multiplicative invariant algebra $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ of the weight lattice $\Lambda = \Lambda(\Phi)$ is a polynomial algebra over $\mathbb{Z}$, with the orbit sums $\mathsf{orb}(\varpi_i) = \sum_{w \in \mathcal{W}/\mathcal{W}_{\varpi_i}} \mathbf{x}^{w(\varpi_i)}$ of the fundamental weights ϖ_i acting as variables. Thus, putting

$$\Lambda_+ = \bigoplus_{i=1}^{n} \mathbb{Z}_+ \varpi_i \cong \mathbb{Z}_+^n$$

we can view $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ as the algebra of the monoid Λ_+:

$$\mathbb{Z}[\Lambda]^{\mathcal{W}} = \mathbb{Z}[\mathsf{orb}(\varpi_1), \ldots, \mathsf{orb}(\varpi_n)] \cong \mathbb{Z}[\Lambda_+] \tag{2.4}$$

The multiplicative invariant algebra $\mathbb{Z}[L]^{\mathcal{W}}$ of the root lattice $L = L(\Phi)$ is generally not quite as simple, but $\mathbb{Z}[L]^{\mathcal{W}}$ is at least still a monoid algebra. Specifically, recall that $L \subseteq \Lambda$; so we may consider the submonoid $L \cap \Lambda_+$ of L. The following result is a special case of [16, Proposition 6.2.1].

Theorem 2.3.3. *Let $L = L(\Phi)$ be the root lattice of a root system Φ and let $\mathcal{W} = \mathcal{W}(\Phi)$ be its Weyl group. The invariant algebra $\mathbb{Z}[L]^{\mathcal{W}}$ is isomorphic to the monoid algebra of $L \cap \Lambda_+$. On the basis $L \cap \Lambda_+$ of the monoid algebra $\mathbb{Z}[L \cap \Lambda_+]$, the isomorphism is explicitly given by*

$$\begin{array}{ccc} \Omega\colon \mathbb{Z}[L \cap \Lambda_+] & \xrightarrow{\sim} & \mathbb{Z}[L]^{\mathcal{W}} \\ \cup & & \cup \\ \displaystyle\sum_{i=1}^{n} z_i \varpi_i & \longmapsto & \displaystyle\prod_{i=1}^{n} \mathsf{orb}(\varpi_i)^{z_i} \end{array}$$

Proof. Let $\widehat{M}$ be the submonoid of $(\mathbb{Z}[\Lambda]^{\mathcal{W}} \setminus \{0\}, \cdot\,)$ that is generated by the orbit sums $\mathsf{orb}(\varpi_i)$ and put $M = \widehat{M} \cap \mathbb{Z}[L]$; this is a submonoid of $(\mathbb{Z}[L]^{\mathcal{W}} \setminus \{0\}, \cdot\,)$ whose elements are $\mathbb{Z}$-independent, because the elements of $\widehat{M}$ are so by (2.4). Our goal is to show that the monoid M generates $\mathbb{Z}[L]^{\mathcal{W}}$ as a $\mathbb{Z}$-module and that $M \cong L \cap \Lambda_+$.

We begin with a preliminary observation. Each $\mu \in \widehat{M}$ has the form $\mu = \prod_{i=1}^{n} \mathsf{orb}(\varpi_i)^{z_i}$ with unique $z_i \in \mathbb{Z}_+$, and hence μ corresponds to a unique $\ell = \sum_{i=1}^{n} z_i \varpi_i \in \Lambda_+$. We will write $\mu = \mu(\ell)$ and view $\mu(\ell)$ as a (nonzero) element of the group algebra $\mathbb{Z}[\Lambda]$. Each $f \in \mathbb{Z}[\Lambda]$ can be uniquely written as $f = \sum_{\lambda \in \Lambda} f_\lambda \lambda$ with all $f_\lambda \in \mathbb{Z}$ and $\operatorname{Supp} f := \{\lambda \in \Lambda \mid f_\lambda \neq 0\}$ a finite subset of Λ. Observe that $\operatorname{Supp}(f f') \subseteq \{\lambda + \lambda' \mid \lambda \in \operatorname{Supp} f, \lambda' \in \operatorname{Supp} f'\}$ clearly holds for any two $f, f' \in \mathbb{Z}[\Lambda]$. Since $\operatorname{Supp} \mathsf{orb}(\varpi_i) = \mathcal{W}(\varpi_i) = \{w(\varpi_i) \mid w \in \mathcal{W}\}$ for all i, we obtain

$$\varnothing \neq \operatorname{Supp}(\mu(\ell)) \subseteq \left\{ \sum_{i=1}^{n} \sum_{j=1}^{z_i} w_{i,j}(\varpi_i) \mid w_{i,j} \in \mathcal{W} \right\}$$

(In fact, since each $\mathsf{orb}(\varpi_i)$ involves only non-negative $\mathbb{Z}$-coefficients, namely 0 or 1, it is easy to see that the $\subseteq$ above is an equality, but this will not be essential here.) Recall that Λ/L is $\mathcal{W}$-trivial by (2.3). Therefore, each $\sum_{i=1}^{n}\sum_{j=1}^{z_i} w_{i,j}(\varpi_i)$ is congruent to $\ell = \sum_{i=1}^{n} z_i\varpi_i$ modulo L. Therefore, if $\mathrm{Supp}(\mu(\ell)) \cap L$ is nonempty, then we must have $\ell \in L$, and this in turn implies that $\mathrm{Supp}(\mu(\ell)) \subseteq L$, that is, $\mu(\ell) \in \mathbb{Z}[L]$. Since $\mu(\ell) \in \mathbb{Z}[L]$ trivially implies that $\mathrm{Supp}(\mu(\ell)) \cap L$ is nonempty, we obtain the following equivalences:

$$\mu(\ell) \in \mathbb{Z}[L] \iff \mathrm{Supp}(\mu(\ell)) \cap L \neq \varnothing \iff \ell \in L \tag{2.5}$$

Let $f \in \mathbb{Z}[L]^{\mathcal{W}}$ be given. Then $f \in \mathbb{Z}[\Lambda]^{\mathcal{W}} = \mathbb{Z}[\widehat{M}]$ by (2.4); so $f = \sum_{\mu\in\widehat{M}} z_\mu\mu$ with unique $z_\mu \in \mathbb{Z}$. Let $n(f)$ denote the number of μ with nonzero coefficient z_μ in this expression. We show by induction on $n(f)$ that $f \in \mathbb{Z}[M]$. The case $n(f) = 0$ (i.e., $f = 0$) being obvious, assume that $f \neq 0$. Since $f = \sum_{\mu\in\widehat{M}} z_\mu\mu \in \mathbb{Z}[L]$, some $\mu \in \widehat{M}$ with $z_\mu \neq 0$ must satisfy $\mathrm{Supp}(\mu) \cap L \neq \varnothing$. By (2.5), we conclude that $\mu \in \mathbb{Z}[L] \cap \widehat{M} = M$. Thus, $f' = f - z_\mu\mu$ belongs to $\mathbb{Z}[L]^{\mathcal{W}}$ and satisfies $n(f') = n(f) - 1$. By induction, $f' \in \mathbb{Z}[M]$, and so $f \in \mathbb{Z}[M]$ as well. This proves the desired equality $\mathbb{Z}[L]^{\mathcal{W}} = \mathbb{Z}[M]$. Finally, the equivalences in (2.5) also show that the (multiplicative) monoid M is isomorphic to the (additive) monoid $L \cap \Lambda_+$ via $\ell \mapsto \mu(\ell)$. This completes the proof of the theorem. □

It remains to describe the structure of the monoid $L \cap \Lambda_+$ for a given irreducible root system Φ, that is, we need to describe the set of all $\sum_{i=1}^{n} z_i\varpi_i \in \Lambda_+$ that do belong to L. A method for determining a system of fundamental invariants and a Hironaka decomposition of the invariant algebra $\mathbb{Z}[L]^{\mathcal{W}} \cong \mathbb{Z}[L \cap \Lambda_+]$ will be described in Section 2.3.4 below.

2.3.4 Hilbert Bases of Monoids

We first recall some general facts about commutative monoids. Throughout, M denotes a commutative monoid, with binary operation written as $+$. One says that M is *cancellative* if

$$a + c = b + c \quad \Longrightarrow \quad a = b \qquad (a, b, c, \in M)$$

and *torsion-free* if

$$na = nb \quad \Longrightarrow \quad a = b \qquad (a, b \in M\,, n \in \mathbb{Z}_{>0})$$

It is well-known and not hard to see that commutative monoids M that are cancellative and torsion-free are exactly the monoids that are isomorphic to submonoids of torsion-free abelian groups. If M is also finitely generated then this abelian group can be chosen finitely generated as well, and so M embeds into a lattice, L. Finitely generated commutative monoids that are cancellative and torsion-free are often simply referred to as *affine monoids*, and we will do so as well in the following. An affine monoid M is called *positive* if M has no units (that is, invertible elements) other than 0. In this case, an element $0 \neq m \in M$ is called *indecomposable* if $m = a + b$ $(a, b \in M)$ implies $a = 0$ or $b = 0$. For more on affine monoids, we refer to Bruns and Herzog [5, 6.1].

For future use, we note the following lemma which shows that every positive affine monoid M has a unique smallest generating set; this is called the *Hilbert basis* of M.

Lemma 2.3.4. *Let M be a positive affine monoid. Then M has finitely many indecomposable elements, say $m_1, \ldots, m_s$. The m_i generate M, and every generating set for M contains the m_i.*

Proof. 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. For this, we use the fact that there is a monoid homomorphism $\varphi : M \to \mathbb{Z}_+$ satisfying $\varphi(m) > 0$ for all $0 \neq m \in M$; see, e.g., Swan [26, Theorem 4.5]. Now consider an element $0 \neq m \in M$. If m is not indecomposable, then write $m = a + b$ with $0 \neq a, b \in M$. Then $\varphi(a), \varphi(b) < \varphi(m)$. By induction we know that a and b can be written as sums of indecomposable elements of M, and hence so can m. □

Hilbert bases of monoids are important in many contexts besides invariant theory, e.g., in the study of toric varieties [25, Chapter 13] and in integer programming

[21]. Therefore, the algorithmic aspects of Hilbert bases have been thoroughly explored and many computer algebra systems contain routines that compute Hilbert bases. Later in this thesis, we will use the (freely available) algebra system CoCoA to calculate the Hilbert basis for a particular monoid that arises as in Theorem 2.3.3 from the root lattice of the irreducible root system of type A_n.

Now let us focus more specifically on the monoid

$$M = L \cap \Lambda_+$$

that was considered in Theorem 2.3.3. This monoid is positive affine: M is cancellative and torsion-free, because M is a submonoid of the lattice Λ; positivity follows from the fact that $M \subseteq \Lambda_+$; and finite generation is clear from Noether's Theorem, which yields that $\mathbb{Z}[L]^{\mathcal{W}} \cong \mathbb{Z}[M]$ is an affine algebra. Alternatively, a finite Hilbert basis for $M = L \cap \Lambda_+$ can be constructed by the following procedure from [16, 6.3.5], which is based on the usual proof of Gordan's Lemma; see, e.g., [5, 6.1.2].

Consider the weight lattice $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}\varpi_i$ as before. Since Λ/L is finite, we may define $z_i \in \mathbb{Z}_{>0}$ to be the order of ϖ_i modulo L and write

$$m_i = z_i\varpi_i \in L \qquad (i = 1, \ldots, n) \tag{2.6}$$

Since the ϖ_i form an $\mathbb{R}$-basis of Euclidean space $\mathbb{E}$, we have $\mathbb{E} = \bigoplus_{i=1}^n \mathbb{R}m_i$ and $L \cap \bigoplus_{i=1}^n \mathbb{R}_+m_i = L \cap \bigoplus_{i=1}^n \mathbb{R}_+\varpi_i = L \cap \Lambda_+ = M$. Put

$$K = \Big\{\sum_{i=1}^n t_i m_i \in \mathbb{E} \mid 0 \le t_i \le 1\Big\} \supset K^\circ = \Big\{\sum_{i=1}^n r_i m_i \in \mathbb{E} \mid 0 \le r_i < 1\Big\}.$$

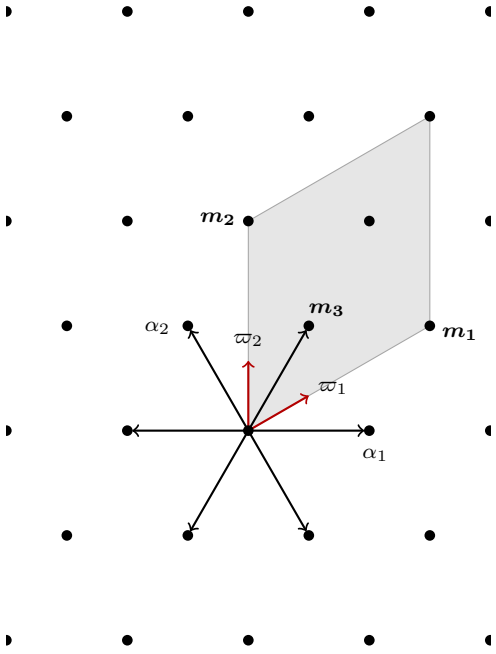
Then $K \cap L \subseteq M$ and $K \cap L$ is finite, being the intersection of a compact and a discrete subset of $\mathbb{E}$. We claim that $K \cap L$ generates the monoid M. To see this, note that each $m \in \bigoplus_{i=1}^n \mathbb{R}_+m_i$ can be uniquely written as

$$m = m' + m'' \tag{2.7}$$

with $m' \in \bigoplus_{i=1}^n \mathbb{Z}_+m_i \subseteq L$ and $m'' \in K^\circ$. If $m \in M$, then the summand m'' belongs to $K^\circ \cap L$. Since $m_1, \ldots, m_n$ also belong to $K \cap L$, equation (2.7)

exhibits m as an element of the monoid generated by $K \cap L$, which proves our claim. Note that $m_1, \ldots, m_n$ are indecomposable elements of $M = L \cap \Lambda_+$. The preceding argument shows that all other indecomposable elements of M belong to $K^\circ \cap L$. Denoting these additional indecomposables of M (if any) by $m_{n+1}, \ldots, m_s$ we obtain the desired Hilbert basis $\{m_1, \ldots, m_s\}$ for $M = L \cap \Lambda_+$.

As an illustration, we depict the situation for the root system of type A_2 again. Here, we have $m_1 = 3\varpi_1$, $m_2 = 3\varpi_2$ and $m_3 = \varpi_1 + \varpi_2 = \alpha_1 + \alpha_2$. The gray region is the zonotope K.



(2.8)

For the record, let us summarize the foregoing in a proposition.

Proposition 2.3.5. *Assume the notation of Theorem 2.3.3.*

(a) *The Hilbert basis of the monoid $M = L \cap \Lambda_+$ is given by the elements m_i $(i = 1, \ldots, n)$ defined in* (2.6) *together with the indecomposable elements of M that belong to the finite subset $K^\circ \cap L$ of M.*

(b) *The monoid M decomposes as $M = \bigsqcup_{m \in K^\circ \cap L} m + M_0$ with $M_0 = \bigoplus_{i=1}^n \mathbb{Z}_+ m_i$.*

(c) *Primary invariants for the invariant algebra $\mathbb{Z}[L]^{\mathcal{W}}$ are given by the elements*

$$\mu_i \underset{\text{def}}{=} \Omega(m_i) = \mathsf{orb}(\varpi_i)^{z_i} \qquad (i = 1, \ldots, n)$$

where z_i is the order of ϖ_i modulo L. A Hironaka decomposition of $\mathbb{Z}[L]^{\mathcal{W}}$ is given by

$$\mathbb{Z}[L]^{\mathcal{W}} = \bigoplus_{m \in K^\circ \cap L} \Omega(m)\mathbb{Z}[\mu_1, \ldots, \mu_n]$$

Proof. Part (a) was stated above, part (b) is immediate from (2.7), and (c) in turn is clear from (b) and Theorem 2.3.3. □

2.4 Class Groups

As mentioned before, in addition to finding generators of multiplicative invariant algebras, we also seek to describe some characteristics of these algebras. One important feature is the class group. In brief, the class group $\mathrm{Cl}(R)$ can be defined for an arbitrary Krull domain R, and it measures the "unique factorization defect" of R: the class group $\mathrm{Cl}(R)$ is trivial precisely if R is a UFD. For the detailed definition of Krull domains and class groups, which are both rather technical, we refer to Fossum [10] or Bourbaki [3]. For our purposes, it will suffice to remark that, for commutative noetherian domains, being a Krull domain is the same as being integrally closed. This includes all multiplicative invariant algebras $\Bbbk[L]^G$ over any commutative noetherian domain $\Bbbk$.

For polynomial invariant algebras $S(V)^{\mathcal{G}}$, where V is a vector space over a field $\Bbbk$ and $\mathcal{G}$ is a finite group acting linearly on V, the class group is known by [1, Theorem 3.9.2]:

$$\mathrm{Cl}(S(V)^{\mathcal{G}}) = \mathrm{Hom}(\mathcal{G}/\mathcal{R}, \Bbbk^\times) \tag{2.9}$$

where $\mathcal{R}$ denotes the (normal) subgroup of $\mathcal{G}$ that is generated by the elements that act as pseudoreflections on V.

The class group of multiplicative invariants has a more complicated structure; it has been determined, for arbitrary multiplicative invariant algebras, in [16, Theorem 4.1.1]. In this section, we will describe the class group in the special case of a Weyl group acting on a root lattice.

In order to state the result, we briefly recall some general facts about reflections on arbitrary lattices $L \cong \mathbb{Z}^n$. An automorphism $s \in \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$ is called a

reflection if the endomorphism $1 - s \in \mathrm{End}(L) \cong \mathrm{Mat}_n(\mathbb{Z})$ has rank 1. It is not hard to show that, in this case, s must be conjugate in $\mathrm{GL}(L)$ to exactly one of the following two matrices:

$$\begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$$

In the former case, s is called a *diagonalizable reflection*; this case is characterized by the isomorphism $H^1(\langle s \rangle, L) \cong \mathbb{Z}/2\mathbb{Z}$, while in the non-diagonalizable case, we have $H^1(\langle s \rangle, L) = 0$. See [16, Section 1.7.1] for details on the foregoing as well as for a proof of the next lemma.

Lemma 2.4.1. *Let $\mathcal{G}$ be a finite subgroup of $\mathrm{GL}(L)$ for some lattice L and let $\mathcal{D}$ denote the subgroup of $\mathcal{G}$ that is generated by the diagonalizable reflections in $\mathcal{G}$. Then $\mathcal{D}$ is a normal subgroup of $\mathcal{G}$ that is an elementary abelian 2-group of rank r, where r is the number of diagonalizable reflections in $\mathcal{G}$.*

With this, we have the following description of the class group of the multiplicative invariant algebra of a root lattice.

Theorem 2.4.2. *Let $L = L(\Phi)$ be the root lattice of a root system Φ, let $\mathcal{W} = \mathcal{W}(\Phi)$ be its Weyl group, and let $\mathcal{D}$ denote the subgroup of $\mathcal{W}$ that is generated by the diagonalizable reflections. Then:*

(a) $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{W}}) \cong H^1(\mathcal{W}/\mathcal{D}, L^{\mathcal{D}})$. *In particular, if $\mathcal{D} = \{1\}$ then $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{W}}) \cong \Lambda/L$, where Λ is the weight lattice of Φ.*

(b) *If Φ is irreducible and $\mathcal{D} \neq \{1\}$ then $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{W}}) = 0$.*

Proof. The first isomorphism in (a) is just a special case of [16, Theorem 4.1.1]. Now Lemma 2.3.2 gives $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{W}}) \cong H^1(\mathcal{W}, L) \cong \Lambda/L$ if $\mathcal{D} = \{1\}$.

For (b), note that $\mathcal{D} \neq \{1\}$ implies $L^{\mathcal{D}} \subsetneq L$ by **(R1)**. If the root system Φ is irreducible then this forces $L^{\mathcal{D}} = 0$, because the $\mathbb{Q}[\mathcal{W}]$-module $L \otimes \mathbb{Q}$ is irreducible; see [2, Corollaire to Prop. VI.1.5]. Thus, (a) gives $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{W}}) = 0$ in this case. $\square$

2.5 Veronese Algebras

In this section, we collect some ring theoretic facts on Veronese algebras. Much of this material is well-known or "folklore", at least for algebras over a field. However, I am not aware of a reference for parts (c) and (d) of Proposition 2.5.1 below. Moreover, since we are working over the integers $\mathbb{Z}$ in this thesis, we include proofs for an arbitrary commutative base ring $\Bbbk$.

Let $R = R^0 \oplus R^1 \oplus R^2 \oplus \dots$ be an arbitrary graded $\Bbbk$-algebra (not necessarily commutative). Thus, all R^i are $\Bbbk$-submodules of R, called the *homogeneous components* of R, and $R^i R^j \subseteq R^{i+j}$ holds for all i and j. In particular, R^0 is a $\Bbbk$-subalgebra of R. Elements of R^i are said to be of *degree* i. We will mostly be interested in the case where the algebra R is generated by R^1 and satisfies $R^0 = \Bbbk$. In this case, we will say that R is 1-*generated*, for short. Let $\mathsf{T}(R^1)$ denote the tensor algebra of the $\Bbbk$-module R^1; this is a graded $\Bbbk$-algebra with i^{th} homogeneous component

$$(R^1)^{\otimes i} = \underbrace{R^1 \otimes R^1 \otimes \cdots \otimes R^1}_{i \text{ factors}}$$

where $\otimes = \otimes_{\Bbbk}$ and $(R^1)^{\otimes 0} = \Bbbk$. The algebra R is 1-generated iff the canonical map $\mathsf{T}(R^1) \to R$, given by the embedding $R^1 \hookrightarrow R$ and the universal property of the tensor algebra, is surjective. We let I_R denote the kernel of this map. The ideal I_R is called the *relation ideal* and any collection generators of I_R is called a *set of defining relations* for the algebra R. Thus, we have an exact sequence

$$0 \longrightarrow I_R \longrightarrow \mathsf{T}(R^1) \longrightarrow R \longrightarrow 0$$

Since the epimorphism $\mathsf{T}(R^1) \twoheadrightarrow R$ maps $(R^1)^{\otimes i}$ to R^i, we have $I_R = \bigoplus_{i \geq 0} I_R^i$ with $I_R^i = I_R \cap R^i$. Thus, we may always choose *homogeneous* defining relations for R. Thus, the above short exact sequence amounts to short exact sequences

$$0 \longrightarrow I_R^i \longrightarrow (R^1)^{\otimes i} \longrightarrow R^i \longrightarrow 0 \tag{2.10}$$

for each $i \geq 0$. It is easy to see that R has no defining relations of degree i if and only if the following map, given by multiplication, is surjective:

$$(R^1 \otimes I_R^{i-1}) \oplus (I_R^{i-1} \otimes R^1) \longrightarrow I_R^i \tag{2.11}$$

For a given positive integer c, the c^{th} *Veronese subalgebra* of R is defined by

$$R^{(c)} = \bigoplus_{i \geq 0} R^{ci}$$

We will view the Veronese subalgebra $R^{(c)}$ as a graded algebra in its own right, with i^{th} homogeneous component

$$(R^{(c)})^i = R^{ci}$$

Proposition 2.5.1. *Let $R = \bigoplus_{i \geq 0} R^i$ be a graded $\Bbbk$-algebra, where $\Bbbk$ is some commutative ring, and let $R^{(c)} = \bigoplus_{i \geq 0} R^{ci}$ be the the c^{th} Veronese subalgebra of R. Then:*

(a) *If R is 1-generated, then $R^{(c)}$ is also 1-generated.*

(b) *Let R be 1-generated. If R has no defining relations of degree $> (i-1)c+1$, then $R^{(c)}$ has no defining relations of degree $> i$.*

(c) *If R is a (commutative) Cohen-Macaulay ring, then so is $R^{(c)}$.*

(d) *If R is a (commutative) Krull domain, then so is $R^{(c)}$. The embedding $R^{(c)} \hookrightarrow R$ gives rise to a homomorphism of class groups $\mathrm{Cl}(R^{(c)}) \to \mathrm{Cl}(R)$.*

Proof. Our proofs of (a) and (b) closely follow [19, Section 3.2]. Throughout, let us put $S = R^{(c)}$ for brevity.

(a) If R is generated by R^1, then all multiplication maps $(R^1)^{\otimes i} \to R^i$ are surjective. It follows that $R^i R^j = R^{i+j}$ holds for all i and j, not just $\subseteq$. We further conclude that multiplication maps

$$(S^1)^{\otimes i} = (R^c)^{\otimes i} = \underbrace{R^c \otimes_{\Bbbk} R^c \otimes_{\Bbbk} \cdots \otimes_{\Bbbk} R^c}_{i \text{ factors}} \to R^{ci} = S^i$$

are surjective, which proves (a).

(b) In view of (2.11) we need to show that

$$(S^1 \otimes I_S^{j-1}) \oplus (I_S^{j-1} \otimes S^1) \longrightarrow I_S^j \quad \text{is onto for } j > i \tag{2.12}$$

Since the multiplication map $(R^1)^{\otimes c} \longrightarrow S^1 = R^c$ is onto, (2.10) yields the following commutative diagrams with exact rows, for each $j \geq 0$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_R^{cj} & \longrightarrow & (R^1)^{\otimes cj} & \longrightarrow & R^{cj} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & I_S^{j} & \longrightarrow & (S^1)^{\otimes j} & \longrightarrow & S^{j} & \longrightarrow & 0 \end{array}$$

Therefore, in order to prove (2.12), it is enough to show that

$$\left((R^1)^{\otimes c} \otimes I_R^{c(j-1)}\right) \oplus \left(I_R^{c(j-1)} \otimes (R^1)^{\otimes c}\right) \longrightarrow I_R^{cj} \quad \text{is onto for } j > i \qquad (2.13)$$

By our hypothesis on R and (2.11), we know that $(R^1 \otimes I_R^{k-1}) \oplus (I_R^{k-1} \otimes R^1) \longrightarrow I_R^k$ is onto if $k-1 > c(i-1)$. It follows that, for all positive integers t with $k - t > c(i-1)$, the map $\bigoplus_{l=0}^{t} \left((R^1)^{\otimes l} \otimes I_R^{k-t} \otimes (R^1)^{\otimes (t-l)}\right) \longrightarrow I_R^k$ is onto. Now assume that $j > i$ and let $k = cj$ and $t = 2c-1$. Then $k - t = c(j-2) + 1 \geq c(i-1) + 1$ and so the foregoing yields surjectivity of the map

$$\bigoplus_{l=0}^{2c-1} \left((R^1)^{\otimes l} \otimes I_R^{c(j-2)+1} \otimes (R^1)^{\otimes (2c-1-l)}\right) \longrightarrow I_R^{cj}$$

Finally, the above map factors through the map in (2.13), and hence the latter map is surjective as well, which was to be shown.

(c) From now on, we assume that R is commutative. Clearly, R is integral over $S = R^{(c)}$. Also, the projection of $R \twoheadrightarrow S$ with kernel $\bigoplus_{c \nmid i} R^i$ is a "Reynolds operator", that is, the map is S-linear and the restriction to S is equal to the identity on S. Therefore, by a result of Hochster and Eagon [5, Theorem 6.4.5], the Cohen-Macaulay property descends from R to S.

(d) Assume that R is a Krull domain and let K denote the field of fractions of R. Moreover, let F denote the field of fractions of $S = R^{(c)}$; so $F \subseteq K$. In order to show that S is a Krull domain, it suffices to prove that $S = R \cap F$; see [10, Proposition 1.2]. The inclusion $\subseteq$ being clear, consider an element $0 \neq a \in R \cap F$. Then there is a nonzero $b \in S$ such that $ab \in S$. We need to show that this forces $a \in S$. Suppose otherwise. Then we may assume that $a = a_s +$ (components of higher degree) with $0 \neq a_s \in R^s$ and $c \nmid d$. Similarly, write $b = b_{ct} +$ (components of higher degree) with $0 \neq b_{ct} \in R^{ct}$. Then $ab = a_s b_{ct} +$

(components of higher degree) with $0 \neq a_s b_{ct} \in R^{s+ct}$, contradicting the fact that $ab \in S$. This shows that S is a Krull domain. As for class groups, we have already pointed out in the proof of (c) that R is integral over S. The homomorphism $\mathrm{Cl}(S) \to \mathrm{Cl}(R)$ now follows from [10, Proposition 6.4(b)]. □

It follows from part (b) above that if R is 1-generated with no defining relations of degree $> c+1$, then $R^{(c)}$ has no defining relations of degree > 2.

Corollary 2.5.2. *Let $R = \Bbbk[t_1, t_2, \ldots, t_d]$ denote the (commutative) polynomial algebra in $d \geq 2$ commuting variables over the commutative ring $\Bbbk$ and let $S = R^{(2)}$ denote the second Veronese subring of R. Then:*

(a) *S has algebra generators $x_i = t_i^2$ with $1 \leq i \leq d$ and $x_{i,j} = t_i t_j$ with $1 \leq i < j \leq d$.*

(b) *Defining relations for S are given by $[x_i, x_j] = [x_i, x_{k,l}] = [x_{k,l}, x_{r,s}] = 0$ and $x_j x_j = x_{i,j}^2$.*

(c) *If $\Bbbk$ is Cohen-Macaulay, then so is S. Indeed, we have the decomposition*

$$S = \bigoplus_{1 \leq i_1 < j_1 < i_2 < \cdots < i_r < j_r \leq d} x_{i_1,j_1} x_{i_2,j_2} \ldots x_{i_r,j_r} \, \Bbbk[x_1, x_2, \ldots, x_d]$$

where we allow $r = 0$, the corresponding summand being $\Bbbk[x_1, x_2, \ldots, x_d]$.

(d) *If $\Bbbk$ is a Krull domain, then so is S. If $\Bbbk$ has characteristic $\neq 2$, then $\mathrm{Cl}(S) \cong \mathrm{Cl}(\Bbbk) \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. All parts follow more or less directly from the corresponding parts of Proposition 2.5.1.

For (a), note that the elements x_i and $x_{i,j}$ generate the $\Bbbk$-module $R^2 = S^1$, and hence they form algebra generators of S.

For (b), use the fact that $[t_i, t_j] = 0$ for $i < j$ are defining relations for R, of degree 2. In view of the remark just before the statement of the corollary, S has no defining relations of degree > 2. It is easy to see that the indicated relations are exactly the relations among the x_i and $x_{i,j}$ of degree ≤ 2.

For (c), recall that the polynomial algebra R is Cohen-Macaulay if (and only if) the base ring $\Bbbk$ is Cohen-Macaulay. Therefore, S is Cohen-Macaulay as well by Proposition 2.5.1(c). For the indicated Hironaka decomposition, note that the generators in (a) and the relations in (b) immediately imply that

$$S = \sum_{1 \leq i_1 < j_1 < i_2 < \cdots < i_r < j_r \leq d} x_{i_1,j_1} x_{i_2,j_2} \ldots x_{i_r,j_r} \, \Bbbk[x_1, x_2, \ldots, x_d]$$

Since the variables t_i are algebraically independent, this sum is direct.

Finally, for (d), assume that $\Bbbk$ is a Krull domain. Then the polynomial algebra $R = \Bbbk[t_1, t_2, \ldots, t_d]$ is a Krull domain as well by [10, Proposition 1.6], and hence so is S by Proposition 2.5.1(d).

As for the structure of the class group, we use the fact that S is free over $\Bbbk$; in fact all homogeneous components R^i of the polynomial algebra $R = \Bbbk[t_1, t_2, \ldots, t_d]$ are free over $\Bbbk$. Therefore, the embedding $\Bbbk \hookrightarrow S$ gives rise to a map $\mathrm{Cl}(\Bbbk) \to \mathrm{Cl}(S)$ by [10, Proposition 6.4(a)]. By Proposition 2.5.1(d) we also have a map $\mathrm{Cl}(S) \to \mathrm{Cl}(R)$ coming from the inclusion $S \hookrightarrow R$. The composite map $\mathrm{Cl}(\Bbbk) \to \mathrm{Cl}(S) \to \mathrm{Cl}(R)$ is an isomorphism $\mathrm{Cl}(\Bbbk) \cong \mathrm{Cl}(R)$ by [10, Theorem 8.1]. It follows that $\mathrm{Cl}(\Bbbk)$ injects as a direct summand into $\mathrm{Cl}(S)$. The image of $\mathrm{Cl}(\Bbbk)$ in $\mathrm{Cl}(S)$ is generated by the classes of all primes of the form $\mathfrak{p}S$, where $\mathfrak{p}$ is a height-1 prime of $\Bbbk$; it is easy to see that $\mathfrak{p}S$ is indeed a prime of S (of height 1). On the other hand, by [10, Corollary 7.2], there is a surjection $\mathrm{Cl}(S) \twoheadrightarrow \mathrm{Cl}(S_{\mathcal{C}})$, where $\mathcal{C}$ denotes the set of nonzero elements of $\Bbbk$, and the kernel of this map is generated by the very same primes $\mathfrak{p}S$. Therefore, $\mathrm{Cl}(S)/\mathrm{Cl}(\Bbbk) \cong \mathrm{Cl}(S_{\mathcal{C}})$. Finally, $S_{\mathcal{C}}$ is just the second Veronese algebra of the polynomial algebra $K[t_1, t_2, \ldots, t_d]$, where K is the field of fractions of $\Bbbk$. The class group of $S_{\mathcal{C}}$ has been determined in [20, Example 1 on page 58] to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This proves part (d). $\square$

Since we will be exclusively concerned with commutative algebras in later sections, we will not list the commuting relations, such as the relations $[x_i, x_j] = [x_i, x_{k,l}] = [x_{k,l}, x_{r,s}] = 0$ in Corollary 2.5.2, in our future results. Thus, in the context of commutative algebras, the defining relations for the Veronese algebra $S = R^{(2)}$ in Corollary 2.5.2 are the relations $x_j x_j = x_{i,j}^2$.

CHAPTER 3

Multiplicative Invariants of Classical Root Lattices

In this chapter, we calculate the multiplicative invariant algebras for the classical root lattices using the general facts and notation set up in the previous chapter. Our description of the root systems and their associated data follows Bourbaki [2] as in Chapter 2. Throughout, we work in $\mathbb{R}^n$, with the usual inner product, and we let $\{\varepsilon_i\}_1^n$ denote the standard orthonomal basis of $\mathbb{R}^n$.

3.1 Type B_n

We start with the root lattice for the root system of type B_n $(n \geq 2)$, because it has particularly nice invariants and will be used as an aid in calculating the invariants of the other three classical root lattices. We are mainly interested in the multiplicative invariants under the Weyl group $\mathcal{W} = \mathcal{W}(\mathsf{B}_n)$; however we also include the invariants under the symmetric group $\mathcal{S}_n \leq \mathcal{W}$ here, since they will be useful for finding invariants of the root lattice of type A_n. To find the invariants for B_n we need not invoke the general methods described above in 2.3.3 and 2.3.4, since this is a particularly nice lattice. Instead we use a more straightforward purely invariant theoretic approach. In fact, all that is needed here is the fundamental theorem for $\mathcal{S}_n$-invariants; see, e.g., [4, Théorème 1 on p. A IV.58].

3.1.1 Root system, root lattice and Weyl group

The root system of type B_n is the following subset of $\mathbb{E} = \mathbb{R}^n$:

$$\Phi = \{\pm\varepsilon_i \mid 1 \leq i \leq n\} \cup \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq n\} \tag{3.1}$$

The root lattice $L(\Phi) = \mathbb{Z}\Phi$ will be denoted by B_n; so

$$B_n = \bigoplus_{i=1}^{n} \mathbb{Z}\varepsilon_i$$

The Weyl group $\mathcal{W} = \mathcal{W}(\Phi)$ is the semidirect product of the group of all permutation matrices in $\mathrm{GL}(\mathbb{E}) = \mathrm{GL}_n(\mathbb{R})$ with the group of all diagonal matrices $\mathcal{D}_n \leq \mathrm{GL}_n(\mathbb{Z})$. The group of permutation matrices is isomorphic to the symmetric group $\mathcal{S}_n$, operating by permuting the basis $\{\varepsilon_i\}_1^n$ via $\sigma(\varepsilon_i) = \varepsilon_{\sigma(i)}$. The diagonal group $\mathcal{D}_n \cong \{\pm 1\}^n$ operates via $\varepsilon_i \mapsto \pm\varepsilon_i$. Thus,

$$\mathcal{W} = \mathcal{D}_n \rtimes \mathcal{S}_n \cong \{\pm 1\}^n \rtimes \mathcal{S}_n$$

3.1.2 Diagonalizable reflections

We determine the subgroup $\mathcal{D} \leq \mathcal{W}$ that is generated by the diagonalizable reflections on B_n ; see Lemma 2.4.1 and Theorem 2.4.2. Note that $\mathcal{D}_n$ is generated by the diagonalizable reflections d_i with $d_i(\varepsilon_j) = \varepsilon_j$ for $i \neq j$ and $d_i(\varepsilon_i) = -\varepsilon_i$. Thus, we have $\mathcal{D}_n \leq \mathcal{D}$. In fact, equality holds here. To see this, recall from Lemma 2.4.1 that $\mathcal{D}$ is abelian; so $\mathcal{D} \cap \mathcal{S}_n$ is contained in the centralizer $C_{\mathcal{S}_n}(\mathcal{D}_n)$ of $\mathcal{D}_n$ in $\mathcal{S}_n$. Since $C_{\mathcal{S}_n}(\mathcal{D}_n) = \{1\}$, we must have

$$\mathcal{D} = \mathcal{D}_n$$

3.1.3 Multiplicative $\mathcal{W}$-invariants

Setting $x_i := \mathbf{x}^{\varepsilon_i}$ we form the group algebra,

$$\mathbb{Z}[B_n] = \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]$$

We start by determining invariants under the normal subgroup $\mathcal{D}_n$. This has been carried out in detail in [16, Example 3.5.1], but we briefly review the calculation. Since $\mathbb{Z}[B_n] \cong \mathbb{Z}[x^{\pm 1}]^{\otimes n}$ and $\mathcal{D}_n \cong \{\pm 1\}^n$, it is easy to see that $\mathbb{Z}[B_n]^{\mathcal{D}_n} \cong \left(\mathbb{Z}[x^{\pm 1}]^{\{\pm 1\}}\right)^{\otimes n}$. It is also straightforward to check that $\mathbb{Z}[x^{\pm 1}]^{\{\pm 1\}} = \mathbb{Z}[x + x^{-1}]$. (This is also covered by Example 3.2.1 below.) . Thus, we obtain

$$\mathbb{Z}[B_n]^{\mathcal{D}_n} = \mathbb{Z}[\varphi_1, \ldots, \varphi_n] \qquad \text{with} \quad \varphi_i := x_i + x_i^{-1}$$

This is a polynomial algebra over $\mathbb{Z}$. The subgroup $\mathcal{S}_n \leq \mathcal{W}$ permutes the "variables" φ_i in the standard fashion: $\sigma(\varphi_i) = \varphi_{\sigma(i)}$. Now we use the fundamental theorem for $\mathcal{S}_n$-invariants to get the final result:

$$\boxed{\mathbb{Z}[B_n]^{\mathcal{W}} = \mathbb{Z}[\sigma_1, \ldots, \sigma_n]} \tag{3.2}$$

where σ_i denotes the i^{th} elementary symmetric function in the variables $\varphi_1, \ldots, \varphi_n$. In particular, we see that $\mathbb{Z}[B_n]^{\mathcal{W}}$ is a polynomial algebra over $\mathbb{Z}$, giving

$$\mathrm{Cl}(\mathbb{Z}[B_n]^{\mathcal{W}}) = 0$$

This is of course consistent with Theorem 2.4.2(b) and our determination of $\mathcal{D}$ above. We also mention that the fact that $\mathbb{Z}[B_n]^{\mathcal{W}}$ is a polynomial algebra is also a consequence of the Bourbaki's theorem for multiplicative invariants of weight lattices, because B_n is easily shown to be isomorphic to the weight lattice of the root system of type C_n which will be discussed later.

3.1.4 Multiplicative $\mathcal{S}_n$-invariants

Now we restrict the group action on B_n to the permutation subgroup $\mathcal{S}_n \leq \mathcal{W}$. First notice that

$$\mathbb{Z}[B_n] = \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}] = \mathbb{Z}[x_1, x_2, \ldots, x_n][s_n^{-1}]$$

where $s_n = x_1 x_2 \ldots x_n$ is the n^{th} elementary symmetric polynomial in the variables x_i. Just as above, the $\mathcal{S}_n$ action is given by $\sigma(x_i) = x_{\sigma(i)}$ for all $\sigma \in S_n$. The fundamental theorem for $\mathcal{S}_n$-invariants gives $\mathbb{Z}[x_1, x_2, \ldots, x_n]^{\mathcal{S}_n} \cong \mathbb{Z}[s_1, s_2, \ldots, s_n]$

where s_j is the j^{th} elementary symmetric function in the variables x_i. Since we clearly have

$$(\mathbb{Z}[x_1, x_2, \ldots, x_n][s_n^{-1}])^{\mathcal{S}_n} = \mathbb{Z}[x_1, x_2, \ldots, x_n]^{\mathcal{S}_n}[s_n^{-1}]$$

it follows that,

$$\boxed{\mathbb{Z}[B_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, s_2, \ldots, s_{n-1}, s_n^{\pm 1}] \cong \mathbb{Z}[\mathbb{Z}_+^{n-1} \oplus \mathbb{Z}]} \tag{3.3}$$

This is a mixed Laurent polynomial ring or, alternatively, the monoid $\mathbb{Z}$-algebra of the (additive) monoid $\mathbb{Z}_+^{n-1} \oplus \mathbb{Z}$.

3.2 Type A_n

Next, we look at the root lattice of the root system of type A_n; this root lattice will be denoted by A_n. Actually, we will consider the root lattice A_{n-1} $(n \geq 2)$, because this fits better with the notation of Section 3.1 which we will continue to use.

3.2.1 Root system, root lattice and Weyl group

Here, we take $\mathbb{E}$ to be the subspace of $\mathbb{R}^n$ consisting of all points whose coordinate sum is 0. The root system of type A_{n-1} is given by

$$\Phi = \{\varepsilon_i - \varepsilon_j \mid 1 \leq i, j \leq n, i \neq j\} \tag{3.4}$$

Note that Φ is contained in the root system of type B_n as displayed in (3.1). Therefore, the root lattice $A_{n-1} = \mathbb{Z}\Phi$ is contained in the root lattice B_n. The Weyl Group $\mathcal{W} = \mathcal{W}(\mathsf{A}_{n-1})$ is the subgroup $\mathcal{S}_n \leq \mathcal{W}(\mathsf{B}_n)$ permuting the basis $\{\varepsilon_i\}_1^n$ of $\mathbb{E} = \mathbb{R}^n$ as usual:

$$\mathcal{W} = \mathcal{S}_n$$

It is easy to see that the vectors

$$\alpha_i := \varepsilon_i - \varepsilon_{i+1} \qquad (i = 1, \ldots, n-1)$$

form a base of the root system Φ. So the root lattice $A_{n-1} = L(\Phi)$ is given by

$$A_{n-1} = \bigoplus_{i=1}^{n-1} \mathbb{Z}\alpha_i$$

Note that there is an exact sequence of $\mathcal{S}_n$-lattices, that is, an exact sequence of free abelian groups with $\mathcal{S}_n$-equivariant maps,

$$0 \longrightarrow A_{n-1} \longrightarrow B_n \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{3.5}$$

Here $\mathbb{Z}$ has the trivial $\mathcal{S}_n$-action and the map $B_n \to \mathbb{Z}$ sends $\varepsilon_i \mapsto 1$.

3.2.2 Multiplicative $\mathcal{W}$-invariants

Using the notation for B_n above, we set $y_i := \mathbf{x}^{\alpha_i} = \frac{x_i}{x_{i+1}}$ to get the group algebra

$$\mathbb{Z}[A_{n-1}] = \mathbb{Z}[y_1^{\pm 1}, y_2^{\pm 1}, \ldots, y_{n-1}^{\pm 1}]$$

From (3.5), we see that $\mathbb{Z}[A_{n-1}]$ is the degree-zero component of the Laurent polynomial algebra $\mathbb{Z}[B_n] = \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]$, graded by total degree in the variables x_i. Since the action of $\mathcal{W} = \mathcal{S}_n$ is obviously degree-preserving, it follows that the multiplicative invariant algebra $\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n}$ is the degree-zero component of $\mathbb{Z}[B_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, s_2, \ldots, s_n^{\pm 1}]$; see (3.3). Since $\deg s_i = i$, it is easy to see that a $\mathbb{Z}$-basis for the degree-zero component of $\mathbb{Z}[s_1, s_2, \ldots, s_n^{\pm 1}]$ is given by the elements

$$\frac{s_1^{l_1} s_2^{l_2} \cdots s_{n-1}^{l_{n-1}}}{s_n^{l_n}} \qquad \text{where } l_i \in \mathbb{Z}_+ \text{ and } \sum_{i=1}^{n-1} i l_i = n l_n$$

Hence $\mathbb{Z}[A_{n-1}]^{\mathcal{W}}$ is isomorphic to the monoid $\mathbb{Z}$-algebra $\mathbb{Z}[M_{n-1}]$, where M_{n-1} is the following submonoid of $\mathbb{Z}_+^{n-1}$:

$$\boxed{M_{n-1} = \left\{ (l_1, l_2, \ldots, l_{n-1}) \in \mathbb{Z}_+^{n-1} \mid \sum_{i=1}^{n-1} i l_i \in (n) \right\}} \tag{3.6}$$

The isomorphism is explicitly given by

$$\boxed{\begin{array}{ccc} \mathbb{Z}[M_{n-1}] & \xrightarrow{\sim} & \mathbb{Z}[A_{n-1}]^{\mathcal{W}} \\ \cup & & \cup \\ (l_1, l_2, \ldots, l_{n-1}) & \longmapsto & \dfrac{s_1^{l_1} s_2^{l_2} \cdots s_{n-1}^{l_{n-1}}}{s_n^{l_n}} \end{array}} \tag{3.7}$$

with $l_n = \frac{1}{n}\sum_{i=1}^{n-1} i l_i$.

While describing all the indecomposable elements of the monoid M_{n-1} is a difficult task for general n, we can easily find the $n-1$ indecomposables that correspond to the primary invariants for $\mathbb{Z}[A_{n-1}]^{\mathcal{W}}$ using Proposition 2.3.5(c) above. It suffices to find z_i, the order of our fundamental weights, ϖ_i, modulo A_{n-1}. Then applying the isomorphism $\Omega : \mathbb{Z}[A_{n-1} \cap \Lambda_+] \xrightarrow{\sim} \mathbb{Z}[A_{n-1}]^{\mathcal{W}}$ in Theorem 2.3.3 to the indecomposable elements $m_i = z_i\varpi_i$ will give us the primary invariants for this lattice. In detail, the fundamental weights ϖ_i with respect to the above base $\{\alpha_i\}_1^{n-1}$ of Φ are given by (see [2])

$$\begin{aligned} \varpi_i &= \varepsilon_1 + \cdots + \varepsilon_i - \frac{i}{n}\sum_{j=1}^{n} \varepsilon_j \\ &= \frac{1}{n}[(n-i)(\alpha_1 + 2\alpha_2 + \cdots + (i-1)\alpha_{i-1}) + i((n-i)\alpha_i + (n-i-i)\alpha_{i+1} + \cdots + \alpha_{n-1})] \\ &= \alpha_1 + 2\alpha_2 + \cdots + (i-1)\alpha_{i-1} - \frac{i}{n}(\alpha_1 + 2\alpha_2 + \cdots + (i-1)\alpha_{i-1} - (n-i)\alpha_i - \cdots - \alpha_{n-1}) \end{aligned}$$

To guarantee that $m_i = z_i\varpi_i \in A_{n-1}$, we must have integral coefficients for all α_i. So z_i must be the smallest positive integer that satisfies the condition $z_i \cdot \frac{i}{n} \in \mathbb{Z}$. Explicitly, $z_i = \frac{n}{i_n}$ with

$$i_n = \gcd(i, n)$$

Now applying Ω gives primary invariants $\pi_i = \mathsf{orb}(\varpi_i)^{\frac{n}{i_n}}$. One can easily calculate the $\mathcal{S}_n$-orbit sum of ϖ_i from the first expression for ϖ_i given above:

$$\mathsf{orb}(\varpi_i) = s_i s_n^{-\frac{i}{n}}$$

where s_i is the i^{th} elementary symmetric function in $x_1, \ldots, x_n$ as before. Hence $\mathbb{Z}[A_{n-1}]^{\mathcal{W}}$ has the following primary invariants:

$$\boxed{\pi_i = s_i^{\frac{n}{i_n}} s_n^{-\frac{i}{i_n}} \quad i = 1, \ldots, n-1} \tag{3.8}$$

Example 3.2.1. For $n = 2$, the submonoid $M_1 \subseteq \mathbb{Z}_+$ is generated by 2, giving the single generator $\pi_1 = \frac{s_1^2}{s_2} = y_1 + y_1^{-1} + 2$ of $\mathbb{Z}[A_1]^{\mathcal{S}_2}$. Omitting the obviously unnecessary summand 2, we obtain

$$\mathbb{Z}[A_1]^{\mathcal{S}_2} = \mathbb{Z}[y_1 + y_1^{-1}]$$

a polynomial algebra. Note that $y_1 + y_1^{-1} = \mathsf{orb}(\alpha_1)$.

Example 3.2.2. For $n = 3$, we have three generators for our monoid M_2 as was already depicted earlier in (2.8): $m_1 = (3, 0)$, $m_2 = (0, 3)$ and $m_3 = (1, 1)$. By (3.7), these generators correspond to the fundamental invariants $\pi_1 = \frac{s_1^3}{s_3}$, $\pi_2 = \frac{s_2^3}{s_3^2}$ and $\mu = \frac{s_1 s_2}{s_3}$ respectively. The monoid relation $3m_3 = m_1 + m_2$ becomes $\mu^3 = \pi_1\pi_2$ in $\mathbb{Z}[A_2]^{\mathcal{S}_3}$. This yields the following presentation for the multiplicative invariant algebra:

$$\mathbb{Z}[A_2]^{\mathcal{S}_3} = \mathbb{Z}[\pi_1, \pi_2, \mu] \cong \mathbb{Z}[x, y, z]/(z^3 - xy)$$

Evidently, a Hironaka decomposition of $\mathbb{Z}[A_2]^{\mathcal{S}_3}$ is

$$\mathbb{Z}[A_2]^{\mathcal{S}_3} = \mathbb{Z}[\pi_1, \pi_2] \oplus \mu\mathbb{Z}[\pi_1, \pi_2] \oplus \mu^2\mathbb{Z}[\pi_1, \pi_2]$$

This is in fact exactly the Hironaka decomposition provided by Proposition 2.3.5(c), because $K^\circ \cap A_2 = \{0, m_3, 2m_3\}$; see (2.8).

When explicitly written out in terms of the standard generators y_i of the Laurent polynomial algebra $\mathbb{Z}[A_{n-1}] = \mathbb{Z}[y_1^{\pm 1}, y_2^{\pm 1}, \ldots, y_{n-1}^{\pm 1}]$, the above fundamental invariants π_1, π_2, μ have rather unwieldy expressions. A more economical system of fundamental invariants for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$ is given by

$$\begin{aligned}
\mu - 3 &= y_1 + y_1^{-1} + y_2 + y_2^{-1} + y_1y_2 + y_1^{-1}y_2^{-1} && = \mathsf{orb}(\alpha_1) \\
\pi_1 - 3\mu + 3 &= y_1^2y_2 + y_1^{-1}y_2 + y_1^{-1}y_2^{-2} && = \mathsf{orb}(2\alpha_1 + \alpha_2) \\
\pi_2 - 3\mu + 3 &= y_1y_2^2 + y_1y_2^{-1} + y_1^{-2}y_2^{-1} && = \mathsf{orb}(\alpha_1 + 2\alpha_2)
\end{aligned}$$

3.2.3 Computations

For general n, it is difficult to write down all secondary invariants, a Hironaka decomposition, and the defining relations for $\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n}$. However, as we already

mentioned in Section 2.3.4, one can use the computer algebra system CoCoA to find Hilbert bases for monoids. In this section, we will illustrate this for the monoid M_{n-1} from (3.6) in particular cases. Once we have the Hilbert basis for M_{n-1} available, we can then use Theorem 2.3.3 and Proposition 2.3.5 to find the fundamental invariants and a Hironaka decomposition. We will use the following description of the monoid M_{n-1}, which is clearly equivalent to (3.6):

$$M_{n-1} = \left\{(l_1, l_2, \ldots, l_{n-1}, x) \in \mathbb{Z}_+^n \mid \sum_{i=1}^{n-1} il_i - nx = 0\right\}$$

Thus, M_{n-1} is the kernel in $\mathbb{Z}_+^n$ of the following matrix:

$$A = [1, 2, 3, \cdots, n-1, -n]$$

Here are two sample calculations with CoCoA, for $n = 3$ and $n = 4$:

$\mathbf{n = 3}$:

```
A:=Mat([[1,2,-3]]);
HilbertBasisKer(A);
[[1, 1, 1], [3, 0, 1], [0, 3, 2]]
```

The first two components of the output vectors tell us the Hilbert basis of our monoid M_2: $(1, 1)$, $(3, 0)$ and $(0, 3)$. This does of course agree with the Hilbert basis exhibited in (2.8) and used again in Example 3.2.2 above. The resulting fundamental invariants, a Hironaka decompositon and a presentation of the invariant algebra $\mathbb{Z}[A_2]^{S_3}$ has already been worked out in Example 3.2.2.

$\mathbf{n = 4}$:

```
A:=Mat([[1,2,3,-4]]);
HilbertBasisKer(A);
[[0, 2, 0, 1], [1, 0, 1, 1], [2, 1, 0, 1],
[0, 1, 2, 2], [4, 0, 0, 1], [0, 0, 4, 3]]
```

Here we obtain the following Hilbert basis of M_3: $(0, 2, 0)$, $(1, 0, 1)$, $(2, 1, 0)$, $(0, 1, 2)$, $(4, 0, 0)$ and $(0, 0, 4)$. To obtain a presentation of the invariant algebra

$\mathbb{Z}[A_3]^{\mathcal{S}_4} \cong \mathbb{Z}[M_3]$, we will consider the polynomial algebra $\mathbb{Z}[x, y, z, u, v, w]$ in six variables and the epimorphism

$$\mathbb{Z}[x, y, z, u, v, w] \twoheadrightarrow S := \mathbb{Z}[M_3]$$

sending each variable to one of the elements in our Hilbert basis:

$$x \mapsto (4, 0, 0) \quad y \mapsto (0, 2, 0) \quad z \mapsto (0, 0, 4)$$
$$u \mapsto (2, 1, 0) \quad v \mapsto (1, 0, 1) \quad w \mapsto (0, 1, 2)$$

We will denote the kernel of this map by I. Our goal is to find generators of the ideal I; these are the desired defining relations for S. To this end, we view $M_3 \subseteq \mathbb{Z}_+^3$ and the algebra S as contained in the polynomial algebra in three variables:

$$S = \mathbb{Z}[M_3] \subseteq T := \mathbb{Z}[\mathbb{Z}_+^3] \cong \mathbb{Z}[a, b, c]$$

For example, the Hilbert basis element $(4, 0, 0)$ of M_3 becomes the monomial a^4 when viewed in $\mathbb{Z}[a^{\pm 1}, b^{\pm 1}, c^{\pm 1}]$, and $(0, 1, 2)$ becomes bc^2. The Laurent polynomial algebra $\mathbb{Z}[a^{\pm 1}, b^{\pm 1}, c^{\pm 1}]$ can be presented as the image of the polynomial algebra in the variables a, b, c plus one extra variable, d, which serves as the inverse of the product abc. Thus, we may consider the map

$$T[x, y, z, u, v, w] \twoheadrightarrow T$$

that is the identity on T and maps the variables $x, \ldots, w$ as indicated above. Thus, we have nine variables altogether. The ideal I arises as the so-called elimination ideal, eliminating the variables a, b, c, d. For more details, we refer to Algorithm 4.5 in [25, page 32]. The computation is carried out with the computer algebra system MAGMA (V2.19-10):

```
> Z := IntegerRing();
> S<a,b,c,x,y,z,u,v,w>:= PolynomialRing(Z,9);
> I:=ideal<S|x-a^4,y-b^2,z-c^4,u-a^2*b,v-a*c,w-b*c^2>;
> EliminationIdeal(I,3);
Ideal of Polynomial ring of rank 9 over Integer Ring
Order: Lexicographical
Variables: a, b, c, x, y, z, u, v, w
```

```
Basis:
[
    z*u - v^2*w,
    y*v^2 - u*w,
    y*z - w^2,
    x*w - u*v^2,
    x*y - u^2,
    x*z - v^4
]
```

To summarize, we have obtained the following presentation of our multiplicative invariant algebra:

$$\begin{aligned}\mathbb{Z}[A_3]^{\mathcal{S}_4} &\cong \mathbb{Z}[M_3] \\ &\cong \mathbb{Z}[x,y,z,u,v,w]/(zu-v^2w, yv^2-uw, yz-w^2, xw-uv^2, xy-u^2, xz-v^4)\end{aligned}$$

The first defining relation, $zu-v^2w$, for example, comes from the equation $(0,0,4)+(2,1,0) = 2(1,0,1)+(0,1,2)$ in M_3.

As with the example for $n=3$, we may also write down a Hironaka description for our invariant algebra. Recall our six monoid generators are:

$$\begin{aligned} m_1 &= (4,0,0) \quad m_2 = (0,2,0) \quad m_3 = (0,0,4) \\ m_4 &= (2,1,0) \quad m_5 = (1,0,1) \quad m_6 = (0,1,2)\end{aligned}$$

By (3.7), these generators correspond to the fundamental invariants $\pi_1 = \frac{s_1^4}{s_4}$, $\pi_2 = \frac{s_2^2}{s_4}$, $\pi_3 = \frac{s_3^4}{s_4^3}$, $\mu_1 = \frac{s_1^2 s_2}{s_4}$, $\mu_2 = \frac{s_1 s_3}{s_4}$ and $\mu_3 = \frac{s_2 s_3^2}{s_4^2}$ respectively.

With the above notation the Hironaka decomposition of $\mathbb{Z}[A_3]^{\mathcal{S}_4}$ is

$$\begin{aligned}\mathbb{Z}[A_3]^{\mathcal{S}_4} =& \mathbb{Z}[\pi_1,\pi_2,\pi_3] \bigoplus \oplus_{i=1}^3 \mu_i \mathbb{Z}[\pi_1,\pi_2,\pi_3] \bigoplus \oplus_{i=2}^3 \mu_2^i \mathbb{Z}[\pi_1,\pi_2,\pi_3] \\ & \bigoplus \mu_1\mu_2 \mathbb{Z}[\pi_1,\pi_2,\pi_3] \bigoplus \mu_2\mu_3 \mathbb{Z}[\pi_1,\pi_2,\pi_3]\end{aligned}$$

Again, this Hironaka decomposition is provided by Proposition 2.3.5(c).

3.2.4 Class group

For A_1, we know from Example 3.2.2 above that $\mathrm{Cl}(\mathbb{Z}[A_1]^{\mathcal{S}_2}) = 0$ since this invariant algebra is a polynomial ring. To find the class group $\mathrm{Cl}(\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n})$ for

$n \geq 3$, we use Theorem 2.4.2. First, following [16, Example 4.2.2], I will show that

$$\mathcal{D} = \{1\}$$

To see this, we first notice that the only elements of $\mathcal{S}_n$ that act as reflections on A_{n-1} are transpositions. Moreover, if $\sigma \in \mathcal{S}_n$ is a transposition then [16, Lemma 2.8.2] gives $H^1(\langle\sigma\rangle, A_{n-1}) = 0$, because σ has fixed points in $\{1, 2, \ldots, n\}$ for $n \geq 3$. Therefore, σ does not act as a diagonalizable reflection on A_{n-1}, proving that $\mathcal{D} = \{1\}$, as claimed. Now Theorem 2.4.2(a) gives

$$\mathrm{Cl}(\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n}) \cong H^1(\mathcal{S}_n, A_{n-1}) \cong \Lambda/A_{n-1}$$

where Λ is the weight lattice of the root system of type A_{n-1}. This group is known to be cyclic of order n. Indeed, the factor Λ/A_{n-1} can be found in [2, Planche I, (VIII)], and the group $H^1(\mathcal{S}_n, A_{n-1})$ is also covered by [16, Lemma 2.8.2]. Here, we derive the same result in a different way, using formula (2.3):

$$\Lambda/A_{n-1} = (A_{n-1} \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{S}_n}$$

In order to determine the invariants on the right, note that each element $z \in A_{n-1} \otimes \mathbb{Q}/\mathbb{Z}$ can be uniquely written as $z = \sum_{i=1}^{n-1} \alpha_i \otimes \overline{q}_i$ with $\overline{q}_i \in \mathbb{Q}/\mathbb{Z}$. We will simply write $z = \sum_i \overline{q}_i \alpha_i$. Now suppose that $z \in (A_{n-1} \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{S}_n}$. Then, in particular, $(12\ldots n)z = z$. Since $(12\ldots n)\alpha_i = \alpha_{i+1}$ for $1 \leq i \leq n-2$ and $(12\ldots n)\alpha_{n-1} = \varepsilon_n - \varepsilon_1 = -\alpha_1 - \alpha_2 - \cdots - \alpha_{n-1}$, this condition becomes

$$\overline{q}_1\alpha_2 + \overline{q}_2\alpha_3 + \cdots + \overline{q}_{n-2}\alpha_{n-1} + \overline{q}_{n-1}(-\alpha_1 - \alpha_2 - \cdots - \alpha_{n-1}) = \sum_i \overline{q}_i\alpha_i$$

which amounts to the following system of equations in $\mathbb{Q}/\mathbb{Z}$:

$$\begin{aligned}
\overline{q}_1 &= -\overline{q}_{n-1} \\
\overline{q}_2 &= -\overline{q}_{n-1} + \overline{q}_1 \\
&\vdots \\
\overline{q}_{n-1} &= -\overline{q}_{n-1} + \overline{q}_{n-2}
\end{aligned}$$

Putting $\overline{q} = -\overline{q}_{n-1}$, we obtain that $\overline{q}_i = i\overline{q}$ for $1 \leq i \leq n-1$ and so $z = \sum_i i\overline{q}\alpha_i$. The equation $\overline{q}_{n-1} = -\overline{q} = (n-1)\overline{q}$ shows that $\overline{q} \in \mathrm{ann}_{\mathbb{Q}/\mathbb{Z}}(n) = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

One can easily check that z is also invariant under (12) and hence under all of $\mathcal{S}_n$. In sum, we have again shown that $(A_{n-1} \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{S}_n} \cong \mathbb{Z}/n\mathbb{Z}$ and hence

$$\boxed{\mathrm{Cl}(\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n}) \cong \mathbb{Z}/n\mathbb{Z} \qquad (n \geq 3)}$$

3.3 Type C_n

We continue using the notation of Sections 3.1 and 3.2.

3.3.1 Root system, root lattice and Weyl group

Here, $\mathbb{E} = \mathbb{R}^n$ and

$$\Phi = \{\pm 2\varepsilon_i \mid 1 \leq i \leq n\} \cup \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq n\} \tag{3.9}$$

This root system contains the root system of type A_{n-1} from (3.4), and it is identical to the root system of type B_n displayed in (3.1) except for the factor 2 in the first set of roots above. The Weyl group is exactly the same as for type B_n:

$$\mathcal{W} = \mathcal{D}_n \rtimes \mathcal{S}_n \cong \{\pm 1\}^n \rtimes \mathcal{S}_n$$

If $n = 2$ then the root systems of type B_n and C_n are isomorphic, and so we may assume that $n \geq 3$ below. By the foregoing the root lattice $L = L(\Phi)$, which will be denoted by C_n, is sandwiched between the root lattices A_{n-1} and B_n. Under the exact sequence (3.5), the root lattice C_n is the preimage of $2\mathbb{Z}$ in B_n; so C_n fits into the following short exact sequence of $\mathcal{W}$-lattices:

$$0 \longrightarrow C_n \longrightarrow B_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \tag{3.10}$$

where each basis element ε_i of B_n is mapped to $\bar{1} \in \mathbb{Z}/2\mathbb{Z}$. The vectors $\alpha_i := \varepsilon_i - \varepsilon_{i+1}$ for $i = 1, \ldots, n-1$ together with $\alpha_n = 2\varepsilon_n$ form a base of the root system Φ, and hence these vectors are also a $\mathbb{Z}$-basis of the root lattice of C_n.

3.3.2 Multiplicative $\mathcal{W}$-invariants

Sequence (3.10) will help us calculate multiplicative invariants of the root lattice C_n, just as (3.5) did with A_{n-1}. As before, we let $x_i = \mathbf{x}^{\varepsilon_i}$ and $y_i = \mathbf{x}^{\alpha_i}$; so $y_i = \frac{x_i}{x_{i+1}}$ for $i = 1, \ldots, n-1$ and $y_n = x_n^2$. Then

$$\mathbb{Z}[C_n] = \mathbb{Z}[y_1^{\pm 1}, y_2^{\pm 1}, \ldots, y_n^{\pm 1}]$$

We deduce from (3.10) that $\mathbb{Z}[C_n]$ is the subalgebra of $\mathbb{Z}[B_n] = \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]$ that is spanned by the monomials of even total degree in the x_is. Using this observation, we can easily find the invariants $\mathbb{Z}[C_n]^{\mathcal{W}}$. Indeed, note that the action of $\mathcal{S}_n$ on $\mathbb{Z}[B_n] = \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]$ is degree preserving and $\mathcal{D}_n$ preserves at least the *parity* of the degree. Thus, $\mathcal{W} = \mathcal{D}_n \rtimes \mathcal{S}_n$ preserves parities of degrees as well, which allows us to conclude that $\mathbb{Z}[C_n]^{\mathcal{W}}$ is the even-degree component of $\mathbb{Z}[B_n]^{\mathcal{W}} = \mathbb{Z}[\sigma_1, \ldots, \sigma_n]$, where

$$\boxed{\sigma_i = \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I| = i}} \prod_{j \in I} (x_j + x_j^{-1})}$$

is the i^{th} elementary symmetric function in the variables $x_j + x_j^{-1}$ $(j = 1, 2, \ldots, n)$ as in (3.2). Therefore, a $\mathbb{Z}$-basis for $\mathbb{Z}[C_n]^{\mathcal{W}}$ is given by $\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ with $\sum_{i=1}^n il_i \in 2\mathbb{Z}$. These observations prove most of part (a) of the following theorem which was already stated as Theorem 1.2.1 in the Introduction.

Theorem 3.3.1. (a) ***Algebra structure:*** *$\mathbb{Z}[C_n]^{\mathcal{W}}$ is isomorphic to the monoid algebra $\mathbb{Z}[M_n]$ with*

$$M_n = \Big\{(l_1, l_2, \ldots, l_n) \in \mathbb{Z}_+^n \mid \sum_{i=1}^n il_i \equiv 0 \bmod 2\Big\}$$

The isomorphism is given by

$$\begin{array}{ccc} \mathbb{Z}[M_n] & \xrightarrow{\sim} & \mathbb{Z}[C_n]^{\mathcal{W}} \\ \cup & & \cup \\ (l_1, l_2, \ldots, l_n) & \longmapsto & \sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n} \end{array}$$

The monoid M_n decomposes as $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor} \oplus V$ with

$$V = \left\{ (k_1, k_2, \ldots, k_{\lceil \frac{n}{2} \rceil}) \in \mathbb{Z}_+^{\lceil \frac{n}{2} \rceil} \mid \sum_i k_i \equiv 0 \bmod 2 \right\}$$

Thus, $\mathbb{Z}[C_n]^{\mathcal{W}}$ is a polynomial ring in $\lfloor \frac{n}{2} \rfloor$ variables over the second Veronese subring of a polynomial algebra in $\lceil \frac{n}{2} \rceil$ variables over $\mathbb{Z}$.

(b) ***Fundamental invariants:*** *The algebra $\mathbb{Z}[C_n]^{\mathcal{W}}$ is generated by the following $n + \binom{\lceil \frac{n}{2} \rceil}{2}$ invariants:*

$$\pi_i = \begin{cases} \sigma_i & \text{for } i \text{ even} \\ \sigma_i^2 & \text{for } i \text{ odd} \end{cases}$$

$$\gamma_{i,j} = \sigma_i \sigma_j \quad (1 \leq i < j \leq n \text{ and } i, j \text{ both odd})$$

The π_i are primary invariants and the $\gamma_{i,j}$ are secondary: $\mathbb{Z}[\pi_1, \ldots, \pi_n]$ is a polynomial algebra over $\mathbb{Z}$ and $\mathbb{Z}[C_n]^{\mathcal{W}}$ is a finite module over $\mathbb{Z}[\pi_1, \ldots, \pi_n]$.

(c) ***Hironaka decomposition:***

$$\mathbb{Z}[C_n]^{\mathcal{W}} = \bigoplus_{\substack{1 \leq i_1 < j_1 < i_2 < \cdots < i_t < j_t \leq n \\ \text{all odd}}} \gamma_{i_1,j_1} \gamma_{i_2,j_2} \ldots \gamma_{i_t,j_t} \, \mathbb{Z}[\pi_1, \ldots, \pi_n]$$

(Here, we allow $t = 0$, the corresponding summand being $\mathbb{Z}[\pi_1, \ldots, \pi_n]$.)

(d) ***Defining relations:*** *The $\binom{\lceil \frac{n}{2} \rceil}{2}$ relations*

$$\pi_i \pi_j = \gamma_{i,j}^2 \qquad (1 \leq i < j \leq n \text{ and } i, j \text{ both odd})$$

are defining relations for $\mathbb{Z}[C_n]^{\mathcal{W}}$.

Proof. The isomorphism $\mathbb{Z}[C_n]^{\mathcal{W}} \cong \mathbb{Z}[M_n]$, with the indicated monoid M_n, has been proved in the remarks preceding the statement of the theorem. For the decomposition $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor} \oplus V$, note that

$$\sum_i i l_i \equiv 0 \bmod 2 \iff \sum_{i \text{ odd}} l_i \equiv 0 \bmod 2$$

The unrestricted components in even positions form the factor $\mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor}$, the components in odd positions the factor V. The decomposition $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor} \oplus V$ leads to an algebra isomorphism

$$\mathbb{Z}[M_n] \cong \mathbb{Z}[\mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor}] \otimes \mathbb{Z}[V]$$

where the first factor is a polynomial algebra in $\lfloor \frac{n}{2} \rfloor$ variables over $\mathbb{Z}$ and $\mathbb{Z}[V]$ is the second Veronese subring of the polynomial algebra $\mathbb{Z}[\mathbb{Z}_+^{\lceil \frac{n}{2} \rceil}] \cong \mathbb{Z}[t_1, \ldots, t_{\lceil \frac{n}{2} \rceil}]$ as in Corollary 2.5.2. Equivalently, $\mathbb{Z}[M_n]$ is a polynomial algebra in $\lfloor \frac{n}{2} \rfloor$ variables over the Veronese subring. This proves (a).

Now for the fundamental invariants in (b). The σ_i with i even are the variables of the polynomial factor $\mathbb{Z}[\mathbb{Z}_+^{\lfloor \frac{n}{2} \rfloor}]$ above. For the fundamental invariants of the Veronese factor $\mathbb{Z}[V]$, it suffices to quote Corollary 2.5.2(a). This proves (b). The Hironaka decomposition and the defining relations in (c) and (d) are immediate from Corollary 2.5.2 as well. □

We remark that the generators π_i, $\gamma_{i,j}$ of the monoid M_n exhibited in the proof of Theorem 3.3.1 above are clearly indecomposable elements of M_n. Therefore, they form the *Hilbert basis* of M_n.

Example 3.3.2. When $n = 2$, the monoid M_2 has generators $(2, 0)$ and $(0, 1)$. These generators correspond to the following algebra generators:

$$\begin{aligned}
\pi_1 = \sigma_1^2 &= (x_1 + x_1^{-1} + x_2 + x_2^{-1})^2 \\
&= y_1^2 y_2 + y_1^{-2} y_2^{-1} + y_2 + y_2^{-1} + 2y_1 y_2 + 2y_1 + 2y_1^{-1} + 2y_1^{-1} y_2^{-1} + 4 \\
\pi_2 = \sigma_2 &= (x_1 + x_1^{-1})(x_2 + x_2^{-1}) \\
&= y_1 y_2 + y_1 + y_1^{-1} + y_1^{-1} y_2^{-1}
\end{aligned}$$

giving $\mathbb{Z}[C_2]^{\mathcal{W}} \cong \mathbb{Z}[\sigma_1^2, \sigma_2]$, a polynomial algebra. Since C_2 is isomorphic to B_2, this is of course in agreement with what we found for $\mathbb{Z}[B_2]^{\mathcal{W}}$ earlier. Again, the fundamental invariant π_1 could be replaced by $\pi_1' = \pi_1 - 2\pi_2 - 4$ to obtain the following system of fundamental invariants:

$$\begin{aligned}
\pi_1' &= \pi_1 - 2\pi_2 - 4 = y_1^2 y_2 + y_1^{-2} y_2^{-1} + y_2 + y_2^{-1} = \mathsf{orb}(y_2) \\
\pi_2 &= y_1 y_2 + y_1 + y_1^{-1} + y_1^{-1} y_2^{-1} = \mathsf{orb}(y_1)
\end{aligned}$$

Example 3.3.3. When $n = 3$ we have monoid generators $(2,0,0), (0,1,0), (0,0,2)$ and $(1,0,1)$. For simplicity of notation define $s^{\pm} := s + s^{-1}$ for a summand s. Using this notation we may now write the algebra generators that correspond to our monoid generators.

$$\begin{aligned}
\pi_1 &= \sigma_1^2 = (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1})^2 \\
&= 2\sum_1^2 y_i^{\pm} + y_3^{\pm} + 2\sum_1^2 (y_1 y_2^i y_3)^{\pm} + 2 \sum_{\substack{i<j \\ |i-j|=1}} (y_i y_j)^{\pm} + (y_1^2 y_2^2 y_3)^{\pm} + (y_2^2 y_3)^{\pm} + 6 \\
\pi_2 &= \sigma_2 = \sum_{i<j} (x_i + x_i^{-1})(x_j + x_j^{-1}) \\
&= \sum_1^2 (y_1 y_2^i y_3)^{\pm} + y_1^{\pm} + y_2^{\pm} + (y_1 y_2)^{\pm} + (y_2 y_3)^{\pm} \\
\pi_3 &= \sigma_3^2 = \left((x_1 + x_1^{-1})(x_2 + x_2^{-1})(x_3 + x_3^{-1})\right)^2 \\
&= 8 + 4 \sum_{\substack{i \le j \\ i,j \in \{0,1\}}} (y_1^{2i} y_2^{2j} y_3)^{\pm} + 2 \sum_{\substack{i \le j \\ i \in \{0,1\}, j \in \{1,2\} \\ |i-j| \le 2}} (y_1^{2i} y_2^{2j} y_3^2)^{\pm} + 2 \sum_{\substack{i,j \in \{0,1\} \\ i+j \neq 0}} (y_1^{2i} y_2^{2j})^{\pm} \\
&\quad + \sum_{i=-1,1} (y_1^{2i} y_3^{-1})^{\pm} + (y_1^2 y_2^4 y_3^3)^{\pm} + (y_1^2 y_2^4 y_3)^{\pm} \\
\gamma_{1,3} &= \sigma_1 \sigma_3 = (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1})(x_1 + x_1^{-1})(x_2 + x_2^{-1})(x_3 + x_3^{-1}) \\
&= (y_1^2 y_2)^{\pm} + (y_1 y_2^3 y_3^2)^{\pm} + (y_1^2 y_2^3 y_3^2)^{\pm} + (y_1^{-1} y_2)^{\pm} + (y_1^2 y_2 y_3)^{\pm} + (y_1 y_3)^{\pm} + (y_1 y_2^2)^{\pm} + (y_1 y_2^2 y_3^2)^{\pm} \\
&\quad + (y_1^{-1} y_2 y_3)^{\pm} + (y_1 y_2^3 y_3)^{\pm} + (y_1^{-1} y_3)^{\pm} + (y_1^2 y_2^3 y_3)^{\pm} + 2((y_1 y_2 y_3)^{\pm} + (y_1 y_2^2 y_3)^{\pm} + y_2 y_3)^{\pm}) \\
&\quad + 2((y_1 y_2)^{\pm} + y_2^{\pm} + y_1^{\pm})
\end{aligned}$$

with the obvious relation $\pi_1 \pi_3 = \gamma_{1,3}^2$. Setting $x := \pi_1, y := \pi_2, z := \pi_3$ and $w := \gamma_{1,3}$ we have

$$\mathbb{Z}[C_3]^{\mathcal{W}} \cong \mathbb{Z}[x, y, z, w]/(xz - w^2)$$

3.3.3 Class group

We have already pointed out that $\mathbb{Z}[C_2]^{\mathcal{W}}$ is a polynomial algebra over $\mathbb{Z}$, giving $\mathrm{Cl}(\mathbb{Z}[C_2]^{\mathcal{W}}) = 0$. Thus, we will assume that $n \geq 3$ below. Recall that $\mathbb{Z}[C_n]^{\mathcal{W}}$ is a polynomial ring in $\lfloor \frac{n}{2} \rfloor$ variables over the second Veronese subring of a polynomial algebra in $\lceil \frac{n}{2} \rceil$ variables over $\mathbb{Z}$ by Theorem 3.3.1(a). It is a standard fact that $\mathrm{Cl}(R[x]) \cong \mathrm{Cl}(R)$ holds for any Krull domain R; see [10, Theorem 8.1]. Thus, it would be possible to use the structure of the class groups of Veronese algebras

(Corollary 2.5.2(d)) in order to calculate $\mathrm{Cl}(\mathbb{Z}[C_n]^{\mathcal{W}})$. However, we will use Theorem 2.4.2 instead.

First we must find the subgroup $\mathcal{D}$ consisting of all diagonalizable reflections in $\mathcal{W}$.

Lemma 3.3.4. *If $n \geq 3$, then $\mathcal{D} = \{1\}$.*

Proof. Recall from Lemma 2.4.1 that $\mathcal{D}$ is an elementary abelian normal 2-subgroup of the Weyl group $\mathcal{W} = \mathcal{D}_n \rtimes \mathcal{S}_n$. We first claim that $\mathcal{D} \subseteq \mathcal{D}_n$. Indeed, otherwise the image of $\mathcal{D}$ in $\mathcal{S}_n$ would be a nontrivial elementary abelian normal 2-subgroup of $\mathcal{S}_n$, which forces $n = 4$ and the image to be contained in the Klein 4-subgroup of $\mathcal{S}_4$. However, it is easy to see that no element of the form $d\sigma \in \mathcal{W}$, with $d \in \mathcal{D}_4$ and $\sigma \in \mathcal{S}_4$ a product of two disjoint 2-cycles, acts as a reflection on C_n (or, equivalently, on B_n). Therefore, we must have $\mathcal{D} \subseteq \mathcal{D}_n$ as claimed. Recall further, from Section 3.1.2, that the only elements of $\mathcal{D}_n$ that act as reflections are the elements $d_i \in \mathcal{D}_n$ with $d_i(\varepsilon_j) = \varepsilon_j$ for $i \neq j$ and $d_i(\varepsilon_i) = -\varepsilon_i$. We will show that $H^1(\langle d_i \rangle, C_n) = 0$; so none of these elements acts as a diagonalizable reflection on C_n (even though they do so on B_n). For this, we use the short exact sequence (3.10). The associated long exact cohomology sequence gives an exact sequence of groups

$$B_n^{\langle d_i \rangle} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow H^1(\langle d_i \rangle, C_n) \longrightarrow H^1(\langle d_i \rangle, B_n) \longrightarrow H^1(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z})$$

First, the map $B_n^{\langle d_i \rangle} \to \mathbb{Z}/2\mathbb{Z}$ is onto, because any ε_j $(j \neq i)$ belongs to $B_n^{\langle d_i \rangle}$ and has nontrivial image in $(\mathbb{Z}/2\mathbb{Z})^{\langle d_i \rangle} = \mathbb{Z}/2\mathbb{Z}$. Therefore, the above sequence becomes

$$0 \longrightarrow H^1(\langle d_i \rangle, C_n) \longrightarrow H^1(\langle d_i \rangle, B_n) \longrightarrow H^1(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z})$$

Next, the group $H^1(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ is generated by the map h with $h(d_i) = \bar{1} \in \mathbb{Z}/2\mathbb{Z}$. We also know that $H^1(\langle d_i \rangle, B_n) \cong \mathbb{Z}/2\mathbb{Z}$, since d_i is a diagonalizable reflection on B_n. Explicitly,

$$\begin{aligned} H^1(\langle d_i \rangle, B_n) &= \mathrm{Der}(\langle d_i \rangle, B_n)/\mathrm{Inn}(\langle d_i \rangle, B_n) \\ &\cong \mathrm{ann}_{B_n}(d_i + 1)B_n/(d_i - 1)B_n \\ &= \langle \varepsilon_i + 2\mathbb{Z}\varepsilon_i \rangle \cong \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

with generator the class of the derivation $\delta \in \mathrm{Der}(\langle d_i \rangle, B_n)$ that is given by $\delta(d_i) = \varepsilon_i$. The map $H^1(\langle d_i \rangle, B_n) \to H^1(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z})$ sends δ to h; so $H^1(\langle d_i \rangle, B_n) \xrightarrow{\sim} H^1(\langle d_i \rangle, \mathbb{Z}/2\mathbb{Z})$. The last exact sequence above therefore shows that $H^1(\langle d_i \rangle, C_n) = 0$ as desired. □

Now Theorem 2.4.2(a) gives $\mathrm{Cl}(\mathbb{Z}[C_n]^{\mathcal{W}}) \cong H^1(\mathcal{W}, C_n) \cong \Lambda/C_n$, where Λ is the weight lattice of the root system of type C_n. The factor Λ/C_n is known to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$; see [2, Planche III, (VIII)]. Let us summarize the result in the following proposition, for which I will give a direct proof below.

Proposition 3.3.5. $\mathrm{Cl}(\mathbb{Z}[C_n]^{\mathcal{W}}) \cong \mathbb{Z}/2\mathbb{Z}$ *for* $n \geq 3$.

Proof. By (2.3), we must find $(C_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{W}}$. We start by calculating $(C_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{D}_n}$ following the method of Section 3.2.4. Each element $z \in C_n \otimes \mathbb{Q}/\mathbb{Z}$ can be uniquely written as $z = \sum_{i=1}^{n} \overline{q}_i \alpha_i$ with $\overline{q}_i \in \mathbb{Q}/\mathbb{Z}$. If $z \in (C_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{D}_n}$, then $d_i z = z$ for all i. In particular,

$$d_1 z = \overline{q}_1(-\alpha_1 - 2\alpha_2 - \cdots - 2\alpha_{n-1} - \alpha_n) + \overline{q}_2\alpha_2 + \cdots + \overline{q}_n\alpha_n = z$$

gives the following equations in $\mathbb{Q}/\mathbb{Z}$:

$$\begin{aligned} -\overline{q}_1 &= \overline{q}_1 \\ -2\overline{q}_1 + \overline{q}_j &= \overline{q}_j \quad \text{for } 1 < j < n \\ -\overline{q}_1 + \overline{q}_n &= \overline{q}_n \end{aligned}$$

So $\overline{q}_1 = 0$. For $1 < i < n$, the condition $d_i z = z$ becomes

$$\begin{aligned} &\overline{q}_1\alpha_1 + \cdots + \overline{q}_{i-1}(\alpha_{i-1} + 2\alpha_i + \cdots + 2\alpha_{n-1} + \alpha_n) \\ &+\overline{q}_i(-\alpha_i - 2\alpha_{i+1} - \cdots - 2\alpha_{n-1} - \alpha_n) + \cdots + \overline{q}_n\alpha_n = z \end{aligned}$$

This gives the relations:

$$\begin{aligned} 2\overline{q}_{i-1} - \overline{q}_i &= \overline{q}_i \\ 2\overline{q}_{i-1} - 2\overline{q}_i + \overline{q}_j &= \overline{q}_j \quad \text{for } i < j < n \\ \overline{q}_{i-1} - \overline{q}_i + \overline{q}_n &= \overline{q}_n \end{aligned}$$

So we have $\overline{q}_{i-1} = \overline{q}_i$ for $1 < i < n-1$, but $\overline{q}_1 = 0$ giving $\overline{q}_i = 0$ for $1 \leq i < n$. Lastly consider the equation $d_n z = z$. This will give relation $\overline{q}_{n-1} - \overline{q}_n = \overline{q}_n$. But $\overline{q}_{n-1} = 0$ so we have $\overline{q}_n = -\overline{q}_n$, or $2\overline{q}_n = 0$. Setting $\overline{q}_n := \overline{q}$ gives the invariant $\overline{q}\alpha_n$, with $\overline{q} \in \mathrm{ann}_{\mathbb{Q}/\mathbb{Z}}(2) = \frac{1}{2}\mathbb{Z}/\mathbb{Z} = \{\overline{0}, \overline{\frac{1}{2}}\} \cong \mathbb{Z}/2\mathbb{Z}$. In sum, we have shown that $(C_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{D}_n}$ has order 2, with generator $\overline{\frac{1}{2}}\alpha_n$.

Finally, any $\sigma \in \mathcal{S}_{n-1}$ fixes $\overline{\frac{1}{2}}\alpha_n$, and if $\sigma(n) = i < n$, then

$$\sigma(\overline{\tfrac{1}{2}}\alpha_n) = \overline{1}\alpha_i + \overline{1}\alpha_{i+1} + \cdots + \overline{1}\alpha_{n-1} + \overline{\tfrac{1}{2}}\alpha_n = \overline{\tfrac{1}{2}}\alpha_n$$

This shows that $\overline{\frac{1}{2}}\alpha_n$ is fixed by $\mathcal{S}_n$, proving the proposition. □

3.4 Type D_n

The last classical root lattice is type D_n with $n \geq 4$. Continuing with the same notation as used above, we will calculate the multiplicative invariants and their class group for the root lattice D_n associated to this root system.

3.4.1 Root system, root lattice and Weyl group

The set of roots is the subset of $\mathbb{E} = \mathbb{R}^n$ given by

$$\Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq n\} \tag{3.11}$$

This root system is contained in the root system of type C_n. The Weyl group for D_n is a proper subgroup of $\mathcal{W}(\mathsf{C}_n) = \mathcal{D}_n \rtimes \mathcal{S}_n$:

$$\mathcal{W} = \mathcal{W}(\mathsf{D}_n) = (\mathcal{D}_n \cap \mathrm{SL}_n(\mathbb{Z})) \rtimes \mathcal{S}_n$$

We remark that this root system is often considered for $n \geq 3$; see [2, Planche IV]. However, for $n = 3$, the root system is isomorphic to the root system of type A_3. The description of $\mathcal{W}$ above becomes the standard description of $\mathcal{W}(\mathsf{A}_3) = \mathcal{S}_4$ as the semidirect product of $\mathcal{S}_3$ with a Klein 4-group. Therefore, the material below is only new for $n \geq 4$.

The vectors $\alpha_i := \varepsilon_i - \varepsilon_{i+1}$ for $i = 1, \ldots, n-1$ and $\alpha_n = \varepsilon_{n-1} + \varepsilon_n$ form a base for the root system Φ, giving in particular a $\mathbb{Z}$-basis for the root lattice D_n. Note that the α_i with $1 \leq i \leq n-1$ were also part of the $\mathbb{Z}$-basis of the root lattice C_n considered in Section 3.3.1. The last basis vectors, $\varepsilon_{n-1} + \varepsilon_n$ for D_n and $2\varepsilon_n$ for C_n, are related by $2\varepsilon_n + \alpha_{n-1} = \varepsilon_{n-1} + \varepsilon_n$. Therefore, the root lattices C_n and D_n are identical. Thus, by (3.10) above,

$$D_n = \Big\{ \textstyle\sum_i z_i\varepsilon_i \in \bigoplus_{i=1}^{n} \mathbb{Z}\varepsilon_i \mid \sum_i z_i \text{ is even} \Big\} \tag{3.12}$$

3.4.2 Multiplicative $\mathcal{W}$-invariants

To calculate the multiplicative invariants for the root lattice D_n , we will use Theorem 2.3.3 and Proposition 2.3.5. The invariant algebra $\mathbb{Z}[D_n]^{\mathcal{W}}$ could also be calculated using a more elementary approach, similar to what we did for C_n and A_n , but the algebraic structure as a monoid algebra would be difficult to obtain in this way. Recall that Theorem 2.3.3 states that $\mathbb{Z}[D_n]^{\mathcal{W}}$ is isomorphic to the monoid algebra of the monoid $D_n \cap \Lambda_+$ with $\Lambda_+ = \bigoplus_{i=1}^{n} \mathbb{Z}_+\varpi_i$, the isomorphism $\Omega : \mathbb{Z}[D_n \cap \Lambda_+] \xrightarrow{\sim} \mathbb{Z}[D_n]^{\mathcal{W}}$ being given by

$$\begin{array}{ccc} \mathbb{Z}[D_n \cap \Lambda_+] & \xrightarrow{\sim} & \mathbb{Z}[D_n]^{\mathcal{W}} \\ \cup & & \cup \\ \displaystyle\sum_{i=1}^{n} l_i\varpi_i & \longmapsto & \displaystyle\prod_{i=1}^{n} \mathsf{orb}(\varpi_i)^{l_i} \end{array}$$

In the following theorem, we determine $D_n \cap \Lambda_+$ explicitly and use the isomorphism above to give the description of our invariant algebra.

As usual, we put $x_i = \mathbf{x}^{\varepsilon_i}$ and we let

$$\boxed{\sigma_i = \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=i}} \prod_{j \in I} (x_j + x_j^{-1})}$$

denote the i^{th} elementary symmetric function in the variables $x_1 + x_1^{-1}, \ldots, x_n + x_n^{-1}$ $(j = 1, 2, \ldots, n)$; these elements are invariant under $\mathcal{W}(\mathsf{B}_n)$, which contains $\mathcal{W}$.

As we will review in the proof of Theorem 3.4.1 below, the weight lattice Λ is not contained in $\bigoplus_{i=1}^n \mathbb{Z}\varepsilon_i$ but in the larger sublattice $\bigoplus_{i=1}^n \mathbb{Z}\frac{1}{2}\varepsilon_i$ of the Euclidean space $\mathbb{E}$; so we will work in this setting as well. The Weyl group $\mathcal{W}$ stabilizes both lattices. We put $y_i = \mathbf{x}^{\frac{1}{2}\varepsilon_i}$ and

$$\boxed{\tau_\pm = \sum_{\substack{(d_1,\dots,d_n)\in\{\pm1\}^n \\ \prod_i d_i = \pm 1}} y_1^{d_1} y_2^{d_2} \cdots y_n^{d_n}}$$

Note that τ_+ is the $\mathcal{W}$-orbit sum of the lattice element $\frac{1}{2}(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n)$, because the $\mathcal{W}$-orbit of this element consists of all $\frac{1}{2}(d_1\varepsilon_1+\cdots+d_n\varepsilon_n)$ with $d_i = \pm 1$ and $\prod_i d_i = 1$. Similarly, τ_- is the $\mathcal{W}$-orbit sum of $\frac{1}{2}(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_{n-1}-\varepsilon_n)$. Using this along with the notation in 2.3.3 and 2.3.4 we give the following theorem.

Theorem 3.4.1. (a) ***Monoid algebra structure:*** *$\mathbb{Z}[D_n]^{\mathcal{W}}$ is isomorphic to the monoid algebra $\mathbb{Z}[M_n]$ with*

$$M_n = \Big\{(l_i) \in \mathbb{Z}_+^n \mid l_{n-1}+l_n \in 2\mathbb{Z} \quad \textit{and} \quad \tfrac{l_{n-1}+l_n}{2}\, n + l_{n-1} + \sum_{\substack{i\le n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}\Big\}$$

The isomorphism is given by

$$\begin{array}{ccc} \mathbb{Z}[M_n] & \xrightarrow{\sim} & \mathbb{Z}[D_n]^{\mathcal{W}} \\ \cup & & \cup \\ (l_1, l_2, \dots, l_n) & \longmapsto & \sigma_1^{l_1}\cdots\sigma_{n-2}^{l_{n-2}}\tau_-^{l_{n-1}}\tau_+^{l_n} \end{array}$$

The monoid M_n decomposes as $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n-2}{2} \rfloor} \oplus W$ with

$$W = \Big\{(k_i) \in \mathbb{Z}_+^{\lceil \frac{n+2}{2} \rceil} \mid k_1 + k_2 \in 2\mathbb{Z} \quad \textit{and} \quad \tfrac{k_1+k_2}{2}\, n + \sum_{i\ge 2} k_i \in 2\mathbb{Z}\Big\}$$

(b) ***Fundamental invariants for n even:*** *Put*

$$\pi_i = \begin{cases} \sigma_i^2 & \textit{for } i \textit{ odd} \\ \sigma_i & \textit{for } i \textit{ even} \end{cases} \quad (1 \le i \le n-2) \qquad \textit{and} \qquad \pi_{n-1} = \tau_-^2\,,\ \pi_n = \tau_+^2$$

Moreover, put

$$\gamma_i = \sigma_i\tau_-\tau_+ \quad \textit{for } 1 \le i \le n-2,\ i \textit{ odd}$$
$$\gamma_{i,j} = \sigma_i\sigma_j \qquad \textit{for } 1 \le i < j \le n-2 \textit{ both odd}$$

The above $\frac{1}{8}(n^2+6n)$ *elements generate the invariant algebra* $\mathbb{Z}[D_n]^{\mathcal{W}}$*, with the* π_i *serving as primary invariants.*

(c) ***Fundamental invariants for*** n ***odd:*** *Put*

$$\pi_i = \begin{cases} \sigma_i^2 & \textit{for } i \textit{ odd} \\ \sigma_i & \textit{for } i \textit{ even} \end{cases} \quad (1 \le i \le n-2) \qquad \textit{and} \qquad \pi_{n-1} = \tau_-^4\,,\ \pi_n = \tau_+^4$$

Moreover, put

$$\gamma_{i,j} = \sigma_i\sigma_j \quad \textit{for } 1 \le i < j \le n-2 \textit{ both odd}$$
$$\gamma_{n-1,n} = \tau_-\tau_+$$
$$\gamma_{i,n-1} = \sigma_i\tau_-^2 \quad \textit{for } 1 \le i \le n-2 \textit{ odd}$$
$$\gamma_{i,n} = \sigma_i\tau_+^2 \quad \textit{for } 1 \le i \le n-2 \textit{ odd}$$

The above $\frac{1}{8}(n^2+12n+3)$ *elements generate the invariant algebra* $\mathbb{Z}[D_n]^{\mathcal{W}}$*, with the* π_i *serving as primary invariants.*

Proof. (a) We need to describe the submonoid $D_n \cap \Lambda_+$ of $\Lambda_+ = \bigoplus_{i=1}^n \mathbb{Z}_+\varpi_i$. By [2, Planche IV] the root system of type D_n has the following fundamental weights with respect to the base $\{\alpha_i\}_1^n$ of the root system that was exhibited in Section 3.4.1:

$$\begin{aligned}
\varpi_i &= \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_i \qquad (1 \le i \le n-2) \\
&= \alpha_1 + 2\alpha_2 + \cdots + (i-1)\alpha_{i-1} + i(\alpha_i + \alpha_{i+1} + \cdots + \alpha_{n-2}) + \tfrac{1}{2}i(\alpha_{n-1} + \alpha_n) \\
\varpi_{n-1} &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-2} + \varepsilon_{n-1} - \varepsilon_n) \\
&= \tfrac{1}{2}(\alpha_1 + 2\alpha_2 + \cdots + (n-2)\alpha_{n-2} + \tfrac{1}{2}n\alpha_{n-1} + \tfrac{1}{2}(n-2)\alpha_n) \\
\varpi_n &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-2} + \varepsilon_{n-1} + \varepsilon_n) \\
&= \tfrac{1}{2}(\alpha_1 + 2\alpha_2 + \cdots + (n-2)\alpha_{n-2} + \tfrac{1}{2}(n-2)\alpha_{n-1} + \tfrac{1}{2}n\alpha_n)
\end{aligned}$$

In view of (3.12), an element $\sum_i l_i\varpi_i \in \Lambda_+$ $(l_i \in \mathbb{Z}_+)$ belongs to D_n if and only if the following two conditions are satisfied:

$$l_{n-1} + l_n \in 2\mathbb{Z} \tag{3.13}$$

and

$$\sum_{i=1}^{n-2} il_i + \tfrac{1}{2}(n-2)l_{n-1} + \tfrac{1}{2}nl_n \in 2\mathbb{Z} \tag{3.14}$$

Indeed, (3.13) is equivalent to the condition $\sum_i l_i\varpi_i \in \bigoplus_{i=1}^n \mathbb{Z}\varepsilon_i$, while (3.14) expresses the defining condition that $\sum_i z_i$ must be even in (3.12). Observe further that (3.14) can be rewritten as follows:

$$\tfrac{l_{n-1}+l_n}{2}\, n + l_{n-1} + \sum_{\substack{i\le n-2\\ i \text{ odd}}} l_i \in 2\mathbb{Z} \tag{3.15}$$

This yields the monoid M_n as well as the isomorphism

$$\begin{array}{ccc} M_n & \xrightarrow{\sim} & D_n \cap \Lambda_+ \\ \cup & & \cup \\ (l_1, l_2, \ldots, l_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} l_i\varpi_i \end{array}$$

The decomposition $M_n \cong \mathbb{Z}_+^{\lfloor \frac{n-2}{2} \rfloor} \oplus W$ is clear, because (3.14) imposes no condition on the $\lfloor \frac{n-2}{2} \rfloor$ components l_i for even $i \le n-2$. In the description of W, we have also relabeled l_n as k_1, l_{n-1} as k_2 etc.

To justify the indicated isomorphism $\mathbb{Z}[M_n] \xrightarrow{\sim} \mathbb{Z}[D_n]^{\mathcal{W}}$, we need to determine the $\mathcal{W}$-orbit sums $\mathsf{orb}(\varpi_i)$. The $\mathcal{W}$-orbit of $\varpi_i = \varepsilon_1+\varepsilon_2+\cdots+\varepsilon_i$ with $1 \le i \le n-2$ consists of all possible $\pm\varepsilon_{j_1} \pm \varepsilon_{j_2} \pm \cdots \pm \varepsilon_{j_i}$ with $j_1 < \cdots < j_i$. Therefore, the corresponding orbit sum evaluates to

$$\mathsf{orb}(\varpi_i) = \sigma_i$$

Finally, we have already pointed out before the statement of the theorem that

$$\mathsf{orb}(\varpi_n) = \tau_+ \qquad \text{and} \qquad \mathsf{orb}(\varpi_{n-1}) = \tau_-$$

This completes the proof of (a).

To obtain fundamental invariants for $\mathbb{Z}[D_n]^{\mathcal{W}}$, we determine the Hilbert basis for our monoid $M_n \cong D_n \cap \Lambda_+$ using the procedure described in Section 2.3.4. As in that section, we put

$$m_i = z_i\varpi_i \qquad (i = 1, 2, \ldots, n)$$

where z_i is the order of ϖ_i modulo D_n. It is easy to find the z_i for the fundamental weights ϖ_i:

$$z_i = \begin{cases} 1 & \text{if } i \text{ is even} \\ 2 & \text{if } i \text{ is odd} \end{cases} \qquad (1 \leq i \leq n-2) \tag{3.16}$$

and

$$z_{n-1} = z_n = \begin{cases} 2 & \text{if } n \text{ is even} \\ 4 & \text{if } n \text{ is odd} \end{cases} \tag{3.17}$$

This gives the elements $m_i = z_i\varpi_i$ $(i = 1, \ldots, n)$ in the Hilbert basis, which by (a) yield the fundamental invariants

$$\pi_i = \mathsf{orb}(\varpi_i)^{z_i}$$

in both (b) and (c).

As we have seen in Section 2.3.4, the remaining elements of the Hilbert basis of $D_n \cap \Lambda_+$ all belong to $D_n \cap K^\circ$, where $K^\circ = \left\{\sum_{i=1}^n t_i m_i \in \mathbb{E} \mid 0 \leq t_i < 1\right\}$. So we are looking for indecomposable elements of M having the form

$$(l_1, \ldots, l_n) = (t_1 z_1, \ldots, t_n z_n) \in \mathbb{Z}_+^n \quad \text{with } 0 \leq t_i < 1$$

and such that conditions (3.13) and (3.15) are satisfied. Since each $l_i \in \mathbb{Z}_+$, equations (3.16) and (3.17) yield the following restrictions on what l_i can be:

$$l_i = \begin{cases} 0 & \text{if } i \text{ is even} \\ 0 \text{ or } 1 & \text{if } i \text{ is odd} \end{cases} \qquad (1 \leq i \leq n-2) \tag{3.18}$$

and

$$l_{n-1}, l_n \in \begin{cases} \{0,1,2,3\} & \text{if } n \text{ is odd} \\ \{0,1\} & \text{if } n \text{ is even} \end{cases} \tag{3.19}$$

First, suppose that $l_{n-1} = l_n = 0$. Then (3.13) certainly holds and condition (3.15) becomes $\sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$. Since the l_i in this sum are either 0 or 1 by (3.18),

condition (3.15) just says that there must be an even number of $l_i = 1$ for odd $i \leq n-2$. The corresponding indecomposable elements of M_n are obtained by taking just two of these $l_i = 1$. In sum, we have obtained the following indecomposable elements of $D_n \cap \Lambda_+$:

$$m_{i,j} = \varpi_i + \varpi_j \qquad (1 \leq i < j \leq n-2 \text{ and } i, j \text{ both odd})$$

The element $m_{i,j}$ yields the fundamental invariants $\gamma_{i,j} = \sigma_i \sigma_j = \mathsf{orb}(\varpi_i)\,\mathsf{orb}(\varpi_i)$ in (b) and (c). Note that

$$\gamma_{i,j}^2 = \pi_i \pi_j \tag{3.20}$$

From now on, we assume that l_{n-1}, l_n are not both zero. For this we start with

Case 1: n is even. Since $l_{n-1} + l_n \in 2\mathbb{Z}$ by (3.13), condition (3.19) says we must have $l_{n-1} = l_n = 1$. Now (3.15) becomes

$$n + 1 + \sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$$

with all $l_i \in \{0, 1\}$ by (3.18). To satisfy the above condition we must have an odd number of $l_i = 1$. Taking exactly one nonzero $l_i = 1$ gives the remaining indecomposable elements for M_n:

$$b_i = \varpi_i + \varpi_{n-1} + \varpi_n$$

Indeed, any n-tuple $(l_1, \ldots, l_{n-2}, 1, 1) \in M_n$ with $2k+1$ of the $l_i = 1$ may be written as a sum $(l_1, \ldots, l_{n-2}, 1, 1) = (l'_1, \ldots, l'_{n-2}, 0, 0) + (l_1, \ldots, l_{n-2}, 1, 1)$ with $2k$ of the $l'_i = 1$ and exactly one $l_j = 1$ $(j \neq i)$. Since the second summand corresponds to b_j and the first one can be written in terms of the Hilbert basis elements $m_{r,s}$ constructed earlier, we have found the complete Hilbert basis of M_n. By isomorphism in (a), the basis element b_i yields the fundamental invariant $\gamma_i = \sigma_i \tau_- \tau_+$ giving a total of $\frac{1}{8}(n^2 + 6n)$ basis elements for our monoid, and hence fundamental invariants, when n is even. Note that

$$\gamma_i^2 = \pi_i \pi_{n-1} \pi_n \tag{3.21}$$

Together with (3.20), this relation shows that the invariant algebra $\mathbb{Z}[D_n]^{\mathcal{W}}$ is integral over the subalgebra $\mathbb{Z}[\pi_1, \ldots, \pi_n]$; so the π_i form a set of primary invariants.

Case 2: n is odd. By (3.19), if either l_{n-1} or l_n are zero, the other must be 2 to satisfy (3.13). This leads to the possibilities $(l_{n-1}, l_n) = (2, 0)$ or $(l_{n-1}, l_n) = (0, 2)$. In either case (3.15) becomes

$$n + 2 + \sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$$

with all $l_i \in \{0, 1\}$ by (3.18). Therefore, we must have an odd number of $l_i = 1$. As above, indecomposable monoid elements are obtained by taking one $l_i = 1$ and all others zero. So we have indecomposable elements

$$m_{i,n-1} = \varpi_i + 2\varpi_{n-1} \qquad \text{and} \qquad m_{i,n} = \varpi_i + 2\varpi_n$$

giving fundamental invariants $\gamma_{i,n-1} = \sigma_i \tau_-^2$ and $\gamma_{i,n} = \sigma_i \tau_+^2$. Now assume that neither l_{n-1} nor l_n are zero; so l_{n-1} and l_n belong to $\{1, 2, 3\}$ by (3.19) and their sum must be even by (3.13). First assume that $l_{n-1} = l_n$. Then (3.15) becomes

$$l_n(n+1) + \sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$$

Since $n + 1$ is even, this amounts to the sum $\sum l_i$ being even. The only indecomposable element of M_n resulting from this situation is obtained by letting all $l_i = 0$ for $1 \leq i \leq n - 2$ and $l_{n-1} = l_n = 1$, which gives the Hilbert basis element

$$m_{n-1,n} = \varpi_{n-1} + \varpi_n$$

and the corresponding fundamental invariant, $\gamma_{n-1,n} = \tau_- \tau_+$.

Finally, if we allow one of l_{n-1}, l_n to be 1 and the other 3, then (3.15) gives one of the two equations:

$$2n + 1 + \sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$$

$$2n + 3 + \sum_{\substack{i \leq n-2 \\ i \text{ odd}}} l_i \in 2\mathbb{Z}$$

In either case, we must have an odd number of nonzero $l_i = 1$ in the sum to satisfy this condition. It follows that we can write this as $m + m'$ where m has an odd number of $l_i = 1$ and $l_{n-1} = 2$, (or $l_n = 2$, depending on which we took to be 3 above), and m' is the indecomposable element $(0, \ldots, 0, 1, 1)$. This completes our Hilbert basis when n is odd, giving a total of $\frac{1}{8}(n^2 + 12n + 3)$ indecomposable elements. Again, we see that the squares of the fundamental invariants $\gamma_{i,j}, \gamma_{i,n-1}$ and $\gamma_{i,n}$ with $i \leq n-2$ as well as the fourth power of $\gamma_{n-1,n}$ belong to the subalgebra $\mathbb{Z}[\pi_1, \ldots, \pi_n]$ of $\mathbb{Z}[D_n]^{\mathcal{W}}$; so the π_i form a system of primary invariants. This completes the proof. □

We remark that one can also use the description in Proposition 2.3.5 to write down a Hironaka decomposition for $\mathbb{Z}[D_n]^{\mathcal{W}}$, though it is not particularly nice or compact so we omit it here.

Example 3.4.2. For $n = 3$, our fundamental weights are

$$\begin{aligned}
\varpi_1 &= \varepsilon_1 = \alpha_1 + \tfrac{1}{2}(\alpha_2 + \alpha_3) \\
\varpi_2 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 - \varepsilon_3) = \tfrac{1}{2}(\alpha_1 + \tfrac{3}{2}\alpha_2 + \tfrac{1}{2}\alpha_3) \\
\varpi_3 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3) = \tfrac{1}{2}(\alpha_1 + \tfrac{1}{2}\alpha_2 + \tfrac{3}{2}\alpha_3)
\end{aligned}$$

The theorem above then gives the following Hilbert basis for $M_3 \cong \Lambda_+ \cap D_3$, in the same notation that was used in the proof:

$$\begin{array}{ccc}
m_1 = 2\varpi_1 & m_2 = 4\varpi_2 & m_3 = 4\varpi_3 \\
m_{2,3} = \varpi_2 + \varpi_3 & m_{1,2} = \varpi_1 + 2\varpi_2 & m_{1,3} = \varpi_1 + 2\varpi_3
\end{array}$$

Using the notation above, we obtain the following fundamental invariants for $\mathbb{Z}[D_3]^{\mathcal{W}}$:

$$\begin{aligned}
\pi_1 &= \sigma_1^2 = (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1})^2 \\
\pi_2 &= \tau_-^4 = (\mathsf{orb}((x_1x_2x_3^{-1})^{\frac{1}{2}}))^4 \\
&= ((x_1x_2x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3^{-1})^{\frac{1}{2}})^4 \\
\pi_3 &= \tau_+^4 = (\mathsf{orb}((x_1x_2x_3)^{\frac{1}{2}}))^4 \\
&= ((x_1x_2x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3^{-1})^{\frac{1}{2}})^4 \\
\gamma_{2,3} &= \tau_-\tau_+ \\
&= [(x_1x_2x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3^{-1})^{\frac{1}{2}})^4]\cdot \\
&\quad [(x_1x_2x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3^{-1})^{\frac{1}{2}}] \\
\gamma_{1,2} &= \sigma_1\tau_-^2 \\
&= (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1})((x_1x_2x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3^{-1})^{\frac{1}{2}})^2 \\
\gamma_{1,3} &= \sigma_1\tau_+^2 \\
&= (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1})((x_1x_2x_3)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3)^{\frac{1}{2}} + (x_1x_2^{-1}x_3^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3^{-1})^{\frac{1}{2}})^2
\end{aligned}$$

As noted at the beginning of this section, $\mathbb{Z}[D_3]^{\mathcal{W}} \cong \mathbb{Z}[A_3]^{\mathcal{S}_4}$. This algebra was already discussed in detail in Section 3.2.3, with the aid of the computer algebra systems CoCoA and MAGMA. Though it is not immediately obvious how to consolidate the above description with our earlier one, note that we did obtain the same number of fundamental invariants with our new approach.

Example 3.4.3. For $n = 4$, our fundamental weights are

$$\begin{aligned}
\varpi_1 &= \varepsilon_1 = \alpha_1 + \alpha_2 + \tfrac{1}{2}(\alpha_3 + \alpha_4) \\
\varpi_2 &= \varepsilon_1 + \varepsilon_2 = \alpha_1 + 2\alpha_2 + \alpha_3 + \alpha_4 \\
\varpi_3 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4) = \tfrac{1}{2}(\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4) \\
\varpi_4 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4) = \tfrac{1}{2}(\alpha_1 + 2\alpha_2 + \alpha_3 + 2\alpha_4)
\end{aligned}$$

Following the method in the proof of Theorem 3.4.1, we find the following Hilbert basis for $M_4 \cong \Lambda_+ \cap D_4$:

$$m_1 = 2\varpi_1,\ m_2 = \varpi_2,\ m_3 = 2\varpi_3,\ m_4 = 2\varpi_4,\ b_1 = \varpi_1 + \varpi_3 + \varpi_4$$

Using the notation above, we obtain the following fundamental invariants for $\mathbb{Z}[D_4]^{\mathcal{W}}$:

$$\pi_1 = \sigma_1^2 = (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1} + x_4 + x_4^{-1})^2$$

$$\pi_2 = \sigma_2 = \sum_{i<j} x_i x_j + \sum_{i\neq j} x_i^{-1} x_j + \sum_{i<j} x_i^{-1} x_j^{-1}$$

$$\begin{aligned}\pi_3 = \tau_-^2 &= (\mathsf{orb}((x_1x_2x_3x_4^{-1})^{\frac{1}{2}}))^2 \\ &= ((x_1x_2x_3x_4^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2x_3x_4)^{\frac{1}{2}} + (x_1x_2^{-1}x_3x_4)^{\frac{1}{2}} + (x_1x_2x_3^{-1}x_4)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3x_4^{-1})^{\frac{1}{2}} \\ &+ (x_1^{-1}x_2x_3^{-1}x_4^{-1})^{\frac{1}{2}} + (x_1x_2^{-1}x_3^{-1}x_4^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3^{-1}x_4)^{\frac{1}{2}})^2\end{aligned}$$

$$\begin{aligned}\pi_4 = \tau_+^2 &= (\mathsf{orb}((x_1x_2x_3x_4)^{\frac{1}{2}}))^2 \\ &= ((x_1x_2x_3x_4)^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3x_4)^{\frac{1}{2}} + (x_1^{-1}x_2x_3^{-1}x_4)^{\frac{1}{2}} + (x_1^{-1}x_2x_3x_4^{-1})^{\frac{1}{2}} + (x_1x_2^{-1}x_3^{-1}x_4)^{\frac{1}{2}} \\ &+ (x_1x_2^{-1}x_3x_4^{-1})^{\frac{1}{2}} + (x_1x_2x_3^{-1}x_4^{-1})^{\frac{1}{2}} + (x_1^{-1}x_2^{-1}x_3^{-1}x_4^{-1})^{\frac{1}{2}})^2\end{aligned}$$

$$\begin{aligned}\gamma_1 &= \sigma_1\tau_-\tau_+ \\ &= (x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1} + x_4 + x_4^{-1})(\mathsf{orb}(x_1x_2x_3x_4^{-1}))(\mathsf{orb}(x_1x_2x_3x_4))\end{aligned}$$

3.4.3 Class Group

We will use Theorem 2.4.2 to calculate $\mathrm{Cl}(\mathbb{Z}[D_n]^{\mathcal{W}})$ for $n \geq 4$. To this end, we must first find $\mathcal{D}$, the group of diagonalizable reflections in $\mathcal{W}$. But, as we noted earlier, D_n and C_n are the same lattice and $\mathcal{W}(\mathsf{D}_n)$ is a subgroup of $\mathcal{W}(\mathsf{C}_n)$. Since there are no nonidentity elements of $\mathcal{W}(\mathsf{C}_n)$ that act as a diagonalizable reflection on $D_n = C_n$ by Lemma 3.3.4 , we conclude that $\mathcal{D} = \{1\}$ for D_n as well. Now Theorem 2.4.2(a) gives

$$\mathrm{Cl}(\mathbb{Z}[D_n]^{\mathcal{W}}) \cong H^1(\mathcal{W}, C_n) \cong \Lambda/D_n$$

where Λ is the weight lattice of the root system of type D_n. The factor Λ/D_n is known to be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for n even and $\mathbb{Z}/4\mathbb{Z}$ for n odd; see [2, Planche III, (VIII)]. Let us summarize the result in the following proposition, for which we will give a direct proof using invariants below.

Proposition 3.4.4. $\mathrm{Cl}(\mathbb{Z}[D_n]^{\mathcal{W}}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } n \textit{ is even} \\ \mathbb{Z}/4\mathbb{Z} & \textit{if } n \textit{ is odd} \end{cases}$

Proof. As with the previous two root lattices, we will calculate $(D_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{W}}$ to find our class group. The calculations here will be similar to those in the proof of

Proposition 3.3.5. As in that proof, any $z \in D_n \otimes \mathbb{Q}/\mathbb{Z}$ has a unique expression of the form

$$z = \sum_{i=1}^{n} \overline{q}_i \alpha_i$$

with α_i as in Section 3.4.1 and $\overline{q}_i \in \mathbb{Q}/\mathbb{Z}$. The group $\mathcal{W} = (\mathcal{D}_n \cap \mathrm{SL}_n(\mathbb{Z})) \rtimes \mathcal{S}_n$ is generated by the permutations $\sigma = (1\,2\,\ldots\,n), \tau = (1\,2) \in \mathcal{S}_n$ together with the diagonal matrix $\delta \in \mathcal{D}_n$ having -1 in positions $(1,1)$ and $(2,2)$ with all other diagonal entries being 1. Thus, $z \in (D_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{W}}$ if and only if the following three conditions are satisfied:

$$\delta(z) = z\,,\ \sigma(z) = z \qquad \text{and} \qquad \tau(z) = z$$

Straightforward computations give the following formulas:

$$\delta(z) = (-\overline{q}_1)\alpha_1 + (-\overline{q}_2)\alpha_2 + \sum_{i=3}^{n-2}(\overline{q}_i - 2\overline{q}_2)\alpha_i + (\overline{q}_{n-1} - \overline{q}_2)\alpha_{n-1} + (\overline{q}_n - \overline{q}_2)\alpha_n$$

$$\sigma(z) = (\overline{q}_n - \overline{q}_{n-1})\alpha_1 + \sum_{i=2}^{n-2}(\overline{q}_{i-1} + \overline{q}_n - \overline{q}_{n-1})\alpha_i + (\overline{q}_{n-2} - \overline{q}_{n-1})\alpha_{n-1} + \overline{q}_n\alpha_n$$

$$\tau(z) = (\overline{q}_2 - \overline{q}_1)\alpha_1 + \sum_{i=2}^{n} \overline{q}_i \alpha_i$$

Thus, the condition $\delta(z) = z$ is equivalent to

$$2\overline{q}_1 = 0 \qquad \text{and} \qquad \overline{q}_2 = 0 \tag{3.22}$$

while $\sigma(z) = z$ is equivalent to

$$\overline{q}_n - \overline{q}_{n-1} = \overline{q}_1\,,\ \overline{q}_{i-1} + \overline{q}_1 = \overline{q}_i\ (2 \le i \le n-2) \quad \text{and} \quad \overline{q}_{n-2} = 2\overline{q}_{n-1} \tag{3.23}$$

Finally, $\tau(z) = z$ amounts to the condition $\overline{q}_2 - \overline{q}_1 = \overline{q}_1$, which already follows from (3.22). Conditions (3.22) and (3.23) are readily seen to be equivalent to the following set of conditions

$$2\overline{q}_1 = 0\,, \quad \overline{q}_{n-2} = 2\overline{q}_{n-1}\,, \quad \overline{q}_n = \overline{q}_1 + \overline{q}_{n-1}$$

and

$$\overline{q}_i = \begin{cases} 0 & \text{for } i \le n-2,\ i \text{ even} \\ \overline{q}_1 & \text{for } i \le n-2,\ i \text{ odd} \end{cases}$$

When n is even, then these conditions imply that $0 = \overline{q}_{n-2} = 2\overline{q}_{n-1}$. Thus, in this case, the element $z \in D_n \otimes \mathbb{Q}/\mathbb{Z}$ is $\mathcal{W}$-invariant if and only if

$$z = \overline{q}_1\Big(\sum_{\substack{i\leq n-2\\ i \text{ odd}}} \alpha_i\Big) + \overline{q}_{n-1}\alpha_{n-1} + (\overline{q}_1 + \overline{q}_{n-1})\alpha_n \quad \text{with} \quad 2\overline{q}_1 = 2\overline{q}_{n-1} = 0$$

Therefore, the invariant group $(D_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{W}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if n is even.

For odd n, we have $\overline{q}_1 = \overline{q}_{n-2} = 2\overline{q}_{n-1}$ and $z \in \big(D_n \otimes \mathbb{Q}/\mathbb{Z}\big)^{\mathcal{W}}$ if and only if

$$z = 2\overline{q}_{n-1}\Big(\sum_{\substack{i\leq n-2\\ i \text{ odd}}} \alpha_i\Big) + \overline{q}_{n-1}\alpha_{n-1} + 3\overline{q}_{n-1}\alpha_n \quad \text{with} \quad 4\overline{q}_{n-1} = 0$$

This shows that $(D_n \otimes \mathbb{Q}/\mathbb{Z})^{\mathcal{W}}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if n is odd, thereby finishing the proof of the proposition. $\square$

CHAPTER 4

Multiplicative Invariants of Exceptional Root Lattices

Of the five exceptional root systems, the root lattices of $\mathsf{G}_2, \mathsf{F}_4$, and E_8 are all identical to their weight lattices; see Bourbaki [2, Planches VII, VIII, IX]. Thus, by Bourbaki's Theorem, we know that the multiplicative invariant algebras are isomorphic to polynomial rings with a system of variables given by the orbit sums of the fundamental weights. This leaves only the types E_6 and E_7 to consider; the multiplicative invariant algebras of the root lattices for these types are computed below. Because the Weyl groups in question are very large, we will use Theorem 2.3.3 and Proposition 2.3.5 to calculate the multiplicative invariant algebras. Throughout, we follow the notations of [2, Planches V and VI].

4.1 Type E_6

4.1.1 Root system, root lattice and Weyl group

Here, $\mathbb{E}$ is the subspace of $\mathbb{R}^8$ that is orthogonal to $\varepsilon_6 - \varepsilon_7$ and to $\varepsilon_7 + \varepsilon_8$. The set of roots is the subset of $\mathbb{E}$ that is given by

$$\Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \le i < j \le 5\} \\ \cup\ \{\pm\tfrac{1}{2}(\varepsilon_8 - \varepsilon_7 - \varepsilon_6 + \sum_{i=1}^{5}(-1)^{\nu(i)}\varepsilon_i) \mid \sum_{i=1}^{5}\nu(i) \in 2\mathbb{Z}\} \quad (4.1)$$

Here $\nu(i) \in \{0, 1\}$. Thus, there are $4 \cdot \binom{5}{2} + 2^5 = 72$ roots. A base for this root system is given by

$$\alpha_1 = \tfrac{1}{2}(\varepsilon_1 + \varepsilon_8) - \tfrac{1}{2}(\varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6 + \varepsilon_7)$$
$$\alpha_2 = \varepsilon_1 + \varepsilon_2$$
$$\alpha_i = \varepsilon_{i-1} - \varepsilon_{i-2} \qquad (i = 3, \ldots, 6)$$

The root lattice of E_6 will be denoted by E_6; so $E_6 = \bigoplus_{i=1}^{6} \mathbb{Z}\alpha_i$.

The Weyl group $\mathcal{W} = \mathcal{W}(\mathsf{E}_6)$ has order $2^7\,3^4\,5 = 51\,840$. The group $\mathcal{W}$ has a number of interesting realizations; see Bourbaki [2, Exercise 2 on page 228] and Humphreys [14, Section 2.12]. For example, $\mathcal{W}$ can be described as the automorphism group of the famous configuration of 27 lines on a cubic surface. The rotation subgroup $\mathcal{W}^+ = \{w \in \mathcal{W} \mid \det w = 1\}$ is isomorphic to the projective symplectic group $\mathrm{PSp}_4(3)$ over $\mathbb{F}_3$; the latter group is the unique simple group of order $25\,920$. See the *Atlas of Finite Groups* [7]. Denoting the standard inner product of $\mathbb{R}^8$ by $(\,.\,,\,.\,)$ as usual, the quadratic form $\frac{1}{2}(x, x)$ yields a non-degenerate quadratic form on the 6-dimensional $\mathbb{F}_2$-vector space $\overline{E}_6 = E_6/2E_6$. The action of $\mathcal{W}$ on $\overline{E}_6$ preserves this form, and this induces an isomorphism

$$\boxed{\mathcal{W} \cong O_6(2)} \quad (4.2)$$

in the notation of [7].

4.1.2 Multiplicative $\mathcal{W}$-invariants

By Theorem 2.3.3 we know that

$$\mathbb{Z}[E_6]^{\mathcal{W}} \cong \mathbb{Z}[\Lambda_+ \cap E_6]$$

where $\Lambda_+ = \bigoplus_{i=1}^{6} \mathbb{Z}_+ \varpi_i$ and ϖ_i are the fundamental weights with respect to the above base $\{\alpha_i\}_1^6$ of the root system. Explicitly,

$$\begin{aligned}
\varpi_1 &= \tfrac{2}{3}(\varepsilon_8 - \varepsilon_7 - \varepsilon_6) = \tfrac{1}{3}(4\alpha_1 + 3\alpha_2 + 5\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6) \\
\varpi_2 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 - \varepsilon_6 - \varepsilon_7 + \varepsilon_8) \\
&= \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6 \\
\varpi_3 &= \tfrac{5}{6}(\varepsilon_8 - \varepsilon_7 - \varepsilon_6) + \tfrac{1}{2}(-\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5) \\
&= \tfrac{1}{3}(5\alpha_1 + 6\alpha_2 + 10\alpha_3 + 12\alpha_4 + 8\alpha_5 + 4\alpha_6) \\
\varpi_4 &= \varepsilon_3 + \varepsilon_4 + \varepsilon_5 - \varepsilon_6 - \varepsilon_7 + \varepsilon_8 \\
&= 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6 \\
\varpi_5 &= \tfrac{2}{3}(\varepsilon_8 - \varepsilon_7 - \varepsilon_6) + \varepsilon_4 + \varepsilon_5 \\
&= \tfrac{1}{3}(4\alpha_1 + 6\alpha_2 + 8\alpha_3 + 12\alpha_4 + 10\alpha_5 + 5\alpha_6) \\
\varpi_6 &= \tfrac{1}{3}(\varepsilon_8 - \varepsilon_7 - \varepsilon_6) + \varepsilon_5 \\
&= \tfrac{1}{3}(2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6)
\end{aligned}$$

In order to further describe the invariant algebra $\mathbb{Z}[E_6]^{\mathcal{W}}$, we need to analyze the monoid

$$M = \Lambda_+ \cap E_6$$

Hilbert basis of M. Let $z \in M$ and write $z = l_1\varpi_1 + \cdots + l_6\varpi_6$ with $l_i \in \mathbb{Z}_+$. Then we know that the coefficients of each α_i in our base must be integral. This

gives the following conditions:

$$\begin{aligned}
\text{coefficient of } \alpha_1 : &\quad \tfrac{4}{3}l_1 + l_2 + \tfrac{5}{3}l_3 + 2l_4 + \tfrac{4}{3}l_5 + \tfrac{2}{3}l_6 \in \mathbb{Z} \\
\alpha_2 : &\quad l_1 + 2l_2 + 2l_3 + 3l_4 + 2l_5 + l_6 \in \mathbb{Z} \\
\alpha_3 : &\quad \tfrac{5}{3}l_1 + 2l_2 + \tfrac{10}{3}l_3 + 4l_4 + \tfrac{8}{3}l_5 + \tfrac{4}{3}l_6 \in \mathbb{Z} \\
\alpha_4 : &\quad 2l_1 + 3l_2 + 4l_3 + 6l_4 + 4l_5 + 2l_6 \in \mathbb{Z} \\
\alpha_5 : &\quad \tfrac{4}{3}l_1 + 2l_2 + \tfrac{8}{3}l_3 + 4l_4 + \tfrac{10}{3}l_5 + \tfrac{5}{3}l_6 \in \mathbb{Z} \\
\alpha_6 : &\quad \tfrac{2}{3}l_1 + l_2 + \tfrac{4}{3}l_3 + 2l_4 + \tfrac{5}{3}l_5 + \tfrac{4}{3}l_6 \in \mathbb{Z}
\end{aligned}$$

Note that the conditions at α_2 and α_4 are automatically satisfied for any $(l_1, \ldots, l_6) \in \mathbb{Z}_+^6$, and the remaining conditions do not impose any restrictions on l_2 and l_4. Therefore, our system of conditions can be rewritten as follows:

$$\begin{aligned}
&4l_1 + 5l_3 + 4l_5 + 2l_6 \in 3\mathbb{Z} \qquad && 5l_1 + 10l_3 + 8l_5 + 4l_6 \in 3\mathbb{Z} \\
&4l_1 + 8l_3 + 10l_5 + 5l_6 \in 3\mathbb{Z} \qquad && 2l_1 + 4l_3 + 5l_5 + 4l_6 \in 3\mathbb{Z}
\end{aligned}$$

Finally, reducing mod 3 we see that all four conditions are equivalent to the single condition $l_1 + 2l_3 + l_5 + 2l_6 \in 3\mathbb{Z}$. Thus, we are left with the following description of our monoid:

$$M = \Lambda_+ \cap E_6 \cong \{(l_1, \ldots, l_6) \in \mathbb{Z}_+^6 \mid l_1 + 2l_3 + l_5 + 2l_6 \in 3\mathbb{Z}\} \cong \mathbb{Z}_+^2 \oplus W$$

where

$$W = \{(k_1, k_2, k_3, k_4) \in \mathbb{Z}_+^4 \mid k_1 + 2k_2 + k_3 + 2k_4 \in 3\mathbb{Z}\}$$

A Hilbert basis for the monoid W can be obtained by using using the method described above in Proposition 2.3.5 or by simply using CoCoA as in Section 3.2.3. To carry out the latter approach, we will use the following description of the monoid W:

$$W = \left\{(k_1, k_2, k_3, k_4, x) \in \mathbb{Z}_+^5 \mid k_1 + 2k_2 + k_3 + 2k_4 - 3x = 0\right\}$$

Thus, W is the kernel in $\mathbb{Z}_+^5$ of the matrix $A = [1, 2, 1, 2, -3]$, which can be obtained with CoCoA as follows:

```
A:=Mat([[1,2,1,2,-3]]);
HilbertBasisKer(A);

[[0, 0, 1, 1, 1], [1, 0, 0, 1, 1], [0, 1, 1, 0, 1],
[1, 1, 0, 0, 1], [0, 0, 3, 0, 1], [1, 0, 2, 0, 1],
[2, 0, 1, 0, 1], [3, 0, 0, 0, 1], [0, 0, 0, 3, 2],
[0, 1, 0, 2, 2], [0, 2, 0, 1, 2], [0, 3, 0, 0, 2]]
```

Deleting the auxiliary fifth coordinate and reordering the above CoCoA output, we see that the Hilbert basis of W is given by the following elements:

$$\begin{array}{llll} m_1 = (3,0,0,0) & m_2 = (0,3,0,0) & m_3 = (0,0,3,0) & m_4 = (0,0,0,3) \\ m_5 = (1,1,0,0) & m_6 = (1,0,0,1) & m_7 = (0,1,1,0) & m_8 = (0,0,1,1) \\ m_9 = (1,0,2,0) & m_{10} = (0,1,0,2) & m_{11} = (0,2,0,1) & m_{12} = (2,0,1,0) \end{array} \tag{4.3}$$

In order to obtain the Hilbert basis for M, we need to convert each of the above 4-tuples $(k_1, \ldots, k_4) \in \mathbb{Z}_+^4$ into the a 6-tuple $(k_1, 0, k_2, 0, k_3, k_4)$, and we also need to add the 6-tuples

$$(0,1,0,0,0,0) \qquad \text{and} \qquad (0,0,0,1,0,0) \tag{4.4}$$

to the list.

Fundamental invariants. By Theorem 2.3.3, the isomorphism $\mathbb{Z}[M] \xrightarrow{\sim} \mathbb{Z}[E_6]^{\mathcal{W}}$ is given by $(l_1, \ldots, l_6) \mapsto \prod_{i=1}^6 \mathsf{orb}(\varpi_i)^{l_i}$. In view of the preceding paragraph,

$$\mathbb{Z}[M] \cong \mathbb{Z}[W] \otimes \mathbb{Z}[t_1, t_2]$$

where the variables t_1 and t_2 correspond to the Hilbert basis elements in (4.4). These give the following two fundamental invariants that are algebraically independent from each other and all other fundamental invariants:

$$\mathsf{orb}(\varpi_2) \qquad \text{and} \qquad \mathsf{orb}(\varpi_4)$$

The remaining Hilbert basis elements (k_1, k_2, k_3, k_4) from (4.3) give 12 additional fundamental invariants

$$\mathsf{orb}(\varpi_1)^{k_1}\, \mathsf{orb}(\varpi_3)^{k_2}\, \mathsf{orb}(\varpi_5)^{k_3}\, \mathsf{orb}(\varpi_6)^{k_4}$$

In view of the size of the Weyl group $\mathcal{W}$, it is not feasible or useful to explicitly write out these orbit sums.

Relations. Relations between the 12 fundamental invariants coming from (4.3), and hence a presentation of the invariant algebra $\mathbb{Z}[E_6]^{\mathcal{W}}$, can be obtained by the method of Section 3.2.3 for $n = 4$. In detail, we need 12 variables, one for each of the Hilbert basis elements m_i, and 4 extra variables for the embedding $M \hookrightarrow \mathbb{Z}_+^4$. Here is the MAGMA computation:

```
> Z := IntegerRing();
> S<a,b,c,d,x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12>:=
      PolynomialRing(Z,16);
> I:=ideal<S|x1-a^3,x2-b^3,x3-c^3,x4-d^3,x5-a*b,x6-a*d,
      x7-b*c,x8-c*d,x9-a*c^2,x10-b*d^2,x11-b^2*d,x12-a^2*c>;
> EliminationIdeal(I,4);
Ideal of Polynomial ring of rank 16 over Integer Ring
Order: Lexicographical
Variables: a, b, c, d, x1, x2, x3, x4, x5, x6, x7, x8, x9,
      x10, x11, x12
Basis:
[
    x7*x10 - x8*x11,
    x6*x9 - x8*x12,
    x5*x10 - x6*x11,
    x5*x9 - x7*x12,
    x5*x8 - x6*x7,
    x6*x7*x8 - x9*x10,
    x6*x7^2 - x9*x11,
    x6^2*x7 - x10*x12,
    x5*x6*x7 - x11*x12,
    x4*x12 - x6^2*x8,
    x4*x11 - x10^2,
    x4*x9 - x6*x8^2,
    x4*x7 - x8*x10,
    x4*x5 - x6*x10,
    x3*x12 - x9^2,
    x3*x11 - x7^2*x8,
    x3*x10 - x7*x8^2,
    x3*x6 - x8*x9,
    x3*x5 - x7*x9,
```

```
    x3*x4 - x8^3,
    x2*x12 - x5^2*x7,
    x2*x10 - x11^2,
    x2*x9 - x5*x7^2,
    x2*x8 - x7*x11,
    x2*x6 - x5*x11,
    x2*x4 - x10*x11,
    x2*x3 - x7^3,
    x1*x11 - x5^2*x6,
    x1*x10 - x5*x6^2,
    x1*x9 - x12^2,
    x1*x8 - x6*x12,
    x1*x7 - x5*x12,
    x1*x4 - x6^3,
    x1*x3 - x9*x12,
    x1*x2 - x5^3
]
```

4.1.3 Class Group

Using the description above along with Theorem 2.4.2, we can find the class group for the invariant algebra $\mathbb{Z}[E_6]^{\mathcal{W}}$. We know that the Weyl group $\mathcal{W} \cong O_6(2)$ contains a simple subgroup of index 2, which is its unique nontrivial normal subgroup. It follows that the subgroup of diagonalizable reflections, $\mathcal{D}$, is trivial. Hence, by Theorem 2.4.2(a), the class group is isomorphic to the factor Λ/L. This group is known [2, (VIII) in Planche V]:

$$\boxed{\mathrm{Cl}(\mathbb{Z}[E_6]^{\mathcal{W}}) \cong \mathbb{Z}/3\mathbb{Z}}$$

4.2 Type E_7

4.2.1 Root system, root lattice and Weyl group

Here, $\mathbb{E}$ is the subspace of $\mathbb{R}^8$ that is orthogonal $\varepsilon_7 + \varepsilon_8$. The set of roots is

$$\Phi = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \le i < j \le 6\} \quad \cup \quad \{\pm(\varepsilon_7 - \varepsilon_8)\}$$
$$\cup \quad \{\tfrac{1}{2}(\varepsilon_7 - \varepsilon_8 + \sum_{i=1}^{6}(-1)^{\nu(i)}\varepsilon_i \mid \sum_{i=1}^{8}\nu(i) \text{ odd}\} \quad (4.5)$$

A base for this root system is given by

$$\alpha_1 = \tfrac{1}{2}(\varepsilon_1 + \varepsilon_8) - \tfrac{1}{2}(\varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6 + \varepsilon_7)$$
$$\alpha_2 = \varepsilon_1 + \varepsilon_2$$
$$\alpha_i = \varepsilon_{i-1} - \varepsilon_{i-2} \qquad (i = 3, \ldots, 7)$$

So our root lattice is $E_7 = \bigoplus_{i=1}^{7} \mathbb{Z}\alpha_i$.

The Weyl group for E_7 is the direct product of $\mathbb{Z}/2\mathbb{Z}$ and the unique simple group of order $1\,451\,520$ (which can be described as $\mathrm{PSp}_6(2)$).

The Weyl group $\mathcal{W} = \mathcal{W}(\mathsf{E}_7)$ has order $2^{10}\,3^4\,5\,7 = 2\,903\,040$. By Bourbaki [2, Exercise 3 on page 229] (see also Humphreys [14, Section 2.12]), there is an isomorphism of groups

$$\boxed{\mathcal{W} \cong \{\pm 1\} \times O_7(2)}$$

which arises similar to the earlier description of $\mathcal{W}(\mathsf{E}_6)$: the form $\frac{1}{2}(x, x)$ yields a non-degenerate quadratic form on the 7-dimensional $\mathbb{F}_2$-vector space $E_7/2E_7$, and this form is preserved by the action of $\mathcal{W}$. The restriction of the action to the rotation subgroup $\mathcal{W}^+ = \{w \in \mathcal{W} \mid \det w = 1\}$ is an isomorphism $\mathcal{W}^+ \cong O_7(2)$, and the kernel of the action is $\{\pm 1\}$. The latter group $O_7(2)$ is the unique simple group of order $1\,451\,520$.

4.2.2 Multiplicative $\mathcal{W}$-invariants

We follow the outline of our treatment of type E_6. First, we find a Hilbert basis for the monoid

$$M = \Lambda_+ \cap E_7$$

First we list the fundamental weights with repeat to the above base $\{\alpha_i\}$:

$$\begin{aligned}
\varpi_1 &= \varepsilon_8 - \varepsilon_7 = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7 \\
\varpi_2 &= \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6 - 2\varepsilon_7 + 2\varepsilon_8) \\
&= \tfrac{1}{2}(4\alpha_1 + 7\alpha_2 + 8\alpha_3 + 12\alpha_4 + 9\alpha_5 + 6\alpha_6 + 3\alpha_7) \\
\varpi_3 &= \tfrac{1}{2}(-\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6 - 3\varepsilon_7 + 3\varepsilon_8) \\
&= 3\alpha_1 + 4\alpha_2 + 6\alpha_3 + 8\alpha_4 + 6\alpha_5 + 4\alpha_6 + 2\alpha_7 \\
\varpi_4 &= \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6 + 2(\varepsilon_8 - \varepsilon_7) \\
&= 4\alpha_1 + 6\alpha_2 + 8\alpha_3 + 12\alpha_4 + 9\alpha_5 + 6\alpha_6 + 3\alpha_7 \\
\varpi_5 &= \varepsilon_4 + \varepsilon_5 + \varepsilon_6 + \tfrac{3}{2}(\varepsilon_8 - \varepsilon_7) \\
&= \tfrac{1}{2}(6\alpha_1 + 9\alpha_2 + 12\alpha_3 + 18\alpha_4 + 15\alpha_5 + 10\alpha_6 + 5\alpha_7) \\
\varpi_6 &= \varepsilon_5 + \varepsilon_6 - \varepsilon_7 + \varepsilon_8 \\
&= 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 2\alpha_7 \\
\varpi_7 &= \varepsilon_6 + \tfrac{1}{2}(\varepsilon_8 - \varepsilon_7) \\
&= \tfrac{1}{2}(2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7)
\end{aligned}$$

Hilbert basis of M. Note that ϖ_1, ϖ_3, ϖ_4 and ϖ_6 already belong to E_7. Therefore,

$$M = \mathbb{Z}_+\varpi_1 \oplus \mathbb{Z}_+\varpi_3 \oplus \mathbb{Z}_+\varpi_4 \oplus \mathbb{Z}_+\varpi_6 \oplus M' \cong \mathbb{Z}_+^4 \oplus M'$$

with

$$M' = E_7 \cap \bigoplus_{i=2,5,7} \mathbb{Z}_+\varpi_i$$

Now let $l_2\varpi_2 + l_5\varpi_5 + l_7\varpi_7 \in M'$, with $l_i \in \mathbb{Z}_+$. Then the coefficients of each α_i in our base must be integral. One can easily check that the coefficients of $\alpha_1, \alpha_3, \alpha_4$

and α_6 are automatically integral. Looking at the coefficients of the remaining elements of our base gives

$$\begin{aligned} \text{coefficient of } \alpha_2 : &\qquad \tfrac{7}{2}l_2 + \tfrac{9}{2}l_5 + \tfrac{3}{2}l_7 \in \mathbb{Z} \\ \alpha_5 : &\qquad \tfrac{9}{2}l_2 + \tfrac{15}{2}l_5 + \tfrac{5}{2}l_7 \in \mathbb{Z} \\ \alpha_7 : &\qquad \tfrac{3}{2}l_2 + \tfrac{5}{2}l_5 + \tfrac{3}{2}l_7 \in \mathbb{Z} \end{aligned}$$

This reduces to the single condition $l_2 + l_5 + l_7 \in 2\mathbb{Z}$, giving

$$M' \cong \{(l_2, l_5, l_7) \in \mathbb{Z}_+^3 \mid l_2 + l_5 + l_7 \in 2\mathbb{Z}\}$$

As above, one easily finds the following Hilbert basis for the monoid M':

$$\begin{aligned} m_1 &= (2,0,0) \\ m_2 &= (0,2,0) \\ m_3 &= (0,0,2) \\ m_4 &= (1,1,0) \\ m_5 &= (1,0,1) \\ m_6 &= (0,1,1) \end{aligned}$$

Structure of the invariant algebra $\mathbb{Z}[E_7]^{\mathcal{W}}$. Note that the monoid algebra $\mathbb{Z}[M']$ is just the second Veronese subalgebra $R^{(2)}$ of a polynomial algebra $R = \mathbb{Z}[t_2, t_5, t_7]$ in three variables. The structure of such algebras has been explained in Corollary 2.5.2. It follows that the invariant algebra $\mathbb{Z}[E_7]^{\mathcal{W}}$ has the following description:

$$\mathbb{Z}[E_7]^{\mathcal{W}} \cong \mathbb{Z}[M] \cong \mathbb{Z}[M'] \otimes \mathbb{Z}[t_1, t_3, t_4, t_6] \cong R^{(2)}[t_1, t_3, t_4, t_6]$$

a polynomial algebra in four variables over $R^{(2)}$. Fundamental invariants are given by the following four that correspond to the variables t_1, t_3, t_4, t_6,

$$\mathsf{orb}(\varpi_1),\ \mathsf{orb}(\varpi_3),\ \mathsf{orb}(\varpi_4),\ \mathsf{orb}(\varpi_6)$$

together with the following six invariants that correspond to the above monoid generators $m_1, \ldots, m_6$,

$$\mathsf{orb}(\varpi_2)^2,\ \mathsf{orb}(\varpi_5)^2,\ \mathsf{orb}(\varpi_7)^2,\ \mathsf{orb}(\varpi_2)\,\mathsf{orb}(\varpi_5),\ \mathsf{orb}(\varpi_2)\,\mathsf{orb}(\varpi_7),\ \mathsf{orb}(\varpi_5)\,\mathsf{orb}(\varpi_7)$$

4.2.3 Class Group

From the structure of the Weyl group, $\mathcal{W} \cong \{\pm 1\} \times O_7(2)$, we know that the only nontrivial normal subgroups of $\mathcal{W}$ are $\{\pm 1\}$ and $O_7(2)$. Only the former is an elementary abelian 2-group, but -1 is not a reflection. By Lemma 2.4.1 it follows that the subgroup of diagonalizable reflections, $\mathcal{D}$, is trivial. Hence, by Theorem 2.4.2(a), the class group is isomorphic to the factor Λ/L, which is known [2, (VIII) in Planche VI]:

$$\boxed{\mathrm{Cl}(\mathbb{Z}[E_7]^{\mathcal{W}}) \cong \mathbb{Z}/2\mathbb{Z}}$$

Alternatively, we could arrive at the same conclusion using the fact that the invariant algebra $\mathbb{Z}[E_7]^{\mathcal{W}}$ is a polynomial algebra over the second Veronese subalgebra $R^{(2)}$ of $R = \mathbb{Z}[t_2, t_5, t_7]$. Indeed, by [10, Theorem 8.1], it follows that $\mathrm{Cl}(\mathbb{Z}[E_7]^{\mathcal{W}}) \cong \mathrm{Cl}(R^{(2)})$, and the latter group was calculated in Corollary 2.5.2.

REFERENCES

[1] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[2] N. Bourbaki. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*. Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968.

[3] Nicolas Bourbaki. *Algèbre commutative. Chapitre 7: Diviseurs*. Actualités Scientifiques et Industrielles, No. 1314. Hermann, Paris, 1965.

[4] Nicolas Bourbaki. *Éléments de mathématique*, volume 864 of *Lecture Notes in Mathematics*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7].

[5] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[6] Claude Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal

subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[8] Daniel R. Farkas. Multiplicative invariants. *Enseign. Math. (2)*, 30(1-2):141–157, 1984.

[9] Daniel R. Farkas. Toward multiplicative invariant theory. In *Group actions on rings (Brunswick, Maine, 1984)*, volume 43 of *Contemp. Math.*, pages 69–80. Amer. Math. Soc., Providence, RI, 1985.

[10] Robert M. Fossum. *The divisor class group of a Krull domain*. Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74.

[11] David Hilbert. Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890.

[12] David Hilbert. Ueber die vollen Invariantensysteme. *Math. Ann.*, 42(3):313–373, 1893.

[13] James E. Humphreys. *Introduction to Lie algebras and representation theory*. Springer-Verlag, New York-Berlin, 1972. Graduate Texts in Mathematics, Vol. 9.

[14] James E. Humphreys. *Reflection groups and Coxeter groups*, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[15] Camille Jordan. Mémoire sur les équations différentielles linéaires à intégrale algébrique. *J. Reine Angew. Math.*, 84:89–215, 1878.

[16] Martin Lorenz. *Multiplicative invariant theory*, volume 135 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, VI.

[17] E. Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachr. Ges. Wiss. Göttingen*, pages 28–35, 1926.

[18] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1915.

[19] Alexander Polishchuk and Leonid Positselski. *Quadratic algebras*, volume 37 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2005.

[20] P. Samuel. *Lectures on unique factorization domains*. Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30. Tata Institute of Fundamental Research, Bombay, 1964.

[21] Alexander Schrijver. *Theory of linear and integer programming*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Ltd., Chichester, 1986. A Wiley-Interscience Publication.

[22] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canadian J. Math.*, 6:274–304, 1954.

[23] N. J. A. Sloane. Error-correcting codes and invariant theory: new applications of a nineteenth-century technique. *Amer. Math. Monthly*, 84(2):82–107, 1977.

[24] Robert Steinberg. On a theorem of Pittie. *Topology*, 14:173–177, 1975.

[25] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

[26] Richard G. Swan. Gubeladze's proof of Anderson's conjecture. In *Azumaya algebras, actions, and modules (Bloomington, IN, 1990)*, volume 124 of *Contemp. Math.*, pages 215–250. Amer. Math. Soc., Providence, RI, 1992.

[27] Hermann Weyl. Invariants. *Duke Math. J.*, 5:489–502, 1939.

[28] Herbert S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006.