Encyclopaedia of Mathematical Sciences
Volume 135

Invariant Theory and Algebraic Transformation Groups VI

Subseries Editors:
R.V. Gamkrelidze V.L. Popov

Martin Lorenz

Multiplicative Invariant Theory

Springer

Author

Martin Lorenz
Department of Mathematics
Temple University
Philadelphia, PA 19122, USA
e-mail: lorenz@math.temple.edu

Founding editor of the Encyclopaedia of Mathematical Sciences:
R. V. Gamkrelidze

Mathematics Subject Classification (2000):
Primary: 13A50
Secondary: 13H10, 13D45, 20C10, 12F20

ISSN 0938-0396
ISBN 3-540-24323-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media GmbH
springeronline.com
©Springer-Verlag Berlin Heidelberg 2005
Printed in The Netherlands

Typesetting: by the author using a Springer LaTeX macro package
Production: LE-TeX Jelonek, Schmidt & Vöckler GbR, Leipzig
Cover Design: E. Kirchner, Heidelberg, Germany
Printed on acid-free paper 46/3142 YL 5 4 3 2 1 0

To my mother, Martha Lorenz,

and

to the memory of my father,
Adolf Lorenz (1925 – 2001)

Preface

Multiplicative invariant theory, as a research area in its own right, is of relatively recent vintage: the systematic investigation of multiplicative invariants was initiated by Daniel Farkas in the 1980s. Since then the subject has been pursued by a small but growing number of researchers, and at this point it has reached a stage in its development where a coherent account of the basic results achieved thus far is desirable. Such is the goal of this book.

The topic of multiplicative invariant theory is intimately tied to integral representations of finite groups. Therefore, the field has a predominantly discrete, algebraic flavor. Geometry, specifically the theory of algebraic groups, enters the picture through Weyl groups and their root lattices as well as via character lattices of algebraic tori.

I have tried to keep this book reasonably self-contained. The core results on multiplicative invariants are presented with complete proofs often improving on those found in the literature. The prerequisites from representation theory and the theory of root systems are assembled early in the text, for the most part with references to Curtis and Reiner [44], [45] and Bourbaki [24].

For multiplicative invariant *algebras*, Chapters 3–8 give an essentially complete account of the state of the subject to date. On the other hand, more is known about multiplicative invariant *fields* than what found its way into this book. The reader may wish to consult the monographs by Saltman [186] and Voskresenskiĭ [220] for additional information. A novel feature of the present text is the full and streamlined derivation of the known rationality properties of the field of matrix invariants in Chapter 9. This material could heretofore only be found in the original sources which are widely spread in the literature.

A more detailed overview of the contents of this book is offered in the Introduction below. In addition, each of the subsequent chapters has its own introductory section; those of Chapters 4–9 are quite extensive, giving complete statements of the main results proved and delineating the pertinent algebraic background. The book concludes with a chapter on research problems. I hope that it will stimulate further interest in the field of multiplicative invariant theory.

Acknowledgements

Dan Farkas' early work on multiplicative invariants ([59], [60], [61]) provided the initial impetus for my own research on the subject. I also owe an enormous debt to Don Passman at whose invitation I spent a postdoctoral year at UW-Madison in 1978/9 and who has been a good friend ever since. In many ways, I have tried to emulate his book "Infinite Group Rings" [147] in these notes. More recently, I have benefitted from the insights of Nicole Lemire and Zinovy Reichstein, both through their own work on multiplicative invariant theory and through collaborations on related topics. For comments on earlier drafts and help with various aspects of this book, I wish to thank Jacques Alev, Esther Beneish, Frank DeMeyer, Steve Donkin, Victor Guba, Jens Carsten Jantzen, Gregor Kemper, Gabriele Nebe, Wilhelm Plesken, and David Saltman.

I am grateful to Vladimir Popov for inviting me to write this account of my favorite research area and to the anonymous referees for their constructive suggestions.

While writing this book, I was supported in part by the National Science Foundation under grant DMS-9988756 and by the Leverhulme Foundation (Research Interchange Grant F/00158/X).

My greatest debt is to my family: to my daughter Esther for her unwavering support over many years and long distances and to my wife Maria and our children, Gabriel, Dalia and Aidan, whose loving and energetic presence is keeping me grounded.

Temple University, Philadelphia *Martin Lorenz*
December 2004

Contents

Introduction

The Setting

Multiplicative actions arise from a representation $G \to \mathrm{GL}(L)$ of a group G on a lattice L. Thus, L is a free $\mathbb{Z}$-module of finite rank on which G acts by automorphisms, a G-lattice for short. The G-action on L extends uniquely to an action by $\Bbbk$-algebra automorphisms on the group algebra $\Bbbk[L]$ over any chosen commutative base ring $\Bbbk$. Multiplicative invariant theory is concerned with the study of the subalgebra

$$\Bbbk[L]^G = \{f \in \Bbbk[L] \mid g(f) = f \text{ for all } g \in G\}$$

of all G-invariant elements of $\Bbbk[L]$, the *multiplicative invariant algebra* (over $\Bbbk$) that is associated with the G-lattice L.

The terminology "multiplicative", introduced by Farkas [59], derives from the fact that, inside $\Bbbk[L]$, the lattice L becomes a multiplicative subgroup of the group $\mathrm{U}(\Bbbk[L])$ of units of $\Bbbk[L]$. Indeed, identifying L with $\mathbb{Z}^n$ by choosing a $\mathbb{Z}$-basis, the G-action on L is given by matrices in $\mathrm{GL}_n(\mathbb{Z})$, the group algebra $\Bbbk[L]$ becomes the Laurent polynomial algebra $\Bbbk[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, and the image of L in $\Bbbk[L]$ is the group of monomials in the variables x_i and their inverses. For this reason, multiplicative actions are sometimes called *monomial actions* or *purely monomial actions* (in order to distinguish them from their twisted versions; see below). The terminologies "exponential actions" [24] or "lattice actions" can also be found in the literature.

Various generalizations of this basic set-up are of interest, notably the so-called twisted multiplicative actions. Here, the the group G acts on the group ring $\Bbbk[L]$ of a lattice L by ring automorphisms that are merely required to map $\Bbbk$ to itself. Thus, G also acts on $\mathrm{U}(\Bbbk[L])/\,\mathrm{U}(\Bbbk)$. For a domain $\Bbbk$, the latter group is isomorphic to L, thereby making L a G-lattice in the twisted setting as well. If $\Bbbk$ is a field, the group algebra $\Bbbk[L]$ is often replaced by its field of fractions, denoted by $\Bbbk(L)$. Any G-action on $\Bbbk[L]$ extends uniquely to $\Bbbk(L)$. In the case of (twisted) multiplicative actions, the resulting fields $\Bbbk(L)$ with G-action are called *(twisted) multiplicative G-fields*.

Example. Let $\mathcal{S}_3$ denote the symmetric group on $\{1, 2, 3\}$ and let $L = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$ be a lattice of rank 2. Sending the generators $s = (1, 2)$ and $t = (1, 2, 3)$ of $\mathcal{S}_3$ to the matrices $\left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$, we obtain an integral representation $\mathcal{S}_3 \longrightarrow \mathrm{GL}(L) \cong \mathrm{GL}_2(\mathbb{Z})$. Thus, the action of $\mathcal{S}_3$ on L is given by $s(a_1) = -a_1$, $s(a_2) = a_1 + a_2$, $t(a_1) = a_2$ and $t(a_2) = -a_1 - a_2$. The resulting multiplicative action on $\Bbbk[L] \cong \Bbbk[x_1^{\pm 1}, x_2^{\pm 1}]$ is determined by $s(x_1) = x_1^{-1}$, $s(x_2) = x_1 x_2$, $t(x_1) = x_2$ and $t(x_2) = x_1^{-1} x_2^{-1}$. As will be explained in Example 3.5.6 below, the invariant algebra $\Bbbk[L]^{\mathcal{S}_3}$ is generated by the "fundamental invariants"

$$\begin{aligned} \alpha &= x_1 + x_2 + x_1 x_2 + x_1^{-1} x_2^{-1} + x_1^{-1} + x_2^{-1} \ , \\ \beta &= x_1 x_2^2 + x_1^{-2} x_2^{-1} + x_1 x_2^{-1} \ , \\ \gamma &= x_1^2 x_2 + x_1^{-1} x_2 + x_1^{-1} x_2^{-2} \ . \end{aligned}$$

Here, α is the sum over the $\mathcal{S}_3$-orbit of x_1 in $\Bbbk[L]$, and β and γ are the $\mathcal{S}_3$-orbit sums of $x_1 x_2^2$ and $x_1^2 x_2$, respectively. The algebra $\Bbbk[L]^{\mathcal{S}_3}$ is not regular; it is isomorphic to $\Bbbk[x, y, z]/(z^3 - xy)$. However, the multiplicative invariant field $\Bbbk(L)^{\mathcal{S}_3}$ is purely transcendental of degree 2. — This example describes the multiplicative invariants of the $\mathcal{S}_3$-action on the so-called root lattice A_2. We will return to it on several occasions in the text; see in particular Examples 1.8.1, 3.5.6, 6.3.2 and 9.6.3 where all assertions made in the foregoing will be substantiated.

Multiplicative and Polynomial Invariants

For the most part, algebraic invariant theory is concerned with the investigation of algebras of polynomial invariants over a field $\Bbbk$. These come from a linear representation $G \longrightarrow \mathrm{GL}(V)$ of a group G on a $\Bbbk$-vector space V by extending the G-action on V to the symmetric algebra $\mathsf{S}(V)$. The resulting action of G on $\mathsf{S}(V)$ is often called a *linear action*. Identifying $\mathsf{S}(V)$ with a polynomial algebra over $\Bbbk$ by means of a choice of basis for V, the action can also be thought of as an action by *linear substitutions of the variables*. Therefore, the subalgebra $\mathsf{S}(V)^G$ of all G-invariant polynomials in $\mathsf{S}(V)$ is usually called an algebra of polynomial invariants.

There is a common way of viewing linear and multiplicative actions. Indeed, both the symmetric algebra $\mathsf{S}(V)$ and the group algebra $\Bbbk[L]$ are Hopf algebras over $\Bbbk$. Moreover, there are canonical isomorphisms $\mathrm{GL}(V) \cong \mathrm{Aut}_{\mathsf{Hopf}}(\mathsf{S}(V))$ and $\mathrm{GL}(L) \cong \mathrm{Aut}_{\mathsf{Hopf}}(\Bbbk[L])$. Thus, both types of actions arise from a homomorphism

$$G \longrightarrow \mathrm{Aut}_{\mathsf{Hopf}}(H)$$

for some reduced affine commutative Hopf algebra H. Working over an algebraically closed base field $\Bbbk$, we may view H as the ring $\mathcal{O}(\varGamma)$ of regular functions of an affine algebraic group $\varGamma$ and $\mathrm{Aut}_{\mathsf{Hopf}}(H)$ as the group $\mathrm{Aut}(\varGamma)$ of automorphisms of $\varGamma$. In the case of linear actions, the group $\varGamma$ in question is the additive group of affine space $\mathbb{A}^n = \mathbb{G}_{\mathrm{a}}^n$ while multiplicative actions correspond to algebraic tori $\mathbb{G}_{\mathrm{m}}^n$.

To a large extent, the local study of the algebra of multiplicative invariants $\Bbbk[L]^{\mathcal{G}}$ of a finite group $\mathcal{G}$ reduces to the classical case of polynomial invariants, at least when $\Bbbk$ is an algebraically closed field whose characteristic does not divide the order of $\mathcal{G}$. Indeed, $\mathcal{G}$ acts linearly on the $\Bbbk$-vector space $L_{\Bbbk} = L \otimes_{\mathbb{Z}} \Bbbk$, and hence on its symmetric algebra $\mathsf{S}(L_{\Bbbk})$. Luna's slice theorem [128] implies that, for any maximal ideal $\mathfrak{M}$ of $\Bbbk[L]$, there is an isomorphism of the completions

$$\widehat{\Bbbk[L]^{\mathcal{G}}_{\mathfrak{m}}} \cong \widehat{\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}_{\mathsf{S}_+}} \ ,$$

where $\mathfrak{m} = \mathfrak{M} \cap \Bbbk[L]^{\mathcal{G}}$, $\mathcal{G}_{\mathfrak{M}}$ is the decomposition group of $\mathfrak{M}$, and S_+ denotes the maximal ideal of $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}$ consisting of all $\mathcal{G}_{\mathfrak{M}}$-invariant polynomials having constant term 0; see Proposition 7.3.1.

Special Features of Multiplicative Actions

Despite the aforementioned connections, multiplicative actions display some features that contrast sharply with their linear counterparts:

- Even though multiplicative actions can of course be considered for arbitrary groups G, the study of their invariant algebras quickly reduces to the case of *finite groups*. Indeed, given a G-lattice L for an infinite group G, let L_{fin} denote the set of all elements of L whose G-orbit is finite. Then L_{fin} is a G-sublattice of L on which G acts through a finite quotient, $\mathcal{G}$, and it is easy to see that $\Bbbk[L]^G \subseteq \Bbbk[L_{\text{fin}}]$. Thus,
$$\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^{\mathcal{G}} \ .$$
As a consequence, multiplicative invariant algebras $\Bbbk[L]^G$ are always affine (i.e., finitely generated) $\Bbbk$-algebras; see Proposition 3.3.1 and Corollary 3.3.2 below.
- The base ring $\Bbbk$ plays a rather subordinate role. Indeed, multiplicative invariants are always defined over $\mathbb{Z}$,
$$\Bbbk[L]^G \cong \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G \ ;$$
see Proposition 3.3.1. Many properties of $\mathbb{Z}[L]^G$ transfer directly to $\Bbbk[L]^G$. For example, if G acts as a reflection group on L then, as we will show in Section 6.3, $\mathbb{Z}[L]^G$ is a free module of finite rank over some polynomial subring. Consequently, multiplicative invariants of reflection groups are Cohen-Macaulay, for any Cohen-Macaulay base ring $\Bbbk$ (Corollary 6.1.2). On the other hand, polynomial invariants of finite pseudoreflection groups can fail to be Cohen-Macaulay if the characteristic of the base field divides the group order (Nakajima [136]).
- By a classical result of Jordan [102], the group $\mathrm{GL}_n(\mathbb{Z})$ has only finitely many finite subgroups up to conjugacy. Therefore, working over a fixed base ring $\Bbbk$, there are only finitely many multiplicative invariant algebras $\Bbbk[L]^G$, up to isomorphism, with $\operatorname{rank} L \leq n$. For small values of n, the finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ are readily accessible by means of various computer algebra systems (e.g., GAP [71], CARAT [34]). In principle, this opens the possibility of establishing a complete data base for multiplicative invariants in low ranks. This has not yet been realized, however.

- A property of polynomial invariants, of great practical and theoretical importance, is the existence of a natural grading by “total degree in the variables”. This is no longer true of multiplicative invariants: in general, there is no $\mathbb{Z}_+$-grading $\Bbbk[L]^G = \bigoplus_{n\geq 0} R_n$ with $R_0 = \Bbbk$. Thus, the familiar graded-local setting of polynomial invariants is not available when investigating multiplicative invariants. This manifests itself in the fact that class groups, Picard groups etc. of multiplicative invariants have a more complicated structure than the corresponding items for polynomial invariants.

Origins and Uses of Multiplicative Invariants

The early history of multiplicative invariant theory is somewhat opaque. The origins of the subject lie in Lie theory which has a rich supply of lattices that are associated with root systems. Bourbaki’s “Groupes et algèbres de Lie” [24] devotes a section (chap. VI §3) to multiplicative invariants under the name exponential invariants. Steinberg [204] and Richardson [165], [166] are further sources with a Lie theoretic orientation. The term “multiplicative invariant theory” was coined by Daniel Farkas [59], [60] who, originally motivated by his research on infinite group algebras, elevated the subject to a research area in its own right.

Multiplicative group actions occur naturally in a variety of contexts:

Centers and prime ideals of group algebras. The center of the group algebra $\Bbbk[\Gamma]$ of an arbitrary group Γ can be described as the invariant algebra $\Bbbk[\Delta]^\Gamma$ for the conjugation action of Γ on the subgroup Δ consisting of all elements of Γ whose Γ-conjugacy class is finite. If $\Bbbk[\Gamma]$ is prime noetherian then Δ is a lattice and the center of $\Bbbk[\Gamma]$ is a multiplicative invariant algebra. Of particular interest is the special case where Γ is a crystallographic group. All multiplicative invariant algebras $\Bbbk[L]^G$ are centers of suitable crystallographic group algebras $\Bbbk[\Gamma]$, and conversely. In a more general setting, a key ingredient in the theory of prime ideals in group algebras of polycyclic-by-finite groups Γ is the Bergman-Roseblade Theorem on multiplicative actions ([15, Theorem 1], [170, Theorem D]; see also Farkas [59, §1]).

Representation rings of Lie algebras. The representation ring $R(\mathfrak{g})$ of a finite-dimensional complex semisimple Lie algebra $\mathfrak{g}$ is a multiplicative invariant algebra over $\mathbb{Z}$: $R(\mathfrak{g}) \cong \mathbb{Z}[\Lambda]^{\mathcal{W}}$. Here, Λ is the weight lattice of $\mathfrak{g}$ and $\mathcal{W}$ the Weyl group. The isomorphism is effected by the notion of a character for $\mathfrak{g}$-modules (Bourbaki [26, Théorème VIII.7.2]). Suitably completed versions of $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ form the setting for the character, denominator and multiplicity formulas for Kac-Moody algebras $\mathfrak{g} = \mathfrak{g}(C)$ (cf. Kac [103]).

Rationality problems and relative sections. Let F/K be a rational extension of fields, that is, $F = K(t_1, \dots, t_d)$ with algebraically independent generators t_i over K. Assume that the group G acts by automorphims on F which map K to itself. Noether’s rationality problem, in the generalized form studied today, asks under which circumstances the extension F^G/K^G of invariant fields is also rational, or at least stably rational, retract rational …; see Section 9.1 for the definitions. The problem originated from considerations in constructive Galois theory (Noether [141]). The special case of (twisted) multiplicative $\mathcal{G}$-fields, for a finite group $\mathcal{G}$, has received particular attention; see especially the work of Colliot-Thélène and Sansuc [41],[42], Hajja and Kang [84],[85],[86], Lemire [115], Lenstra [118], Saltman [179], [181], [182],[186], Swan [209], and Voskresenskiĭ [217], [219],[220]. The interest in (twisted) multiplicative $\mathcal{G}$-fields is fueled in part by their connection with algebraic tori; see Section 3.10. Furthermore, by constructing suitable relative sections in the sense of Katsylo [105] (see also Popov [152] and Popov-Vinberg [153]), one can oftentimes show that the field $\mathcal{K}(X)^G$ of invariant rational functions under the action of an algebraic group G on an irreducible algebraic variety X is isomorphic to the multiplicative invariant field $\Bbbk(L)^{\mathcal{G}}$ of some finite group $\mathcal{G}$. This will be explained in Chapter 9. In the case where X is the space M_n^r of r-tuples of $n \times n$-matrices over $\Bbbk$ and the group $G = \mathrm{PGL}_n$ operates by simultaneous conjugation, Procesi [154] has constructed a relative section leading to an isomorphism $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n} \cong \Bbbk(L_{n,r})^{\mathcal{S}_n}$, where $L_{n,r}$ is a certain lattice for the symmetric group $\mathcal{S}_n$; see Theorem 9.8.2. This approach was subsequently refined and systematically exploited by Formanek [64], [65], Bessenrodt and Le Bruyn [17], Beneish [8], [12], [10], [13] and others.

Algebraic tori. Let $\mathcal{G}$ be a finite group and $\Bbbk$ an algebraically closed field. As was mentioned above, multiplicative $\mathcal{G}$-actions on $\Bbbk[L]$ correspond to $\mathcal{G}$-actions on the algebraic torus $T = \mathbb{G}_{\mathrm{m}}^n$ ($n = \operatorname{rank} L$). Since $T/\mathcal{G} = \operatorname{Spec} \Bbbk[L]^{\mathcal{G}}$, properties of $\Bbbk[L]^{\mathcal{G}}$ translate into properties of the quotient $T/\mathcal{G}$. It is easy to see that $T/\mathcal{G}$ is never a torus if the $\mathcal{G}$-action is nontrivial (Corollary 3.4.2). However, if $\mathcal{G}$ acts as a reflection group on L then $T/\mathcal{G}$ is at least an affine toric variety. This follows from the fact that the multiplicative invariant algebra $\Bbbk[L]^{\mathcal{G}}$ of a reflection group $\mathcal{G}$ is always a semigroup algebra (Theorems 6.1.1 and 7.5.1).

Overview of the Contents

Our main focus is on regular multiplicative actions as opposed to birational ones, that is, for the most part we are concerned with multiplicative actions on the group algebra $\Bbbk[L]$ rather than its field of fractions, $\Bbbk(L)$. Multiplicative invariant fields $\Bbbk(L)^G$, along with their twisted versions, do however feature extensively and explicitly in Chapter 9 and implicitly in Chapter 2 which deploys a range of representation theoretic tools needed for their investigation. Moreover, we adopt a primarily algebraic point of view, keeping prerequisites from algebraic geometry to a minimum. On a few occasions in Chapters 7 and 9, however, we have found it convenient to use geometric language. For a more geometric birational perspective on multiplicative and other actions, see the works of Colliot-Thélène and Sansuc and Voskresenskiĭ cited above.

Each individual chapter is preceded by its own introduction. Here, we limit ourselves to a description of the contents in rather broad strokes:

Chapters 1 and 2 are entirely devoted to group actions on lattices. Aside from furnishing some basic definitions, notations and examples to be used throughout the text, the main purpose of these chapters is to collect the purely representation theoretic techniques and results needed for the investigation of multiplicative invariant algebras and fields later on. In Chapter 1, we in particular review the rudiments of root lattices and weight lattices in some detail, following Bourbaki [24], while Chapter 2 revolves around permutation lattices and the notion of flasque equivalence of lattices. Our presentation regarding this notion leans rather heavily on Colliot-Thélène and Sansuc [41],[42]. Chapter 2 also offers a simplified account of Esther Beneish's method [8] of restriction to the Sylow normalizer, a crucial ingredient in her new proof of the Bessenrodt-Le Bruyn stable rationality theorem [17] for the field of matrix invariants $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ for $n = 5$ and 7. This proof is presented in Chapter 9 along with proofs of Formanek's rationality theorems for the cases $n \leq 4$ [64], [65] and of Saltman's retract rationality result for all prime values of n [177].

Multiplicative invariant algebras $\Bbbk[L]^G$ and their twisted analogs make their proper formal entrance in Chapter 3. Finite generation of $\Bbbk[L]^G$, the existence of a $\mathbb{Z}$-structure, and the fact that it suffices to consider the case of finite group actions are quickly derived in Section 3.3. Chapter 3 also contains a large supply of examples, including explicit descriptions of all invariant algebras $\mathbb{Z}[L]^G$ with $\operatorname{rank} L = 2$. The theoretical highlight is Bourbaki's theorem [24] which asserts that multiplicative invariant algebras of weight lattices over the Weyl group are polynomial algebras (Theorem 3.6.1). The converse also holds: all multiplicative invariant algebras that are polynomial algebras come from weight lattices. The latter result, due to Farkas [59] and Steinberg [204], is proved in Chapter 7 (Corollary 7.1.2). Bourbaki's theorem and its converse can be viewed as a multiplicative analog of the classical theorem of Shephard-Todd and Chevalley [196], [37] for polynomial invariants.

Various aspects of the algebraic structure of multiplicative invariant algebras $\Bbbk[L]^{\mathcal{G}}$, for a finite group $\mathcal{G}$, are discussed in Chapters 4 through 8, each of which is loosely based on an earlier publication of the author ([121], [123], [124], [122], [120]). Chapter 4 addresses the question when $\Bbbk[L]^{\mathcal{G}}$ is a unique factorization domain. This is answered in Theorem 4.1.1 which gives a formula for the class group $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}})$, the obstruction to the unique factorization property. The Picard group $\mathrm{Pic}(\Bbbk[L]^{\mathcal{G}})$, a subgroup of $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}})$, is calculated in Chapter 5 (Theorem 5.1.1). In contrast with the case of polynomial invariants, which have trivial Picard groups (see Example 5.5.2), it turns out that $\mathrm{Pic}(\Bbbk[L]^{\mathcal{G}})$ can be nontrivial. Motivated by the Shephard-Todd-Chevalley Theorem we completely determine the structure of $\Bbbk[L]^{\mathcal{G}}$ for finite reflection groups $\mathcal{G}$ in Chapter 6: they are affine normal semigroup algebras (Theorem 6.1.1). In particular, multiplicative invariant algebras of finite reflection groups are always Cohen-Macaulay (for any Cohen-Macaulay base ring $\Bbbk$), but they are generally not regular. The question as to when multiplicative invariant algebras are regular is settled in Theorem 7.1.1. The Cohen-Macaulay property of multiplicative invariants is addressed in a systematic fashion in Chapter 8. While the main result, Theorem 8.1.1, falls short of fully determining when exactly multiplicative invariant algebras are Cohen-Macaulay, we hope that the material of this chapter will be useful for researchers in invariant theory, even if they are not primarily interested in multiplicative invariants: for the most part, we work in a general ring theoretic context and we have included, among other things, a detailed discussion of the celebrated Ellingsrud-Skjelbred spectral sequences [55] for local cohomology.

A recurring theme throughout Chapters 4 – 8 is the role of reflections and their generalizations. Specifically, an element $g \in \mathcal{G}$ is said to act as a k-reflection on the lattice L if the sublattice $\{g(m) - m \mid m \in L\}$ of L has rank at most k or, equivalently, if the g-fixed points in $L \otimes_{\mathbb{Z}} \mathbb{Q}$ have codimension at most k. We will refer to 1-reflections and 2-reflections as reflections and bireflections, respectively. Figure depicts some relations between these properties, straight from linear algebra, and certain ring theoretic properties of the multiplicative invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$.

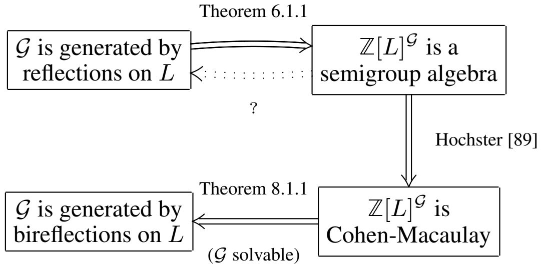
Theorem 6.1.1
$\mathcal{G}$ is generated by reflections on L
$\mathbb{Z}[L]^{\mathcal{G}}$ is a semigroup algebra
?
Hochster [89]
Theorem 8.1.1
$\mathcal{G}$ is generated by bireflections on L
$\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay
($\mathcal{G}$ solvable)

Fig. 1. Generalized reflections and ring theoretic properties

Multiplicative invariant fields, ordinary and twisted, are finally taken up in Chapter 9. The focal point of this chapter is Noether's rationality problem. The various versions of "rationality" for field extensions are discussed in some detail, with particular emphasis on the case of function fields of algebraic tori. The main features of Chapter 9 are the aforementioned Formanek-Procesi description of the field of matrix invariants $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ as a multiplicative invariant field of the symmetric group (Theorem 9.8.2) and the various rationality results for $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ that have been derived from this description.

The last chapter, Chapter 10, is devoted to research problems. Some of these summarize and complement problem areas that are touched on in previous chapters, while others concern issues of current interest that did not end up in the main body of the text (algorithms, essential dimension estimates). Since multiplicative invariant theory has come into its own only fairly recently, the subject is very much in flux and our present state of knowledge is still quite rudimentary. It will doubtless soon be superseded and the author can only hope that this book contributes to this by acting as a stimulant to further research in the field of multiplicative invariant theory.

Notations and Conventions

All actions will be written on the left. In particular, all modules are left modules. Finite groups will be denoted by script symbols, such as $\mathcal{G}$, while possibly infinite groups will be written in ordinary roman type, G. Throughout, $\Bbbk$ will denote a commutative base ring. All actions are trivial on $\Bbbk$. Any further assumptions on $\Bbbk$ will be explicitly stated whenever they are needed.

Here is a list of the main abbreviations and symbols used in the text.

General

$\mathbb{Z}_+, \mathbb{R}_+$	the set of non-negative integers and the non-negative reals
$\mathbb{N}$	the set of natural numbers, $\{1, 2, \dots\}$
$\mathbb{F}_p$	the field with p elements
$\coprod$	disjoint union (for sets)

Groups

$\mathcal{S}_n$	the symmetric group on $\{1, 2, \dots, n\}$
$\mathcal{A}_n$	the alternating subgroup of $\mathcal{S}_n$
$\mathcal{C}_n$	the cyclic group of order n
$\mathcal{D}_n$	the dihedral group of order n
$H^i(G, \,.\,)$	ordinary cohomology of G
$\widehat{H}^i(\mathcal{G}, \,.\,)$	Tate cohomology of the finite group $\mathcal{G}$
$\text{Ш}^i(\mathcal{G}, \,.\,)$	$\bigcap_{g \in \mathcal{G}} \operatorname{Ker}\left(\operatorname{res}^{\mathcal{G}}_{\langle g \rangle} : \widehat{H}^i(\mathcal{G}, \,.\,) \to \widehat{H}^i(\langle g \rangle, \,.\,)\right)$

Vector spaces

$V^* = \operatorname{Hom}_{\Bbbk}(V, \Bbbk)$	the dual space of the $\Bbbk$-vector space V
$\langle \,.\,, . \,\rangle$	the evaluation form $V^* \times V \to \Bbbk$
$\mathsf{S}(V)$	the symmetric algebra of V
$\mathsf{K}(V) = Q(\mathsf{S}(V))$	the field of fractions of $\mathsf{S}(V)$
$\mathcal{O}(V) = \mathsf{S}(V^*)$	the algebra of polynomial functions on V

$\mathcal{K}(V) = \mathsf{K}(V^*)$	the field of rational functions on V

Lattices

$L \cong \mathbb{Z}^n$	a lattice
$L_{\Bbbk}$	$L \otimes_{\mathbb{Z}} \Bbbk$ (most often used with $\Bbbk = \mathbb{Q}$ or $\Bbbk = \mathbb{R}$)
$L_{(p)}$	$L \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at p
$L \vee L'$	L and L' belong to the same genus; see §1.2.2
$L \underset{\text{fl}}{\sim} L'$	L and L' are flasque equivalent; see Section 2.7
g_L	the operator in $\mathrm{GL}(L)$ given by the action of an element $g \in G$
$\mathrm{Ker}_G(L)$	the kernel of the action of G on L, that is, the set of all $g \in G$ with $g_L = \mathrm{Id}_L$
$L^* = \mathrm{Hom}_{\mathbb{Z}}(L, \mathbb{Z})$	the dual lattice
L^G	the sublattice of G-invariants in L
$\mathsf{S}^n L$	the n^{th} symmetric power of L
$\bigwedge^n L$	the n^{th} exterior power of L
$L{\uparrow}_G^H = \mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} L$	the induced H-lattice (for $H \geq G$)
$L{\downarrow}_H^G$	the restricted H-lattice (for $H \leq G$)
$\varepsilon_{G/H}$	the augmentation map $\mathbb{Z}[G/H] \to \mathbb{Z}$, $gH \mapsto 1$; see §1.3.1
$N_{G/H}$	the norm map $\mathbb{Z} \to \mathbb{Z}[G/H]$, $1 \mapsto \sum_{g \in G/H} gH$; see §1.3.1
$I_{G/H}$	the kernel of the augmentation map $\varepsilon_{G/H}$
$\mathbb{Z}^-$, U_n, A_{n-1}	the sign lattice, the standard permutation lattice and the root lattice for the symmetric group $\mathcal{S}_n$; see §1.3.3
$\mathsf{SP}_{\mathcal{G}}$	the monoid of stable permutation equivalence classes of $\mathcal{G}$-lattices, for a finite group $\mathcal{G}$; see Section 2.3

Rings and modules

$\mathrm{Spec}\, R$	the set of prime ideals of R
$\mathrm{U}(R)$	the group of units of the ring R
$\mathrm{Cl}(R)$	the class group of the Krull domain R
$\mathrm{Pic}(R)$	Picard group of R
R-Mod	the category of all left R-modules
R-proj	the category of finitely generated projective left R-modules
$\mathrm{grade}(\mathfrak{a}, M)$	the grade of $\mathfrak{a}$ on M; see Section 8.2
$\mathrm{height}(\mathfrak{a}, M)$	height of $\mathfrak{a}$ on M; see Section 8.2
$\varGamma_{\mathfrak{a}}$	the $\mathfrak{a}$-torsion functor; see Section 8.3
$H^i_{\mathfrak{a}} = R^i \varGamma_{\mathfrak{a}}$	local cohomology with support in $\mathfrak{a}$; see Section 8.3

(Semi-) Group algebras

$\Bbbk$	a commutative base ring, a base field in Chapter 9
$\Bbbk[L]$ ($\Bbbk[M]$, $\Bbbk[\mathcal{G}]$)	the (semi-)group algebra of the lattice L (monoid M, group $\mathcal{G}$) over $\Bbbk$

$\mathbf{x}^m$	the basis element of $\Bbbk[L]$ corresponding to the element $m \in L$
$\underline{S} = \{\mathbf{x}^m \mid m \in S\}$	the image of a subset $S \subseteq L$ in the group algebra $\Bbbk[L]$
$\varepsilon \colon \Bbbk[L] \to \Bbbk$	is the augmentation map, $\varepsilon(\mathbf{x}^m) = 1$ for $m \in L$
$\mathfrak{E} = \operatorname{Ker} \varepsilon$	the augmentation ideal of $\Bbbk[L]$
$\Bbbk(L) = Q(\Bbbk[L])$	the field of fractions of $\Bbbk[L]$ (for a field $\Bbbk$)
$R[L]_\gamma$	the group ring $R[L]$ of L over R with a twisted multiplicative G-action
$K(L)_\gamma = Q(K[L]_\gamma)$	the field of fractions of $K[L]_\gamma$ (K is some G-field)

Group actions

R^G	invariant subring of R under a G-action on R
$R\#G$	the skew group ring associated with a G-action on R
G_x	isotropy group of x in G
$G(x)$	the G-orbit of x
$I_G(\mathfrak{P})$	the inertia group in G of a (prime) ideal $\mathfrak{P}$ of R
$I_R(G)$	the ideal of R that is generated by all elements $r - g(r)$ $(r \in R, g \in G)$; see Section 4.5
$\operatorname{tr}_{\mathcal{G}}$	the trace map $R \to R^{\mathcal{G}}$, $r \mapsto \sum_{g \in \mathcal{G}} g(r)$ ($\mathcal{G}$ a finite group)
$\operatorname{tr}_{\mathcal{G}/\mathcal{H}}$	the relative trace map $R^{\mathcal{H}} \to R^{\mathcal{G}}$; see Section 8.5
$R^{\mathcal{G}}_{\mathcal{H}}$	the image of the relative trace map $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}$
$\rho = \rho_{\mathcal{G}}$	the Reynolds operator $\lvert\mathcal{G}\rvert^{-1} \operatorname{tr}_{\mathcal{G}} \colon R \to R^{\mathcal{G}}$ ($\mathcal{G}$ a finite group with $\lvert\mathcal{G}\rvert^{-1} \in R$); similarly with $L_{\mathbb{Q}}$ in place of R

Root systems

$\mathcal{W}(\Phi)$	the Weyl group of the root system Φ
$\operatorname{Aut}(\Phi)$	the automorphism group of Φ
$L(\Phi)$	the root lattice of Φ
$\Lambda(\Phi)$	the weight lattice of Φ
$\Phi_{\mathcal{G}}(L)$	the root system that is associated with the $\mathcal{G}$-lattice L; see Section 1.9

Algebraic geometry

$\mathcal{O}(X)$	the algebra of regular functions of the algebraic variety X over $\Bbbk$
$\mathcal{K}(X)$	the field of rational functions of the irreducible algebraic variety X
$\operatorname{dom} f$	the domain of definition of a rational map f
$\mathbb{G}_{\mathrm{m}}$, $\mathbb{G}_{\mathrm{a}}$	the multiplicative group and the additive group

1

Groups Acting on Lattices

1.1 Introduction

Aside from introducing the basic terminology and notations concerning lattices, this chapter serves the dual purpose of (1) deploying a range of tools for the investigation of lattices later in the text and (2) providing some background on integral representations of groups and integral matrix groups along with a number of examples. In particular, we review the fundamentals pertaining to root systems and lattices that are associated with them in some detail. This material will make frequent appearances throughout the text. Our standard reference for the module theoretic material is Curtis and Reiner [44]; for root systems we follow Bourbaki [24].

Throughout this chapter, G denotes a group.

1.2 G-Lattices

A *lattice* L is a free $\mathbb{Z}$-module of finite rank; so $L \cong \mathbb{Z}^n$ where $n = \operatorname{rank} L$. Lattices are traditionally written additively and we will do so throughout. If a group G acts on L by means of a homomorphism $G \to \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$ then L is called a *G-lattice*. In other words, G-lattices are modules over the integral group ring $\mathbb{Z}[G]$ (*G-modules*, for short) that are free of finite rank over $\mathbb{Z}$. Homomorphisms of G-lattices are identical with G-module homomorphisms, that is, G-equivariant $\mathbb{Z}$-linear maps. If the structure map $G \to \mathrm{GL}(L)$ needs to be made explicit, it will be written as $g \mapsto g_L$. The image of an element $m \in L$ under g_L will simply be denoted by $g(m)$. We put $\mathrm{Ker}_G(L) = \{g \in G \mid g_L = \mathrm{Id}_L\}$. A G-lattice (or G-module) L is called *faithful* if $\mathrm{Ker}_G(L) = 1$. For any G-lattice L, we put

$$L^G = \{m \in L \mid g(m) = m \text{ for all } g \in G\} ,$$

the sublattice of G-invariants in L. The G-lattice L is said to be *effective* if $L^G = \{0\}$, and *trivial* if $L^G = L$.

1.2.1 Rational Type

To any G-module L, we may associate the module

$$L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q} \tag{1.1}$$

over the rational group algebra $\mathbb{Q}[G]$. If this module is irreducible, L is called *rationally irreducible*. Two G-modules L and L' are said to be *rationally isomorphic* if $L_{\mathbb{Q}} \cong L'_{\mathbb{Q}}$ as $\mathbb{Q}[G]$-modules. In this case, replacing L' by an isomorphic copy inside $L_{\mathbb{Q}}$, we may assume that $L \supseteq L'$ and L/L' is finite.

1.2.2 Genus

For any G-lattice L and any prime $p \in \mathbb{Z}$, we write $L_{(p)} = L \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at p. Two G-lattices L and L' are said to be *locally isomorphic* if $L_{(p)} \cong L'_{(p)}$ as $\mathbb{Z}_{(p)}[G]$-modules for all primes p. In this case, L and L' are also said to belong to the same *genus*; in short, $L \vee L'$. Clearly,

$$L \cong L' \;\Rightarrow\; L \vee L' \;\Rightarrow\; L_{\mathbb{Q}} \cong L'_{\mathbb{Q}} \,.$$

If G is a finite group $\neq 1$, it suffices to check the condition $L_{(p)} \cong L'_{(p)}$ for all primes p dividing the order of G; see [44, 31.2(ii)]. Moreover, for lattices over finite groups,

$$L \vee L' \iff L^s \cong L'^s \quad \text{for some } s > 0\,; \tag{1.2}$$

see Swan and Evans [211, Theorem 6.11].

1.3 Examples

1.3.1 Some Permutation Lattices

When viewed as a lattice over some group G, the unadorned symbol

$$\mathbb{Z}$$

will always denote the integers with trivial G-action. More generally, for any subgroup H of G with $[G : H] < \infty$, we may form the G-lattice

$$\mathbb{Z}[G/H] = \bigoplus_g \mathbb{Z}gH\,,$$

where g runs over a transversal for the collection G/H of left cosets of H in G. The G-action on $\mathbb{Z}[G/H]$ is given by $g(g'H) = gg'H$ for $g, g' \in G$. Thus, G permutes a $\mathbb{Z}$-basis of the lattice $\mathbb{Z}[G/H]$. Lattices of this type are called *permutation lattices*; they will be considered in detail in Chapter 2. There are G-lattice homomorphisms, called *augmentation* and *norm*,

$$\varepsilon_{G/H} \colon \mathbb{Z}[G/H] \to \mathbb{Z} \quad \text{and} \quad N_{G/H} \colon \mathbb{Z} \to \mathbb{Z}[G/H] \; ; \tag{1.3}$$

they are defined by $\varepsilon_{G/H}(gH) = 1$ and $N_{G/H}(1) = \sum_{g \in G/H} gH$. Putting

$$I_{G/H} = \operatorname{Ker} \varepsilon_{G/H} \tag{1.4}$$

we obtain an exact sequence of G-lattices

$$0 \to I_{G/H} \xrightarrow{\text{incl.}} \mathbb{Z}[G/H] \xrightarrow{\varepsilon_{G/H}} \mathbb{Z} \to 0 \, . \tag{1.5}$$

1.3.2 Free and Projective Lattices

For a finite group $\mathcal{G}$, the group ring $\mathbb{Z}[\mathcal{G}]$, viewed as module over itself via left multiplication, is a permutation $\mathcal{G}$-lattice, the so-called the *regular $\mathcal{G}$-lattice*. Any $\mathcal{G}$-lattice isomorphic to a finite direct sum $\mathbb{Z}[\mathcal{G}]^r$ is called *free*. Direct summands of free $\mathcal{G}$-lattices are called *projective*. By a celebrated theorem of Swan [207] (see also [44, 32.11]), any projective $\mathcal{G}$-lattice L is *locally free*, that is,

$$L \vee \mathbb{Z}[\mathcal{G}]^r \tag{1.6}$$

for some r (necessarily equal to $\operatorname{rank} L/|\mathcal{G}|$).

1.3.3 The Symmetric Group

Throughout, we let $\mathcal{S}_n$ denote the symmetric group on $\{1, \ldots, n\}$. Lattices for $\mathcal{S}_n$ will play an important role in later sections, in particular the following $\mathcal{S}_n$-lattices. First, the sign homomorphism $\operatorname{sgn} \colon \mathcal{S}_n \to \{\pm 1\}$ with kernel $\mathcal{A}_n$, the alternating group, gives rise to a non-trivial $\mathcal{S}_n$-lattice structure on $\mathbb{Z}$. This lattice will be called the *sign lattice* for $\mathcal{S}_n$ and denoted by

$$\mathbb{Z}^- \, .$$

Next, identifying $\mathcal{S}_{n-1}$ with the subgroup $\operatorname{stab}_{\mathcal{S}_n}(n)$ of $\mathcal{S}_n$, we may form the $\mathcal{S}_n$-lattice $\mathbb{Z}[\mathcal{S}_n/\mathcal{S}_{n-1}]$ as in (a) above. This lattice is isomorphic to the *standard permutation $\mathcal{S}_n$-lattice*, U_n:

$$U_n = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n \tag{1.7}$$

with $s \in \mathcal{S}_n$ acting by $s(e_i) = e_{s(i)}$. The augmentation map $\varepsilon_n = \varepsilon_{\mathcal{S}_n/\mathcal{S}_{n-1}}$ in (1.3) takes the form

$$\varepsilon_n \colon U_n \twoheadrightarrow \mathbb{Z} \, , \qquad e_i \mapsto 1 \, . \tag{1.8}$$

The kernel of $I_{\mathcal{S}_n/\mathcal{S}_{n-1}}$ of ε_n will be denoted by A_{n-1}; so

$$A_{n-1} = \left\{ \sum_{i=1}^{n} z_i e_i \in U_n \Big| \sum_i z_i = 0 \right\} \, . \tag{1.9}$$

The augmentation sequence (1.5) now becomes

$$0 \to A_{n-1} \xrightarrow{\text{incl.}} U_n \xrightarrow{\varepsilon_n} \mathbb{Z} \to 0 \,. \tag{1.10}$$

The $\mathcal{S}_n$-lattices $\mathbb{Z}^-$ and A_{n-1} are rationally irreducible. The corresponding irreducible $\mathbb{Q}[\mathcal{S}_n]$-modules are also known as the Specht modules $S^{(1^n)}$ and $S^{(n-1,1)}$ for the partitions (1^n) and $(n-1,1)$ of n; see, e.g., [70]. The standard permutation lattice U_n is rationally isomorphic, but not isomorphic, to the direct sum $\mathbb{Z} \oplus A_{n-1}$.

1.4 Standard Lattice Constructions

As was already implicitly used above, the direct sum of a finite collection of G-lattices is a G-lattice in the obvious way. In this section, we review some further standard constructions of G-lattices.

Throughout, G will denote a group and L and L' will be G-lattices.

1.4.1 Tensor Products, Symmetric and Exterior Powers

The tensor product $L \otimes_{\mathbb{Z}} L'$ is a G-lattice with the "diagonal" G-action,

$$g(m \otimes m') = g(m) \otimes g(m')$$

for $m \in L$, $m' \in L'$ and $g \in G$. In particular, the n-fold tensor product $L^{\otimes n} = L \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} L$ (n factors) becomes a G-lattice in this fashion. The G-action on $L^{\otimes n}$ passes down to the symmetric power $\mathsf{S}^n L$ and the exterior power $\bigwedge^n L$, making them G-lattices as well. For the general definitions of $\mathsf{S}^n L$ and $\bigwedge^n L$ and the fact that both are $\mathbb{Z}$-free of finite rank, we refer to [25]; see in particular pp. III.75, III.87. For future use, we review the case $n = 2$ in detail:

By definition, $\mathsf{S}^2 L$ is the quotient of $L^{\otimes 2}$ modulo the sublattice that is generated by the elements $m \otimes m' - m' \otimes m$ for $m, m' \in L$. We will write $mm' \in \mathsf{S}^2 L$ for the image of $m \otimes m'$; so $mm' = m'm$. If $\{m_1, \ldots, m_r\}$ is any $\mathbb{Z}$-basis of L then a $\mathbb{Z}$-basis of $\mathsf{S}^2 L$ is given by $\{m_i m_j \mid 1 \le i \le j \le r\}$. Similarly, $\bigwedge^2 L$ is the quotient of $L^{\otimes 2}$ modulo the sublattice that is generated by the elements $m \otimes m$ for $m \in L$. Denoting the image of $m \otimes m'$ in $\bigwedge^2 L$ by $m \wedge m'$, a $\mathbb{Z}$-basis of $\bigwedge^2 L$ is given by $\{m_i \wedge m_j \mid 1 \le i < j \le r\}$. Thus,

$$\operatorname{rank} \mathsf{S}^2 L = \binom{1+r}{2} \quad \text{and} \quad \operatorname{rank} \textstyle\bigwedge^2 L = \binom{r}{2}$$

with $r = \operatorname{rank} L$. In the following lemma, we let $\tau \colon L^{\otimes 2} \to L^{\otimes 2}$ denote the switch map given by $\tau(m \otimes m') = m' \otimes m$.

Lemma 1.4.1. *Let L be a G-lattice. Then:*

(a) *The kernel of the canonical map $L^{\otimes 2} \twoheadrightarrow \bigwedge^2 L$ is the sublattice of symmetric tensors $(L^{\otimes 2})^\tau = \{x \in L^{\otimes 2} \mid \tau(x) = x\}$. Furthermore, there is an exact sequence of G-modules*

$$0 \to \mathsf{S}^2 L \longrightarrow (L^{\otimes 2})^\tau \longrightarrow L \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to 0 \,.$$

(b) *There is an exact sequence of G-lattices*

$$0 \to \bigwedge^2 L \longrightarrow L^{\otimes 2} \xrightarrow{\text{can.}} \mathsf{S}^2 L \to 0 \,.$$

Proof. Fix a $\mathbb{Z}$-basis $\{m_1, \ldots, m_r\}$ for L.

(a) The elements $\{m_i \otimes m_i, m_i \otimes m_j + m_j \otimes m_i \mid 1 \leq i < j \leq r\}$ form a $\mathbb{Z}$-basis of $(L^{\otimes 2})^\tau$. Thus, $(L^{\otimes 2})^\tau \subseteq K := \operatorname{Ker}\left(L^{\otimes 2} \overset{\text{can.}}{\twoheadrightarrow} \bigwedge^2 L\right)$, and $(L^{\otimes 2})^\tau$ and K have the same rank. Since $L^{\otimes 2}/(L^{\otimes 2})^\tau$ is $\mathbb{Z}$-free, we conclude that $(L^{\otimes 2})^\tau$ is equal to K. For the exact sequence, consider the map $\varphi\colon \mathsf{S}^2 L \to (L^{\otimes 2})^\tau$ given by $mm' \mapsto m \otimes m' + m' \otimes m$. This is a well-defined map of G-lattices which is injective, since the $\mathbb{Z}$-basis $\{m_i m_j \mid 1 \leq i \leq j \leq r\}$ of $\mathsf{S}^2 L$ maps to $\mathbb{Z}$-independent elements. Finally, the map $L \to (L^{\otimes 2})^\tau / \operatorname{Im}\varphi$ sending $m \mapsto m \otimes m + \operatorname{Im}\varphi$ is an epimorphism of G-modules with kernel $2L$. The desired sequence follows.

(b) Define the sublattice of antisymmetric tensors in $L^{\otimes 2}$ by $(L^{\otimes 2})^{-\tau} = \{x \in L^{\otimes 2} \mid \tau(x) = -x\}$. A $\mathbb{Z}$-basis of this sublattice is given by $\{m_i \otimes m_j - m_j \otimes m_i \mid 1 \leq i < j \leq r\}$. As in the proof of (a), one sees that $(L^{\otimes 2})^{-\tau}$ is the kernel of the canonical map $L^{\otimes 2} \twoheadrightarrow \mathsf{S}^2 L$. Sending $m \wedge m' \mapsto m \otimes m' - m' \otimes m$ $(m, m' \in L)$, we obtain a well-defined map of G-lattices $\bigwedge^2 L \to (L^{\otimes 2})^{-\tau}$ which sends the basis $\{m_i \wedge m_j \mid 1 \leq i < j \leq r\}$ of $\bigwedge^2 L$ to the above basis of $(L^{\otimes 2})^{-\tau}$. Hence, $\bigwedge^2 L$ is isomorphic to $(L^{\otimes 2})^{-\tau}$, proving the lemma. □

1.4.2 Hom and Duals

The set $\operatorname{Hom}_{\mathbb{Z}}(L, L')$ of all $\mathbb{Z}$-linear maps $f\colon L \to L'$ is a G-lattice with G acting by the rule

$$(gf)(m) = g(f(g^{-1}m)) \,.$$

In particular, taking $L' = \mathbb{Z}$, we obtain the *dual lattice* $L^* = \operatorname{Hom}_{\mathbb{Z}}(L, \mathbb{Z})$ with G-action

$$(gf)(m) = f(g^{-1}m)) \,.$$

(These actions can also be considered, more generally, for G-modules.) There are canonical isomorphisms of G-lattices

$$L \xrightarrow{\sim} L^{**} \quad \text{and} \quad L^* \otimes_{\mathbb{Z}} L' \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}}(L, L')$$

given by $m \mapsto (f \mapsto f(m))$ and $f \otimes m' \mapsto (m \mapsto f(m)m')$, respectively; see [44, 10.26 and 10.30].

If $L \cong L^*$ as G-lattices then L is called *self-dual*. Important examples of self-dual lattices are the permutation lattices introduced in §1.3.1; see §1.4.3 below. If the group G is finite then L and L^* are always at least rationally isomorphic, because $L_{\mathbb{Q}}$ and $L^*_{\mathbb{Q}}$ have the same $\mathbb{Z}$-valued character; see [44, p. 246]. However, the $\mathcal{S}_n$-lattice A_{n-1} in (1.9), for example, is not self-dual. In fact, we will see later (Examples 3.5.6 and 3.6.2) that A_{n-1} and A^*_{n-1} have quite different multiplicative invariant algebras.

1.4.3 Restriction and Induction

If H is any subgroup of G then the G-lattice L may also be viewed as H-lattice. The resulting H-lattice, called *restricted*, will be denoted by

$$L{\downarrow}_H^G \ .$$

Suppose that the index $[G : H]$ is finite and let M be an H-lattice. Then the G-module $\mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} M$ is in fact a G-lattice; it is called the *induced* G-lattice and denoted by

$$M{\uparrow}_H^G \ .$$

For example, the permutation G-lattice $\mathbb{Z}[G/H]$ considered in §1.3.1 is isomorphic to $\mathbb{Z}{\uparrow}_H^G$.

Dualizing commutes with induction:

$$M^*{\uparrow}_H^G \cong \left(M{\uparrow}_H^G\right)^* \ ; \tag{1.11}$$

see [44, 10.28]. In particular, since the trivial H-lattice $\mathbb{Z}$ is clearly self-dual, we see that permutation lattices are self-dual. Moreover, there is an isomorphism of G-lattices, sometimes referred to as “Frobenius reciprocity”,

$$L \otimes_{\mathbb{Z}} \left(M{\uparrow}_H^G\right) \ \cong \ \left(L{\downarrow}_H^G \otimes_{\mathbb{Z}} M\right){\uparrow}_H^G \ ; \tag{1.12}$$

this isomorphism is valid for modules rather than just lattices [44, 10.20]. As a consequence of (1.12), there is an embedding of G-lattices

$$L \hookrightarrow L{\downarrow}_H^G{\uparrow}_H^G \ . \tag{1.13}$$

It is obtained by applying $L \otimes_{\mathbb{Z}} (\,.\,)$ to the embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}{\uparrow}_H^G$, $1 \mapsto \sum_{g \in G/H} g \otimes 1$, and using (1.12) for $M = \mathbb{Z}$ together with the fact that $(\,.\,) \otimes_{\mathbb{Z}} \mathbb{Z}$ is naturally equivalent to the identity.

Finally, if H' is another subgroup of G then the Mackey decomposition theorem yields an isomorphism of H'-lattices

$$M{\uparrow}_H^G{\downarrow}_{H'}^G \cong \bigoplus_{x \in H' \backslash G/H} \left({}^x M{\downarrow}_{H' \cap {}^x H}^{{}^x H}\right){\uparrow}_{H' \cap {}^x H}^{H'} \ . \tag{1.14}$$

Here, $H' \backslash G/H$ denotes a representative set of the (H', H)-double cosets in G. Moreover, ${}^x H = xHx^{-1}$ and ${}^x M$ is the ${}^x H$-lattice $x \otimes M \subseteq M{\uparrow}_H^G$. Again, the isomorphism (1.14) holds more generally for modules; see [44, 10.13].

1.5 Indecomposable Lattices

A G-lattice L is called *indecomposable* if it cannot be written as $L = L_1 \oplus L_2$ with nonzero G-lattices L_i. For example, the $\mathcal{S}_n$-lattice A_{n-1} in (1.9) is indecomposable, being rationally irreducible. Moreover, the permutation lattices $\mathbb{Z}[G/H] = \mathbb{Z}\uparrow_H^G$ considered in §1.4.3 are all indecomposable [44, 32.14].

Clearly, every G-lattice can be decomposed as a direct sum of finitely many indecomposable G-lattices. However, the Krull-Schmidt Theorem fails in general: the decomposition into indecomposable lattices need not be unique up to isomorphism, even for lattices over a finite group $\mathcal{G}$; see, e.g., [97], [88], [7]. Moreover, the set of isomorphism classes of indecomposable $\mathcal{G}$-lattices is usually infinite. The following result, due to Jones [99, 100] (see also [44, 33.6]), describes when this set is finite ("finite representation type"):

Theorem 1.5.1. *Let $\mathcal{G}$ be a finite group. There are only finitely many indecomposable $\mathcal{G}$-lattices (up to isomorphism) precisely if, for each prime p dividing the order $|\mathcal{G}|$, the Sylow p-subgroups of $\mathcal{G}$ are cyclic of order p or p^2.*

The groups $\mathcal{G}$ in this theorem are all metacyclic, that is, they are extensions of one cyclic group by another; see [168, 10.1.10].

Complete sets of indecomposable $\mathcal{G}$-lattices (up to isomorphism) are known for very few finite groups $\mathcal{G}$ only. For the cyclic group $\mathcal{G} = \mathcal{C}_{p^2}$ of order p^2 (p a prime) the lattices are described in [44, 34.35]; for the metacyclic groups $\mathcal{G} = \mathcal{C}_p \rtimes \mathcal{C}_q$ (p, q primes) with $\mathcal{C}_q$ acting faithfully on $\mathcal{C}_p$, see [44, 34.51]. Further references to the literature can be found in [44, p. 753].

We discuss the case of groups of prime order in some more detail:

Example 1.5.2 (Indecomposable lattices for groups of prime order)**.** Let $\mathcal{C}_p$ denote the cyclic group of prime order, p. There are $2h_p + 1$ non-isomorphic indecomposable $\mathcal{C}_p$-lattices, where h_p is the class number of the cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$. These lattices are described in [44, 34.31]. When $h_p = 1$ — this happens precisely for $p \le 19$ [222, Theorem 11.1] — a complete set of non-isomorphic indecomposable $\mathcal{C}_p$-lattices is given by the trivial lattice $\mathbb{Z}$, the regular lattice $\mathbb{Z}[\mathcal{C}_p]$, and the lattice $A_{p-1}\downarrow_{\mathcal{C}_p}^{\mathcal{S}_p}$. Here, $\mathcal{C}_p$ is viewed as the Sylow p-subgroup of $\mathcal{S}_p$. The lattice $A_{p-1}\downarrow_{\mathcal{C}_p}^{\mathcal{S}_p}$ is rationally irreducible; in fact, $(A_{p-1}\downarrow_{\mathcal{C}_p}^{\mathcal{S}_p})_{\mathbb{Q}} \cong \mathbb{Q}(e^{2\pi i/p})$, with a fixed generator of $\mathcal{C}_p$ acting by multiplication with $e^{2\pi i/p}$. For $p = 2$, the lattice $A_{p-1}\downarrow_{\mathcal{C}_p}^{\mathcal{S}_p}$ is isomorphic to the sign lattice $\mathbb{Z}^-$ for $\mathcal{S}_2 = \mathcal{C}_2$. Thus, every $\mathcal{C}_2$-lattice L can be written in the form

$$L \cong \mathbb{Z}[\mathcal{C}_2]^r \oplus \mathbb{Z}^s \oplus (\mathbb{Z}^-)^t\,. \tag{1.15}$$

This is easy to see directly: Say $\mathcal{C}_2 = \langle x \rangle$. Then $(x+1)(L) \subseteq L^{\mathcal{C}_2}$. Thus, x acts on L as a matrix of the form $x_L = \begin{pmatrix} \mathbf{1}_{u\times u} & \boldsymbol{\xi} \\ & -\mathbf{1}_{v\times v} \end{pmatrix}$, where $u = \operatorname{rank} L^{\mathcal{C}_2}$, $v = \operatorname{rank} L/L^{\mathcal{C}_2}$ and $\boldsymbol{\xi} \in \mathrm{M}_{u\times v}(\mathbb{Z})$. Put $M = \begin{pmatrix} \boldsymbol{\alpha} & \boldsymbol{\gamma} \\ & \boldsymbol{\beta} \end{pmatrix}$ with $\boldsymbol{\alpha} \in \mathrm{GL}_u(\mathbb{Z})$, $\boldsymbol{\beta} \in \mathrm{GL}_v(\mathbb{Z})$ and $\boldsymbol{\gamma} \in \mathrm{M}_{u\times v}(\mathbb{Z})$. Then $Mx_LM^{-1} = \begin{pmatrix} \mathbf{1}_{u\times u} & \boldsymbol{\xi}' \\ & -\mathbf{1}_{v\times v} \end{pmatrix}$ with $\boldsymbol{\xi}' = (\boldsymbol{\alpha}\boldsymbol{\xi} - 2\boldsymbol{\gamma})\boldsymbol{\beta}^{-1}$. A suitable choice of M leads to $\boldsymbol{\xi}' = \begin{pmatrix} \mathbf{1}_{r\times r} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, where r is the rank of the matrix $\boldsymbol{\xi}$ mod 2. (Note that $\mathrm{GL}_n(\mathbb{Z})$ maps onto $\mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z})$ for all n.) This implies the isomorphism (1.15), with $s = u - r$ and $t = v - r$.

1.6 Conditioning the Lattice

Let $\mathcal{G}$ be a finite group and L a $\mathcal{G}$-lattice. It is often useful to replace L by a related but better behaved lattice. In this section, we describe two such lattices.

1.6.1 The Effective Quotient

Let $\overline{} : L \twoheadrightarrow L/L^{\mathcal{G}}$ denote the canonical map, where $L^{\mathcal{G}}$ is the sublattice of $\mathcal{G}$-invariants in L. Note that $\overline{L} = L/L^{\mathcal{G}}$ is a $\mathcal{G}$-lattice and the map $\overline{}$ is $\mathcal{G}$-equivariant; so we have an extension of $\mathcal{G}$-lattices

$$0 \longrightarrow L^{\mathcal{G}} \longrightarrow L \xrightarrow{\;\overline{}\;} \overline{L} \longrightarrow 0\,. \tag{1.16}$$

Let

$$\mathcal{G}_m = \{g \in \mathcal{G} \mid g(m) = m\}$$

denote the isotropy (stabilizer) subgroup of $m \in L$ in $\mathcal{G}$, and similarly for $\overline{m} \in \overline{L}$. Then

$$\mathcal{G}_m = \mathcal{G}_{\overline{m}} \tag{1.17}$$

holds for all $m \in L$. This follows from the fact that tensoring sequence (1.16) with $\mathbb{Q}$ yields the *split* sequence of $\mathbb{Q}[\mathcal{G}]$-modules $0 \longrightarrow L_{\mathbb{Q}}^{\mathcal{G}} \longrightarrow L_{\mathbb{Q}} \longrightarrow \overline{L}_{\mathbb{Q}} \longrightarrow 0$ with $L \subseteq L_{\mathbb{Q}}$, $\overline{L} \subseteq \overline{L}_{\mathbb{Q}}$. As a consequence of (1.17), $\overline{L}$ is an effective $\mathcal{G}$-lattice, that is, $\overline{L}^{\mathcal{G}} = \{0\}$. Clearly, every $\mathcal{G}$-lattice homomorphism from L to some effective $\mathcal{G}$-lattice factors through $\overline{L}$. We will call $\overline{L}$ the *effective quotient* of L.

1.6.2 The Lattice $\Lambda_{\mathcal{G}}(L)$

Extend the $\mathcal{G}$-action from L to the $\mathbb{Q}$-vector space $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$ and define $\rho \in \operatorname{End}_{\mathbb{Q}[\mathcal{G}]}(L_{\mathbb{Q}})$ by

$$\rho(v) = |\mathcal{G}|^{-1} \sum_{g \in \mathcal{G}} g(v)\,. \tag{1.18}$$

Then ρ is an idempotent projection of $L_{\mathbb{Q}}$ onto the space of $\mathcal{G}$-invariants $L_{\mathbb{Q}}^{\mathcal{G}}$ and

$$L_{\mathbb{Q}} = \rho(L_{\mathbb{Q}}) \oplus \pi(L_{\mathbb{Q}})\,,$$

where $\pi = \operatorname{Id} - \rho \in \operatorname{End}_{\mathbb{Q}[\mathcal{G}]}(L_{\mathbb{Q}})$. We define

$$\Lambda = \Lambda_{\mathcal{G}}(L) = \{v \in \pi(L_{\mathbb{Q}}) \mid (\operatorname{Id} - g)(v) \in L \text{ for all } g \in \mathcal{G}\}\,. \tag{1.19}$$

and

$$\widehat{L} = \rho(L) \oplus \Lambda\,. \tag{1.20}$$

Lemma 1.6.1. *$\widehat{L}$ is a $\mathcal{G}$-lattice with $L \subseteq \widehat{L}$. Moreover, $\widehat{L}/L$ is finite and $\mathcal{G}$-trivial. If L is effective then $\widehat{L} = \Lambda$ and $\Lambda/L \cong H^1(\mathcal{G}, L)$.*

Proof. Note that, for all $g \in \mathcal{G}$, $(\mathrm{Id} - g_L)\rho = 0$ holds in $\mathrm{End}_{\mathbb{Q}}(L_{\mathbb{Q}})$, and so $(\mathrm{Id} - g_L)\pi = \mathrm{Id} - g_L$. Therefore, $\pi(L) \subseteq \Lambda$ and so $L \subseteq \widetilde{L} := \rho(L) \oplus \pi(L) \subseteq \widehat{L}$. By definition, $\widehat{L}/L$ is $\mathcal{G}$-trivial. Consequently, $\widehat{L}/\widetilde{L} = \Lambda/\pi(L)$ is contained in $(\pi(L_{\mathbb{Q}})/\pi(L))^{\mathcal{G}}$. The exact sequence $0 = \pi(L_{\mathbb{Q}})^{\mathcal{G}} \to (\pi(L_{\mathbb{Q}})/\pi(L))^{\mathcal{G}} \to H^1(\mathcal{G}, \pi(L)) \to H^1(\mathcal{G}, \pi(L_{\mathbb{Q}})) = 0$ shows that

$$(\pi(L_{\mathbb{Q}})/\pi(L))^{\mathcal{G}} \cong H^1(\mathcal{G}, \pi(L)) .$$

Since $H^1(\mathcal{G}, \pi(L))$ is finite, we conclude that $\widehat{L}/\widetilde{L}$ is finite. Moreover $|\mathcal{G}|\widetilde{L} \subseteq L$, which proves that $\widehat{L}/L$ is finite. Finally, if L is effective then $\rho = 0$ and $\pi = \mathrm{Id}$, and hence $\widehat{L} = \Lambda$ and $\Lambda/L = (L_{\mathbb{Q}}/L)^{\mathcal{G}}$. The above isomorphism now shows that $\Lambda/L \cong H^1(\mathcal{G}, L)$, as we have claimed. □

1.7 Reflections and Generalized Reflections

Let V be a vector space. An endomorphism φ of V is called a *k-reflection* if

$$\mathrm{rank}(\varphi - \mathrm{Id}_V) \leq k .$$

We will refer to 1-reflections and 2-reflections as *reflections* and *bireflections*, respectively. (In Bourbaki [24], reflections are more narrowly defined as 1-reflections of order 2, and nonidentity 1-reflections are called pseudo-reflections.)

Now suppose that the group G acts on V by means of a representation $G \to \mathrm{GL}(V)$, $g \mapsto g_V$. An element $g \in G$ is said to act as a k-reflection on V if g_V is a k-reflection, that is, the subspace

$$[g, V] = \mathrm{Im}(g_V - \mathrm{Id}_V) = \{g(v) - v \mid v \in V\} \tag{1.21}$$

satisfies $\dim[g, V] \leq k$. One easily verifies that, for $g, h \in G$,

$$[g^{-1}, V] = [g, V] \tag{1.22}$$

$$[{}^h g, V] = h([g, V]) \tag{1.23}$$

$$[gh, V] \subseteq [g, V] + [h, V] \tag{1.24}$$

Here, ${}^h g = hgh^{-1}$. Thus, inverses and conjugates of k-reflections are k-reflections, and products of k-reflections and k'-reflections are $(k + k')$-reflections. In particular, the subgroups

$$\mathcal{R}_V^k(G) = \langle g \in G \mid g \text{ acts as a } k\text{-reflection on } V \rangle . \tag{1.25}$$

form an increasing sequence of normal subgroups of G such that $\mathcal{R}_V^k(G)\mathcal{R}_V^{k'}(G) \subseteq \mathcal{R}_V^{k+k'}(G)$. The minimum k with $\mathcal{R}_V^k(G) \neq 1$ is called the *class* of G on V in Gordeev [75]. The group G is called emph$k$-reflection group on V if $G = \mathcal{R}_V^k(G)$.

Proposition 1.7.1. *If G is a k-reflection group on V then every subgroup of index m is a km-reflection group on V.*

Proof. In view of equations (1.22) - (1.24), the proposition is a consequence of the following purely group theoretical fact.

Claim. Let G be a group and let S be a fixed generating set of G that is closed under taking inverses and G-conjugates. Then any subgroup $H \leq G$ with $[G : H] \leq m$ can be generated by elements that can be written as products of length $\leq m$ with factors from S.

I am indebted to Victor Guba for the following geometric proof. My terminology concerning graphs follows [50] or [194].

Let Γ be the graph with vertex set $H\backslash G$, the set of right cosets of H in G, and with oriented edge set $H\backslash G \times S$. An oriented edge $e = (Hg, s)$ can be visualized as a directed line segment from the vertex Hg to Hgs labelled by s:

$$e\colon\ Hg \bullet\!\xrightarrow{s}\!\bullet Hgs$$

There are $m = [G : H]$ vertices and any two vertices can be joined by a path in Γ, since S generates G. Each path p is labelled by a group word in S. The inverse path, denoted by p^{-1} and thought of as travelling along p in the opposite direction, is labelled by the inverse word. The paths from the vertex H to itself are labelled exactly by the words representing elements of the subgroup H.

Now choose a maximal subtree T of Γ. This is a subgraph of Γ containing all m vertices of Γ and the inverses of all its edges. Furthermore, for any two vertices v and w, there is a unique path from v to w in T which involves no backtracking; this path is called the T-geodesic from v to w. For any vertex v, let $p(v)$ denote the T-geodesic from the vertex H to v. For any edge e that is not an edge of T, consider the path $p(v)ep(w)^{-1}$, where v and w are the initial and the terminal vertex of e. This is a path from H to H, and so its label defines a group element $h(e) \in H$. The elements $h(e)$ generate H. To see this, write a given $h \in H$ as a word in S and consider the path p from H to H that is labelled by this word. If all edges of p belong to T then $h = 1$. Otherwise let e_0 be the first edge of p that does not belong to T, let w be its terminal vertex, and let p' be the tail of p from w to H. Then $h = h(e_0)h'$, where $h' \in H$ corresponds to the path $p(w)p'$ from H to H. Since the latter path has fewer edges not belonging to T, we may conclude by induction that h' can be generated by the elements $h(e)$. Therefore, these elements do indeed generate H.

It suffices to show that each $h(e)$ can be written as a product of length $\leq m$ in S. Recall that $h(e)$ is represented by the path $p(v)ep(w)^{-1}$, as above. Let p be the longest common initial segment of $p(v)$ and $p(w)$ and write $p(v) = pq$, $p(w) = pr$. Then qer^{-1} is a closed path in Γ without any repeated vertices other than its end vertices; this follows from the fact that q and r are geodesic paths in a tree. Therefore, the path qer^{-1} has length at most m, the number of vertices in Γ. Its label defines an element $g \in G$ of length $\leq m$ in S, and $h(e) = {}^{x}g$ where $x \in G$ is given by the label of the common initial segment p. Since ${}^{x}S \subseteq S$, we conclude that $h(e)$ also has length $\leq m$ in S. This proves the claim, and hence the proposition. □

1.7.1 Reflections on Lattices

The foregoing applies in particular to lattices L via the embedding $L \subseteq L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$: if L is a G-lattice then an element $g \in G$ is said to act as a k-reflection on L if and only if g is a k-reflection on $L_{\mathbb{Q}}$. Explicitly, this means that the sublattice

$$[g, L] = \{g(m) - m \mid m \in L\} \tag{1.26}$$

of L has rank at most k or, equivalently, the g-fixed points of the $\mathbb{Q}$-space $L_{\mathbb{Q}}$ have codimension at most k.

Now assume that L is a $\mathcal{G}$-lattice of rank n, where $\mathcal{G}$ is a finite group. Let $g \in \mathcal{G}$ act as a nonidentity reflection on L. Then the endomorphism $g_L \in \mathrm{GL}(L)$ is conjugate in $\mathrm{GL}(L_{\mathbb{Q}}) \cong \mathrm{GL}_n(\mathbb{Q})$ to the diagonal matrix $\mathrm{diag}(-1, 1, \ldots, 1)_{n\times n}$. In particular, g_L has order 2 and

$$L_g^- := \mathrm{Ker}_L(g_L + \mathrm{Id}_L) \cong \mathbb{Z} \tag{1.27}$$

By (1.15), the $\langle g\rangle$-lattice L is isomorphic to $\mathbb{Z}^{n-1} \oplus \mathbb{Z}^-$ or to $\mathbb{Z}^{n-2} \oplus \mathbb{Z}[\langle g_L\rangle]$.

In the former case, g_L is conjugate in $\mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$ to

$$d = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

and $H^1(\langle g\rangle, L) \cong H^1(\langle g\rangle, \mathbb{Z}^-) \cong \mathbb{Z}/2\mathbb{Z}$. We shall call g a *diagonalizable reflection* on L in this case.

In the second case, g_L is conjugate in $\mathrm{GL}_n(\mathbb{Z})$ to

$$s = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

and $H^1(\langle g\rangle, L) = \{0\}$.

Lemma 1.7.2. *Let L be a faithful $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group. Let $d_1, \ldots, d_r \in \mathcal{G}$ be the distinct non-identity reflections on L which are diagonalizable. Then $\mathcal{D} = \langle d_1, \ldots, d_r\rangle$ is a normal subgroup of $\mathcal{G}$ and $\mathcal{D} \cong C_2^r$. Moreover,*

$$L = L^{\mathcal{D}} \oplus \bigoplus_{i=1}^{r} \mathbb{Z}\ell_i\ ,$$

with $d_i(\ell_i) = -\ell_i$, $d_i(\ell_j) = \ell_j$ $(i \neq j)$. The group $\mathcal{G}$ stabilizes the sublattice of $\mathcal{D}$-invariants $L^{\mathcal{D}}$ and permutes the lattices $\mathbb{Z}\ell_i$.

Proof. The d_i are exactly those nonidentity reflections in $\mathcal{G}$ that belong to the congruence subgroup $\Gamma(2) = \{\gamma \in \mathrm{GL}(L) \mid \gamma \text{ is trivial on } L/2L\}$. Since every torsion element of $\Gamma(2)$ has order 2 (e.g., [31, Exercise II.4.3]), $\mathcal{D}$ is an elementary abelian 2-group. Clearly, $\mathcal{G}$ permutes the d_i. Therefore, $\mathcal{G}$ stabilizes $\mathcal{D}$ and $L^{\mathcal{D}}$ and permutes the sublattices $L^-_{d_i} = \mathrm{Ker}_L(d_i + \mathrm{Id}_L)$.

By (1.27), we may write $L^-_{d_i} = \mathbb{Z}\ell_i$; so $d_i(\ell_i) = -\ell_i$. It remains to show that $d_i(\ell_j) = \ell_j$ holds for $i \neq j$ and $L = L^{\mathcal{D}} \oplus \bigoplus_{i=1}^r \mathbb{Z}\ell_i$. This will also imply that $\mathcal{D}$ has rank r. For any d_i, we have $L = L^+_{d_i} \oplus L^-_{d_i}$, where $L^+_{d_i}$ is the sublattice of d_i-invariants in L. Both summands are $\mathcal{D}$-stable, because $\mathcal{D}$ is commutative. Any d_j with $i \neq j$ must act trivially on $L^-_{d_i} = \mathbb{Z}\ell_i$. For, otherwise d_j would have to act as -1 on $L^-_{d_i}$ and trivially on $L^+_{d_i}$, and hence $d_j = d_i$. Thus, $L^-_{d_i} \subseteq L^+_{d_j}$ and so $L^+_{d_j} = \left(L^+_{d_i} \cap L^+_{d_j}\right) \oplus L^-_{d_i}$. Therefore, $L = \left(L^+_{d_i} \cap L^+_{d_j}\right) \oplus L^-_{d_i} \oplus L^-_{d_j}$ and the asserted decomposition follows by induction. □

1.8 Lattices Associated with Root Systems

A large supply of interesting lattices and groups are constructed from root systems. Therefore, we include here a review of this topic. Complete details and much more information can be found in Bourbaki [24] or Humphreys [93], for example.

1.8.1 Root Systems

Let V be a finite-dimensional nonzero $\mathbb{R}$-vector space. Put $V^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ and let $\langle .\,, . \rangle \colon V^* \times V \to \mathbb{R}$ denote the evaluation pairing. A subset $\Phi \subseteq V$ is called a *reduced root system* in V if the following axioms are satisfied:

(R1) Φ is finite, does not contain 0, and spans V.

(R2) For each $m \in \Phi$ there exists a linear form $m^\vee \in V^*$ with $\langle m^\vee, m\rangle = 2$ and such that the reflection $s_m \in \mathrm{End}_{\mathbb{R}}(V)$ that is defined by

$$s_m(v) = v - \langle m^\vee, v\rangle m$$

maps Φ to itself. (It follows from **R1** that $m^\vee$ is uniquely determined by these conditions; see [24, p. 143].)

(R3) $\langle m^\vee, \Phi\rangle \subseteq \mathbb{Z}$ holds for all $m \in \Phi$.

(R4) If $m \in \Phi$ then $2m \notin \Phi$.

Sometimes reduced root systems are simply called *root systems* in the literature or else *crystallographic root systems*. The linear forms $m^\vee$ $(m \in \Phi)$ form a reduced root system in V^* which is denoted by $\Phi^\vee$.

A root system Φ in V is called *irreducible* if it is not possible to write $V = V_1 \oplus V_2$ and $\Phi = \Phi_1 \cup \Phi_2$ with nonzero subspaces $V_i \subseteq V$ and root systems Φ_i in V_i. The irreducible reduced root systems have been classified: they are known as the root systems of types A_n $(n \geq 1)$, B_n $(n \geq 2)$, C_n $(n \geq 3)$, D_n $(n \geq 4)$ E_6, E_7, E_8,

F_4, and G_2. Type A_n in particular will make frequent appearances in later sections. It will be described in detail in Example 1.8.1 below. For the other types, see [24, Planches I - IX].

1.8.2 Weyl Group and Automorphism Group

The *automorphism group* of a reduced root system $\varPhi$ in V is defined by

$$\operatorname{Aut}(\varPhi) = \{g \in \operatorname{GL}(V) \mid g(\varPhi) \subseteq \varPhi\} .$$

By virtue of **R1**, $\operatorname{Aut}(\varPhi)$ is a finite subgroup of $\operatorname{GL}(V)$. The reflections s_m in **R2** are elements of order 2 in $\operatorname{Aut}(\varPhi)$; they generate the so-called *Weyl group* of $\varPhi$:

$$\mathcal{W} = \mathcal{W}(\varPhi) = \langle s_m \mid m \in \varPhi \rangle .$$

Since $\varPhi^\vee$ spans V^*, the space $V^{\mathcal{W}}$ of $\mathcal{W}$-invariants in V is $\{0\}$.

The canonical isomorphism $\operatorname{GL}(V) \xrightarrow{\sim} \operatorname{GL}(V^*), u \mapsto {}^t u^{-1}$ (t = transpose), sends $\operatorname{Aut}(\varPhi)$ to $\operatorname{Aut}(\varPhi^\vee)$ and $\mathcal{W}(\varPhi)$ to $\mathcal{W}(\varPhi^\vee)$; see [24, p. 144]. In practise, one usually identifies V^* with V by means of a fixed $\operatorname{Aut}(\varPhi)$-invariant positive definite bilinear form on V. Such a form always exists since $\operatorname{Aut}(\varPhi)$ is finite. In this fashion, $\varPhi^\vee$ can be viewed as a root system in V.

1.8.3 Base of a Root System

A subset $\varDelta$ of a root system $\varPhi$ in V is called a *base* of $\varPhi$ if

(B1) $\varDelta$ is a basis of the vector space V, and

(B2) Every root $m \in \varPhi$ can be written as $m = \sum_{a \in \varDelta} z_a a$ or as $m = -\sum_{a \in \varDelta} z_a a$ with non-negative integers $z_a \in \mathbb{Z}_+$. Thus,

$$\varPhi = \mathbb{Z}_+ \varDelta \coprod -\mathbb{Z}_+ \varDelta .$$

A base always exists and is essentially unique: the Weyl group $\mathcal{W} = \mathcal{W}(\varPhi)$ acts simply transitively on the set of all bases for $\varPhi$. Moreover, if $\varDelta$ is a base for $\varPhi$ then $\varPhi = \{s(a) \mid a \in \varDelta, s \in \mathcal{W}\}$ and $\varDelta^\vee = \{a^\vee \mid a \in \varDelta\}$ is a base for $\varPhi^\vee$; see [24, pp. 153/4 and 167].

1.8.4 Root Lattice and Weight Lattice

The *root lattice*, $L = L(\varPhi)$, and the *weight lattice*, $\varLambda = \varLambda(\varPhi)$, of $\varPhi$ are defined by

$$L = \mathbb{Z}\varPhi = \{\sum_{m \in \varPhi} z_m m \mid z_m \in \mathbb{Z}\}$$

and

$$\varLambda = \{v \in V \mid \langle m^\vee, v \rangle \in \mathbb{Z} \text{ for all } m \in \varPhi\} .$$

Both L and Λ are stable under $\mathrm{Aut}(\Phi)$; they are faithful and effective lattices for $\mathrm{Aut}(\Phi)$ and for $\mathcal{W}(\Phi)$. By axiom **R3**, $L \subseteq \Lambda$. Furthermore, the definition of Λ implies that the Weyl group $\mathcal{W} = \mathcal{W}(\Phi)$ acts trivially on Λ/L. The weight lattice Λ can be calculated directly from the root lattice L :

$$\Lambda = \Lambda_{\mathcal{W}}(L) \ . \tag{1.28}$$

Here, the right hand side is defined by (1.19). Thus, Λ/L is finite and isomorphic to $H^1(\mathcal{W}, L)$; see Lemma 1.6.1. Identifying $\mathrm{Aut}(\Phi)$ with $\mathrm{Aut}(\Phi^\vee)$ as explained in §1.8.2, we can view $L(\Phi^\vee)$ as $\mathrm{Aut}(\Phi)$-lattice. In fact,

$$\Lambda(\Phi) \cong L(\Phi^\vee)^* \tag{1.29}$$

as $\mathrm{Aut}(\Phi)$-lattices.

Any base Δ of Φ is clearly a $\mathbb{Z}$-basis for the root lattice $L(\Phi)$. The basis of V that is dual to the basis $\Delta^\vee$ of V^* forms a $\mathbb{Z}$-basis of the weight lattice $\Lambda(\Phi)$. The elements of this basis are called the *fundamental weights* (or *fundamental dominant weights*) relative to Δ.

Example 1.8.1 (Type A_n)**.** Let V denote the kernel of the linear form $\mathbb{R}^{n+1} \to \mathbb{R}$ sending all canonical basis vectors e_i of $\mathbb{R}^{n+1}$ to 1. Then

$$\Phi = \{e_i - e_j \mid i \neq j, 1 \leq i, j \leq n+1\}$$

is a root system in V, the so-called root system of type A_n. A base Δ for Φ is given by the roots

$$a_i = e_i - e_{i+1} \quad (i = 1, \ldots, n) \ .$$

The Weyl group $\mathcal{W}(A_n)$ is the symmetric group $\mathcal{S}_{n+1}$ on $\{1, \ldots, n+1\}$, acting on V via the standard $\mathcal{S}_{n+1}$-permutation operation on $\mathbb{R}^{n+1}$: $s(e_i) = e_{s(i)}$ $(s \in \mathcal{S}_{n+1})$. The automorphism group of Φ is given by

$$\mathrm{Aut}(A_n) = \{\pm 1\} \times \mathcal{S}_{n+1} \qquad (n \geq 2) \ , \tag{1.30}$$

where -1 acts on V by multiplication with -1; for $n = 1$, one has $\mathrm{Aut}(A_1) = \mathcal{S}_2$.

The standard bilinear form on $\mathbb{R}^{n+1}$, $(e_i, e_j) = \delta_{i,j}$ (Kronecker delta), is positive definite and $\mathrm{Aut}(A_n)$-invariant. Identifying V^* with V by means of this form, we have $m^\vee = m$ for all $m \in \Phi$; so $\Phi^\vee = \Phi$.

The root lattice $L = \mathbb{Z}\Phi$ will simply be written as A_n; so

$$A_n = \left\{ \sum_{i=1}^{n+1} z_i e_i \,\middle|\, z_i \in \mathbb{Z}, \sum_i z_i = 0 \right\} = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n \ .$$

This lattice was already introduced earlier in (1.9). By (1.29), the weight lattice $\Lambda(A_n)$ can be identified with A_n^*; it is explicitly given by

$$\Lambda(A_n) = A_n + \mathbb{Z}a \quad \text{with} \quad a = e_1 - \tfrac{1}{n+1} \sum_1^{n+1} e_i = \sum_{i=1}^{n} \tfrac{n+1-i}{n+1} a_i \in V \ .$$

Note that $\Lambda(A_n)/A_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$ with trivial $\mathcal{S}_{n+1}$-action. Thus, we have an exact sequence of $\mathcal{S}_{n+1}$-modules

$$0 \to A_n \longrightarrow A_n^* \longrightarrow \mathbb{Z}/(n+1)\mathbb{Z} \to 0\,. \tag{1.31}$$

1.9 The Root System Associated with a Faithful $\mathcal{G}$-Lattice

Let L be a faithful $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group. As in (1.25), we define the reflection subgroup of $\mathcal{G}$ by

$$\mathcal{R} = \mathcal{R}_L^1(\mathcal{G}) = \langle g \in \mathcal{G} \mid g \text{ acts as a reflection on } L\rangle\,.$$

For each reflection $g \in \mathcal{G}$, denote the two possible generators of $L_g^- = \mathrm{Ker}_L(g_L + \mathrm{Id}_L)$ by $\pm\ell_g$; see (1.27). Define

$$\Phi = \Phi_{\mathcal{G}}(L) = \{\pm\ell_g \mid g \text{ a reflection in } \mathcal{G}\}\,. \tag{1.32}$$

We shall show that Φ is a reduced root system with Weyl group $\mathcal{R}$ and that $\mathcal{R}$ has a complement in $\mathcal{G}$. These are well-known facts; see, e.g., Bourbaki [24], Farkas [61], Humphreys [94], and Lemire [115].

View $\mathcal{G}$ as acting (faithfully) on the real vector space $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$ and let $\rho\colon L_{\mathbb{R}} \twoheadrightarrow L_{\mathbb{R}}^{\mathcal{R}}$ be the projection defined by $\rho(v) = |\mathcal{R}|^{-1}\sum_{g\in\mathcal{R}} g(v)$. Note that $\rho \in \mathrm{End}_{\mathbb{R}[\mathcal{G}]}(L_{\mathbb{R}})$, since $\mathcal{R}$ is normal in $\mathcal{G}$. Put $\pi = \mathrm{Id} - \rho \in \mathrm{End}_{\mathbb{R}[\mathcal{G}]}(L_{\mathbb{R}})$ and let

$$V = \mathrm{Ker}_{L_{\mathbb{R}}}(\rho) = \pi(L_{\mathbb{R}})\,.$$

Thus, $L_{\mathbb{R}} = L_{\mathbb{R}}^{\mathcal{R}} \oplus V$, both summands are $\mathcal{G}$-stable, and $\mathcal{R}$ acts faithfully and effectively on V.

Proposition 1.9.1. *Let L be a faithful $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and let $\mathcal{R} = \mathcal{R}_L^1(\mathcal{G})$, $\Phi = \Phi_{\mathcal{G}}(L)$ and V be defined as above. Then:*

(a) *Φ is a reduced root system in V. The Weyl group $\mathcal{W}(\Phi)$ is the restriction of $\mathcal{R}$ to V and the weight lattice $\Lambda(\Phi)$ is the lattice $\Lambda_{\mathcal{R}}(L)$ defined in* (1.19). *Both Φ and $\Lambda(\Phi)$ are stable under $\mathcal{G}$.*

(b) *Fix a base Δ for Φ. Then $\mathcal{G}_\Delta = \{g \in \mathcal{G} \mid g(\Delta) = \Delta\}$ is a complement for $\mathcal{R}$ in $\mathcal{G}$; so $\mathcal{G} = \mathcal{R} \rtimes \mathcal{G}_\Delta$.*

Proof. (a) Note that, for each reflection $g \in \mathcal{G}$, we can write $\rho = \rho' \circ (g_L + \mathrm{Id}_L)$ for some $\rho' \in \mathrm{End}_{\mathbb{R}}(L_{\mathbb{R}})$. Hence, $L_g^- = \mathrm{Ker}_L(g + \mathrm{Id}) \subseteq \mathrm{Ker}_{L_{\mathbb{R}}}(\rho) = V$, and so $\Phi \subseteq V$. Also, $\mathcal{G}$ permutes the reflections in $\mathcal{G}$ by conjugation. Thus, the action of $\mathcal{G}$ on L permutes the various L_g^- for reflections $g \in \mathcal{G}$, and hence $\mathcal{G}$ stabilizes the collection of all their generators, that is, Φ.

We verify axioms **R1** - **R4** in §1.8.1 for Φ.

As for **R1**, only the fact that Φ spans V requires comment. To see this, let $V' = \mathbb{R}\Phi$ denote the $\mathbb{R}$-linear span of Φ in V. Note that V' is a $\mathcal{G}$-stable subspace of V, because Φ is $\mathcal{G}$-stable. By Maschke's Theorem, we may write $V = V' \oplus U$ for some

$\mathcal{G}$-stable subspace U. Each reflection $g \in \mathcal{G}$ acts trivially on L/L_g^-, and hence on $V/V' = U$. Therefore, $U \subseteq V^{\mathcal{R}} = \{0\}$ and so $V = V'$, as required.

To prove **R2**, let $g \in \mathcal{G}$ act as a reflection on L. Then g maps Φ to itself, since Φ is $\mathcal{G}$-stable. Moreover, since g has order 2 , we have $g(v) - v \in \operatorname{Ker}_V(g + \operatorname{Id}) = \mathbb{R}\ell_g$ for all $v \in V$. Thus, $g(v) = v + r_{g,v}\ell_g$ for some $r_{g,v} \in \mathbb{R}$. The map $v \mapsto r_{g,v}$ is the required linear form $\ell_g^\vee \in V^*$.

For **R3**, note that, choosing $v \in \Phi$ in the preceding paragraph, we obtain $g(v) - v \in \operatorname{Ker}_L(g + \operatorname{Id}) = \mathbb{Z}\ell_g$; so $\langle \ell_g^\vee, v\rangle = r_{g,v} \in \mathbb{Z}$, as required.

Finally, since L/L_g^- is $\mathbb{Z}$-free, no element of $2L$ can be a generator of L_g^-. This proves **R4**, thereby completing the proof that Φ is a reduced root system in V.

In our present setting, the reflections s_m $(m \in \Phi)$ in **R2** are given by $s_{\pm\ell_g} = g_V$ for each reflection $g \in \mathcal{G}$. Thus, the Weyl group $\mathcal{W} = \mathcal{W}(\Phi)$ is $\mathcal{R}$ acting on V.

Finally, by (1.19) and (1.28), the weight lattice of $\Phi = \Phi_{L,\mathcal{G}}$ can be written as

$$\Lambda(\Phi) = \Lambda_{\mathcal{W}}(L(\Phi)) = \{v \in L(\Phi) \otimes_{\mathbb{Z}} \mathbb{Q} \mid (\operatorname{Id} - g)(v) \in L(\Phi) \text{ for all } g \in \mathcal{R}\}\ .$$

Since $L(\Phi) \otimes_{\mathbb{Z}} \mathbb{Q} = \pi(L_{\mathbb{Q}})$, we obtain that $\Lambda(\Phi) = \Lambda_{\mathcal{R}}(L)$. Also, since $L(\Phi)$ and $\mathcal{R}$ are $\mathcal{G}$-stable, so is $\Lambda(\Phi)$.

(b) For each $g \in \mathcal{G}$, $g(\Delta)$ is another base of $\Phi = \Phi_{\mathcal{G}}(L)$. Since $\mathcal{W}(\Phi) = \mathcal{R}$ acts simply transitively on the set of bases of Φ (see §1.8.3), there exists a unique $r \in \mathcal{R}$ with $g(\Delta) = r(\Delta)$. This proves (b). □

1.10 Finite Subgroups of $\mathrm{GL}_n(\mathbb{Z})$

By a celebrated theorem of Jordan [102], each $\mathrm{GL}_n(\mathbb{Z})$ has only finitely many finite subgroups, $\mathcal{G}$, up to conjugacy. The actual numbers, even for relatively small n, do however quickly become rather formidable while the number of maximal finite subgroups grows at a much slower rate; see Table 1.1. [1]

Proposition 1.1. *Let Φ be an irreducible reduced root system not of type C_4 and let $L = L(\Phi)$ be its root lattice. The action of* $\operatorname{Aut}(\Phi)$ *on L realizes* $\operatorname{Aut}(\Phi)$ *as a maximal finite subgroup of* $\mathrm{GL}(L)$.

Proof. Say Φ is a root system in the real vector space V. There exists a unique (up to scalar multiples) positive definite symmetric bilinear form $\beta\colon V \times V \to \mathbb{R}$ that is invariant under $\operatorname{Aut}(\Phi)$; see [24, Prop. VI.1.3 and Prop. VI.1.7]. Suppose that $\operatorname{Aut}(\Phi) \subseteq \mathcal{G}$ for some finite subgroup $\mathcal{G}$ of $\mathrm{GL}(L)$. Then $\mathcal{G}$ fixes some positive definite symmetric bilinear form $\beta'\colon V \times V \to \mathbb{R}$. Indeed, β' can be obtained by averaging any positive definite symmetric bilinear form on V over $\mathcal{G}$. Since β' is in particular $\operatorname{Aut}(\Phi)$-invariant, we have $\beta' = c\beta$ for some positive scalar c, by uniqueness of β. Thus, β is $\mathcal{G}$-invariant. Therefore, $\mathcal{G}$ stabilizes the set

[1] The first column is contained in [150]. The number of maximal finite subgroups, up to conjugacy, can be computed with CARAT [34]. For $\mathrm{GL}_6(\mathbb{Z})$, it was communicated to me by Nebe and Schulz.

Table 1.1. Finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$

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

$S = \{\ell \in L \setminus \{0\} \mid \beta(\ell,\ell)$is minimal$\}$. By [24, Exercise VI.1.19], S is the set of "short roots" in Φ. In case Φ has only one root length, we conclude that $\mathcal{G}$ stabilizes Φ and hence is contained in $\mathrm{Aut}(\Phi)$, as desired.

This leaves the root systems of types B_n, C_n, F_4 and G_2 to consider. Direct inspection of these root systems using [24, Planches II,III,VIII,IX] reveals that in all cases but C_n $(n \geq 4)$, the set $T = \{\ell \in L \setminus (S \cup \{0\}) \mid \beta(\ell,\ell)$is minimal$\}$ is the set of long roots in Φ. Since T is $\mathcal{G}$-stable, we again conclude that $\mathcal{G}$ maps Φ to itself, and hence $\mathcal{G} \subseteq \mathrm{Aut}(\Phi)$.

The above reasoning does not apply to type $C_n = B_n^\vee$ $(n \geq 4)$: the sum of two orthogonal short simple roots in Φ has the same length as a long root but is not a root in this case. However,

$$\mathrm{Aut}(C_n) = \mathrm{Aut}(B_n) \cong \{\pm 1\} \wr \mathcal{S}_n \ , \tag{1.33}$$

and the weight lattice $\Lambda(C_n)$ coincides with the root lattice $L(B_n)$. Thus, $L(C_n) \otimes \mathbb{Q} = L(B_n) \otimes \mathbb{Q}$ as rational representations of $\mathrm{Aut}(C_n) = \mathrm{Aut}(B_n)$. Moreover, for $n \neq 4$, one knows that the action of $\mathrm{Aut}(B_n)$ on $L(B_n) \otimes \mathbb{Q}$ realizes $\mathrm{Aut}(B_n)$ as a maximal finite subgroup of $\mathrm{GL}(L(B_n) \otimes \mathbb{Q}) = \mathrm{GL}_n(\mathbb{Q})$; see [149, (II.8)]. Therefore, the action of $\mathrm{Aut}(C_n)$ on $L(C_n)$ realizes $\mathrm{Aut}(C_n)$ as a maximal finite subgroup of $\mathrm{GL}(L(C_n))$ if $n \neq 4$. □

We remark that, by (1.29), $L(C_n) \cong \Lambda(B_n)^*$ as $\mathrm{Aut}(C_n)$-lattices, and $\Lambda(B_4) = L(F_4)$; see [24]. The action of $\mathrm{Aut}(C_4)$ on $L(C_4) \cong L(F_4)^*$ embeds $\mathrm{Aut}(C_4)$ as a subgroup of ${}^t\mathrm{Aut}(F_4)$, with index 3.

1.10.1 Representative Groups

The conjugacy classes of all finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ are well-known and easy to determine; cf., e.g., Newman [140, p. 180]. A full set of non-trivial representative groups is listed in Table 1.2. We use the following notations:

$$d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad x = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}. \tag{1.34}$$

Moreover, $\mathrm{Aut}(\varPhi)$ and $\mathcal{W}(\varPhi)$ without further explanation denote the automorphism group and the Weyl group of the root system $\varPhi$ acting on the root lattice $L(\varPhi) = \mathbb{Z}\varPhi$.

Table 1.2. The nontrivial finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$

label	generators; see (1.34)	isomorphism type	description
$\mathcal{G}_1$	x, s	$\mathcal{D}_{12}$	$\mathrm{Aut}(A_2) = \mathcal{W}(G_2)$
$\mathcal{G}_2$	d, s	$\mathcal{D}_8 \cong \{\pm 1\} \wr \mathcal{S}_2$	$\mathrm{Aut}(B_2) = \mathcal{W}(B_2)$
$\mathcal{G}_3$	$x^2, -s$	$\mathcal{D}_6 \cong \mathcal{S}_3$	$\mathcal{W}(A_2)$
$\mathcal{G}_4$	x^2, s	$\mathcal{D}_6 \cong \mathcal{S}_3$	$\mathcal{W}(A_2)$ on $A_2^* \cong \overline{U_3}$; see (3.15)
$\mathcal{G}_5$	$d, -d$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{W}(A_1) \times \mathcal{W}(A_1)$
$\mathcal{G}_6$	$s, -s$	$\mathcal{C}_2 \times \mathcal{C}_2$	
$\mathcal{G}_7$	x	$\mathcal{C}_6$	$\mathrm{Aut}(A_2) \cap \mathrm{SL}_2(\mathbb{Z})$
$\mathcal{G}_8$	ds	$\mathcal{C}_4$	$\mathrm{Aut}(B_2) \cap \mathrm{SL}_2(\mathbb{Z})$
$\mathcal{G}_9$	x^2	$\mathcal{C}_3$	
$\mathcal{G}_{10}$	$x^3 = -\mathrm{Id}$	$\mathcal{C}_2$	
$\mathcal{G}_{11}$	d	$\mathcal{C}_2$	$\mathcal{W}(A_1) \times \langle \mathrm{Id}_{\mathbb{Z}} \rangle$
$\mathcal{G}_{12}$	s	$\mathcal{C}_2 \cong \mathcal{S}_2$	$\mathcal{S}_2$ on U_2; see (1.7)

Representatives for the conjugacy classes of all finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ for $n = 3$ can be found in Tahara [214]. (It was pointed out in [1] that the group listed as W_5 on the page 198 in [214] is redundant.) For representative finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ with $n \leq 4$, see Brown et al. [30]. The maximal finite subgroups of $\mathrm{GL}_4(\mathbb{Z})$ and $\mathrm{GL}_5(\mathbb{Z})$, up to conjugacy, were first determined in Dade [46] and Ryškov-Lomakina [174], respectively.

Alternatively, representatives for the conjugacy classes of finite subgroups $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$ with $n \leq 4$ can be accessed through the crystallographic groups library “crystcat” of the computer algebra system GAP [71]. The more specialized computer algebra system CARAT [34], [145] provides the groups $\mathcal{G}$ (and more) up to $n = 6$. Moreover, GAP and MAGMA [20] both have data bases of all maximal finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ for n up to 31. These are based on Nebe [137], [138]. Note that if $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Q})$ is finite then $\mathcal{G}$ stabilizes the lattice $L = \sum_{g \in \mathcal{G}} g(\mathbb{Z}^n)$ in $\mathbb{Q}^n$. Any $\mathbb{Z}$-basis of L is $\mathbb{Q}$-basis of $\mathbb{Q}^n$. Hence, $g\mathcal{G}g^{-1} \subseteq \mathrm{GL}_n(\mathbb{Z})$ for some $g \in \mathrm{GL}_n(\mathbb{Q})$.

1.10.2 Sizes: The Minkowski Bound

The least common multiple of the orders of all finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ or, equivalently, of $\mathrm{GL}_n(\mathbb{Q})$ is given by the *Minkowski bound* [133]:

$$M(n) = \prod_p p^{\left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots} \tag{1.35}$$

Here, $\lfloor x \rfloor$ denotes the greatest integer $\leq x$ and p runs over all primes. The p-factors for $p > n+1$ are all equal to 1. More generally, by Schur [191], the order of any finite subgroup $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{C})$ all of whose elements have rational trace divides $M(n)$.

The asymptotic order of $M(n)$ has been calculated by Katznelson [107]:

$$\lim_{n \to \infty} (M(n)/n!)^{1/n} = \prod_p p^{1/(p-1)^2} \approx 3.4109 \, .$$

A related issue is the determination of the largest finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$. Note that $\mathrm{Aut}(B_n) = \{\pm 1\} \wr \mathcal{S}_n$ is a subgroup of order $2^n n!$. Feit [62] has shown that, for all $n > 10$ and for $n = 1, 3, 5$, the finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ of maximal order are precisely the conjugates of $\mathrm{Aut}(B_n)$. For the remaining values of n, Feit also characterizes the largest finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ and shows that they are unique up to conjugacy. Feit's proof depends essentially on an unpublished manuscript of Weisfeiler [225] which establishes the best known upper bound for the Jordan number $j(n)$. Recall that a classical result of Jordan [101] asserts the existence of a number $j(n)$, depending only on n, such that every finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ contains an abelian normal subgroup of index at most $j(n)$. Since $\mathcal{S}_{n+1} \leq \mathrm{GL}_n(\mathbb{C})$ via the action on $A_n \otimes_{\mathbb{Z}} \mathbb{C}$, one certainly has $j(n) \geq (n+1)!$. It is commonly believed that equality holds for large enough n. Weisfeiler [225] proves the almost sharp bound $j(n) \leq (n+2)!$ for $n > 63$. An alternative proof of Feit's theorem for large values of n has been given by Friedland [68] who relies on Weisfeiler [226] instead. The latter article announces the weaker upper bound $j(n) \leq n^{a \log n + b} n!$. Weisfeiler's work in both [225] and [226] uses the classification of finite simple groups.

For further information on the subject of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ and of $\mathrm{GL}_n(\mathbb{Q})$, see, e.g., Nebe and Plesken [139] and Plesken [149].

2

Permutation Lattices and Flasque Equivalence

2.1 Introduction

The main purpose of this chapter is to furnish some lattice theoretic tools for the investigation of multiplicative field invariants in Chapter 9. This material will not be required elsewhere in this book. In particular, the rather technical sections 2.11 and 2.12 are only needed for the proof of Theorem 9.8.3. These sections draw on work of Beneish [8], Bessenrodt-Le Bruyn [17], and Formanek [64], [65].

Throughout, $\mathcal{G}$ denotes a finite group. We will discuss various types of $\mathcal{G}$-lattices, all closely related to permutation lattices, and an important equivalence relation between $\mathcal{G}$-lattices, called flasque equivalence, which goes back to Endo-Miyata [57], Voskresenskiĭ [219], and Colliot-Thélène and Sansuc [41], [42]. Our presentation with regard to flasque equivalence follows Colliot-Thélène and Sansuc.

2.2 Permutation Lattices

A $\mathcal{G}$-lattice L is called a *permutation lattice* if it has a $\mathbb{Z}$-basis, say X, that is permuted by the action of $\mathcal{G}$. We will write such a lattice as

$$L = \mathbb{Z}[X] \ .$$

If $\mathcal{G}\backslash X$ denotes a full representative set of the $\mathcal{G}$-orbits in X and $\mathcal{G}_x = \operatorname{stab}_{\mathcal{G}}(x)$ is the isotropy group of $x \in X$ then

$$L \cong \bigoplus_{x \in \mathcal{G}\backslash X} \mathbb{Z}{\uparrow}_{\mathcal{G}_x}^{\mathcal{G}} \ .$$

The summands $\mathbb{Z}{\uparrow}_{\mathcal{G}_x}^{\mathcal{G}} \cong \mathbb{Z}[\mathcal{G}/\mathcal{G}_x]$ are indecomposable $\mathcal{G}$-lattices; see Section 1.5. Permutation lattices of this form were considered earlier in Section 1.3, notably the standard permutation lattice $U_n \cong \mathbb{Z}{\uparrow}_{\mathcal{S}_{n-1}}^{\mathcal{S}_n}$ for the symmetric group $\mathcal{G} = \mathcal{S}_n$; see (1.7). As we have remarked in §1.4.3, all permutation lattices are self-dual.

Direct sums and tensor products of permutation lattices are permutation lattices: $\mathbb{Z}[X] \oplus \mathbb{Z}[X'] \cong \mathbb{Z}[X \coprod X']$ and $\mathbb{Z}[X] \otimes \mathbb{Z}[X'] \cong \mathbb{Z}[X \times X']$, where $X \coprod X'$ is the disjoint union of the $\mathcal{G}$-sets X and X' and $X \times X'$ their cartesian product. Moreover, for any subgroup $\mathcal{H} \leq \mathcal{G}$, restriction $.\downarrow^{\mathcal{G}}_{\mathcal{H}}$ and induction $.\uparrow^{\mathcal{G}}_{\mathcal{H}}$ both send permutation lattices to permutation lattices: for restriction this is obvious from the description $L = \mathbb{Z}[X]$, while the case of induction follows from the "transitivity" relation $.\uparrow^{\mathcal{H}}_{\mathcal{H}_x}\uparrow^{\mathcal{G}}_{\mathcal{H}} \cong \ .\uparrow^{\mathcal{G}}_{\mathcal{H}_x}$.

2.3 Stable Permutation Equivalence

Two $\mathcal{G}$-lattices L and L' are said to be *stably permutation equivalent* if $L \oplus P \cong L' \oplus P'$ holds for suitable permutation $\mathcal{G}$-lattices P and P'. Since direct sums of permutation lattices are permutation, this defines an equivalence relation on $\mathcal{G}$-lattices, coarser than isomorphism. Following Colliot-Thélène and Sansuc [41], we will denote the stable permutation class of the $\mathcal{G}$-lattice L by

$$[L] \ .$$

If $[L] = [0]$, that is, if $L \oplus P \cong P'$ holds for suitable permutation $\mathcal{G}$-lattices P and P', then the $\mathcal{G}$-lattice L is called *stably permutation*.

The stable permutation class $[L \oplus L']$, for any two $\mathcal{G}$-lattices L and L', depends only on $[L]$ and $[L']$. Thus we may define $[L] + [L'] = [L \oplus L']$, thereby turning the set of stable permutation classes of $\mathcal{G}$-lattices into a commutative monoid with identity element $[0]$. This monoid will be denoted by

$$\mathsf{SP}_{\mathcal{G}} \ .$$

Duality of $\mathcal{G}$-lattices passes down to $\mathsf{SP}_{\mathcal{G}}$ and, for any subgroup $\mathcal{H} \leq \mathcal{G}$, induction and restriction yield well-defined monoid homomorphisms $.\uparrow^{\mathcal{G}}_{\mathcal{H}} \colon \mathsf{SP}_{\mathcal{H}} \to \mathsf{SP}_{\mathcal{G}}$ and $.\downarrow^{\mathcal{G}}_{\mathcal{H}} \colon \mathsf{SP}_{\mathcal{G}} \to \mathsf{SP}_{\mathcal{H}}$.

The following lemma will be needed later for the the symmetric group $\mathcal{G} = \mathcal{S}_n$. In this case, the lemma is due to Endo and Miyata [58, Theorem 3.3]. Recall that all irreducible $\mathbb{Q}[\mathcal{S}_n]$-modules are in fact absolutely irreducible or, in other words, $\mathbb{Q}$ is a splitting field for $\mathcal{S}_n$; see [45, 75.1]. For more general results on recognizing stable permutation equivalence, see Bessenrodt and Le Bruyn [17, §2].

Lemma 2.3.1. *Assume that $\mathbb{Q}$ is a splitting field for $\mathcal{G}$. Then any two $\mathcal{G}$-lattices in the same genus (see §1.2.2) are stably permutation equivalent. In particular, all projective $\mathcal{G}$-lattices are stably permutation.*

Proof. We first show that the two assertions of the lemma are in fact equivalent. Indeed, by Swan's Theorem (1.6), any projective $\mathcal{G}$-lattice L satisfies $L \vee \mathbb{Z}[\mathcal{G}]^r$ for some r. Therefore, the second assertion follows from the first. Conversely, assume that projective $\mathcal{G}$-lattices are stably permutation. If L and L' are $\mathcal{G}$-lattices in the same genus then, by a theorem of Roiter [169] (see also [44, 31.28]), we have

$$L \oplus \mathbb{Z}[\mathcal{G}] \cong L' \oplus I \tag{2.1}$$

for some $\mathcal{G}$-lattice I with $I \vee \mathbb{Z}[\mathcal{G}]$. By (1.2), I is projective and hence stably permutation. Therefore, (2.1) implies that L and L' are stably permutation equivalent.

The proof of the second assertion uses the projective class group $\mathrm{Cl}(\mathbb{Z}[\mathcal{G}])$ of the group ring $\mathbb{Z}[\mathcal{G}]$. Curtis-Reiner [45, Chapter 6] and Reiner [161] are good references on this topic.

By definition, $\mathrm{Cl}(\mathbb{Z}[\mathcal{G}])$ is the kernel of the canonical map

$$K_0(\mathbb{Z}[\mathcal{G}]) \to \prod_p K_0(\mathbb{Z}_{(p)}[\mathcal{G}]) ,$$

where p runs over the primes in $\mathbb{Z}$ and $K_0(\,.\,)$ denotes the Grothendieck group of the category of all finitely generated projective modules over the ring in question. Writing $\langle L \rangle$ for the element of $K_0(\mathbb{Z}[\mathcal{G}])$ defined by the projective $\mathcal{G}$-lattice L, Swan's Theorem (1.6) implies that $\langle L \rangle - r\langle \mathbb{Z}[\mathcal{G}] \rangle \in \mathrm{Cl}(\mathbb{Z}[\mathcal{G}])$ for some r. Let Λ be a maximal $\mathbb{Z}$-order in $\mathbb{Q}[\mathcal{G}]$ containing $\mathbb{Z}[\mathcal{G}]$, and let $\mathrm{Cl}(\Lambda)$ denote the class group of Λ, defined exactly as for $\mathbb{Z}[\mathcal{G}]$; see [45, 39.12]. The canonical map $\Lambda \otimes_{\mathbb{Z}[\mathcal{G}]} .\, : K_0(\mathbb{Z}[\mathcal{G}]) \to K_0(\Lambda)$ induces a (surjective) map $\mathrm{Cl}(\mathbb{Z}[\mathcal{G}]) \to \mathrm{Cl}(\Lambda)$. By Oliver [143, Theorem 5], the kernel of this map is the subgroup

$$\widetilde{\mathrm{Cl}}^q(\mathbb{Z}[\mathcal{G}]) = \{\langle L_1 \rangle - \langle L_2 \rangle \mid L_1 \oplus P \cong L_2 \oplus P \text{ for some permutation lattice } P\} .$$

Moreover, our hypothesis that $\mathbb{Q}$ is a splitting field for $\mathcal{G}$ implies that the class group $\mathrm{Cl}(\Lambda)$ is trivial. (The maximal order Λ decomposes according to the Wedderburn decomposition of $\mathbb{Q}[\mathcal{G}]$, and a description of the class groups of maximal orders in central simple algebras is given in [45, 49.32] or [161, 35.14].) Therefore, any projective $\mathcal{G}$-lattice L satisfies $\langle L \rangle - r\langle \mathbb{Z}[\mathcal{G}] \rangle \in \widetilde{\mathrm{Cl}}^q(\mathbb{Z}[\mathcal{G}])$ for some r, and so $L \oplus P \cong \mathbb{Z}[\mathcal{G}]^r \oplus P$. This proves that L is stably permutation. □

2.4 Permutation Projective Lattices

A $\mathcal{G}$-lattice L is called *permutation projective* or *invertible* if $[L]$ is an invertible element of the monoid $\mathsf{SP}_{\mathcal{G}}$ of stable permutation classes of $\mathcal{G}$-lattices. (The group of invertible elements of $\mathsf{SP}_{\mathcal{G}}$ is called the *permutation class group* of $\mathcal{G}$ in Dress [53].) In other words, L is permutation projective if and only if L is a direct summand of some permutation $\mathcal{G}$-lattice. This is a local condition:

Lemma 2.4.1. *A $\mathcal{G}$-lattice L is permutation projective if and only if L is permutation projective as $\mathcal{G}_p$-lattice for all Sylow subgroups $\mathcal{G}_p$ of $\mathcal{G}$.*

One direction is obvious: if L is permutation projective then so are all restrictions $L{\downarrow}^{\mathcal{G}}_{\mathcal{H}}$, because restrictions of permutation lattices are permutation lattices. The converse will be proved in §2.6.

2.5 $\widehat{H}^i$-trivial, Flasque and Coflasque Lattices

We will use the notation $\widehat{H}^i(\mathcal{G}, \,.\,)$ $(i \in \mathbb{Z})$ for the Tate cohomology functors of the finite group $\mathcal{G}$. For $i \geq 1$, $\widehat{H}^i(\mathcal{G}, \,.\,)$ is identical with the ordinary cohomology functor $H^i(\mathcal{G}, \,.\,)$. We will be primarily concerned the groups $\widehat{H}^1(\mathcal{H}, L)$ and $\widehat{H}^{-1}(\mathcal{H}, L)$ for a $\mathcal{G}$-lattice L and subgroups $\mathcal{H}$ of $\mathcal{G}$. The group $\widehat{H}^{-1}(\mathcal{H}, L)$ has the form

$$\widehat{H}^{-1}(\mathcal{H}, L) = L(\mathcal{H})/[\mathcal{H}, L] \,, \tag{2.2}$$

where

$$[\mathcal{H}, L] = \sum_{g\in\mathcal{H}} [g, L] \quad \text{and} \quad L(\mathcal{H}) = \{m \in L \mid \sum_{h\in\mathcal{H}} h(m) = 0\} \,. \tag{2.3}$$

Here, $[g, L] = \{g(m) - m \mid m \in L\}$, as in (1.26); it suffices to let g run over a set of generators of the group $\mathcal{H}$ in the definition of $[\mathcal{H}, L]$; see (1.22) and (1.24). A good background reference for Tate cohomology in general is Brown [31, Chap. VI].

A $\mathcal{G}$-module M is called $\widehat{H}^i$-trivial if $\widehat{H}^i(\mathcal{H}, M) = 0$ holds for all subgroups $\mathcal{H} \leq \mathcal{G}$. By [31, III.9.5(ii) and VI.5.5], it is enough to check the condition $\widehat{H}^i(\mathcal{H}, M) = 0$ for all p-subgroups $\mathcal{H} \leq \mathcal{G}$, where p runs over the prime divisors of $|\mathcal{G}|$.

If L is a $\mathcal{G}$-lattice then we have a duality pairing $\widehat{H}^i(\mathcal{G}, L^*) \otimes_{\mathbb{Z}} \widehat{H}^{-i}(\mathcal{G}, L) \longrightarrow \mathbb{Z}/|\mathcal{G}|\mathbb{Z}$ given by the cup product; see [31, Exercise VI.7.3]. This gives rise to an isomorphism of finite abelian groups

$$\widehat{H}^i(\mathcal{G}, L^*) \cong \widehat{H}^{-i}(\mathcal{G}, L) \,. \tag{2.4}$$

Consequently, L is $\widehat{H}^i$-trivial if and only if L^* is $\widehat{H}^{-i}$-trivial.

Following Colliot-Thélène and Sansuc [41], $\widehat{H}^1$-trivial $\mathcal{G}$-lattices are also called *coflasque*. Equivalently, L is coflasque iff $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(P, L) = 0$ holds for all permutation projective $\mathcal{G}$-lattices P. This follows from the isomorphism

$$\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(\mathbb{Z}{\uparrow}_{\mathcal{H}}^{\mathcal{G}}, L) \cong \widehat{H}^1(\mathcal{H}, L) \,; \tag{2.5}$$

see, e.g., [35, p. 118].

Similarly, $\widehat{H}^{-1}$-trivial $\mathcal{G}$-lattices are called *flasque*; they can be characterized by the condition that $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, P) = 0$ holds for all permutation projective $\mathcal{G}$-lattices P.

For any subgroup $\mathcal{H} \leq \mathcal{G}$, restriction $\,.\,{\downarrow}_{\mathcal{H}}^{\mathcal{G}}$ clearly sends $\widehat{H}^i$-trivial $\mathcal{G}$-modules to $\widehat{H}^i$-trivial $\mathcal{H}$-modules. As for induction, the Eckmann-Shapiro Lemma gives an isomorphism of functors

$$\widehat{H}^i(\mathcal{G}, \,.{\uparrow}_{\mathcal{H}}^{\mathcal{G}}) \cong \widehat{H}^i(\mathcal{H}, \,.\,) \,; \tag{2.6}$$

see [31, VI.5.2]. In conjunction with (1.14), this implies that induction $\,.{\uparrow}_{\mathcal{H}}^{\mathcal{G}}$ sends $\widehat{H}^i$-trivial $\mathcal{H}$-modules to $\widehat{H}^i$-trivial $\mathcal{G}$-modules. In particular, since $\widehat{H}^{-1}(\mathcal{H}, \mathbb{Z}) = \widehat{H}^1(\mathcal{H}, \mathbb{Z}) = \{0\}$ holds for all finite groups $\mathcal{H}$, we conclude that the $\mathcal{G}$-lattice $\mathbb{Z}{\uparrow}_{\mathcal{H}}^{\mathcal{G}}$ is flasque and coflasque. Since finite direct sums of $\mathcal{G}$-modules are $\widehat{H}^i$-trivial if and only if all summands are, we obtain:

Lemma 2.5.1. *Permutation projective $\mathcal{G}$-lattices are both flasque and coflasque.*

2.6 Flasque and Coflasque Resolutions

An exact sequence of $\mathcal{G}$-lattices

$$0 \to L \longrightarrow P \longrightarrow F \to 0 \tag{2.7}$$

with P a permutation lattice and F flasque is called a *flasque resolution* of L. Similarly, an exact sequence of $\mathcal{G}$-lattices

$$0 \to C \longrightarrow P \longrightarrow L \to 0 \tag{2.8}$$

with P permutation and C coflasque is called a *coflasque resolution* of L. Dualizing a flasque resolution for L gives a coflasque resolution for L^*, and conversely.

Lemma 2.6.1. *Flasque and coflasque resolutions exist for every $\mathcal{G}$-lattice L. Moreover, the stable permutation classes $[F]$ and $[C]$ in* (2.7) *and* (2.8) *depend only on the class $[L]$ of L.*

Proof. By duality, it suffices to treat the case of coflasque resolutions.

Given L, define $P = \bigoplus_{\mathcal{H}} L^{\mathcal{H}}\uparrow_{\mathcal{H}}^{\mathcal{G}}$, where $L^{\mathcal{H}}$ is the sublattice of $\mathcal{H}$-fixed points in L and $\mathcal{H}$ ranges over all subgroup of $\mathcal{G}$. Note that P is a permutation $\mathcal{G}$-lattice. The inclusions $L^{\mathcal{H}} \hookrightarrow L$ can be assembled to yield a $\mathcal{G}$-epimorphism $f\colon P \twoheadrightarrow L$ with $f(P^{\mathcal{H}}) = L^{\mathcal{H}}$ for all $\mathcal{H} \leq \mathcal{G}$. Putting $C = \operatorname{Ker}(f)$ we obtain an exact sequence of the form (2.8). From the cohomology sequence

$$\cdots \to P^{\mathcal{H}} \xrightarrow{f} L^{\mathcal{H}} \longrightarrow H^1(\mathcal{H}, C) \longrightarrow H^1(\mathcal{H}, P) \to \ldots$$

that is associated with this sequence together with the fact that P is coflasque (Lemma 2.5.1) we infer that C is coflasque, thereby proving the desired coflasque resolution of L.

For uniqueness, let $0 \to C' \to P' \to L \to 0$ be another coflasque resolution of L. Consider the pullback diagram (see, e.g., Hilton and Stammbach [87, Sect. II.6])

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & C \arrow[r] & P \arrow[u] \arrow[r] & L \arrow[u] \arrow[r] & 0 \\
0 \arrow[r] & C \arrow[u, equal] \arrow[r] & X \arrow[u] \arrow[r] & P' \arrow[u] \arrow[r] & 0 \\
 & & C' \arrow[u] \arrow[r, equal] & C' \arrow[u] & \\
 & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd} \tag{2.9}$$

Since C and C' are coflasque, the middle row and column split giving an isomorphism $C \oplus P \cong C' \oplus P$; so $[C] = [C']$. Finally, given a coflasque resolution (2.8) for L and a permutation lattice Q, the sequence $0 \to C \to P \oplus Q \to L \oplus Q \to 0$ is a coflasque resolution of $L \oplus Q$. This shows that the class $[C]$ in (2.8) only depends on $[L]$. □

The foregoing can be used to complete the proof of Lemma 2.4.1.

Proof of Lemma 2.4.1. Let L be a $\mathcal{G}$-lattice. We first note that

> *L is permutation projective if and only if* $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, C) = 0$ *holds for all coflasque $\mathcal{G}$-lattices C.*

The implication $\Rightarrow$ has already been pointed out in §2.5. For $\Leftarrow$, choose a coflasque resolution $0 \to C \to P \to L \to 0$ of L. Since $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, C) = 0$, this sequence splits; so L is isomorphic to a direct summand of the permutation lattice P.

Now assume that the restrictions $L{\downarrow}^{\mathcal{G}}_{\mathcal{G}_p}$ to all Sylow subgroups $\mathcal{G}_p$ of $\mathcal{G}$ are permutation projective. Then $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}_p]}(L, C) = 0$ holds for all coflasque $\mathcal{G}$-lattices C. Since the restriction map $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, C) \to \prod_p \operatorname{Ext}_{\mathbb{Z}[\mathcal{G}_p]}(L, C)$ is injective (see, e.g., [31, III(2.2) and III(9.5)(ii)]), we conclude that $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, C) = 0$, as desired. □

2.7 Flasque Equivalence

We now discuss a notion of equivalence for $\mathcal{G}$-lattices, coarser than stable permutation equivalence (see §2.3), which will play an important role in the investigation of rationality problems for field extensions in Chapter 9.

We concentrate on flasque resolutions; this is no essential restriction, by duality. In view of Lemma 2.6.1, we may define, for any $\mathcal{G}$-lattice L,

$$[L]^{\mathrm{fl}} = [F] \in \mathsf{SP}_{\mathcal{G}} \ ,$$

where F is the cokernel in any flasque resolution (2.7) of L. Flasque equivalence of $\mathcal{G}$-lattices, written $\underset{\mathrm{fl}}{\sim}$, is defined by

$$L \underset{\mathrm{fl}}{\sim} L' \iff [L]^{\mathrm{fl}} = [L']^{\mathrm{fl}} \ .$$

Clearly, $[0]^{\mathrm{fl}} = [0]$ and $[L \oplus L']^{\mathrm{fl}} = [L]^{\mathrm{fl}} + [L']^{\mathrm{fl}}$, because the direct sum of flasque resolutions of L and L' is a flasque resolution of $L \oplus L'$. Moreover, $[\,.\,]^{\mathrm{fl}}$ commutes with restriction $\,.{\downarrow}^{\mathcal{G}}_{\mathcal{H}}$ and with induction $\,.{\uparrow}^{\mathcal{G}}_{\mathcal{H}}$, and hence both maps preserve flasque equivalence $\underset{\mathrm{fl}}{\sim}$.

Lemma 2.7.1. (a) *If Q is a permutation projective $\mathcal{G}$-lattice then $[Q]^{\mathrm{fl}} = -[Q]$.*

(b) *If $0 \to L \to M \to Q \to 0$ is an exact sequence of $\mathcal{G}$-lattices with Q permutation projective then $[L]^{\mathrm{fl}} + [Q]^{\mathrm{fl}} = [M]^{\mathrm{fl}}$.*

(c) *The following are equivalent for $\mathcal{G}$-lattices L and L' :*

(i) $L \underset{\mathrm{fl}}{\sim} L'$ *;*

(ii) *There exist exact sequences of $\mathcal{G}$-modules $0 \to L \to P \to M \to 0$ and $0 \to L' \to Q \to M \to 0$ with $\mathcal{G}$-lattices P and Q that are stably permutation.*

(iii) *There exist exact sequences of $\mathcal{G}$-lattices* $0 \to L \to E \to P \to 0$ *and* $0 \to L' \to E \to Q \to 0$, *where P and Q are permutation lattices.*

Proof. (a) If $Q \oplus Q' = R$ for some permutation lattice R then $0 \to Q \to R \to Q' \to 0$ is a flasque resolution of Q, by Lemma 2.5.1, and $[Q] + [Q'] = [R] = [0]$ holds in $\mathsf{SP}_{\mathcal{G}}$. Thus, $[Q]^{\mathrm{fl}} = [Q'] = -[Q]$.

(b) Choose a flasque resolution (2.7) of L and consider the pushout diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & P \arrow[r] \arrow[d] & X \arrow[r] \arrow[d] & Q \arrow[r] & 0 \\
 & F \arrow[r, equal] \arrow[d] & F \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Since Q is flasque, the middle row splits; so $X \cong P \oplus Q$. Writing $Q \oplus Q' = R$ as in the proof of (a), the middle column gives the flasque resolution $0 \to M \to P \oplus R \to F \oplus Q' \to 0$, whence $[M]^{\mathrm{fl}} = [F] + [Q'] = [L]^{\mathrm{fl}} + [Q]^{\mathrm{fl}}$.

(c) If $L \underset{\mathrm{fl}}{\sim} L'$ then we may choose flasque resolutions $0 \to L \to P \to F \to 0$ and $0 \to L' \to Q \to F' \to 0$ with $F = F'$. Thus, (i) implies (ii).

Now assume (ii). By adding a suitable permutation lattice to P, Q and M, we may assume that P and Q are in fact permutation lattices. The middle row and column of the pullback diagram

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & L \arrow[r] & P \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & L \arrow[r] \arrow[u, equal] & E \arrow[r] \arrow[u] & Q \arrow[r] \arrow[u] & 0 \\
 & & L' \arrow[r, equal] \arrow[u] & L' \arrow[u] & \\
 & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

yield exact sequences as required in (iii).

Finally, the implication (iii) ⇒ (i) is immediate from part (b). □

2.8 Quasi-permutation Lattices and Monomial Lattices

A $\mathcal{G}$-lattice L such that $L \underset{\mathrm{fl}}{\sim} 0$ is called a *quasi-permutation lattice*. By Lemma 2.7.1(c), L is quasi-permutation if and only if there is an exact sequence of $\mathcal{G}$-lattices

$$0 \to L \to P \to Q \to 0\,,$$

where P and Q are permutation lattices. For example, if L is stably permutation then L is certainly quasi-permutation.

Monomial lattices are further examples of quasi-permutation lattices. Specifically, a $\mathcal{G}$-lattice is called *monomial* if it has a $\mathbb{Z}$-basis that is permuted by $\mathcal{G}$ up to $\pm$-sign or, equivalently, if it is a direct sum of lattices that are induced from rank-1 lattices for suitable subgroups $\mathcal{H} \leq \mathcal{G}$. Any $\mathcal{H}$-lattice of rank 1 is quasi-permutation: it is either the trivial lattice $\mathbb{Z}$ or a lattice $\mathbb{Z}^-$ which fits into an exact sequence $0 \to \mathbb{Z}^- \to \mathbb{Z}\!\uparrow_{\mathcal{N}}^{\mathcal{H}} \to \mathbb{Z} \to 0$, where $\mathcal{N} = \mathrm{Ker}_{\mathcal{H}}(\mathbb{Z}^-)$ has index 2 in $\mathcal{H}$. Therefore, all monomial lattices are indeed quasi-permutation. Moreover, monomial lattices are self-dual, since this holds for $\mathbb{Z}$ and $\mathbb{Z}^-$. Finally, since $H^1(\mathcal{H}, \mathbb{Z}^-) = \mathbb{Z}/2\mathbb{Z}$, the Eckmann-Shapiro Lemma (2.6) implies that H^1 of any monomial lattice is an elementary abelian 2-group.

Example 2.8.1 (The $\mathcal{S}_n$-root lattice A_{n-1})**.** Sequence (1.10) shows that the $\mathcal{S}_n$-root lattice A_{n-1} is quasi-permutation. However, A_{n-1} is neither stably permutation nor monomial (for $n \geq 3$), since $H^1(\mathcal{S}_n, A_{n-1}) \cong \mathbb{Z}/n\mathbb{Z}$; see Lemma 2.8.2 (which we state slightly more generally for future use).

Lemma 2.8.2. *For any subgroup $\mathcal{H} \leq \mathcal{S}_n$, $H^1(\mathcal{H}, A_{n-1}) \cong \mathbb{Z}/h\mathbb{Z}$, where h is the* gcd *of the $\mathcal{H}$-orbit sizes in $\{1, \ldots, n\}$.*

Proof. Sequence (1.10) gives rise to the exact cohomology sequence

$$\cdots \to U_n^{\mathcal{H}} \xrightarrow{\varepsilon_n} \mathbb{Z} \longrightarrow H^1(\mathcal{H}, A_{n-1}) \longrightarrow H^1(\mathcal{H}, U_n) \to \ldots\,.$$

Here, $H^1(\mathcal{H}, U_n) = 0$, since U_n is a permutation lattice and hence coflasque; see Lemma 2.5.1. Using the notation of §1.3.3, the lattice of $\mathcal{H}$-invariants $U_n^{\mathcal{H}}$ has $\mathbb{Z}$-basis $\{\sum_{i \in \mathcal{O}} e_i \mid \mathcal{O}$ is an $\mathcal{H}$-orbit in $\{1, \ldots, n\}\}$. The asserted description of $H^1(\mathcal{H}, A_{n-1})$ follows from this. □

2.9 An Invariant for Flasque Equivalence

This section is based on Colliot-Thélène and Sansuc [42, pp. 199–202]. For any $\mathcal{G}$-module M, define

$$Ш^i(\mathcal{G}, M) = \bigcap_{g \in \mathcal{G}} \mathrm{Ker}\left(\mathrm{res}^{\mathcal{G}}_{\langle g \rangle} : \widehat{H}^i(\mathcal{G}, M) \longrightarrow \widehat{H}^i(\langle g \rangle, M)\right)\,. \tag{2.10}$$

Recall that $\widehat{H}^i(\mathcal{G}, \,.\,) = H^i(\mathcal{G}, \,.\,)$ for $i > 0$. In analogy with the terminology of §2.5, M will be called $Ш^i$-trivial if $Ш^i(\mathcal{H}, M) = 0$ holds for all subgroups $\mathcal{H} \leq \mathcal{G}$.

Of particular interest for us will be the case where M is a $\mathcal{G}$-lattice and $i = 1$ or 2. We will show in Proposition 2.9.2 below that $Ш^2(\mathcal{G}, \,.\,)$ is a $\underset{\text{fl}}{\sim}$-invariant on $\mathcal{G}$-lattices, and $Ш^1(\mathcal{G}, \,.\,)$ will play an important rôle in Chapter 5.

Lemma 2.9.1. *If* $0 \to M \to P \to N \to 0$ *be an exact sequence of* $\mathcal{G}$*-modules with* P *a permutation projective* $\mathcal{G}$*-lattice, then* $\text{Ш}^2(\mathcal{G}, M) \cong \text{Ш}^1(\mathcal{G}, N)$*.*

Proof. The cohomology sequences that are associated with the given exact sequence yield a commutative diagram with exact rows,

$$\begin{tikzcd}
0 = H^1(\mathcal{G}, P) \arrow[r] & H^1(\mathcal{G}, N) \arrow[r] \arrow[d, "\mathrm{res}"] & H^2(\mathcal{G}, M) \arrow[r] \arrow[d, "\mathrm{res}"] & H^2(\mathcal{G}, P) \arrow[d, "\mathrm{res}"] \\
0 = \prod_g H^1(\langle g \rangle, P) \arrow[r] & \prod_g H^1(\langle g \rangle, N) \arrow[r] & \prod_g H^2(\langle g \rangle, M) \arrow[r] & \prod_g H^2(\langle g \rangle, P)
\end{tikzcd}$$

Therefore, we obtain an exact sequence

$$0 \to \text{Ш}^1(\mathcal{G}, N) \longrightarrow \text{Ш}^2(\mathcal{G}, M) \longrightarrow \text{Ш}^2(\mathcal{G}, P) \,.$$

Here, $\text{Ш}^2(\mathcal{G}, P) = 0$, because $\text{Ш}^2(\mathcal{G}, \,.\,)$ is additive on direct sums and, for any subgroup $\mathcal{H} \leq \mathcal{G}$, the group $H^2(\mathcal{G}, \mathbb{Z}{\uparrow}_{\mathcal{H}}^{\mathcal{G}}) \cong \mathrm{Hom}(\mathcal{H}, \mathbb{Q}/\mathbb{Z})$ is detected by restrictions to cyclic subgroups. The asserted isomorphism $\text{Ш}^2(\mathcal{G}, M) \cong \text{Ш}^1(\mathcal{G}, N)$ follows. □

Note that, for any $\mathcal{G}$-lattice L, the groups $\widehat{H}^{\pm 1}(\mathcal{G}, L)$ depend only on the stable permutation class $[L] \in \mathsf{SP}_{\mathcal{G}}$, because $H^{\pm 1}(\mathcal{G}, \,.\,)$ is trivial on permutation $\mathcal{G}$-lattices. In particular, $\widehat{H}^{\pm 1}(\mathcal{G}, [L]^{\mathrm{fl}})$ are well-defined.

Proposition 2.9.2. (a) *For any* $\mathcal{G}$*-lattice* L*,*

$$\text{Ш}^2(\mathcal{G}, L) \cong H^1(\mathcal{G}, [L]^{\mathrm{fl}}) \,.$$

In particular, direct summands of quasi-permutation lattices are Ш^2*-trivial.*
(b) *Direct summands of monomial lattices are* Ш^1*-trivial.*

Proof. (a) Let $0 \to L \to P \to F \to 0$ be a flasque resolution of L; so $[L]^{\mathrm{fl}} = [F]$. By periodicity of cohomology for cyclic groups (see, e.g., [31, 9.2]), we have $H^1(\langle g \rangle, [L]^{\mathrm{fl}}) \cong \widehat{H}^{-1}(\langle g \rangle, F) = 0$ for all $g \in \mathcal{G}$, because F is flasque. Therefore, $\text{Ш}^1(\mathcal{G}, [L]^{\mathrm{fl}}) = H^1(\mathcal{G}, [L]^{\mathrm{fl}})$. Lemma 2.9.1 now yields $H^1(\mathcal{G}, [L]^{\mathrm{fl}}) \cong \text{Ш}^2(\mathcal{G}, L)$.

Any quasi-permutation lattice L satisfies $[L]^{\mathrm{fl}} = [0]$, and hence $\text{Ш}^2(\mathcal{G}, L) = 0$. The latter holds for direct summands of L as well, by additivity of $\text{Ш}^2(\mathcal{G}, \,.\,)$. Finally, the property of being a direct summand of a quasi-permutation lattice survives restrictions to subgroups. Therefore, direct summands of quasi-permutation lattices are Ш^2-trivial.

(b) Arguing as in the last paragraph of the proof of (a), it suffices to show that $\text{Ш}^1(\mathcal{G}, L) = \{0\}$ holds for $L = \mathbb{Z}_{\varphi}{\uparrow}_{\mathcal{H}}^{\mathcal{G}}$. Here, $\mathbb{Z}_{\varphi}$ denotes the $\mathcal{H}$-lattice $\mathbb{Z}$ with $\mathcal{H}$ acting via a homomorphism $\varphi \colon \mathcal{H} \to \{\pm 1\}$. We may assume that φ is nontrivial, because otherwise L is a permutation module and the assertion is clear. Thus,

$$H^1(\mathcal{G}, L) \cong H^1(\mathcal{H}, \mathbb{Z}_{\varphi}) = \mathbb{Z}/2\mathbb{Z} \,,$$

where the first isomorphism is the Eckmann-Shapiro isomorphism (2.6). This isomorphism is equal to the composite

$$\mathrm{proj}^* \circ \mathrm{res}^{\mathcal{G}}_{\mathcal{H}} \colon H^1(\mathcal{G}, L) \to H^1(\mathcal{H}, L) \to H^1(\mathcal{H}, \mathbb{Z}_\varphi)\ ,$$

where $\mathrm{proj}\colon L = \mathbb{Z}_\varphi {\uparrow}_{\mathcal{H}}^{\mathcal{G}} \twoheadrightarrow \mathbb{Z}_\varphi$ is the projection onto the $\mathcal{H}$-direct summand $1 \otimes \mathbb{Z}_\varphi \cong \mathbb{Z}_\varphi$ of L; see [31, Exercise III.8.2]. Fixing $g \in \mathcal{H}$ with $\varphi(g) = -1$, the restriction map $H^1(\mathcal{H}, \mathbb{Z}_\varphi) = \mathbb{Z}/2\mathbb{Z} \to H^1(\langle g \rangle, \mathbb{Z}_\varphi) = \mathbb{Z}/2\mathbb{Z}$ is an isomorphism, and hence so is the map $\mathrm{res}^{\mathcal{H}}_{\langle g \rangle} \circ \mathrm{proj}^* \circ \mathrm{res}^{\mathcal{G}}_{\mathcal{H}} = \mathrm{proj}^* \circ \mathrm{res}^{\mathcal{G}}_{\langle g \rangle}$. This proves that $\mathrm{res}^{\mathcal{G}}_{\langle g \rangle} \colon H^1(\mathcal{G}, L) \to H^1(\langle g \rangle, L)$ is injective, whence $Ш^1(\mathcal{G}, L) = \{0\}$. □

2.10 Overview of Lattice Types

Figure 2.10 depicts the various types of lattices discussed in this section and their relations to each other.

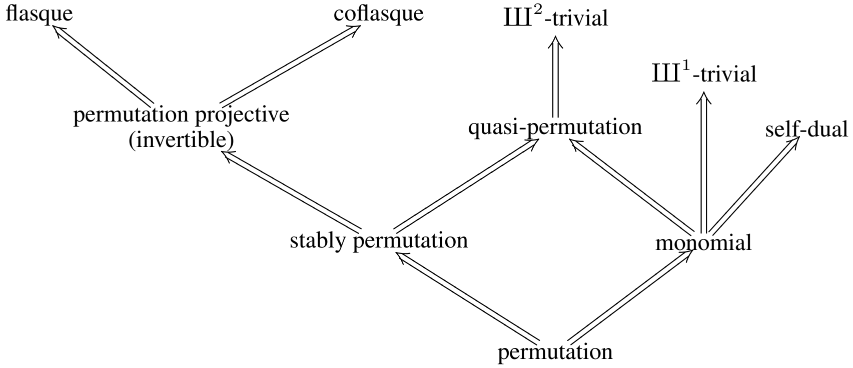

Fig. 2.1. $\mathcal{G}$-lattices related to permutation lattices

For certain special groups, more can be said:

2.10.1 Metacyclic Groups

By results of Endo-Miyata [57, Theorem 1.5] and Colliot-Thélène and Sansuc [41, Cor. 2 and Prop. 2], the following conditions are equivalent:

(i) All Sylow subgroups of $\mathcal{G}$ are cyclic;
(ii) flasque and coflasque $\mathcal{G}$-lattices are identical;
(iii) all flasque (coflasque) $\mathcal{G}$-lattices are permutation projective;
(iv) $[I^*_{\mathcal{G}}]^{\mathrm{fl}}$ is invertible in $\mathsf{SP}_{\mathcal{G}}$.

For a description of the groups $\mathcal{G}$ in (i), see [168, 10.1.10]: they are extensions of one cyclic group by another ("metacyclic"). In (iv), $I_{\mathcal{G}}$ denotes the augmentation kernel $I_{\mathcal{G}/\langle 1 \rangle}$; see (1.4). Thus, $I^*_{\mathcal{G}}$ is the cokernel of the norm map $N_{\mathcal{G}} \colon \mathbb{Z} \to \mathbb{Z}[\mathcal{G}]$ in (1.3).

2.10.2 $\mathcal{C}_2 \times \mathcal{C}_2$ and $\mathcal{Q}_8$

If $\mathcal{G} = \mathcal{C}_2 \times \mathcal{C}_2$ is the Klein 4-group then all $\mathcal{G}$-lattices that are both flasque and coflasque are actually stably permutation; see Colliot-Thélène and Sansuc [41, Prop. 4]. In particular, permutation projective and stably permutation $\mathcal{G}$-lattices coincide or, in other words, the unit group $\mathrm{U}(\mathsf{SP}_{\mathcal{G}})$ is trivial. The latter fact is also true for the quaternion group $\mathcal{Q}_8$ of order 8; see [41, Remarque R5].

2.11 Restriction to the Sylow Normalizer

The following technical lemma has been distilled from Beneish [8]; it will only be needed for the proof of Proposition 2.12.2(b), which in turn will only be used in the proof of Theorem 9.8.3.

Lemma 2.11.1. *Assume that, for some prime p, any two distinct Sylow p-subgroups of $\mathcal{G}$ have trivial intersection. Fix a Sylow p-subgroup, $\mathcal{G}_p$, and let $\mathcal{N} = N_{\mathcal{G}}(\mathcal{G}_p)$ denote its normalizer in $\mathcal{G}$. Let L be a $\mathcal{G}$-lattice such that $pQ \subseteq L \subseteq Q$ for some stably permutation $\mathcal{G}$-lattice Q. Then*

$$L{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \underset{\text{fl}}{\sim} L \oplus P$$

for some projective $\mathcal{G}$-lattice P.

Proof. By hypothesis, there is an exact sequence of $\mathcal{G}$-modules

$$0 \to L \to Q \to V \to 0 \tag{2.11}$$

with $pV = 0$. Thus, we obtain the exact sequence

$$0 \to L{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \longrightarrow Q{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \longrightarrow V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \to 0\,. \tag{2.12}$$

Note that the $\mathcal{G}$-lattice $Q{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}}$ is stably permutation, as Q is.

We will construct another short exact sequence of $\mathcal{G}$-modules terminating in $V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}}$ and with middle term a stably permutation $\mathcal{G}$-lattice, but originating in $L \oplus P$ for some projective $\mathcal{G}$-lattice P. By criterion (ii) in Lemma 2.7.1(c), this will prove the desired equivalence $L{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \underset{\text{fl}}{\sim} L \oplus P$.

Note that (1.12) yields isomorphisms

$$V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \cong \mathbb{Z}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \otimes_{\mathbb{Z}} V \cong \mathbb{F}_p{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \otimes_{\mathbb{F}_p} V\,. \tag{2.13}$$

Let $\varepsilon_{\mathcal{G}/\mathcal{N}} \colon \mathbb{Z}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} = \mathbb{Z}[\mathcal{G}/\mathcal{N}] \to \mathbb{Z}$ be the augmentation defined by $\varepsilon_{\mathcal{G}/\mathcal{N}}(g\mathcal{N}) = 1$ and let $I_{\mathcal{G}/\mathcal{N}}$ denote its kernel, as in (1.3), (1.4). Furthermore, let $\overline{} = (\,.\,) \otimes_{\mathbb{Z}} \mathbb{F}_p$ denote reduction mod p. Then $\overline{I_{\mathcal{G}/\mathcal{N}}}$ is the kernel of $\overline{\varepsilon_{\mathcal{G}/\mathcal{N}}} \colon \mathbb{F}_p{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \to \mathbb{F}_p$. Since p does not divide the index $[\mathcal{G} : \mathcal{N}]$, the map $\overline{\varepsilon_{\mathcal{G}/\mathcal{N}}}$ splits. Thus,

$$\mathbb{F}_p{\uparrow}_{\mathcal{N}}^{\mathcal{G}} = \mathbb{F}_p \oplus \overline{I_{\mathcal{G}/\mathcal{N}}}\,. \tag{2.14}$$

We claim that $\overline{I_{\mathcal{G}/\mathcal{N}}}$ is $\mathbb{F}_p[\mathcal{G}]$-projective. Indeed, by (1.14),

$$\mathbb{F}_p{\uparrow}_{\mathcal{N}}^{\mathcal{G}}{\downarrow}_{\mathcal{G}_p}^{\mathcal{G}} = \bigoplus_{x \in \mathcal{G}_p \backslash \mathcal{G}/\mathcal{N}} \mathbb{F}_p{\uparrow}_{\mathcal{G}_p \cap {}^x\mathcal{N}}^{\mathcal{G}_p}$$

Our hypothesis on $\mathcal{G}_p$ implies that $\mathcal{G}_p \cap {}^x\mathcal{N} = 1$ when $x \notin \mathcal{N}$, because $\mathcal{G}_p \cap {}^x\mathcal{N}$ is contained ${}^x\mathcal{G}_p$, the unique Sylow p-subgroup of ${}^x\mathcal{N}$. Therefore, the right hand side of the above equality has the form $\mathbb{F}_p \oplus \mathbb{F}_p[\mathcal{G}_p]^r$ for some r, and hence $\overline{I_{\mathcal{G}/\mathcal{N}}}{\downarrow}_{\mathcal{G}_p}^{\mathcal{G}} \cong \mathbb{F}_p[\mathcal{G}_p]^r$. This implies that $\overline{I_{\mathcal{G}/\mathcal{N}}}$ is a projective $\mathbb{F}_p[\mathcal{G}]$-module (see, e.g., [44, 19.5(ix)]), as we have claimed.

From (2.13) and (2.14) we obtain

$$V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \cong V \oplus \left(\overline{I_{\mathcal{G}/\mathcal{N}}} \otimes_{\mathbb{F}_p} V\right) . \tag{2.15}$$

Since $\overline{I_{\mathcal{G}/\mathcal{N}}}$ is $\mathbb{F}_p[\mathcal{G}]$-projective, $\overline{I_{\mathcal{G}/\mathcal{N}}} \otimes_{\mathbb{F}_p} V$ is a projective $\mathbb{F}_p[\mathcal{G}]$-module as well, by (1.12). Hence $\overline{I_{\mathcal{G}/\mathcal{N}}} \otimes_{\mathbb{F}_p} V$ has projective dimension 1 as $\mathbb{Z}[\mathcal{G}]$-module; see, e.g., [224, 4.3.1]. Choose a $\mathbb{Z}[\mathcal{G}]$-resolution $0 \to P \to F \to \overline{I_{\mathcal{G}/\mathcal{N}}} \otimes_{\mathbb{F}_p} V \to 0$ with F a free $\mathbb{Z}[\mathcal{G}]$-module and P projective. In view of (2.11) and (2.15), we obtain the desired second sequence for $V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}}$:

$$0 \to L \oplus P \longrightarrow Q \oplus F \longrightarrow V{\downarrow}_{\mathcal{N}}^{\mathcal{G}}{\uparrow}_{\mathcal{N}}^{\mathcal{G}} \to 0 \tag{2.16}$$

with $Q \oplus F$ clearly stably permutation. This proves the lemma. □

2.12 Some $\mathcal{S}_n$-Lattices

This section is devoted to a detailed analysis of the squares $A_{n-1}^{\otimes 2}$, $\mathsf{S}^2 A_{n-1}$ and $\bigwedge^2 A_{n-1}$ of the $\mathcal{S}_n$-lattice A_{n-1} introduced in §1.3.3. These results will only be needed in Section 9.8.

Part (b) of the following lemma is from Lemire-Lorenz [117] while (d) is due to Formanek [65].

Lemma 2.12.1. (a) *The $\mathcal{S}_n$-lattice $\mathsf{S}^2 A_{n-1}$ is coflasque for all n.*

(b) *If n is odd then $\mathsf{S}^2 A_{n-1}$ is stably permutation. In fact,*

$$\mathsf{S}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z} \cong \mathbb{Z}{\uparrow}_{\mathcal{S}_2 \times \mathcal{S}_{n-2}}^{\mathcal{S}_n} \oplus U_n \oplus \mathbb{Z} \ ,$$

where $\mathcal{S}_2 \times \mathcal{S}_{n-2}$ is the stabilizer in $\mathcal{S}_n$ of the subset $\{1, 2\}$ of $\{1, \ldots, n\}$. In particular, $A_{n-1}^{\otimes 2} \underset{\text{fl}}{\sim} \bigwedge^2 A_{n-1}$ holds for odd n.

(c) *For $n \geq 3$, there is an exact sequence of $\mathcal{S}_n$-lattices*

$$0 \to K_n \to \mathsf{S}^2 A_{n-1} \to U_n \to 0$$

with K_n rationally irreducible for $n \geq 4$ and $K_3 = 0$.

(d) *For $n = 4$, there is an isomorphism of $\mathcal{S}_4$-lattices*

$$\mathsf{S}^2 A_3 \oplus \mathbb{Z} \cong \mathbb{Z}{\uparrow}_{\mathcal{D}_8}^{\mathcal{S}_4} \oplus U_4 \ ,$$

where $\mathcal{D}_8$ is a Sylow 2-subgroup of $\mathcal{S}_4$.

Proof. (a) We first show that there is an exact sequence of $\mathcal{S}_n$-modules

$$0 \to \mathsf{S}^2 A_{n-1} \longrightarrow \mathbb{Z}{\uparrow}_{\mathcal{S}_2 \times \mathcal{S}_{n-2}}^{\mathcal{S}_n} \xrightarrow{\rho} A_{n-1} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to 0 \ . \tag{2.17}$$

Put $Q = \mathbb{Z}{\uparrow}_{\mathcal{S}_2 \times \mathcal{S}_{n-2}}^{\mathcal{S}_n} \cong \bigoplus_{1 \le i < j \le n} \mathbb{Z}\{i, j\}$. By Lemma 1.4.1(a), it suffices to show that $Q \cong (A_{n-1}^{\otimes 2})^{\tau}$, the sublattice of symmetric tensors in $A_{n-1}^{\otimes 2}$. Letting $\{e_i\}$ denote the canonical permutation basis of U_n as in §1.3.3, we have

$$(A_{n-1}^{\otimes 2})^{\tau} \subseteq (U_n^{\otimes 2})^{\tau} = \left(\bigoplus_{i=1}^{n} \mathbb{Z}(e_i \otimes e_i) \right) \oplus \left(\bigoplus_{1 \le i < j \le n} \mathbb{Z}(e_i \otimes e_j + e_j \otimes e_i) \right) \ .$$

The first summand on the right is isomorphic to U_n, while the second is isomorphic to Q via $e_i \otimes e_j + e_j \otimes e_i \mapsto \{i, j\}$. Using the $\mathbb{Z}$-basis $b_i = e_i - e_n$ $(i = 1, \dots, n-1)$ of A_{n-1}, we obtain an analogous decomposition for $(A_{n-1}^{\otimes 2})^{\tau}$. The projection of $(A_{n-1}^{\otimes 2})^{\tau}$ onto the summand $\bigoplus_{1 \le i < j \le n} \mathbb{Z}(e_i \otimes e_j + e_j \otimes e_i) \cong Q$ is easily seen to be an isomorphism, thereby establishing the sequence (2.17). Using $\overline{\ .\ } = (\,.\,) \otimes \mathbb{Z}/2\mathbb{Z}$ to denote reduction mod 2 and identifying the middle term in (2.17) with Q, the map ρ is explicitly given by $\rho(\{i, j\}) = \overline{e}_i + \overline{e}_j$.

We now show that $H^1(\mathcal{H}, \mathsf{S}^2 A_{n-1}) = 0$ holds for all subgroups $\mathcal{H} \le \mathcal{S}_n$. From (2.17), we obtain the exact sequence $Q^{\mathcal{H}} \xrightarrow{\rho} \overline{A}_{n-1}^{\mathcal{H}} \to H^1(\mathcal{H}, \mathsf{S}^2 A_{n-1}) \to H^1(\mathcal{H}, Q) = 0$. Thus, we need to show that

$$\rho(Q^{\mathcal{H}}) = \overline{A}_{n-1}^{\mathcal{H}} \ . \tag{2.18}$$

Now, $\overline{A}_{n-1}^{\mathcal{H}} \subseteq \overline{U}_n^{\mathcal{H}}$ and $\overline{U}_n^{\mathcal{H}}$ consists of all elements $\widehat{E} = \sum_{i \in E} \overline{e}_i$, where E is an $\mathcal{H}$-invariant subset of $\{1, \dots, n\}$. Furthermore, $\widehat{E}$ belongs to $\overline{A}_{n-1}^{\mathcal{H}}$ precisely if E has even size. Putting $\pi_E = \sum_{\substack{i,j \in E \\ i<j}} \{i, j\} \in Q^{\mathcal{H}}$, one calculates

$$\rho(\pi_E) = \sum_{\substack{i,j \in E \\ i<j}} \overline{e}_i + \overline{e}_j = (|E| - 1)\widehat{E} \ .$$

Thus, $\rho(\pi_E) = \widehat{E}$ for all E of even size, and so (2.18) is proved.

(b) We continue with the above notation. If n is odd then

$$\overline{U}_n = \overline{A}_{n-1} \oplus \overline{\mathbb{Z}} \cdot \sum_{i=1}^{n} \overline{e}_i \ .$$

By sending $1 \in \mathbb{Z}$ to $\sum_{i=1}^{n} \overline{e}_i$, we can enlarge sequence (2.17) to an exact sequence of $\mathcal{S}_n$-modules $0 \to \mathsf{S}^2 A_{n-1} \oplus \mathbb{Z} \longrightarrow Q \oplus \mathbb{Z} \longrightarrow \overline{U}_n \to 0$. Consider the pullback diagram

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & \mathsf{S}^2 A_{n-1} \oplus \mathbb{Z} \arrow[r] & Q \oplus \mathbb{Z} \arrow[r] \arrow[u] & \overline{U}_n \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \mathsf{S}^2 A_{n-1} \oplus \mathbb{Z} \arrow[r] \arrow[u, equal] & X \arrow[r] \arrow[u] & U_n \arrow[r] \arrow[u] & 0 \\
 & & U_n \arrow[r, equal] \arrow[u] & U_n \arrow[u, "\cdot 2"'] & \\
 & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

The middle column and middle row both split, the latter by (a). This yields the asserted isomorphism.

The fact that $A_{n-1}^{\otimes 2} \underset{\mathrm{fl}}{\sim} \bigwedge^2 A_{n-1}$ now follows from Lemmas 1.4.1(b) and 2.7.1(b).

(c) Define $\varphi\colon A_{n-1}^{\otimes 2} \to U_n$ by $\varphi(b_i \otimes b_j) = e_n + \delta_{i,j} e_i$, where $b_i = e_i - e_n$ $(i = 1, \ldots, n-1)$. This map is clearly surjective for $n \geq 3$ and it passes down to the symmetric square $\mathsf{S}^2 A_{n-1}$. Equivariance for $\mathcal{S}_n$ can be checked by direct calculation. Alternatively, use the $\mathcal{S}_n$-isomorphism

$$A_{n-1} \otimes_{\mathbb{Z}} U_n \xrightarrow{\sim} \bigoplus_{r \neq s} \mathbb{Z}(e_r \otimes e_s)\,, \quad (e_s - e_r) \otimes e_s \mapsto e_r \otimes e_s \tag{2.19}$$

and the $\mathcal{S}_n$-epimorphism

$$\bigoplus_{r \neq s} \mathbb{Z}(e_r \otimes e_s) \twoheadrightarrow U_n\,, \quad e_r \otimes e_s \mapsto e_s\,.$$

The map φ is the restriction of the composite of these maps to $A_{n-1}^{\otimes 2}$. The desired sequence now follows by letting K_n denote the kernel of the epimorphism $\mathsf{S}^2 A_{n-1} \twoheadrightarrow U_n$ afforded by φ. Counting ranks, we see that $K_3 = 0$. For $n \geq 4$, the $\mathbb{Q}[\mathcal{S}_n]$-module $\mathsf{S}^2 A_{n-1} \otimes_{\mathbb{Z}} \mathbb{Q}$ decomposes as the direct sum of the Specht modules $S^{(n)} = \mathbb{Q}$, $S^{(n-1,1)} = A_{n-1} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $S^{(n-2,2)}$; see, e.g., Fulton and Harris [70, Exercise 4.19]. Thus, we must have

$$K_n \otimes_{\mathbb{Z}} \mathbb{Q} \cong S^{(n-2,2)}\,,$$

which shows that K_n is rationally irreducible.

(d) The group $\mathcal{S}_4$ decomposes as the semidirect product $\mathcal{S}_4 = \mathcal{V}_4 \rtimes \mathcal{S}_3$, where $\mathcal{V}_4$ is the normal subgroup that is generated by the permutation $(1,2)(3,4)$. One checks that $\mathcal{V}_4$ acts trivially on K_4 and $K_4\big|_{\mathcal{S}_3} \cong A_2$. Thus, the augmentation sequence (1.10) for $\mathcal{S}_3$, $0 \to A_2 \to U_3 = \mathbb{Z}{\uparrow}_{\langle(1,2)\rangle}^{\mathcal{S}_3} \to \mathbb{Z} \to 0$, inflates to an exact sequence of $\mathcal{V}_4$-trivial $\mathcal{S}_4$-lattices $0 \to K_4 \to \mathbb{Z}{\uparrow}_{\mathcal{D}_8}^{\mathcal{S}_4} \to \mathbb{Z} \to 0$, where $\mathcal{D}_8 = \langle \mathcal{V}_4, (1,2) \rangle$ is a Sylow 2-subgroup of $\mathcal{S}_4$. Now consider the pushout diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & K_4 \arrow[r] \arrow[d] & \mathbb{Z}\uparrow^{\mathcal{S}_4}_{\mathcal{D}_8} \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathsf{S}^2 A_3 \arrow[r] \arrow[d] & X \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r] & 0 \\
 & U_4 \arrow[r, equal] \arrow[d] & U_4 \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

where the first row is the above exact sequence and the first column is the sequence of part (c). The middle row and column both split, because U_4 and $\mathbb{Z}$ are permutation lattices and $\mathbb{Z}\uparrow^{\mathcal{S}_4}_{\mathcal{D}_8}$ and $\mathsf{S}^2 A_3$ are coflasque, the latter by (a). Therefore, $X \cong \mathsf{S}^2 A_3 \oplus \mathbb{Z} \cong \mathbb{Z}\uparrow^{\mathcal{S}_4}_{\mathcal{D}_8} \oplus U_4$, proving (d). □

Using Proposition 2.9.2 one can show that, for even $n \geq 6$, $\mathsf{S}^2 A_{n-1}$ is not quasi-permutation; see Lemire-Lorenz [117, Lemma 4.5].

The next proposition is due to Bessenrodt and Le Bruyn [17]. Part (b) is a crucial ingredient in the proof of Bessenrodt and Le Bruyn's celebrated rationality result for the field of matrix invariants in degrees 5 and 7; see Theorem 9.8.3 below. The original proof of (b) given in [17] relied on massive amounts of computer calculation. A direct proof was subsequently found by Beneish [8]. Our presentation is based on Beneish's paper [8], with some simplifications.

Proposition 2.12.2. (a) *If p is prime then the $\mathcal{S}_p$-lattice $A^*_{p-1} \otimes_{\mathbb{Z}} A_{p-1}$ is stably permutation and $A^{\otimes 2}_{p-1}$ is permutation projective.*

(b) *For $p = 5$ and $p = 7$, the $\mathcal{S}_p$-lattice $A^{\otimes 2}_{p-1}$ is flasque equivalent to A^*_{p-1}.*

Proof. We let $\otimes = \otimes_{\mathbb{Z}}$.

(a) Put $P_p = A_{p-1} \otimes U_p$ and recall from (2.19) that P_p is a permutation lattice. Since permutation lattices are self-dual, it follows that $P_p \cong A^*_{p-1} \otimes U_p$. Thus, tensoring the augmentation sequence (1.10), $0 \to A_{p-1} \to U_p \to \mathbb{Z} \to 0$, with A^*_{p-1} we obtain an exact sequence $0 \to A^*_{p-1} \otimes A_{p-1} \to P_p \to A^*_{p-1} \to 0$, and dualizing (1.10) yields $0 \to \mathbb{Z} \to U_p \to A^*_{p-1} \to 0$. Consider the the pullback diagram

(2.20)

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & A^*_{p-1} \otimes A_{p-1} \arrow[r] & P_p \arrow[r] \arrow[u] & A^*_{p-1} \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & A^*_{p-1} \otimes A_{p-1} \arrow[r] \arrow[u, equal] & X \arrow[r] \arrow[u] & U_p \arrow[r] \arrow[u] & 0 \\
 & & \mathbb{Z} \arrow[r, equal] \arrow[u] & \mathbb{Z} \arrow[u] & \\
 & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

By Lemma 2.5.1, the middle column splits, because X is an extension of permutation lattices; so $X \cong P_p \oplus \mathbb{Z}$ is a permutation lattice. The middle row also splits: it represents an element in $\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_p]}(U_p, A_{p-1}^* \otimes A_{p-1}) \cong H^1(\mathcal{S}_{p-1}, A_{p-1}^* \otimes A_{p-1})$ (see (2.5)) and $\big(A_{p-1}^* \otimes A_{p-1}\big)\!\downarrow_{\mathcal{S}_{p-1}}$ is a permutation lattice, because $A_{p-1}\!\downarrow_{\mathcal{S}_{p-1}} \cong U_{p-1} \cong A_{p-1}^*\!\downarrow_{\mathcal{S}_{p-1}}$. Therefore, we obtain an isomorphism

$$(A_{p-1}^* \otimes A_{p-1}) \oplus U_p \cong P_p \oplus \mathbb{Z} \tag{2.21}$$

thereby proving that $A_{p-1}^* \otimes A_{p-1}$ is stably permutation.

We now turn to $A_{p-1}^{\otimes 2}$. In order to show that this lattice is permutation projective, it is enough to show that the restrictions to all Sylow q-subgroups $\mathcal{G}_q \leq \mathcal{S}_p$ are permutation projective; see Lemma 2.4.1. For primes $q \neq p$, we may assume that $\mathcal{G}_q \leq \mathcal{S}_{p-1} = \mathrm{stab}_{\mathcal{S}_p}(p)$. As we pointed out in the previous paragraph of the proof, $A_{p-1}^{\otimes 2}\!\downarrow_{\mathcal{G}_q} \cong \big(A_{p-1}^* \otimes A_{p-1}\big)\!\downarrow_{\mathcal{G}_q}$ is in fact a permutation $\mathcal{G}_q$-lattice in this case. Now consider $\mathcal{G}_p$; this is a cyclic of order p, say $\mathcal{G}_p = \langle x \rangle$. Then $A_{p-1}\!\downarrow_{\mathcal{G}_p} \cong (x-1)\mathbb{Z}[\mathcal{G}_p]$ and $A_{p-1}^*\!\downarrow_{\mathcal{G}_p} \cong \mathbb{Z}[\mathcal{G}_p]/\mathbb{Z}(\sum_{i=0}^{p-1} x^i)$. Multiplication with $x-1$ yields an isomorphism $\mathbb{Z}[\mathcal{G}_p]/\mathbb{Z}(\sum_{i=0}^{p-1} x^i) \xrightarrow{\sim} (x-1)\mathbb{Z}[\mathcal{G}_p]$. Therefore, we again conclude that $A_{p-1}^{\otimes 2} \cong A_{p-1}^* \otimes A_{p-1}$ as $\mathcal{G}_p$-lattices, and we know already that the latter lattice is stably permutation. This completes the proof of (a).

(b) Let p be any odd prime; we will specialize p towards the end of the proof. Tensoring the augmentation sequence (1.10) with A_{p-1} we obtain an exact sequence of $\mathcal{S}_p$-lattices $0 \to A_{p-1}^{\otimes 2} \to P_p \to A_{p-1} \to 0$, where $P_p = A_{p-1} \otimes U_p$ is the permutation lattice used in the proof of (a). Dualizing this sequence yields a flasque resolution of A_{p-1}^*, because $A_{p-1}^{\otimes 2}$ is permutation projective by (a). Thus,

$$[A_{p-1}^*]^{\mathrm{fl}} = [A_{p-1}^{\otimes 2}]^* \,. \tag{2.22}$$

Since $[A_{p-1}^{\otimes 2}]^{\mathrm{fl}} = -[A_{p-1}^{\otimes 2}]$, by Lemma 2.7.1(a), the assertion $[A_{p-1}^*]^{\mathrm{fl}} = [A_{p-1}^{\otimes 2}]^{\mathrm{fl}}$ of (b) becomes $[A_{p-1}^{\otimes 2}]^* = -[A_{p-1}^{\otimes 2}]$. This is equivalent to $[A_{p-1}^{\otimes 2} \oplus \big(A_{p-1}^{\otimes 2}\big)^*] = 0$ and in view of Lemma 2.7.1(a), the latter condition can be restated as

$$A_{p-1}^{\otimes 2} \oplus \big(A_{p-1}^{\otimes 2}\big)^* \underset{\mathrm{fl}}{\sim} 0 \,. \tag{2.23}$$

Our goal is to verify (2.23) for $p = 5$ and $p = 7$.

For simplicity, put $L = A_{p-1}^{\otimes 2} \oplus \big(A_{p-1}^{\otimes 2}\big)^*$, a permutation projective $\mathcal{S}_p$-lattice. Furthermore, let $\mathcal{G}_p$ denote a Sylow p-subgroup of $\mathcal{S}_p$ and let $\mathcal{N}$ be its normalizer in $\mathcal{S}_p$. Since $\mathcal{G}_p$ has order p, we may apply Lemma 2.11.1. Recall from (1.31) that there is an exact sequence of $\mathcal{S}_p$-modules $0 \to A_{p-1} \to A_{p-1}^* \to \mathbb{F}_p \to 0$. Hence we also have an exact sequence $0 \to pA_{p-1}^* \cong A_{p-1}^* \to A_{p-1} \to W \to 0$ with $pW = 0$. Tensoring the first of these sequences with A_{p-1} and the second with A_{p-1}^*, we obtain exact sequences $0 \to A_{p-1}^{\otimes 2} \to Q \to V_1 \to 0$ and $0 \to \big(A_{p-1}^{\otimes 2}\big)^* \to Q \to V_2 \to 0$, where $Q = A_{p-1}^* \otimes A_{p-1}$ and $pV_i = 0$. Lemma 2.11.1 in conjunction with Lemma 2.3.1 now yields:

$$A_{p-1}^{\otimes 2} \underset{\mathrm{fl}}{\sim} A_{p-1}^{\otimes 2}\!\downarrow_{\mathcal{N}}^{\mathcal{S}_p}\uparrow_{\mathcal{N}}^{\mathcal{S}_p} \quad \text{and} \quad \big(A_{p-1}^{\otimes 2}\big)^* \underset{\mathrm{fl}}{\sim} \big(A_{p-1}^{\otimes 2}\big)^*\!\downarrow_{\mathcal{N}}^{\mathcal{S}_p}\uparrow_{\mathcal{N}}^{\mathcal{S}_p} \,. \tag{2.24}$$

Therefore, $L{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p}{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \underset{\text{fl}}{\sim} L$, and so (2.23) becomes

$$L{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p}{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \underset{\text{fl}}{\sim} 0\,. \tag{2.25}$$

In order to prove (2.25), note that $\mathcal{N}$ is a semidirect product, $\mathcal{N} = \mathcal{G}_p \rtimes \mathcal{C}$, with $\mathcal{C}$ cyclic of order $p-1$. We may choose $\mathcal{C}$ so that $\mathcal{C}$ fixes p and is transitive on $\{1,\dots,p-1\}$. Therefore, $A_{p-1}{\downarrow}_{\mathcal{C}}^{\mathcal{S}_p} \cong \mathbb{Z}[\mathcal{C}]$ is $\mathcal{C}$-free, and so is the tensor product of A_{p-1} with any other $\mathcal{C}$-lattice, by (1.12). Let $\overline{} = (\,.\,) \otimes_{\mathbb{Z}} \mathbb{F}_p$ denote reduction mod p. We will show that, for suitable $\mathcal{N}$-lattices X and Y which are stably permutation and $\mathcal{C}$-free, there is an $\mathbb{F}_p[\mathcal{N}]$-isomorphism

$$\overline{L}{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p} \oplus \overline{X} \;\cong\; \overline{Y}\,. \tag{2.26}$$

This will imply (2.25). For, by Curtis-Reiner [44, 30.17] and [45, 81.17], the isomorphism (2.26) is equivalent to $L_{(p)}{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p} \oplus X_{(p)} \;\cong\; Y_{(p)}$, where $(\,.\,)_{(p)}$ denotes localization at p, as in §1.2.2. The latter isomorphism implies the existence of a short exact sequence of $\mathcal{N}$-modules $0 \to L{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p} \oplus X \to Y \to T \to 0$ with T finite and $T_{(p)} = 0$. Since X, Y and L are $\mathcal{C}$-free, their localizations at all primes $q \neq p$ are projective $\mathbb{Z}_{(q)}[\mathcal{N}]$-modules ([44, 19.5(ix)]). Therefore, $T_{(q)}$ has projective dimension at most 1 over $\mathbb{Z}_{(q)}[\mathcal{N}]$, and since $T_{(p)} = 0$, it follows that T has projective dimension at most 1 over $\mathbb{Z}[\mathcal{N}]$; see [44, proof of 8.19]. Fix a projective resolution $0 \to P_1 \to P_0 \to T \to 0$ and consider the induced exact sequences $0 \to L{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p}{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \oplus X{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to Y{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to T{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to 0$ and $0 \to P_1{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to P_0{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to T{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \to 0$. Since $X{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p}$, $Y{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p}$ and both $P_i{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p}$ are stably permutation, the latter two by Lemma 2.3.1, criterion (ii) in Lemma 2.7.1(c) tells us that $L{\downarrow}_{\mathcal{N}}^{\mathcal{S}_p}{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \underset{\text{fl}}{\sim} P_1{\uparrow}_{\mathcal{N}}^{\mathcal{S}_p} \underset{\text{fl}}{\sim} 0$, thereby proving (2.25).

It remains to establish (2.26). To construct Y, let $\mathcal{D}$ denote the unique subgroup of $\mathcal{N}$ containing $\mathcal{G}_p$ and satisfying $[\mathcal{D} : \mathcal{G}_p] = 2$; this is a dihedral group of order $2p$. Put

$$Y = \mathbb{Z}[\mathcal{N}/\mathcal{D}] \otimes_{\mathbb{Z}} A_{p-1}^{\otimes 2} \cong A_{p-1}^{\otimes 2}{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p}{\uparrow}_{\mathcal{D}}^{\mathcal{N}}\ .$$

Note that Y is $\mathcal{C}$-free, because A_{p-1} is a tensor factor. We claim that Y is stably permutation. Indeed, as $\mathcal{D}$-lattices, we have $U_p{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p} \cong \mathbb{Z}[\mathcal{D}/\mathcal{D}\cap\mathcal{C}]$ and so $A_{p-1}{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p} \cong I_{\mathcal{D}/\mathcal{D}\cap\mathcal{C}}$, using the notation of (1.4). Thus we know from Colliot-Thélène and Sansuc [41, Prop. 3 and Remarque R4] that $A_{p-1}^{*}{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p}$ is quasi-permutation. In view of (2.22) (which remains valid under restriction to $\mathcal{D}$; see Section 2.7), this says that $\left(A_{p-1}^{\otimes 2}\right)^{*}{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p}$ is stably permutation. Therefore, $A_{p-1}^{\otimes 2}{\downarrow}_{\mathcal{D}}^{\mathcal{S}_p}$ is stably permutation as well, and hence so is Y.

Fix generators x for $\mathcal{G}_p$ and y for $\mathcal{C}$; so x has order p, y has order $p-1$, and $yx = x^{\theta}y$, where $\theta \in \mathbb{F}_p^{*}$ is a primitive $(p-1)^{\text{st}}$ root of unity. Moreover, $\mathcal{N} = \langle x, y\rangle$ and $\mathcal{D} = \langle x, y^{p-1/2}\rangle$. For each $i \in \mathbb{Z}/(p-1)\mathbb{Z}$, let $\mathbb{F}_p^{(i)}$ denote the 1-dimensional $\mathbb{F}_p[\mathcal{N}]$-module with trivial $\mathcal{G}_p$-action and with y acting by multiplication with θ^{i}. Then $\mathbb{F}_p^{(i)} \otimes_{\mathbb{F}_p} \mathbb{F}_p^{(j)} \cong \mathbb{F}_p^{(i+j)}$, $\left(\mathbb{F}_p^{(i)}\right)^{*} \cong \mathbb{F}_p^{(-i)}$, and $\mathbb{F}_p[\mathcal{N}/\mathcal{G}_p] \cong \bigoplus_{i\in\mathbb{Z}/(p-1)\mathbb{Z}} \mathbb{F}_p^{(i)}$. We have

$$U_p{\downarrow_{\mathcal{N}}} \cong \mathbb{F}_p{\uparrow_{\mathcal{C}}^{\mathcal{N}}} \cong \mathbb{F}_p[\mathcal{G}_p]\ ,$$

with x acting on $\mathbb{F}_p[\mathcal{G}_p]$ by multiplication and y by conjugation. This module is uniserial with composition factors $(x-1)^i\mathbb{F}_p[\mathcal{G}_p]/(x-1)^{i+1}\mathbb{F}_p[\mathcal{G}_p] \cong \mathbb{F}_p^{(i)}$, via $(x-1)^i \mapsto 1$. In particular, $\overline{A_{p-1}} \cong (x-1)\mathbb{F}_p[\mathcal{G}_p]$ has head $\overline{A_{p-1}}/(x-1)\overline{A_{p-1}} \cong \mathbb{F}_p^{(1)}$, while $\overline{A_{p-1}^*}$ has head $\mathbb{F}_p^{(0)}$. Therefore, as $\mathbb{F}_p[\mathcal{N}]$-modules,

$$\mathbb{F}_p^{(1)} \otimes_{\mathbb{F}_p} \overline{A_{p-1}^*} \cong \overline{A_{p-1}}\ . \tag{2.27}$$

The isomorphism (2.27) gives:

$$\mathbb{F}_p^{(p-3)} \otimes_{\mathbb{F}_p} \overline{A_{p-1}^{\otimes 2}} \cong \left(\mathbb{F}_p^{(-1)} \otimes_{\mathbb{F}_p} \overline{A_{p-1}}\right)^{\otimes 2} \cong \overline{(A_{p-1}^{\otimes 2})^*}\ . \tag{2.28}$$

Now we finally specialize p. First, let $p = 5$. Then $\mathbb{F}_5[\mathcal{N}/\mathcal{D}] \cong \mathbb{F}_5^{(0)} \oplus \mathbb{F}_5^{(2)}$ and (2.28) yields

$$\overline{Y} \cong \mathbb{F}_5[\mathcal{N}/\mathcal{D}] \otimes_{\mathbb{F}_5} \overline{A_4^{\otimes 2}} \cong \overline{A_4^{\otimes 2}} \oplus \left(\mathbb{F}_5^{(2)} \otimes_{\mathbb{F}_5} \overline{A_4^{\otimes 2}}\right) \cong \overline{A_4^{\otimes 2}} \oplus \overline{(A_4^{\otimes 2})^*} = \overline{L}{\downarrow_{\mathcal{N}}^{\mathcal{S}_5}}\ .$$

This proves (2.26) (with $X = 0$) for $p = 5$.

For $p = 7$, we have $\mathbb{F}_7[\mathcal{N}/\mathcal{D}] \cong \mathbb{F}_7^{(0)} \oplus \mathbb{F}_7^{(2)} \oplus \mathbb{F}_7^{(4)}$ and, as in the calculation for $p = 5$, we obtain

$$\overline{Y} \cong \overline{L}{\downarrow_{\mathcal{N}}^{\mathcal{S}_7}} \oplus \left(\mathbb{F}_7^{(2)} \otimes_{\mathbb{F}_7} \overline{A_6^{\otimes 2}}\right)$$

By (2.27), $\mathbb{F}_7^{(2)} \otimes_{\mathbb{F}_7} \overline{A_6^{\otimes 2}} \cong \mathbb{F}_7^{(3)} \otimes_{\mathbb{F}_7} \overline{A_6^*} \otimes_{\mathbb{F}_7} \overline{A_6} \cong \overline{X}$, where we have put $X = (\mathbb{Z}^- \otimes_{\mathbb{Z}} A_6^* \otimes_{\mathbb{Z}} A_6){\downarrow_{\mathcal{N}}^{\mathcal{S}_7}}$. The lattice X is certainly $\mathcal{C}$-free, having a tensor factor A_6. In order to show that X is stably permutation, let $\alpha \in H^1(\mathcal{N}, \mathbb{Z}^-)$ denote the class of the extension $0 \to \mathbb{Z}^- \to \mathbb{Z}[\mathcal{N}/\mathcal{N} \cap \mathcal{A}_7] \to \mathbb{Z} \to 0$. Tensoring this extension with $B = A_6^* \otimes_{\mathbb{Z}} A_6$ we obtain an extension $0 \to X \to B{\downarrow_{\mathcal{N}\cap\mathcal{A}_7}^{\mathcal{N}}}{\uparrow_{\mathcal{N}\cap\mathcal{A}_7}^{\mathcal{N}}} \to B \to 0$ representing the element $\beta = \mathrm{Id}_B \vee \alpha \in \mathrm{Ext}_{\mathbb{Z}[\mathcal{N}]}(B, X)$; see [129, VIII.4]. It suffices to show that $\beta = 0$, because B is stably permutation by part (a). But $2\beta = 0$, because α has order 2, and $7\beta = 0$, because B is $\mathcal{C}$-free and so $\mathrm{res}_{\mathcal{C}}^{\mathcal{N}}\, \beta = 0$. This establishes (2.26) for $p = 7$, and hence the proposition is proved. □

The assertion that $A_{p-1}^{\otimes 2}$ is permutation projective in part (a) above can be made more precise. In fact, using assertion (a), Beneish proves in [8, Lemma 2.8] that $A_{p-1}^{\otimes 2}$ is isomorphic to a direct summand of the permutation lattice $\mathbb{Z}{\uparrow_{\mathcal{S}_{p-2}}^{\mathcal{S}_p}} \oplus \mathbb{Z}{\uparrow_{\mathcal{G}_p}^{\mathcal{S}_p}}$, where $\mathcal{G}_p$ is a Sylow p-subgroup of $\mathcal{S}_p$. Part (b) of the Proposition is no longer true for primes $p > 7$; see [17, Corollary 1]. Finally, it is known that $A_{n-1}^{\otimes 2}$ is quasi-permutation precisely for $n = 2$ and $n = 3$; see Cortella-Kunyavskiĭ [43] and Lemire-Lorenz [117, §4.1].

3

Multiplicative Actions

3.1 Introduction

In this chapter, we take up the subject of multiplicative actions and their invariants proper along with some of its ramifications. In Section 3.3 we show that, in investigating multiplicative invariant algebras, one can always reduce to the case where the acting group is finite and we may always work over $\mathbb{Z}$. A number of explicit calculations of multiplicative invariant algebras over $\mathbb{Z}$ for various finite groups, including all finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$, are carried out in Section 3.5. Section 3.6 features a theorem of Bourbaki [24] which states that multiplicative invariant algebras of weight lattices under the action of the Weyl group are polynomial algebras. Finally, we discuss twisted multiplicative actions and their connections with algebraic tori.

3.2 The Group Algebra of a G-Lattice

3.2.1 Group Algebras

Let L be a lattice. The group algebra of L over the commutative base ring $\Bbbk$ will be written as $\Bbbk[L]$; it contains a copy of L as a subgroup of the group of multiplicative units $\mathrm{U}(\Bbbk[L])$ and this copy of L forms a $\Bbbk$-basis of $\Bbbk[L]$. Working inside $\Bbbk[L]$, we must pass from the additive notation of L to a multiplicative notation. In order to make this passage explicit, we will write the basis element of $\Bbbk[L]$ corresponding to the lattice element $m \in L$ as

$$\mathbf{x}^m \ ;$$

so $\mathbf{x}^0 = 1$, $\mathbf{x}^{m+m'} = \mathbf{x}^m\mathbf{x}^{m'}$, and $\mathbf{x}^{-m} = (\mathbf{x}^m)^{-1}$. When a subset $M \subseteq L$ is to be explicitly viewed inside the group algebra $\Bbbk[L]$, it will be denoted by $\underline{M}$; so $\underline{M} = \{\mathbf{x}^m \mid m \in M\}$.

Every $f \in \Bbbk[L]$ has a unique expression as

$$f = \sum_{m \in L} k_m \mathbf{x}^m \tag{3.1}$$

with $k_m \in \Bbbk$ and $\{m \in L \mid k_m \neq 0\}$ a finite subset of L, called the *support* of f and denoted by $\operatorname{Supp} f$. A fixed choice of $\mathbb{Z}$-basis $\{e_i \mid i = 1, \ldots, n\}$ of L, or a fixed isomorphism $L \cong \mathbb{Z}^n$, gives rise to a $\Bbbk$-algebra isomorphism of $\Bbbk[L]$ with the Laurent polynomial algebra $\Bbbk[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ via $\mathbf{x}^{e_i} \mapsto x_i$. Therefore, we may think of the representatives $\mathbf{x}^m \in \Bbbk[L]$ of lattice elements $m \in L$ as monomials in $x_1^{\pm 1}, \ldots, x_n^{\pm 1}$.

3.2.2 Multiplicative Actions

If L is a G-lattice for some group G then the action of G on L extends uniquely to an action by $\Bbbk$-algebra automorphisms on $\Bbbk[L]$ via

$$g\Big(\sum_{m \in L} k_m \mathbf{x}^m\Big) = \sum_{m \in L} k_m \mathbf{x}^{g(m)} \ . \tag{3.2}$$

This type of action is called a *multiplicative action*. More general G-actions, called *twisted multiplicative*, will be considered in Section 3.8.

3.3 Reduction to Finite Groups, $\mathbb{Z}$-structure, and Finite Generation

Let L be a G-lattice, where G is an arbitrary group. The multiplicative action (3.2) of G on $\Bbbk[L]$ is a permutation action: $\{\mathbf{x}^m \mid m \in L\}$ is a G-stable $\Bbbk$-basis of $\Bbbk[L]$. Therefore, the $\Bbbk$-linear structure of $\Bbbk[L]^G$ is easily described: The support $\operatorname{Supp} f$ of any invariant $f \in \Bbbk[L]^G$ is a finite G-stable subset of L, and hence $\operatorname{Supp} f$ is contained in the G-sublattice

$$L_{\text{fin}} = \{m \in L \mid \text{the } G\text{-orbit } G(m) \text{ is finite}\} \ . \tag{3.3}$$

More precisely, f is a $\Bbbk$-linear combination of *G-orbit sums*

$$\mathsf{orb}(m) = \mathsf{orb}_{G,\Bbbk}(m) := \sum_{m' \in G(m)} \mathbf{x}^{m'} \ \in \Bbbk[L]^G$$

with $m \in L_{\text{fin}}$. Different orbit sums have disjoint supports, and hence they are $\Bbbk$-independent. Thus:

$$\Bbbk[L]^G = \bigoplus_{m \in G \backslash L_{\text{fin}}} \Bbbk \, \mathsf{orb}(m) \ , \tag{3.4}$$

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

Note that, since L_{fin} is finitely generated, the subgroup $\operatorname{Ker}_G(L_{\text{fin}})$ has finite index in G; so G acts on L_{fin} through the finite quotient $\mathcal{G} = G / \operatorname{Ker}_G(L_{\text{fin}})$.

Further, the group ring $\Bbbk[L]$ is defined over $\mathbb{Z}$, $\Bbbk[L] = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]$, and each orbit sum has the form $\mathsf{orb}_{G,\Bbbk}(m) = 1_{\Bbbk} \otimes_{\mathbb{Z}} \mathsf{orb}_{G,\mathbb{Z}}(m)$. Hence, by (3.4), $\mathbb{Z}[L]^G$ is a *$\mathbb{Z}$-structure* for the multiplicative invariant algebra $\Bbbk[L]^G$. To summarize:

Proposition 3.3.1. *Let L be a G-lattice for an arbitrary group G and let $\Bbbk$ be a commutative base ring. Then $L_{\text{fin}} = \{m \in L \mid G(m) \text{ is finite}\}$ is a faithful $\mathcal{G}$-lattice, where $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$ is a finite group . Furthermore:*

(a) $\Bbbk[L]^G = \Bbbk[L_{\text{fin}}]^{\mathcal{G}}$, *and*
(b) $\Bbbk[L]^G = \Bbbk \otimes_{\mathbb{Z}} \mathbb{Z}[L]^G$.

These observations have the following consequences.

Corollary 3.3.2. *Each multiplicative invariant algebra $\Bbbk[L]^G$ is an affine $\Bbbk$-algebra. Moreover, given a base ring $\Bbbk$ and a bound N, there is only a finite supply of multiplicative invariant algebras $\Bbbk[L]^G$ (up to isomorphism) with* $\operatorname{rank} L \leq N$.

Proof. Since $\mathbb{Z}[L_{\text{fin}}]$ is affine over the noetherian ring $\mathbb{Z}$ and $\mathcal{G} = G/\operatorname{Ker}_G(L_{\text{fin}})$ is finite, Noether's finiteness theorem (e.g., [22, Théorème V.1.2]) implies that $\mathbb{Z}[L_{\text{fin}}]^{\mathcal{G}}$ is an affine $\mathbb{Z}$-algebra. Therefore, by the proposition, $\Bbbk[L]^G = \Bbbk \otimes \mathbb{Z}[L_{\text{fin}}]^{\mathcal{G}}$ is affine over $\Bbbk$.

The finite group $\mathcal{G}$ embeds into $\mathrm{GL}_n(\mathbb{Z})$, where $n = \operatorname{rank} L_{\text{fin}}$. By the foregoing, the number of isomorphism classes of multiplicative invariant algebras $\Bbbk[L]^G$, with $\operatorname{rank} L$ is bounded by N, is at most equal to the sum of the numbers of conjugacy classes of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ with $n \leq N$; see Section 1.10. □

3.4 Units and Semigroup Algebras

Even though multiplicative invariant algebras arise from an action on a group algebra $\Bbbk[L]$, it turns out that $\Bbbk[L]^G$ is never a group algebra over $\Bbbk$ unless G acts trivially on the sublattice L_{fin} in (3.3). In order to justify this claim, we use the following simple lemma on unit groups.

Lemma 3.4.1. *Let L be a G-lattice and $\Bbbk$ a commutative domain. Then* $\mathrm{U}(\Bbbk[L]) = \mathrm{U}(\Bbbk) \times \underline{L}$ *and* $\mathrm{U}(\Bbbk[L]^G) = \mathrm{U}(\Bbbk) \times \underline{L}^G$.

Proof. It suffices to show that $\mathrm{U}(\Bbbk[L]) = \mathrm{U}(\Bbbk) \times \underline{L}$, because this implies that $\mathrm{U}(\Bbbk[L]^G) = \mathrm{U}(\Bbbk[L])^G = \mathrm{U}(\Bbbk) \times \underline{L}^G$. Note also that $k\mathbf{x}^m \in \mathrm{U}(\Bbbk) \times \underline{L}$ has inverse $k^{-1}\mathbf{x}^{-m}$; so $\mathrm{U}(\Bbbk) \times \underline{L} \subseteq \mathrm{U}(\Bbbk[L])$. In order to show that equality holds here, fix a *monomial order* for $\Bbbk[L]$. By definition, this is a total order $\succ$ on L that is compatible with addition: $m \succ n$ implies $m + \ell \succ n + \ell$ for $m, n, \ell \in L$. (For example, the lexicographic order with respect to any $\mathbb{Z}$-basis of L will do.) For any nonzero $f \in \Bbbk[L]$, define $\mathbf{max}(f)$ and $\mathbf{min}(f)$ to be the largest and the smallest element of the support $\operatorname{Supp} f$ with respect to $\succ$. Since $\Bbbk$ is a domain, it is easy to see that

$$\mathbf{max}(ff') = \mathbf{max}(f) + \mathbf{max}(f') \quad \text{and} \quad \mathbf{min}(ff') = \mathbf{min}(f) + \mathbf{min}(f')$$

holds for all nonzero $f, f' \in \Bbbk[L]$. Now suppose that $ff' = 1$. Then $\mathbf{max}(f) + \mathbf{max}(f') = 0 = \mathbf{min}(f) + \mathbf{min}(f')$. Since $\mathbf{max}(f) + \mathbf{max}(f') \geq \mathbf{min}(f) + \mathbf{max}(f') \geq \mathbf{min}(f) + \mathbf{min}(f')$, we conclude that $\mathbf{max}(f) = \mathbf{min}(f)$ and similarly for f'. This implies that f and f' belong to $\mathrm{U}(\Bbbk) \times \underline{L}$. □

Corollary 3.4.2. *Let L be a G-lattice, where G is an arbitrary group, and let $\Bbbk$ be a commutative ring. The invariant algebra $\Bbbk[L]^G$ is a group algebra over $\Bbbk$ precisely if the action of G on the lattice L_{fin} in* (3.3) *is trivial. In particular, if G is finite then $\Bbbk[L]^G$ is a group algebra over $\Bbbk$ only if G acts trivially.*

Proof. One direction is immediate from Proposition 3.3.1. Conversely, suppose that $\Bbbk[L]^G$ is isomorphic to a group algebra over $\Bbbk$. By Proposition 3.3.1, we may replace L by L_{fin}, thereby reducing to the case where G is finite, and we may also replace $\Bbbk$ by some prime factor; so $\Bbbk$ is a domain. Since group algebras are generated, as $\Bbbk$-algebras, by their units, we conclude from Lemma 3.4.1 that $\Bbbk[L]^G = \Bbbk[L^G]$. Thus, on the one hand, $\Bbbk[L]$ is integral over $\Bbbk[L]^G$, since G is finite, while on the other, L/L^G is $\mathbb{Z}$-free and hence $\Bbbk[L]$ is a Laurent polynomial algebra in $r = \operatorname{rank} L/L^G$ many variables over $\Bbbk[L]^G$. Thus, we must have $r = 0$. □

While multiplicative invariant algebras $\Bbbk[L]^{\mathcal{G}}$ of finite groups $\mathcal{G}$ can never be group algebras if $\mathcal{G}$ acts nontrivially, it turns out that in many cases $\Bbbk[L]^{\mathcal{G}}$ is at least a *semigroup algebra*. Explicit examples will be presented in Section 3.5 and the phenomenon will be fully explained in Theorem 6.1.1. Recall that a $\Bbbk$-algebra R is a semigroup algebra (or monoid algebra) if R has a $\Bbbk$-basis, M, that is a submonoid of the multiplicative monoid $(R, \cdot\,)$; so $1 \in M$ and M is closed under multiplication. In analogy with the notation $\Bbbk[L]$ for group algebras, $\Bbbk[M]$ will denote the semigroup algebra over $\Bbbk$ of a monoid M. For example, the semigroup algebra of the monoid $M = \mathbb{Z}_+^r \oplus \mathbb{Z}^s$ is isomorphic to the mixed Laurent polynomial algebra $\Bbbk[x_1, \dots, x_r, x_{r+1}^{\pm 1}, \dots, x_{r+s}^{\pm 1}]$ over $\Bbbk$. We will only be concerned with commutative monoids M and, as with lattices, it is customary to write them additively. Gilmer [73] is a good reference for the algebraic structure of general commutative semigroup algebras $\Bbbk[M]$. We mention the following basic facts:

- $\Bbbk[M]$ is an affine (f.g.) $\Bbbk$-algebra if and only if the monoid M is finitely generated, and
- $\Bbbk[M]$ is a domain if and only if $\Bbbk$ is a domain and M is *cancellative* ($a + c = b + c \Rightarrow a = b$ for all $a, b, c, \in M$) and *torsion-free* ($na = nb \Rightarrow a = b$ for $a, b \in M$ and $n \in \mathbb{N}$).

The first assertion is obvious; for the second, see [73, Theorem 8.1]. 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 M embeds into some lattice L, and we may clearly assume that $\langle M \rangle_{\text{group}} = L$. Finitely generated commutative monoids that are cancellative and torsion-free are often simply referred to as *affine semigroups*; see, e.g., Bruns and Herzog [32, 6.1]. An affine semigroup M is called *normal* if $nm \in M$ for $m \in \langle M \rangle_{\text{group}}$ and $n \in \mathbb{N}$ implies $m \in M$.

- $\Bbbk[M]$ is an affine $\Bbbk$-algebra that is a normal domain if and only if $\Bbbk$ is a normal domain and the monoid M is an affine normal semigroup.

For a proof, see [73, Corollary 12.11]. An affine semigroup M is called *positive* if M has no units other than 0 and an element $0 \neq m \in M$ is called *indecomposable* if $m = a + b$ $(a, b \in M)$ implies $a = 0$ or $b = 0$.

Lemma 3.4.3. *Let M be a positive affine semigroup. 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 $\{m_1, \ldots, m_s\}$.*

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 [210, 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. □

The unique smallest generating set constructed in the above lemma is called the *Hilbert basis* of M. An algorithm computing the Hilbert basis for any affine semigroup without non-trivial units can be found in Sturmfels [206, Algorithm 13.2].

3.5 Examples

In this section, we explicitly calculate the multiplicative invariant algebras of certain $\mathcal{G}$-lattices L for various finite groups $\mathcal{G}$. Throughout, we will work over $\Bbbk = \mathbb{Z}$. The results over arbitrary commutative base rings $\Bbbk$ then follow by base change; see Proposition 3.3.1(b). Examples 3.5.1, 3.5.4, 3.5.5, 3.5.6 and 3.5.7 below describe the multiplicative invariant algebras of certain reflection groups, while the group in Example 3.5.3 is a bireflection group. Table 3.1 list the multiplicative invariant algebras for lattices of rank 2; the groups in question are those in Table 1.2. The invariant algebras for the groups $\mathcal{G}_7$, $\mathcal{G}_8$ and $\mathcal{G}_9$ were obtained by direct calculation; the details for all other groups in Table 3.1 are given below.

We will repeatedly use the following obvious observation, valid for any base ring $\Bbbk$. Suppose that we have decompositions $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and $L = L_1 \oplus L_2$ with $\mathcal{G}$-sublattices L_i such that $\mathcal{G}_j$ acts trivially on L_i for $i \neq j$. Then

$$\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[L]_1^{\mathcal{G}_1} \otimes_{\Bbbk} \Bbbk[L]_2^{\mathcal{G}_2} . \tag{3.5}$$

Example 3.5.1 (The diagonal subgroup of $\mathrm{GL}_n(\mathbb{Z})$)**.** Let

$$\mathcal{T}_n = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{n \times n} \subseteq \mathrm{GL}_n(\mathbb{Z})$$

be the group of diagonal matrices, with the canonical action on $L = \bigoplus_{i=1}^n \mathbb{Z}e_i$: $t = \mathrm{diag}(t_1, \ldots, t_n) \in \mathcal{T}_n$ acts by $t(e_i) = t_i e_i$. Put $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[L]$ and $\xi_i = x_i + x_i^{-1}$. We claim that

$$\mathbb{Z}[L]^{\mathcal{T}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n] , \tag{3.6}$$

a polynomial algebra in n variables. Indeed, formula (3.5) reduces the claim to the case $n = 1$. Then $\mathbb{Z}[L] = \mathbb{Z}[x^{\pm 1}]$ and $\mathcal{T}_1 = \langle t \rangle \cong \mathcal{C}_2$ acts by $t(x) = x^{-1}$. Writing $\mathbb{Z}[x^{\pm 1}] = \mathbb{Z}[\xi] \oplus x\mathbb{Z}[\xi]$ with $\xi = x + x^{-1}$, it is easy to see that $\mathbb{Z}[x^{\pm 1}]^{\mathcal{T}_1} = \mathbb{Z}[\xi]$, as claimed.

The next example will make use of the following lemma on adding a summand of rank 1.

Lemma 3.5.2. *Let $L = L' \oplus \mathbb{Z}_\varphi$, where L' is a $\mathcal{G}$-lattice and $\mathbb{Z}_\varphi = \mathbb{Z}$ with $\mathcal{G}$ acting via a non-trivial homomorphism $\varphi \colon \mathcal{G} \to \{\pm 1\}$. Put $\mathcal{N} = \operatorname{Ker} \varphi$ and suppose that $\Bbbk[L']^{\mathcal{N}} = \Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^{m} \alpha_j \Bbbk[L']^{\mathcal{G}}$. Then:*

$$\Bbbk[L]^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} (\alpha_j x + s(\alpha_j) x^{-1}) \Bbbk[L']^{\mathcal{G}}[\xi] ,$$

where $x = \mathbf{x}^{(0_{L'},1)} \in \Bbbk[L]$, $\xi = x + x^{-1}$, and $s \in \mathcal{G} \setminus \mathcal{N}$.

Proof. Put $R = \Bbbk[L']^{\mathcal{G}} \oplus \bigoplus_{i \geq 1} \Bbbk[L']^{\mathcal{N}} \xi^i$; this is a $\mathcal{G}$-stable subalgebra of $\Bbbk[L]^{\mathcal{N}}$ such that $R^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi]$. Define additive maps $D, \rho \colon R \to \Bbbk[L]^{\mathcal{N}}$ by $D(r) = \frac{s(r)-r}{\xi}$ and $\rho(r) = r + xD(r)$.

Claim. $\Bbbk[L]^{\mathcal{G}} = \rho(R)$.

First, $s(\rho(r)) = s(r) - x^{-1}D(r) = \rho(r)$ holds for $r \in R$; so $\rho(R) \subseteq \Bbbk[L]^{\mathcal{G}}$. For the reverse inclusion, write $\Bbbk[L]$ in the form $\Bbbk[L] = \Bbbk[L'][\xi] \oplus x\Bbbk[L'][\xi]$ and consider an element $f = f_0 + xf_1 \in \Bbbk[L]$, with $f_i \in \Bbbk[L'][\xi]$. Then $s(f) = (s(f_0) + \xi s(f_1)) - xs(f_1)$ while for $g \in \mathcal{N}$, one has $g(f) = g(f_0) + xg(f_1)$. Hence, $f \in \Bbbk[L]^{\mathcal{G}}$ if and only if f_0 and f_1 belong to $\Bbbk[L'][\xi]^{\mathcal{N}} = \bigoplus_{i \geq 0} \Bbbk[L']^{\mathcal{N}} \xi^i$ and the following two conditions are satisfied:

$$\begin{aligned} s(f_1) &= -f_1 \\ s(f_0) &= f_0 + \xi f_1 \end{aligned}$$

The last equation gives: $f_0 \in R$ and $f_1 = D(f_0)$. Therefore, $f = \rho(f_0) \in \rho(R)$ and the claim is proved.

To complete the proof of the lemma, we use our hypothesis that $\Bbbk[L']^{\mathcal{N}} = \Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^{m} \alpha_j \Bbbk[L']^{\mathcal{G}}$. This results in the following expression for R:

$$\begin{aligned} R &= \Bbbk[L']^{\mathcal{G}} \oplus \bigoplus_{i \geq 1} \left(\Bbbk[L']^{\mathcal{G}} + \sum_{j=1}^{m} \alpha_j \Bbbk[L']^{\mathcal{G}} \right) \xi^i \\ &= \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} \alpha_j \xi \Bbbk[L']^{\mathcal{G}}[\xi] . \end{aligned}$$

The map ρ is $R^{\mathcal{G}}$-linear and its restriction to $R^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi]$ is the identity. Therefore, the claim implies that

$$\Bbbk[L]^{\mathcal{G}} = \Bbbk[L']^{\mathcal{G}}[\xi] + \sum_{j=1}^{m} \rho(\alpha_j \xi)\Bbbk[L']^{\mathcal{G}}[\xi] \, .$$

Finally, $\rho(\alpha_j \xi) = \alpha_j x^{-1} + s(\alpha_j)x$. To obtain the exact expression for $\Bbbk[L]^{\mathcal{G}}$ as stated in the lemma, replace α_j by $s(\alpha_j)$ throughout. □

Example 3.5.3 (The diagonal subgroup of $\mathrm{SL}_n(\mathbb{Z})$)**.** Let $\mathcal{T}_n = \mathrm{diag}(\pm 1, \dots, \pm 1)_{n\times n}$ be as in Example 3.5.1 and consider the group

$$\mathcal{G} = \mathcal{T}_n \cap \mathrm{SL}_n(\mathbb{Z})$$

with the canonical action on $L = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$. As in Example 3.5.1, put $x_i = \mathbf{x}^{e_i}$, $\xi_i = x_i + x_i^{-1} \in \mathbb{Z}[L]$. We claim that

$$\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[\xi_1, \dots, \xi_n] \oplus \theta_n \mathbb{Z}[\xi_1, \dots, \xi_n] \, , \tag{3.7}$$

where $\theta_n = \sum_{g\in\mathcal{G}} g(x_1 x_2 \dots x_n) = \mathsf{orb}(\sum_i e_i)$. We argue by induction on n. For $n = 1$, the claim says that $\mathbb{Z}[x^{\pm 1}] = \mathbb{Z}[x + x^{-1}] \oplus x\mathbb{Z}[x + x^{-1}]$, which is clear. For the inductive step, we invoke Lemma 3.5.2, with $L' = \bigoplus_{i=1}^{n-1} \mathbb{Z}e_i$ and $\mathcal{N} = \mathcal{T}_{n-1} \cap \mathrm{SL}_{n-1}(\mathbb{Z})$. Since $\mathcal{G}$ acts on L' as the full diagonal group $\mathcal{T}_{n-1}$, we know by Example 3.5.1 that $\mathbb{Z}[L']^{\mathcal{G}} = \mathbb{Z}[\xi_1, \dots, \xi_{n-1}]$. Moreover, by induction, $\mathbb{Z}[L']^{\mathcal{N}} = \mathbb{Z}[\xi_1, \dots, \xi_{n-1}] \oplus \theta_{n-1}\mathbb{Z}[\xi_1, \dots, \xi_{n-1}]$. Thus, Lemma 3.5.2 with $s = \mathrm{diag}(-1, 1, \dots, 1, -1)$ gives:

$$\begin{aligned} \mathbb{Z}[L]^{\mathcal{G}} &= \mathbb{Z}[\xi_1, \dots, \xi_{n-1}][\xi_n] + (\theta_{n-1}x_n + s(\theta_{n-1})x_n^{-1})\mathbb{Z}[\xi_1, \dots, \xi_{n-1}][\xi_n] \\ &= \mathbb{Z}[\xi_1, \dots, \xi_n] + \theta_n \mathbb{Z}[\xi_1, \dots, \xi_n] \, . \end{aligned}$$

Since the sum is clearly direct, (3.7) is proved.

Specializing to $n = 2$, we obtain the invariants of multiplicative inversion in rank 2; this is group $\mathcal{G}_{10}$ in Table 1.2:

$$\mathbb{Z}[L]^{\mathcal{G}_{10}} = \mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2] \quad \text{with } \theta = x_1 x_2 + x_1^{-1} x_2^{-1}.$$

The generating invariants satisfy the relation $\theta\xi_1\xi_2 = \theta^2 + \xi_1^2 + \xi_2^2 - 4$; so

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[x, y, z]/(x^2 + y^2 + z^2 - xyz - 4) \, .$$

The invariant rings in this example are not semigroup algebras over $\mathbb{Z}$; see Section 10.2.

Example 3.5.4 (Multiplicative invariants of the root lattice B_n)**.** The root lattice of the root system of type B_n will simply be written as B_n; so $B_n = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$. By [24, Planche II],

$$\mathrm{Aut}(B_n) = \mathcal{W}(B_n) = \{\pm 1\} \wr \mathcal{S}_n \, .$$

This group can be written as $\mathcal{W}(B_n) = \mathcal{T}_n \rtimes \mathcal{S}_n$, where $\mathcal{T}_n = \mathrm{diag}(\pm 1, \dots, \pm 1)_{n\times n}$ acts as in Example 3.5.1 and $s(e_i) = e_{s(i)}$ for $s \in \mathcal{S}_n$. Putting $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[B_n]$, as usual, the invariants of the normal subgroup $\mathcal{T}_n$ are given by Example 3.5.1:

$\mathbb{Z}[B_n]^{\mathcal{T}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n]$ with $\xi_i = x_i + x_i^{-1}$. The group $\mathcal{S}_n$ acts on the polynomial ring $\mathbb{Z}[B_n]^{\mathcal{T}_n}$ by $s(\xi_i) = \xi_{s(i)}$ for $s \in \mathcal{S}_n$. Hence, the fundamental theorem for $\mathcal{S}_n$-invariants (e.g., [27, p. A IV.58]) yields that

$$\mathbb{Z}[B_n]^{\{\pm 1\} \wr \mathcal{S}_n} = \mathbb{Z}[\xi_1, \ldots, \xi_n]^{\mathcal{S}_n} = \mathbb{Z}[\sigma_1, \ldots, \sigma_n] \,, \tag{3.8}$$

where

$$\sigma_i = \sum_{j_1 < \ldots < j_i} \xi_{j_1} \xi_{j_2} \cdots \xi_{j_i}$$

is the i^{th} elementary symmetric function in $\xi_1, \ldots, \xi_n$. Thus, $\mathbb{Z}[B_n]^{\{\pm 1\} \wr \mathcal{S}_n}$ is a polynomial ring in n variables. The special case $n = 2$ yields the invariants for group $\mathcal{G}_2$ in Table 3.1.

Example 3.5.5 (Multiplicative $\mathcal{S}_n$-invariants of U_n)**.** Restricting the lattice B_n in Example 3.5.4 to the symmetric group $\mathcal{S}_n$ we obtain the standard permutation lattice U_n for $\mathcal{S}_n$; see §1.3.3. As before, let $\{e_i\}_1^n$ denote the permutation basis of U_n and write $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[U_n]$. Then the element $\mathbf{x}^{\sum_1^n e_i} \in \mathbb{Z}[U_n]$ becomes the n^{th} elementary symmetric function $s_n = \prod_1^n x_i$. Moreover,

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

and $\mathcal{S}_n$ acts via $s(x_i) = x_{s(i)}$ $(s \in \mathcal{S}_n)$. By the fundamental theorem for $\mathcal{S}_n$-invariants, $\mathbb{Z}[x_1, \ldots, x_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_n]$, where s_i is the i^{th} elementary symmetric function in $x_1, \ldots, x_n$. Therefore,

$$\mathbb{Z}[U_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}] \cong \mathbb{Z}[\mathbb{Z}_+^{n-1} \oplus \mathbb{Z}] \,, \tag{3.9}$$

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

Example 3.5.6 (Multiplicative $\mathcal{S}_n$-invariants of A_{n-1})**.** We continue with the notation of Example 3.5.5. Note that $\mathbb{Z}[U_n] = \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is $\mathbb{Z}$-graded by total degree in the x_i's and the action of $\mathcal{S}_n$ respects this grading. Using the standard basis $a_i = e_i - e_{i+1}$ $(i = 1, \ldots, n-1)$ of the root lattice A_{n-1}, as in Example 1.8.1, and putting $y_i = \mathbf{x}^{a_i} = \frac{x_i}{x_{i+1}}$, the group ring $\mathbb{Z}[A_{n-1}]$ can be written as

$$\mathbb{Z}[A_{n-1}] = \mathbb{Z}[y_1^{\pm 1}, \ldots, y_{n-1}^{\pm 1}] = \mathbb{Z}[\frac{x_i}{x_j} \mid 1 \leq i, j \leq n] \,.$$

This is the degree 0-component $\mathbb{Z}[U_n]_0$ of $\mathbb{Z}[U_n]$. Hence,

$$\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} = \mathbb{Z}[U_n]_0^{\mathcal{S}_n} \,,$$

the ring of $\mathcal{S}_n$-invariants of total degree 0 in $\mathbb{Z}[U_n]$. By equation (3.9), a $\mathbb{Z}$-basis of $\mathbb{Z}[U_n]_0^{\mathcal{S}_n}$ is given by the elements $s_1^{t_1} \ldots s_{n-1}^{t_{n-1}} / s_n^{t_n}$ with $t_i \in \mathbb{Z}_+$ and $\sum_{i=1}^{n-1} i t_i = n t_n$. Therefore,

$$\mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} \cong \mathbb{Z}[M] \,,$$

where M is the submonoid of $\mathbb{Z}_+^{n-1}$ consisting of all $(t_1, \ldots, t_{n-1})$ so that $\sum_i it_i$ is divisible by n. The isomorphism sends the element $m = (t_1, \ldots, t_{n-1}) \in M$ to the basis element

$$\mu_m = s_n^{-\frac{1}{n}\sum_i it_i} \cdot \prod_{i=1}^{n-1} s_i^{t_i} \in \mathbb{Z}[A_{n-1}]^{\mathcal{S}_n} \ .$$

Taking $n = 2$, for example, the monoid M is generated by $m = (2)$ and we obtain the fundamental invariant $\mu_m = s_1^2/s_2 = y_1 + y_1^{-1} + 2$. Thus, $\mathbb{Z}[A_1]^{\mathcal{S}_2} = \mathbb{Z}[y_1 + y_1^{-1}]$ is a polynomial algebra. This is just the special case $n = 1$ of Example 3.5.1, since A_1 is the sign lattice $\mathbb{Z}^-$ for $\mathcal{S}_2$.

For $n = 3$, the monoid M has generators $m_1 = (3, 0)$, $m_2 = (0, 3)$ and $m_3 = (1, 1)$. This yields the fundamental invariants $\mu_1 = s_1^3/s_3$, $\mu_2 = s_2^3/s_3^2$ and $\mu_3 = s_1 s_2/s_3$ for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$. Note that $\mu_1\mu_2 = \mu_3^3$; so we obtain the presentation

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

A more economical system of fundamental invariants for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$ is given by

$$\begin{aligned} \mu_3 - 3 &= y_1 + y_1^{-1} + y_2 + y_2^{-1} + y_1 y_2 + y_1^{-1} y_2^{-1} &&= \mathsf{orb}(a_1) \\ \mu_1 - 3\mu_3 + 3 &= y_1^2 y_2 + y_1^{-1} y_2 + y_1^{-1} y_2^{-2} &&= \mathsf{orb}(2a_1 + a_2) \\ \mu_2 - 3\mu_3 + 3 &= y_1 y_2^2 + y_1 y_2^{-1} + y_1^{-2} y_2^{-1} &&= \mathsf{orb}(a_1 + 2a_2) \end{aligned}$$

Example 3.5.7 (non-diagonal Klein 4-group)**.** Consider the group $\mathcal{G} = \mathcal{G}_6 = \langle s, -s \rangle \cong \mathcal{C}_2 \times \mathcal{C}_2$ of Table 1.2. Here, $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Note that both generators s and $-s$ act as (non-diagonalizable) reflections on $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$. Their product, $g = s(-s) \in \mathcal{G}$, acts as $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, as in Example 3.5.3 above. Thus, using Example 3.5.3 and its notation, we obtain $\mathbb{Z}[L]^{\mathcal{G}} = R^{\langle s \rangle}$ with $R = \mathbb{Z}[L]^{\langle g \rangle} = \mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2]$. Since s interchanges ξ_1 and ξ_2 and leaves θ invariant, the invariant ring is given by

$$\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[\sigma_1, \sigma_2] \oplus \theta\mathbb{Z}[\sigma_1, \sigma_2] \ ,$$

where $\sigma_1 = \xi_1 + \xi_2$ and $\sigma_2 = \xi_1 \xi_2$ are the 1st and 2nd elementary symmetric functions in ξ_1, ξ_2. An alternative set of fundamental invariants is

$$\begin{aligned} \mu_1 &= \theta + 2 = x_1 x_2 + x_1^{-1} x_2^{-1} + 2 \ , \\ \mu_2 &= \sigma_2 - \theta + 2 = x_1 x_2^{-1} + x_1^{-1} x_2 + 2 \ , \\ \mu_3 &= \sigma_1 = x_1 + x_1^{-1} + x_2 + x_2^{-1} \ . \end{aligned}$$

These invariants satisfy the relation $\mu_3^2 = \mu_1\mu_2$; so we obtain the presentation

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[x, y, z]/(z^2 - xy) \ .$$

This shows that $\mathbb{Z}[L]^{\mathcal{G}}$ is isomorphic to the semigroup algebra $\mathbb{Z}[M]$, where M is the submonoid of $\mathbb{Z}_+^2$ that is generated by the elements $(2, 0)$, $(0, 2)$ and $(1, 1)$.

Table 3.1. Multiplicative invariants in rank 2

group $\mathcal{G}$ (cf. Table 1.2)	invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$	reference
$\mathcal{G}_1 \cong \mathcal{D}_{12}$	polynomial algebra $\mathbb{Z}[\alpha, \beta]$ $\alpha = x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_1x_2 + x_1^{-1}x_2^{-1}$ $\beta = x_1x_2^{-1} + x_1^{-1}x_2 + x_1^2x_2 + x_1x_2^2 + x_1^{-2}x_2^{-1} + x_1^{-1}x_2^{-2}$	Example 3.7.1
$\mathcal{G}_2 \cong \mathcal{D}_8$	polynomial algebra $\mathbb{Z}[\xi_1 + \xi_2, \xi_1\xi_2]$ with $\xi_i = x_i + x_i^{-1}$	Example 3.5.4 for $n = 2$
$\mathcal{G}_3 \cong \mathcal{S}_3$	semigroup algebra $\mathbb{Z}[\mu_1, \mu_2] \oplus \mu_3\mathbb{Z}[\mu_1, \mu_2]$ $\mu_1 = s_1^3/s_3$, $\mu_2 = s_2^3/s_3^2$, $\mu_3 = s_1s_2/s_3$ $s_i = s_i(x_1, x_2, x_3)$ the i^{th} elem. symm. function relation: $\mu_1\mu_2 = \mu_3^3$	Example 3.5.6 for $n = 3$
$\mathcal{G}_4 \cong \mathcal{S}_3$	polynomial algebra $\mathbb{Z}[\eta_+, \eta_-]$ $\eta_+ = x_1 + x_2 + x_1^{-1}x_2^{-1}$, $\eta_- = x_1^{-1} + x_2^{-1} + x_1x_2$	Example 3.7.1 for $n = 3$
$\mathcal{G}_5 \cong \mathcal{C}_2 \times \mathcal{C}_2$	polynomial algebra $\mathbb{Z}[\xi_1, \xi_2]$ with $\xi_i = x_i + x_i^{-1}$	Example 3.5.1 for $n = 2$
$\mathcal{G}_6 \cong \mathcal{C}_2 \times \mathcal{C}_2$	semigroup algebra $\mathbb{Z}[\mu_1, \mu_2] \oplus \mu_3\mathbb{Z}[\mu_1, \mu_2]$ $\mu_1 = x_1x_2 + x_1^{-1}x_2^{-1} + 2$, $\mu_2 = x_1x_2^{-1} + x_1^{-1}x_2 + 2$, $\mu_3 = x_1 + x_1^{-1} + x_2 + x_2^{-1}$ relation: $\mu_1\mu_2 = \mu_3^2$	Example 3.5.7
$\mathcal{G}_7 \cong \mathcal{C}_6$	$\mathbb{Z}[\tau_1, \tau_2] \oplus \sigma\mathbb{Z}[\tau_1, \tau_2]$ $\tau_1 = \eta_+ + \eta_-$, $\tau_2 = \eta_+\eta_-$, $\sigma = \eta_+\varphi + \eta_-\varphi_-$ with η_+, η_-, φ as for $\mathcal{G}_9$ and $\varphi_- = x_1^{-1}x_2^{-2} + x_1^2x_2 + x_1^{-1}x_2 + 6$ relation: $\sigma^2 = \tau_1(\tau_2+9)\sigma - \tau_2(\tau_2+9)^2 + (\tau_1^2 - 4\tau_2)(3\tau_1\tau_2 - \tau_1^3 - 27)$	
$\mathcal{G}_8 \cong \mathcal{C}_4$	$\mathbb{Z}[\sigma_1, \sigma_2] \oplus \rho\mathbb{Z}[\sigma_1, \sigma_2]$ $\sigma_1 = \xi_1 + \xi_2$, $\sigma_2 = \xi_1\xi_2$, where $\xi_i = x_i + x_i^{-1}$, and $\rho = x_1x_2^2 + x_1^{-1}x_2^{-2} + x_1^2x_2^{-1} + x_1^{-2}x_2 + 3\sigma_1$ relation: $\rho^2 = \rho\sigma_1(\sigma_2 + 4) + 4\sigma_1^2\sigma_2 - \sigma_1^4 - \sigma_2(\sigma_2 + 4)^2$	
$\mathcal{G}_9 \cong \mathcal{C}_3$	$\mathbb{Z}[\eta_+, \eta_-] \oplus \varphi\mathbb{Z}[\eta_+, \eta_-]$ $\eta_+ = x_1 + x_2 + x_1^{-1}x_2^{-1}$, $\eta_- = x_1^{-1} + x_2^{-1} + x_1x_2$, $\varphi = x_1x_2^2 + x_1^{-2}x_2^{-1} + x_1x_2^{-1} + 6$ relation: $\varphi\eta_+\eta_- = \eta_+^3 + \eta_-^3 + \varphi^2 - 9\varphi + 27$	

Table 3.1. (continued)

group $\mathcal{G}$ (cf. Table 1.2)	invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$	reference
$\mathcal{G}_{10} \cong \mathcal{C}_2$	$\mathbb{Z}[\xi_1, \xi_2] \oplus \theta\mathbb{Z}[\xi_1, \xi_2]$ $\xi_i = x_i + x_i^{-1}, \theta = x_1x_2 + x_1^{-1}x_2^{-1}$ relation: $\theta\xi_1\xi_2 = \theta^2 + \xi_1^2 + \xi_2^2 - 4$	Example 3.5.3
$\mathcal{G}_{11} \cong \mathcal{C}_2$	Laurent polynomial algebra $\mathbb{Z}[x_1 + x_1^{-1}, x_2^{\pm 1}]$	Example 3.5.1 for $n = 1$ and (3.5)
$\mathcal{G}_{12} \cong \mathcal{C}_2$	Laurent polynomial algebra $\mathbb{Z}[x_1 + x_2, (x_1x_2)^{\pm 1}]$	Example 3.5.5 for $n = 2$

3.6 Multiplicative Invariants of Weight Lattices

The following result is classical; see [24, Théorème VI.3.1 and Exemple 1]. We use the notation and terminology of Section 1.8.

Theorem 3.6.1 (Bourbaki)**.** *Let $\Lambda = \Lambda(\Phi)$ be the weight lattice of a reduced root system Φ and let $\mathcal{W} = \mathcal{W}(\Phi)$ denote its Weyl group. Then the multiplicative invariant algebra $\mathbb{Z}[\Lambda]^{\mathcal{W}}$ is a polynomial algebra over $\mathbb{Z}$: the $\mathcal{W}$-orbit sums of a set of fundamental weights are algebraically independent generators.*

Proof. Fix a base $\Delta = \{a_i\}$ of Φ and let $\{m_j\} \subseteq \Lambda$ be the corresponding set of fundamental weights; so $\langle a_i^\vee, m_j\rangle = \delta_{i,j}$. Put

$$\Lambda_+ = \{m \in \Lambda \mid \langle a^\vee, m\rangle \geq 0 \text{ for all } a \in \Delta\} = \bigoplus_j \mathbb{Z}_+ m_j \ . \tag{3.10}$$

The argument depends on the following standard facts about root systems:

(a) Every $\mathcal{W}$-orbit in Λ meets the set Λ_+ in exactly one point; see [24, Théorème VI.1.2(ii)].
(b) Define a partial order on Λ by $m \geq m' \iff m - m' \in \bigoplus_{a\in\Delta} \mathbb{R}_+ a$. Then $m \geq g(m)$ holds for all $m \in \Lambda_+$ and $g \in \mathcal{W}$; see [24, Prop. VI.1.18].
(c) The restriction of $\geq$ to Λ_+ satisfies the descending chain condition. In fact, for each $m \in \Lambda_+$, there are only finitely many $m' \in \Lambda_+$ with $m \geq m'$; see [24, p. 187] or [93, Lemma 13.2.B].

By (a) and (3.4), we have:

$$\mathbb{Z}[\Lambda]^{\mathcal{W}} = \bigoplus_{m \in \Lambda_+} \mathbb{Z}\,\mathsf{orb}(m) \ . \tag{3.11}$$

Define elements $f_m \in \mathbb{Z}[\Lambda]^{\mathcal{W}}$ $(m \in \Lambda_+)$ by

$$f_m = \prod_j \mathsf{orb}(m_j)^{z_j} \ ,$$

where $m = \sum_j z_j m_j$ with (uniquely determined) $z_j \in \mathbb{Z}_+$. The theorem asserts that the family $F = \{f_m\}_{m \in \Lambda_+}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\Lambda]^{\mathcal{W}}$.

To prove this, note that, with respect to the partial order $\geq$ of (b), each $m \in \Lambda_+$ is the unique largest element of the support $\mathrm{Supp}(\mathsf{orb}(m)) = \mathcal{W}(m)$. Since $\geq$ is compatible with addition (i.e., $m \geq m' \Rightarrow m + w \geq m' + w$ for $m, m', w \in \Lambda$), we deduce that m is the unique largest element in $\mathrm{Supp}\, f_m$ and its $\mathbb{Z}$-coefficient is 1. Therefore, by (3.11), f_m can be written as a finite sum

$$f_m = \mathsf{orb}(m) + \sum_{\substack{m' \in \Lambda_+ \\ m' < m}} z_{m,m'}\, \mathsf{orb}(m') \ . \tag{3.12}$$

This formula implies that the family $F = \{f_m\}_{m \in \Lambda_+}$ is $\mathbb{Z}$-independent, because $\{\mathsf{orb}(m)\}_{m \in \Lambda_+}$ is. Also, each orbit sum $\mathsf{orb}(m)$ $(m \in \Lambda_+)$ is a $\mathbb{Z}$-linear combination of elements in F. Otherwise (c) would allow us to pick a counterexample m that is minimal with respect to $\geq$. Thus, all $\mathsf{orb}(m')$ in (3.12) can be expressed in terms of F, and hence $\mathsf{orb}(m)$ as well, a contradiction. This completes the proof that F is a $\mathbb{Z}$-basis of $\mathbb{Z}[\Lambda]^{\mathcal{W}}$. □

The converse of Bourbaki's theorem is also true: all multiplicative invariant algebras that are polynomial algebras come from weight lattices; see Corollary 7.1.2 below. Since the root lattice B_n is equal to the weight lattice for C_n, Example 3.5.4 provides an illustration of Theorem 3.6.1. Here is a second example:

Example 3.6.2 (Multiplicative $\mathcal{S}_n$-invariants of A_{n-1}^*)**.** As was pointed out in Example 1.8.1, we may think of A_{n-1}^* as the weight lattice $\Lambda(A_{n-1})$ of the root system A_{n-1}. Put $\ell_i = e_i - \frac{1}{n}\sum_{j=1}^n e_j \in \Lambda(A_{n-1}) = A_{n-1}^*$, where $\{e_i\}_1^n$ denotes the canonical permutation basis of U_n as in Example 3.5.5. Then the elements $m_i = \sum_{j=1}^i \ell_j = \sum_{j=1}^i e_j - \frac{i}{n}\sum_{j=1}^n e_j$ are the fundamental weights of A_{n-1} corresponding to the base $\Delta = \{e_i - e_{i+1}\}_1^{n-1}$. Putting $x_i = \mathbf{x}^{e_i} \in \mathbb{Z}[U_n]$ and $\xi_i = \mathbf{x}^{\ell_i} \in \mathbb{Z}[A_{n-1}^*]$ and letting s_i denote the i^{th} elementary symmetric function we calculate the $\mathcal{S}_n$-orbit sum of m_i as follows:

$$\begin{aligned}
\mathsf{orb}(m_i) &= \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I| = i}} \mathbf{x}^{\sum_{j \in I} e_j - \frac{i}{n}\sum_{j=1}^n e_j} \\
&= s_i(x_1, \dots, x_n) \cdot s_n(x_1, \dots, x_n)^{-i/n} \\
&= s_i(\xi_1, \dots, \xi_n) \ .
\end{aligned} \tag{3.13}$$

By Theorem 3.6.1, the elements $s_i(\xi_1, \dots, \xi_n)$ are algebraically independent generators of $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$. A direct verification, independent of Theorem 3.6.1, will be given in Example 3.7.1 below.

3.7 Passage to an Effective Lattice

Let L be a lattice for the finite group $\mathcal{G}$ and let $\overline{L} = L/L^{\mathcal{G}}$ denote its effective quotient; see Section 1.6. The canonical map $\overline{} : L \twoheadrightarrow \overline{L}$ extends to $k[L]$:

$$\overline{} : \Bbbk[L] \twoheadrightarrow \Bbbk[\overline{L}] = k[L/L^{\mathcal{G}}] , \quad \mathbf{x}^m \mapsto \mathbf{x}^{m+L^{\mathcal{G}}} \ (m \in L) .$$

It follows from (1.17) that the orbit sum of an element $m \in L$ satisfies

$$\overline{\mathsf{orb}(m)} = \mathsf{orb}(\overline{m}) .$$

Moreover, $\mathsf{orb}(\overline{a}) = \mathsf{orb}(\overline{b})$ is equivalent to $\mathsf{orb}(a) = \mathsf{orb}(b)\mathbf{x}^c$ for some $c \in L^{\mathcal{G}}$. Consequently, (3.4) implies that

$$\Bbbk[\overline{L}]^{\mathcal{G}} = \overline{\Bbbk[L]^{\mathcal{G}}} \cong \Bbbk[L]^{\mathcal{G}} / \left(\mathbf{x}^m - 1 \mid m \in L^{\mathcal{G}}\right) . \tag{3.14}$$

Here, it suffices to let m run over a $\mathbb{Z}$-basis of $L^{\mathcal{G}}$. The isomorphism (3.14) cannot in general be strengthened to $\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[\overline{L}]^{\mathcal{G}} \otimes_k \Bbbk[L^{\mathcal{G}}]$; cf. Example 4.2.1 below.

Example 3.7.1 (Multiplicative $\mathcal{S}_n$-invariants of A_{n-1}^*, revisited)**.** The invariant algebra $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ can also be calculated from (3.14). Indeed, dualizing the augmentation sequence (1.10) and using the fact that $\mathbb{Z}$ and U_n are self-dual (being permutation lattices) one obtains an exact sequence of $\mathcal{S}_n$-lattices

$$0 \to \mathbb{Z} \longrightarrow U_n \longrightarrow A_{n-1}^* \to 0 .$$

Thus,

$$A_{n-1}^* \cong U_n/U_n^{\mathcal{S}_n} = \overline{U_n} , \tag{3.15}$$

and so (3.14) applies. In detail, using the notation of Example 3.5.5, the $\mathcal{S}_n$-invariants $U_n^{\mathcal{S}_n}$ are spanned by the element $\sum_1^n e_i$ and $\mathbf{x}^{\sum_1^n e_i} \in \mathbb{Z}[U_n]$ is the n^{th} elementary symmetric function $s_n = \prod_1^n x_i$. By (3.9), $\mathbb{Z}[U_n]^{\mathcal{S}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]$, and so (3.14) yields that $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ is isomorphic to $\mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]/(s_n - 1)$. Thus,

$$\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n} \cong \mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n} \cong \mathbb{Z}[s_1, \ldots, s_{n-1}] , \tag{3.16}$$

a polynomial algebra in $n-1$ variables.

To make the connection with the description of $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n}$ given in Example 3.6.2, we use the $\mathcal{S}_n$-lattice isomorphism

$$\overline{U_n} \xrightarrow{\sim} \Lambda(A_{n-1}) , \quad \overline{e_i} \mapsto \ell_i = e_i - \frac{1}{n}\sum_{j=1}^n e_j . \tag{3.17}$$

This isomorphism yields an isomorphism $\mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n} \xrightarrow{\sim} \mathbb{Z}[\Lambda(A_{n-1})]^{\mathcal{S}_n}$ sending the generators s_i in (3.16) to the generators $s_i(\xi_1, \ldots, \xi_n)$ constructed in Example 3.6.2.

Finally, we point put how the foregoing yields the fundamental invariants for the groups $\mathcal{G}_1$ and $\mathcal{G}_4$ in Table 3.1. Under the second isomorphism in (3.16), i^{th} elementary symmetric function s_i becomes the orbit sum $\mathsf{orb}(\overline{e_1} + \cdots + \overline{e_i})$. Thus, writing $y_i = \mathbf{x}^{\overline{e_i}} \in \mathbb{Z}[\overline{U_n}]$, we obtain the following fundamental invariants in $\mathbb{Z}[A_{n-1}^*]^{\mathcal{S}_n} \cong \mathbb{Z}[\overline{U_n}]^{\mathcal{S}_n}$ for $n = 3$:

$$\begin{aligned} \eta_1 &= \mathsf{orb}(\overline{e_1}) = y_1 + y_2 + y_1^{-1}y_2^{-1} \\ \eta_2 &= \mathsf{orb}(\overline{e_1} + \overline{e_2}) = y_1y_2 + y_1^{-1} + y_2^{-1} \end{aligned}$$

This takes care of group $\mathcal{G}_4$. For $\mathcal{G}_1$, note that $\mathcal{G}_1 = \langle \mathcal{G}_4, -\operatorname{Id}\rangle$ and $-\operatorname{Id}$ interchanges the above two invariants η_1 and η_2. Thus we have the following fundamental invariants for $\mathcal{G}_1$:

$$\begin{aligned} \eta_1 + \eta_2 &= y_1 + y_1^{-1} + y_2 + y_2^{-1} + y_1y_2 + y_1^{-1}y_2^{-1} \\ \eta_1\eta_2 - 3 &= y_1y_2^{-1} + y_1^{-1}y_2 + y_1^2y_2 + y_1^{-2}y_2^{-1} + y_1y_2^2 + y_1^{-1}y_2^{-2} \end{aligned}$$

3.8 Twisted Multiplicative Actions

3.8.1 The Setting

Let R be some commutative domain and let $R[L]$ be the group algebra of the lattice L over R. Suppose a group G acts by ring automorphisms on $R[L]$ in such a way that $g(R) \subseteq R$ holds for all $g \in G$. In short, $R \subseteq R[L]$ is an extension of G-rings. Then G stabilizes the unit groups of $\mathrm{U}(R)$ and $\mathrm{U}(R[L])$. By Lemma 3.4.1, $\mathrm{U}(R[L]) = \mathrm{U}(R) \times \underline{L}$. Hence, the lattice L becomes a G-lattice that fits into an exact sequence of G-modules

$$1 \to \mathrm{U}(R) \to \mathrm{U}(R[L]) \to L \to 1\,. \tag{3.18}$$

This extension of G-modules need not split. The G-action on $R[L]$ is called *twisted multiplicative* and the group ring $R[L]$ will be called a *twisted multiplicative G-ring*. We will use the notation

$$R[L]_\gamma$$

to denote $R[L]$ with a twisted multiplicative action. Explicitly, the action of $g \in G$ on $R[L]_\gamma$ is given by the formula

$$g(\sum_{m \in L} r_m \mathbf{x}^m) = \sum_{m \in L} g(r_m)\gamma_{g(m)}(g)\mathbf{x}^{g(m)} \tag{3.19}$$

for suitable elements $\gamma_{g(m)}(g) \in \mathrm{U}(R)$. The map $\gamma(g)\colon m \mapsto \gamma_m(g)$ belongs to $\operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$. Moreover, viewing $\operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$ as G-module as in §1.4.2, we have the identity

$$\gamma(gg') = (g\gamma(g'))\gamma(g) \tag{3.20}$$

for $g, g' \in G$. Thus, $\gamma\colon G \to \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$ is a 1-cocycle. Let γ' be a 1-cocycle in the same cohomology class as γ; so $\gamma'(g) = \gamma(g)fg(f)^{-1}$ for some $f \in \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))$. Then the map $R[L]_\gamma \to R[L]_{\gamma'}$, $r\mathbf{x}^m \mapsto rf(m)\mathbf{x}^m$, is an isomorphism of G-rings that is the identity on R. Therefore, we may view γ as an element of $H^1(G, \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R)))$. Under the standard isomorphism $H^1(G, \operatorname{Hom}_{\mathbb{Z}}(L, \mathrm{U}(R))) \cong \operatorname{Ext}_{\mathbb{Z}[G]}(L, \mathrm{U}(R))$ (see Brown [31, Proposition III.2.2]), γ becomes the class of the extension (3.18).

Example 3.8.1. Twisted multiplicative actions often arise in the investigation of ordinary multiplicative actions as follows. Given an extension of G-lattices $0 \to N \to M \to L \to 0$, the ordinary multiplicative action of G on $\Bbbk[M]$ can be viewed as a twisted multiplicative action on $R[L]_\gamma$, with $R = \Bbbk[N]$ and γ the image of the class in $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, N)$ of the given lattice extension under the G-embedding $N \hookrightarrow \mathrm{U}(R)$.

3.8.2 The Split Case

Twisted multiplicative actions with trivial extension class γ will simply be written as

$$R[L]\ .$$

In this case, the action (3.19) simplifies to

$$g(\sum_{m\in L} r_m \mathbf{x}^m) = \sum_{m\in L} g(r_m)\mathbf{x}^{g(m)}\ . \tag{3.21}$$

Of course, if G acts trivially on R then (3.19) is an ordinary multiplicative action (3.2). In the following, the notation $\Bbbk[L]$, for a G-lattice L, will always stand for the group algebra of L over $\Bbbk$ with the ordinary multiplicative action (3.2). In other words, all group actions on $\Bbbk$ are assumed trivial.

Twisted multiplicative actions of the form (3.21) are particularly important in the case where $R = K$ is a field and G is a finite group acting faithfully by automorphisms on K. The invariant algebra $K[L]^G$ is then called an *algebra of torus invariants*. The connection with algebraic tori will be explained in Section 3.10 below.

3.8.3 Linearization via Permutation Lattices

Let L be a lattice and $\Bbbk$ a commutative domain. Any group action by $\Bbbk$-algebra automorphisms on $\Bbbk[L]$ is twisted multiplicative. Thus, the remarks in §3.8.1 lead to the following description of the automorphism group of $\Bbbk[L]$:

$$\operatorname{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L]) = \operatorname{Hom}(L, \mathrm{U}(\Bbbk)) \rtimes \mathrm{GL}(L) \tag{3.22}$$

with $\mathrm{GL}(L)$ acting by the ordinary multiplicative action (3.2) and with

$$f(\mathbf{x}^m) = f(m)\mathbf{x}^m$$

for $f \in \operatorname{Hom}(L, \mathrm{U}(\Bbbk))$ and $m \in L$. These actions commute by the rule $gf = g(f)g$ for $g \in \mathrm{GL}(L)$ and $f \in \operatorname{Hom}(L, \mathrm{U}(\Bbbk))$, where $g(f) \in \operatorname{Hom}(L, \mathrm{U}(\Bbbk))$ is defined as in §1.4.2.

As an application, we present the following linearization result which is essentially proved in Barge [4].

Proposition 3.8.2. *Let* $\Bbbk$ *be an algebraically closed field of characteristic* 0 *and let* $\mathcal{G}$ *be a finite group acting by* $\Bbbk$*-algebra automorphisms on* $\Bbbk[L]$*. Assume that, viewed as* $\mathcal{G}$*-lattice as in* (3.18)*,* L *is rationally isomorphic to some permutation* $\mathcal{G}$*-lattice. Then there exists a finite extension* $\widetilde{\mathcal{G}}$ *of* $\mathcal{G}$ *and a linear* $\Bbbk$*-representation* $\widetilde{\mathcal{G}} \to \mathrm{GL}(V)$ *so that*

$$\Bbbk[L]^{\mathcal{G}} \cong \mathsf{S}(V)^{\widetilde{\mathcal{G}}}[1/f]$$

for some $0 \neq f \in \mathsf{S}(V)^{\widetilde{\mathcal{G}}}$.

Proof. We may assume that $\mathcal{G}$ acts faithfully on $\Bbbk[L]$; so $\mathcal{G} \subseteq \mathrm{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L]) = \mathrm{Hom}(L, \Bbbk^*) \rtimes \mathrm{GL}(L)$. The action of $\mathcal{G}$ on L is given by the map $\varphi \colon \mathcal{G} \hookrightarrow \mathrm{Hom}(L, \Bbbk^*) \rtimes \mathrm{GL}(L) \overset{\text{can.}}{\twoheadrightarrow} \mathrm{GL}(L)$. Furthermore, $\mathcal{G} \subseteq \mathrm{Hom}(L, \Bbbk^*) \rtimes \varphi(\mathcal{G})$. By hypothesis, there is a permutation $\mathcal{G}$-lattice P with $L \subseteq P$ and P/L finite. Let $\psi \colon \mathcal{G} \to \mathrm{GL}(P)$ denote its structure map. Restriction from P to L gives an isomorphism $\psi(\mathcal{G}) \xrightarrow{\sim} \varphi(\mathcal{G})$ and an exact sequence $0 \to \mathrm{Hom}(P/L, \Bbbk^*) \to \mathrm{Hom}(P, \Bbbk^*) \to \mathrm{Hom}(L, \Bbbk^*) \to 0$, and these maps combine to give an epimorphism $\rho \colon \mathrm{Hom}(P, \Bbbk^*) \rtimes \psi(\mathcal{G}) \twoheadrightarrow \mathrm{Hom}(L, \Bbbk^*) \rtimes \varphi(\mathcal{G})$ with kernel $\mathcal{N} = \mathrm{Hom}(P/L, \Bbbk^*) \cong P/L$. Let $\widetilde{\mathcal{G}}$ denote the inverse image of $\mathcal{G}$ under ρ; so we have an extension of groups $1 \to \mathcal{N} \to \widetilde{\mathcal{G}} \xrightarrow{\rho} \mathcal{G} \to 1$. It is easy to see that $\Bbbk[P]^{\mathcal{N}} = \Bbbk[L]$. Therefore, $\Bbbk[P]^{\widetilde{\mathcal{G}}} = \Bbbk[L]^{\mathcal{G}}$. Finally, let $\{m_1, \dots, m_n\}$ be a $\mathbb{Z}$-basis of P that is permuted by the action of $\mathcal{G}$. Then $\mathrm{Hom}(P, \Bbbk^*) \rtimes \psi(\mathcal{G})$ stabilizes the $\Bbbk$-subspace $V = \bigoplus_i \Bbbk \mathbf{x}^{m_i}$ of $\Bbbk[P]$, and hence so does $\widetilde{\mathcal{G}}$. Moreover, $\Bbbk[P] = \mathsf{S}(V)[1/f]$, where $f = \prod_i \mathbf{x}^{m_i}$ is a $\widetilde{\mathcal{G}}$-semiinvariant, that is, $g(f) = \lambda(g)f$ for some $\lambda \in \mathrm{Hom}(\widetilde{\mathcal{G}}, \Bbbk^*)$. Replacing f by $f^{|\widetilde{\mathcal{G}}|}$ we can make f invariant. Hence, $\Bbbk[L]^{\mathcal{G}} = \Bbbk[P]^{\widetilde{\mathcal{G}}} = \mathsf{S}(V)^{\widetilde{\mathcal{G}}}[1/f]$, as desired. □

3.9 Hopf Structure

The group algebra $\Bbbk[L]$ is a *Hopf algebra* over $\Bbbk$: the comultiplication $\Delta \colon \Bbbk[L] \to \Bbbk[L] \otimes_{\Bbbk} \Bbbk[L]$, counit (or augmentation) $\varepsilon \colon \Bbbk[L] \to \Bbbk$, and antipode $S \colon \Bbbk[L] \to \Bbbk[L]$ are given by $\Bbbk$-linear extension of the rules

$$\Delta(\mathbf{x}^m) = \mathbf{x}^m \otimes \mathbf{x}^m \ , \ \varepsilon(\mathbf{x}^m) = 1 \ , \ S(\mathbf{x}^m) = \mathbf{x}^{-m}$$

for $m \in L$. If $\Bbbk$ has no idempotents other than 0 and 1, the set of "monomials" $\underline{L} = \{\mathbf{x}^m \mid m \in L\}$ can be characterized as the set of group-like elements of $\Bbbk[L]$,

$$\underline{L} = \{f \in \Bbbk[L] \mid \Delta(f) = f \otimes f, \varepsilon(f) = 1\} \ . \tag{3.23}$$

Thus, every Hopf morphism $\Bbbk[L] \to \Bbbk[L]$ must map $\underline{L}$ to itself. In particular,

$$\mathrm{Aut}_{\mathrm{Hopf}}(\Bbbk[L]) \cong \mathrm{GL}(L) \ .$$

3.10 Torus Invariants

We briefly sketch the connection of algebras of torus invariants as introduced in Section 3.8 with algebraic tori. For background on algebraic groups, we refer to Borel [19]. The algebra of regular functions of an algebraic group G will be denoted by $\mathcal{O}(G)$.

By definition, an algebraic $\Bbbk$-torus, for a field $\Bbbk$, is an affine algebraic group T defined over $\Bbbk$ so that, over the algebraic closure of $\Bbbk$, T becomes isomorphic to $\mathbb{G}_{\mathrm{m}}^n = \mathbb{G}_{\mathrm{m}} \times \cdots \times \mathbb{G}_{\mathrm{m}}$ (n factors) for some n. Here, $\mathbb{G}_{\mathrm{m}} = \mathrm{GL}_1$ is the multiplicative group, that is, the algebraic group defined by the Hopf algebra $\mathcal{O}(\mathbb{G}_{\mathrm{m}}) = \Bbbk[t^{\pm 1}] \cong \Bbbk[\mathbb{Z}]$. It is known that T already becomes isomorphic to $\mathbb{G}_{\mathrm{m}}^n$ over some finite Galois extension $K/\Bbbk$; see [19, 8.11]. Explicitly, this means that the Hopf algebra $\mathcal{O}(K \otimes_{\Bbbk} T) = K \otimes_{\Bbbk} \mathcal{O}(T)$ is isomorphic to the group algebra $K[L]$ with $L \cong \mathbb{Z}^n$; see [19, 8.5]. By (3.23), the lattice L can be identified with the character group

$$X(K \otimes_{\Bbbk} T) = \mathrm{Hom}_{\mathsf{Hopf}}(K[t^{\pm 1}], K \otimes_{\Bbbk} \mathcal{O}(T)) \ .$$

The action of the Galois group $\mathcal{G} = \mathrm{Gal}(K/\Bbbk)$ on K induces $\mathcal{G}$-actions on $\mathcal{O}(K \otimes_{\Bbbk} T)$ and on $X(K \otimes_{\Bbbk} T)$, thereby making L a $\mathcal{G}$-lattice. Moreover,

$$\mathcal{O}(T) = (K \otimes_{\Bbbk} \mathcal{O}(T))^{\mathcal{G}} \cong K[L]^{\mathcal{G}} \ ;$$

so $\mathcal{O}(T)$ is an algebra of torus invariants as in Section 3.8. Conversely, given a field K with a faithful action by a finite group $\mathcal{G}$ and a $\mathcal{G}$-lattice L, the Galois descent lemma (Lemma 9.4.1 below) implies that $K[L] = K \otimes_{\Bbbk} K[L]^{\mathcal{G}}$, where $\Bbbk = K^{\mathcal{G}}$ is the subfield of $\mathcal{G}$-invariants; so $K[L]^{\mathcal{G}} = \mathcal{O}(T)$ for some $\Bbbk$-torus T.

4

Class Group

4.1 Introduction

In this chapter, we determine the class group of a multiplicative invariant algebra. Throughout, we work over a Krull domain $\Bbbk$.

Recall that a commutative domain R is called a *Krull domain* if it satisfies the following three conditions:

(a) $R_{\mathfrak{P}}$ is a discrete valuation domain for each height 1-prime $\mathfrak{P}$ of R,
(b) $\bigcap_{\mathfrak{P}} R_{\mathfrak{P}} = R$, where $\mathfrak{P}$ runs over the height 1-primes of R, and
(c) each $0 \neq r \in R$ is contained in only finitely many height 1-primes of R.

Conditions (a) and (b) imply that R is integrally closed, because all $R_{\mathfrak{P}}$ are. If R is noetherian, (c) is automatic and the above conditions are in fact equivalent to R being integrally closed; see Bourbaki [23] or Fossum [67]. Any unique factorization domain is a Krull domain but the converse is far from true. For an arbitrary Krull domain R, the class group $\mathrm{Cl}(R)$ is defined so as to measure the "unique factorization defect": $\mathrm{Cl}(R)$ is trivial precisely if R is a UFD. We will review the definition of $\mathrm{Cl}(R)$ in Section 4.3 below.

Turning to the special case of multiplicative invariants $R = \Bbbk[L]^{\mathcal{G}}$, it follows from [67, 1.2, 1.6 and 1.8] that $\Bbbk[L]^{\mathcal{G}}$ is a Krull domain if and only if $\Bbbk$ is. In this case, we have the following formula [121].

Theorem 4.1.1. *Let L be a faithful lattice for the finite group $\mathcal{G}$ and let $\Bbbk$ be a Krull domain. Then*

$$\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \cong \mathrm{Cl}(\Bbbk) \oplus \mathrm{Hom}(\mathcal{G}/\mathcal{R}, \mathrm{U}(\Bbbk)) \oplus H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}}),$$

where $\mathcal{R} = \mathcal{R}^1_L(\mathcal{G})$ denotes the subgroup of $\mathcal{G}$ that is generated by all elements acting as reflections on L and $\mathcal{D}$ is the subgroup generated by the diagonalizable reflections.

Recall from Section 1.7 that an element $g \in \mathcal{G}$ is called a reflection on L if the endomorphism $g_L - \mathrm{Id}_L \in \mathrm{End}_{\mathbb{Z}}(L)$ has rank 1; a reflection $g \in \mathcal{G}$ is called diagonalizable if g_L is conjugate in $\mathrm{GL}(L)$ to a diagonal matrix.

The term $\operatorname{Hom}(\mathcal{G}/\mathcal{R}, \mathrm{U}(\Bbbk))$ mimics the well-known class group formulas for polynomial invariants and for invariants under of finite group actions on local unique factorization domains (cf. Benson [14] and Singh [197], or [121]), while the term $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}})$ reflects the arithmetic restrictions inherent in the setting of multiplicative actions. Note that $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}}) \cong H^1(\mathcal{G}, L^{\mathcal{D}})$ via inflation.

The proof of Theorem 4.1.1 presented here is a simplified version of the author's original calculation in [121]. As all previous calculations of class groups of invariant rings, it is based on Samuel's method of Galois descent as developed in [187]. This material is reviewed in Section 4.4 after briefly recalling some basic facts pertaining to Krull domains, class groups, and ramification in Section 4.3.

4.2 Some Examples

The first example substantiates a remark made in Section 3.7.

Example 4.2.1. Let $\mathcal{G} = \mathcal{S}_2$ and $L = A_1 \oplus U_2$; see §1.3.3. So $L \cong \mathbb{Z}^3$ and the nonidentity element of $\mathcal{G}$ acts via the matrix $\left(\begin{array}{c|cc} -1 & & \\ \hline & & 1 \\ & 1 & \end{array}\right)$. Then $L^{\mathcal{G}} \cong \mathbb{Z}$ and $\overline{L} = L/L^{\mathcal{G}} \cong \mathbb{Z}^- \oplus \mathbb{Z}^-$. So $\mathbb{Z}[\overline{L}]^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[L^{\mathcal{G}}] \cong \mathbb{Z}[\overline{L}]^{\mathcal{G}}[t^{\pm 1}]$ is a Laurent polynomial algebra over $\mathbb{Z}[\overline{L}]^{\mathcal{G}}$. By Fossum [67, 8.1 and 7.3], the class group of $\mathbb{Z}[\overline{L}]^{\mathcal{G}}[t^{\pm 1}]$ is identical with $\mathrm{Cl}(\mathbb{Z}[\overline{L}]^{\mathcal{G}})$ which, by Theorem 4.1.1, evaluates to $\operatorname{Hom}(\mathcal{G}, \{\pm 1\}) \oplus H^1(\mathcal{G}, \overline{L}) = (\mathbb{Z}/2\mathbb{Z})^3$. On the other hand, Theorem 4.1.1 also gives $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{G}}) = \operatorname{Hom}(\mathcal{G}, \{\pm 1\}) \oplus H^1(\mathcal{G}, L) = (\mathbb{Z}/2\mathbb{Z})^2$. Therefore, $\mathbb{Z}[L]^{\mathcal{G}} \not\cong \mathbb{Z}[\overline{L}]^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[L^{\mathcal{G}}]$.

Next, we calculate the class group of the multiplicative invariant algebra of the root lattice A_{n-1} for the symmetric group $\mathcal{S}_n$. We use the notation of §1.3.3.

Example 4.2.2. For any Krull domain $\Bbbk$ and any $n > 2$,

$$\mathrm{Cl}(\Bbbk[A_{n-1}]^{\mathcal{S}_n}) \cong \mathrm{Cl}(\Bbbk) \oplus \mathbb{Z}/n\mathbb{Z} \; . \tag{4.1}$$

For $n = 2$, A_{n-1} is the sign lattice $\mathbb{Z}^-$ whose multiplicative invariant algebra is a polynomial algebra over $\Bbbk$ (see Example 3.5.6); so the class group is equal to $\mathrm{Cl}(\Bbbk)$ in this case. To prove (4.1), note that $\mathcal{R} = \mathcal{S}_n$ holds in Theorem 4.1.1. Indeed, an element $s \in \mathcal{S}_n$ is a reflection on A_{n-1} if and only if s is a reflection on U_n, and the latter holds precisely if s is a transposition. Furthermore, since any transposition s has fixed points for $n > 2$, Lemma 2.8.2 yields that $H^1(\langle s \rangle, A_{n-1})$ is trivial; so $\mathcal{D} = \{1\}$ holds in Theorem 4.1.1; see Section 1.7. Hence, $\mathrm{Cl}(\Bbbk[A_{n-1}]^{\mathcal{S}_n}) \cong \mathrm{Cl}(\Bbbk) \oplus H^1(\mathcal{S}_n, A_{n-1})$ and a second appeal to Lemma 2.8.2 proves (4.1). — This example is a special case of Proposition 6.3.1 below.

4.3 Krull Domains and Class Groups

Let R be a Krull domain with field of fractions F, and denote by $X^{(1)} = X^{(1)}(R)$ the set of height 1-primes of R. The localizations $R_{\mathfrak{P}}$ for $\mathfrak{P} \in X^{(1)}$ are discrete valuation domains with corresponding valuations $v_{\mathfrak{P}}\colon F^* \twoheadrightarrow \mathbb{Z}$. The class group $\mathrm{Cl}(R)$ of R is the quotient

$$\mathrm{Cl}(R) = \operatorname{Div} R / \operatorname{Prin} R\,,$$

where $\operatorname{Div} R$ denotes the free abelian group with basis $\{[\mathfrak{P}] \mid \mathfrak{P} \in X^{(1)}\}$ and $\operatorname{Prin} R$ is the subgroup of principal divisors $\operatorname{div}(x) = \sum_{\mathfrak{P}\in X^{(1)}} v_{\mathfrak{P}}(x)[\mathfrak{P}]$ for $x \in F^*$.

Now let $S \subseteq R$ be an inclusion of Krull domains. Then, for every $\mathfrak{p} \in X^{(1)}(S)$, there are at most finitely many $\mathfrak{P} \in X^{(1)}(R)$ satisfying $\mathfrak{P} \cap S = \mathfrak{p}$. As usual, we say that $\mathfrak{P}$ lies over $\mathfrak{p}$ in this case. We have $\mathfrak{p}R_{\mathfrak{P}} = \mathfrak{P}^e R_{\mathfrak{P}}$ for some $e = e(\mathfrak{P}/\mathfrak{p})$, called the ramification index of $\mathfrak{p}$ in $\mathfrak{P}$. Sending $[\mathfrak{p}] \mapsto \sum_{\mathfrak{P}} e(\mathfrak{P}/\mathfrak{p})[\mathfrak{P}]$, where $\mathfrak{P}$ runs over the height 1-primes of R lying over $\mathfrak{p}$, we obtain a homomorphism $\operatorname{Div} S \to \operatorname{Div} R$. If R is either integral over S or flat as S-module then this map passes down to a homomorphism of class groups $i\colon \mathrm{Cl}(S) \to \mathrm{Cl}(R)$; see Bourbaki [23, p. 18ff] or Fossum [67, p. 30ff].

We now specialize to the case where $S = R^{\mathcal{G}}$ is the ring of invariants of the action of a finite group $\mathcal{G}$ on the Krull domain R. Then $R^{\mathcal{G}}$ is a Krull domain as well (see, e.g., [67, p. 82]) and R is integral over $R^{\mathcal{G}}$. Thus, by the foregoing, we have a canonical map of class groups

$$i_{\mathcal{G}}\colon\ \mathrm{Cl}(R^{\mathcal{G}}) \longrightarrow \mathrm{Cl}(R)\,. \tag{4.2}$$

Moreover, for each height 1-prime $\mathfrak{p}$ of $R^{\mathcal{G}}$, the primes $\mathfrak{P}$ of R lying over $\mathfrak{p}$ form a single $\mathcal{G}$-orbit and all have height 1; cf. [22, Théorème V.2.2(i)] and Lemma 8.5.3(a) below. Hence, the ramification index $e(\mathfrak{P}/\mathfrak{p})$ is independent of $\mathfrak{P}$ and will therefore simply be denoted by $e(\mathfrak{p})$. Thus, the map $i_{\mathcal{G}}$ sends the class of $\mathfrak{p}$ to $e(\mathfrak{p})$ times the sum of the classes of all primes $\mathfrak{P}$ lying over $\mathfrak{p}$.

Returning to multiplicative actions now, we will use the notation and hypotheses of Theorem 4.1.1. The following lemma reduces the calculation of $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}})$ to the case where $\Bbbk$ is a field.

Lemma 4.3.1. *Let K denote the field of fractions of the Krull domain $\Bbbk$. Then $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \cong \mathrm{Cl}(\Bbbk) \oplus \mathrm{Cl}(K[L]^{\mathcal{G}})$.*

Proof. Since $\Bbbk[L]^{\mathcal{G}}$ is free over $\Bbbk$, by (3.4), the inclusion of Krull domains $\Bbbk \hookrightarrow \Bbbk[L]^{\mathcal{G}}$ give rise to a map of class groups $\mathrm{Cl}(\Bbbk) \to \mathrm{Cl}(\Bbbk[L]^{\mathcal{G}})$. The composite of this map with $i_{\mathcal{G}}\colon\ \mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \to \mathrm{Cl}(\Bbbk[L])$ is an isomorphism $\mathrm{Cl}(\Bbbk) \xrightarrow{\sim} \mathrm{Cl}(\Bbbk[L])$; see [67, 8.1 and 7.3]. Therefore, $\mathrm{Cl}(\Bbbk)$ injects as a direct summand into $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}})$. The image of $\mathrm{Cl}(\Bbbk)$ is generated by the classes of all primes of the form $\mathfrak{p} = p\Bbbk[L]^{\mathcal{G}}$, where p is a height 1-prime of $\Bbbk$; it follows from Proposition 3.3.1(b) that $\mathfrak{p}$ is indeed a prime of $\Bbbk[L]^{\mathcal{G}}$, clearly of height 1. On the other hand, by [67, 7.2], there is a canonical surjection $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \twoheadrightarrow \mathrm{Cl}(K[L]^{\mathcal{G}})$ whose kernel is generated by the very same $\mathfrak{p} = p\Bbbk[L]^{\mathcal{G}}$, whence the lemma. □

4.4 Samuel's Exact Sequence

As in Section 4.3, let R be any Krull domain and let $\mathcal{G}$ be a finite group acting by automorphisms on R. We assume, without essential loss, that the action of $\mathcal{G}$ on R is faithful.

There is a useful exact sequence, due to Samuel [187], that allows to compute the kernel of the map $i_{\mathcal{G}}$ in (4.2) in many instances:

$$0 \to \operatorname{Ker} i_{\mathcal{G}} \longrightarrow H^1(\mathcal{G}, \mathrm{U}(R)) \longrightarrow \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} \ . \tag{4.3}$$

Here, $\mathrm{U}(R)$ denotes the group of units of R and $\mathfrak{p}$ runs over the primes of height 1 in $R^{\mathcal{G}}$. Detailed proofs of (4.3) can be found in [67, pp. 82–83], [187, Chap. 1 §1], or [121]. The sequence ultimately is a consequence of Hilbert's "Theorem 90": $H^1(\mathcal{G}, F^*)$ is trivial for the field of fractions F of R.

The following application of (4.3) will be instrumental for the calculation of the class group of multiplicative invariants. We denote the inertia group of a prime $\mathfrak{P}$ of R by $I_{\mathcal{G}}(\mathfrak{P})$; so

$$I_{\mathcal{G}}(\mathfrak{P}) = \{g \in \mathcal{G} \mid g(r) - r \in \mathfrak{P} \text{ for all } r \in R\} \ . \tag{4.4}$$

Lemma 4.4.1. *Assume the finite group $\mathcal{G}$ acts faithfully on the unique factorization domain R. Assume further that, for all height 1-primes $\mathfrak{P}$ of R, the invariant subring $R^{I_{\mathcal{G}}(\mathfrak{P})}$ is a unique factorization domain. Then*

$$\mathrm{Cl}(R^{\mathcal{G}}) \cong \bigcap_{\mathfrak{P}} \operatorname{Ker}\left(\operatorname{res}^{\mathcal{G}}_{I_{\mathcal{G}}(\mathfrak{P})} \colon H^1(\mathcal{G}, \mathrm{U}(R)) \to H^1(I_{\mathcal{G}}(\mathfrak{P}), \mathrm{U}(R))\right) \ ,$$

where $\mathfrak{P}$ runs over the height 1-primes of R.

Proof. By hypothesis on R, we have $\mathrm{Cl}(R) = 0$; so sequence (4.3) takes the form

$$0 \to \mathrm{Cl}(R^{\mathcal{G}}) \longrightarrow H^1(\mathcal{G}, \mathrm{U}(R)) \longrightarrow \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} \ .$$

For each subgroup $\mathcal{H} \leq \mathcal{G}$, there is an analogous sequence and these sequences fit into a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Cl}(R^{\mathcal{G}}) \arrow[r] \arrow[d] & H^1(\mathcal{G}, \mathrm{U}(R)) \arrow[r] \arrow[d, "\operatorname{res}^{\mathcal{G}}_{\mathcal{H}}"] & \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} \arrow[d, "\rho^{\mathcal{G}}_{\mathcal{H}}"] \\
0 \arrow[r] & \mathrm{Cl}(R^{\mathcal{H}}) \arrow[r] & H^1(\mathcal{H}, \mathrm{U}(R)) \arrow[r] & \bigoplus_{\mathfrak{q}} \mathbb{Z}/e(\mathfrak{q})\mathbb{Z}
\end{tikzcd}$$

with $\mathfrak{p}$ and $\mathfrak{q}$ running over the height 1-primes of $R^{\mathcal{G}}$ and $R^{\mathcal{H}}$, respectively. The first vertical map is the canonical map coming from the (integral) extension of Krull domains $R^{\mathcal{G}} \subseteq R^{\mathcal{H}}$; see Section 4.3. The map $\rho^{\mathcal{G}}_{\mathcal{H}}$ sends the summand $\mathbb{Z}/e(\mathfrak{p})\mathbb{Z}$

"diagonally" to $\bigoplus_{\mathfrak{q}\colon\, \mathfrak{q}\cap R^{\mathcal{G}}=\mathfrak{p}} \mathbb{Z}/e(\mathfrak{q})\mathbb{Z}$. Note that each $e(\mathfrak{q})$ in this sum divides $e(\mathfrak{p})$; see [121, §1.4] for more details.

Now let $\mathcal{H} = I_{\mathcal{G}}(\mathfrak{P})$ be the inertia group of a height 1-prime $\mathfrak{P}$ of R. Then $\mathrm{Cl}(R^{\mathcal{H}}) = 0$, by hypothesis, and so $\mathrm{Cl}(R^{\mathcal{G}})$ embeds into $\mathrm{Ker}(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}})$. Hence, we have an embedding $\mathrm{Cl}(R^{\mathcal{G}}) \hookrightarrow \bigcap_{\mathcal{H}} \mathrm{Ker}(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}})$. In order to prove that this embedding is in fact an isomorphism, it suffices to show that $\bigcap_{\mathcal{H}} \mathrm{Ker}(\rho^{\mathcal{G}}_{\mathcal{H}}) = 0$. Starting with a height 1-prime $\mathfrak{p}$ of $R^{\mathcal{G}}$, choose a prime $\mathfrak{P}$ of R lying over $\mathfrak{p}$ and put $\mathcal{H} = I_{\mathcal{G}}(\mathfrak{P})$ and $\mathfrak{q} = \mathfrak{P} \cap R^{\mathcal{H}}$. Then $e(\mathfrak{p}) = e(\mathfrak{q})$; see, e.g., Serre [193, Chap. 1 §7]. Hence, the map $\rho^{\mathcal{G}}_{\mathcal{H}}$ is injective on the summand $\mathbb{Z}/e(\mathfrak{p})\mathbb{Z}$. Consequently, the product map $\{\rho^{\mathcal{G}}_{\mathcal{H}}\}$ is injective on all of $\bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z}$, as desired. □

4.5 Generalized Reflections on Rings

Let R denote a commutative ring and $\mathcal{G}$ a finite group acting by automorphisms on R. Following Gordeev and Kemper [76], we say that an element $g \in \mathcal{G}$ acts as a *k-reflection* on R if g belongs to the inertia group $I_{\mathcal{G}}(\mathfrak{P})$ of some prime ideal $\mathfrak{P} \in \operatorname{Spec} R$ with height $\mathfrak{P} \leq k$. As usual, the cases $k = 1$ and $k = 2$ will be referred to as *reflections* and *bireflections* on R, respectively. Define ideals $I_R(\mathcal{G})$ and $I_R(g)$ for each $g \in \mathcal{G}$ by

$$I_R(g) = \sum_{r\in R}(g(r) - r)R \tag{4.5}$$

and

$$I_R(\mathcal{G}) = \sum_{g\in\mathcal{G}} I_R(g) \tag{4.6}$$

Note that $I_R(g) = I_R(g^{-1})$ and $I_R(gg') \subseteq I_R(g) + I_R(g')$. Thus, it suffices to let g run over a set of generators of the group $\mathcal{G}$ in (4.6). Evidently, $g \in I_{\mathcal{G}}(\mathfrak{P})$ is equivalent to $\mathfrak{P} \supseteq I_R(g)$. Thus,

$$g \text{ is a } k\text{-reflection on } R \text{ if and only if height } I_R(g) \leq k. \tag{4.7}$$

We now specialize to the case of a multiplicative action of a finite group $\mathcal{G}$ on $R = \Bbbk[L]$, where L is a $\mathcal{G}$-lattice and $\Bbbk$ is some commutative base ring. In the next lemma, we determine the height of the ideal $I_{\Bbbk[L]}(\mathcal{G})$. For a cyclic group $\mathcal{G} = \langle g\rangle$, the lemma asserts that height $I_R(g) = \operatorname{rank}[g, L]$. Thus, g acts as a k-reflection on $\Bbbk[L]$ in the present sense if and only if g is a k-reflection on L in the sense of Section 1.7.

Recall that Tate cohomology group $\widehat{H}^{-1}(\mathcal{G}, L)$ has the form $\widehat{H}^{-1}(\mathcal{G}, L) = L(\mathcal{G})/[\mathcal{G}, L]$ with $L(\mathcal{G})$ and $[\mathcal{G}, L]$ as in (2.3).

Lemma 4.5.1. *With the above notation,*

$$\Bbbk[L]/I_{\Bbbk[L]}(\mathcal{G}) \cong \Bbbk[L/[\mathcal{G}, L]] \cong \Bbbk[\widehat{H}^{-1}(\mathcal{G}, L)][L/L(\mathcal{G})]\ ,$$

a Laurent polynomial ring over the group algebra $\Bbbk[\widehat{H}^{-1}(\mathcal{G}, L)]$. Moreover,

$$\text{height } I_{\Bbbk[L]}(\mathcal{G}) = \operatorname{rank}[\mathcal{G}, L] = \operatorname{rank} L - \operatorname{rank} L^{\mathcal{G}}\ .$$

Proof. Put $I = I_{\Bbbk[L]}(\mathcal{G})$ and note that an alternative set of generators of I is given by the elements $\mathbf{x}^{g(m)-m} - 1$ with $m \in L$ and $g \in \mathcal{G}$. This explains the isomorphism $\Bbbk[L]/I \cong \Bbbk[L/[\mathcal{G}, L]]$. Since $L/[\mathcal{G}, L] \cong \widehat{H}^{-1}(\mathcal{G}, L) \oplus L/L(\mathcal{G})$, the isomorphism $\Bbbk[L/[\mathcal{G}, L]] \cong \Bbbk[\widehat{H}^{-1}(\mathcal{G}, L)][L/L(\mathcal{G})]$ also follows.

The rational group algebra of $\mathcal{G}$ decomposes as

$$\mathbb{Q}[\mathcal{G}] = \mathbb{Q}\sum_{g\in\mathcal{G}} g \oplus \sum_{g\in\mathcal{G}} \mathbb{Q}(g-1) .$$

This implies $L \otimes_{\mathbb{Z}} \mathbb{Q} = \big(L^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Q}\big) \oplus ([\mathcal{G}, L] \otimes_{\mathbb{Z}} \mathbb{Q})$, and hence $\operatorname{rank} L = \operatorname{rank} L^{\mathcal{G}} + \operatorname{rank}[\mathcal{G}, L]$.

We now show that, for any minimal covering prime $\mathfrak{P}$ of I, we have

$$\operatorname{height} \mathfrak{P} = \operatorname{rank}[\mathcal{G}, L] .$$

Put $A = L/[\mathcal{G}, L]$ and $\overline{\mathfrak{P}} = \mathfrak{P}/I$, a minimal prime of $\Bbbk[L]/I = \Bbbk[A]$. Further, put $\mathfrak{p} = \overline{\mathfrak{P}} \cap \Bbbk = \mathfrak{P} \cap \Bbbk$. Since the extension $\Bbbk \hookrightarrow \Bbbk[A] = \Bbbk[L]/I$ is free, $\mathfrak{p}$ is a minimal prime of $\Bbbk$; see [28, Cor. to Prop. VIII.2.2]. Hence, descending chains of primes in $\Bbbk[L]$ starting with $\mathfrak{P}$ correspond in a 1-to-1 fashion to descending chains of primes of $Q(\Bbbk/\mathfrak{p})[L]$ starting with the prime that is generated by $\mathfrak{P}$. Thus, replacing $\Bbbk$ by $Q(\Bbbk/\mathfrak{p})$, we may assume that $\Bbbk$ is a field. But then

$$\operatorname{height} \mathfrak{P} = \dim \Bbbk[L] - \dim \Bbbk[L]/\mathfrak{P} = \operatorname{rank} L - \dim \Bbbk[L]/\mathfrak{P} .$$

Let $\overline{\mathfrak{P}}_0 = \overline{\mathfrak{P}} \cap \Bbbk[A_0]$, where $A_0 \cong \widehat{H}^{-1}(\mathcal{G}, L)$ denotes the torsion subgroup of A. Since primes of $\Bbbk[A_0]$ generate primes in $\Bbbk[A]$, we have $\overline{\mathfrak{P}} = \overline{\mathfrak{P}}_0 \Bbbk[A]$ and so $\Bbbk[L]/\mathfrak{P} \cong \Bbbk_0[A/A_0]$, where $\Bbbk_0 = \Bbbk[A_0]/\overline{\mathfrak{P}}_0$ is a field. Thus, $\dim \Bbbk[L]/\mathfrak{P} = \operatorname{rank} A/A_0$. Finally, $\operatorname{rank} A/A_0 = \operatorname{rank} A = \operatorname{rank} L - \operatorname{rank}[\mathcal{G}, L]$, which completes the proof. □

We now concentrate on reflections and height 1-primes. In the following lemma, we assume the hypotheses of Theorem 4.1.1.

Lemma 4.5.2. *The nonidentity inertia groups $I_{\mathcal{G}}(\mathfrak{P})$ of height 1-primes $\mathfrak{P}$ of $\Bbbk[L]$ are exactly the subgroups of $\mathcal{G}$ that are generated by a nonidentity reflection on L. For each reflection $1 \neq g \in \mathcal{G}$, the ring of multiplicative invariants has the form*

$$\Bbbk[L]^{\langle g\rangle} \cong \Bbbk[\mathbb{Z}^{n-1} \oplus \mathbb{Z}_+] ,$$

where $n = \operatorname{rank} L$. In particular, $\operatorname{Cl}(\Bbbk[L]^{\langle g\rangle}) = \operatorname{Cl}(\Bbbk)$.

Proof. Let $\mathcal{H} = I_{\mathcal{G}}(\mathfrak{P})$ be a nonidentity inertia group of some height 1-prime $\mathfrak{P}$ of $\Bbbk[L]$. Since $I_{\Bbbk[L]}(\mathcal{H}) \subseteq \mathfrak{P}$ and $\mathfrak{P}$ has height 1, it follows from Lemma 4.5.1 that $[\mathcal{H}, L]$ has rank 1. Hence, all elements $1 \neq g \in \mathcal{H}$ are reflections; in particular, they have determinant -1. Thus, $\mathcal{H} \cap \operatorname{SL}(L) = \{1\}$ and so $\mathcal{H}$ has order 2, with generator a single reflection.

Conversely, let $1 \neq g \in \mathcal{G}$ be a reflection and put $\mathcal{H} = \langle g\rangle$. Then $[\mathcal{H}, L] = [g, L]$ has rank 1, and hence $\operatorname{height} I(\mathcal{H}) = 1$, by Lemma 4.5.1. Therefore, $\mathcal{H} \subseteq I_{\mathcal{G}}(\mathfrak{P})$

for some height 1-prime $\mathfrak{P}$ of $\Bbbk[L]$, and the first paragraph of the proof implies that $I_{\mathcal{G}}(\mathfrak{P}) = \mathcal{H}$.

In order to determine the algebra of invariants $\Bbbk[L]^{\langle g\rangle}$ for a reflection $1 \neq g \in \mathcal{G}$, identify the group $\langle g\rangle$ with $\mathcal{S}_2$ and recall from §1.7.1 that the $\langle g\rangle$-lattice L is either isomorphic to $\mathbb{Z}^{n-1} \oplus A_1$ or to $\mathbb{Z}^{n-2} \oplus U_2$. In either case, $\Bbbk[L]^{\langle g\rangle}$ is isomorphic to $\Bbbk[\mathbb{Z}^{n-1} \oplus \mathbb{Z}_+]$; see Examples 3.5.5 and 3.5.6. The formula $\mathrm{Cl}(\Bbbk[L]^{\langle g\rangle}) = \mathrm{Cl}(\Bbbk)$ now follows from Fossum [67, 8.1 and 7.3]. □

4.6 Proof of Theorem 4.1.1

First, by Lemma 4.3.1, we may replace $\Bbbk$ by its field of fractions K. Note that $\mathrm{Hom}(\mathcal{G}, K^*) = \mathrm{Hom}(\mathcal{G}, \mathrm{U}(\Bbbk))$, since $\Bbbk$ is integrally closed. Thus, in the following, we assume that $\Bbbk$ is a field. In particular $\Bbbk[L]$ is a unique factorization domain and so are all invariant subalgebras $\Bbbk[L]^{I_{\mathcal{G}}(\mathfrak{P})}$ for height 1-primes $\mathfrak{P}$ of $\Bbbk[L]$, by Lemma 4.5.2. Therefore, Lemma 4.4.1 applies and, in view of Lemma 4.5.2, we obtain the formula

$$\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \cong \bigcap_{\mathcal{H}} \mathrm{Ker}\left(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}\colon H^1(\mathcal{G}, \mathrm{U}(\Bbbk[L])) \longrightarrow H^1(\mathcal{H}, \mathrm{U}(\Bbbk[L]))\right) , \tag{4.8}$$

where $\mathcal{H}$ runs over the subgroups of $\mathcal{G}$ that are generated by a nonidentity reflection. To evaluate this expression, recall from Lemma 3.4.1 that $\mathrm{U}(\Bbbk[L]) = \Bbbk^* \times \underline{L}$; so $H^1(\mathcal{G}, \mathrm{U}(\Bbbk[L])) = \mathrm{Hom}(\mathcal{G}, \Bbbk^*) \oplus H^1(\mathcal{G}, L)$ and similarly for all subgroups $\mathcal{H}$. The right hand side of (4.8) is the direct sum of the terms

$$\bigcap_{\mathcal{H}} \mathrm{Ker}\left(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}\colon \ \mathrm{Hom}(\mathcal{G}, \Bbbk^*) \longrightarrow \mathrm{Hom}(\mathcal{H}, \Bbbk^*)\right) \tag{4.9}$$

and

$$\bigcap_{\mathcal{H}} \mathrm{Ker}\left(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}\colon H^1(\mathcal{G}, L)) \longrightarrow H^1(\mathcal{H}, L))\right) . \tag{4.10}$$

The intersection (4.9) can be identified with $\mathrm{Hom}(\mathcal{G}/\mathcal{R}, \Bbbk^*)$, where $\mathcal{R}$ is the subgroup of $\mathcal{G}$ that is generated by all reflections. In (4.10), it suffices to let $\mathcal{H}$ run over the subgroups of $\mathcal{G}$ that are generated by a diagonalizable reflection, because $H^1(\mathcal{H}, L)$ is trivial otherwise. Therefore, letting $\mathcal{D} = \langle d_1\rangle \times \ldots \times \langle d_r\rangle$ denote the subgroup of $\mathcal{G}$ that is generated by all diagonalizable reflections d_i, as in Lemma 1.7.2, the intersection (4.10) is the kernel of the composite map

$$H^1(\mathcal{G}, L) \xrightarrow{\mathrm{res}^{\mathcal{G}}_{\mathcal{D}}} H^1(\mathcal{D}, L) \xrightarrow{\mathrm{res}} \prod_{i=1}^{r} H^1(\langle d_i\rangle, L) ,$$

where $\mathrm{res} = \{\mathrm{res}^{\mathcal{G}}_{\langle\, d_i\rangle}\}$ is the product of the restrictions. But Lemma 1.7.2 easily implies that both $H^1(\mathcal{D}, L)$ and $\prod_{i=1}^{r} H^1(\langle d_i\rangle, L)$ are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ and res is in fact an isomorphism. So (4.10) is equal to $\mathrm{Ker}(\mathrm{res}^{\mathcal{G}}_{\mathcal{D}})$, and the latter is isomorphic to $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}})$ via inflation; see, e.g., [193, Chap. VII, Prop. 4]. This completes the proof of Theorem 4.1.1. □

5

Picard Group

5.1 Introduction

The *Picard group* of a commutative ring R, denoted $\operatorname{Pic} R$, is the set of isomorphism classes of invertible R-modules; see Section 5.2 below for details. If R is a Krull domain then $\operatorname{Pic}(R)$ embeds into the class group $\operatorname{Cl}(R)$. This embedding is an isomorphism if R is regular. $\operatorname{Pic}(\,.\,)$ defines a functor from commutative rings to abelian groups. In particular, if G is a group acting by automorphisms on R and R^G is the subring of G-invariants then the inclusion $R^G \hookrightarrow R$ yields a canonical homomorphism

$$j_G \colon \operatorname{Pic}(R^G) \longrightarrow \operatorname{Pic}(R)\ . \tag{5.1}$$

In this chapter, we determine the kernel of this map in the case of a multiplicative action of a finite group $\mathcal{G}$; so $R = \Bbbk[L]$ is the group algebra of a $\mathcal{G}$-lattice L over the commutative ring $\Bbbk$. The structure of the Picard group $\operatorname{Pic}(\Bbbk[L])$ is quite involved in general; see Weibel [223]. However, when $\Bbbk$ is an integrally closed domain then the embedding $\Bbbk \hookrightarrow \Bbbk[L]$ yields an isomorphism $\operatorname{Pic}(\Bbbk) \xrightarrow{\sim} \operatorname{Pic}(\Bbbk[L])$ by Bass and Murthy [6, 5.10]; see also [223, 1.5.2]. Moreover, since the augmentation map $\varepsilon \colon \Bbbk[L]^{\mathcal{G}} \to \Bbbk$ (see 3.9) is the identity on $\Bbbk$, we know that $\operatorname{Pic}(\Bbbk)$ is always a direct summand of $\operatorname{Pic}(\Bbbk[L]^{\mathcal{G}})$. Thus, if $\Bbbk$ is an integrally closed domain, then

$$\operatorname{Pic}(\Bbbk[L]^{\mathcal{G}}) = \operatorname{Pic}(\Bbbk) \oplus \operatorname{Ker} j_{\mathcal{G}}\ . \tag{5.2}$$

To compute $\operatorname{Ker} j_{\mathcal{G}}$, we recall the definition

$$\text{Ш}^1(\mathcal{G}, L) = \bigcap_{g \in \mathcal{G}} \operatorname{Ker}\Big(\operatorname{res}^{\mathcal{G}}_{\langle g \rangle} \colon H^1(\mathcal{G}, L) \longrightarrow H^1(\langle g \rangle, L)\Big) \tag{5.3}$$

from Section 2.9. The result then reads as follows:

Theorem 5.1.1. *Let L be a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and let $\Bbbk$ be a commutative domain with $|\mathcal{G}|^{-1} \in \Bbbk$. Then* $\operatorname{Ker} j_{\mathcal{G}} \cong \text{Ш}^1(\mathcal{G}, L)$. *In particular, if $\Bbbk$ is also integrally closed then* $\operatorname{Pic}(\Bbbk[L]^{\mathcal{G}}) \cong \operatorname{Pic}(\Bbbk) \oplus \text{Ш}^1(\mathcal{G}, L)$.

The kernel of the restriction map $\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}\colon H^1(\mathcal{G},L) \longrightarrow H^1(\mathcal{H},L)$, for any subgroup $\mathcal{H} \leq \mathcal{G}$, has the following simple description. Let n be any multiple of $|\mathcal{G}|$ and let $\overline{} = (\,.\,) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ denote reduction mod n. The exact sequence of $\mathcal{G}$-modules $0 \to L \xrightarrow{\cdot n} L \longrightarrow \overline{L} \to 0$ gives rise to the cohomology sequence

$$L^{\mathcal{G}} \xrightarrow{\overline{}} \overline{L}^{\mathcal{G}} \longrightarrow H^1(\mathcal{G},L) \xrightarrow{\cdot n=0} H^1(\mathcal{G},L)\;.$$

Therefore, $H^1(\mathcal{G},L) \cong \overline{L}^{\mathcal{G}}/\overline{L^{\mathcal{G}}}$ and similarly for $\mathcal{H}$. In terms of these isomorphisms, $\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}$ is the canonical map $\overline{L}^{\mathcal{G}}/\overline{L^{\mathcal{G}}} \to \overline{L}^{\mathcal{H}}/\overline{L^{\mathcal{H}}}$ coming from the inclusions $\overline{L}^{\mathcal{G}} \subseteq \overline{L}^{\mathcal{H}}$ and $\overline{L^{\mathcal{G}}} \subseteq \overline{L^{\mathcal{H}}}$. Therefore,

$$\operatorname{Ker}\left(\mathrm{res}^{\mathcal{G}}_{\mathcal{H}}\right) \cong \overline{L^{\mathcal{H}}}/\overline{L^{\mathcal{G}}}\;. \tag{5.4}$$

We further remark that, letting $g \in \mathcal{G}$ in (5.3) run over the reflections on L only, the resulting intersection is isomorphic to $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}})$ in the notation of Theorem 4.1.1; see the computation of the term (4.10) in Section 4.6. Thus, $\text{Ш}^1(\mathcal{G},L)$ embeds into $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}})$.

5.1.1 Experiments

The group $\text{Ш}^1(\mathcal{G},L)$ is trivial for all $\mathcal{G}$-lattices L of rank 2. Indeed, $\mathrm{SL}_2(\mathbb{Z})$ acts fixed point freely on $L = \mathbb{Z}^2$; so $L^{\langle g\rangle} = 0$ holds for every $1 \neq g \in \mathrm{SL}_2(\mathbb{Z})$. Therefore, (5.4) shows that $\text{Ш}^1(\mathcal{G},L) = 0$ if $\mathcal{G}$ intersects $\mathrm{SL}_2(\mathbb{Z})$ nontrivially. In the opposite case, $\mathcal{G}$ is cyclic, having order at most 2, and so $\text{Ш}^1(\mathcal{G},L) = 0$ again.

A search of the crystallographic groups library "crystcat" of GAP [71] yields that among the 73 conjugacy classes of finite subgroups of $\mathcal{G} \leq \mathrm{GL}_3(\mathbb{Z})$, exactly 2 lead to a nontrivial $\text{Ш}^1(\mathcal{G},L)$. They are represented by two subgroups of $\mathcal{S}_4$ acting on the root lattice A_3, namely the alternating group $\mathcal{A}_4$ and its Sylow 2-subgroup $\cong \mathcal{C}_2 \times \mathcal{C}_2$; see also Colliot-Thélène and Sansuc [42, p. 201-202] for the latter group. In both cases, $\text{Ш}^1(\mathcal{G},A_3)$ has order 2. The 710 conjugacy classes of finite subgroups of $\mathrm{GL}_4(\mathbb{Z})$ altogether yield 9 with nontrivial $\text{Ш}^1(\mathcal{G},L)$, of order 2 in all cases. The above two groups $\mathcal{G} = \mathcal{A}_4$ and $\mathcal{G} = \mathcal{C}_2 \times \mathcal{C}_2$ in rank 3 account for 4 of these 9 cases: $\left({}^{\mathcal{G}}\;{}_{1}\right)$ and $\left({}^{\mathcal{G}}\;{}_{\pm 1}\right)$.

By contrast, the Picard group for algebras of polynomial invariants over a field is always trivial as has been shown by Kang [104, Theorem 2.4]; see also Example 5.5.2 below.

5.2 Invertible Modules

Let R be any commutative ring. An R-module P is called *invertible* (or an algebraic line bundle) if the following equivalent conditions are satisfied; see, e.g., Bass [5, p. 132]:

(a) $P \otimes_R Q \cong R$ for some R-module Q;

(b) P is finitely generated projective of constant rank 1, that is, $P_{\mathfrak{P}} \cong R_{\mathfrak{P}}$ holds for all primes $\mathfrak{P}$ of R;

(c) P is finitely generated projective and $\mathrm{End}_R(P) = R$.

The Picard group of R, written $\mathrm{Pic}(R)$, is the set of isomorphism classes of all invertible R-modules. Denoting the isomorphism class of P by $[P]$, one defines a multiplication in $\mathrm{Pic}(R)$ by $[P][P'] = [P \otimes_R P']$. This makes $\mathrm{Pic}(R)$ an abelian group with identity element $[R]$; the inverse of $[P]$ in $\mathrm{Pic}(R)$ is $[P^*]$, where $P^* = \mathrm{Hom}_R(P, R)$ is the dual of P.

The group $\mathrm{Pic}(\,.\,)$ is functorial: if $S \to R$ is a homomorphism of commutative rings and Q is an invertible S-module then $P = R \otimes_S Q$ is an invertible R-module and $[Q] \mapsto [P]$ gives a group homomorphism $\mathrm{Pic}(S) \to \mathrm{Pic}(R)$. The map j_G of (5.1) arises in this way from the embedding $R^G \hookrightarrow R$.

5.3 The Skew Group Ring

We continue to let R denote a commutative ring. Further, let G be an arbitrary group acting by automorphisms on R, written $r \mapsto g(r)$, and let R^G denote the subring of G-invariants of R. The *skew group ring* of G over R, denoted by

$$R\#G\,,$$

is an associative ring containing R as a subring and G as a subgroup of $\mathrm{U}(R\#G)$, the group of units of $R\#G$. The elements of G form a free basis of $R\#G$ as left R-module. Multiplication in $R\#G$ is based on the rule $(rg)(r'g') = rg(r')gg'$ for $r, r' \in R$ and $g, g' \in G$. The ring R becomes an $(R\#G, R^{\mathcal{G}})$-bimodule via

$$rg \cdot r' \cdot s = rg(r')s \qquad (r, r' \in R,\ s \in R^{\mathcal{G}},\ g \in G)\,.$$

The left $R\#G$-module structure on R defined by this rule will be called "canonical". The endomorphism ring of the canonical $R\#G$-module has the form

$$\mathrm{End}_{R\#G}(R) \cong R^G\,; \tag{5.5}$$

an explicit isomorphism is given by $f \mapsto f(1)$. If ${}_{R\#G}V$ and ${}_{R\#G}W$ are two $R\#G$-modules then $V \otimes_R W$ becomes an $R\#G$-module by letting R act as usual and G diagonally: $g(v \otimes w) = gv \otimes gw$. Similarly, $\mathrm{Hom}_R(V, W)$ becomes an $R\#G$-module by letting R act as usual and G via $(gf)(v) = gf(g^{-1}v)$. Note that the $R\#G$-homomorphisms coincide with the G-invariants under this action: $\mathrm{Hom}_{R\#G}(V, W) = \mathrm{Hom}_R(V, W)^G$.

Lemma 5.3.1. *The group $H^1(G, \mathrm{U}(R))$ classifies the isomorphism classes of left $R\#G$-module structures on R that extend the regular R-module structure. The multiplication in $H^1(G, \mathrm{U}(R))$ corresponds to $\otimes_R$ and the identity element of $H^1(G, \mathrm{U}(R))$ corresponds to the canonical $R\#G$-module.*

Proof. Let $d\colon \mathcal{G} \to \mathrm{U}(R)$ be a cocycle; so $d(gg') = d(g)g(d(g'))$ holds for all $g, g' \in G$. Define R_d to be R with $R\#G$-action

$$rg \cdot r' = rd(g)g(r')$$

for $r, r' \in R$, $g \in G$. Then R_d is an $R\#G$-module whose restriction to R is the regular R-module. For any two cocycles d_1, d_2, multiplication in R gives an isomorphism $R_{d_1} \otimes_R R_{d_2} \cong R_{d_1 d_2}$. Moreover, R_d is isomorphic to the canonical module ${}_{R\#G}R$ if and only if there is a G-equivariant R-isomorphism $R_d \xrightarrow{\sim} R$. The latter is given by a unit $u \in \mathrm{U}(R)$, and G-equivariance translates into $d(g) = g(u)u^{-1}$ for all $g \in G$. Thus, $R_d \cong_{R\#G} R$ precisely if the cocycle d is principal. Finally, if $\cdot$ is any $R\#G$-module action on R extending the regular R-action then $d(g) = g \cdot 1$ $(g \in G)$ yields a cocycle $d\colon G \to \mathrm{U}(R)$ so that R, with the given $R\#G$-module structure, equals R_d. □

5.4 The Trace Map

Retaining the notation of Section 5.3, we now consider the situation where the acting group is finite; it will be denoted by $\mathcal{G}$. Then we can define the *trace map* (sometimes also called *transfer map*) of the action of $\mathcal{G}$ on R by

$$\mathrm{tr}_{\mathcal{G}}\colon R \longrightarrow R^{\mathcal{G}} , \quad r \mapsto \sum_{g \in \mathcal{G}} g(r) .$$

We will often work under the hypothesis that the trace map is surjective or, equivalently, $\mathrm{tr}_{\mathcal{G}}(r) = 1$ for some $r \in R$. This hypothesis is easily checked if R is a an algebra over some commutative ring $\Bbbk \subseteq R^{\mathcal{G}}$ such that there is an augmentation map $\varepsilon\colon R \to \Bbbk$ satisfying $\varepsilon(g(r)) = \varepsilon(r)$ for all $g \in \mathcal{G}$ and $r \in R$. In this case,

$$\mathrm{tr}_{\mathcal{G}} \text{ is surjective if and only if } |\mathcal{G}|^{-1} \in \Bbbk. \tag{5.6}$$

To see this, observe that $\varepsilon(\mathrm{tr}_{\mathcal{G}}(r)) = |\mathcal{G}|\varepsilon(r)$ holds for all $r \in R$, by hypothesis on ε. Hence, $\mathrm{tr}_{\mathcal{G}}(r) = 1$ implies that $|\mathcal{G}|^{-1} \in \Bbbk$. Conversely, if $|\mathcal{G}|^{-1} \in \Bbbk$ then $f = |\mathcal{G}|^{-1}$ satisfies $\mathrm{tr}_{\mathcal{G}}(f) = 1$. This observation covers the case of multiplicative actions, using the augmentation of Section 3.9, as well as the case of linear actions on polynomial algebras, using evaluation of polynomials at 0.

Returning to general commutative rings R, note that $\mathrm{tr}_{\mathcal{G}}(r) = t \cdot r$, where $t = \sum_{g \in \mathcal{G}} g \in R\#\mathcal{G}$ is the “symmetrizer” element. We define $\mathfrak{G}$ to be the ideal of the skew group ring $R\#\mathcal{G}$ that is generated by t,

$$\mathfrak{G} = R\#\mathcal{G}tR\#\mathcal{G} = RtR . \tag{5.7}$$

Here, the second equality holds because $g \cdot t = t = t \cdot g$ for all $g \in \mathcal{G}$.

Finally, (.)-proj will denote the category of finitely generated (= f.g.) projective modules over the ring in question.

Lemma 5.4.1. *Assume that the trace map $\mathrm{tr}_{\mathcal{G}}$ is surjective. Then:*

(a) *An $R\#\mathcal{G}$-module ${}_{R\#\mathcal{G}}V$ is (f.g.) projective if and only if the restriction ${}_RV$ is (f.g.) projective.*

(b) *Let A denote the full subcategory of $R\#\mathcal{G}$-proj consisting of all P satisfying $\mathfrak{G}P = P$. Then the functor ${}_{R\#\mathcal{G}}R \otimes_{R^{\mathcal{G}}} (\,.\,)$ and the functor $(\,.\,)^{\mathcal{G}}$ of $\mathcal{G}$-invariants yield an equivalence of categories $R^{\mathcal{G}}$-$\mathsf{proj} \approx \mathsf{A}$.*

Proof. (a) Since $R\#\mathcal{G}$ is finite over R, ${}_{R\#\mathcal{G}}V$ is finitely generated iff ${}_RV$ is. Also, if ${}_{R\#\mathcal{G}}V$ is projective then ${}_RV$ is projective as well, because $R\#\mathcal{G}$ is free over R. Conversely, assume that V is projective as R-module. Fix an $R\#\mathcal{G}$-epimorphism $\pi\colon F \twoheadrightarrow V$, where F is a free $R\#\mathcal{G}$-module. Then there is an R-splitting $\sigma \in \mathrm{Hom}_R(V,F)$ with $\pi\sigma = \mathrm{Id}_V$. By hypothesis, there is an element $x \in R$ with $\mathrm{tr}_{\mathcal{G}}(x) = 1$. View $\mathrm{Hom}_R(V,F)$ as $R\#\mathcal{G}$-module as in Section 5.3 and put $\sigma' = e\sigma$ with $e = tx \in R\#\mathcal{G}$. Then $\sigma' \in \mathrm{Hom}_R(V,F)^{\mathcal{G}}$ and it is straightforward to verify that $\pi\sigma' = \mathrm{Id}_V$. Thus, V is an $R\#\mathcal{G}$-direct summand of F.

(b) The canonical $R\#\mathcal{G}$-module ${}_{R\#\mathcal{G}}R$ is projective by (a). Let $\mathsf{add}({}_{R\#\mathcal{G}}R)$ denote the full subcategory of $R\#\mathcal{G}$-proj consisting of all f.g. $R\#\mathcal{G}$-modules that are isomorphic to a direct summand of some direct sum of copies of ${}_{R\#\mathcal{G}}R$. We first show that $\mathsf{A} = \mathsf{add}({}_{R\#\mathcal{G}}R)$. Fixing $x \in R$ with $\mathrm{tr}_{\mathcal{G}}(x) = 1$, as in (a), we have $t \cdot x = 1$ in ${}_{R\#\mathcal{G}}R$. So ${}_{R\#\mathcal{G}}R$ belongs to A, and hence so does every member of $\mathsf{add}({}_{R\#\mathcal{G}}R)$. Conversely, any P in A satisfies $P = \mathfrak{G}P = RtP$. Since $Rt \cong_{R\#\mathcal{G}} R$ as $R\#\mathcal{G}$-modules, a suitable direct sum of copies of ${}_{R\#\mathcal{G}}R$ maps onto P and this map splits, because P is projective. Thus, P belongs to $\mathsf{add}({}_{R\#\mathcal{G}}R)$.

Now consider the functors $E = {}_{R\#\mathcal{G}}R \otimes_{R^{\mathcal{G}}} (\,.\,)\colon R^{\mathcal{G}}$-$\mathsf{proj} \longrightarrow \mathsf{add}({}_{R\#\mathcal{G}}R)$ and $F = (\,.\,)^{\mathcal{G}}\colon \mathsf{add}({}_{R\#\mathcal{G}}R) \longrightarrow R^{\mathcal{G}}$-$\mathsf{proj}$. For Q in $R^{\mathcal{G}}$-proj, let

$$\varphi_Q : Q \to (F \circ E)(Q) = ({}_{R\#\mathcal{G}}R \otimes_{R^{\mathcal{G}}} Q)^{\mathcal{G}}$$

denote the $R^{\mathcal{G}}$-linear map given by $\varphi_Q(q) = 1 \otimes q$. Then

$$\varphi_{R^{\mathcal{G}}} : R^{\mathcal{G}} \to \left({}_{R\#\mathcal{G}}R \otimes_{R^{\mathcal{G}}} R^{\mathcal{G}}\right)^{\mathcal{G}}$$

is an isomorphism, and hence so is $\varphi_{(R^{\mathcal{G}})^n}$ for every n and φ_Q for every Q in $R^{\mathcal{G}}$-proj. Thus φ is a natural equivalence of functors $\mathrm{Id}_{R^{\mathcal{G}}\text{-}\mathsf{proj}} \cong F \circ E$. Similarly, defining $\psi_P : (E \circ F)(P) = {}_{R\#\mathcal{G}}R \otimes_{R^{\mathcal{G}}} (P^{\mathcal{G}}) \to P$ for P in $\mathsf{add}({}_{R\#\mathcal{G}}R)$ by $\psi_P(r \otimes p) = rp$, we obtain a natural equivalence of functors $E \circ F \cong \mathrm{Id}_{\mathsf{add}({}_{R\#\mathcal{G}}R)}$. This proves the category equivalence $R^{\mathcal{G}}$-$\mathsf{proj} \approx \mathsf{add}({}_{R\#\mathcal{G}}R) = \mathsf{A}$. □

5.5 The Kernel of the Map $\mathrm{Pic}(R^G) \to \mathrm{Pic}(R)$

We now turn to the kernel of the map $j_G\colon \mathrm{Pic}(R^G) \to \mathrm{Pic}(R)$ in (5.1). For each prime ideal $\mathfrak{P}$ of R, let $I_G(\mathfrak{P})$ denote the inertia group in G (see (4.4)) and define

$$\rho_{\mathfrak{P}}\colon H^1(G,\mathrm{U}(R)) \longrightarrow H^1(I_G(\mathfrak{P}),\mathrm{U}(R/\mathfrak{P})) = \mathrm{Hom}(I_G(\mathfrak{P}),\mathrm{U}(R/\mathfrak{P})) \quad (5.8)$$

via restriction $\operatorname{res}^G_{I_G(\mathfrak{P})}\colon H^1(G,\mathrm{U}(R)) \longrightarrow H^1(I_G(\mathfrak{P}),\mathrm{U}(R))$ and the canonical map $\mathrm{U}(R)\to\mathrm{U}(R/\mathfrak{P})$. Then we have the following description of $\operatorname{Ker} j_G$ implicit in [123].

Proposition 5.5.1. *Let R be a commutative ring and G a group acting by automorphisms on R. Then the kernel of $j_G\colon \operatorname{Pic}(R^G)\to\operatorname{Pic}(R)$ embeds into*

$$\bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}}\ ,$$

where $\mathfrak{P}$ runs over the primes of R. For the action of a finite group $\mathcal{G}$ such that the trace map $\operatorname{tr}_{\mathcal{G}}$ is surjective, this embedding is an isomorphism.

Proof. Let $[Q]\in\operatorname{Ker} j_G$; so there is an isomorphism of R-modules

$$\varphi\colon R\otimes_{R^G} Q \xrightarrow{\sim} R\,.$$

Now $R\otimes_{R^G} Q$ is also a left $R\#G$-module via the $(R\#G,R^G)$-bimodule structure on R; see Section 5.3. Thus, the isomorphism φ defines an $R\#G$-module structure on R extending the regular R-module structure. By Lemma 5.3.1, this yields an element $[d_Q]\in H^1(G,\mathrm{U}(R))$.

For simplicity, let $S(\mathfrak{P})$ denote the skew group ring $S(\mathfrak{P})=(R/\mathfrak{P})\#I_G(\mathfrak{P})$; this is actually an ordinary group ring, since $I_G(\mathfrak{P})$ acts trivially on $R/\mathfrak{P}$. The element $\rho_{\mathfrak{P}}([d_Q])\in H^1(I_G(\mathfrak{P}),\mathrm{U}(R/\mathfrak{P}))$ corresponds to the $S(\mathfrak{P})$-module structure on $R/\mathfrak{P}$ afforded by

$$(R/\mathfrak{P})\otimes_R\varphi\colon\ (R/\mathfrak{P})\otimes_{R^G} Q\cong(R\otimes_{R^G} Q)/\mathfrak{P}(R\otimes_{R^G} Q)\xrightarrow{\sim} R/\mathfrak{P}\,.$$

Since $I_G(\mathfrak{P})$ acts trivially on $(R/\mathfrak{P})\otimes_{R^G} Q$, the $I_G(\mathfrak{P})$-action on $\mathcal{R}/\mathfrak{P}$ on the right is also trivial; so the $S(\mathfrak{P})$-module structure on $R/\mathfrak{P}$ obtained from $(R/\mathfrak{P})\otimes_R\varphi$ is the canonical one. By Lemma 5.3.1, this translates into $\rho_{\mathfrak{P}}([d_Q])$ being the identity element of $H^1(I_G(\mathfrak{P}),\mathrm{U}(R/\mathfrak{P}))$. Thus, $[d_Q]$ belongs to $\operatorname{Ker}\rho_{\mathfrak{P}}$ and we obtain a map

$$\delta\colon\ \operatorname{Ker} j_G\longrightarrow\bigcap_{\mathfrak{P}}\operatorname{Ker}\rho_{\mathfrak{P}}\ ,\qquad [Q]\mapsto[d_Q]\,.$$

This map is easily seen to be multiplicative. To check that δ is injective, suppose that $[d_Q]=1\in H^1(G,\mathrm{U}(R))$; so $R\otimes_{R^G} Q\xrightarrow{\sim}_{R\#G} R$, the canonical $R\#G$-module. Then $\operatorname{Hom}_{R\#G}(R,R\otimes_{R^G} Q)\cong\operatorname{End}_{R\#G}(R)\cong R^G$ as R^G-modules; see (5.5). Combining this isomorphism with the R^G-map $Q\to\operatorname{Hom}_{R\#G}(R,R\otimes_{R^G} Q)$, $q\mapsto(r\mapsto r\otimes q)$, we obtain an R^G-module map $Q\to R^G$. Since $Q_{\mathfrak{p}}\cong R^G_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of R^G, this map is an isomorphism. Therefore, $[Q]=1\in\operatorname{Pic}(R^G)$. This proves that δ is an embedding $\operatorname{Ker} j_G\hookrightarrow\bigcap_{\mathfrak{P}}\operatorname{Ker}\rho_{\mathfrak{P}}$.

Now assume that G is finite, denoted $\mathcal{G}$, and that $\operatorname{tr}_{\mathcal{G}}$ is surjective. Let $[d]\in\bigcap_{\mathfrak{P}}\operatorname{Ker}\rho_{\mathfrak{P}}$ be given and let $P=R_d$ be a corresponding $R\#\mathcal{G}$-module, defined (up to isomorphism) by Lemma 5.3.1. Since ${}_RP\cong R$, Lemma 5.4.1(a) implies that P is projective. By Lemma 5.4.1(b), P has the form $P\cong R\otimes_{R^{\mathcal{G}}} Q$ for some Q in $R^{\mathcal{G}}$-proj (necessarily invertible) precisely if $\mathfrak{G}P = P$ holds. Thus, in order to show that $[d] \in \operatorname{Im}\delta$, we have to check that $\mathfrak{G}P = P$. Suppose otherwise. Then $\mathfrak{G}P \subseteq \mathfrak{M}P$ for some maximal ideal $\mathfrak{M}$ of R, and so $\mathfrak{G}P \subseteq \bigcap_{g\in\mathcal{G}} g(\mathfrak{M})P = \mathfrak{M}^o P$, where $\mathfrak{M}^o = \bigcap_{g\in\mathcal{G}} g(\mathfrak{M})$. Therefore, $\mathfrak{G}$ annihilates the $R\#\mathcal{G}$-module $P/\mathfrak{M}^o P$. Letting $\mathcal{G}_{\mathfrak{M}} = \operatorname{stab}_{\mathcal{G}}(\mathfrak{M})$ denote the decomposition group of $\mathfrak{M}$, the Chinese remainder theorem implies that

$$P/\mathfrak{M}^o P \cong R\#\mathcal{G} \otimes_{R\#\mathcal{G}_{\mathfrak{M}}} P/\mathfrak{M}P\,; \tag{5.9}$$

as $R\#\mathcal{G}$-modules, and the $R\#\mathcal{G}_{\mathfrak{M}}$-action on $P/\mathfrak{M}P$ factors through $(R/\mathfrak{M})\#\mathcal{G}_{\mathfrak{M}}$. Now, $[d] \in \operatorname{Ker}\rho_{\mathfrak{M}}$ and $\rho_{\mathfrak{M}}$ factors as $H^1(\mathcal{G},\mathrm{U}(R)) \xrightarrow{\rho'_{\mathfrak{M}}} H^1(\mathcal{G}_{\mathfrak{M}},\mathrm{U}(R/\mathfrak{M})) \xrightarrow{\rho''_{\mathfrak{M}}} H^1(I_{\mathcal{G}}(\mathfrak{M}),\mathrm{U}(R/\mathfrak{M}))$ by restriction along $\mathcal{G} \supseteq \mathcal{G}_{\mathfrak{M}} \supseteq I_{\mathcal{G}}(\mathfrak{M})$. Here, $\operatorname{Ker}\rho''_{\mathfrak{M}} \cong H^1(\mathcal{G}_{\mathfrak{M}}/I_{\mathcal{G}}(\mathfrak{M}), U(R/\mathfrak{M}))$ is trivial, by Hilbert's "Theorem 90" (cf. Serre [193, Prop. VII.4 and Prop. X.2]). We conclude that $[d] \in \operatorname{Ker}\rho'_{\mathfrak{M}}$. In other words, the $(R/\mathfrak{M})\#\mathcal{G}_{\mathfrak{M}}$-module $P/\mathfrak{M}P$ is isomorphic to the canonical $(R/\mathfrak{M})\#\mathcal{G}_{\mathfrak{M}}$-module, $R/\mathfrak{M}$. The symmetrizer $t_{\mathfrak{M}} = \sum_{g\in\mathcal{G}_{\mathfrak{M}}} g \in (R/\mathfrak{M})\#\mathcal{G}_{\mathfrak{M}}$ acts as the trace $\operatorname{tr}_{\mathcal{G}_{\mathfrak{M}}}$ on $R/\mathfrak{M}$. Moreover, our surjectivity hypothesis on $\operatorname{tr}_{\mathcal{G}}$ implies that $\operatorname{tr}_{\mathcal{G}_{\mathfrak{M}}} : R/\mathfrak{M} \to (R/\mathfrak{M})^{\mathcal{G}_{\mathfrak{M}}}$ is surjective as well. The isomorphism (5.9) now shows that the action of $\sum_{g\in\mathcal{G}} g = \sum_{g\in\mathcal{G}/\mathcal{G}_{\mathfrak{M}}} g t_{\mathfrak{M}}$ on $P/\mathfrak{M}^o P$ is nonzero, contradicting the fact that $\mathfrak{G}$ annihilates $P/\mathfrak{M}^o P$. Thus, we must have $\mathfrak{G}P = P$, as desired. □

Example 5.5.2 (Triviality of Pic for polynomial invariants; Kang [104])**.** Let $\Bbbk$ be a field and let $R = \mathsf{S}(V)$ denote the symmetric algebra of a $\Bbbk$-vector space V. Suppose that the group G acts by $\Bbbk$-algebra automorphisms on R. Then $\operatorname{Pic}(R)$ is trivial and $\mathrm{U}(R) = \Bbbk^*$. So Proposition 5.5.1 gives that $\operatorname{Pic}(R^G)$ embeds into the kernel of the restriction map $\rho_{\mathfrak{P}} \colon \operatorname{Hom}(G,\Bbbk^*) \to \operatorname{Hom}(I_G(\mathfrak{P}),\mathrm{U}(R/\mathfrak{P}))$ for all primes $\mathfrak{P}$ of R. If there is a G-stable $\mathfrak{P}$ with $R/\mathfrak{P} = \Bbbk$ then this map is the identity map and we conclude that $\operatorname{Pic}(R^G)$ is trivial. In particular, this holds for linear actions, that is, G acts on $R = \mathsf{S}(V)$ by means of a linear representation $G \to \mathrm{GL}(V)$: take $\mathfrak{P} = V\mathsf{S}(V)$.

5.6 The Case of Multiplicative Actions

In this section, we calculate the intersection $\bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}}$ in Proposition 5.5.1 for a multiplicative action of a finite group $\mathcal{G}$ on $R = \Bbbk[L]$. The Proof of Theorem 5.1.1 will then follow immediately.

Lemma 5.6.1. *Let $R = \Bbbk[L]$ denote the group algebra of the $\mathcal{G}$-lattice L over the commutative domain $\Bbbk$. Assume that $|\mathcal{G}| \neq 0$ in $\Bbbk$. Then the intersection $\bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}}$ in Proposition 5.5.1 is isomorphic to $\text{Ш}^1(\mathcal{G},L)$; see* (5.3).

Proof. By Lemma 3.4.1, $\mathrm{U}(\Bbbk[L]) = \mathrm{U}(\Bbbk) \times \underline{L}$; so

$$H^1(\mathcal{G},\mathrm{U}(\Bbbk[L])) = \operatorname{Hom}(\mathcal{G},\mathrm{U}(\Bbbk)) \oplus H^1(\mathcal{G},L)\,.$$

For the augmentation ideal $\mathfrak{E} = \operatorname{Ker}\varepsilon$ of $\Bbbk[L]$ (see Section 3.9), we have $\Bbbk[L]/\mathfrak{E} = \Bbbk$ and $I_{\mathcal{G}}(\mathfrak{E}) = \mathcal{G}$. The map $\rho_{\mathfrak{E}}$ of (5.8) in this case becomes

$$\rho_{\mathfrak{E}}\colon\ \operatorname{Hom}(\mathcal{G}, \mathrm{U}(\Bbbk)) \oplus H^1(\mathcal{G}, L) \xrightarrow{\operatorname{Id}\oplus 0} \operatorname{Hom}(\mathcal{G}, \mathrm{U}(\Bbbk))\ .$$

Therefore, $\operatorname{Ker}\rho_{\mathfrak{E}} = H^1(\mathcal{G}, L)$, and hence $\bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}} = \bigcap_{\mathfrak{P}} \operatorname{Ker} r_{\mathfrak{P}}$, where $r_{\mathfrak{P}}$ is the restriction of the map $\rho_{\mathfrak{P}}$ in (5.8) to the summand $H^1(\mathcal{G}, L)$ of $H^1(\mathcal{G}, \mathrm{U}(\Bbbk[L]))$.

For each $g \in \mathcal{G}$, let $I(g) = I_{\Bbbk[L]}(g)$ be defined as in (4.5); so $\mathfrak{P} \supseteq I(g)$ is equivalent with $g \in I_{\mathcal{G}}(\mathfrak{P})$. By Lemma 4.5.1, $\Bbbk[L]/I(g)$ is isomorphic to a Laurent polynomial ring over the group ring $\Bbbk[H^1(\langle g\rangle, L)]$. Since $|\mathcal{G}| \cdot H^1(\langle g\rangle, L) = 0$, our hypotheses on $\Bbbk$ imply that $\Bbbk[H^1(\langle g\rangle, L)]$ is reduced, that is, $\Bbbk[H^1(\langle g\rangle, L)]$ has no nonzero nilpotent elements. Hence, $\Bbbk[L]/I(g)$ is reduced as well, and so

$$\bigcap_{\mathfrak{P}:\mathfrak{P}\supseteq I(g)} \mathfrak{P} = I(g)\ .$$

Now consider a cocycle $d\colon \mathcal{G} \to L$ and let $[d]$ denote its class in $H^1(\mathcal{G}, L)$. Then:

$$\begin{aligned}
[d] \in \bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}} &\iff \forall \mathfrak{P}\ \forall g \in I_{\mathcal{G}}(\mathfrak{P}):\ \ \mathbf{x}^{d(g)} \equiv 1 \mod \mathfrak{P}\\
&\iff \forall g \in \mathcal{G}:\ \ \mathbf{x}^{d(g)} - 1 \in \bigcap_{\mathfrak{P}:\mathfrak{P}\supseteq I(g)} \mathfrak{P} = I(g)\\
&\iff \forall g \in \mathcal{G}:\ \ d(g) \in [g, L]\\
&\iff \forall g \in \mathcal{G} : [d] \in \operatorname{Ker}\operatorname{res}^{\mathcal{G}}_{\langle g\rangle}\ .
\end{aligned}$$

This completes the proof of the lemma. □

We are now ready to prove Theorem 5.1.1.

Proof of Theorem 5.1.1. By (5.6), our hypothesis on $|\mathcal{G}|$ ensures that the trace map $\operatorname{tr}_{\mathcal{G}}\colon \Bbbk[L] \longrightarrow \Bbbk[L]^{\mathcal{G}}$ is surjective. Therefore, Proposition 5.5.1 implies that $\operatorname{Ker} j_{\mathcal{G}}$ is isomorphic to $\bigcap_{\mathfrak{P}} \operatorname{Ker}\rho_{\mathfrak{P}}$. By Lemma 5.6.1, this intersection is isomorphic to $\text{Ш}^1(\mathcal{G}, L)$. Therefore, $\operatorname{Ker} j_{\mathcal{G}} \cong \text{Ш}^1(\mathcal{G}, L)$. The rest now follows from (5.2). □

We remark that if we only assume that $|\mathcal{G}| \neq 0$ in $\Bbbk$ rather than $|\mathcal{G}|^{-1} \in \Bbbk$ then the same proof still shows that $\operatorname{Ker} j_{\mathcal{G}}$ embeds into $\text{Ш}^1(\mathcal{G}, L)$.

6

Multiplicative Invariants of Reflection Groups

6.1 Introduction

This chapter is devoted to the proof that multiplicative invariant algebras of reflection groups are semigroup algebras. Some instances of this phenomenon have occurred earlier in Examples 3.5.5, 3.5.6, 3.5.7 and in Theorem 3.6.1 and Lemma 4.5.2. We refer to Section 1.7 for the basics concerning reflections and reflection groups and to 3.4 for semigroup algebras. The main result reads as follows; for a more detailed version, see Proposition 6.2.1 below.

Theorem 6.1.1. *Let $\mathcal{G}$ be a finite group acting as a reflection group on the lattice L. Then there is a submonoid M of $(\mathbb{Z}[L]^{\mathcal{G}}, \cdot\,)$ whose elements form a $\mathbb{Z}$-basis of the invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$. Consequently, for any commutative base ring $\Bbbk$, $\Bbbk[L]^{\mathcal{G}}$ is isomorphic to the semigroup algebra $\Bbbk[M]$.*

Following [124] we will derive this result from Theorem 3.6.1. A proof over $\mathbb{C}$ is implicit in earlier work of Farkas [61]. It suffices to treat the case where the base ring is $\mathbb{Z}$. In view of Proposition 3.3.1(b), the assertion that $\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[M]$ for an arbitrary base ring $\Bbbk$ is then an immediate consequence.

We note the following corollary of Theorem 6.1.1. For the definition of Cohen-Macaulay rings, we refer to Chapter 8.

Corollary 6.1.2. *Suppose that $\mathcal{G}$ acts as a reflection group on L.*

(a) *If $\Bbbk$ is a Cohen-Macaulay ring then $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay as well.*
(b) *If $\Bbbk$ is a PID then all projective $\Bbbk[L]^{\mathcal{G}}$-modules are free.*
(c) *The group $Ш^1(\mathcal{G}, L)$ is trivial.*

Proof. Since $\mathbb{Z}[L]^{\mathcal{G}}$ is an affine normal domain, the monoid M is an affine normal semigroup; see Section 3.4. By a result of Hochster [89, Theorem 1] (see also Bruns and Herzog [32, Theorem 6.3.5(a)]), the semigroup algebra $\Bbbk[M]$ is Cohen-Macaulay for any Cohen-Macaulay ring $\Bbbk$, and hence so is $\Bbbk[L]^{\mathcal{G}}$, thereby proving (a). (A self-contained proof of (a) will be given in Section 6.3 below.) Part (b) is a consequence of Gubeladze's theorem [79] which asserts that projective $\Bbbk[M]$-modules are free when $\Bbbk$ is a PID. In particular, $\operatorname{Pic}(\mathbb{Q}[L]^{\mathcal{G}})$ is trivial, and hence so is $Ш^1(\mathcal{G}, L)$ by Theorem 5.1.1. This proves (c). $\square$

Part (a) of the corollary contrasts interestingly with the situation for linear actions: polynomial invariants of finite pseudoreflection groups can fail to be Cohen-Macaulay if the characteristic of the base field divides the group order; see, e.g., Nakajima [136, Example 4.1].

6.2 Proof of Theorem 6.1.1

Let $\mathcal{G}$ be a finite group acting as a reflection group on the lattice L. We may assume without loss of generality that L is a faithful $\mathcal{G}$-lattice. Consider the lattice

$$\widehat{L} = \rho(L) \oplus \Lambda = \widehat{L}^{\mathcal{G}} \oplus \Lambda$$

defined in (1.19) and (1.20); so $L \subseteq \widehat{L} \subseteq L_{\mathbb{Q}}$. By Proposition 1.9.1(a), we know that $\Lambda = \Lambda_{\mathcal{G}}(L)$ is the weight lattice of some reduced root system with Weyl group $\mathcal{G}$. Choose a set of fundamental weights $\{m_1, \ldots, m_r\} \subseteq \Lambda$ and put

$$\Lambda_+ = \bigoplus_{i=1}^{r} \mathbb{Z}_+ m_i$$

as in (3.10). Then we have the following more precise version of Theorem 6.1.1.

Proposition 6.2.1. (a) $\mathbb{Z}[\widehat{L}]^{\mathcal{G}} = \mathbb{Z}[\widehat{L}^{\mathcal{G}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\mathsf{orb}(m_1), \ldots, \mathsf{orb}(m_r)]$. *The $\mathcal{G}$-orbit sums* $\mathsf{orb}(m_i)$ $(m_i \in \Lambda)$ *are algebraically independent. Thus,* $\mathbb{Z}[\widehat{L}]^{\mathcal{G}}$ *is the semigroup algebra* $\mathbb{Z}[\widehat{M}]$ *of the monoid*

$$\widehat{M} = \Big(\langle \mathbf{x}^m, \mathsf{orb}(m_i) \mid m \in \widehat{L}^{\mathcal{G}}, 1 \le i \le r\rangle, \cdot\Big) \cong \Big(\widehat{L}^{\mathcal{G}} \oplus \Lambda_+, +\Big) .$$

(b) *Put* $M = \widehat{M} \cap \mathbb{Z}[L]$, *a submonoid of* $(\mathbb{Z}[L]^{\mathcal{G}}, \cdot)$. *Then*

$$M \cong \Big((\widehat{L}^{\mathcal{G}} \oplus \Lambda_+) \cap L, +\Big) \cong \Big(L^{\mathcal{G}} \oplus (\pi(L) \cap \Lambda_+), +\Big) ,$$

where $\pi = \operatorname{Id} - \rho$. *The elements of M form a $\mathbb{Z}$-basis of* $\mathbb{Z}[L]^{\mathcal{G}}$.

Proof. (a) The decomposition $\widehat{L} = \widehat{L}^{\mathcal{G}} \oplus \Lambda$ implies that $\mathbb{Z}[\widehat{L}]^{\mathcal{G}} = \mathbb{Z}[\widehat{L}^{\mathcal{G}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\Lambda]^{\mathcal{G}}$. Moreover, by Theorem 3.6.1, we know that the orbit sums $\mathsf{orb}(m_i)$ form an algebraically independent set of generators for $\mathbb{Z}[\Lambda]^{\mathcal{G}}$. This proves that $\mathbb{Z}[\widehat{L}]^{\mathcal{G}}$ is isomorphic to the semigroup algebra $\mathbb{Z}[\widehat{M}]$. Every $\ell \in \widehat{L}^{\mathcal{G}} \oplus \Lambda_+$ can be written as $\ell = m + \sum_{i=1}^{r} z_i m_i$, with uniquely determined $m \in \widehat{L}^{\mathcal{G}}$, $z_i \in \mathbb{Z}_+$. An explicit isomorphism $\widehat{L}^{\mathcal{G}} \oplus \Lambda_+ \to \widehat{M}$ is given by

$$\ell = m + \sum_{i=1}^{r} z_i m_i \mapsto \mu(\ell) = \mathrm{x}^m \,\mathsf{orb}(m_1)^{z_1} \cdot \ldots \cdot \mathsf{orb}(m_r)^{z_r} \,. \tag{6.1}$$

(b) Clearly, $M = \widehat{M} \cap \mathbb{Z}[L]$ is a submonoid of $(\mathbb{Z}[L]^{\mathcal{G}}, \cdot\,)$ whose elements are $\mathbb{Z}$-independent, as the elements of $\widehat{M}$ are. Our goal is to show that the monoid M is a $\mathbb{Z}$-basis for the invariant algebra $\mathbb{Z}[L]^{\mathcal{G}}$ and to determine its structure.

Let $f \in \mathbb{Z}[L]^{\mathcal{G}}$ be given. Then $f \in \mathbb{Z}[\widehat{L}]^{\mathcal{G}} = \mathbb{Z}[\widehat{M}]$; so f can be uniquely written as $f = \sum_{\mu \in \widehat{M}} z_\mu \mu$ with $z_\mu \in \mathbb{Z}$. 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 $f \neq 0$. Each $\mu \in \widehat{M}$ has the form $\mu = \mu(\ell)$ for a unique $\ell = m + \sum_{i=1}^{r} z_i m_i \in \widehat{L}^{\mathcal{G}} \oplus \Lambda_+$ as in (6.1). Since the factors x^m and $\mathsf{orb}(m_i)$ of $\mu(\ell)$ only involve non-negative $\mathbb{Z}$-coefficients (in fact, only 0 or 1), we have

$$\mathrm{Supp}(\mu(\ell)) = \{m + \sum_{i=1}^{r} \sum_{j=1}^{z_i} g_{i,j}(m_i) \mid g_{i,j} \in \mathcal{G}\} \,.$$

By Lemma 1.6.1, $\widehat{L}/L$ is $\mathcal{G}$-trivial. Hence, all $m + \sum_{i=1}^{r} \sum_{j=1}^{z_i} g_{i,j}(m_i)$ are congruent to $\ell = m + \sum_{i=1}^{r} z_i m_i$ modulo L. Therefore,

$$\mu(\ell) \in \mathbb{Z}[L] \iff \mathrm{Supp}(\mu(\ell)) \cap L \neq \varnothing \iff \ell \in L \,. \tag{6.2}$$

Since $f \in \mathbb{Z}[L]$, some $\mu \in \widehat{M}$ with $z_\mu \neq 0$ must satisfy $\mathrm{Supp}(\mu) \cap L \neq \varnothing$. By (6.2), we conclude that $\mu \in \mathbb{Z}[L] \cap \widehat{M} = M$. Thus, $f' = f - z_\mu \mu$ belongs to $\mathbb{Z}[L]^{\mathcal{G}}$ 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 $\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[M]$.

The equivalences in (6.2) also show that the (multiplicative) monoid M is isomorphic to the (additive) monoid $(\widehat{L}^{\mathcal{G}} \oplus \Lambda_+) \cap L$ via $\ell \mapsto \mu(\ell)$. Finally, the projection $\pi = \mathrm{Id} - \rho$ (see §1.6.2) sends $(\widehat{L}^{\mathcal{G}} \oplus \Lambda_+) \cap L$ onto $\pi(L) \cap \Lambda_+$, with kernel $L^{\mathcal{G}}$. Since $\pi(L)$ is free abelian, this map splits; so $(\widehat{L}^{\mathcal{G}} \oplus \Lambda_+) \cap L \cong L^{\mathcal{G}} \oplus (\pi(L) \cap \Lambda_+)$. This completes the proof. □

6.3 Computing the Ring of Invariants

We continue with the notation of Section 6.2. The proof of Proposition 6.2.1 gives a method for explicitly calculating the ring of invariants $\mathbb{Z}[L]^{\mathcal{G}}$. In this section, we describe some reductions producing certain easily predictable pieces of $\mathbb{Z}[L]^{\mathcal{G}}$. We also construct a set of fundamental invariants for $\mathbb{Z}[L]^{\mathcal{G}}$, calculate the class group $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{G}})$ in terms of a suitable weight lattice, and verify the Cohen-Macaulay property of $\mathbb{Z}[L]^{\mathcal{G}}$.

6.3.1 Reduction to an Effective Lattice

As in Section 1.6, let $\overline{L} = L/L^{\mathcal{G}}$ denote the effective quotient of L. An element $g \in \mathcal{G}$ acts as a reflection on $\overline{L}$ if and only if g does so on L. Hence, $\mathcal{G}$ acts as a reflection group on $\overline{L}$. We claim that

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L^{\mathcal{G}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\overline{L}]^{\mathcal{G}} \,. \tag{6.3}$$

Indeed, by Proposition 6.2.1(b), $\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[M]$ and $M = \underline{L^{\mathcal{G}}} \times M_+$, where $\underline{L^{\mathcal{G}}} = \{\mathbf{x}^m \mid m \in L^{\mathcal{G}}\}$ and $M_+ \cong \pi(L) \cap \Lambda_+$. Hence, $\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L^{\mathcal{G}}] \otimes_{\mathbb{Z}} \mathbb{Z}[M_+]$ and $\mathbb{Z}[M_+] \cong \mathbb{Z}[L]^{\mathcal{G}} / \left(\mathbf{x}^m - 1 \mid m \in L^{\mathcal{G}}\right)$. Since the right hand side is isomorphic to $\mathbb{Z}[\overline{L}]^{\mathcal{G}}$, by (3.14), the asserted isomorphism (6.3) follows.

6.3.2 Reduction to an Indecomposable Lattice

If $L = L_1 \oplus L_2$ for suitable $\mathcal{G}$-lattices L_1 and L_2 then

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L_1]^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[L_2]^{\mathcal{G}} \,. \tag{6.4}$$

Indeed, every reflection $g \in \mathcal{G}$ acts nontrivially on exactly one of the summands, and so $\mathcal{G}$ decomposes as $\mathcal{G}_1 \times \mathcal{G}_2$, where $\mathcal{G}_1$ is generated by the reflections $g \in \mathcal{G}$ that act trivially on L_2 and similarly for $\mathcal{G}_2$. Therefore, (6.4) follows from (3.5). Note also that $\mathcal{G}$ acts as a reflection group on both L_1 and L_2.

6.3.3 Removing Diagonalizable Reflections

As in §1.7.1, we put $\mathcal{D} = \langle d_1, \dots, d_r \rangle$, where $d_1, \dots, d_r$ are the elements of $\mathcal{G}$ that act as diagonalizable reflections on L. We claim that

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L^{\mathcal{D}}]^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[\mathbb{Z}_+^r] \,. \tag{6.5}$$

Recall from Lemma 1.7.2 that the $\mathcal{G}$-lattice L decomposes as $L = L^{\mathcal{D}} \oplus L_0$ with $L_0 = \bigoplus_{i=1}^r \mathbb{Z}\ell_i$ and $d_i(\ell_i) = -\ell_i$, $d_i(\ell_j) = \ell_j$ $(i \neq j)$. Thus, (6.4) gives $\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L^{\mathcal{D}}]^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[L_0]^{\mathcal{G}}$. We we have to show that $\mathbb{Z}[L_0]^{\mathcal{G}}$ is a polynomial algebra over $\mathbb{Z}$. This is a consequence of Theorem 3.6.1 (see the proof of Theorem 7.1.1 (d) $\Rightarrow$ (e) below), but it is also easy to see directly: by Lemma 1.7.2, the group $\mathcal{G}$ permutes the summands $\mathbb{Z}\ell_i$ of L_0 and (6.4) allows us to assume that $\mathcal{G}$ does in fact permute the $\mathbb{Z}\ell_i$ transitively. Furthermore, by Example 3.5.1,

$$\mathbb{Z}[L_0]^{\mathcal{D}} = \mathbb{Z}[\lambda_1, \dots, \lambda_r] \qquad \text{with} \quad \lambda_i = \mathbf{x}^{\ell_i} + \mathbf{x}^{-\ell_i} \,,$$

and $\mathcal{G}$ permutes the λ_i transitively. Moreover, any reflection $g \in \mathcal{G}$ either fixes all λ_i or interchanges exactly two of them. Thus, $\mathcal{G}$ acts on $\{\lambda_1, \dots, \lambda_r\}$ as a transitive permutation group that is generated by transpositions, hence as the full symmetric group $\mathcal{S}_r$. By the fundamental theorem for $\mathcal{S}_r$-invariants, we conclude that $\mathbb{Z}[L_0]^{\mathcal{G}} = \mathbb{Z}[\lambda_1, \dots, \lambda_r]^{\mathcal{S}_r}$ is a polynomial algebra over $\mathbb{Z}$. This proves (6.5).

We remark that $\mathcal{G}$ acts as a reflection group without diagonalizable reflections on $L^{\mathcal{D}}$. This follows from the decomposition $\mathcal{G} = \mathcal{G}\big|_{L^{\mathcal{D}}} \times \mathcal{G}\big|_{L_0}$; see §6.3.2.

6.3.4 Class Group

Let $\overline{L} = L/L^{\mathcal{G}}$ denote the effective quotient of L, as above, and put

$$L' = \overline{L}^{\overline{\mathcal{D}}} ,$$

where $\overline{\mathcal{D}}$ denotes the subgroup of $\mathcal{G}$ that is generated by the elements acting as diagonalizable reflections on $\overline{L}$. Let

$$\Lambda' = \Lambda_{\mathcal{G}}(L')$$

denote the weight lattice that is associated with the action of $\mathcal{G}$ on L'; see Proposition 1.9.1(a). Fix a set of fundamental weights $m_1, \ldots, m_t \in \Lambda'$ and let

$$\Lambda'_+ = \bigoplus_i \mathbb{Z}_+ m_i$$

denote the corresponding monoid of dominant weights. The following proposition summarizes the foregoing and determines the class group of $\mathbb{Z}[L]^{\mathcal{G}}$.

Proposition 6.3.1. *Let $\mathcal{G}$ be a finite group acting faithfully as a reflection group on the lattice L. Then, with the above notation,*

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[L']^{\mathcal{G}} \otimes_{\mathbb{Z}} \mathbb{Z}[\mathbb{Z}_+^r \oplus \mathbb{Z}^s] ,$$

where $s = \operatorname{rank} L^{\mathcal{G}}$ and r is the number of elements of $\mathcal{G}$ that act as diagonalizable reflections on $\overline{L}$. Moreover,

$$\mathbb{Z}[L']^{\mathcal{G}} \cong \mathbb{Z}[\Lambda'_+ \cap L'],$$

the semigroup ring of the monoid $\Lambda'_+ \cap L'$. The class group of $\Bbbk[L]^{\mathcal{G}}$, for any Krull domain $\Bbbk$, is given by

$$\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) = \mathrm{Cl}(\Bbbk) \oplus \Lambda'/L' .$$

Proof. The first isomorphism follows from (6.3) and (6.5). Since the $\mathcal{G}$-lattice L' is effective, Proposition 6.2.1(b) yields the second isomorphism.

After tensoring with $\Bbbk$, the first isomorphism implies that $\mathrm{Cl}(\Bbbk[L]^{\mathcal{G}}) \cong \mathrm{Cl}(\Bbbk[L']^{\mathcal{G}})$; see Fossum [67, 8.1 and 7.3]. Since $\mathcal{G}$ acts as a reflection group without diagonalizable reflections on the effective lattice L' (see §6.3.3), Theorem 4.1.1 and Lemma 1.6.1 yield $\mathrm{Cl}(\Bbbk[L']^{\mathcal{G}}) \cong \mathrm{Cl}(\Bbbk) \oplus H^1(\mathcal{G}, L') \cong \mathrm{Cl}(\Bbbk) \oplus \Lambda'/L'$. This completes the proof. □

For related result on class groups of semigroup algebras related to root systems, see Popov [151] and Strickland [205].

6.3.5 Fundamental Invariants and the Cohen-Macaulay Property

In view of §6.3.1, we may concentrate on the case where L is effective. Then Proposition 6.2.1(b) gives

$$\mathbb{Z}[L]^{\mathcal{G}} \cong \mathbb{Z}[\Lambda_+ \cap L] ,$$

where $\Lambda_+ = \bigoplus_{i=1}^n \mathbb{Z}_+ m_i$ for some collection of fundamental weights $m_1, \dots, m_n$.

The monoid $\Lambda_+ \cap L$ has a finite Hilbert basis; see Section 3.4. To explicitly construct this basis, consider the weight lattice $\Lambda = \bigoplus_{i=1}^n \mathbb{Z} m_i$, as before. Since Λ/L is finite, we may define

$$\ell_i = z_i m_i \in L \qquad (i = 1, \dots, n) ,$$

where $z_i \in \mathbb{N}$ is the order of m_i modulo L. Put $V = L_{\mathbb{R}} = \bigoplus_{i=1}^n \mathbb{R}\ell_i$ and

$$K = \{\sum_{i=1}^n t_i \ell_i \in V \mid 0 \leq t_i \leq 1\} \supset K^\circ = \{\sum_{i=1}^n r_i \ell_i \in V \mid 0 \leq r_i < 1\} .$$

Then $K \cap L \subseteq \Lambda_+$ is finite, being the intersection of a compact and a discrete subset of V. We claim that $K \cap L$ generates the monoid $\Lambda_+ \cap L$. Indeed, any $\ell \in \Lambda_+ \cap L$ can be uniquely written as

$$\ell = \ell' + \ell'' \tag{6.6}$$

with $\ell' \in \bigoplus_{i=1}^n \mathbb{Z}_+ \ell_i$ and $\ell'' \in K^\circ$. Since $\ell, \ell' \in L$, ℓ'' belongs to $K \cap L$ as do $\ell_1, \dots, \ell_n$. Hence, (6.6) exhibits ℓ as an element of the monoid generated by $K \cap L$, which proves our claim. Note that $\ell_1, \dots, \ell_n$ are indecomposable elements of $\Lambda_+ \cap L$, that is, they cannot be written as $m' + m''$ with nonzero $m', m'' \in \Lambda_+ \cap L$. The preceding argument shows that all indecomposable elements of $\Lambda_+ \cap L$ belong to $K \cap L$. Denoting additional indecomposables of $\Lambda_+ \cap L$ besides $\ell_1, \dots, \ell_n$ (if any) by $\ell_{n+1}, \dots, \ell_s$ we obtain the desired Hilbert basis $\{\ell_1, \dots, \ell_s\}$ for $\Lambda_+ \cap L$.

By Proposition 6.2.1, the Hilbert basis $\{\ell_1, \dots, \ell_s\}$ of $\Lambda_+ \cap L$ yields the following system of generating invariants for $\mathbb{Z}[L]^{\mathcal{G}}$:

$$\mu_i = \mu(\ell_i) \qquad (i = 1, \dots, s) ,$$

where $\mu(\ell)$ is defined by (6.1). Here, $\mu_1 = \mathsf{orb}(m_1)^{z_1}, \dots, \mu_n = \mathsf{orb}(m_n)^{z_n}$ are algebraically independent, as the $\mathsf{orb}(m_i)$'s are; so $\mathbb{Z}[\mu_1, \dots, \mu_n]$ is a polynomial subring of $\mathbb{Z}[L]^{\mathcal{G}}$. Moreover, by (6.6), the elements $\mu(\ell'')$ with $\ell'' \in K^\circ \cap L$ give a free basis for $\mathbb{Z}[L]^{\mathcal{G}}$ as a module over $\mathbb{Z}[\mu_1, \dots, \mu_n]$. This shows that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay. After tensoring with $\Bbbk$, we obtain the same conclusion for any Cohen-Macaulay base ring $\Bbbk$, thereby giving a direct proof of Corollary 6.1.2(a).

Example 6.3.2 (Multiplicative $\mathcal{S}_3$-invariants of A_2, revisited)**.** Recall that a base for the root system A_2 is given by $a_i = e_i - e_{i+1}$ $(i = 1, 2)$, with corresponding fundamental weights

$$m_1 = \tfrac{2}{3}e_1 - \tfrac{1}{3}e_2 - \tfrac{1}{3}e_3 = \tfrac{2}{3}a_1 + \tfrac{1}{3}a_2 ,$$
$$m_2 = \tfrac{1}{3}e_1 + \tfrac{1}{3}e_2 - \tfrac{2}{3}e_3 = \tfrac{1}{3}a_1 + \tfrac{2}{3}a_2 ;$$

see Examples 1.8.1 and 3.6.2. The procedure described above results in the following Hilbert basis for the monoid $\Lambda_+ \cap A_2 = (\mathbb{Z}_+ m_1 \oplus \mathbb{Z}_+ m_2) \cap (\mathbb{Z}a_1 \oplus \mathbb{Z}a_2)$:

$$\ell_1 = 3m_1 \ , \ \ell_2 = 3m_2 \quad \text{and} \quad \ell_3 = m_1 + m_2 \ ; \tag{6.7}$$

see Figure 6.1. Writing $x_i = \mathbf{x}^{e_i}$ $(i = 1, 2, 3)$ and using the orbit sum formula (3.13) of Example 3.6.2, we obtain the following fundamental invariants $\mu_i = \mu(\ell_i)$ for $\mathbb{Z}[A_2]^{\mathcal{S}_3}$:

$$\begin{aligned}
\mu_1 &= \mathsf{orb}(m_1)^3 = \frac{(x_1 + x_2 + x_3)^3}{x_1 x_2 x_3} \ , \\
\mu_2 &= \mathsf{orb}(m_2)^3 = \frac{(x_1 x_2 + x_2 x_3 + x_1 x_3)^3}{(x_1 x_2 x_3)^2} = (x_1 x_2 x_3)(x_1^{-1} + x_2^{-1} + x_3^{-1})^3 \ , \\
\mu_3 &= \mathsf{orb}(m_1)\,\mathsf{orb}(m_2) = \frac{(x_1 + x_2 + x_3)(x_1 x_2 + x_2 x_3 + x_1 x_3)}{x_1 x_2 x_3} = 3 + \sum_{i \neq j} \frac{x_i}{x_j} \ .
\end{aligned}$$

These generators are identical with those found earlier in Example 3.5.6.

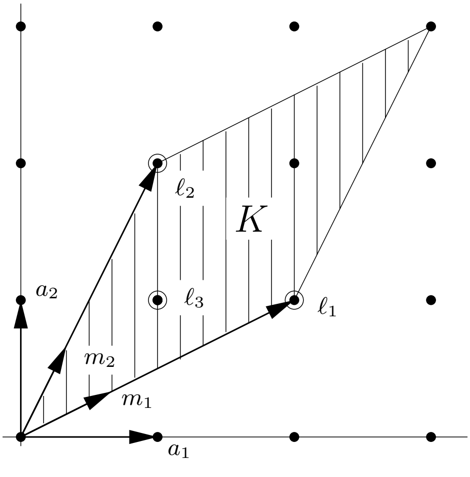

Fig. 6.1. type A_2

6.4 SAGBI Bases

In this section, we describe an interesting result of Reichstein [159] on SAGBI bases (subalgebra analog of Gröbner bases for ideals), a notion introduced by Robbiano and Sweedler [167] in the context of polynomial algebras. The modifications necessary for Laurent polynomial algebras are due to Reichstein. For simplicity, we work over a base field $\Bbbk$; see [159, Remark 7.2] for the modifications needed to deal with more general coefficient rings.

Recall from Section 3.4 that a monomial order for $\Bbbk[L]$ is a total order $\succ$ on L such that $m \succ n$ implies $m+\ell \succ n+\ell$ for all $m, n, \ell \in L$. A familiar example of such an order is the lexicographic order $\succ_{\text{lex}}$ with respect to a fixed $\mathbb{Z}$-basis $\{m_1, \dots, m_r\}$ of L: $\sum_i z_i m_i \succ_{\text{lex}} \sum_i z_i' m_i$ if and only if the first nonzero difference $z_i - z_i'$ is positive.

Given a monomial order, we can define the leading exponent, $\mathbf{max}(f)$, for any non-zero $f \in \Bbbk[L]$ to be the largest element of the support $\operatorname{Supp} f$ with respect to $\succ$; so

$$f = k_{\max} \mathbf{x}^{\mathbf{max}(f)} + \sum_{\substack{m \in L \\ \mathbf{max}(f) \succ m}} k_m \mathbf{x}^m$$

with $k_{\max} \in \Bbbk^*$. The coefficient $k_{\max}$ is called the *leading coefficient* of f, $\mathbf{x}^{\mathbf{max}(f)}$ the *leading monomial*, and $k_{\max}\mathbf{x}^{\mathbf{max}(f)}$ the *leading term*. Note that

$$\mathbf{max}(fg) = \mathbf{max}(f) + \mathbf{max}(g)$$

holds for all nonzero $f, g \in \Bbbk[L]$. Thus, for any $\Bbbk$-subalgebra R of $\Bbbk[L]$, the set

$$\mathbf{max}(R) = \{\mathbf{max}(f) \mid 0 \neq f \in R\}$$

is a submonoid of L. A collection of elements $\{f_i \mid i \in I\} \subseteq R$ is called a *SAGBI basis* of R if the following requirements are satisfied:

(a) the monoid $\mathbf{max}(R)$ is generated by $\{\mathbf{max}(f_i) \mid i \in I\}$, and
(b) the following algorithm "subduction algorithm" terminates for every input $f \in R$: If $f = 0$ then stop. Otherwise write $\mathbf{max}(f) = \sum_i n_i \mathbf{max}(f_i)$ with $n_i \in \mathbb{Z}_+$; this is possible by (a). Define $k \in \Bbbk^*$ to be the leading coefficient of f divided by the leading coefficient of $\prod_i f_i^{n_i}$; so f and $k \prod_i f_i^{n_i}$ have the same leading terms. Replace f by the new input $f_1 = f - k \prod_i f_i^{n_i}$ and proceed.

Note that the expression $\mathbf{max}(f) = \sum_i n_i \mathbf{max}(f_i)$ in (b) is generally not uniquely determined. Thus, each step in the subduction algorithm involves a choice. Each loop of the algorithm replaces a nonzero input $f \in R$ with a new $f_1 \in R$ which is either 0, in which case the algorithm terminates, or else f_1 satisfies $\mathbf{max}(f_1) \prec \mathbf{max}(f)$. If the process stops then the original input is explicitly written as a member of the subalgebra $\Bbbk[f_i \mid i \in I] \subseteq R$. However, the monoid $\mathbf{max}(R)$ need not be well-ordered with respect to $\succ$. For example, if $\mathbf{max}(R)$ contains a nonzero unit m then we may arrange that $0 \succ m$ and obtain the infinite descending chain $0 \succ m \succ 2m \succ \dots$ in $\mathbf{max}(R)$. Therefore, termination of the algorithm is not a priori guaranteed. Condition (b) postulates that the subduction algorithm does in fact eventually terminate for every input $f \in R$ no matter what choices are made.

We are primarily interested in the case where $R = \Bbbk[L]^{\mathcal{G}}$ is a multiplicative invariant algebra under the action of a finite group $\mathcal{G}$ on L. In this case, it follows from (3.4) that

$$\mathbf{max}(\Bbbk[L]^{\mathcal{G}}) = \{m \in L \mid m \succeq g(m) \text{ for all } g \in \mathcal{G}\} =: L^{\succ} .$$

Reichstein [159, Theorem 1.4] has shown that the monoid $L^{\succ}$ is finitely generated if and only if $\mathcal{G}$ acts as a reflection group on L. Note that both m and $-m$ belong to $L^{\succ}$ precisely, if $m \in L^{\mathcal{G}}$. Therefore, $L^{\succ}$ can only be well-ordered if $\mathcal{G}$ acts effectively on L. By [159, Proposition 5.5], the monoid $L^{\succ}$ is indeed well-ordered with respect to $\succ$ if $\mathcal{G}$ acts as a reflection group on L and $L^{\mathcal{G}} = 0$. Consequently, the subduction algorithm will always stop in this case, and every collection of invariants $f_i \in \Bbbk[L]^{\mathcal{G}}$ whose leading exponents $\mathbf{max}(f_i)$ generate the monoid $\mathbf{max}(\Bbbk[L]^{\mathcal{G}}) = L^{\succ}$ is a SAGBI basis for $\Bbbk[L]^{\mathcal{G}}$. With a more careful selection of the f_i's one can overcome the restriction to effective actions. Thus, we have the following remarkable theorem.

Theorem 6.4.1 (Reichstein)**.** *Let L be a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and let $\succ$ be any monomial order. Then the following are equivalent:*

(a) *the monoid $\mathbf{max}(\Bbbk[L]^{\mathcal{G}}) = L^{\succ}$ is finitely generated;*
(b) *$\Bbbk[L]^{\mathcal{G}}$ has a finite SAGBI basis;*
(c) *$\mathcal{G}$ acts as a reflection group on L.*

For the proof, we refer to the original publication of Reichstein [159]. Note that (c) above makes no reference to the chosen monomial order $\succ$ and the theorem requires no assumptions on $\succ$. In fact, if $\mathcal{G}$ acts effectively as a reflection group on L then, as Reichstein points out in [159, Remark 7.1], there is a canonical SAGBI basis for $\Bbbk[L]^{\mathcal{G}}$ which is independent of the choice of $\succ$. To see this, recall that the monoid $L^{\succ}$ is finitely generated with $\mathrm{U}(L^{\succ}) = \{0\}$ in this case and $L^{\succ}$ is clearly cancellative and torsion-free, being contained in L. Hence, by Lemma 3.4.3, $L^{\succ}$ has a unique Hilbert basis, $\{\ell_1, \dots, \ell_s\}$. The orbit sums

$$f_i = \mathsf{orb}(\ell_i)$$

satisfy $\mathbf{max}(f_i) = \ell_i$ and so, by the foregoing, $\{f_1, \dots, f_s\}$ is a SAGBI basis for $\Bbbk[L]^{\mathcal{G}}$. This SAGBI basis is independent of $\succ$. For, the cone $C = \mathbb{R}_+ L^{\succ}$ in $V = L_{\mathbb{R}}$ that is spanned by $L^{\succ}$ is a chamber, in the sense of Bourbaki [24, V.1.3], for the collection of hyperplanes $V^{\langle g \rangle} = \{v \in V \mid g(v) = v\}$ where g runs over the reflections in $\mathcal{G}$, and $L^{\succ} = C \cap L$; see [159]. Thus, by [24, Lemme V.3.2], C is determined by $\mathcal{G}$, up to replacing C by $g(C)$ for some $g \in \mathcal{G}$, and similarly for L and its Hilbert basis. Since f_i remains unchanged under replacing ℓ_i by some $g(\ell_i)$, our assertion follows.

We illustrate this construction with an example taken from Tesemma [215].

Example 6.4.2 (Canonical SAGBI basis for the $\mathcal{S}_3$-invariants of A_2)**.** As in Example 1.8.1, we write the $\mathcal{S}_3$-lattice A_2 as $A_2 = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$. Identifying A_2 with $\mathbb{Z}^2$ by means of this basis and using the lexicographical order $\succ = \succ_{\text{lex}}$ on A_2 as the underlying monomial order, one obtains

$$A_2^{\succ} = \{(a, b) \in \mathbb{Z}^2 \mid 2a \geq b \geq a/2\} .$$

The monoid $A_2^{\succ}$ has the following Hilbert basis:

$$\ell_1 = (2,1),\ \ell_2 = (1,2),\ \ell_3 = (1,1)\ .$$

This is identical with the basis exhibited in (6.7). The orbit sums $f_i = \mathsf{orb}(\ell_i)$ form the desired SAGBI basis for $\Bbbk[A_2]^{\mathcal{S}_3}$. Writing $y_j = \mathbf{x}^{a_j} = \frac{x_j}{x_{j+1}}$ as in Example 3.5.6, the f_i are explicitly given by:

$$\begin{aligned}
f_1 &= y_1^2 y_2 + y_1^{-1} y_2^{-2} + y_1^{-1} y_2 = \frac{x_1^3 + x_2^3 + x_3^3}{x_1 x_2 x_3} \\
f_2 &= y_1 y_2^2 + y_1^{-2} y_2^{-1} + y_1 y_2^{-1} = \frac{x_1^3 x_2^3 + x_2^3 x_3^3 + x_1^3 x_3^3}{(x_1 x_2 x_3)^2} \\
f_3 &= y_1 y_2 + y_1^{-1} y_2^{-1} + y_1 + y_2 + y_1^{-1} + y_2^{-1} \\
&= \frac{x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2}{x_1 x_2 x_3}
\end{aligned}$$

The multiplicative submonoid of $\Bbbk[A_2]^{\mathcal{S}_3}$ that is generated by $\{f_1, f_2, f_3\}$ is not $\Bbbk$-independent:

$$f_1 f_2 - f_3^3 + 3 f_1 f_3 + 3 f_2 f_3 + 6 f_1 + 6 f_2 + 9 f_3 + 9 = 0\ .$$

7

Regularity

7.1 Introduction

It is a standard fact from commutative algebra that any maximal ideal $\mathfrak{m}$ of a commutative noetherian ring R satisfies the inequality $\operatorname{height} \mathfrak{m} \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$, where $k = R/\mathfrak{m}$ is the residue field of $\mathfrak{m}$. The ring R is called *regular* if equality holds for all $\mathfrak{m}$. Localizations of regular rings at multiplicatively closed subsets are again regular. Moreover, regular rings are normal, that is, they are finite direct products of integrally closed domains. If R has finite (Krull) dimension $\dim R$, regularity is equivalent with finite global dimension. In this case, the two dimensions have the same value, $\operatorname{gl\,dim} R = \dim R$; see Serre [192, Cor. 2 to Thm. IV.9]. The group algebra $\Bbbk[L]$ of a lattice L is regular if and only if the base ring $\Bbbk$ is; cf., e.g., Bruns and Herzog [32, Theorem 2.2.13].

The following theorem is a combination of the main result of [122] and earlier results of Farkas [60], Steinberg [204] and Richardson [165, Prop. 4.1], [166, Prop. 13.3].

Theorem 7.1.1. *Let L be a faithful $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and let $\Bbbk$ be a regular commutative ring so that $|\mathcal{G}| \neq 0$ in $\Bbbk$. Then the following assertions are equivalent:*

(a) *The algebra of multiplicative invariants $\Bbbk[L]^{\mathcal{G}}$ is regular;*
(b) *$\Bbbk[L]$ is projective as $\Bbbk[L]^{\mathcal{G}}$-module;*
(c) *$\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[\mathbb{Z}_+^r \oplus \mathbb{Z}^s]$, a mixed Laurent polynomial algebra over $\Bbbk$;*
(d) *$\mathcal{G}$ acts as a reflection group on L and $\mathbb{Z}[L]^{\mathcal{G}}$ is a unique factorization domain.*
(e) *The effective quotient $\overline{L} = L/L^{\mathcal{G}}$ of L is isomorphic to the weight lattice of some reduced root system with $\mathcal{G}$ acting as the Weyl group.*

Accepting this theorem for now, we make a number of comments. First, part (b) can be strengthened to:

(b$_1$) *$\Bbbk[L]$ is free over $\Bbbk[L]^{\mathcal{G}}$.*

Indeed, in view of (d) or (e), all assertions of the theorem are equivalent to regularity of $\mathbb{Z}[L]^{\mathcal{G}}$. Then $\mathbb{Z}[L]$ is projective over $\mathbb{Z}[L]^{\mathcal{G}}$ and $\mathbb{Z}[L]^{\mathcal{G}}$ is a mixed Laurent polynomial algebra. By the generalized Quillen-Suslin theorem (e.g., Lam [113, p. 144]) or Corollary 6.1.2(b), we conclude that $\mathbb{Z}[L]$ is actually free over $\mathbb{Z}[L]^{\mathcal{G}}$. Assertion (b$_1$) now follows by tensoring with $\Bbbk$.

Furthermore, in view of Theorem 4.1.1 and Proposition 6.3.1, part (d) can be reformulated in either of the following ways:

(d$_1$) *$\mathcal{G}$ acts as a reflection group on L and $\Lambda' = L'$ in the notation of* §6.3.4.

(d$_2$) *$\mathcal{G}$ acts as a reflection group on L and $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}}) = 0$, where $\mathcal{D}$ is the subgroup of $\mathcal{G}$ generated by the diagonalizable reflections on L; see* §1.7.1.

These formulations provide regularity criteria that are readily accessible to explicit computations. Table 7.1 gives the statistics for ranks $n \leq 4$; it was obtained using the crystallographic groups library of GAP [71]. The two reflection groups in rank 2 leading to non-regular multiplicative invariant algebras have been discussed in Examples 3.5.6 and 3.5.7.

Table 7.1. Regular invariant algebras ($L = \mathbb{Z}^n$)

n	# finite $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$ (up to conjugacy)	# reflection groups $\mathcal{G}$ (up to conjugacy)	# cases with $\mathbb{Z}[L]^{\mathcal{G}}$ regular
2	13	9	7
3	73	29	18
4	710	102	51

Finally, in part (c) of Theorem 7.1.1, we must have $s = \operatorname{rank} L^{\mathcal{G}}$. Indeed, if $\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[\mathbb{Z}_+^r \oplus \mathbb{Z}^s]$ then, replacing $\Bbbk$ a prime image if necessary, Lemma 3.4.1 gives $\mathrm{U}(\Bbbk[L]^{\mathcal{G}}) = \mathrm{U}(\Bbbk) \times \underline{L^{\mathcal{G}}}$ while $\Bbbk[\mathbb{Z}_+^r \oplus \mathbb{Z}^s]$ has group of units $\mathrm{U}(\Bbbk) \times \mathbb{Z}^s$. In particular, we obtain the following converse to Theorem 3.6.1. The result is due to Farkas [59, Main Theorem] (over $\mathbb{C}$) and it is also implicit in Steinberg [204].

Corollary 7.1.2 (Farkas, Steinberg)**.** *Let L be a faithful $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and let $\Bbbk$ be a regular commutative ring with $|\mathcal{G}| \neq 0$ in $\Bbbk$. Then $\Bbbk[L]^{\mathcal{G}}$ is a polynomial algebra over $\Bbbk$ if and only if L is isomorphic to the weight lattice of some reduced root system with $\mathcal{G}$ acting as the Weyl group.*

7.2 Projectivity over Invariants

The equivalence (a) $\iff$ (b) is a special case of a more general fact about finite group actions on rings. The noetherian hypothesis in the following lemma is minor: by Noether's finiteness theorem it is satisfied whenever R is an affine algebra over some noetherian subring $\Bbbk \subseteq R^{\mathcal{G}}$; see, e.g., Bourbaki [22, Théorème V.1.2]. In general, however, there are regular domains R which are not noetherian over the invariant subring $R^{\mathcal{G}}$ under the action of some finite group $\mathcal{G}$; see Chuang and Lee [39] or Montgomery [135, Example 5.5].

Lemma 7.2.1. *Let R be a commutative ring and let $\mathcal{G}$ be a finite group acting by automorphisms on R. Assume that R is regular and noetherian as module over the invariant subring $R^{\mathcal{G}}$. Then $R^{\mathcal{G}}$ is regular if and only if R is projective as $R^{\mathcal{G}}$-module.*

Proof. First assume that $R^{\mathcal{G}}$ is regular. We have to show that, for each maximal ideal $\mathfrak{m}$ of $R^{\mathcal{G}}$, the localization $R_{\mathfrak{m}} = R \otimes_{R^{\mathcal{G}}} R^{\mathcal{G}}_{\mathfrak{m}}$ is free over $R^{\mathcal{G}}_{\mathfrak{m}}$. Note that $R^{\mathcal{G}}_{\mathfrak{m}} = (R_{\mathfrak{m}})^{\mathcal{G}} \subseteq R_{\mathfrak{m}}$ is a finite extension of regular rings. Moreover, the maximal ideals of $R_{\mathfrak{m}}$ are exactly the primes lying over the maximal ideal of $R^{\mathcal{G}}_{\mathfrak{m}}$. By [22, Théorème V.2.2(i)], these primes form a single $\mathcal{G}$-orbit, and hence they all have the same height. Freeness of $R_{\mathfrak{m}}$ over $R^{\mathcal{G}}_{\mathfrak{m}}$ now follows from Eisenbud [54, Corollary 18.17].

Conversely, assume that R is projective over $R^{\mathcal{G}}$. Fix a maximal ideal $\mathfrak{m}$ of $R^{\mathcal{G}}$ and choose a maximal ideal $\mathfrak{M}$ of R lying over $\mathfrak{m}$. Then we have maps $R^{\mathcal{G}}_{\mathfrak{m}} \hookrightarrow R_{\mathfrak{m}} \to R_{\mathfrak{M}}$. The former makes $R_{\mathfrak{m}} = R \otimes_{R^{\mathcal{G}}} R^{\mathcal{G}}_{\mathfrak{m}}$ a free $R^{\mathcal{G}}_{\mathfrak{m}}$-module, by hypothesis, and the latter is flat, being a localization map. Therefore, $R_{\mathfrak{M}}$ is flat over $R^{\mathcal{G}}_{\mathfrak{m}}$. Since $R_{\mathfrak{M}}$ is regular, it follows that $R^{\mathcal{G}}_{\mathfrak{m}}$ is regular as well; see, e.g., Bruns and Herzog [32, Theorem 2.2.12(a)]. □

7.3 Linearization by the Slice Method

In this section, L denotes a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group. If $\Bbbk$ is an algebraically closed field whose characteristic does not divide the order of $\mathcal{G}$ then the local study of the multiplicative invariant algebra $\Bbbk[L]^{\mathcal{G}}$ reduces to the classical case of polynomial invariants. Indeed, $\mathcal{G}$ acts linearly on the $\Bbbk$-vector space $L_{\Bbbk} = L \otimes_{\mathbb{Z}} \Bbbk$, and hence on the symmetric algebra $\mathsf{S}(L_{\Bbbk})$. The algebra of invariants $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}}$ associated with this action is an ordinary algebra of polynomial invariants. Proposition 7.3.1 below details the connection between the invariant subalgebras of $\Bbbk[L]$ and of $\mathsf{S}(L_{\Bbbk})$. The proposition is an application of Luna's slice theorem [128]. An excellent exposition of this theorem, for reductive groups in characteristic 0, can be found in Slodowy [198]; an appendix by Knop gives a complete proof. For arbitrary characteristics, see Bardsley and Richardson [2].

We let $\mathfrak{E}$ denote the augmentation ideal of $\Bbbk[L]$,

$$\mathfrak{E} = \operatorname{Ker}(\varepsilon)\ , \tag{7.1}$$

where $\varepsilon\colon \Bbbk[L] \to \Bbbk$ is the augmentation map defined by $\varepsilon(\mathbf{x}^m) = 1$ $(m \in L)$, as in Section 3.9. Furthermore, $\widehat{\ }$ denotes completions of local rings and $\mathcal{G}_{\mathfrak{M}} = \operatorname{stab}_{\mathcal{G}}(\mathfrak{M})$ denotes the decomposition group of the ideal $\mathfrak{M}$ of $\Bbbk[L]$.

Proposition 7.3.1. *Assume that $\Bbbk$ is an algebraically closed field. Let $\mathfrak{M}$ be a maximal ideal of $\Bbbk[L]$ and let $\mathfrak{m} = \mathfrak{M} \cap \Bbbk[L]^{\mathcal{G}}$. Then:*

(a) $\widehat{\Bbbk[L]^{\mathcal{G}}_{\mathfrak{m}}} \cong \widehat{\Bbbk[L]^{\mathcal{G}_{\mathfrak{M}}}_{\mathfrak{e}}}$, *where* $\mathfrak{e} = \mathfrak{E} \cap \Bbbk[L]^{\mathcal{G}_{\mathfrak{M}}}$.

(b) *If* $\operatorname{char} \Bbbk$ *does not divide the order of* $\mathcal{G}_{\mathfrak{M}}$ *then* $\widehat{\Bbbk[L]^{\mathcal{G}}_{\mathfrak{m}}} \cong \widehat{\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}_{\mathsf{S}_+}}$, *where* S_+ *denotes the maximal ideal of* $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}$ *consisting of all* $\mathcal{G}_{\mathfrak{M}}$*-invariant polynomials having constant term* 0.

Proof. Put $X = \operatorname{Spec} \Bbbk[L]$ and let $x \in X$ be the point corresponding to $\mathfrak{M}$. Then X is an algebraic torus on which $\mathcal{G}$ acts by automorphisms and x has stabilizer $\mathcal{G}_x = \mathcal{G}_{\mathfrak{M}}$. Since $\mathcal{G}$ is finite, the orbit $\mathcal{G}(x)$ of x is closed and separable and the tangent space $T_x(\mathcal{G}(x))$ is the zero-space. Therefore, by [2, Proposition 7.3], there exists an open affine $\mathcal{G}_x$-subvariety S of X with $x \in S$ such that the morphism $S/\mathcal{G}_x \to X/\mathcal{G}$ which comes from the quotient morphism $\pi\colon X \to X/\mathcal{G}$ is étale at x. Thus, letting $\mathcal{O}(X/\mathcal{G}) = \mathcal{O}(X)^{\mathcal{G}}$ denote the algebra of regular functions on $X/\mathcal{G}$ and similarly for $S/\mathcal{G}_x$, we have

$$\widehat{\mathcal{O}(X)^{\mathcal{G}}_{\pi(x)}} \cong \widehat{\mathcal{O}(S)^{\mathcal{G}_x}_{x}} .$$

Since S is open in X, we have $\mathcal{O}(S)_x \cong \mathcal{O}(X)_x$ and so $\mathcal{O}(S)^{\mathcal{G}_x}_x \cong \mathcal{O}(X)^{\mathcal{G}_x}_x$. Translation by x, $t \mapsto xt$, is a $\mathcal{G}_x$-equivariant automorphism of the torus X sending the identity 1 to x. Hence, $\mathcal{O}(X)^{\mathcal{G}_x}_x \cong \mathcal{O}(X)^{\mathcal{G}_x}_1$ and so

$$\widehat{\mathcal{O}(X)^{\mathcal{G}}_{\pi(x)}} \cong \widehat{\mathcal{O}(X)^{\mathcal{G}_x}_{1}} .$$

This is the isomorphism asserted in (a). See also Raynaud [156, Chap. X, Théorème 1] or SGA1 [78, Prop. V.2.2].

For (b), assume that $\operatorname{char} \Bbbk$ does not divide the order of $\mathcal{G}_x$, or equivalently, that $\mathcal{G}_x$ is linearly reductive over $\Bbbk$. In view of (a), we may assume that $\mathcal{G} = \mathcal{G}_{\mathfrak{M}}$ and $x = 1$. The canonical map $\mathfrak{E} \to (T_1 X)^* = \mathfrak{E}/\mathfrak{E}^2$ is a map of $\Bbbk[\mathcal{G}]$-modules. By hypothesis on $\operatorname{char} \Bbbk$, this map has a $\Bbbk[\mathcal{G}]$-linear section $\mathfrak{E}/\mathfrak{E}^2 \to \mathfrak{E}$ and this section lifts to a $\mathcal{G}$-equivariant algebra map $\mathcal{O}(T_1 X) = \mathsf{S}(\mathfrak{E}/\mathfrak{E}^2) \to \mathcal{O}(X)$. Hence we obtain a morphism of $\mathcal{G}$-varieties $X \to T_1 X$, $1 \mapsto 0$, which is étale at 1. Thus,

$$\widehat{\mathcal{O}(X)^{\mathcal{G}}_1} \cong \widehat{\mathcal{O}(T_1 X)^{\mathcal{G}}_0} = \widehat{\mathsf{S}(\mathfrak{E}/\mathfrak{E}^2)^{\mathcal{G}}_{\mathsf{S}_+}} .$$

Part (b) now follows from the $\Bbbk[\mathcal{G}]$-isomorphism

$$\begin{array}{rcll} L_{\Bbbk} = L \otimes_{\mathbb{Z}} \Bbbk & \xrightarrow{\cong} & \mathfrak{E}/\mathfrak{E}^2 & \\ m \otimes 1 & \longmapsto & \mathbf{x}^m - 1 + \mathfrak{E}^2 & \qquad (m \in L) \end{array}$$

This completes the proof of the proposition. □

As an application one obtains the following regularity criterion.

Corollary 7.3.2. *In the situation of Proposition 7.3.1(b),* $\Bbbk[L]^{\mathcal{G}}_{\mathfrak{m}}$ *is regular if and only if* $\mathcal{G}_{\mathfrak{M}}$ *acts as a reflection group on* L.

Proof. A noetherian local ring is regular if and only if its completion is; cf., e.g., Bruns and Herzog [32, Proposition 2.2.2]. Thus, by Proposition 7.3.1(b), $\Bbbk[L]^{\mathcal{G}}_{\mathfrak{m}}$ is regular if and only if $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}_{\mathsf{S}_+}$ is regular. Now, $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}$ is a positively graded algebra with graded radical S_+. By a standard result on graded algebras (e.g., [32, Exercise 2.2.25]), $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}_{\mathsf{S}_+}$ is regular if and only if $\mathsf{S}(L_{\Bbbk})^{\mathcal{G}_{\mathfrak{M}}}$ is a polynomial algebra and, by the Shephard-Todd-Chevalley Theorem (e.g., [24, Théorème V.5.4]), the latter condition is equivalent to $\mathcal{G}_{\mathfrak{M}}$ acting as a reflection group on $L_{\Bbbk}$. Thus, $\mathcal{G}_{\mathfrak{M}}$ is generated by elements g so that that the subspace $L_{\Bbbk}^{\langle g\rangle}$ of g-fixed points in $L_{\Bbbk}$ has codimension at most 1; see Section 1.7. Finally, for each $g \in \mathcal{G}_{\mathfrak{M}}$, we have

$$\operatorname{rank} L^{\langle g\rangle} = \dim_{\Bbbk} L_{\Bbbk}^{\langle g\rangle} .$$

This is obvious for $\operatorname{char}\Bbbk = 0$. If $\operatorname{char}\Bbbk = p > 0$ then $L_{\Bbbk}^{\langle g\rangle} = L_{\mathbb{F}_p}^{\langle g\rangle} \otimes_{\mathbb{F}_p} \Bbbk$ and $L^{\langle g\rangle}$ maps onto $L_{\mathbb{F}_p}^{\langle g\rangle}$, because p does not divide the order of g. The above equality follows. In particular, g is a pseudoreflection on $L_{\Bbbk}$ if and only if g is a reflection on L. This proves the corollary. □

7.4 Proof of Theorem 7.1.1

By Lemma 7.2.1, we know that (a) and (b) are equivalent. It remains to establish the equivalence of (a), (c), (d) and (e).

We first show that regularity of $\Bbbk[L]^{\mathcal{G}}$ forces $\mathcal{G}$ to act as a reflection group on L. By Proposition 3.3.1(b), we may replace $\Bbbk$ by any localization $\Bbbk_{\mathfrak{p}}$. Choosing $\mathfrak{p}$ to be a minimal prime not containing $|\mathcal{G}|$ we reduce to the case where $\Bbbk$ is a field whose characteristic does not divide $|\mathcal{G}|$. Passing to the algebraic closure of the prime subfield of $\Bbbk$ (see [32, Remark 2.2.16]), we may further assume that $\Bbbk$ is algebraically closed. Thus, Corollary 7.3.2 applies with $\mathfrak{M} = \mathfrak{E}$, the augmentation ideal of $\Bbbk[L]$, and we obtain that $\mathcal{G}_{\mathfrak{E}} = \mathcal{G}$ is a reflection group on L, as desired.

In view of Theorem 6.1.1, we conclude that (a) implies that $\Bbbk[L]^{\mathcal{G}}$ is a regular semigroup algebra over $\Bbbk$, and these are known to be mixed Laurent polynomial algebras; see [32, Exercise 6.1.11]. Alternatively, Corollary 6.1.2(c) tells us that $\text{Ш}^1(\mathcal{G}, L)$ is trivial. After reducing to the case where $\Bbbk$ is a field whose characteristic does not divide $|\mathcal{G}|$ as above, we deduce from Theorem 5.1.1 that $\operatorname{Pic}(\Bbbk[L]^{\mathcal{G}})$ is trivial, and hence so is $\operatorname{Cl}(\Bbbk[L]^{\mathcal{G}})$. By Proposition 6.3.1, the latter fact implies that $\varLambda' = L'$ and that $\Bbbk[L]^{\mathcal{G}}$ is a mixed Laurent polynomial algebra, for any base ring $\Bbbk$. Thus, (a) implies (c). Since the converse is standard, (a) and (c) are equivalent. Note further that the above argument also shows that (a) implies (d).

We now show that (d) implies (e). As in §6.3.4, let $\overline{L} = L/L^{\mathcal{G}}$ denote the effective quotient of L, $\overline{\mathcal{D}}$ the subgroup of $\mathcal{G}$ that is generated by the elements acting as diagonalizable reflections on $\overline{L}$, and $L' = \overline{L}^{\overline{\mathcal{D}}}$. By Lemma 1.7.2, we know that $\overline{L} = L' \oplus L''$, where $L'' = \bigoplus_{i=1}^{r} \mathbb{Z}\ell_i$ with $\mathcal{G}$ permuting the summands $\mathbb{Z}\ell_i$. Now (d_1) gives $\varLambda' = \varLambda_{\mathcal{G}}(L') = L'$; so Proposition 1.9.1 tells us that L' is the weight lattice of some reduced root system with $\mathcal{G}$ acting as the Weyl group. This is also true for L''.

For, L'' splits into a direct sum of lattices formed by the orbits of $\mathcal{G}$ on $\{\mathbb{Z}\ell_i\}$. Considering each of these summands in turn, we may assume that $\mathcal{G}$ permutes the $\mathbb{Z}\ell_i$ transitively. Thus, $\mathcal{G}$ acts on L'' as the semidirect product $\{\pm 1\} \wr \mathcal{S}_r$. This is exactly the Weyl group action on the weight lattice of a root system of type C_r $(r \geq 2)$ or A_1 $(r = 1)$; see Bourbaki [24, Planches I,III]. This proves (e).

Finally, assume (e). Then $\mathcal{G}$ acts as a reflection group on $\overline{L}$ and hence on L. Thus, (6.3) gives $\Bbbk[L]^{\mathcal{G}} \cong \Bbbk[L^{\mathcal{G}}] \otimes_{\Bbbk} \Bbbk[\overline{L}]^{\mathcal{G}}$. Furthermore, by Theorem 3.6.1, we know that $\Bbbk[\overline{L}]^{\mathcal{G}}$ is a polynomial algebra; so $\Bbbk[L]^{\mathcal{G}}$ is a mixed Laurent polynomial algebra over $\Bbbk$. This proves the implication (e) ⇒ (c), thereby completing the proof of the theorem. □

7.5 Regularity at the Identity

The following result takes up the theme of Chapter 6. Recall that $\varepsilon\colon \Bbbk[L] \to \Bbbk$ is the augmentation map and $\mathfrak{E} = \operatorname{Ker} \varepsilon$ denotes the augmentation ideal of $\Bbbk[L]$; see (7.1).

Theorem 7.5.1. *Let L denote a faithful lattice for the finite group $\mathcal{G}$ and let $\Bbbk$ be a commutative noetherian domain with $|\mathcal{G}| \neq 0$ in $\Bbbk$. Then the following assertions are equivalent:*

(a) $\Bbbk[L]^{\mathcal{G}}$ *is regular at the ideal* $\mathfrak{E} \cap \Bbbk[L]^{\mathcal{G}}$*;*
(b) $\mathcal{G}$ *acts as a reflection group on L;*
(c) $\Bbbk[L]^{\mathcal{G}} = \Bbbk[M]$ *is a semigroup algebra with* $\varepsilon(M) \subseteq \Bbbk \setminus \{0\}$.

Proof. The implication (a) ⇒ (b) was established in the first paragraph of the proof of Theorem 7.1.1 in Section 7.4. Furthermore, (b) ⇒ (c) follows from Proposition 6.2.1 which asserts that if $\mathcal{G}$ acts as a reflection group on L then $\Bbbk[L]^{\mathcal{G}}$ is a semigroup algebra $\Bbbk[M]$ for some submonoid $M \subseteq \left(\Bbbk[L]^{\mathcal{G}}, \cdot\right)$ whose elements are products of certain orbit sums $\mathsf{orb}(m)$ with $m \in \widehat{L}$, some $\mathcal{G}$-lattice containing L. Since all $\varepsilon(\mathsf{orb}(m)) = [\mathcal{G} : \mathcal{G}_m] \cdot 1$ are nonzero in $\Bbbk$, the same is true for each element of $\varepsilon(M)$. Therefore, $\varepsilon(M) \subseteq \Bbbk \setminus \{0\}$ proving (c).

In order to show that (c) ⇒ (a), it will again be convenient to use geometric language. We may replace $\Bbbk$ by the algebraic closure of its field of fractions, thereby reducing the problem to the case where $\Bbbk$ is an algebraically closed field whose characteristic does not divide the order of $\mathcal{G}$; see [32, Remark 2.2.16]. Our hypothesis that $\Bbbk[L]^{\mathcal{G}} = \Bbbk[M]$ is a semigroup algebra, necessarily affine normal, is equivalent to $Y = \operatorname{Spec} \Bbbk[L]^{\mathcal{G}}$ being an affine toric variety. We briefly sketch the connection; for more information on toric varieties, see Danilov [47], Fulton [69] or Oda [142]. Recall from Section 3.4 that the monoid M embeds into some lattice A with $A = \langle M \rangle_{\text{group}}$. This embedding extends to an embedding of $\Bbbk$-algebras $\Bbbk[L]^{\mathcal{G}} = \Bbbk[M] \hookrightarrow \Bbbk[A]$. Put $T = \operatorname{Hom}(A, \Bbbk^*)$, an algebraic torus over $\Bbbk$ with $\Bbbk[A] = \mathcal{O}(T)$; see 3.10. The embedding $\Bbbk[L]^{\mathcal{G}} \hookrightarrow \Bbbk[A]$ corresponds to a dominant morphism of varieties $\Phi\colon T \to Y$. Explicitly, using the identification

$$Y = \operatorname{Spec} \Bbbk[M] = \operatorname{Hom}_{\Bbbk\text{-alg}}(\Bbbk[M], \Bbbk) = \operatorname{Hom}_{\text{monoid}}(M, (\Bbbk, \cdot)) ,$$

the map Φ is just restriction $T = \operatorname{Hom}(A, \Bbbk^*) \to Y = \operatorname{Hom}_{\text{monoid}}(M, (\Bbbk, \cdot))$. The torus T acts on Y by multiplication: for $\tau \in T$ and $\mu \in Y$, define $\tau\mu \colon M \to \Bbbk$ by $\tau\mu(m) = \tau(m)\mu(m)$ $(m \in M)$. This gives a morphism of varieties $T \times Y \to Y$ which fits into a commutative diagram of algebraic varieties

$$\begin{tikzcd}
T \arrow[r, "\Phi"] & Y \\
T \times T \arrow[u, "\text{mult.}"] \arrow[r, "\operatorname{Id} \times \Phi"] & T \times Y \arrow[u]
\end{tikzcd}$$

The image $\Phi(T) \subseteq Y$ is a dense T-orbit in Y which is explicitly given by

$$\Phi(T) = \{\mu \in Y \mid \mu(M) \subseteq \Bbbk^*\} .$$

Thus, our hypothesis $\varepsilon(M) \subseteq \Bbbk^*$ says that $\varepsilon\big|_{\Bbbk[L]^{\mathcal{G}}} \in \Phi(T)$.

The singular locus Y_{sing} of Y is a closed T-stable subset of Y. Hence, $\Phi(T) \subseteq Y_{\text{reg}} = Y \setminus Y_{\text{sing}}$, because otherwise $\Phi(T) \subseteq Y_{\text{sing}}$ and hence $Y = \overline{\Phi(T)} \subseteq Y_{\text{sing}}$, which is impossible. Therefore, $\varepsilon\big|_{\Bbbk[L]^{\mathcal{G}}} \in Y_{\text{reg}}$ or, in other words, $\Bbbk[L]^{\mathcal{G}}$ is regular at $\mathfrak{E} \cap \Bbbk[L]^{\mathcal{G}}$. This proves (a) and completes the proof of the theorem. □

8

The Cohen-Macaulay Property

8.1 Introduction

Cohen-Macaulay rings form an important class of commutative noetherian rings, wide enough to encompass most other classes of well-behaved rings (see Fig. 8.4 below), yet restricted enough to avoid unwanted pathologies and allow for a sound dimension theory. The definition of Cohen-Macaulay rings is slightly technical in nature and the main tools for their investigation are furnished by homological algebra, but the theory has surprising and pleasantly concrete applications in many fields, notably in algebraic combinatorics; see, e.g., Stanley [202]. An excellent background reference for Cohen-Macaulay rings is the monograph [32] by Bruns and Herzog.

The Cohen-Macaulay problem in invariant theory of finite groups is the question to what extent the Cohen-Macaulay property passes from a commutative ring R to a subring $R^{\mathcal{G}}$ of invariants under the action of a finite group $\mathcal{G}$. This is essentially a problem in "modular" invariant theory: it is a well-known fact that the Cohen-Macaulay property descends from R to $R^{\mathcal{G}}$ whenever the trace map $\operatorname{tr}_{\mathcal{G}} \colon R \to R^{\mathcal{G}}$, $r \mapsto \sum_{g \in G} g(r)$, is surjective; see Corollary 8.5.2 below. In general, however, the property usually does not transfer to $R^{\mathcal{G}}$, even in the special case of linear actions on polynomial algebras. The Cohen-Macaulay problem for polynomial invariants has been rather thoroughly explored without, apparently, being near a final solution.

In this chapter, we will describe what is known about the Cohen-Macaulay problem for multiplicative invariants $\Bbbk[L]^{\mathcal{G}}$; the main result, Theorem 8.1.1 below, is from [120]. It is a standard fact that $\Bbbk[L]^{\mathcal{G}}$ can only be Cohen-Macaulay when $\Bbbk$ is so (see Proposition 8.4.1(a) below). However, even when the coefficient ring $\Bbbk$ is Cohen-Macaulay, rather stringent additional conditions on the action of $\mathcal{G}$ on the lattice L are required in order to ensure that $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay. Recall from Section 1.7 that an element $g \in \mathcal{G}$ is said to act as a *bireflection* on L if the sublattice $[g, L] = \{g(m) - m \mid m \in L\}$ of L has rank at most 2. For any subgroup $\mathcal{H} \leq \mathcal{G}$, we put

$$\mathcal{R}^2(\mathcal{H}) = \langle g \in \mathcal{H} \mid g \text{ acts as a } k\text{-reflection on } L \rangle \ .$$

Furthermore, as usual, $\mathcal{G}_m = \{g \in \mathcal{G} \mid g(m) = m\}$ denotes the isotropy group of $m \in L$. The main result now reads as follows.

Theorem 8.1.1. *Let L be a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and assume that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay. Then $\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)$ is a perfect group (i.e., equal to its commutator subgroup) for all $m \in L$. If $\mathcal{G}$ acts non-trivially on L then some isotropy group $\mathcal{G}_m$ is non-perfect, and hence some element of $\mathcal{G}$ acts as a non-trivial bireflection on L.*

While certainly not laying the Cohen-Macaulay problem for multiplicative invariants to rest, Theorem 8.1.1 does have a number of noteworthy applications. It leads to an almost complete description of all $\mathcal{S}_n$-lattices L such that $\mathbb{Z}[L]^{\mathcal{S}_n}$ is Cohen-Macaulay; see Example 8.11.3 below. Moreover, the last assertion of Theorem 8.1.1 immediately implies the following multiplicative version of Kemper's 3-copies conjecture:

Corollary 8.1.2. *If $\mathcal{G}$ acts non-trivially on L and $r \geq 3$ then $\mathbb{Z}[L^{\oplus r}]^{\mathcal{G}}$ is not Cohen-Macaulay.*

The 3-copies conjecture was originally formulated by Kemper in [108, Vermutung 3.12] for polynomial invariants. The conjecture in this case states that if $\mathcal{G} \to \mathrm{GL}(V)$ is a non-trivial modular representation of a finite group $\mathcal{G}$ then the algebra of invariants $\mathsf{S}(V^{\oplus r})^{\mathcal{G}}$ is not Cohen-Macaulay for any $r \geq 3$. This is still open.

The major part of this chapter, Sections 8.2 – 8.8, serves to deploy the homological tools needed for the investigation of the Cohen-Macaulay problem. This material, is developed in the framework of general commutative rings, usually under some noetherian hypothesis. After providing some background on Cohen-Macaulay rings, we describe in 8.6 the celebrated spectral sequences of Ellingsrud and Skjelbred supplying some details not included in the original article [55]. Our main result on general invariant rings of finite groups, Theorem 8.8.1, is an application of these spectral sequences. In short, the result states that if R and $R^{\mathcal{G}}$ are both Cohen-Macaulay and $H^i(\mathcal{G}, R) = 0$ for $0 < i < k$ then $H^k(\mathcal{G}, R)$ is detected by $(k+1)$-reflections on R in the sense of Section 4.5. Only Sections 8.9 – 8.11 are devoted specifically to multiplicative invariants. Unless mentioned otherwise, the results and examples in this chapter are from [125] and [120].

8.2 Height and Grade

Let R denote a commutative ring. The *height* of a prime $\mathfrak{p} \in \operatorname{Spec} R$ is defined to be the supremum of the lengths t of all strictly descending chains $\mathfrak{p} = \mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_t$ with $\mathfrak{p}_i \in \operatorname{Spec} R$. For an arbitrary ideal $\mathfrak{a}$ of R, one defines

$$\operatorname{height} \mathfrak{a} = \inf\{\operatorname{height} \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec} R, \mathfrak{p} \supseteq \mathfrak{a}\}$$

with the usual convention that $\inf \varnothing = \infty$. For added flexibility in changing rings, the following module theoretic variant will be useful. For any finitely generated (left) R-module M, we put

$$\operatorname{height}(\mathfrak{a}, M) = \operatorname{height}(\mathfrak{a} + \operatorname{ann}_R M / \operatorname{ann}_R M) ,$$

where $\operatorname{ann}_R M$ is the annihilator ideal of M in R. Thus, $\operatorname{height} \mathfrak{a} = \operatorname{height}(\mathfrak{a}, R)$. We remark that $\mathfrak{a}M = M$ is equivalent with $\mathfrak{a} + \operatorname{ann}_R M = R$ (see, e.g., Eisenbud [54, Corollary 4.7]); so $\operatorname{height}(\mathfrak{a}, M) = \infty$ holds in this case.

For noetherian rings R, there is a second invariant associated with $\mathfrak{a}$, called the *grade* of $\mathfrak{a}$ (or the *depth* of $\mathfrak{a}$). Among the various descriptions of grade the version based on regular sequences is the most elementary. Let M be an R-module. A sequence $\underline{x} = x_1, x_2, \ldots, x_n$ of elements of R is called *M-regular* or an *M-sequence* if the following two conditions are satisfied

(a) x_i acts injectively on $M / \sum_{j=1}^{i-1} x_j M$ for $i = 1, 2, \ldots, n$, and
(b) $\sum_{j=1}^{n} x_j M \neq M$.

If all x_i belong to the ideal $\mathfrak{a}$ of R then $\underline{x}$ is said to be an M-regular sequence in $\mathfrak{a}$. The sequence $\underline{x}$ is called a *maximal* M-regular sequence in $\mathfrak{a}$ if $x_1, x_2, \ldots, x_n, x_{n+1}$ is not M-regular for any $x_{n+1} \in \mathfrak{a}$. Clearly, any M-regular sequence in $\mathfrak{a}$ is contained in a maximal one, since the chain $(x_1) \subset (x_1, x_2) \subset \ldots$ of ideals of R is strictly increasing. A classical result of Rees [157] asserts that, for any finitely generated R-module M with $\mathfrak{a}M \neq M$, all maximal M-sequences in $\mathfrak{a}$ have the same length, and this length is equal to the least integer $i \geq 0$ with $\operatorname{Ext}^i_R(R/\mathfrak{a}, M) \neq 0$; see also Bruns and Herzog [32, Theorem 1.2.5]. This number is called the *grade of* $\mathfrak{a}$ *on* M; it will be denoted by $\operatorname{grade}(\mathfrak{a}, M)$. The *grade of the ideal* $\mathfrak{a}$ is defined by

$$\operatorname{grade} \mathfrak{a} = \operatorname{grade}(\mathfrak{a}, R) .$$

If $\mathfrak{a}M = M$, one puts $\operatorname{grade}(\mathfrak{a}, M) = \infty$. This is consistent with the description in terms of Ext: $\operatorname{Ext}^i_R(R/\mathfrak{a}, M) = 0$ for all i if and only if $\mathfrak{a}M = M$; see [32, p. 10]. So, for any finitely generated R-module M and any ideal $\mathfrak{a}$ of R, one has

$$\operatorname{grade}(\mathfrak{a}, M) = \inf\{i \mid \operatorname{Ext}^i_R(R/\mathfrak{a}, M) \neq 0\} .$$

The two invariants defined above are related by the fundamental inequality

$$\operatorname{grade}(\mathfrak{a}, M) \leq \operatorname{height}(\mathfrak{a}, M) \tag{8.1}$$

which holds for any finitely generated module M over a commutative noetherian ring R and any ideal $\mathfrak{a}$ of R; see [32, Exercise 1.2.22(a)].

8.3 Local Cohomology

Another descriptions of grade, based on local cohomology, will be convenient for our purposes. We briefly recall the basic definitions and facts; see, e.g., Brodmann and Sharp [29] for complete details.

Let R be a commutative ring and let $R\text{-}\mathsf{Mod}$ denote the category of all (left) R-modules. For any ideal $\mathfrak{a}$ of R, the $\mathfrak{a}$-torsion functor $\varGamma_{\mathfrak{a}} \colon R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ is defined by

$$\varGamma_{\mathfrak{a}}(M) = \bigcup_{n \geq 0} \{m \in M \mid \mathfrak{a}^n m = 0\}$$

for an R-module M. This functor is easily seen to be left exact. The i^{th} *local cohomology* functor with respect to $\mathfrak{a}$, denoted by $H^i_{\mathfrak{a}}$, is the i^{th} right derived functor of $\varGamma_{\mathfrak{a}}$:

$$H^i_{\mathfrak{a}} = R^i \varGamma_{\mathfrak{a}} \,.$$

To compute $H^i_{\mathfrak{a}}(M)$ for an R-module M, one chooses any injective resolution $I\colon 0 \to I^0 \to I^1 \to \ldots$ of M; so $H^0(I) \cong M$ and $H^i(I) = 0$ for $i \neq 0$. Then $H^i_{\mathfrak{a}}(M)$ is the i^{th} cohomology group of the complex $\varGamma_{\mathfrak{a}}(I)\colon 0 \to \varGamma_{\mathfrak{a}}(I^0) \to \varGamma_{\mathfrak{a}}(I^1) \to \ldots$. In particular, $H^0_{\mathfrak{a}}(M) \cong \varGamma_{\mathfrak{a}}(M)$, since $\varGamma_{\mathfrak{a}}$ is left exact.

Now assume that R is noetherian and M is finitely generated. Then

$$\operatorname{grade}(\mathfrak{a}, M) = \inf\{i \mid H^i_{\mathfrak{a}}(M) \neq 0\} \,. \tag{8.2}$$

In particular, $H^i_{\mathfrak{a}}(M) = 0$ for all i if and only if $\mathfrak{a}M = M$; see [29, 6.2.6, 6.2.7].

8.4 Cohen-Macaulay Modules and Rings

Let R be a commutative noetherian ring. A finitely generated R-module M is called *Cohen-Macaulay* if equality holds in equation (8.1) for all ideals $\mathfrak{a}$ of R. It follows from Bruns and Herzog [32, Proposition 1.2.10(a) and Theorem 2.1.3(b)] that it suffices to check the required equality for all maximal ideals $\mathfrak{a}$ of R with $\mathfrak{a} \supseteq \operatorname{ann}_R M$. The ring R is called a *Cohen-Macaulay ring* if R is Cohen-Macaulay as module over itself. Thus, R is Cohen-Macaulay if and only if

$$\operatorname{height} \mathfrak{a} = \operatorname{grade} \mathfrak{a}$$

holds for all (maximal) ideals $\mathfrak{a}$ of R.

We briefly recall some standard facts on Cohen-Macaulay rings; for complete details, the reader is referred to Bruns and Herzog [32]. As shown in Figure 8.4,

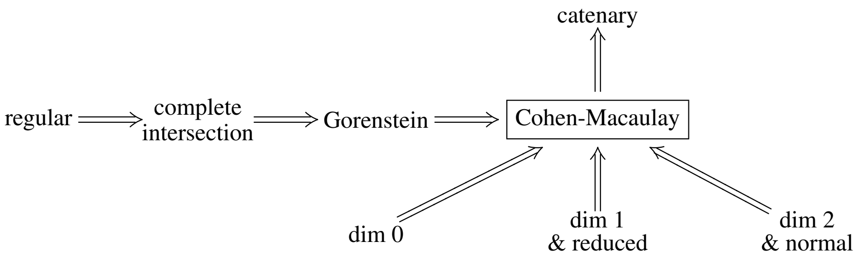

Fig. 8.1. Hierarchy of commutative noetherian rings

the usual classes of "well-behaved" noetherian rings and most "small" noetherian rings are Cohen-Macaulay. Furthermore, localizations of Cohen-Macaulay rings and polynomial rings over Cohen-Macaulay rings are again Cohen-Macaulay [32, Theorem 2.1.3(b) and Theorem 2.1.9]. For future use, we quote the following standard result on the passage of the Cohen-Macaulay property in ring extensions. Recall that a *Reynolds operator* for an extension $R \subseteq S$ of commutative rings is an R-linear map $\rho\colon S \to R$ such that $\rho\big|_R = \mathrm{Id}_R$.

Proposition 8.4.1. *Let $R \subseteq S$ be an extension of commutative noetherian rings.*

(a) *Assume that S is faithfully flat over R. Then S is Cohen-Macaulay if and only if R and all fibres $S_{\mathfrak{P}}/\mathfrak{p}S_{\mathfrak{P}}$ are Cohen-Macaulay where $\mathfrak{P} \in \operatorname{Spec} S$ and $\mathfrak{p} = \mathfrak{P} \cap R$.*

(b) (Hochster and Eagon [90]) *Assume that S is integral over R and that there is a Reynolds operator $\rho\colon S \to R$. If S is Cohen-Macaulay then so is R.*

Proof. For (a), see [32, Exercise 2.1.23] and for (b), [32, Theorem 6.4.5] or [90]. □

For many purposes, the most useful and down-to-earth description of Cohen-Macaulay rings is the following.

Theorem 8.4.2. *Let R be a commutative domain that is an affine algebra over some commutative PID $\Bbbk$. Assume that R is a finite module over the polynomial subalgebra $P = \Bbbk[x_1, \dots, x_n] \subseteq R$. Then:*

$$R \text{ is Cohen-Macaulay} \qquad \Longleftrightarrow \qquad R \text{ is a free } P\text{-module.}$$

Proof. $\Leftarrow$: Since P is Cohen-Macaulay, this implication follows from Proposition 8.4.1(a).

$\Rightarrow$: For every maximal ideal $\mathfrak{m}$ of P, $P_{\mathfrak{m}} \subseteq R_{\mathfrak{m}} = R \otimes_P P_{\mathfrak{m}}$ is a finite extension of noetherian domains, with $R_{\mathfrak{m}}$ Cohen-Macaulay and $P_{\mathfrak{m}}$ regular local. By Matsumura [131, (18.H) Theorem 46], $R_{\mathfrak{m}}$ is free over $P_{\mathfrak{m}}$. Therefore, R is projective over P, and hence free by the Quillen-Suslin theorem. □

8.5 The Cohen-Macaulay Property for Invariant Rings

Let $\mathcal{G}$ be a finite group acting by automorphisms on the commutative ring R. If R is Cohen-Macaulay then we would like to know if the invariant subring $R^{\mathcal{G}}$ is Cohen-Macaulay as well. More generally, suppose we already know that $R^{\mathcal{H}}$ is Cohen-Macaulay for some subgroup $\mathcal{H} \leq \mathcal{G}$. A useful device in passing from $R^{\mathcal{H}}$ to $R^{\mathcal{G}}$ is the *relative trace map* $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}\colon R^{\mathcal{H}} \to R^{\mathcal{G}}$; it is defined by

$$\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r) = \sum_{g \in \mathcal{G}/\mathcal{H}} g(r) \qquad (r \in R^{\mathcal{H}}) ,$$

where $\mathcal{G}/\mathcal{H}$ denotes any transversal for the cosets $g\mathcal{H}$ of $\mathcal{H}$ in $\mathcal{G}$. Each choice of transversal yields the same map. For $\mathcal{H} = 1$ one obtains the ordinary trace map $\operatorname{tr}_{\mathcal{G}}$ as in 5.4. We will write

$$R^{\mathcal{G}}_{\mathcal{H}} = \operatorname{Im}(\operatorname{tr}_{\mathcal{G}/\mathcal{H}}) \ .$$

Since $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}$ is $R^{\mathcal{G}}$-linear, $R^{\mathcal{G}}_{\mathcal{H}}$ is an ideal of $R^{\mathcal{G}}$.

Lemma 8.5.1. *Put $\mathfrak{a} = \sum_{\mathcal{H}} R^{\mathcal{G}}_{\mathcal{H}}$, where $\mathcal{H}$ runs over all subgroups of $\mathcal{G}$ so that $R^{\mathcal{H}}$ is Cohen-Macaulay. Then, for every prime ideal $\mathfrak{p}$ of $R^{\mathcal{G}}$ so that $\mathfrak{p} \not\supseteq \mathfrak{a}$, the localization $R^{\mathcal{G}}_{\mathfrak{p}}$ is Cohen-Macaulay.*

Proof. By hypothesis, $\mathfrak{p} \not\supseteq R^{\mathcal{G}}_{\mathcal{H}}$ for some $\mathcal{H}$ such that $R^{\mathcal{H}}$ is Cohen-Macaulay. Let $R_{\mathfrak{p}}$ denote the localization of R at the multiplicative subset $R^{\mathcal{G}} \setminus \mathfrak{p}$. The $\mathcal{G}$-action on R extends to $R_{\mathfrak{p}}$ and $(R_{\mathfrak{p}})^{\mathcal{G}} = R^{\mathcal{G}}_{\mathfrak{p}}$. Similarly, $(R_{\mathfrak{p}})^{\mathcal{H}} = R^{\mathcal{H}}_{\mathfrak{p}}$, and this ring is Cohen-Macaulay. By choice of $\mathfrak{p}$ the relative trace map $\operatorname{tr}_{\mathcal{G}/\mathcal{H}} \colon (R_{\mathfrak{p}})^{\mathcal{H}} \to (R_{\mathfrak{p}})^{\mathcal{G}}$ is onto. Fix an element $c \in (R_{\mathfrak{p}})^{\mathcal{H}}$ so that $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(c) = 1$ and define $\rho\colon (R_{\mathfrak{p}})^{\mathcal{H}} \to (R_{\mathfrak{p}})^{\mathcal{G}}$ by $\rho(x) = \operatorname{tr}_{\mathcal{G}/\mathcal{H}}(cx)$. This map is a Reynolds operator in the sense of 8.4. Since $(R_{\mathfrak{p}})^{\mathcal{H}}$ is integral over $(R_{\mathfrak{p}})^{\mathcal{G}}$, Proposition 8.4.1(b) implies that $(R_{\mathfrak{p}})^{\mathcal{G}}$ is Cohen-Macaulay, which proves the lemma. □

If $\mathfrak{a} = R^{\mathcal{G}}$ holds in the above lemma then $R^{\mathcal{G}}$ is Cohen-Macaulay. In particular, we obtain the following fact first pointed out by Hochster and Eagon [90, Proposition 13].

Corollary 8.5.2. *Suppose that R is Cohen-Macaulay. If the trace map $\operatorname{tr}_{\mathcal{G}} \colon R \to R^{\mathcal{G}}$ is surjective then $R^{\mathcal{G}}$ is Cohen-Macaulay as well.*

We now turn to height and grade for invariant rings. For this, we will assume that R is noetherian as $R^{\mathcal{G}}$-module. By Noether's finiteness theorem, this assumption is satisfied whenever R is an affine algebra over some noetherian subring $\Bbbk \subseteq R^{\mathcal{G}}$; see [22, Théorème V.1.2]. In particular, the case of multiplicative actions over a noetherian base ring $\Bbbk$ is certainly covered.

Lemma 8.5.3. *Let $\mathfrak{A}$ be an ideal of R and let M be a left module over the skew group ring $R\#\mathcal{G}$ (see 5.3). Put $\mathfrak{a} = \mathfrak{A} \cap R^{\mathcal{G}}$. Then:*

(a) $\operatorname{height}(\mathfrak{A}, M) = \operatorname{height}(\mathfrak{a}, M)$.
(b) *If R is noetherian as $R^{\mathcal{G}}$-module and M is finitely generated then*

$$\operatorname{grade}(\mathfrak{A}, M) = \operatorname{grade}(\mathfrak{a}, M) \ .$$

Proof. (a) We begin with some observations on the integral extension of rings

$$R^{\mathcal{G}} / \operatorname{ann}_{R^{\mathcal{G}}} M \hookrightarrow R / \operatorname{ann}_R M \ .$$

First, for any $\mathfrak{P} \in \operatorname{Spec} R$,

$$\mathfrak{P} \supseteq \operatorname{ann}_R M \iff \mathfrak{P} \cap R^{\mathcal{G}} \supseteq \operatorname{ann}_{R^{\mathcal{G}}} M \ . \tag{8.3}$$

To prove the nontrivial implication $\Leftarrow$, use Lying Over to find a prime $\mathfrak{Q} \in \operatorname{Spec} R$ with $\operatorname{ann}_R M \subseteq \mathfrak{Q}$ and $\mathfrak{Q} \cap R^{\mathcal{G}} = \mathfrak{P} \cap R^{\mathcal{G}}$. By [22, Théorème V.2.2(i)], $\mathfrak{P} = g(\mathfrak{Q})$ for some $g \in \mathcal{G}$, and so $\mathfrak{P} \supseteq g(\operatorname{ann}_R M) = \operatorname{ann}_R M$, since the ideal $\operatorname{ann}_R M$

is $\mathcal{G}$-stable. This proves (8.3). We conclude that $R^{\mathcal{G}}/\operatorname{ann}_{R^{\mathcal{G}}} M \hookrightarrow R/\operatorname{ann}_R M$ satisfies Going Down. Indeed, by (8.3), this follows from Going Down for $R^{\mathcal{G}} \subseteq R$, which in turn is a consequence of Lying Over and Going Up in conjunction with [22, Théorème V.2.2(i)]. It follows that, for any $\mathfrak{P} \in \operatorname{Spec} R$ with $\mathfrak{P} \supseteq \operatorname{ann}_R M$, we have

$$\operatorname{height}(\mathfrak{P}/\operatorname{ann}_R M) = \operatorname{height}(\mathfrak{P} \cap R^{\mathcal{G}}/\operatorname{ann}_{R^{\mathcal{G}}} M) . \tag{8.4}$$

Now, to prove (a), let $\mathfrak{P}$ be a prime of R with $\mathfrak{P} \supseteq \mathfrak{A} + \operatorname{ann}_R M$ and such that $\operatorname{height}(\mathfrak{A}, M) = \operatorname{height}(\mathfrak{P}/\operatorname{ann}_R M)$. Then $\operatorname{height}(\mathfrak{a}, M) \leq \operatorname{height}(\mathfrak{P} \cap R^{\mathcal{G}}/\operatorname{ann}_{R^{\mathcal{G}}} M)$ and so, by (8.4), $\operatorname{height}(\mathfrak{a}, M) \leq \operatorname{height}(\mathfrak{A}, M)$. For the reverse inequality, choose $\mathfrak{p} \in \operatorname{Spec} R^{\mathcal{G}}$ with $\mathfrak{p} \supseteq \mathfrak{a} + \operatorname{ann}_{R^{\mathcal{G}}} M$ and $\operatorname{height}(\mathfrak{a}, M) = \operatorname{height}(\mathfrak{p}/\operatorname{ann}_{R^{\mathcal{G}}} M)$. We claim that $\mathfrak{p} \supseteq (\mathfrak{A} + \operatorname{ann}_R M) \cap R^{\mathcal{G}}$. To see this, consider $a \in \mathfrak{A}$ and $b \in \operatorname{ann}_R M$ with $a + b \in R^{\mathcal{G}}$. Then $(a+b)^{|\mathcal{G}|} = \prod_{g \in \mathcal{G}} g(a+b) = \prod_{g \in \mathcal{G}} g(a) + c$ with $c \in \operatorname{ann}_R M$. Clearly, $\prod_{g \in \mathcal{G}} g(a) \in \mathfrak{A} \cap R^{\mathcal{G}} = \mathfrak{a}$ and so $c \in \operatorname{ann}_{R^{\mathcal{G}}} M$. Therefore, $(a+b)^{|\mathcal{G}|} \in \mathfrak{a} + \operatorname{ann}_{R^{\mathcal{G}}} M \subseteq \mathfrak{p}$, and so $a+b \in \mathfrak{p}$, as desired. By Lying Over for the integral extension $R^{\mathcal{G}}/(\mathfrak{A} + \operatorname{ann}_R M) \cap R^{\mathcal{G}} \hookrightarrow R/\mathfrak{A} + \operatorname{ann}_R M$, we may choose a prime $\mathfrak{P}$ of R with $\mathfrak{P} \cap R^{\mathcal{G}} = \mathfrak{p}$ and $\mathfrak{P} \supseteq \mathfrak{A} + \operatorname{ann}_R M$. Then $\operatorname{height}(\mathfrak{A}, M) \leq \operatorname{height}(\mathfrak{P}/\operatorname{ann}_R M)$ and, by (8.4), $\operatorname{height}(\mathfrak{P}/\operatorname{ann}_R M) = \operatorname{height}(\mathfrak{p}/\operatorname{ann}_{R^{\mathcal{G}}} M)$. Therefore, $\operatorname{height}(\mathfrak{A}, M) \leq \operatorname{height}(\mathfrak{a}, M)$ which proves (a).

(b) Note that both R and $R^{\mathcal{G}}$ are noetherian rings and M is finitely generated over R and over $R^{\mathcal{G}}$. If $\mathfrak{a}M = M$ then $\mathfrak{A}M = M$ and both grades are ∞. Therefore, we can assume that $\mathfrak{a}M \neq M$. Let $\underline{x} = x_1, \ldots, x_n$ be a maximal M-regular sequence in $\mathfrak{a}$; so $n = \operatorname{grade}(\mathfrak{a}, M)$. Since $\underline{x}$ is also an M-regular sequences in $\mathfrak{A}$, we certainly have $n \leq \operatorname{grade}(\mathfrak{A}, M)$. To prove the reverse inequality, put $\overline{M} = M/\sum_{j=1}^{n} x_j M$ and note that $\mathfrak{a}$ consists of zero divisors on the R-module $\overline{M}$. By Eisenbud [54, Theorem 3.1(b)], $\mathfrak{a} \subset \bigcup_{\mathfrak{Q} \in \operatorname{Ass}_R(\overline{M})} \mathfrak{Q} \cap R^{\mathcal{G}}$, where $\operatorname{Ass}_R(\overline{M})$ is the (finite) set of associated primes of $\overline{M}$. By “prime avoidance” [54, Lemma 3.3], $\mathfrak{a} \subset \mathfrak{Q} \cap R^{\mathcal{G}}$ for some $\mathfrak{Q} \in \operatorname{Ass}_R(\overline{M})$. But then $\underline{x}$ is a maximal M-regular sequence in $\mathfrak{Q}$; so $n = \operatorname{grade}(\mathfrak{Q}, M)$. By Lying Over for the integral extension $R^{\mathcal{G}}/\mathfrak{a} \hookrightarrow R/\mathfrak{A}$, there exists a prime $\mathfrak{P} \in \operatorname{Spec} R$ with $\mathfrak{P} \supseteq \mathfrak{A}$ such that $\mathfrak{Q} \cap R^{\mathcal{G}} = \mathfrak{P} \cap R^{\mathcal{G}}$, and by [22, Théorème V.2.2(i)], $g(\mathfrak{P}) = \mathfrak{Q}$ for some $g \in \mathcal{G}$. Hence, $\operatorname{grade}(\mathfrak{Q}, M) = \operatorname{grade}(\mathfrak{P}, M) \geq \operatorname{grade}(\mathfrak{A}, M)$ and so $n \geq \operatorname{grade}(\mathfrak{A}, M)$. This completes the proof. □

We note the following consequence of Lemma 8.5.3. For a more general ring theoretic result, see Kemper [108, Proposition 1.17].

Proposition 8.5.4. *Let $\mathcal{G}$ be a finite group acting by automorphisms on the commutative ring R and assume that R is noetherian as $R^{\mathcal{G}}$-module. Let M be a finitely generated left module over the skew group ring $R\#\mathcal{G}$. Then M is Cohen-Macaulay as R-module if and only if M is Cohen-Macaulay as $R^{\mathcal{G}}$-module.*

Proof. Recall from (8.3) that the primes $\mathfrak{p} \in \operatorname{Spec} R^{\mathcal{G}}$ with $\mathfrak{p} \supseteq \operatorname{ann}_{R^{\mathcal{G}}} M$ are precisely the primes of the form $\mathfrak{p} = \mathfrak{P} \cap R^{\mathcal{G}}$ with $\mathfrak{P} \in \operatorname{Spec} R$, $\mathfrak{P} \supseteq \operatorname{ann}_R M$. Now, as was noted in the first paragraph of 8.4, M is Cohen-Macaulay as R-module if and only if $\operatorname{grade}(\mathfrak{P}, M) = \operatorname{height}(\mathfrak{P}, M)$ holds for all $\mathfrak{P} \in \operatorname{Spec} R$ with $\mathfrak{P} \supseteq$

$\operatorname{ann}_R M$, and similarly for ${}_{R^{\mathfrak{g}}}M$. Thus, it suffices to invoke Lemma 8.5.3 to finish the proof. □

8.6 The Ellingsrud-Skjelbred Spectral Sequences

In this section, we describe two important spectral sequences, (8.6) and (8.7) below, that were constructed by Ellingsrud and Skjelbred in [55]. Both sequences are incarnations of a general spectral sequence due to Grothendieck. A standard tool in homological algebra, Grothendieck's spectral sequence establishes a relationship between the derived functors of two (covariant) functors $G\colon \mathsf{A} \to \mathsf{B}$ and $F\colon \mathsf{B} \to \mathsf{C}$ and of their composition $FG\colon \mathsf{A} \to \mathsf{C}$. The result holds for abelian categories A, B, C such that A and B have enough injectives (i.e., every object embeds into an injective object). The latter hypothesis makes it possible to define the right derived functors R^nF, R^nG and $R^n(FG)$ $(n \geq 0)$ via injective resolutions, as sketched in 8.3 for the case of torsion functors. For our purposes it suffices to think of the categories involved as categories of modules over some rings. The original source for Grothendieck's result is [77, Theorem 2.4.1]. Proofs can also be found in most modern texts on homological algebra, e.g., Weibel [224, 5.8.3].

Theorem 8.6.1 (Grothendieck)**.** *Let $G\colon \mathsf{A} \to \mathsf{B}$ and $F\colon \mathsf{B} \to \mathsf{C}$ be functors such that F is left exact and, for each injective object I of A, the object $G(I)$ of B is F-acyclic (i.e., $R^nF(G(I)) = 0$ for all $n > 0$). Then, for each object A of A, there exists a first quadrant cohomology spectral sequence*

$$E_2^{p,q} = (R^pF)(R^qG)(A) \Longrightarrow R^{p+q}(FG)(A)$$

Spelled out in more detail, the theorem asserts the existence of a family $E_r^{p,q}$ $(r \geq 2, p, q \in \mathbb{Z})$ of objects of C so that $E_r^{p,q} = 0$ if $p < 0$ or $q < 0$. The initial term $E_2 = \{E_2^{p,q}\}$ has the form as stated. Each E_r is equipped with a differential $d_r = \{d_r^{p,q}\}$ of bi-degree $(r, -r+1)$; so $d_r^{p,q} : E_r^{p,q} \to E_r^{p+r,q-r+1}$ and $d_r d_r = 0$; see Fig. 8.2.

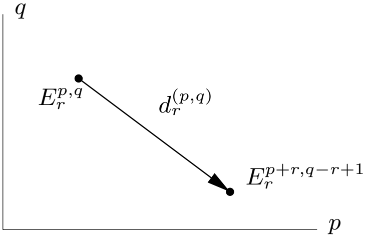

Fig. 8.2. E_r-page

The term E_{r+1} is the homology of E_r with respect to d_r:

$$E_{r+1}^{p,q} = \operatorname{Ker} d_r^{p,q} / \operatorname{Im} d_r^{p-r,q-1+r} \ . \tag{8.5}$$

Since the $E_r^{p,q}$ vanish outside the first quadrant $p, q \geq 0$, it follows that $E_r^{p,q} = E_{r+1}^{p,q} = \cdots$ if $r > \max\{p, q+1\}$. This stable value of $\{E_r^{p,q}\}$ is denoted by $E_\infty^{p,q}$. The $E_\infty^{p,q}$ with $p + q = n$ form the slices of a filtration of $R^n(FG)(A)$: there is a chain

$$0 = \mathfrak{F}^{n+1}R^n(FG)(A) \subseteq \mathfrak{F}^n R^n(FG)(A) \subseteq \cdots \subseteq \mathfrak{F}^0 R^n(FG)(A) = R^n(FG)(A)$$

of subobjects of $R^n(FG)(A)$ in C such that $E_\infty^{p,q} \cong \mathfrak{F}^p R^n(FG)(A)$.

To construct the Ellingsrud-Skjelbred spectral sequences, let S denote a commutative noetherian ring, $\mathcal{G}$ a finite group and $S[\mathcal{G}]$ the group ring of $\mathcal{G}$ over S. Fix an ideal $\mathfrak{a}$ of S and consider the following compositions of functors:

$$S[\mathcal{G}]\text{-}\mathsf{Mod} \xrightarrow{(\,.\,)^{\mathcal{G}}} S\text{-}\mathsf{Mod} \xrightarrow{\Gamma_{\mathfrak{a}}} S\text{-}\mathsf{Mod}$$

and

$$S[\mathcal{G}]\text{-}\mathsf{Mod} \xrightarrow{\Gamma_{\mathfrak{a}}} S[\mathcal{G}]\text{-}\mathsf{Mod} \xrightarrow{(\,.\,)^{\mathcal{G}}} S\text{-}\mathsf{Mod}\ .$$

Here, $(\,.\,)^{\mathcal{G}}$ is the functor of $\mathcal{G}$-fixed points and $\Gamma_{\mathfrak{a}}$ is the torsion functor associated to $\mathfrak{a}$; see 8.3. Viewing $S[\mathcal{G}]$-Mod as a subcategory of S-Mod via $S \subseteq S[\mathcal{G}]$, $\Gamma_{\mathfrak{a}}$ restricts to a functor $S[\mathcal{G}]$-$\mathsf{Mod} \to S[\mathcal{G}]$-$\mathsf{Mod}$. Clearly, the above compositions are identical: $\Gamma_{\mathfrak{a}}(M^{\mathcal{G}}) = \Gamma_{\mathfrak{a}}(M)^{\mathcal{G}}$ holds for any $S[\mathcal{G}]$-module M. Following Ellingsrud and Skjelbred [55] we let $H_{\mathfrak{a}}^n(\mathcal{G}, \,.\,)$ denote the n^{th} right derived functor of this composite functor. Moreover, as usual, $H^n(\mathcal{G}, \,.\,) = R^n(\,.\,)^{\mathcal{G}}$ and $H_{\mathfrak{a}}^n = R^n\Gamma_{\mathfrak{a}}$. Thus, subject to certain technical hypotheses which we will verify below, Theorem 8.6.1 yields two first quadrant cohomology spectral sequences for each $S[\mathcal{G}]$-module M:

$$E_2^{p,q} = H_{\mathfrak{a}}^p(H^q(\mathcal{G}, M)) \Longrightarrow H_{\mathfrak{a}}^{p+q}(\mathcal{G}, M) \tag{8.6}$$

and

$$\mathcal{E}_2^{p,q} = H^p(\mathcal{G}, H_{\mathfrak{a}}^q(M)) \Longrightarrow H_{\mathfrak{a}}^{p+q}(\mathcal{G}, M)\ . \tag{8.7}$$

It remains to check the hypotheses of Theorem 8.6.1: Left exactness of $\Gamma_{\mathfrak{a}}$ on S-Mod and of $(\,.\,)^{\mathcal{G}}$ on $S[\mathcal{G}]$-Mod are standard and easy. The following lemma takes care of the acyclicity hypothesis for injective $S[\mathcal{G}]$-modules.

Lemma 8.6.2. *Let I be an injective left $S[\mathcal{G}]$-module. Then:*

(a) *$I^{\mathcal{G}}$ is an injective S-module. In particular, $H_{\mathfrak{a}}^n(I^{\mathcal{G}}) = 0$ $(n > 0)$.*
(b) *$\Gamma_{\mathfrak{a}}(I)$ is an injective $S[\mathcal{G}]$-module; so $H^n(\mathcal{G}, \Gamma_{\mathfrak{a}}(I)) = 0$ $(n > 0)$.*

Proof. (a) We may view S-modules as $S[\mathcal{G}]$-modules by pulling back along the augmentation map $\varepsilon\colon S[\mathcal{G}] \to S$, $\varepsilon(\sum_{g\in\mathcal{G}} s_g g) = \sum_{g\in\mathcal{G}} s_g$. Consider the "co-induced" S-module $\mathrm{Hom}_{S[\mathcal{G}]}(S, I)$; it is isomorphic to the module of $\mathcal{G}$-fixed points $I^{\mathcal{G}}$, via $f \mapsto f(1)$. Thus, we have natural isomorphism of functors on S-Mod,

$$\mathrm{Hom}_{S[\mathcal{G}]}(\,.\,, I) \cong \mathrm{Hom}_S(\,.\,, I^{\mathcal{G}})\ ;$$

see, e.g., Brown [31, III(3.6)]. Since I is injective, the functor $\mathrm{Hom}_{S[G]}(\,.\,, I)$ is exact, and hence $\mathrm{Hom}_S(\,.\,, I^{\mathcal{G}})$ is an exact functor on S-Mod. In other words, $I^{\mathcal{G}}$ is an injective S-module. The fact that $H^n_{\mathfrak{a}}(I^{\mathcal{G}}) = 0$ for all $n > 0$ is now an immediate consequence of the definition of right derived functors via injective resolutions.

(b) By Baer's criterion (e.g., Weibel [224, 2.3.1]), it is enough to show that for every left ideal J of $S[\mathcal{G}]$ and every $S[\mathcal{G}]$-map $f\colon J \to \Gamma_{\mathfrak{a}}(I)$, there exists an element $m \in \Gamma_{\mathfrak{a}}(I)$ such that $f(x) = xm$ holds for all $x \in J$. Since I is injective, there certainly exists an element $m' \in I$ such that $f(x) = xm'$ for all $x \in J$. Moreover, since S is noetherian, J is finitely generated as S-module, and hence so is $f(J) \subseteq \Gamma_{\mathfrak{a}}(I)$. Therefore, there exist a positive integer r such that $\mathfrak{a}^r f(J) = 0$. Further, $f(J)$ is a submodule of the finitely generated S-module $S[\mathcal{G}]m'$. By the Artin-Rees Lemma [21, Cor. 1 to Thm. III.3.1], there exists a positive integer t such that for all $n \geq 0$,

$$\mathfrak{a}^{n+t} S[\mathcal{G}]m' \cap f(J) = \mathfrak{a}^n \left(\mathfrak{a}^t S[\mathcal{G}]m' \cap f(J)\right) \subseteq \mathfrak{a}^n f(J)\,.$$

Therefore, $\mathfrak{a}^{r+t} S[\mathcal{G}]m' \cap f(J) = 0$. This allows us to extend f to $\widetilde{f}\colon \mathfrak{a}^{r+t}S[\mathcal{G}] + J \to \Gamma_{\mathfrak{a}}(I)$ by defining $\widetilde{f}(x + x') = x'm'$ for all $x \in \mathfrak{a}^{r+t}S[\mathcal{G}]$ and $x' \in J$. Indeed, if $x + x' = y + y'$ with $x, y \in \mathfrak{a}^{r+t}S[\mathcal{G}]$ and $x', y' \in J$ then $(x - y)m' = (y' - x')m' \in \mathfrak{a}^{r+t}S[\mathcal{G}]m' \cap f(J) = 0$; so $x'm' = y'm'$. Once again we use injectivity of I to find $m \in I$ such that $\widetilde{f}(z) = zm$ holds for all $z \in \mathfrak{a}^{r+t}S[\mathcal{G}] + J$. If $z \in \mathfrak{a}^{r+t}$ then $zm = \widetilde{f}(z) = \widetilde{f}(z + 0) = 0$. Therefore, $m \in \Gamma_{\mathfrak{a}}(I)$, as required. This completes the proof that $\Gamma_{\mathfrak{a}}(I)$ is an injective $S[\mathcal{G}]$-module. As in (a), it follows that $H^n(\mathcal{G}, \Gamma_{\mathfrak{a}}(I)) = 0$ for all $n > 0$. □

8.7 Annihilators of Cohomology Classes

We continue to assume that R is a commutative ring and $\mathcal{G}$ a finite group acting on R. Moreover, M will denote a left module over the skew group ring $R\#\mathcal{G}$. Later on we will focus on the case where $M = R$ is the canonical $R\#\mathcal{G}$-module; see 5.3. For each $r \in R^{\mathcal{G}}$, the map $M \to M$, $m \mapsto rm$, is $\mathcal{G}$-equivariant and hence it induces a map on cohomology $r\cdot\colon H^*(\mathcal{G}, M) \to H^*(\mathcal{G}, M)$. In this way, $H^*(\mathcal{G}, M) = \bigoplus_{n\geq 0} H^n(\mathcal{G}, M)$ becomes a module over $R^{\mathcal{G}}$. Our goal in this section is to give height estimate for the annihilator $\operatorname{ann}_{R^{\mathcal{G}}}(x)$ of an element $x \in H^*(\mathcal{G}, M)$.

We need a technical lemma. Recall that $I_{\mathcal{G}}(\mathfrak{P}) = \{g \in \mathcal{G} \mid g(r) - r \in \mathfrak{P}\,\forall r \in R\}$ denotes the inertia group of the prime ideal $\mathfrak{P} \in \operatorname{Spec} R$ and $R^{\mathcal{G}}_{\mathcal{H}}$ is the image of the relative trace map $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}\colon R^{\mathcal{H}} \to R^{\mathcal{G}}$ for a subgroup $\mathcal{H} \leq \mathcal{G}$; see 8.5. Furthermore, as usual, we write ${}^g\mathcal{H} = g\mathcal{H}g^{-1}$ for $g \in \mathcal{G}$.

Lemma 8.7.1. *For any prime ideal* $\mathfrak{P} \in \operatorname{Spec} R$*,*

$$\mathfrak{P} \supseteq R^{\mathcal{G}}_{\mathcal{H}} \iff [I_{\mathcal{G}}(\mathfrak{P}) : I_{{}^g\mathcal{H}}(\mathfrak{P})] \in \mathfrak{P} \quad \textit{for all } g \in \mathcal{G}$$

Proof. The implication $\Leftarrow$ is a consequence of the identity

$$\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r) \equiv \sum_{g \in I_{\mathcal{G}}(\mathfrak{P})\backslash\mathcal{G}/\mathcal{H}} [I_{\mathcal{G}}(\mathfrak{P}) : I_{{}^g\mathcal{H}}(\mathfrak{P})]\, g(r) \mod \mathfrak{P} \tag{8.8}$$

for $r \in R^{\mathcal{H}}$. To prove this formula, write $\mathcal{G}$ as a disjoint union $\mathcal{G} = \coprod_g I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}$ with g running over $I_{\mathcal{G}}(\mathfrak{P})\backslash\mathcal{G}/\mathcal{H}$, and for each g, let $I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}/\mathcal{H}$ be a set of the coset representatives of $\mathcal{H}$ in the double coset $I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}$. Then, modulo $\mathfrak{P}$,

$$\begin{aligned} \operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r) &= \sum_{g \in I_{\mathcal{G}}(\mathfrak{P})\backslash\mathcal{G}/\mathcal{H}} \; \sum_{g' \in I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}/\mathcal{H}} g'(r) \\ &\equiv \sum_{g \in I_{\mathcal{G}}(\mathfrak{P})\backslash\mathcal{G}/\mathcal{H}} |I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}/\mathcal{H}| g(r) \mod \mathfrak{P} \end{aligned}$$

where the last $\equiv$ holds because each g' has the form $g' = fgh$ with $f \in I_{\mathcal{G}}(\mathfrak{P})$ and $h \in \mathcal{H}$, and so $g'(r) \equiv g(r) \mod \mathfrak{P}$. Finally, $|I_{\mathcal{G}}(\mathfrak{P})g\mathcal{H}/\mathcal{H}| = [I_{\mathcal{G}}(\mathfrak{P}) : I_{{}^g\mathcal{H}}(\mathfrak{P})]$, which proves equation (8.8).

For $\Rightarrow$, assume that $\mathfrak{P} \supseteq R^{\mathcal{G}}_{\mathcal{H}}$. Note that $R^{\mathcal{G}}_{\mathcal{H}} = R^{\mathcal{G}}_{{}^g\mathcal{H}}$ for all $g \in \mathcal{G}$, since $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r) = \operatorname{tr}_{\mathcal{G}/{}^g\mathcal{H}}(g(r))$ holds for all $r \in R^{\mathcal{H}}$. Thus, it suffices to show that $[I_{\mathcal{G}}(\mathfrak{P}) : I_{\mathcal{H}}(\mathfrak{P})] \in \mathfrak{P}$. To simplify notation, put $\mathcal{I} = I_{\mathcal{G}}(\mathfrak{P}))$ and let $\mathcal{P}$ denote a Sylow p-subgroup of $\mathcal{I} \cap \mathcal{H} = I_{\mathcal{H}}(\mathfrak{P})$, where p is the characteristic of the field $K = \operatorname{Fract}(R/\mathfrak{P})$. (We let $\mathcal{P} = \{1\}$ if $p = 0$.) Then our desired conclusion, $[\mathcal{I} : \mathcal{I} \cap \mathcal{H}] \in \mathfrak{P}$, is equivalent to

$$[\mathcal{I} : \mathcal{P}] \in \mathfrak{P} \,.$$

Furthermore, our assumption $\mathfrak{P} \supseteq R^{\mathcal{G}}_{\mathcal{H}}$ implies that $\mathfrak{P} \supseteq R^{\mathcal{G}}_{\mathcal{P}}$, because $\operatorname{tr}_{\mathcal{G}/\mathcal{P}} = \operatorname{tr}_{\mathcal{G}/\mathcal{H}} \operatorname{tr}_{\mathcal{H}/\mathcal{P}}$. Thus, leaving $\mathcal{H}$ for $\mathcal{P}$, we may assume that $\mathcal{H} = \mathcal{P}$ is a p-subgroup of $\mathcal{I}$.

Let $\mathcal{D} = \{g \in \mathcal{G} \mid g(\mathfrak{P}) = \mathfrak{P}\}$ denote the decomposition group of $\mathfrak{P}$; so $\mathcal{I} \leq \mathcal{D}$. We claim that

$$\mathfrak{P} \supseteq R^{\mathcal{D}}_{\mathcal{P}} \,.$$

To see this, choose $r \in \bigcap_{g \in \mathcal{G}\backslash\mathcal{D}} g(\mathfrak{P})$ with $r \notin \mathfrak{P}$. Then $s = \prod_{g \in \mathcal{D}} g(r)$ also belongs to $\bigcap_{g \in \mathcal{G}\backslash\mathcal{D}} g(\mathfrak{P})$ but not to $\mathfrak{P}$ and, in addition, $s \in R^{\mathcal{D}}$. Now assume that, contrary to our claim, there exists an element $f \in R^{\mathcal{P}}$ so that $\operatorname{tr}_{\mathcal{D}/\mathcal{P}}(f) \notin \mathfrak{P}$. Then $\operatorname{tr}_{\mathcal{D}/\mathcal{P}}(sf) = s \operatorname{tr}_{\mathcal{D}/\mathcal{P}}(f) \in \bigcap_{g \in \mathcal{G}\backslash\mathcal{D}} g(\mathfrak{P}) \setminus \mathfrak{P}$. Hence $\operatorname{tr}_{\mathcal{G}/\mathcal{P}}(sf) \notin \mathfrak{P}$, contradicting the fact that $\mathfrak{P} \supseteq R^{\mathcal{G}}_{\mathcal{P}}$.

By the claim, we may replace $\mathcal{G}$ by $\mathcal{D}$, thereby reducing to the case where $\mathfrak{P}$ is $\mathcal{G}$-stable. (Note that $\mathcal{I}$ is untouched by this replacement.) So $\mathcal{G}$ acts on $R/\mathfrak{P}$ with kernel $\mathcal{I}$, $\mathcal{P}$ is a p-subgroup of $\mathcal{I}$, and $R^{\mathcal{G}}_{\mathcal{P}} \subseteq \mathfrak{P}$. Thus,

$$0 \equiv \operatorname{tr}_{\mathcal{G}/\mathcal{P}}(r) = \left(\operatorname{tr}_{\mathcal{G}/\mathcal{I}} \circ \operatorname{tr}_{\mathcal{I}/\mathcal{P}}\right)(r) \equiv [\mathcal{I} : \mathcal{P}] \cdot \sum_{g \in \mathcal{G}/\mathcal{I}} g(r) \mod \mathfrak{P}$$

holds for all $r \in R^{\mathcal{P}}$. Our desired conclusion, $[\mathcal{I} : \mathcal{P}] \in \mathfrak{P}$, will follow if we can show that $\sum_{g \in \mathcal{G}/\mathcal{I}} g(r) \notin \mathfrak{P}$ holds for some $r \in R^{\mathcal{P}}$. But $\sum_{g \in \mathcal{G}/\mathcal{I}} g$ induces a nonzero endomorphism on $R/\mathfrak{P}$, by linear independence of automorphisms of $K = \operatorname{Fract}(R/\mathfrak{P})$; see [27, Théorème V.6.1]. In other words, $\sum_{g \in \mathcal{G}/\mathcal{I}} g(s) \notin \mathfrak{P}$ for some $s \in R$. Putting $r = \prod_{h \in \mathcal{P}} h(s)$, we have $r \in R^{\mathcal{P}}$ and $r \equiv s^{|\mathcal{P}|} \mod \mathfrak{P}$. Since

$|\mathcal{P}|$ is 1 or a power of $p = \operatorname{char} K$, we obtain $\sum_{g\in\mathcal{G}/\mathcal{I}} g(r) \equiv \sum_{g\in\mathcal{G}/\mathcal{I}} g(s^{|\mathcal{P}|}) \equiv \left(\sum_{g\in\mathcal{G}/\mathcal{I}} g(s)\right)^{|\mathcal{P}|} \not\equiv 0 \mod \mathfrak{P}$, as required. This completes the proof of the lemma. □

We are now ready to give the announced height estimate. Recall that, for any subgroup $\mathcal{H} \leq \mathcal{G}$, $\mathcal{H} \subseteq I_{\mathcal{G}}(\mathfrak{P})$ is equivalent to $\mathfrak{P} \supseteq I_R(\mathcal{H})$, where $I_R(\mathcal{H})$ is the ideal of R defined in (4.6).

Proposition 8.7.2. (a) *For each subgroup $\mathcal{H}$ of $\mathcal{G}$, the ideal $R^{\mathcal{G}}_{\mathcal{H}}$ of $R^{\mathcal{G}}$ annihilates the kernel of the restriction map $\operatorname{res}^{\mathcal{G}}_{\mathcal{H}}\colon H^*(\mathcal{G}, M) \to H^*(\mathcal{H}, M)$.*
(b) *For any $x \in H^*(\mathcal{G}, M)$,*

$$\operatorname{height} \operatorname{ann}_{R^{\mathcal{G}}}(x) \geq \inf\{\operatorname{height} I_R(\mathcal{H}) \mid \mathcal{H} \leq \mathcal{G}, \operatorname{res}^{\mathcal{G}}_{\mathcal{H}}(x) \neq 0\} \ .$$

Proof. (a) The action of $R^{\mathcal{G}} = H^0(\mathcal{G}, R)$ on $H^*(\mathcal{G}, M)$ can be interpreted as the cup product

$$H^0(\mathcal{G}, R) \times H^*(\mathcal{G}, M) \xrightarrow{\cup} H^*(\mathcal{G}, R \otimes_{\mathbb{Z}} M) \xrightarrow{\cdot} H^*(\mathcal{G}, M) \ ,$$

where the map denoted by $\cdot$ comes from the $\mathcal{G}$-equivariant map $R \otimes_{\mathbb{Z}} M \to M$, $r \otimes m \mapsto rm$; see, e.g., Brown [31, Exerc. V.4.1]. Furthermore, the relative trace map $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}$ is identical with the corestriction map $\operatorname{cor}^{\mathcal{G}}_{\mathcal{H}}\colon H^0(\mathcal{H}, R) \to H^0(\mathcal{G}, R)$; cf. [31, p. 81]. The transfer formula for cup products [31, V(3.8)] gives

$$\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r)x = \cdot\left(\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r) \cup x\right) = \cdot\left(\operatorname{cor}^{\mathcal{G}}_{\mathcal{H}}(r \cup \operatorname{res}^{\mathcal{G}}_{\mathcal{H}}(x))\right)$$

for $r \in R^{\mathcal{H}}$ and $x \in H^*(\mathcal{G}, M)$. Therefore, if $\operatorname{res}^{\mathcal{G}}_{\mathcal{H}}(x) = 0$ then $\operatorname{tr}_{\mathcal{G}/\mathcal{H}}(r)x = 0$.

(b) Put $\mathfrak{X} = \{\mathcal{H} \leq \mathcal{G} \mid \operatorname{res}^{\mathcal{G}}_{\mathcal{H}}(x) = 0\}$. By (a), $R^{\mathcal{G}}_{\mathcal{H}} \subseteq \operatorname{ann}_{R^{\mathcal{G}}}(x)$ for all $\mathcal{H} \in \mathfrak{X}$. To prove (b), we may assume that $\operatorname{ann}_{R^{\mathcal{G}}}(x)$ is a proper ideal of $R^{\mathcal{G}}$; for, otherwise $\operatorname{height} \operatorname{ann}_{R^{\mathcal{G}}}(x) = \infty$. Let $\mathfrak{p}$ be any prime ideal of $R^{\mathcal{G}}$ with $\mathfrak{p} \supseteq \operatorname{ann}_{R^{\mathcal{G}}}(x)$ and let $\mathfrak{P}$ be a prime of R lying over $\mathfrak{p}$. Then $\operatorname{height} \mathfrak{P} = \operatorname{height} \mathfrak{p}$, by Lemma 8.5.3(a), and

$$R^{\mathcal{G}}_{\mathcal{H}} \subseteq \mathfrak{P} \quad \text{for all } \mathcal{H} \in \mathfrak{X}.$$

By Lemma 8.7.1, the above inclusion implies that

$$[I_{\mathcal{G}}(\mathfrak{P}) : I_{\mathcal{H}}(\mathfrak{P})] \in \mathfrak{P} \quad \text{for all } \mathcal{H} \in \mathfrak{X} \ .$$

Put $p = \operatorname{char} \operatorname{Fract}(R/\mathfrak{P})$ and let $\mathcal{P} \leq I_{\mathcal{G}}(\mathfrak{P})$ be a Sylow p-subgroup of $I_{\mathcal{G}}(\mathfrak{P})$. (Again, $\mathcal{P} = \{1\}$ if $p = 0$.) Then $I_R(\mathcal{P}) \subseteq \mathfrak{P}$ and $[I_{\mathcal{G}}(\mathfrak{P}) : \mathcal{P}] \notin \mathfrak{P}$. Hence, $\mathcal{P} \notin \mathfrak{X}$ and $\operatorname{height} I_R(\mathcal{P}) \leq \operatorname{height} \mathfrak{P} = \operatorname{height} \mathfrak{p}$. This implies (b). □

8.8 The Restriction Map for Cohen-Macaulay Invariants

Let R denote a commutative ring and let $\mathcal{G}$ a finite group acting by automorphisms on R. We are now ready to construct our main ring theoretic tool for the investigation of the Cohen-Macaulay problem for $R^{\mathcal{G}}$.

Recall from Section 4.5 that an element $g \in \mathcal{G}$ acts as a *k-reflection* on R if g belongs to the inertia group $I_{\mathcal{G}}(\mathfrak{P})$ of some prime ideal $\mathfrak{P} \in \operatorname{Spec} R$ with height $\mathfrak{P} \leq k$ or, equivalently, if height $I_R(g) \leq k$; see (4.7). Put

$$\mathfrak{X}_k = \{\mathcal{H} \leq \mathcal{G} \mid \operatorname{height} I_R(\mathcal{H}) \leq k\} \ . \tag{8.9}$$

Thus, each $\mathcal{H} \in \mathfrak{X}_k$ consists of k-reflections on R.

Theorem 8.8.1. *Assume that R and $R^{\mathcal{G}}$ are both Cohen-Macaulay and that R is noetherian as $R^{\mathcal{G}}$-module. If $H^i(\mathcal{G}, R) = 0$ for $0 < i < k$ then the restriction map*

$$\operatorname{res}^{\mathcal{G}}_{\mathfrak{X}_{k+1}} : H^k(\mathcal{G}, R) \to \prod_{\mathcal{H} \in \mathfrak{X}_{k+1}} H^k(\mathcal{H}, R)$$

is injective.

Proof. We may assume that $H^k(\mathcal{G}, R) \neq 0$. Let $x \in H^k(\mathcal{G}, R)$ be nonzero and put $\mathfrak{a} = \operatorname{ann}_{R^{\mathcal{G}}}(x)$. It suffices to show that

$$\operatorname{grade} \mathfrak{a} \leq k+1 \ . \tag{8.10}$$

Indeed, grade $\mathfrak{a}$ = height $\mathfrak{a}$, since $R^{\mathcal{G}}$ is Cohen-Macaulay. Thus, (8.10) in conjunction with Proposition 8.7.2(b) implies that $k+1 \geq \operatorname{height} I_R(\mathcal{H})$ for some $\mathcal{H} \leq \mathcal{G}$ with $\operatorname{res}^{\mathcal{G}}_{\mathcal{H}}(x) \neq 0$. The proposition follows from this. Furthermore, R is Cohen-Macaulay as $R^{\mathcal{G}}$-module, by Proposition 8.5.4. Hence, $\operatorname{grade}(\mathfrak{a}, R) = \operatorname{height}(\mathfrak{a}, R)$ and, by definition, $\operatorname{height}(\mathfrak{a}, R) = \operatorname{height} \mathfrak{a}$. Therefore,

$$\operatorname{grade} \mathfrak{a} = \operatorname{grade}(\mathfrak{a}, R) \ . \tag{8.11}$$

To proceed, we use the Ellingsrud-Skjelbred spectral sequences (8.6) and (8.7) with $S = R^{\mathcal{G}}$ and $M = R$. Recall from (8.2) that $\operatorname{grade} \mathfrak{a} = \inf\{p \mid H^p_{\mathfrak{a}}(R^{\mathcal{G}}) \neq 0\}$ and from equation (8.6) that $H^p_{\mathfrak{a}}(R^{\mathcal{G}}) = E_2^{p,0}$. Thus, (8.10) will follow if we can show that

$$E_2^{k+1,0} \neq 0 \ . \tag{8.12}$$

But $E_2^{0,k} \neq 0$, since $x \in \Gamma_{\mathfrak{a}}(H^k(\mathcal{G}, R)) = E_2^{0,k}$. Moreover, by equation (8.5), $E_{r+1}^{0,k} = \operatorname{Ker} d_r^{0,k}$ for all $r \geq 2$, since the spectral sequence vanishes outside the first quadrant. Now, our hypothesis $H^q(\mathcal{G}, R) = 0$ for $0 < q < k$ yields that $E_2^{p,q} = 0$ for $0 < q < k$ and so $E_r^{p,q} = 0$ for $0 < q < k$ and all $r \geq 2$. Therefore, $d_r^{0,k} = 0$ if $r \neq k+1$. We conclude that $E_{k+1}^{0,k} = E_2^{0,k} \neq 0$ and $E_\infty^{0,k} = \operatorname{Ker} d_{k+1}^{0,k}$. Thus, in order to prove (8.12), it suffices to show that

$$E_\infty^{0,k} = 0 \ . \tag{8.13}$$

For, (8.13) implies that $d_{k+1}^{0,k}$ embeds $E_{k+1}^{0,k} \neq 0$ into $E_{k+1}^{k+1,0}$ (see Fig. 8.2) forcing the latter to be nonzero, and hence $E_2^{k+1,0} \neq 0$ as well.

Now suppose, for a contradiction, that (8.10) is false. Then, by (8.11) and (8.2), $H^q_{\mathfrak{a}}(R) = 0$ for all $q \leq k+1$. Invoking the $\mathcal{E}$-sequence (8.7) we have $\mathcal{E}_2^{p,q} = 0$ if $q \leq k+1$ and so $H^n_{\mathfrak{a}}(\mathcal{G}, R) = 0$ for $n \leq k+1$. Returning to E-sequence (8.6), we conclude that $E_\infty^{p,q} = 0$ if $p + q \leq k+1$, which in particular includes (8.13). This contradiction completes the proof of the theorem. □

Note that the vanishing hypothesis on $H^i(\mathcal{G}, R)$ is vacuous for $k = 1$. Thus, $H^1(\mathcal{G}, R)$ is detected by bireflections whenever R and $R^{\mathcal{G}}$ are both Cohen-Macaulay and R is noetherian as $R^{\mathcal{G}}$-module.

8.9 The Case of Multiplicative Invariants

For the remainder of this chapter, we will focus on the special case of multiplicative actions. Throughout, L will denote a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a finite group, and $\Bbbk[L]$ will be the group algebra of L over the commutative ring $\Bbbk$ with the usual multiplicative $\mathcal{G}$-action (3.2).

To set the stage, we begin with some basic observations:

(a) $\Bbbk[L]$ is Cohen-Macaulay if and only if the base ring $\Bbbk$ is Cohen-Macaulay.
(b) If the multiplicative invariant algebra $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay then $\Bbbk$ must be Cohen-Macaulay. Conversely, if $\Bbbk$ is Cohen-Macaulay and $|\mathcal{G}|$ is invertible in $\Bbbk$ then $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay.

Here, (a) follows from the general facts on Cohen-Macaulay rings mentioned in 8.4. The first assertion in (b) is a consequence of Proposition 8.4.1(a), since the invariant algebra $\Bbbk[L]^{\mathcal{G}}$ is free as $\Bbbk$-module by (3.4). Finally, the second assertion in (b) follows from Corollary 8.5.2, since the hypothesis of $|\mathcal{G}|$ amounts to the trace map $\operatorname{tr}_{\mathcal{G}} \colon \Bbbk[L] \to \Bbbk[L]^{\mathcal{G}}$ being surjective; see (5.6). Thus, our main interest will be in the case where $\Bbbk$ is Cohen-Macaulay but $|\mathcal{G}|$ is not invertible in $\Bbbk$. In fact, we will later concentrate on the case where the base ring $\Bbbk$ is $\mathbb{Z}$. This is justified in part by the following lemma.

Lemma 8.9.1. *The following are equivalent:*

(a) $\mathbb{Z}[L]^{\mathcal{G}}$ *is Cohen-Macaulay;*
(b) $\Bbbk[L]^{\mathcal{G}}$ *is Cohen-Macaulay whenever* $\Bbbk$ *is;*
(c) $\Bbbk[L]^{\mathcal{G}}$ *is Cohen-Macaulay for* $\Bbbk = \mathbb{Z}/|\mathcal{G}|\mathbb{Z}$*;*
(d) $\mathbb{F}_p[L]^{\mathcal{G}}$ *is Cohen-Macaulay for all primes* p *dividing* $|\mathcal{G}|$.

Proof. (a) $\Rightarrow$ (b): Assume that $\Bbbk$ is Cohen-Macaulay and put $S = \Bbbk[L]^{\mathcal{G}}$. By Proposition 8.4.1(a), applied to the free extension of rings $\Bbbk \hookrightarrow S$, we know that S is Cohen-Macaulay if (and only if) all fibres $S_{\mathfrak{P}}/\mathfrak{p}S_{\mathfrak{P}}$ are Cohen-Macaulay, where $\mathfrak{P} \in \operatorname{Spec} S$ and $\mathfrak{p} = \mathfrak{P} \cap \Bbbk$. But $S_{\mathfrak{P}}/\mathfrak{p}S_{\mathfrak{P}}$ is a localization of $Q(\Bbbk/\mathfrak{p}) \otimes_{\Bbbk} S \cong Q(\Bbbk/\mathfrak{p})[L]^{\mathcal{G}}$; see Proposition 3.3.1(b). Therefore, it suffices to show that $Q(\Bbbk/\mathfrak{p})[L]^{\mathcal{G}}$ is Cohen-Macaulay. In other words, we may assume that $\Bbbk$ is a field. By Bruns and Herzog [32, Theorem 2.1.10], we may further assume that $\Bbbk = \mathbb{F}_p$, because the case of characteristic 0 is trivial by observation (b) above. But $\mathbb{F}_p[L]^{\mathcal{G}} \cong \mathbb{Z}[L]^{\mathcal{G}}/(p)$ by Proposition 3.3.1(b). Since $\mathbb{Z}[L]^{\mathcal{G}}$ is assumed Cohen-Macaulay, [32, Theorem 2.1.3(a)] yields that $\mathbb{F}_p[L]^{\mathcal{G}}$ is Cohen-Macaulay, as desired.

(b) $\Rightarrow$ (c) is clear, since $\mathbb{Z}/|\mathcal{G}|\mathbb{Z}$ is Cohen-Macaulay (dimension 0).

(c) $\Rightarrow$ (d): Let $\Bbbk = \mathbb{Z}/|\mathcal{G}|\mathbb{Z}$ and write $|\mathcal{G}| = \prod_p p^{n_p}$ with $n_p \neq 0$. Then $(\mathbb{Z}/p^{n_p}\mathbb{Z})[L]^{\mathcal{G}}$ is a localization of $\Bbbk[L]^{\mathcal{G}}$, and hence $(\mathbb{Z}/p^{n_p}\mathbb{Z})[L]^{\mathcal{G}}$ is Cohen-Macaulay.

It follows from [32, Theorem 2.1.3(a)] that $\mathbb{Z}_{(p)}[L]^{\mathcal{G}}$ and $\mathbb{F}_p[L]^{\mathcal{G}} \cong \mathbb{Z}_{(p)}[L]^{\mathcal{G}}/(p)$ are Cohen-Macaulay.

(d) ⇒ (a): If p does not divide $|\mathcal{G}|$ then $\mathbb{F}_p[L]^{\mathcal{G}}$ is Cohen-Macaulay by observation (b) above. Therefore, (d) implies that $\mathbb{F}_p[L]^{\mathcal{G}}$ is Cohen-Macaulay for all primes p. Now let $\mathfrak{P}$ be a maximal ideal of $\mathbb{Z}[L]$. Then $\mathfrak{P} \cap \mathbb{Z} = (p)$ for some prime p and $\mathbb{Z}[L]^{\mathcal{G}}_{\mathfrak{P}}/(p)$ is a localization of $\mathbb{Z}[L]^{\mathcal{G}}/(p) = \mathbb{F}_p[L]^{\mathcal{G}}$. Thus, $\mathbb{Z}[L]^{\mathcal{G}}_{\mathfrak{P}}/(p)$ is Cohen-Macaulay and [32, Theorem 2.1.3(a)] further implies that $\mathbb{Z}[L]^{\mathcal{G}}_{\mathfrak{P}}$ is Cohen-Macaulay. Since $\mathfrak{P}$ was arbitrary, (a) follows. □

Since normal rings of Krull dimension at most 2 are Cohen-Macaulay, implication (d) ⇒ (b) of the lemma in particular yields the following corollary.

Corollary 8.9.2. *Assume that the lattice L has rank at most 2. Then $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay if and only if $\Bbbk$ is Cohen-Macaulay.*

Next, we show that the Cohen-Macaulay property of $\Bbbk[L]^{\mathcal{G}}$ only depends on the rational type of L, that is, the isomorphism class of $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$ as $\mathbb{Q}[\mathcal{G}]$-module.

Proposition 8.9.3. *If $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay then so is $\Bbbk[L']^{\mathcal{G}}$ for any $\mathcal{G}$-lattice L' that is rationally isomorphic to L.*

Proof. Assume that $L_{\mathbb{Q}} \cong L'_{\mathbb{Q}}$, say $L \supseteq L'$ and L/L' is finite. Then $\Bbbk[L]$ is finite over $\Bbbk[L']$ which in turn is integral over $\Bbbk[L']^{\mathcal{G}}$. Therefore, $\Bbbk[L]$ is integral over $\Bbbk[L']^{\mathcal{G}}$, and hence so is $\Bbbk[L]^{\mathcal{G}}$. In order to show that the Cohen-Macaulay property descends from $\Bbbk[L]^{\mathcal{G}}$ to $\Bbbk[L']^{\mathcal{G}}$, we will use Proposition 8.4.1(b). For the requisite Reynolds operator, consider the truncation map

$$\pi\colon \Bbbk[L] \longrightarrow \Bbbk[L'] , \quad \sum_{m \in L} k_m \mathbf{x}^m \mapsto \sum_{m \in L'} k_m \mathbf{x}^m .$$

This map is a Reynolds operator for the extension $\Bbbk[L] \supseteq \Bbbk[L']$ and $\pi(g(f)) = g(\pi(f))$ holds for all $g \in \mathcal{G}$, $f \in \Bbbk[L]$. Therefore, π restricts to a Reynolds operator $\Bbbk[L]^{\mathcal{G}} \longrightarrow \Bbbk[L']^{\mathcal{G}}$ and the proposition follows. □

The proposition in particular allows to reduce the general case of the Cohen-Macaulay problem for multiplicative invariants to the case of effective $\mathcal{G}$-lattices, that is, lattices L with $L^{\mathcal{G}} = 0$. Recall from §1.6.1 that, for any $\mathcal{G}$-lattice L, the quotient $L/L^{\mathcal{G}}$ is an effective $\mathcal{G}$-lattice.

Corollary 8.9.4. *$\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay if and only if this holds for $\Bbbk[L/L^{\mathcal{G}}]^{\mathcal{G}}$.*

Proof. By Proposition 8.9.3, we may replace L by $L' = L^{\mathcal{G}} \oplus L/L^{\mathcal{G}}$. But $\Bbbk[L']^{G} \cong \Bbbk[L/L^{\mathcal{G}}]^{\mathcal{G}} \otimes_{\Bbbk} \Bbbk[L^{\mathcal{G}}]$ is isomorphic to the group algebra of the lattice $L^{\mathcal{G}}$ over $\Bbbk[L/L^{\mathcal{G}}]^{\mathcal{G}}$. Thus, by observation (a) above, $\Bbbk[L']^{\mathcal{G}}$ is Cohen-Macaulay if and only if $\Bbbk[L/L^{\mathcal{G}}]^{\mathcal{G}}$ is Cohen-Macaulay. The corollary follows. □

8.10 Proof of Theorem 8.1.1

The proof of Theorem 8.1.1 is ultimately an application of Theorem 8.8.1. We will need some preliminary observations on isotropy groups $\mathcal{G}_m = \{g \in \mathcal{G} \mid g(m) = m\}$ of lattice elements $m \in L$ and on the nature of the restriction map considered in Theorem 8.1.1 in the special case of multiplicative actions.

8.10.1 Isotropy Groups

Recall that the group $\mathcal{G}$ is said to be *perfect* if $\mathcal{G}^{\mathrm{ab}} = \mathcal{G}/[\mathcal{G},\mathcal{G}] = 1$.

Proposition 8.10.1. *Assume that L is a faithful $\mathcal{G}$-lattice such that all minimal isotropy groups $1 \neq \mathcal{G}_m$ $(m \in L)$ are perfect. Then* $\operatorname{rank} L/L^{\mathcal{H}} \geq 8$ *holds for every subgroup* $1 \neq \mathcal{H} \leq \mathcal{G}$.

In the setting of multiplicative actions, the class of subgroups $\mathfrak{X}_k$ defined in (8.9) takes the form

$$\mathfrak{X}_k = \{\mathcal{H} \leq \mathcal{G} \mid \operatorname{rank} L/L^{\mathcal{H}} \leq k\}\ ; \tag{8.14}$$

see Lemma 4.5.1. Thus, the conclusion of Proposition 8.10.1 can also be stated as follows:

$$\mathfrak{X}_k = \{1\} \text{ for all } k < 8.$$

The proof of Proposition 8.10.1 depends on two lemmas the first of which is well-known. Recall that the $\mathcal{G}$-action on a module M is called *fixed-point-free* if $g(m) \neq m$ holds for all $0 \neq m \in M$ and $1 \neq g \in \mathcal{G}$.

Lemma 8.10.2. (a) *The set of isotropy groups $\{\mathcal{G}_m \mid m \in L\}$ is closed under conjugation and under taking intersections. The unique smallest member of the set is* $\operatorname{Ker}_{\mathcal{G}}(L) = \{g \in \mathcal{G} \mid g_L = \mathrm{Id}_L\}$.

(b) *If $\mathcal{G}_m$ $(m \in L)$ is a minimal isotropy group such that $\mathcal{G}_m \neq \operatorname{Ker}_{\mathcal{G}}(L)$ then $\mathcal{G}_m/\operatorname{Ker}_{\mathcal{G}}(L)$ acts fixed-point-freely on $L/L^{\mathcal{G}_m} \neq 0$.*

Proof. Both parts are in effect assertions about the $\mathbb{Q}[\mathcal{G}]$-module $V = L_{\mathbb{Q}}$, because the collection of isotropy groups $\mathcal{G}_m$ remains unchanged when allowing $m \in V$ and $\mathcal{G}$ acts fixed-point-freely on L if and only if it does so on V. Moreover, for any subgroup $\mathcal{H} \leq \mathcal{G}$, $L/L^{\mathcal{H}}$ is an $\mathcal{H}$-lattice with $L/L^{\mathcal{H}} \otimes_{\mathbb{Z}} \mathbb{Q} \cong V/V^{\mathcal{H}}$.

(a) The first assertion is clear, since ${}^g\mathcal{G}_m = \mathcal{G}_{g(m)}$ holds for all $g \in \mathcal{G}$ and $m \in V$. For the second assertion, let M be a non-empty subset of V and put $\mathcal{G}_M = \bigcap_{m \in M} \mathcal{G}_m$. We must show that $\mathcal{G}_M = \mathcal{G}_m$ for some $m \in V$. Put $W = V^{\mathcal{G}_M}$. If $g \in \mathcal{G} \setminus \mathcal{G}_M$ then $W^{\langle g \rangle} = \{w \in W \mid g(w) = w\}$ is a proper subspace of W, since some element of $M \subseteq W$ is not fixed by g. Any $m \in W \setminus \bigcup_{g \in \mathcal{G} \setminus \mathcal{G}_M} W^{\langle g \rangle}$ satisfies $\mathcal{G}_m = \mathcal{G}_M$. The statement about $\operatorname{Ker}_{\mathcal{G}}(L)$ is now clear, since $\operatorname{Ker}_{\mathcal{G}}(L) = \bigcap_{m \in L} \mathcal{G}_m$.

(b) Let $\mathcal{H} = \mathcal{G}_m$ be a minimal member of $\{\mathcal{G}_m \mid m \in V\} \setminus \{\operatorname{Ker}_{\mathcal{G}}(L)\}$; so $V^{\mathcal{H}} \neq V$. As $\mathbb{Q}[\mathcal{H}]$-modules, $V \cong V^{\mathcal{H}} \oplus V/V^{\mathcal{H}}$. If $0 \neq v \in V/V^{\mathcal{H}}$ then $\mathcal{H}_v = \mathcal{H} \cap \mathcal{G}_v \subsetneq \mathcal{H}$. In view of (a), our minimality assumption on $\mathcal{H}$ forces $\mathcal{H}_v = \operatorname{Ker}_{\mathcal{G}}(L)$. Thus, $\mathcal{H}/\operatorname{Ker}_{\mathcal{G}}(L)$ acts fixed-point-freely on $V/V^{\mathcal{H}}$. □

Lemma 8.10.3. *Assume that $\mathcal{G}$ is a nontrivial perfect group acting fixed-point-freely on the nonzero lattice L. Then $\mathcal{G}$ is isomorphic to the binary icosahedral group $2.\mathcal{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_5)$ and $\operatorname{rank} L$ is a multiple of 8.*

Proof. Put $V = L \otimes_{\mathbb{Z}} \mathbb{C}$, a nonzero fixed-point-free $\mathbb{C}[\mathcal{G}]$-module. By a well-known theorem of Zassenhaus (see Wolf [227, Theorem 6.2.1]), $\mathcal{G}$ is isomorphic to the binary icosahedral group $2.\mathcal{A}_5$ and the irreducible constituents of V are 2-dimensional. The binary icosahedral group has two irreducible complex representations of degree 2; they are Galois conjugates of each other and both have Frobenius-Schur indicator -1. We denote the corresponding $\mathbb{C}[\mathcal{G}]$-modules by V_1 and V_2. Both V_i occur with the same multiplicity in V, since V is defined over $\mathbb{Q}$. Thus, $V \cong (V_1 \oplus V_2)^m$ for some m and $\operatorname{rank} L = 4m$. We have to show that m is even. Since both V_i have indicator -1, it follows that $V_1 \oplus V_2$ is not defined over $\mathbb{R}$, whereas each V_i^2 is defined over $\mathbb{R}$; see Isaacs [96, 9.21]. Thus, letting $G_0(\mathbb{C}[\mathcal{G}])$ denote the Grothendieck group of the category of all finitely generated $\mathbb{C}[\mathcal{G}]$-modules and similarly for $\mathbb{R}[\mathcal{G}]$, the module $V_1 \oplus V_2$ represents an element x of order 2 in the cokernel of the scalar extension map $\mathbb{C}\otimes_{\mathbb{R}} \colon G_0(\mathbb{R}[\mathcal{G}]) \to G_0(\mathbb{C}[\mathcal{G}])$, and $mx = 0$. Therefore, m must be even, as desired. □

Proof of Proposition 8.10.1. Let $1 \neq \mathcal{H} \leq \mathcal{G}$ and put $\overline{\mathcal{H}} = \bigcap_{m \in L^{\mathcal{H}}} \mathcal{G}_m$. Then $\overline{\mathcal{H}} \supseteq \mathcal{H}$ and $L^{\overline{\mathcal{H}}} = L^{\mathcal{H}}$. Lemma 8.10.2(a) further implies that $\overline{\mathcal{H}} = \mathcal{G}_m$ for some m. Replacing $\mathcal{H}$ by $\overline{\mathcal{H}}$, we may assume that $\mathcal{H}$ is a nonidentity isotropy group. If $\mathcal{H}$ is not minimal then replace $\mathcal{H}$ by a smaller nonidentity isotropy group; this does not increase the value of $\operatorname{rank} L/L^{\mathcal{H}}$. Thus, we may assume that $\mathcal{H}$ is a minimal nonidentity isotropy group, and hence $\mathcal{H}$ is perfect. By Lemma 8.10.2(b), $\mathcal{H}$ acts fixed-point-freely on $L/L^{\mathcal{H}} \neq 0$ and Lemma 8.10.3 implies that $\operatorname{rank} L/L^{\mathcal{H}} \geq 8$, proving the proposition. □

8.10.2 The Restriction Map

Let $\mathfrak{X}$ denote any collection of subgroups of $\mathcal{G}$ that is closed under conjugation and under taking subgroups. We will give a reformulation of injectivity of the restriction map

$$\operatorname{res}^{\mathcal{G}}_{\mathfrak{X}} \colon H^k(\mathcal{G}, \Bbbk[L]) \to \prod_{\mathcal{H} \in \mathfrak{X}} H^k(\mathcal{H}, \Bbbk[L])$$

that was considered in Theorem 8.8.1 in the special case where $\mathfrak{X} = \mathfrak{X}_{k+1}$.

Lemma 8.10.4. *The map $\operatorname{res}^{\mathcal{G}}_{\mathfrak{X}} \colon H^k(\mathcal{G}, \Bbbk[L]) \to \prod_{\mathcal{H} \in \mathfrak{X}} H^k(\mathcal{H}, \Bbbk[L])$ is injective if and only if the restriction maps*

$$H^k(\mathcal{G}_m, \Bbbk) \to \prod_{\substack{\mathcal{H} \in \mathfrak{X} \\ \mathcal{H} \leq \mathcal{G}_m}} H^k(\mathcal{H}, \Bbbk)$$

are injective for all $m \in L$.

Proof. As $\mathcal{G}$-module,

$$\Bbbk[L] \cong \bigoplus_{m \in \mathcal{G}\backslash L} \Bbbk[\mathcal{G}/\mathcal{G}_m] ,$$

where $\mathcal{G}\backslash L$ is any transversal for the $\mathcal{G}$-orbits in L. If $\mathcal{H} \leq \mathcal{G}$ is any subgroup of $\mathcal{G}$ then

$$\Bbbk[\mathcal{G}/\mathcal{G}_m]{\downarrow}^{\mathcal{G}}_{\mathcal{H}} \cong \bigoplus_{g \in \mathcal{H}\backslash\mathcal{G}/\mathcal{G}_m} \Bbbk[\mathcal{H}/{}^g\mathcal{G}_m \cap \mathcal{H}] ;$$

see (1.14). Therefore, $\operatorname{res}^{\mathcal{G}}_{\mathcal{H}} \colon H^k(\mathcal{G}, \Bbbk[L]) \to H^k(\mathcal{H}, \Bbbk[L])$ is the direct sum of the restriction maps

$$H^k(\mathcal{G}, \Bbbk[\mathcal{G}/\mathcal{G}_m]) \to H^k(\mathcal{H}, \Bbbk[\mathcal{G}/\mathcal{G}_m]) = \bigoplus_{g \in \mathcal{H}\backslash\mathcal{G}/\mathcal{G}_m} H^k(\mathcal{H}, \Bbbk[\mathcal{H}/{}^g\mathcal{G}_m \cap \mathcal{H}]) .$$

Using the Eckmann-Shapiro Lemma (2.6), the latter map can be rewritten as follows:

$$\begin{array}{rcc} \rho_{\mathcal{H},m} \colon H^k(\mathcal{G}_m, \Bbbk) & \to & \displaystyle\bigoplus_{g \in \mathcal{H}\backslash\mathcal{G}/\mathcal{G}_m} H^k({}^g\mathcal{G}_m \cap \mathcal{H}, \Bbbk) \\ {[f]} & \mapsto & ([\underline{h} \mapsto f(g^{-1}\underline{h}g)])_g \end{array}$$

Here $[\,.\,]$ denotes the cohomology class of a k-cocycle and $\underline{h}$ stands for a k-tuple of elements of ${}^g\mathcal{G}_m \cap \mathcal{H}$. Therefore,

$$\operatorname{Ker} \rho_{\mathcal{H},m} = \bigcap_{g \in \mathcal{H}\backslash\mathcal{G}/\mathcal{G}_m} \operatorname{Ker} \left(\operatorname{res}^{\mathcal{G}_m}_{\mathcal{G}_m \cap \mathcal{H}^g} \colon H^k(\mathcal{G}_m, \Bbbk) \to H^k(\mathcal{G}_m \cap \mathcal{H}^g, \Bbbk) \right) .$$

Thus, $\operatorname{Ker} \operatorname{res}^{\mathcal{G}}_{\mathfrak{X}}$ is isomorphic to the direct sum of the kernels of the restriction maps

$$H^k(\mathcal{G}_m, \Bbbk) \to \prod_{\mathcal{H} \in \mathfrak{X}} H^k(\mathcal{G}_m \cap \mathcal{H}^g, \Bbbk)$$

with $m \in \mathcal{G}\backslash L$. Finally, by hypothesis on $\mathfrak{X}$, the groups $\mathcal{G}_m \cap \mathcal{H}^g$ with $\mathcal{H} \in \mathfrak{X}$ are exactly the groups $\mathcal{H} \in \mathfrak{X}$ with $\mathcal{H} \leq \mathcal{G}_m$. The lemma follows. □

8.10.3 The Proof

We are now ready to prove Theorem 8.1.1. Recall that, for any subgroup $\mathcal{H} \leq \mathcal{G}$, $\mathcal{R}^2(\mathcal{H})$ denotes the subgroup generated by the elements of $\mathcal{H}$ that act as bireflections on L or, equivalently, by the subgroups of $\mathcal{H}$ that belong to $\mathfrak{X}_2$; see (8.14). We assume that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay. Throughout, we let $\Bbbk = \mathbb{Z}/|\mathcal{G}|\mathbb{Z}$; so $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay as well, by Lemma 8.9.1.

We first show that $\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)$ is a perfect group for all $m \in L$. Indeed, Theorem 8.8.1 implies that the restriction $H^1(\mathcal{G}, \Bbbk[L]) \to \prod_{\mathcal{H} \in \mathfrak{X}_2} H^1(\mathcal{H}, \Bbbk[L])$ is injective. By Lemma 8.10.4, this says that all restrictions

$$H^1(\mathcal{G}_m, \Bbbk) \to \prod_{\substack{\mathcal{H} \in \mathfrak{X}_2 \\ \mathcal{H} \leq \mathcal{G}_m}} H^1(\mathcal{H}, \Bbbk)$$

are injective. Now, by our choice of $\Bbbk$, $H^1(\mathcal{H}, \Bbbk) = \mathrm{Hom}(\mathcal{H}^{\mathrm{ab}}, \Bbbk) \cong \mathcal{H}^{\mathrm{ab}}$ and similarly for $\mathcal{G}_m$. Therefore, injectivity of the above map is equivalent to $\mathcal{G}_m^{\mathrm{ab}}$ being generated by the images of all $\mathcal{H} \leq \mathcal{G}_m$ with $\mathcal{H} \in \mathfrak{X}_2$. In other words, $\mathcal{G}_m^{\mathrm{ab}}$ is generated by the image of $\mathcal{R}^2(\mathcal{G}_m)$, and hence, $\big(\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)\big)^{\mathrm{ab}}$ is trivial, as desired.

Now assume that $\mathcal{G}$ acts non-trivially on L. Our goal is to show that some isotropy group $\mathcal{G}_m$ is non-perfect. Suppose otherwise. Replacing $\mathcal{G}$ by $\mathcal{G}/\operatorname{Ker}_{\mathcal{G}}(L)$ we may assume that $1 \neq \mathcal{G}$ acts faithfully on L. Then $\mathfrak{X}_k = \{1\}$ for all $k < 8$, by Proposition 8.10.1. Put $\ell = \inf\{i > 0 \mid H^i(\mathcal{G}, \Bbbk[L]) \neq 0\}$ and suppose that $\ell < 7$. Then Theorem 8.8.1 implies that $0 \neq H^\ell(\mathcal{G}, \Bbbk[L])$ embeds into $\prod_{\mathcal{H} \in \mathfrak{X}_{\ell+1}} H^\ell(\mathcal{H}, \Bbbk[L])$ which is trivial, because $\mathfrak{X}_{\ell+1} = \{1\}$. This contradiction shows that $\ell \geq 7$. By the Eckmann-Shapiro Lemma (2.6) (or Lemma 8.10.4 with $\mathfrak{X} = \{1\}$), this says that

$$H^i(\mathcal{G}_m, \Bbbk) = 0 \text{ for all } m \in L \text{ and all } 0 < i < 7.$$

On the other hand, choosing $\mathcal{G}_m$ minimal with $\mathcal{G}_m \neq 1$, we know by Lemmas 8.10.2(b) and 8.10.3 that $\mathcal{G}_m$ is isomorphic to the binary icosahedral group $2.\mathcal{A}_5$. The cohomology of $2.\mathcal{A}_5$ is 4-periodic (see Brown [31, p. 155]). Hence, $H^3(\mathcal{G}_m, \Bbbk) \cong \widehat{H}^{-1}(\mathcal{G}_m, \Bbbk) = \mathrm{ann}_{\Bbbk}(\sum_{g \in \mathcal{G}_m} g) \cong \mathbb{Z}/|\mathcal{G}_m|\mathbb{Z} \neq 0$; see (2.2) for $\widehat{H}^{-1}$. This contradiction completes the proof of Theorem 8.1.1. □

8.11 Examples

Example 8.11.1 (Multiplicative $\mathcal{A}_n$-invariants of U_n)**.** Using the notation of Example 3.5.5, we restrict the $\mathcal{S}_n$-action on the standard permutation lattice U_n to the alternating group $\mathcal{A}_n$. Note that $\mathcal{A}_n$ acts as a bireflection group on U_n; this is easy to see directly and also follows from Proposition 1.7.1. Exactly as in Example 3.5.5, we have

$$\mathbb{Z}[U_n]^{\mathcal{A}_n} = \mathbb{Z}[x_1, \ldots, x_n]^{\mathcal{A}_n}[s_n^{-1}]\,,$$

where $s_n = \prod_1^n x_i$ is the n^{th} elementary symmetric function. The ring $\mathbb{Z}[x_1, \ldots, x_n]^{\mathcal{A}_n}$ of polynomial $\mathcal{A}_n$-invariants is known (Revoy [163], or see Smith [199, Theorem 1.3.5]):

$$\mathbb{Z}[x_1, \ldots, x_n]^{\mathcal{A}_n} = \mathbb{Z}[s_1, \ldots, s_n] \oplus d\mathbb{Z}[s_1, \ldots, s_n]\,,$$

where s_i is the i^{th} elementary symmetric function in $x_1, \ldots, x_n$ and

$$d = \tfrac{1}{2}\left(\varDelta + \varDelta_+\right)$$

with $\varDelta_+ = \prod_{i<j}(x_i + x_j)$ and $\varDelta = \prod_{i<j}(x_i - x_j)$, the Vandermonde determinant. Thus,

$$\mathbb{Z}[U_n]^{\mathcal{A}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}] \oplus d\mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}] \tag{8.15}$$

This ring is Cohen-Macaulay, being a finite free extension of the mixed Laurent polynomial ring $\mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]$.

Example 8.11.2 (Multiplicative $\mathcal{A}_n$-invariants of A_{n-1})**.** Continuing with the notation of Example 8.11.1, we now consider the root lattice $A_{n-1} \subseteq U_n$ as $\mathcal{A}_n$-lattice. The invariant algebra $\mathbb{Z}[A_{n-1}]^{\mathcal{A}_n}$ is easily seen to be Cohen-Macaulay. In fact, the lattice U_n is rationally equivalent to $A_{n-1} \oplus \mathbb{Z}$ and so we know from Example 8.11.1 and Proposition 8.9.3 that $\mathbb{Z}[A_{n-1} \oplus \mathbb{Z}]^{\mathcal{A}_n}$ is Cohen-Macaulay. Moreover, $\mathbb{Z}[A_{n-1} \oplus \mathbb{Z}]^{\mathcal{A}_n} \cong \mathbb{Z}[A_{n-1}]^{\mathcal{A}_n}[\mathbb{Z}]$ and hence $\mathbb{Z}[A_{n-1}]^{\mathcal{A}_n}$ is Cohen-Macaulay, by observation (a) in 8.9.

Alternatively, exactly as in Example 3.5.6, one obtains that

$$\mathbb{Z}[A_{n-1}]^{\mathcal{A}_n} = \mathbb{Z}[U_n]_0^{\mathcal{A}_n} ,$$

where $\mathbb{Z}[U_n]_0$ denotes the degree-0 component of $\mathbb{Z}[U_n] = \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ graded by total degree in the variables x_i. Since all s_i in d in (8.15) are homogeneous, with $\deg d = \binom{n}{2}$, we conclude that

$$\mathbb{Z}[A_{n-1}]^{\mathcal{A}_n} = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]_0 \oplus d\mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]_{-\binom{n}{2}} \tag{8.16}$$

Putting $\mu_i = s_i^n / s_n^i$ as in Example 3.5.6 and in §6.3.5, we obtain a polynomial subalgebra $P = \mathbb{Z}[\mu_1, \ldots, \mu_n] \subseteq \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}]_0$ so that both summands in (8.16) are free over P.

Example 8.11.3 ($\mathcal{S}_n$-lattices)**.** Let L be an $\mathcal{S}_n$-lattice such that $\mathbb{Z}[L]^{\mathcal{S}_n}$ is Cohen-Macaulay. Theorem 8.1.1 implies that $\mathcal{S}_n$ acts as a bireflection group on L, and hence on all simple constituents of the rationalization $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$. The simple $\mathbb{Q}[\mathcal{S}_n]$-modules are the Specht modules S^λ for partitions λ of n. If $n \geq 7$ then the only partitions λ so that $\mathcal{S}_n$ acts as a bireflection group on S^λ are (n), (1^n) and $(n-1, 1)$; this follows from the lists in Huffman [91] and Wales [221]. The corresponding Specht modules are the rationalizations of $\mathbb{Z}$, the sign lattice $\mathbb{Z}^-$, and the root lattice A_{n-1}. Thus, if $n \geq 7$ and $\mathbb{Z}[L]^{\mathcal{S}_n}$ is Cohen-Macaulay then we must have

$$L_{\mathbb{Q}} \cong \mathbb{Q}^r \oplus \left(\mathbb{Q}^-\right)^s \oplus \left(A_{n-1}\right)_{\mathbb{Q}}^t$$

with $s + t \leq 2$. In most cases, $\mathbb{Z}[L]^{\mathcal{S}_n}$ is easily seen to be Cohen-Macaulay. Indeed, Corollary 8.9.4 allows us to assume that $r = 0$. If $s+t \leq 1$ then $\mathcal{S}_n$ acts as a reflection group on L and so $\mathbb{Z}[L]^{\mathcal{S}_n}$ is Cohen-Macaulay by Corollary 6.1.2(a). When $t = 0$, the same conclusion follows from Corollary 8.9.2 or from Example 3.5.3 (with $n = 2$). This leaves the cases $s = t = 1$ and $s = 0, t = 2$ to consider.

First let $s = t = 1$. By Corollary 8.9.4, we may add a copy of $\mathbb{Z}$ to L so that L becomes rationally isomorphic to $U_n \oplus \mathbb{Z}^-$. Using Example 8.11.1 and its notation in conjunction with Lemma 3.5.2, we obtain the invariants of $U_n \oplus \mathbb{Z}^-$:

$$\mathbb{Z}[U_n \oplus \mathbb{Z}^-]^{\mathcal{S}_n} = R \oplus R\varphi$$

Here, $\varphi = \frac{1}{2}(\varDelta_+ + \varDelta)t + \frac{1}{2}(\varDelta_+ - \varDelta)t^{-1}$ with $t = \mathbf{x}^{(0_{U_n}, 1)} \in \mathbb{Z}[U_n \oplus \mathbb{Z}^-]$, and $R = \mathbb{Z}[s_1, \ldots, s_{n-1}, s_n^{\pm 1}, t + t^{-1}]$. Thus, $\mathbb{Z}[L]^{\mathcal{S}_n}$ is again Cohen-Macaulay.

If $s = 0$ and $t = 2$ then we may replace L by the lattice $U_n^2 = U_n \oplus U_n$. By Lemma 8.9.1 $\mathbb{Z}[U_n^2]^{\mathcal{S}_n}$ is Cohen-Macaulay precisely if $\mathbb{F}_p[U_n^2]^{\mathcal{S}_n}$ is Cohen-Macaulay for all primes $p \leq n$. As in Example 3.5.5, one sees that $\mathbb{F}_p[U_n^2]^{\mathcal{S}_n}$ is a localization of the algebra "vector invariants" $\mathbb{F}_p[x_1, \ldots, x_n, y_1, \ldots, y_n]^{\mathcal{S}_n}$. By Kemper [109, Corollary 3.5], this algebra is known to be Cohen-Macaulay for $n/2 < p \leq n$, but the primes $p \leq n/2$ apparently remain to be dealt with.

Example 8.11.4 (Ranks ≤ 4)**.** By Corollary 8.9.2, $\mathbb{Z}[L]^{\mathcal{G}}$ is always Cohen-Macaulay when $\operatorname{rank} L \leq 2$.

Now let $\operatorname{rank} L = 3$. There are 32 $\mathbb{Q}$-classes of finite subgroups $\mathcal{G} \leq \mathrm{GL}_3(\mathbb{Z})$. The orders of these groups all divide $M(3) = 48$; see §1.10.2. In particular, the groups $\mathcal{G}$ are all solvable and the Sylow 3-subgroup $\mathcal{H} \leq \mathcal{G}$, if nontrivial, is generated by a bireflection of order 3. Therefore, $\mathbb{F}_3[L]^{\mathcal{H}}$ is Cohen-Macaulay; see Proposition 10.1.1 below for a more general result. Since the relative trace $\operatorname{tr}_{\mathcal{G}/\mathcal{H}} \colon \mathbb{F}_3[L]^{\mathcal{H}} \to \mathbb{F}_3[L]^{\mathcal{G}}$ is surjective, Lemma 8.5.1 implies that $\mathbb{F}_3[L]^{\mathcal{G}}$ is Cohen-Macaulay for all finite subgroups $\mathcal{G} \leq \mathrm{GL}_3(\mathbb{Z})$. Therefore, by Lemma 8.9.1 and Theorem 8.1.1, $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay if and only if $\mathbb{F}_2[L]^{\mathcal{G}}$ is Cohen-Macaulay, and for this to occur, $\mathcal{G}$ must be generated by bireflections. It turns out that 3 of the 32 $\mathbb{Q}$-classes consist of non-bireflection groups; these classes are represented by the cyclic groups

$$\left\langle \begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \right\rangle , \quad \left\langle \begin{pmatrix} & 1 & \\ -1 & & \\ & & -1 \end{pmatrix} \right\rangle , \quad \left\langle \begin{pmatrix} & & -1 \\ -1 & & \\ & -1 & \end{pmatrix} \right\rangle$$

of orders 2, 4 and 6 (the latter two classes each split into two $\mathbb{Z}$-classes). For the 29 $\mathbb{Q}$-classes consisting of bireflection groups $\mathcal{G}$, Pathak [148] has checked explicitly by a case-by-case analysis that $\mathbb{F}_2[L]^{\mathcal{G}}$ is indeed Cohen-Macaulay. To summarize: if $\operatorname{rank} L = 3$ then $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay if and only if $\mathcal{G}$ acts as a bireflection group on L, and the correponding $\mathcal{G}$-lattices are known.

In rank 4, there are 227 $\mathbb{Q}$-classes of finite subgroups $\mathcal{G} \leq \mathrm{GL}_4(\mathbb{Z})$. All but 5 of them consist of solvable groups and 4 of the non-solvable classes are bireflection groups, the one exception being represented by $\mathcal{S}_5$ acting on the signed root lattice $\mathbb{Z}^- \otimes_{\mathbb{Z}} A_4$. Thus, if the group $\mathcal{G}/\mathcal{R}^2(\mathcal{G})$ is perfect then it is actually trivial, that is, $\mathcal{G}$ is a bireflection group. It also turns out that, in this case, all isotropy groups $\mathcal{G}_m$ are bireflection groups. There are exactly 71 $\mathbb{Q}$-classes that do not consist of bireflection groups. By the foregoing, they lead to non-Cohen-Macaulay multiplicative invariant algebras. The $\mathbb{Q}$-classes consisting of bireflection groups have not been systematically investigated yet. The searches in rank 4 were performed with GAP [71].

9

Multiplicative Invariant Fields

9.1 Introduction

This chapter is devoted to invariant fields under group actions. The main theme is the rationality problem for invariant fields, also known as Noether's problem. An excellent introduction to this topic and its historical roots can be found in the monograph [98] by Jensen, Ledet and Yui.

Throughout this chapter, $\Bbbk$ is assumed to be a commutative field. All actions are understood to be trivial on $\Bbbk$.

9.1.1 G-Fields and Noether's Problem

Let G be a group. A *G-field* is a field F together with a given action of G by automorphisms on F, written as $f \mapsto g(f)$. As usual, a G-field F is called *faithful* if every $1 \neq g \in G$ acts non-trivially on F. Morphisms of G-fields are G-equivariant field homomorphisms. If F/K is an extension of G-fields then the G-action on K is understood to be the restriction of the action on F.

Recall that a field extension F/K is called *rational* if F/K is finitely generated and purely transcendental:

$$F = K(t_1, \ldots, t_d)$$

with algebraically independent generators t_i over K. In its most general form, the rationality problem for invariant fields, often referred to as the Noether problem, can be stated follows:

> *Given a rational extension of G-fields F/K, is the extension of invariant fields F^G/K^G again rational?*

This problem originated from considerations in constructive Galois theory; see Noether [141]. The connection will be briefly sketched in §9.1.2. Traditionally, it is assumed that K is a trivial G-field (i.e., $K^G = K$); we will indicate this by writing $K = \Bbbk$. Even in this case the answer to Noether's problem is generally negative. Specifically, given a finite group $\mathcal{G}$, form the rational extension field $\Bbbk(x_g \mid g \in \mathcal{G})$

of $\Bbbk$ and let $\mathcal{G}$ act on $\Bbbk(x_g \mid g \in \mathcal{G})$ by $g(x_h) = x_{gh}$ and $g\big|_{\Bbbk} = \mathrm{Id}_{\Bbbk}$. The invariant subfield of this action will be denoted by $\Bbbk(\mathcal{G})$; so

$$\Bbbk(\mathcal{G}) = \Bbbk(x_g \mid g \in \mathcal{G})^{\mathcal{G}} . \tag{9.1}$$

Lenstra [118] has determined exactly when $\Bbbk(\mathcal{G})/\Bbbk$ is rational for any finite abelian group $\mathcal{G}$. For example, for the cyclic group $\mathcal{C}_8$ of order 8, the extension $\mathbb{Q}(\mathcal{C}_8)/\mathbb{Q}$ is not rational; see [118, Corollary 7.2]. Earlier, Swan [208] and Voskresenskiĭ [218] had shown independently that $\mathbb{Q}(\mathcal{C}_p)/\mathbb{Q}$ is non-rational for the primes $p = 47, 112, 223, \ldots$. In view of these examples and others, one often asks for the field extension F^G/K^G in Noether's problem to at least enjoy some weakened version of rationality.

9.1.2 Versions of Rationality

There are several relaxed notions of rationality for field extensions: a field extension F/K is called

- *stably rational* if there is an extension field $E \supseteq F$ such that E/F and E/K are both rational,
- *retract rational* if F is the field of fractions of some K-subalgebra R which is a retract of a localized polynomial algebra $K[x_1, \ldots, x_n][1/f]$, that is, there are K-algebra maps

$$\begin{tikzcd} R \arrow[r, shift left, "\mu"] & K[x_1, \ldots, x_n][1/f] \arrow[l, shift left, "\pi"] \end{tikzcd}$$

  so that $\pi \circ \mu = \mathrm{Id}_R$,
- *unirational* if there is an extension field $E \supseteq F$ such that E/K is rational.

We will not be concerned with unirationality in the sequel, because in the setting of Noether's problem with $K = \Bbbk$, the extension $F^G/\Bbbk$ is clearly unirational. Retract rational extensions were introduced by Saltman [175]. They are of importance in constructive Galois theory: Given $\Bbbk$ and a finite group $\mathcal{G}$, let $\Bbbk(\mathcal{G})$ be defined as in (9.1). By a result due to Saltman [175] for infinite K and to DeMeyer-McKenzie [48] in general, the extension $\Bbbk(\mathcal{G})/\Bbbk$ is retract rational if and only if there exists a *generic polynomial* $f = f(t_1, \ldots, t_m)(x) \in \Bbbk(t_1, \ldots, t_m)[x]$ for Galois field extensions E/F of K with group $\mathcal{G}$. Explicitly, this means that $t_1, \ldots, t_m$ are indeterminates over $\Bbbk$ and f is a separable polynomial in $\Bbbk(t_1, \ldots, t_m)[x]$ with Galois group $\mathcal{G}$ having the property that, for any Galois extension E/F with $\mathrm{Gal}(E/F) = \mathcal{G}$ and $F \supseteq \Bbbk$, there exist $\lambda_1, \ldots, \lambda_m \in F$ so that E is the splitting field of the separable polynomial $f(\lambda_1, \ldots, \lambda_m)(x) \in F[x]$.

The above versions of rationality are successively weaker:

$$\text{rational} \;\Rightarrow\; \text{stably rational} \;\Rightarrow\; \text{retract rational} \;\Rightarrow\; \text{unirational} .$$

All these implications are obvious except, perhaps, for the fact that stably rational extensions are retract rational; see Proposition 9.3.3 below. None of the implications is reversible in general. Lenstra [118, Remark 5.7] has shown that if the extension $\Bbbk(\mathcal{G})/\Bbbk$ in (9.1) is stably rational for a finite abelian group $\mathcal{G}$ then $\Bbbk(\mathcal{G})/\Bbbk$ is actually rational. In particular, the aforementioned non-rational extensions $\mathbb{Q}(\mathcal{C}_p)/\mathbb{Q}$ ($p = 47, 112, 223, \dots$) are not stably rational either. However, by a result of Saltman [177] (see Theorem 9.6.6), $\mathbb{Q}(\mathcal{C}_p)/\mathbb{Q}$ is always retract rational, for any prime p, while Lenstra's non-rational extension $\mathbb{Q}(\mathcal{C}_8)/\mathbb{Q}$ is not even retract rational. For further examples and references to the literature we refer the reader to the book [98] by Jensen, Ledet and Yui and to Le Bruyn's excellent survey on the rationality problem, [114].

9.1.3 Linear and Multiplicative G-Fields

Given a linear representation $G \to \mathrm{GL}(V)$ of the group G on a finite-dimensional $\Bbbk$-vector space V, we obtain an action of G on the symmetric algebra $\mathsf{S}(V)$ and hence on the field of fractions

$$\mathsf{K}(V) = Q(\mathsf{S}(V)) \ .$$

Note that $\mathsf{K}(V)$ is a rational extension of $\Bbbk$; we will call G-fields of this form *linear*. When viewing V as an algebraic variety over $\Bbbk$, it is customary to pass to the contragredient representation $G \to \mathrm{GL}(V^*)$ and to consider the corresponding G-actions on the algebra of polynomial functions on V,

$$\mathcal{O}(V) = \mathsf{S}(V^*) \ ,$$

and on the algebra of rational functions on V,

$$\mathcal{K}(V) = \mathsf{K}(V^*) \ .$$

Similarly, ordinary and twisted multiplicative G-actions on $\Bbbk[L]$ and $K[L]_\gamma$ (see Section 3.8) can be extended to the respective fields of fractions

$$\Bbbk(L) = Q(\Bbbk[L]) \quad \text{and} \quad K(L)_\gamma = Q(K[L]_\gamma) \ .$$

The resulting G-fields will be called *(twisted) multiplicative*. The extensions $\Bbbk(L)/\Bbbk$ and $K(L)_\gamma/K$ are clearly rational. The associated extensions of invariant fields, $\Bbbk(L)^G/\Bbbk$ and $K(L)_\gamma^G/K^G$, and their relations to linear invariant fields will form the main focal point of this chapter.

The field $\Bbbk(\mathcal{G})$ in (9.1), for example, can be viewed as the multiplicative invariant field $\Bbbk(L)^{\mathcal{G}}$ of the regular $\mathcal{G}$-lattice $L = \mathbb{Z}[\mathcal{G}]$, and $\Bbbk(\mathcal{G})$ can also be viewed as the linear invariant field $\mathsf{K}(V)^{\mathcal{G}}$ with $V = \Bbbk[\mathcal{G}]$. A similar remark holds for any permutation $\mathcal{G}$-lattice L.

It is a remarkable fact that linear invariant fields $\mathcal{K}(V)^G$ of (infinite) algebraic groups G are often isomorphic to suitable multiplicative invariant fields $\Bbbk(L)^{\mathcal{G}}$ for a finite group $\mathcal{G}$. An important instance of this phenomenon occurs when $V = \mathrm{M}_n^r(\Bbbk)$ is the space of r-tuples of $n \times n$-matrices over $\Bbbk$ and the group $G = \mathrm{PGL}_n(\Bbbk)$ operates on V by simultaneous conjugation. When $\Bbbk$ is algebraically closed and $r \geq 2$, we will see in Theorem 9.8.2 below that

$$\mathcal{K}(\mathrm{M}_n^r(\Bbbk))^{\mathrm{PGL}_n(\Bbbk)} \cong \Bbbk(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \oplus \left(U_n^{\otimes 2}\right)^{r-2})^{\mathcal{S}_n} \ .$$

9.2 Stable Isomorphism

Let G be a group. Two G-fields F and F' are called *stably isomorphic* provided there is an isomorphism of G-fields

$$F(x_1,\dots,x_r) \xrightarrow{\sim} F'(y_1,\dots,y_s)$$

for suitable r and s, where the x's and y's are G-invariant commuting indeterminates over F and F', respectively. In case F and F' contain a common G-subfield K and the above isomorphism is the identity on K, we say that F and F' are stably isomorphic over K. Taking $G = \langle 1 \rangle$, one obtains analogous notions for fields without group action: two fields F and F' are said to be stably isomorphic (over a common subfield K) if there are rational extensions E/F and E'/F' so that $E \cong E'$ (and the isomorphism is the identity on K).

Lemma 9.2.1. *Let F/K and F'/K be extensions of $\mathcal{G}$-fields, where $\mathcal{G}$ is a finite group.*

(a) *If $F = K(x_1,\dots,x_r)$ for $\mathcal{G}$-invariant indeterminates x_i then*

$$F^{\mathcal{G}} = K^{\mathcal{G}}(x_1,\dots,x_r)$$

is rational over $K^{\mathcal{G}}$. Conversely, if K is a faithful $\mathcal{G}$-field and $F^{\mathcal{G}}/K^{\mathcal{G}}$ is rational then $F = K(x_1,\dots,x_r)$ for $\mathcal{G}$-invariant indeterminates x_i.

(b) *If F and F' are stably isomorphic over K then $F^{\mathcal{G}}$ and $F'^{\mathcal{G}}$ are stably isomorphic over $K^{\mathcal{G}}$.*

Proof. (a) If $F = K(x_1,\dots,x_r)$ for indeterminates $x_i \in F^{\mathcal{G}}$ then $K[x_1,\dots,x_r]^{\mathcal{G}} = K^{\mathcal{G}}[x_1,\dots,x_r]$. Since $\mathcal{G}$ is finite, we have $F^{\mathcal{G}} = Q(K[x_1,\dots,x_r]^{\mathcal{G}})$; see, e.g., Bourbaki [22, Prop. V.1.23]. Thus, $F^{\mathcal{G}} = Q(K^{\mathcal{G}}[x_1,\dots,x_r]) = K^{\mathcal{G}}(x_1,\dots,x_r)$.

For the converse, assume that $F^{\mathcal{G}} = K^{\mathcal{G}}(x_1,\dots,x_r)$ for elements x_i that are algebraically independent over $K^{\mathcal{G}}$. Since $K/K^{\mathcal{G}}$ is algebraic, the x_i are also algebraically independent over K. Put $E = K(x_1,\dots,x_r) \subseteq F$. Since $E \supseteq F^{\mathcal{G}}$, we have $E^{\mathcal{G}} = F^{\mathcal{G}}$. By Galois theory, $[E : E^{\mathcal{G}}] = |\mathcal{G}| = [F : F^{\mathcal{G}}]$ and so $E = F$.

(b) By (a), any K-isomorphism of $\mathcal{G}$-fields $F(x_1,\dots,x_r) \xrightarrow{\sim} F'(y_1,\dots,y_s)$ with $\mathcal{G}$-invariant indeterminates x_i, y_j restricts to a $K^{\mathcal{G}}$-isomorphism

$$F^{\mathcal{G}}(x_1,\dots,x_r) \xrightarrow{\sim} F'^{\mathcal{G}}(y_1,\dots,y_s)\,.$$

So $F^{\mathcal{G}}$ and $F'^{\mathcal{G}}$ are stably isomorphic over $K^{\mathcal{G}}$. □

9.3 Retract Rationality

The notion of retract rationality has the flavor of "projectivity"; this will be made explicit in Lemma 9.3.2 below. We will need the following observation due to Swan [208, Lemma 8]. For later use it is stated here with an operating group $\mathcal{G}$.

Lemma 9.3.1. *Let F/K be an extension of $\mathcal{G}$-fields. Assume that $F = Q(R) = Q(S)$ for suitable $\mathcal{G}$-stable affine K-subalgebras R and S. Then there are nonzero elements $r \in R^{\mathcal{G}}$, $s \in S^{\mathcal{G}}$ so that $R[1/r] = S[1/s]$.*

Proof. By [22, Prop. V.1.23], F can be obtained from R by inverting the nonzero elements of $R^{\mathcal{G}}$, and similarly for S. Since R is affine, we conclude that there is a nonzero $s_0 \in S^{\mathcal{G}}$ with $R \subseteq S[1/s_0]$. Similarly, $S[1/s_0] \subseteq R[1/r_0]$ for some nonzero $r_0 \in R^{\mathcal{G}}$. Thus, $S[1/s_0][1/r_0] = R[1/r_0]$. Now, $r_0 = t/s_0^n$ for suitable $t \in S^{\mathcal{G}}$ and $n \in \mathbb{Z}_+$, and so $S[1/s_0][1/r_0] = S[1/s_0t]$. The lemma follows by taking $r = r_0$ and $s = s_0t$. □

A homomorphism of K-algebras $\alpha\colon A \to B$ is said to be split if there exists a homomorphism $\beta\colon B \to A$ such that $\alpha \circ \beta = \mathrm{Id}_B$. In this case, B is also called a *retract* of A. If B is a retract of A then any localization $B[1/b]$ of B is a retract of some localization $A[1/a]$: just consider the extensions of α and β,

$$\begin{tikzcd} B[1/b] \arrow[r, shift left, "\beta"] & A[1/\beta(b)] \arrow[l, shift left, "\alpha"] \end{tikzcd} \quad , \tag{9.2}$$

and take $a = \beta(b)$.

The definition of retract rationality as given in §9.1.2 can be rephrased as follows: the field extension F/K is retract rational if and only if $F = Q(R)$ for some K-subalgebra $R \subseteq F$ which is a retract of a localized polynomial algebra $K[x_1, \ldots, x_n][1/f]$. The following lemma gives an alternative formulation.

Lemma 9.3.2. *A field extension F/K is retract rational if and only if F/K is finitely generated and the following condition is satisfied: if $F = Q(S)$ for some affine K-subalgebra $S \subseteq F$ and $\alpha\colon A \twoheadrightarrow S$ is an epimorphism of K-algebras then there exists an $a \in A$ such that $\alpha(a) \neq 0$ and the extension of α, $A[1/a] \twoheadrightarrow S[1/\alpha(a)]$, is split.*

Proof. First note that the above version implies the original definition. For, we may write $F = Q(S)$ for some affine K-subalgebra $S \subseteq F$, since F/K is finitely generated. Now choose any epimorphism $\alpha\colon K[x_1, \ldots, x_n] \twoheadrightarrow S$ and an element $f \in K[x_1, \ldots, x_n]$ such that the extension $K[x_1, \ldots, x_n][1/f] \twoheadrightarrow S[1/\alpha(f)]$ splits and take $R = S[1/\alpha(f)]$.

For the converse, assume that $F = Q(R)$ for some K-subalgebra $R \subseteq F$ which is a retract of a localized polynomial algebra $K[x_1, \ldots, x_n][1/f]$. Then F/K is certainly finitely generated, because R is an affine K-algebra. Write $F = Q(S)$ where $S \subseteq F$ is some affine K-subalgebra. By Lemma 9.3.1, there are elements $0 \neq r \in R$ and $0 \neq s \in S$ so that $R[1/r] = S[1/s]$. By (9.2), $R[1/r] = S[1/s]$ is a retract of some localization of $K[x_1, \ldots, x_n][1/f]$. Any such localization has the form $K[x_1, \ldots, x_n][1/f']$ for some $0 \neq f' \in K[x_1, \ldots, x_n]$; see the proof of Lemma 9.3.1. Thus, we have K-algebra maps

$$\begin{tikzcd} S[1/s] \arrow[r, shift left, "\mu"] & K[x_1, \ldots, x_n][1/f'] \arrow[l, shift left, "\pi"] \end{tikzcd}$$

so that $\pi \circ \mu = \mathrm{Id}_{S[1/s]}$. Now consider a K-algebra epimorphism $\alpha\colon A \twoheadrightarrow S$. Choose $a_0 \in A$ with $\alpha(a_0) = s$ and let $\alpha\colon A[1/a_0] \twoheadrightarrow S[1/s]$ be the extension of α. Further, choose elements $a_i \in A[1/a_0]$ such that $\alpha(a_i) = \pi(x_i)$ and define $\varphi\colon K[x_1,\ldots,x_n] \to A[1/a_0]$ by $\varphi(x_i) = a_i$. Then $\alpha \circ \varphi = \pi\colon K[x_1,\ldots,x_n] \to S[1/s]$. In particular, $(\alpha \circ \varphi)(f') = \pi(f')$ is invertible in $S[1/s]$ and so we can consider the extensions

$$K[x_1,\ldots,x_n][1/f'] \xrightarrow{\varphi} A[1/a_0][1/\varphi(f')] \overset{\alpha}{\twoheadrightarrow} S[1/s]$$

with $\alpha \circ \varphi = \pi$. Note that $A[1/a_0][1/\varphi(f')] = A[1/a]$ for some $a \in A$ (again, as in the proof of Lemma 9.3.1) and the map $\beta = \varphi \circ \mu\colon S[1/s] \to A[1/a]$ satisfies $\alpha \circ \beta = \alpha \circ \varphi \circ \mu = \pi \circ \mu = \mathrm{Id}_{S[1/s]}$; so $\alpha\colon A[1/a] \twoheadrightarrow S[1/s]$ is split. Finally, since $\alpha(A) = S$, we have $S[1/s] = \alpha(A[1/a]) = S[1/\alpha(a)]$ and $\alpha(a) \neq 0$. This completes the proof. □

Following Saltman [177, Proposition 3.6(a)], we now show that retract rationality is preserved under stable isomorphism.

Proposition 9.3.3. *Let F/K and F'/K be field extensions.*

(a) *Assume that F and F' are stably isomorphic over K. If F/K is retract rational then so is F'/K.*
(b) *If F/K is stably rational then F/K is retract rational.*

Proof. (a) Fix rational extensions E/F and E'/F' so that E and E' are K-isomorphic. The extension E/K is retract rational, because F/K is. Indeed, $E = F(x_1,\ldots,x_n)$ with algebraically independent generators x_i, and $F = Q(R)$ for some K-subalgebra $R \subseteq F$ that is a retract of a localized polynomial algebra $K[t_1,\ldots,t_d][1/f]$. Thus, $R[x_1,\ldots,x_n]$ is a retract of $K[x_1,\ldots,x_n,t_1,\ldots,t_d][1/f]$ and $Q(R[x_1,\ldots,x_n]) = E$, which shows that E/K is retract rational. Hence, we may assume that $F = E$.

Write $F = F'(y_1,\ldots,y_m)$ with algebraically independent y_j, and $F = Q(R)$, as above. Our goal is to show that F'/K is retract rational. Note that F'/K is certainly unirational, as F/K is. In particular, we may assume that F' is infinite. For, otherwise $F' = K$, because K is algebraically closed in F', and we are done. Fix an affine K-subalgebra $A \subseteq F'$ with $F' = Q(A)$. It will suffice to show that, for some nonzero $a \in A$, $A[1/a]$ is is a retract of a localized polynomial algebra. To this end, note that $F = Q(R) = Q(A[y_1,\ldots,y_m])$; so

$$R[1/r] = A[y_1,\ldots,y_m][1/t]$$

holds for suitable nonzero $r \in R$ and $t \in A[y_1,\ldots,y_m]$, by Lemma 9.3.1. Since A is infinite, there exists an A-algebra map $\varphi\colon A[y_1,\ldots,y_m] \to A$ with $\varphi(t) \neq 0$; see Bourbaki [27, Théorème IV.2.2]. Put $a = \varphi(t)$, $A' = A[1/a]$ and write $a = s/r^e$ with $0 \neq s \in R$ and $e \geq 0$. Then

$$A'[y_1,\ldots,y_m][1/t] = R[1/rs]$$

and φ extends uniquely to an A'-algebra map $\varphi\colon A'[y_1,\dots,y_m][1/t] \to A'$; so A' is a retract of $R[1/rs]$. As we remarked above, $R[1/rs]$ is a retract of a localized polynomial algebra, as R is, and hence A' is a retract of a localized polynomial algebra as well. This completes the proof of (a).

(b) Just note that F/K being stably rational says that F is stably isomorphic to K over K. Thus, (b) follows from (a). □

9.4 The “No-name Lemma”

In this section, we gather together some standard facts from field theory. Throughout, $\mathcal{G}$ denotes a finite group. We begin with a lemma often referred to as the Galois descent lemma, invariant basis lemma or Speiser’s lemma [200]. Recall that $K\#\mathcal{G}$ denotes the skew group ring that is associated with the $\mathcal{G}$-field K; see Section 5.3.

Lemma 9.4.1. *Let K be a faithful $\mathcal{G}$-field. Then, for any left $K\#\mathcal{G}$-module W, we have $W \cong K \otimes_{K^{\mathcal{G}}} W^{\mathcal{G}}$ via multiplication, where $W^{\mathcal{G}}$ denotes the $\mathcal{G}$-invariants in W.*

Proof. This lemma is a consequence of the fact that the skew group ring $S = K\#\mathcal{G}$ is Morita equivalent to the invariant subfield $K^{\mathcal{G}}$; see, e.g., Chase, Harrison and Rosenberg [36, Remark 1.5(c)]. We give a self-contained argument.

First, we show that S is a simple ring: Let I be a nonzero ideal of S and choose $0 \neq f = \sum_{g\in\mathcal{G}} k_g g \in I$ so that $\mathrm{Supp}(f) = \{g \in \mathcal{G} \mid k_g \neq 0\}$ has minimal size. We may assume that f has the form $f = 1 + \sum_{1\neq g\in\mathcal{G}} k_g g$. If $k_g \neq 0$ for some $1 \neq g \in \mathcal{G}$ then choose $k \in K$ with $g(k) \neq k$ and form the element $f' = kf - fk = \sum_{1\neq g\in\mathcal{G}}(kk_g - k_g g(k))g$; this is a nonzero element of I whose support is smaller than $\mathrm{Supp}(f)$, contradicting minimality of f. Thus, $1 \in I$ proving simplicity of S.

Applying the foregoing to the ideal of S that is generated by the symmetrizer $t = \sum_{g\in\mathcal{G}} g \in S$ we obtain $1 \in StS = KtK$; see (5.7). For any left S-module W, we have $tW \subseteq W^{\mathcal{G}}$. Consequently, $W = KtK \cdot W = KW^{\mathcal{G}}$, and hence W has a K-basis consisting of elements in $W^{\mathcal{G}}$. This basis is easily seen to be a $K^{\mathcal{G}}$-basis of $W^{\mathcal{G}}$; so $W \cong K \otimes_{K^{\mathcal{G}}} W^{\mathcal{G}}$. □

As an application, suppose that the finite group $\mathcal{G}$ acts by automorphism on the ring R and R contains a $\mathcal{G}$-stable subfield K on which $\mathcal{G}$ acts faithfully. If $R = \langle K, W\rangle_{\text{ring}}$ for some $\mathcal{G}$-stable left K-subspace $W \subseteq R$ then, in fact,

$$R = \langle K, W^{\mathcal{G}}\rangle_{\text{ring}} \; .$$

To see this, just note that W is a left $K\#\mathcal{G}$-submodule of R and apply Lemma 9.4.1. We now concentrate on field extensions. Various versions of the following rationality results are referred to in the literature as the “no-name lemma”; the terminology was introduced by Dolgachev [51].

Lemma 9.4.2. *Let $K \subseteq F$ be an extension of faithful $\mathcal{G}$-fields. Assume that $F = \langle K, W\rangle_{\text{field}}$ for some $\mathcal{G}$-stable K-subspace $W \subseteq F$. Then:*

(a) $F = \langle K, W^{\mathcal{G}} \rangle_{\text{field}}$ *and* $F^{\mathcal{G}} = \langle K^{\mathcal{G}}, W^{\mathcal{G}} \rangle_{\text{field}}$.
(b) *If* $K \subseteq W$ *and* $\dim_K W = 1 + \operatorname{trdeg}_K F < \infty$ *then* $F^{\mathcal{G}}/K^{\mathcal{G}}$ *is rational.*

Proof. (a) The $\mathcal{G}$-action on F and multiplication with K make F a left $K\#\mathcal{G}$-module and W is a $K\#\mathcal{G}$-submodule. Therefore, Lemma 9.4.1 implies that $W = KW^{\mathcal{G}}$. Hence, $F = \langle K, W^{\mathcal{G}} \rangle_{\text{field}}$.

Put $E = \langle K^{\mathcal{G}}, W^{\mathcal{G}} \rangle_{\text{field}} \subseteq F^{\mathcal{G}}$. We want to show that equality holds. Indeed, the E-vector space KE generated by K is a subring of F and $\dim_E KE \le \dim_{K^{\mathcal{G}}} K = |\mathcal{G}|$. Thus, KE is a field, and hence $KE = \langle K, W^{\mathcal{G}} \rangle_{\text{field}} = F$. Therefore, $\dim_E F = \dim_E KE \le |\mathcal{G}| = \dim_{F^{\mathcal{G}}} F$. Since $E \subseteq F^{\mathcal{G}}$ this is only possible if $E = F^{\mathcal{G}}$.

(b) Choose a $K^{\mathcal{G}}$-basis $\{1 = b_0, b_1, \ldots, b_n\}$ of $W^{\mathcal{G}}$. By part (a), $F^{\mathcal{G}} = \langle K^{\mathcal{G}}, b_1, \ldots, b_n \rangle_{\text{field}}$. Since $\operatorname{trdeg}_{K^{\mathcal{G}}} F^{\mathcal{G}} = \operatorname{trdeg}_K F = n$, we conclude that $b_1, \ldots, b_n$ are transcendental over $K^{\mathcal{G}}$. □

We now focus on twisted multiplicative $\mathcal{G}$-fields. Recall from Section 3.8 that, given a $\mathcal{G}$-field K, a $\mathcal{G}$-lattice L and a class $\gamma \in \operatorname{Ext}_{\mathbb{Z}[G]}(L, K^*)$, the notation $K[L]_\gamma$ indicates the group algebra $K[L]$ with the twisted multiplicative $\mathcal{G}$-action (3.19). As in §9.1.3 we put

$$K(L)_\gamma = Q(K[L]_\gamma) \tag{9.3}$$

with the (uniquely) extended $\mathcal{G}$-action. Twisted multiplicative G-fields with trivial extension class γ are simply written as

$$K(L)\ ; \tag{9.4}$$

the action of $\mathcal{G}$ on the group algebra $K[L]$ is then given by formula (3.21).

The following lemma essentially goes back to Masuda [130] and Miyata [134].

Lemma 9.4.3. *Let K be a faithful $\mathcal{G}$-field and L a permutation $\mathcal{G}$-lattice. Then any twisted multiplicative $\mathcal{G}$-ring $K[L]_\gamma$ is a localized polynomial algebra:*

$$K[L]_\gamma \cong K[x_1, \ldots, x_n][1/f]\ ,$$

where the variables x_i and the element f are $\mathcal{G}$-invariant. In particular, $K[L]_\gamma^{\mathcal{G}} = K^{\mathcal{G}}[x_1, \ldots, x_n][1/f]$ is a localized polynomial algebra over $K^{\mathcal{G}}$ and the field extension $K(L)_\gamma^{\mathcal{G}}/K^{\mathcal{G}}$ is rational.

Proof. By Hilbert's "Theorem 90" (e.g., Serre [193, Proposition X.2]), the $\mathcal{G}$-module K^* is H^1-trivial, and so $\operatorname{Ext}_{\mathbb{Z}[\mathcal{G}]}(L, K^*)$ is trivial; see Section 2.5. Therefore, $K[L]_\gamma \cong K[L]$. Fix a $\mathbb{Z}$-basis $\{m_i\}_1^n$ of L that is permuted by the action of $\mathcal{G}$ and put $t_i = \mathbf{x}^{m_i} \in K[L]$. Then $K[L] = K[t_1^{\pm 1}, \ldots, t_n^{\pm 1}] = K[t_1, \ldots, t_n][1/f]$ with $f = \prod_1^n t_i$. The group $\mathcal{G}$ permutes the variables t_i and fixes f. Therefore, $K[L]^{\mathcal{G}} = K[t_1, \ldots, t_n]^{\mathcal{G}}[1/f]$. Put $W = \bigoplus_1^n Kt_i \subseteq K[t_1, \ldots, t_n]$; this is a left $K\#\mathcal{G}$-submodule of $K[t_1, \ldots, t_n]$. By Lemma 9.4.1, W has a K-basis consisting of $\mathcal{G}$-invariant elements $x_1, \ldots, x_n$. Therefore, $K[t_1, \ldots, t_n] = K[x_1, \ldots, x_n]$ and so $K[L]^{\mathcal{G}} = K^{\mathcal{G}}[x_1, \ldots, x_n][1/f]$, as desired. The assertion about $K(L)_\gamma^{\mathcal{G}}/K^{\mathcal{G}}$ is now clear. □

The main effect of the foregoing, for our purposes, is that many rationality problems are essentially equivalent. Parts (a) and (b) of the following proposition are standard. Part (c) is due to Saltman [179, Corollary 1.6]; see also Reichstein [160].

Proposition 9.4.4. *Let $\mathcal{G} \hookrightarrow \mathrm{GL}(V)$ be a faithful linear representation of the finite group $\mathcal{G}$, where V is a finite-dimensional $\Bbbk$-vector space.*

(a) *If $U \subseteq V$ is a faithful subrepresentation then the extension of linear invariant fields $\mathsf{K}(V)^{\mathcal{G}}/\mathsf{K}(U)^{\mathcal{G}}$ is rational.*
(b) *$\mathsf{K}(V)^{\mathcal{G}}/\Bbbk$ is stably isomorphic to $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ for any faithful permutation $\mathcal{G}$-lattice L.*
(c) *If $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational for some faithful $\mathcal{G}$-lattice L then $\mathsf{K}(V)^{\mathcal{G}}/\Bbbk$ is retract rational as well.*

Proof. (a) Apply Lemma 9.4.2(b) with $K = \mathsf{K}(U) \subseteq F = \mathsf{K}(V)$ and $W = KV \subseteq F$. Then $\dim_K W = 1 + \dim_{\Bbbk} V/U = 1 + \operatorname{trdeg}_K F$ and Lemma 9.4.2(b) yields the result.

(b) Put $K = \mathsf{K}(V)$, $K' = \Bbbk(L)$ and consider the multiplicative $\mathcal{G}$-field $F = K(L)$. By Lemma 9.4.3, $F^{\mathcal{G}}/K^{\mathcal{G}}$ is rational. Note that F can also be written as $F = \mathsf{K}(V')$ with $V' = K' \otimes_{\Bbbk} V$. Applying Lemma 9.4.2(b) with $W = K' + V'$, we also obtain that $F^{\mathcal{G}}/K'^{\mathcal{G}}$ is rational. This proves (b).

(c) Fix L and define the fields K, K' and F as in the proof of (b) above. Recall that $F^{\mathcal{G}}/K'^{\mathcal{G}}$ is rational. (This part of the argument only uses faithfulness of L.) Since $K'^{\mathcal{G}}/\Bbbk$ is retract rational, by hypothesis, $F^{\mathcal{G}}/\Bbbk$ is retract rational as well, by Proposition 9.3.3(a). Finally, in Proposition 9.5.4(a) below, we will show that if $F^{\mathcal{G}}/\Bbbk = K(L)^{\mathcal{G}}/\Bbbk$ is retract rational then so is $K^{\mathcal{G}}/\Bbbk$. □

We will see in Proposition 9.6.1(b) that L could be taken to be any faithful quasi-permutation $\mathcal{G}$-lattice in part (b) above. Part (c) implies in particular that, in order to ensure the existence of a generic polynomial for $\mathcal{G}$ over $\Bbbk$, it suffices to find one faithful $\mathcal{G}$-lattice L so that $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational; see §9.1.2.

9.5 Function Fields of Algebraic Tori

This section focuses on multiplicative $\mathcal{G}$-fields of the form $K(L)$ for a finite group $\mathcal{G}$; see (9.4). For the most part, the $\mathcal{G}$-field K will be faithful. In view of the connection with algebraic tori sketched in Section 3.10, the invariant fields $K(L)^{\mathcal{G}}$ are often called *fields of torus invariants* or *function fields of algebraic tori*.

Recall that a $\mathcal{G}$-lattice L is called monomial if L has a $\mathbb{Z}$-basis that is permuted by $\mathcal{G}$ up to a ±-sign; see Section 2.8. The next proposition extends an earlier rationality result (Lemma 9.4.3) for twisted multiplicative invariant fields $K(L)^{\mathcal{G}}_{\gamma}/K^{\mathcal{G}}$ with L a permutation $\mathcal{G}$-lattice (γ is trivial in this case).

Proposition 9.5.1. *Let $\mathcal{G}$ be a finite group and let $F = K(L)$ be a multiplicative $\mathcal{G}$-field with K a faithful $\mathcal{G}$-field. If the $\mathcal{G}$-lattice L is monomial then $F^{\mathcal{G}}/K^{\mathcal{G}}$ is rational.*

Proof. Fix a $\mathbb{Z}$-basis $\{m_i\}_1^n$ of L that is permuted up to ± by the action of $\mathcal{G}$ and put $x_i = \mathbf{x}^{m_i} \in F$. Then $\{x_i\}_1^n$ is a transcendence basis for F/K and

$$g(x_i) = x_{i'}^{\pm 1} \tag{9.5}$$

holds for each $g \in \mathcal{G}$ and each i. Put $y_i = (1 + x_i)^{-1} \in F$. (This change of variables has been borrowed from Hajja and Kang [86].) Then $\{y_i\}_1^n$ is another transcendence basis for F/K and the $\mathcal{G}$-action (9.5) translates into

$$g(y_i) = \begin{cases} y_{i'} & \text{if } + \text{ holds in (9.5);} \\ 1 - y_{i'} & \text{if } - \text{ holds in (9.5).} \end{cases}$$

Thus, Lemma 9.4.2(b) applies with $W = K + \sum_1^n K y_i$, proving rationality of $F^{\mathcal{G}}/K^{\mathcal{G}}$. □

The following example shows that Proposition 9.5.1 is not true in general for twisted multiplicative invariant fields $K(L)_\gamma^{\mathcal{G}}$ with non-trivial γ.

Example 9.5.2 (A non-rational extension)**.** Let $\mathcal{G} = \langle g_1, g_2 \rangle \cong \mathcal{C}_2 \times \mathcal{C}_2$ act on the lattice $N = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$ via $g_i(e_3) = -e_3 + e_i$ and $g_i(e_j) = (2\delta_{i,j} - 1)e_j$ for $j = 1, 2$. Then $M = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ is a $\mathcal{G}$-sublattice of N and $L = N/M \cong \mathbb{Z}$ is monomial, with both g_i acting as -1. Consider the $\mathcal{G}$-fields $F = \Bbbk(N) \supseteq K = \Bbbk(M)$; so $F = K(L)_\gamma$ for some γ. Assuming that $\operatorname{char} \Bbbk \neq 2$ we will show that $F^{\mathcal{G}}/K^{\mathcal{G}}$ is not rational. Writing $x_i = \mathbf{x}^{e_i}$ as usual, we know (Example 3.5.1) that $K^{\mathcal{G}} = \Bbbk(\xi_1, \xi_2)$ with $\xi_i = x_i + x_i^{-1}$. This field can also be written as $K^{\mathcal{G}} = \Bbbk(\mu_1, \mu_2)$, where $\mu_1 = (\frac{x_1+1}{x_1-1})^2$ and $\mu_2 = (\frac{x_2-1}{x_2+1})^2$. The invariant field $F^{\mathcal{G}}$ can be determined as in Hajja and Kang [83, case $W_{14}(174)$]: $F^{\mathcal{G}} = \Bbbk(\mu_1, \sigma, \tau)$ with $\sigma = 2\frac{x_3^2 + x_1 x_2}{x_3(x_1+1)(x_2+1)}$ and $\tau = 2\frac{x_3^2 - x_1 x_2}{x_3(x_1-1)(x_2-1)}$. These generators satisfy the relation

$$\mu_2 \tau^2 - \mu_1 \sigma^2 = (1 - \mu_1)(1 - \mu_2) \, . \tag{9.6}$$

Suppose that $F^{\mathcal{G}}/K^{\mathcal{G}}$ is rational; so $F^{\mathcal{G}} = K^{\mathcal{G}}(y)$ for some y and $\sigma = \sigma(y)$, $\tau = \tau(y)$. We may specialize y to a suitable element $y_0 \in K^{\mathcal{G}}$ so that $\sigma_0 = \sigma(y_0)$ and $\tau_0 = \tau(y_0)$ are well-defined nonzero elements of $K^{\mathcal{G}} = \Bbbk(\mu_1, \mu_2)$; see Bourbaki [27, Théorème IV.2.2]. Writing $\sigma_0 = s/r$ and $\tau_0 = t/r$ with nonzero elements $r, s, t \in \Bbbk[\mu_1, \mu_2]$ with $\gcd(r, s, t) = 1$, relation (9.6) becomes

$$\mu_2 t^2 - \mu_1 s^2 = (1 - \mu_1)(1 - \mu_2) r^2 \tag{9.7}$$

in $\Bbbk[\mu_1, \mu_2]$. Substituting $\mu_2 = 0$ in (9.7), we obtain the equation

$$\mu_1 s(\mu_1, 0)^2 = (\mu_1 - 1) r(\mu_1, 0)^2$$

in $\Bbbk[\mu_1]$. This implies that $s(\mu_1, 0) = r(\mu_1, 0) = 0$. (Otherwise, the irreducible factor μ_1 occurs an odd number of times on the left and an even number of times on the right.) Thus, $s = \mu_2 s_0$ and $r = \mu_2 r'$ for some $s_0, r' \in \Bbbk[\mu_1, \mu_2]$. Similarly, substituting $\mu_1 = 0$ in (9.7), we obtain $t = \mu_1 t_0$ and $r = \mu_1 r''$ for some $t_0, r'' \in \Bbbk[\mu_1, \mu_2]$.

Therefore, $r = \mu_1\mu_2 r_0$ for some $r_0 \in \Bbbk[\mu_1, \mu_2]$. Substituting the expressions for r and s into (9.7) gives

$$\mu_2 t^2 - \mu_1\mu_2^2 s_0^2 = (1-\mu_1)(1-\mu_2)\mu_1^2\mu_2^2 r_0^2 \,.$$

This shows that μ_2 divides t in $\Bbbk[\mu_1, \mu_2]$; so μ_2 divides $\gcd(r,s,t) = 1$, a contradiction. Therefore, $F^{\mathcal{G}}/K^{\mathcal{G}}$ is non-rational.

We now turn to stable rationality and stable isomorphism. The following proposition relates stable isomorphism of multiplicative $\mathcal{G}$-field extensions of the form $K(L)/K$ to the notion of flasque equivalence $\underset{\text{fl}}{\sim}$ that was studied in Section 2.7. Various versions of the result can be found in the literature. Part (c) is identical with Endo and Miyata [56, Theorem 1.6]; see also Lenstra [118, Theorem 1.7]. Further relevant references include Voskresenskiĭ [217], Colliot-Thélène and Sansuc [41] and Swan [208]. Recall that a $\mathcal{G}$-lattice L is called quasi-permutation if $L \underset{\text{fl}}{\sim} 0$ or, equivalently, there is an exact sequence of $\mathcal{G}$-lattices $0 \to L \to P \to Q \to 0$, where P and Q are permutation lattices; see 2.7.

Proposition 9.5.3. *Let $\mathcal{G}$ be a finite group, K a $\mathcal{G}$-field and let L, L' be $\mathcal{G}$-lattices.*

(a) *If the $\mathcal{G}$-fields $K(L)$ and $K(L')$ are stably isomorphic over K then $L \underset{\text{fl}}{\sim} L'$.*

(b) *Conversely, assume that $L \underset{\text{fl}}{\sim} L'$. If $K(L)$ and $K(L')$ are faithful $\mathcal{G}$-fields then $K(L)$ and $K(L')$ are stably isomorphic over K. In particular, $K(L)^{\mathcal{G}}$ and $K(L')^{\mathcal{G}}$ are stably isomorphic over $K^{\mathcal{G}}$ in this case.*

(c) *Assume that the $\mathcal{G}$-field K is faithful. Then the extension $K(L)^{\mathcal{G}}/K^{\mathcal{G}}$ is stably rational if and only if L is quasi-permutation.*

Proof. (a) Put $F = K(L)$ and $F' = K(L')$. By assumption, there is an isomorphism of $\mathcal{G}$-fields

$$E = F(x_1, \ldots, x_r) \xrightarrow{\sim} E' = F'(y_1, \ldots, y_s) \,,$$

which is the identity on K. Here, the x_i and y_j are commuting $\mathcal{G}$-invariant indeterminates over F and F', respectively. Consider the K-algebras

$$R = K[L][x_1, \ldots, x_s] \subseteq E \quad \text{and} \quad R' = K[L'][y_1, \ldots, y_t] \subseteq E' \,.$$

Both R and R' are affine $\mathcal{G}$-stable unique factorization domains, and $Q(R) = E$, $Q(R') = E'$. By Lemma 9.3.1, there are nonzero elements $a \in R^{\mathcal{G}}$ and $a' \in R'^{\mathcal{G}}$ so that

$$R[1/a] \xrightarrow{\sim} R'[1/a'] \,. \tag{9.8}$$

Focusing on R for now, put $M = \mathrm{U}(R[1/a])/K^*$ and note that M is a $\mathcal{G}$-module. Following Swan [208], we will show that there is an exact sequence of $\mathcal{G}$-modules

$$0 \to L \longrightarrow M \longrightarrow P \to 0 \,, \tag{9.9}$$

where P is a permutation $\mathcal{G}$-lattice. Indeed, since R is a UFD, the group $Q(R)^*/\,\mathrm{U}(R)$ is free abelian; a basis is given by a full set of non-associated irreducible elements of R. This basis is permuted by the operation of $\mathcal{G}$ on $Q(R)^*/\operatorname{U}(R)$. Write the element $a \in R^{\mathcal{G}}$ in (9.8) as $a = up_1^{e_1}p_2^{e_2}\dots p_n^{e_n}$ with non-associated irreducibles $p_i \in R$, $u \in \operatorname{U}(R)$ and $e_i > 0$. Since a is $\mathcal{G}$-invariant, the images of $\{p_1, \dots, p_n\}$ in $Q(R)^*/\operatorname{U}(R)$ span a (multiplicative) $\mathcal{G}$-permutation lattice. This will be the lattice P in (9.9). It is easy to see that $\operatorname{U}(R[1/a]) = \langle \operatorname{U}(R), p_1, \dots, p_n \rangle$. Hence we have a short exact sequence of $\mathcal{G}$-modules

$$1 \to \operatorname{U}(R) \longrightarrow \operatorname{U}(R[1/a]) \longrightarrow P \to 1\,.$$

Finally, $\operatorname{U}(R) = \operatorname{U}(K[L]) = K^* \times \underline{L}$ by Lemma 3.4.1. Thus, the sequence above yields the desired sequence (9.9).

Since all this applies to R' as well, we have an analogous sequence $0 \to L' \longrightarrow M' \longrightarrow P' \to 0$ with P' a permutation $\mathcal{G}$-lattice and $M' = \operatorname{U}(R'[1/a'])/K^*$. The isomorphism (9.8) induces an isomorphism of $\mathcal{G}$-lattices $M \xrightarrow{\sim} M'$. In view of Lemma 2.7.1(c), this proves that $L \underset{\text{fl}}{\sim} L'$.

(b) Now assume that $L \underset{\text{fl}}{\sim} L'$; so there are exact sequences of $\mathcal{G}$-lattices $0 \to L \to M \to P \to 0$ and $0 \to L' \to M \to P' \to 0$ with permutation $\mathcal{G}$-lattices P and P'. Put $F = K(L)$, $F' = K(L')$ and $E = K(M)$. Identifying L and L' with their images in M, we have $E = F(P)_\gamma = F'(P')_{\gamma'}$ and, by assumption, F and F' are faithful $\mathcal{G}$-fields. Therefore, by Lemma 9.4.3, $E^{\mathcal{G}}$ is rational over both $F^{\mathcal{G}}$ and $F'^{\mathcal{G}}$ and, consequently, $F^{\mathcal{G}}$ and $F'^{\mathcal{G}}$ are stably isomorphic over $K^{\mathcal{G}}$.

(c) This follows from (a) and (b) by taking $L' = 0$: L is quasi-permutation precisely if $L \underset{\text{fl}}{\sim} 0$ and, putting $F = K(L)$, the extension $F^{\mathcal{G}}/K^{\mathcal{G}}$ is stably rational if and only if F is stably isomorphic to K over K; see Lemma 9.2.1(a). □

The next result is due to Saltman [177], [179], at least for infinite fields K. Our proof of part (b) below works in general. Recall that $\mathsf{SP}_{\mathcal{G}}$ denotes the monoid of stable permutation classes of $\mathcal{G}$-lattices and $[L]^{\text{fl}} \in \mathsf{SP}_{\mathcal{G}}$ is the flasque equivalence class of the $\mathcal{G}$-lattice L; see Sections 2.3 and 2.7.

Proposition 9.5.4 (Saltman). *Let $\mathcal{G}$ be a finite group, K a faithful $\mathcal{G}$-field and L a $\mathcal{G}$-lattice. Then:*

(a) *Assume that K is infinite. If $K(L)^{\mathcal{G}}$ is retract rational over the subfield $\Bbbk \subseteq K^{\mathcal{G}}$ then so is $K^{\mathcal{G}}$.*
(b) *$K(L)^{\mathcal{G}}/K^{\mathcal{G}}$ is retract rational if and only if $[L]^{\text{fl}}$ is invertible in* $\mathsf{SP}_{\mathcal{G}}$.

Proof. (a) Put $F = K(L)$; so $F^{\mathcal{G}}/\Bbbk$ is retract rational and our goal is to show that $K^{\mathcal{G}}/\Bbbk$ is retract rational. Note that $K^{\mathcal{G}}/\Bbbk$ is certainly finitely generated, being a subextension of the finitely generated extension $F^{\mathcal{G}}/\Bbbk$. We first prove the following

Claim. There exists an affine $K^{\mathcal{G}}$-algebra $A \subseteq F^{\mathcal{G}}$ such that $F^{\mathcal{G}} = Q(A)$ and, for any $0 \neq a \in A$, there is a $K^{\mathcal{G}}$-algebra map $\alpha\colon A \to K^{\mathcal{G}}$ with $\alpha(a) \neq 0$.

Indeed, we may take $A = K[L]^{\mathcal{G}}$. Then $Q(A) = F^{\mathcal{G}}$ and, by Noether's finiteness theorem, A is affine over $K^{\mathcal{G}}$, since this certainly holds for $K[L]$. Now let

$0 \neq a \in A$ be given. In order to construct the desired map α, we may replace L by any $\mathcal{G}$-lattice containing L. In particular, replacing L by $L{\downarrow}^{\mathcal{G}}_{\langle 1\rangle}{\uparrow}^{\mathcal{G}}_{\langle 1\rangle}$ (see (1.13)) we may assume that L is free. Then $K[L]^{\mathcal{G}}$ is a localized polynomial algebra $K^{\mathcal{G}}[x_1,\dots,x_m][1/g]$ by Lemma 9.4.3. Since $K^{\mathcal{G}}$ is infinite, the existence of a $K^{\mathcal{G}}$-algebra map $\alpha\colon K^{\mathcal{G}}[x_1,\dots,x_m][1/g] \to K^{\mathcal{G}}$ with $\alpha(a) \neq 0$ follows from [27, Théorème IV.2.2]. This proves the claim.

To complete the proof of part (a), write the algebra A as $A = K^{\mathcal{G}}S$ for some affine $\Bbbk$-algebra $S \subseteq A$. Since $K^{\mathcal{G}}/\Bbbk$ is finitely generated, we may choose S so that $K^{\mathcal{G}} = Q(S \cap K^{\mathcal{G}})$. Hence, $Q(S) = Q(A) = F^{\mathcal{G}}$. By Lemma 9.3.2, some localization of S is a retract of a localized polynomial algebra over $\Bbbk$, say

$$\begin{tikzcd} S[1/s] \arrow[r, shift left, "\mu"] & \Bbbk[x_1,\dots,x_n][1/f] \arrow[l, shift left, "\pi"] \end{tikzcd} \tag{9.10}$$

with $\pi \circ \mu = \mathrm{Id}_{S[1/s]}$. Let $\alpha\colon A \to K^{\mathcal{G}}$ be as in the claim, with $\alpha(s) \neq 0$. Extend α to $A[1/s] \to K^{\mathcal{G}}$ and put $S' = \alpha(S[1/s])$; this is an affine $\Bbbk$-algebra of $K^{\mathcal{G}}$ with $S \cap K^{\mathcal{G}} = \alpha(S \cap K^{\mathcal{G}}) \subseteq S' \subseteq K^{\mathcal{G}} = Q(S \cap K^{\mathcal{G}})$. Hence, $Q(S') = K^{\mathcal{G}}$ and $S' \subseteq S[1/s']$ for some $0 \neq s' \in S \cap K^{\mathcal{G}}$. By (9.2), the retraction (9.10) extends to

$$\begin{tikzcd} S[1/ss'] \arrow[r, shift left, "\mu"] & \Bbbk[x_1,\dots,x_n][1/f'] \arrow[l, shift left, "\pi"] \end{tikzcd}$$

for some $0 \neq f' \in \Bbbk[x_1,\dots,x_n]$. Finally, since $\alpha\colon A[1/s] \to K^{\mathcal{G}}$ is the identity on $K^{\mathcal{G}}$, we also have a retraction $S'[1/s'] \underset{\alpha}{\overset{\beta}{\rightleftarrows}} S[1/ss']$, where β is the inclusion. Therefore, $S'[1/s']$ is a retract of a localized polynomial algebra over $\Bbbk$ and $Q(S'[1/s']) = K^{\mathcal{G}}$, which completes the proof of (a).

(b) First assume that $[L]^{\mathrm{fl}}$ is invertible in $\mathsf{SP}_{\mathcal{G}}$. Thus, there is an exact sequence of $\mathcal{G}$-lattices $0 \to L \to P \to M \to 0$ with P permutation and M invertible. Put $F = K(L)$ and $E = K(P)$. Then F is a faithful $\mathcal{G}$-field and we may assume that F is infinite, because (b) is clear for $L = 0$. Moreover, $E = F(M)$, because Hilbert's "Theorem 90" implies that $\mathrm{Ext}_{\mathbb{Z}[\mathcal{G}]}(M, F^*)$ is trivial; see Section 2.5. Finally, $E^{\mathcal{G}}/K^{\mathcal{G}}$ is rational by Lemma 9.4.3. Therefore, part (a) implies that $F^{\mathcal{G}}/K^{\mathcal{G}}$ is retract rational.

Conversely, assume that $F^{\mathcal{G}}/K^{\mathcal{G}}$ is retract rational. As in the proof of (a), put $A = K[L]^{\mathcal{G}}$ and recall that A is affine over $K^{\mathcal{G}}$ with $Q(A) = F^{\mathcal{G}}$. Therefore, Lemma 9.3.2 yields $K^{\mathcal{G}}$-algebra maps

$$\begin{tikzcd} A[1/a] \arrow[r, shift left, "\mu"] & K^{\mathcal{G}}[x_1,\dots,x_n][1/f] \arrow[l, shift left, "\pi"] \end{tikzcd}$$

with $\pi \circ \mu = \mathrm{Id}$ for suitable nonzero $a \in A$ and $f \in K^{\mathcal{G}}[x_1,\dots,x_n]$. Applying $K \otimes_{K^{\mathcal{G}}} (\,.\,)$ to this diagram and using the fact that $K \otimes_{K^{\mathcal{G}}} A \cong K[L]$ (see Lemma 9.4.1), we obtain $\mathcal{G}$-equivariant K-algebra maps

$$\begin{tikzcd} K[L][1/a] \arrow[r, shift left, "\mu'"] & K[x_1,\dots,x_n][1/f] \arrow[l, shift left, "\pi'"] \end{tikzcd}$$

with $\pi' \circ \mu' = \mathrm{Id}$. Restricting to unit groups modulo K^* we deduce that the $\mathcal{G}$-module $M = \mathrm{U}(K[L][1/a])/K^*$ is a direct summand of $P = \mathrm{U}(K[x_1, \ldots, x_n][1/f])/K^*$. As in the proof of Proposition 9.5.3(a), one sees that P is a permutation $\mathcal{G}$-lattice: a $\mathcal{G}$-stable $\mathbb{Z}$-basis is given by the irreducible factors of f in $K[x_1, \ldots, x_n]$. Therefore, M is a permutation projective $\mathcal{G}$-lattice. Moreover, L embeds into M and, exactly as P, the factor $Q = M/L$ is a permutation $\mathcal{G}$-lattice. Invoking Lemma 2.7.1(a),(b) we obtain $[L]^{\mathrm{fl}} = [M]^{\mathrm{fl}} = -[M]$, which shows that $[L]^{\mathrm{fl}}$ is invertible in $\mathsf{SP}_{\mathcal{G}}$. □

L is monomial	$\underset{\text{Prop. 9.5.1}}{\Longrightarrow}$	$K(L)^{\mathcal{G}}/K^{\mathcal{G}}$ is rational
L is quasi-permutation ($[L]^{\mathrm{fl}} = [0]$ in $\mathsf{SP}_{\mathcal{G}}$)	$\underset{\text{Prop. 9.5.3(c)}}{\Longleftrightarrow}$	$K(L)^{\mathcal{G}}/K^{\mathcal{G}}$ is stably rational
$[L]^{\mathrm{fl}}$ is invertible in $\mathsf{SP}_{\mathcal{G}}$	$\underset{\text{Prop. 9.5.4(b)}}{\Longleftrightarrow}$	$K(L)^{\mathcal{G}}/K^{\mathcal{G}}$ is retract rational

Fig. 9.1. Rationality properties of function fields of tori: $\mathcal{G}$ is a finite group, K a faithful $\mathcal{G}$-field, and L a $\mathcal{G}$-lattice

9.6 Some Rationality Results for Multiplicative Invariant Fields

In this section, we consider ordinary multiplicative $\mathcal{G}$-fields, that is, $\mathcal{G}$-fields of the form $\Bbbk(L) = Q(\Bbbk[L])$, where $\mathcal{G}$ is a finite group, L a $\mathcal{G}$-lattice and $\Bbbk$ a field with trivial $\mathcal{G}$-action. For reference, we state the following proposition which is a special case of results in Section 9.5.

Proposition 9.6.1. *Let L and L' be $\mathcal{G}$-lattices for the finite group $\mathcal{G}$.*

(a) *If the multiplicative $\mathcal{G}$-fields $\Bbbk(L)$ and $\Bbbk(L')$ are stably isomorphic over $\Bbbk$ then $L \underset{\mathrm{fl}}{\sim} L'$.*

(b) *Conversely, if $L \underset{\mathrm{fl}}{\sim} L'$ and L and L' are faithful then the $\mathcal{G}$-fields $\Bbbk(L)$ and $\Bbbk(L')$ are stably isomorphic over $\Bbbk$. In particular, the fixed fields $\Bbbk(L)^{\mathcal{G}}$ and $\Bbbk(L')^{\mathcal{G}}$ are stably isomorphic over $\Bbbk$ in this case.*

(c) *Assume that L is faithful and a direct summand of L'. If $\Bbbk(L')^{\mathcal{G}}/\Bbbk$ is retract rational then $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational as well.*

Proof. Parts (a) and (b) follow from Proposition 9.5.3(a),(b) with $K = \Bbbk$, while (c) follows from Proposition 9.5.4(a) with $K = \Bbbk(L)$. Note that we may assume that K is infinite, since (c) is trivial for $L = 0$. □

We now turn to the question when $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is rational. By a case-by-case analysis, it was shown in Hajja and Kang [84] that the extension $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is rational for all $\mathcal{G}$-lattices L with $\operatorname{rank} L \leq 3$, with the possible exception of the signed root lattice $L = A_3 \otimes_{\mathbb{Z}} \mathbb{Z}^-$ for the symmetric group $\mathcal{G} = \mathcal{S}_4$; rationality for this lattice is apparently still open. Starting with $\operatorname{rank} L = 4$, however, the extension $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ need no longer be rational or even retract rational. Indeed, by a result of Saltman (see Theorem 9.6.6 below), the extension $\mathbb{Q}(\mathcal{C}_8)/\mathbb{Q}$ for the cyclic group $\mathcal{C}_8$ of order 8 is not retract rational. Since $\mathcal{C}_8$ acts faithfully on the lattice $L = \mathbb{Z}^4$ through the matrix $\left(\begin{smallmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right)$, it follows from Proposition 9.4.4(c) that $\mathbb{Q}(L)^{\mathcal{C}_8}/\mathbb{Q}$ is not retract rational either (cf. also Hajja [82, Lemma 3]). Furthermore, for any prime p and any field $\Bbbk$ with $\operatorname{char} \Bbbk \neq p$, Saltman [176] has constructed a group $\mathcal{G}$ of order p^9 such that $\Bbbk(\mathcal{G})/\Bbbk$ is not retract rational. Smaller examples have subsequently been produced by Bogomolov [18] and Saltman [179]. All these non-rationality results for field extensions $K/\Bbbk$ are based on computations of the so-called unramified Brauer group $\operatorname{Br}_{\text{ur}}(K/\Bbbk)$ which was introduced by Saltman in [176],[178]. Retract rationality of $K/\Bbbk$ forces the equality $\operatorname{Br}_{\text{ur}}(K/\Bbbk) = \operatorname{Br}(\Bbbk)$; see [179, Theorem 2.1]. The unramified Brauer group of (twisted) multiplicative invariant fields was determined in Saltman [181]; for linear invariant fields, the calculation was done independently by Bogomolov [18] and Saltman. An alternative calculation of the unramified Brauer group of (twisted) multiplicative invariant fields, via a reduction to the linear case (cf. Proposition 3.8.2), can be found in Barge [3], [4]. In other language, the unramified Brauer group is the case $i = 2$ of the unramified cohomology H^i_{ur} as defined by Colliot-Thélène and Ojanguren in [40]. The unramified cohomology H^3_{ur} of linear and multiplicative invariant fields forms the subject of Saltman [184] and [185]. Finally, we mention a result of Beneish [9, Theorem 2.3]: if $\Bbbk$ algebraically closed and $\mathcal{G}$ is a finite group whose Schur multiplier is zero then for any central extension $\mathcal{G}'$ of $\mathcal{G}$, the fields $\Bbbk(\mathcal{G}')$ and $\Bbbk(\mathcal{G})$ are stably isomorphic over $\Bbbk$.

The following positive result is due to Farkas [61].

Theorem 9.6.2 (Farkas). *If the finite group $\mathcal{G}$ acts as a reflection group on the lattice L then the multiplicative invariant field $\Bbbk(L)^{\mathcal{G}}$ is rational over $\Bbbk$.*

Proof. By [22, Prop. V.1.23], $\Bbbk(L)^{\mathcal{G}} = Q(\Bbbk[L]^{\mathcal{G}})$ and Theorem 6.1.1 tells us that $\Bbbk[L]^{\mathcal{G}} = \Bbbk[M]$ for some affine normal semigroup M. Recall from Section 3.4 that M embeds into some lattice L' with $L' = \langle M \rangle_{\text{group}}$. Then $Q(\Bbbk[M]) = Q(\Bbbk[L']) = \Bbbk(L')$ and so $\Bbbk(L)^{\mathcal{G}} = \Bbbk(L')$ is rational over $\Bbbk$. □

Example 9.6.3 (The multiplicative invariant field of $\mathcal{W}(A_{n-1}) = \mathcal{S}_n$)**.** As an illustration, we calculate the multiplicative invariant field of the $\mathcal{S}_n$-root lattice A_{n-1}. Recall from Example 3.5.6 that $\Bbbk[A_{n-1}]^{\mathcal{S}_n} = \Bbbk[M]$, where M is the multiplicative submonoid consisting of all elements

$$\mu_m = \prod_{i=1}^{n-1} s_i^{t_i} \cdot s_n^{-\frac{1}{n}\sum_i it_i} = \prod_{i=1}^{n-1} \left(\frac{s_i}{s_1^i}\right)^{t_i} \cdot \left(\frac{s_1^n}{s_n}\right)^{\frac{1}{n}\sum_i it_i} \in \Bbbk[A_{n-1}]^{\mathcal{S}_n}$$

with $m = (t_1, \ldots, t_{n-1}) \in \mathbb{Z}_+^{n-1}$ and $\sum_i it_i$ divisible by n. Here, as usual, s_i denotes the i^{th} elementary symmetric function in $x_1, \ldots, x_n$. The group of fractions $\langle M \rangle_{\text{group}}$ is the free abelian multiplicative group generated by the elements s_i/s_1^i $(i = 2, \ldots, n)$. Thus,

$$\Bbbk(A_{n-1})^{\mathcal{S}_n} = \Bbbk(s_i/s_1^i \mid i = 2, \ldots, n) \, .$$

For an alternative proof, without first calculating $\Bbbk[A_{n-1}]^{\mathcal{S}_n}$, see Hajja and Kang [85].

The next result, due to Lemire [115], depends on Theorem 9.6.2 but goes far beyond it. We refer to the original publication [115] for the proof.

Theorem 9.6.4 (Lemire)**.** *Let $\varPhi$ be a reduced root system and $\mathcal{G} = \operatorname{Aut}(\varPhi)$ its automorphism group. Then, for any $\mathcal{G}$-lattice L that is rationally isomorphic to the root lattice of $\varPhi$, the multiplicative invariant field $\Bbbk(L)^{\mathcal{G}}$ is rational over $\Bbbk$.*

Example 9.6.5 (The multiplicative invariant field of $\operatorname{Aut}(A_{n-1})$)**.** We illustrate Lemire's theorem by proving rationality of the invariant field $K = \Bbbk(A_{n-1})^{\mathcal{G}}$ over $\Bbbk$, where $\mathcal{G} = \operatorname{Aut}(A_{n-1}) = \{\pm 1\} \times \mathcal{S}_n$; see (1.30). By Example 9.6.3, $K = \Bbbk(\sigma_2, \ldots, \sigma_n)^{\langle \pm 1 \rangle}$, where $\sigma_i = s_i/s_1^i$. Put $g = -1 \in \mathcal{G}$; so $g(m) = -m$ for all $m \in U_n$ and hence $g(x_i) = x_i^{-1}$, where $x_i = \mathbf{x}^{e_i}$ as usual. Therefore, $g(s_i) = s_{n-i}/s_n$ (with $s_0 = 1$) and hence

$$g(\sigma_i) = \frac{s_{n-i} s_n^i}{s_n s_{n-1}^i} = \sigma_{n-i} \sigma_n^{i-1} \sigma_{n-1}^{-i} \, .$$

This formula shows that g stabilizes the multiplicative sublattice $A = \langle \sigma_2, \ldots, \sigma_n \rangle$ of the field K as well as its sublattice $B = \langle \sigma_{n-1}, \sigma_n \rangle$. Moreover, A/B is a $\langle g \rangle$-permutation lattice and g acts on the sublattice B as the reflection $\left(\begin{smallmatrix} -n+1 & -n \\ n-2 & n-1 \end{smallmatrix} \right)$. The former implies that $K = \Bbbk(A)^{\langle g \rangle}$ is rational over $\Bbbk(B)^{\langle g \rangle}$; see Lemma 9.4.3. Moreover, by Theorem 9.6.2 (or an easy direct verification), $\Bbbk(B)^{\langle g \rangle}$ is rational over $\Bbbk$, thereby proving rationality of $K/\Bbbk$.

We conclude this subsection by stating, without proof, a rationality result of Saltman [177, Theorem 4.12] that was alluded to earlier. The result is stated in [177] for linear rather than multiplicative invariant fields but this difference is insubstantial in view of Propositions 9.4.4(b) and 9.6.1(b).

Theorem 9.6.6 (Saltman)**.** *Let $\mathcal{G}$ be a finite abelian group, L a faithful quasi-permutation $\mathcal{G}$-lattice, $\Bbbk$ an infinite field, and $\mu_q(\overline{\Bbbk})$ the group of all q^{th} roots of unity in an algebraic closure $\overline{\Bbbk}$, where q is the largest power of 2 dividing the exponent of $\mathcal{G}$. Then the extension $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational if and only if $\Bbbk(\mu_q(\overline{\Bbbk}))/\Bbbk$ is cyclic.*

In particular, if $\mathcal{G}$ is a finite abelian group then $\mathbb{Q}(\mathcal{G})/\mathbb{Q}$ is retract rational if and only if $\mathcal{G}$ has no element of order 8; see Ireland and Rosen [95, Theorem 4.2′].

9.7 Some Concepts from Algebraic Geometry

Throughout this section, we assume that $\Bbbk$ is an algebraically closed field. All algebraic varieties and algebraic groups under consideration and all maps between them are assumed to be defined over $\Bbbk$. Furthermore, for simplicity, we assume that all algebraic varieties are irreducible.

9.7.1 Rational Maps

A *rational map* of algebraic varieties $f\colon X \dashrightarrow Y$ is an equivalence class of regular maps $U \to Y$, where U is a nonempty open subset of X; two regular maps $U_1 \to Y$ and $U_2 \to Y$ are considered equivalent if they agree on $U_1 \cap U_2$. The domain of definition $\operatorname{dom} f$ of a rational map f is the union of all open subsets U where f is defined; the complement $X \setminus \operatorname{dom} f$ is called the indeterminacy locus of f. The rational map $f\colon X \dashrightarrow Y$ is called dominant if $f(U)$ is dense in Y for some (and hence every) nonempty open subset $U \subseteq X$ where f is defined. In this case, for any rational map $g\colon Y \dashrightarrow Z$, there is a well-defined composite $g \circ f\colon X \dashrightarrow Z$. In general, the composite $g \circ f$ is well-defined provided, for some (and hence every) nonempty open subset $U \subseteq X$ where f is defined, $f(U)$ is not contained in the indeterminacy locus of g. Rational maps $X \dashrightarrow \mathbb{A}^1$ are called *rational functions* on X; they form an extension field of $\Bbbk$ that will be denoted by $\mathcal{K}(X)$. There is a bijection between the set of dominant rational maps $f\colon X \dashrightarrow Y$ and the set k-algebra maps $\mathcal{K}(Y) \to \mathcal{K}(X)$. A dominant rational map is called birational if the corresponding map of function fields is an isomorphism.

9.7.2 G-Varieties

Let G be an algebraic group. A *G-variety* is an algebraic variety X with a regular action $G \times X \to X$. Morphisms of G-varieties are understood to be G-equivariant. The action of G on X induces actions on the algebras $\mathcal{O}(X)$ and $\mathcal{K}(X)$ of regular and rational functions on X. Here, we are mostly interested in the latter, especially in the invariant subfield $\mathcal{K}(X)^G$.

9.7.3 The Rational Quotient

The field $\mathcal{K}(X)^G$ of invariant rational functions of a G-variety X defines, up to birational equivalence, an algebraic variety X/G with $\mathcal{K}(X/G) = \mathcal{K}(X)^G$. The embedding $\mathcal{K}(X)^G \hookrightarrow \mathcal{K}(X)$ corresponds to a dominant rational map

$$\pi\colon X \dashrightarrow X/G\,,$$

called the *rational quotient* of X with respect to G. The following properties of π will be important for us; see Popov and Vinberg [153, Sect. 2.4] or Reichstein [158, Sect. 2.3] for details:

(a) π separates G-orbits in general position in X: there exists a nonempty open subset $X_0 \subseteq X$ such that π is regular on X_0 and $x, x' \in X_0$ lie in the same G-orbit iff $\pi(x) = \pi(x')$ (Rosenlicht [171, 172]).
(b) π is unique in the following sense. If $f\colon X \dashrightarrow Y$ is a dominant rational map separating G-orbits in general position then there is a birational map $\overline{f}\colon X/G \overset{\sim}{\dashrightarrow} Y$ such that $f = \overline{f} \circ \pi$.

9.7.4 Relative Sections

Let X be a G-variety. In investigating the structure of the invariant algebra $K(X)^G$ the following notion, originally due to Katsylo [105] (see also Popov [152] and Popov-Vinberg [153]) is often useful. Let H be a closed subgroup of the algebraic group G. An H-stable subvariety $S \subseteq X$ is called a *(G,H)-section* if

(a) GS is dense in X and
(b) there is a nonempty open subset $S_0 \subseteq S$ so that $gS_0 \cap S \neq \varnothing$ implies $g \in H$.

Lemma 9.7.1. *Let X be a G-variety and $S \subseteq X$ a (G,H)-section. Then $\mathcal{K}(X)^G \cong \mathcal{K}(S)^H$ via restriction.*

Proof. Let $\pi\colon X \dashrightarrow X/G$ be the rational quotient. The indeterminacy locus of π is a proper G-invariant closed subvariety of X. In view of condition (a), such a subvariety cannot contain S. Since S is irreducible, it follows that the restriction $\pi|_S\colon S \dashrightarrow X/G$ is well-defined. Conditions (a) and (b) above imply that $\pi|_S$ is dominant and separates H-orbits in general position in S. Thus, by uniqueness of the rational quotient map, $S/H \overset{\sim}{\dashrightarrow} X/G$, which proves the lemma. □

9.8 The Field of Matrix Invariants as a Multiplicative Invariant Field

We continue to assume that $\Bbbk$ is an algebraically closed field. Let $\mathrm{M}_n = \mathrm{M}_n(\Bbbk)$ denote the space of $n \times n$-matrices over $\Bbbk$, and let r be an integer ≥ 2. The group $\mathrm{PGL}_n = \mathrm{GL}_n(\Bbbk)/\Bbbk^*$ operates on the space M_n^r of r-tuples of $n \times n$-matrices over $\Bbbk$ by simultaneous conjugation:

$$^{g}(A_1, \dots, A_r) = (gA_1g^{-1}, \dots, gA_rg^{-1}) \tag{9.11}$$

for $g \in \mathrm{PGL}_n$ and $A_i \in \mathrm{M}_n$. As in §9.1.3, this action gives rise to PGL_n-actions on the algebra of polynomial functions on M_n^r,

$$\mathcal{O}(\mathrm{M}_n^r) = \mathsf{S}((\mathrm{M}_n^r)^*) ,$$

and on the algebra of rational functions,

$$\mathcal{K}(\mathrm{M}_n^r) = Q(\mathcal{O}(\mathrm{M}_n^r)) .$$

Explicitly, $\mathcal{O}(\mathrm{M}_n^r)$ is the polynomial algebra over $\Bbbk$ with standard generators $x_{i,j}^{(\ell)}$ $(1 \le i,j \le n, 1 \le \ell \le r)$, where $x_{i,j}^{(\ell)}$ sends $(A_1,\dots,A_r) \in \mathrm{M}_n^r$ to the (i,j)-entry of the matrix A_ℓ. The field $\mathcal{K}(\mathrm{M}_n^r)$ is the rational function field of degree rn^2 over $\Bbbk$,

$$\mathcal{K}(\mathrm{M}_n^r) = \Bbbk(x_{i,j}^{(\ell)} \mid 1 \le i,j \le n, 1 \le \ell \le r)\,.$$

The ultimate goal, as yet unachieved, is to prove (stable, retract) rationality of the invariant field $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ over $\Bbbk$. See Le Bruyn [114] and Formanek [66] for excellent surveys on this and related problems. The algebra $\mathcal{O}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ has been determined by Procesi [155] in characteristic 0 and by Donkin [52] in general. For $r = 1$, the result is classical: $\mathcal{O}(\mathrm{M}_n)^{\mathrm{PGL}_n}$ is a polynomial algebra in n variables over $\Bbbk$; cf., e.g., Springer [201, Theorem 1.5.7].

The invariant field $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ can be expressed as the multiplicative invariant field arising from a suitable lattice for the symmetric group $\mathcal{S}_n$; see Theorem 9.8.2 below. In the present very explicit form, the result was proved by Formanek [64, Theorems 3 and 8] building on work of Procesi [154]. Both these papers are concerned with the center of the so-called generic division algebra $\mathrm{UD}(\Bbbk, n, r)$, but this center can be identified with the invariant field $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$; see Procesi [155] in characteristic 0 and Donkin [52] or Saltman [186] in general. The proof of the Formanek-Procesi theorem given below, using relative sections, follows the outline of Popov [152].

We will need the following auxiliary lemma on twisted multiplicative invariant fields.

Lemma 9.8.1. *Let $K(L)_\gamma$ be a twisted multiplicative G-field, where G is an arbitrary group acting trivially on the field K and on the lattice L. Then $K(L)_\gamma^G = K(M)$, where M is the kernel of the map $L \to \mathrm{Hom}(G, K^*)$, $m \mapsto \gamma_m$; see* (3.20). *In particular, $K(L)_\gamma^G/K$ is rational.*

Proof. Recall from (3.19) that G acts on $K_\gamma[L]$ via

$$g(\sum_{m\in L} k_m \mathbf{x}^m) = \sum_{m \in L} k_m \gamma_m(g)\mathbf{x}^m$$

with $\gamma_m(g) \in K^*$. By (3.20) the map $m \mapsto \gamma_m$ is a homomorphism $L \to \mathrm{Hom}(G, K^*)$. The sublattice $M \subseteq L$ is the kernel of this map. Thus, putting $F = K(M) \subseteq K(L)_\gamma$, we clearly have $F \subseteq K(L)_\gamma^G$. For the reverse inclusion, consider the G-subring $R = F\underline{L} \subseteq K(L)_\gamma$; so $K(L)_\gamma = Q(R)$.

Claim. R has no nontrivial G-stable ideals and $R^G = F$.

To prove this, fix a transversal $\mathcal{T}$ for M in L with $0 \in \mathcal{T}$. Then $R = \bigoplus_{t\in\mathcal{T}} F\mathbf{x}^t$ and G acts on R via $r = \sum_{t\in\mathcal{T}} f_t\mathbf{x}^t \mapsto g(r) = \sum_{t\in\mathcal{T}} f_t\gamma_t(g)\mathbf{x}^t$. If $f_t \neq 0$ for some $t \neq 0$ then $r \notin R^G$, because $\gamma_t(g) \neq 1$ for some $g \in G$. This shows that $R^G = F$. Next let I be a nonzero G-stable ideal of R and choose $0 \neq r \in I$ having a minimal number of nonzero terms $f_t\mathbf{x}^t$. We may assume that $f_0 = 1$. If $r \neq 1$ then, for some $g \in G$, we have $0 \neq r - g(r) = \sum_{0\neq t\in\mathcal{T}} f_t(1-\gamma_t(g))\mathbf{x}^t \in I$; this element has fewer nonzero terms than r, contrary to our choice. Therefore, $r = 1$ which proves the claim.

Now consider an invariant $q \in K(L)^G_\gamma$. Then $I = \{r \in R \mid rq \in R\}$ is a nonzero G-stable ideal of R. Hence, the claim implies that $q \in R^G = F$, as desired. □

Recall that U_n denotes the standard permutation lattice for the symmetric group $\mathcal{S}_n$ and A_{n-1} is its root sublattice; see §1.3.3.

Theorem 9.8.2 (Formanek, Procesi). *Let $r \geq 2$. Then there is a $\Bbbk$-isomorphism*

$$\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n} \cong \Bbbk(L_{n,r})^{\mathcal{S}_n}$$

with $L_{n,r} = U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \oplus \left(U_n^{\otimes 2}\right)^{r-2}$. In particular, $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ is rational over $\mathcal{K}(\mathrm{M}_n^2)^{\mathrm{PGL}_n}$ and

$$\mathcal{K}(\mathrm{M}_n^2)^{\mathrm{PGL}_n} \cong \Bbbk(L_n)^{\mathcal{S}_n} \ ,$$

where $L_n = U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}$.

Proof. Let $T_{n-1} = (\mathbb{G}_{\mathrm{m}})^n/\Delta$ be the maximal torus of PGL_n consisting of the images of the diagonal matrices in GL_n. Here, $\mathbb{G}_{\mathrm{m}} = \Bbbk^*$ is the multiplicative group and $\Delta = \mathbb{G}_{\mathrm{m}}$ denotes the scalar matrices in $(\mathbb{G}_{\mathrm{m}})^n$. The normalizer $N(T_{n-1})$ of T_{n-1} in PGL_n is generated by T_{n-1} and the images in PGL_n of the $n \times n$-permutation matrices; it is isomorphic to the semidirect product $T_{n-1} \rtimes \mathcal{S}_n$ with $\mathcal{S}_n$ acting on T_{n-1} by permuting the n copies of $\mathbb{G}_{\mathrm{m}}$. The $\mathcal{S}_n$-action on T_{n-1} yields an $\mathcal{S}_n$-action on the character lattice $X(T_{n-1}) = \mathrm{Hom}(T_{n-1}, \mathbb{G}_{\mathrm{m}})$ via $(sf)(t) = f(s^{-1}ts)$ for $t \in T_{n-1}$, $s \in \mathcal{S}_n$. Explicitly, $X(\mathbb{G}_{\mathrm{m}}^n) \cong \mathbb{Z}^n$, with $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{Z}^n$ corresponding to $\chi_{\mathbf{i}} \colon (\lambda_1, \ldots, \lambda_n) \mapsto \prod_j \lambda_j^{i_j}$ of $\mathbb{G}_{\mathrm{m}}^n$. The character $\chi_{\mathbf{i}}$ passes down to T_{n-1} if and only if $\lambda^{\sum_j i_j} = 1$ holds for all $\lambda \in \Bbbk^*$ which amounts to $\sum_j i_j = 0$. Taking $\mathcal{S}_n$-actions into account, we see that

$$X(\mathbb{G}_{\mathrm{m}}^n) \cong U_n \qquad \text{and} \qquad X(T_{n-1}) \cong A_{n-1} \tag{9.12}$$

as $\mathcal{S}_n$-lattices.

View M_n^r as a PGL_n-variety isomorphic to affine space $\mathbb{A}^{rn^2}$ via (9.11). Put $S = \mathrm{D}_n \oplus \mathrm{M}_n^{r-1} \subseteq \mathrm{M}_n^r$, where $\mathrm{D}_n \subseteq \mathrm{M}_n$ is the space of diagonal matrices. Then S is a $(\mathrm{PGL}_n, N(T_{n-1}))$-section of M_n^r in the sense of §9.7.4. Indeed, the matrices in M_n with distinct eigenvalues form a PGL_n-stable dense open subset $E \subseteq \mathrm{M}_n$ (cf., e.g., Springer [201, 1.5.6]). The PGL_n-orbits in E are in bijection with the $\mathcal{S}_n$-orbits in $\mathrm{D}_n' = E \cap \mathrm{D}_n$ via Jordan canonical form, and the isotropy group in PGL_n of any matrix in D_n' is exactly T_{n-1}. Thus, we may take $S_0 = \mathrm{D}_n' \oplus \mathrm{M}_n^{r-1}$ in §9.7.4 and Lemma 9.7.1 yields a $\Bbbk$-isomorphism

$$\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n} \cong \mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})^{T_{n-1} \rtimes \mathcal{S}_n} \ .$$

In order to further simplify the right hand side above, let $x_i = x_{i,i}^{(1)}$ and $x_{i,j}^{(\ell)}$ $(2 \leq \ell \leq r)$ be the standard coordinates on D_n and M_n^{r-1} respectively. In this coordinate system, the $\mathcal{S}_n$-action on $\mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})$ is given by

$$s(x_i) = x_{s(i)} \quad \text{and} \quad s(x_{i,j}^{(\ell)}) = x_{s(i),s(j)}^{(\ell)} \,. \tag{9.13}$$

An element $t = (t_1, \ldots, t_n)$ of $T_{n-1} = (\mathbb{G}_\mathrm{m})^n/\Delta$ acts via

$$t(x_i) = x_i \quad \text{and} \quad t(x_{i,j}^{(\ell)}) = t_i^{-1} t_j x_{i,j}^{(\ell)} \,. \tag{9.14}$$

Let $M \leq \mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})^*$ denote the multiplicative group generated by the coordinates x_i, $x_{i,j}^{(\ell)}$ $(\ell \geq 2)$. The torus T_{n-1} acts on M via

$$t(m) = \gamma_m(t) m \quad (t \in T_{n-1}, m \in M) \,,$$

where $\gamma_m \colon T_{n-1} \to \mathbb{G}_\mathrm{m}$ is the character explicitly given by (9.14). Thus, the T_{n-1}-field $\mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})$ is the twisted multiplicative T_{n-1}-field $\Bbbk(M)_\gamma$ and Lemma 9.8.1 gives

$$\mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})^{T_{n-1}} = \Bbbk(L) \,,$$

where L denotes the kernel of the homomorphism $\gamma \colon M \to X(T_{n-1})$, $m \mapsto \gamma_m$. By (9.13), M is $\mathcal{S}_n$-stable and a simple calculation shows that γ is $\mathcal{S}_n$-equivariant. Thus, L is an $\mathcal{S}_n$-sublattice of M and

$$\mathcal{K}(\mathrm{D}_n \oplus \mathrm{M}_n^{r-1})^{T_{n-1} \rtimes \mathcal{S}_n} = \Bbbk(L)^{\mathcal{S}_n} \,,$$

an ordinary multiplicative $\mathcal{S}_n$-invariant field.

In order to establish the first isomorphism in the theorem, we must show that $L \cong U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \oplus \left(U_n^{\otimes 2}\right)^{r-2}$ as $\mathcal{S}_n$-lattices. Using the notation of §1.3.3, equations (9.13) show that the multiplicative $\mathcal{S}_n$-lattice $M = \langle x_i, x_{i,j}^{(\ell)} \rangle$ is isomorphic to the additive $\mathcal{S}_n$-lattice $U_n \oplus \left(U_n^{\otimes 2}\right)^{r-1}$ via $x_i \mapsto e_i \in U_n$ and $x_{i,j}^{(\ell)} \mapsto e_i \otimes e_j \in U_n^{\otimes 2}$. Identifying $X(T_{n-1})$ with A_{n-1} as in (9.12), the map $\gamma \colon M \to X(T_{n-1})$ that was considered above becomes the map $f \colon U_n \oplus \left(U_n^{\otimes 2}\right)^{r-1} \twoheadrightarrow A_{n-1}$ that vanishes on U_n and sends each summand $U_n^{\otimes 2}$ onto A_{n-1} via $(e_i \otimes e_j) \mapsto e_j - e_i$; see (9.14). Therefore, $L = \operatorname{Ker} \gamma \cong \operatorname{Ker} f = U_n \oplus \operatorname{Ker}\left(f\big|_{(U_n^{\otimes 2})^{r-1}}\right)$. Moreover, $\operatorname{Ker}\left(f\big|_{(U_n^{\otimes 2})^{r-1}}\right) \cong \operatorname{Ker}\left(f\big|_{U_n^{\otimes 2}}\right) \oplus \left(U_n^{\otimes 2}\right)^{r-2}$ via $(m_1, \ldots, m_{r-1}) \mapsto (\sum m_i, m_2, \ldots, m_{r-1})$. Therefore,

$$L \cong U_n \oplus L' \oplus \left(U_n^{\otimes 2}\right)^{r-2} \,,$$

where we have put $L' = \operatorname{Ker}\left(f\big|_{U_n^{\otimes 2}}\right)$. It suffices to show that $L' \cong U_n \oplus A_{n-1}^{\otimes 2}$. Note that

$$U_n^{\otimes 2} = \left(\bigoplus_i \mathbb{Z}(e_i \otimes e_i)\right) \oplus \left(\bigoplus_{r \neq s} \mathbb{Z}(e_r \otimes e_s)\right) \,.$$

The elements $e_i \otimes e_i$ span a sublattice of L' isomorphic to U_n. Denoting the second summand above by P, we recall the $\mathcal{S}_n$-isomorphism (2.19):

$$A_{n-1} \otimes U_n \xrightarrow{\sim} P\,, \quad (e_s - e_r) \otimes e_s \mapsto e_r \otimes e_s\ .$$

With this identification, $f|_P$ becomes the map $\mathrm{Id} \otimes \varepsilon_n \colon A_{n-1} \otimes U_n \to A_{n-1} \otimes \mathbb{Z} = A_{n-1}$ with $\varepsilon_n \colon U_n \to \mathbb{Z}$ as in (1.10). Since $\mathrm{Ker}(\mathrm{Id} \otimes \varepsilon_n) = A_{n-1}^{\otimes 2}$, we obtain $L' \cong U_n \oplus A_{n-1}^{\otimes 2}$, as desired.

It remains to show that $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ is rational over $\mathcal{K}(\mathrm{M}_n^2)^{\mathrm{PGL}_n}$. By the foregoing, we may identify $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\mathcal{K}(\mathrm{M}_n^2)^{\mathrm{PGL}_n}$ with $\Bbbk(L_{n,r})^{\mathcal{S}_n}/\Bbbk(L_{n,2})^{\mathcal{S}_n}$ and $L_{n,r} = L_{n,2} \oplus \left(U_n^{\otimes 2}\right)^{r-2}$. Since $\left(U_n^{\otimes 2}\right)^{r-2}$ is a permutation $\mathcal{S}_n$-lattice and $\Bbbk(L_{n,2})$ is a faithful $\mathcal{S}_n$-field, rationality of the extension $\Bbbk(L_{n,r})^{\mathcal{S}_n}/\Bbbk(L_{n,2})^{\mathcal{S}_n}$ follows from Lemma 9.4.3. This completes the proof of the theorem. □

The above description of the field of matrix invariants as a multiplicative $\mathcal{S}_n$-invariant field, in conjunction with the analysis of the certain relevant $\mathcal{S}_n$-lattices in Section 2.12, yields the following rationality result. For $n = 2$, the result ultimately can be traced back to Sylvester [212]; see also Procesi [154, Theorem 2.2]. The cases $n = 3$ and $n = 4$ are due to Formanek [64], [65] while degrees $n = 5$ and $n = 7$ were first treated by Bessenrodt and Le Bruyn [17], with subsequent simplifications by Beneish [8]. Retract rationality of $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\Bbbk$ for prime degrees n was originally proved by different means in Saltman [177]; see also [186, Corollary 14.34]. We essentially follow the approach of Colliot-Thélène and Sansuc [42, proof of Corollary 9.13]. Part (b) is from [117], [127].

Theorem 9.8.3. (a) *The extension $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\Bbbk$ is rational for $n \leq 4$, stably rational for $n = 5$ and $n = 7$, and retract rational for all prime values of n.*

(b) *For all odd $n \geq 5$, $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ is rational over the multiplicative invariant field $\Bbbk(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$.*

Proof. We first show that $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\Bbbk$ is retract rational for prime degrees n. Recall from Theorem 9.8.2 that $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\Bbbk$ is isomorphic to $\Bbbk(L_{n,r})^{\mathcal{S}_n}/\Bbbk$ where $L_{n,r}$ is the $\mathcal{S}_n$-lattice $U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \oplus \left(U_n^{\otimes 2}\right)^{r-2}$. This lattice is faithful and permutation projective, the latter by Proposition 2.12.2(a). Say $L_{n,r}$ is a direct summand of the permutation $\mathcal{S}_n$-lattice P. Proposition 9.6.1(b) implies that $\Bbbk(P)^{\mathcal{S}_n}$ is stably isomorphic over $\Bbbk$ to $\Bbbk(U_n)^{\mathcal{S}_n} = \Bbbk(s_1, \ldots, s_n)$; see Example 3.5.5. Therefore, $\Bbbk(P)^{\mathcal{S}_n}/\Bbbk$ is stably rational, and hence retract rational (Proposition 9.3.3(b)). Retract rationality of $\Bbbk(L_{n,r})^{\mathcal{S}_n}/\Bbbk$ now follows from Proposition 9.6.1(c).

Next, we show that $\Bbbk(L_{n,r})^{\mathcal{S}_n}/\Bbbk$ is stably rational for $n = 5$ and $n = 7$. In both cases, the $\mathcal{S}_n$-lattice $A_{n-1}^{\otimes 2}$ is flasque equivalent to the weight lattice A_{n-1}^*; see Proposition 2.12.2(b). Therefore, $L_{n,r} \underset{\mathrm{fl}}{\sim} A_{n-1}^*$ and Proposition 9.6.1(b) yields that the fields $\Bbbk(L_{n,r})^{\mathcal{S}_n}$ and $\Bbbk(A_{n-1}^*)^{\mathcal{S}_n}$ are stably isomorphic over $\Bbbk$. Since $\Bbbk(A_{n-1}^*)^{\mathcal{S}_n}/\Bbbk$ is rational, by Example 3.7.1 or Proposition 9.6.2, the cases $n = 5$ and $n = 7$ are settled.

For the remainder of the proof we put

$$L_n = U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}\ ,$$

as in Theorem 9.8.2. In view of this result, the objective for the remaining cases $n = 2, 3, 4$ of part (a) is to prove that $\Bbbk(L_n)^{\mathcal{S}_n}/\Bbbk$ is rational. For (b), we will show that $\Bbbk(L_n)^{\mathcal{S}_n}$ is rational over $\Bbbk(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$ for all odd $n \geq 5$. Here, we view $\bigwedge^2 A_{n-1}$ as an $\mathcal{S}_n$-sublattice of $A_{n-1}^{\otimes 2}$ as in Lemma 1.4.1(b).

We first treat the cases $n \leq 3$.

$\mathbf{n = 2}$: The $\mathcal{S}_2$-lattice A_1 is the sign lattice $\mathbb{Z}^-$; so $A_1^{\otimes 2} = \mathbb{Z}$ and $L_2 = U_2 \oplus U_2 \oplus \mathbb{Z}$. By Lemma 9.4.3 with $L = U_2 \oplus \mathbb{Z}$, the field $\Bbbk(L_2)^{\mathcal{S}_2}$ is rational over $\Bbbk(U_2)^{\mathcal{S}_2}$, which in turn is rational over $\Bbbk$; see Example 3.5.5. Therefore, $\Bbbk(L_2)^{\mathcal{S}_2}/\Bbbk$ is rational.

$\mathbf{n = 3}$: Note that the exterior square $\bigwedge^2 A_2 = \mathbb{Z}_{\det A_2}$ is isomorphic to the sign lattice $\mathbb{Z}^-$ for $\mathcal{S}_3$. By Lemma 2.12.1(c), the symmetric square $\mathsf{S}^2 A_2$ is isomorphic to the standard permutation $\mathcal{S}_3$-lattice, U_3. Therefore, the exact sequence in Lemma 1.4.1(b) for $L = A_2$ takes the form $0 \to \mathbb{Z}^- \to A_2^{\otimes 2} \to U_3 \to 0$. This yields an exact sequence of $\mathcal{S}_3$-lattices

$$0 \to \mathbb{Z}^- \oplus U_3 \longrightarrow L_3 \longrightarrow U_3 \oplus U_3 \to 0\ .$$

Lemma 9.4.3 (with $L = U_3 \oplus U_3$) implies that $\Bbbk(L_3)^{\mathcal{S}_3}/\Bbbk(\mathbb{Z}^- \oplus U_3)^{\mathcal{S}_3}$ is rational, and Proposition 9.5.1 (with $L = \mathbb{Z}^-$) gives rationality of $\Bbbk(\mathbb{Z}^- \oplus U_3)^{\mathcal{S}_3}/\Bbbk(U_3)^{\mathcal{S}_3}$. Since $\Bbbk(U_3)^{\mathcal{S}_3}$ is rational over $\Bbbk$, we conclude that $\Bbbk(L_3)^{\mathcal{S}_3}$ is rational over $\Bbbk$ as well. (A different rationality proof for $K(\mathrm{M}_3^2)^{\mathrm{PGL}_3}$ using Clifford algebras can be found in Revoy [164].)

For $n \geq 4$, the $\mathcal{S}_n$-lattice $\bigwedge^2 A_{n-1}$ is faithful; in fact, $\bigwedge^2 A_{n-1} \otimes_{\mathbb{Z}} \mathbb{Q} \cong S^{(n-2,1^2)}$, the Specht module for the partition $(n-2, 1^2)$ of n; see [70, Exercise 4.6]. Furthermore, we know by Lemma 2.12.1(b),(d) that

$$\mathsf{S}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z} \text{ is a permutation lattice for } \mathcal{S}_n \text{ if } n = 4 \text{ or } n \text{ is odd.} \tag{9.15}$$

By Lemma 9.4.3 with $L = U_n$,

$$\Bbbk(L_n)^{\mathcal{S}_n} = \Bbbk(A_{n-1}^{\otimes 2} \oplus U_n)^{\mathcal{S}_n}(t_1, \ldots, t_n)$$

with transcendental elements t_i. The right hand side may also be written as $\Bbbk(A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z})^{\mathcal{S}_n}(t_1, \ldots, t_{n-1})$. The exact sequence in Lemma 1.4.1(b) for $L = A_{n-1}$ leads to an exact sequence of $\mathcal{S}_n$-lattices

$$0 \to \bigwedge^2 A_{n-1} \longrightarrow A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z} \longrightarrow \mathsf{S}^2 A_{n-1} \oplus \mathrm{U}_n \oplus \mathbb{Z} \to 0\ .$$

By (9.15) and Lemma 9.4.3, this sequence implies that $\Bbbk(A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z})^{\mathcal{S}_n}$ is rational over $\Bbbk(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$. Hence, if $n = 4$ or n is odd then $\Bbbk(L_n)^{\mathcal{S}_n} = \Bbbk(A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z})^{\mathcal{S}_n}(t_1, \ldots, t_{n-1})$ is rational over $\Bbbk(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$ as well. This proves part (b) of the theorem for $n = 4$ and all odd $n \geq 5$.

It remains to prove rationality of $\Bbbk(L_4)^{\mathcal{S}_4}/\Bbbk$.

$\mathbf{n = 4}$: The identity $\left(\bigwedge^2 A_3\right) \wedge A_3 = \bigwedge^3 A_3 \cong \mathbb{Z}_{\det A_3} = \mathbb{Z}^-$ shows that

$$\bigwedge^2 A_3 \cong \mathrm{Hom}(A_3, \mathbb{Z}^-) \cong A_3^* \otimes_{\mathbb{Z}} \mathbb{Z}^- \ .$$

It is known (but nontrivial) that $\Bbbk(A_3^* \otimes_{\mathbb{Z}} \mathbb{Z}^-)^{\mathcal{S}_4}$ is rational over $\Bbbk$. This was verified by Formanek [65, Theorems 13 and 14] and later again by Hajja and Kang [84, case $W_8(198)$]. Therefore, $\Bbbk(\bigwedge^2 A_3)^{\mathcal{S}_4}/\Bbbk$ is rational. Since $\Bbbk(L_4)^{\mathcal{S}_4}/\Bbbk(\bigwedge^2 A_3)^{\mathcal{S}_4}$ is rational by the foregoing, it follows that $\Bbbk(L_4)^{\mathcal{S}_4}$ is rational over $\Bbbk$. □

Without proof, we mention the following result, independently due to Schofield [188] and Katsylo [106], which reduces the investigation of the stable structure of $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}/\Bbbk$ to the case where n is a prime power; for a later different proof, see Saltman [183, Theorem 13].

Theorem 9.8.4 (Schofield, Katsylo)**.** *Suppose that* $n = ab$ *with* $\gcd(a, b) = 1$*. Then* $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ *is stably isomorphic over* $\Bbbk$ *to the field of fractions of* $\mathcal{K}(\mathrm{M}_a^r)^{\mathrm{PGL}_a} \otimes_{\Bbbk} \mathcal{K}(\mathrm{M}_b^r)^{\mathrm{PGL}_b}$*.*

This theorem allows to extend the stable rationality and retract rationality results in Theorem 9.8.3(a). Recall that, by Proposition 9.3.3(a), stable isomorphisms preserve retract rationality.

Corollary 9.8.5. (a) $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ *is stably rational over* $\Bbbk$ *for all divisors* n *of* $420 = 4 \cdot 3 \cdot 5 \cdot 7$.

(b) $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ *is retract rational over* $\Bbbk$ *if* n *is either squarefree or twice a squarefree number.*

10

Problems

We conclude our account by suggesting some problems for future research. The selection reflects the author's taste and inclinations and surely many further problems, perhaps even more pressing to some readers, could be added. The level of the problems discussed below ranges from the "famous unsolved" variety and some long-range projects to others that may very well be relatively quick and easy to dispose of. Some of the problems I have not actually tried my hands at myself, while others are presented along with a detailed discussion and solutions to some special cases.

Throughout this chapter, $\mathcal{G}$ denotes a finite group and L is a $\mathcal{G}$-lattice.

10.1 The Cohen-Macaulay Problem

It would be interesting to determine if the conclusion of Theorem 8.1.1 can be strengthened to the effect that all $\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)$ are in fact trivial, that is, the isotropy groups $\mathcal{G}_m$ for $m \in L$ are generated by bireflections on L. I do not know if, for the latter to occur, it is sufficient that just $\mathcal{G}$ is generated by bireflections. The corresponding fact for reflection groups is known to be true: if $\mathcal{G}$ is generated by reflections on L (or, equivalently, on the vector space $L_{\mathbb{Q}}$) then so are all isotropy groups $\mathcal{G}_m$; see Steinberg [203, Theorem 1.5] or Bourbaki [24, Exercise V.6.8(a)].

Problem 1. *If $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay are all isotropy groups $\mathcal{G}_m$ for $m \in L$ generated by bireflections on L?*

Problem 2. *Let $\mathcal{G} \subseteq \mathrm{GL}(V)$ be a finite linear group, where V is some finite-dimensional vector space. If $\mathcal{G}$ is generated by bireflections are all isotropy groups $\mathcal{G}_v$ for $v \in V$ generated by bireflections as well?*

Theorem 8.1.1 guarantees that Problem 1 has a positive answer for solvable groups $\mathcal{G}$. It might be worthwhile to look into Problem 2 more generally for k-reflections. There is essentially a complete classification of finite linear groups generated by bireflections. In arbitrary characteristic, this is due to Guralnick and Saxl [81]; for the case of characteristic zero, see Huffman and Wales [92]. However, other than for finite reflection groups $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ which can be investigated using root systems, no general theory appears to be in place for the unified study of bireflection groups. Therefore, it is not clear if one should expect $\mathbb{Z}[L]^{\mathcal{G}}$ to be Cohen-Macaulay for every finite bireflection group $\mathcal{G} \subseteq \mathrm{GL}(L)$, or even how to approach this problem. Nevertheless, we ask

Problem 3. *Is $\mathbb{Z}[L]^{\mathcal{G}}$ Cohen-Macaulay if and only if $\mathcal{G}$ is generated by bireflections on L?*

As we mentioned in Example 8.11.4, Pathak [148] has checked Problem 3 for lattices L of rank 3. In general, the "only if"-direction is of course part of Problem 1. By Theorem 8.1.1, this direction certainly holds for all groups $\mathcal{G}$ whose simple factors $\mathcal{G}/\mathcal{N}$ with $1 \neq \mathcal{N}$ are abelian. An affirmative answer to Problem 3 would imply that if $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay over $\mathbb{Z}$ then so is $\mathbb{Z}[L']^{\mathcal{G}}$ for any $\mathcal{G}$-sublattice $L' \subseteq L$. It does not seem obvious that this is indeed the case. The case of abelian groups is easy to settle:

Proposition 10.1.1. *Problem 3 has a positive answer when $\mathcal{G}$ is abelian.*

Proof. It suffices to show that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay for any finite abelian group $\mathcal{G}$ acting as a bireflection group on the lattice L. By passing to a rationally isomorphic lattice (Proposition 8.9.3), we may assume that $L = \bigoplus_{i=1}^{r} L_i$, where each L_i is a rationally irreducible $\mathcal{G}$-lattice. We may further assume that $\mathcal{G}$ acts faithfully and effectively on L; see Corollary 8.9.4. We claim that $\operatorname{rank} L_i \leq 2$ holds for all i. To see this, choose a bireflection $g \in \mathcal{G}$ such that $g_{L_i} \neq \mathrm{Id}_{L_i}$. Then $\operatorname{rank}[g, L_i] \leq 2$ and $\operatorname{rank}[g, L_i] = \operatorname{rank} L_i$, because $[g, L_i]$ is a nontrivial $\mathcal{G}$-sublattice of L_i.

First assume that $\operatorname{rank} L_i = 2$ for some i, say $i = 1$. Let $\mathcal{G}_1$ denote the subgroup of $\mathcal{G}$ that is generated by all bireflections $g \in \mathcal{G}$ such that $g_{L_1} \neq \mathrm{Id}_{L_1}$ and let $\mathcal{H}$ be the subgroup generated by the bireflections that act trivially on L_1. Then $\mathcal{G}_1 \subseteq \mathrm{Ker}_{\mathcal{G}}(M)$, where we have put $M = \bigoplus_{i \neq 1} L_i$. Thus, $\mathcal{G} = \mathcal{G}_1 \times \mathcal{H}$ and (3.5) gives $\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[L_1]^{\mathcal{G}_1} \otimes_{\mathbb{Z}} \mathbb{Z}[M]^{\mathcal{H}}$. By Corollary 8.9.2 we know that $\mathbb{Z}[L_1]^{\mathcal{G}_1}$ is Cohen-Macaulay and, arguing by induction on rank, we may assume that $\mathbb{Z}[M]^{\mathcal{H}}$ is Cohen-Macaulay as well. This easily implies that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay.

Thus, we may assume that all L_i have rank 1; so $\mathcal{G} \subseteq \mathrm{diag}(\pm 1, \ldots, \pm 1)_{r \times r}$. Suppose that there is a reflection $1 \neq g \in \mathcal{G}$, say $g_{L_1} \neq \mathrm{Id}_{L_1}$. Then $\mathcal{G} = \langle g \rangle \times \mathcal{H}$, where $\mathcal{H} = \mathrm{Ker}_{\mathcal{G}}(L_1)$, and as above, we conclude that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay. Therefore, we may assume that $\mathcal{G}$ is generated by certain bireflections $g_{i,j}$ $(i \neq j)$ acting as -1 on L_i and L_j and as 1 on all other summands. Defining $i \sim j$ if $i = j$ or $g_{i,j} \in \mathcal{G}$, we obtain an equivalence relation on $\{1, \ldots, r\}$. If there is more than one equivalence class then L and $\mathcal{G}$ decompose and, as above, we may conclude that $\mathbb{Z}[L]^{\mathcal{G}}$ is Cohen-Macaulay. On the other hand, if $g_{i,j} \in \mathcal{G}$ for all $i \neq j$ then $\mathcal{G} = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{r \times r} \cap \mathrm{SL}_r(\mathbb{Z})$ and the result follows from Example 3.5.3. □

The "if"-direction of Problem 3 looking like a long shot, it might be wise to try and establish the Cohen-Macaulay property for some special cases of bireflection actions first.

Problem 4. *Suppose $\mathcal{G}$ acts as a reflection group on L.*

(a) *Is* $\mathbb{Z}[L \oplus L]^{\mathcal{G}}$ *Cohen-Macaulay?*
(b) *Is* $\mathbb{Z}[L]^{\mathcal{H}}$ *Cohen-Macaulay for every subgroup* $\mathcal{H}$ *of* $\mathcal{G}$ *such that* $[\mathcal{G} : \mathcal{H}] = 2$*?*

Recall that the groups $\mathcal{H}$ in (b) do indeed act as bireflection groups on L, by Proposition 1.7.1. Example 8.11.1 is an explicit example for the situation considered in (b), while a solution to (a) would in particular resolve the Cohen-Macaulay problem for $\mathbb{Z}[U_n^2]^{\mathcal{S}_n}$ which was left open in Example 8.11.3.

10.2 Semigroup Algebras

Recall from Theorem 6.1.1 that $\mathbb{Z}[L]^{\mathcal{G}}$ is a semigroup algebra over $\mathbb{Z}$ if $\mathcal{G}$ acts as a reflection group on the lattice L. I do not know if the converse also holds. Thus:

Problem 5. *If* $\mathbb{Z}[L]^{\mathcal{G}}$ *is a semigroup algebra over* $\mathbb{Z}$*, must* $\mathcal{G}$ *act as a reflection group on the lattice* L*?*

A partial converse to Theorem 6.1.1 was given in Theorem 7.5.1. For a different partial converse as well as an alternative proof of Theorem 6.1.1, see Tesemma [215]. Tesemma's proof is heavily influenced by Reichstein's article [159]; it avoids the machinery of root systems and uses monomial orderings (see Section 3.4) and the geometry of polyhedral cones instead. The topological methods of Panyushev [146] (see also Popov and Vinberg [153, p. 242–243]) will likely be helpful in tackling Problem 5. The problem is related to Problem 3 inasmuch as affine normal semigroup algebras over any Cohen-Macaulay base ring are Cohen-Macaulay (Hochster [89, Theorem 1], or see Bruns and Herzog [32, Theorem 6.3.5(a)]). As with Problem 3, an affirmative answer to Problem 5 would imply that if $\mathbb{Z}[L]^{\mathcal{G}}$ is a semigroup algebra over $\mathbb{Z}$ then so is $\mathbb{Z}[L']^{\mathcal{G}}$ for any $\mathcal{G}$-sublattice $L' \subseteq L$. It does not seem clear that this is the case. In fact, if it were known to hold then, arguing as in the proof of Proposition 10.1.1 and using Lemma 10.2.2 below, it would be easy to show that Problem 5 had a positive answer at least for abelian $\mathcal{G}$. Other than with the Cohen-Macaulay problem, it is not even obvious that the question whether or not $\mathbb{Z}[L]^{\mathcal{G}}$ is a semigroup algebra over $\mathbb{Z}$ depends only on the rational type of the $\mathcal{G}$-lattice L. Note that if $\mathbb{Z}[L]^{\mathcal{G}}$ is a semigroup algebra over $\mathbb{Z}$, say $\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[M]$, then the monoid M will have to be an affine normal semigroup; see Section 3.4. Furthermore, the positive part $M/\operatorname{U}(M)$ of M has to be Φ-simplicial in the sense of Gubeladze [80]. Recall that any affine semigroup M embeds into a lattice $L = \langle M\rangle_{\text{group}} \cong \mathbb{Z}^r$. Hence we may view $M \hookrightarrow L_{\mathbb{R}} = \mathbb{R}^r$. Moreover, if M is positive then there is a monoid homomorphism $\varphi : M \to \mathbb{Z}_+$ satisfying $\varphi(m) > 0$ for all $0 \neq m \in M$ (cf. Swan [210, Theorem 4.5]) and we may extend φ to a linear form $\varphi\colon \mathbb{R}^r \to \mathbb{R}$. Following Gubeladze, we put

$$\Phi(M) = \mathbb{R}_+ M \cap \{x \in \mathbb{R}^r \mid \varphi(x) = 1\} ,$$

where $\mathbb{R}_+ M$ is the convex cone in $\mathbb{R}^r$ that is spanned by M. It is easy to see that $\Phi(M)$ is an $(r-1)$-dimensional convex polytope; it is the convex hull of the points $m_i/\varphi(m_i)$, where $\{m_i\}$ is the Hilbert basis of M; see Lemma 3.4.3. The monoid

M is called Φ-simplicial if $\Phi(M)$ is a simplex, that is, $\Phi(M)$ is the convex hull of r points. The following proposition follows from Gubeladze [80, Proposition 1.6].

Proposition 10.2.1. *Let $\Bbbk[M]$ be an affine normal semigroup algebra over the Krull domain $\Bbbk$. Then the class group $\mathrm{Cl}(\Bbbk[M])$ is torsion if and only if $\mathrm{Cl}(\Bbbk)$ is torsion and $M/\operatorname{U}(M)$ is Φ-simplicial.*

Since $\mathbb{Z}[L]^{\mathcal{G}}$ is an affine normal $\mathbb{Z}$-algebra with finite class group $\mathrm{Cl}(\mathbb{Z}[L]^{\mathcal{G}})$ (see Theorem 4.1.1), the monoid $M/\operatorname{U}(M)$ must be Φ-simplicial if $\mathbb{Z}[L]^{\mathcal{G}} = \mathbb{Z}[M]$.

We now present a technical lemma which allows to substantiate the claims, made on various occasions in earlier chapters, that certain multiplicative invariant algebras are not semigroup algebras. For $g \in \mathcal{G}$, put $L(g) = \{m \in L \mid \sum_{h \in \langle g \rangle} h(m) = 0\}$. Thus, $\widehat{H}^{-1}(\langle g \rangle, L) = L(g)/[g, L]$; see (2.2). Elements $g \in \mathcal{G}$ with $\operatorname{rank}[g, L] = \min_{g \in \mathcal{G} \setminus \operatorname{Ker}_{\mathcal{G}}(L)} \operatorname{rank}[g, L]$ will be called “minimal”.

Lemma 10.2.2. *Assume that*

(a) *no element of $\mathcal{G}$ acts as a nonidentity reflection on L, and*
(b) *for some minimal $g \in \mathcal{G}$, $L(g)$ is $\mathcal{G}$-stable and strictly larger than $[g, L]$.*

Then $\Bbbk[L]^{\mathcal{G}}$ is not a semigroup algebra over $\Bbbk$ for any domain $\Bbbk$ with $|\mathcal{G}| \neq 0$ in $\Bbbk$.

Proof. Suppose, for a contradiction, that (a) and (b) hold but $\Bbbk[L]^{\mathcal{G}}$ is a semigroup algebra over $\Bbbk$. Replacing $\mathcal{G}$ by $\mathcal{G}/\operatorname{Ker}_{\mathcal{G}}(L)$, we may assume that L is a faithful $\mathcal{G}$-lattice. Also, passing to the algebraic closure of the field of fractions of $\Bbbk$ (see Proposition 3.3.1(b)), we may assume that $\Bbbk$ is an algebraically closed field with $|\mathcal{G}|^{-1} \in \Bbbk$.

Put $X = \operatorname{Spec} \Bbbk[L]$, $Y = \operatorname{Spec} \Bbbk[L]^{\mathcal{G}} = X/\mathcal{G}$ and let $\pi \colon X \to Y = X/\mathcal{G}$ denote the quotient map. Furthermore, let Y_{sing} denote the singular locus of Y. In view of hypothesis (a), Corollary 7.3.2 says that

$$Z := \pi^{-1}(Y_{\text{sing}}) = \bigcup_{1 \neq g \in \mathcal{G}} X^g \,,$$

where X^g is the subvariety of g-fixed points in X, that is, $X^g = \mathcal{V}_X(I_{\Bbbk[L]}(g))$ with $I_{\Bbbk[L]}(g)$ as in (4.5). By Lemma 4.5.1, $\mathcal{O}(X^g) = \Bbbk[L]/I_{\Bbbk[L]}(g)$ is a Laurent polynomial algebra over the finite group algebra $\Bbbk[\widehat{H}^{-1}(\langle g \rangle, L)]$. Thus, each X^g is a disjoint union of algebraic tori (of dimension equal to $\operatorname{rank} L^{\langle g \rangle}$). The torus containing the augmentation map $\varepsilon \colon \Bbbk[L] \to \Bbbk$ is given by $\mathcal{V}_X(\mathfrak{E}_g \Bbbk[L])$, where $\mathfrak{E}_g$ denotes the kernel of the restriction of ε to $\Bbbk[L(g)]$. This torus will be denoted by $T(g)$.

Now consider the element $g \in \mathcal{G}$ that is provided by hypothesis (b). By minimality, we have $\dim X^g = \dim Z$ and so each irreducible component of X^g is an irreducible component of Z. Further, $\widehat{H}^{-1}(\langle g \rangle, L) \neq 0$ and so X^g has an irreducible component $T \neq T(g)$. Finally, since $L(g)$ is $\mathcal{G}$-stable, the above description of $T(g)$ shows that $T(g)$ is $\mathcal{G}$-stable as well. Therefore, by the separation property of π (see, e.g., Popov and Vinberg [153, Theorem 4.7]), $\pi(T)$ and $\pi(T(g))$ are disjoint irreducible components of Y_{sing}.

On the other hand, since $\Bbbk[L]^{\mathcal{G}}$ is a semigroup algebra, the variety Y is toric; see the proof of Theorem 7.5.1. The torus action on Y stabilizes each irreducible component of Y_{sing}. The unique closed orbit in Y (see [153, Cor. to Theorem 4.7]) is contained in each irreducible component of Y_{sing}, and hence in their intersection. This contradicts our construction of disjoint irreducible components for Y_{sing}. □

We remark that (a) is always satisfied if $\mathcal{G} \subseteq \mathrm{SL}(L)$, because nonidentity reflections have determinant -1. The sublattices $L(g)$ are certainly $\mathcal{G}$-stable when $\mathcal{G}$ is abelian. For an explicit example, let $\mathcal{G} = \mathrm{diag}(\pm 1, \ldots, \pm 1)_{n \times n} \cap \mathrm{SL}_n(\mathbb{Z})$ be the groups considered in Example 3.5.3. The bireflection $s = \mathrm{diag}(-1, 1, \ldots, 1, -1)$ is a minimal element of $\mathcal{G}$ with $L(s)/[s, L] \cong (\mathbb{Z}/2\mathbb{Z})^2$. Therefore, the lemma implies that the invariants $\Bbbk[L]^{\mathcal{G}}$ for any domain $\Bbbk$ of characteristic $\neq 2$ are not semigroup algebras over $\Bbbk$. The following corollary covers in particular the groups $\mathcal{G}_7$, $\mathcal{G}_8$, $\mathcal{G}_9$ and $\mathcal{G}_{10}$ in Table 3.1; these groups represent the conjugacy classes of finite nonidentity subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Corollary 10.2.3. *If $\mathcal{G}$ acts fixed-point-freely on $L/L^{\mathcal{G}}$ and $\operatorname{rank} L/L^{\mathcal{G}} \geq 2$ then $\Bbbk[L]^{\mathcal{G}}$ is not a semigroup algebra over $\Bbbk$ for any domain $\Bbbk$ with $|\mathcal{G}| \neq 0$ in $\Bbbk$.*

Proof. It is easy to see that if $\Bbbk[L]^{\mathcal{G}}$ is a semigroup algebra then so is $\Bbbk[\overline{L}]^{\mathcal{G}}$, where $\overline{L} = L/L^{\mathcal{G}}$. Thus, replacing L by $\overline{L}$, we may assume that $\mathcal{G}$ acts fixed-point-freely on L and $\operatorname{rank} L \geq 2$. Then $L(g) = L$ holds for every $1 \neq g \in \mathcal{G}$, and $L/[g, L]$ has order equal to $|\det(g_L - 1)|$. If g has order p, a prime, then p also divides $\det(g_L - 1)$. Thus, hypotheses (a) and (b) of the lemma are satisfied. □

In a different vein, we propose to investigate generalized multiplicative actions in the following sense.

Problem 6. *Study group actions on semigroup algebras $\Bbbk[M]$ such that the monoid M is mapped to itself.*

Actions of this kind arise in the study of ordinary multiplicative actions as follows. As in Section 1.9, let $\mathcal{R}$ denote the subgroup of $\mathcal{G}$ that is generated by the elements that act as reflections on the lattice L and recall that $\mathcal{G} = \mathcal{R} \rtimes \mathcal{G}_{\triangle}$; see Proposition 1.9.1. The group $\mathcal{G}/\mathcal{R} = \mathcal{G}_{\triangle}$ acts on the invariant algebra $R = \Bbbk[L]^{\mathcal{R}}$ and R is a semigroup algebra $\Bbbk[M]$, by Theorem 6.1.1. Using the explicit construction of the monoid M given in Proposition 6.2.1, it is easy to verify that $\mathcal{G}_{\triangle}$ does in fact stabilize M; so we are in the situation of Problem 6. Moreover, no element of $\mathcal{G}_{\triangle}$ acts as a nonidentity reflection on R in the sense of Section 4.5. (More generally, let $\mathcal{G}$ be a finite group acting by automorphisms on the commutative ring S and let $\mathcal{R}^k(\mathcal{G})$ denote the (normal) subgroup of $\mathcal{G}$ that is generated by all elements acting as k-reflections on S. Then no element of $\mathcal{G}/\mathcal{R}^k(\mathcal{G})$ acts as a nonidentity k-reflection on the invariant subring $S^{\mathcal{R}^k(\mathcal{G})}$.) Thus, the action of $\mathcal{G}_{\triangle}$ on $R = \Bbbk[L]^{\mathcal{R}}$ satisfies the analog of hypothesis (a) in Lemma 10.2.2.

10.3 Computational Issues

The algorithmic side of multiplicative invariant theory is relatively unexplored at present, especially in comparison with polynomial invariants where a highly developed computational theory is in place; see Derksen and Kemper [49]. The lack of an invariant grading renders most algorithms for polynomial invariants obsolete in the setting of multiplicative actions. Nevertheless, the method of computing multiplicative invariants of reflection groups described in Chapter 6 is quite efficient. Using ideas of Göbel [74] in addition to those presented in Chapter 6, Renault [162] has constructed an algorithm that computes the multiplicative invariant algebra $\Bbbk[L]^{\mathcal{G}}$ for any group $\mathcal{G}$ that is contained in a finite reflection subgroup of $\mathrm{GL}(L)$. Renault has implemented his algorithm in the computer algebra system MAGMA [20].

Invariants $f_1, \ldots, f_n \in \Bbbk[L]^{\mathcal{G}}$ are called *primary invariants* if the f_i are algebraically independent over $\Bbbk$ and $\Bbbk[L]^{\mathcal{G}}$ is finite over the polynomial subalgebra $P = \Bbbk[f_1, \ldots, f_n]$; the members of any finite collection of module generators of $\Bbbk[L]^{\mathcal{G}}$ over P are called *secondary invariants*.

Problem 7. *Develop algorithms for the computation of multiplicative invariants. As a start, device an efficient method of finding primary invariants.*

We remark that the number of primary invariants is necessarily equal to $n = \operatorname{rank} L$. Moreover, assuming $\Bbbk$ to be a PID, we know from Theorem 8.4.2 that $\Bbbk[L]$ is free over the polynomial algebra $P = \Bbbk[f_1, \ldots, f_n]$ of primary invariants, say $\Bbbk[L] \cong P^r$. If $\mathcal{G}$ acts faithfully then the order $|\mathcal{G}|$ divides r, by Galois theory. Moreover, if $g_1, \ldots, g_m \in \Bbbk[L]^{\mathcal{G}}$ is any collection of secondary invariants then we must have $m \geq |\mathcal{G}|/r$. It is possible to find a system of $|\mathcal{G}|/r$ secondary invariants precisely if $\Bbbk[L]^{\mathcal{G}}$ is Cohen-Macaulay; cf., e.g., the proof of Derksen and Kemper [49, Theorem 3.7.1]. This lends some computational interest to the Cohen-Macaulay problem.

There is a substantial number of computer algebra packages that are devoted to the investigation of polynomial invariants of (mostly) finite groups; for a list of packages and how to obtain them, see Derksen and Kemper [49, pp. 73–74]. No comparably complete package exists as yet for multiplicative invariants. Renault [162] has assembled a collection of functions, written for the computer algebra system MAGMA [20], which builds on an earlier and more primitive one by the author for GAP 3.4 [71]. [1]

Problem 8. *Create a library of functions for the automated investigation of multiplicative invariants.*

Once reasonably efficient computational tools are at hand, it might be worthwhile to tackle the project of an electronic database for multiplicative invariants. Recall from Corollary 3.3.2 that, working over a fixed base ring $\Bbbk$ (ideally $\Bbbk = \mathbb{Z}$), there are only finitely many multiplicative invariant algebras $\Bbbk[L]^{\mathcal{G}}$ up to isomorphism, for

[1] Available at `www.math.temple.edu/~lorenz/programs/multinv.g`. The package has not been maintained and is definitely in need of further work.

any given $\operatorname{rank} L$. For rank 2, the invariant algebras are listed in Table 3.1. In higher ranks, no such lists exist and the sheer number of the cases to consider, starting with rank 4, would make such lists rather unwieldy unless they are accessible in electronic form.

Problem 9. *Build a database for multiplicative invariants in low ranks.*

The benefits of such a database would include the easy testing of conjectures and, presumably, the creation of interesting new examples of invariant rings. An analogous database for polynomial invariants is already in existence (Kemper et al. [110]).

10.4 Essential Dimension Estimates

Let G be an affine algebraic group defined over an algebraically closed field $\Bbbk$ of characteristic 0. The essential dimension $\operatorname{ed}(G)$ of G, introduced for finite groups by Buhler and Reichstein [33] and in general by Reichstein [158], can be defined using the language of G-varieties; see §9.7.2. A G-variety X is called *generically free* if G acts freely (i.e., with trivial stabilizers) on a dense open subset of X. A *compression* of a generically free G-variety X is a dominant G-equivariant rational map $X \dashrightarrow Y$, where Y is another generically free G-variety. Now,

$$\operatorname{ed}(G) = \min_{Y} \dim Y/G \ , \tag{10.1}$$

where Y runs over all generically free G-varieties for which there exists a G-compression $V \dashrightarrow Y$ for some generically free *linear* G-variety V.

The definition of $\operatorname{ed}(G)$ can be rephrased in terms of the functor

$$H^1(\,.\,, G)\colon \ \mathsf{Fields}\,/\Bbbk \to \mathsf{Sets}$$

as follows; cf. Serre [195], Merkurjev [132], Berhuy and Favi [16]. Define the essential dimension $\operatorname{ed}(x)$ of an element $x \in H^1(K, G)$ as the infimum of all transcendence degrees $\operatorname{trdeg}_{\Bbbk} F$ for subextensions $F/\Bbbk \subseteq K/\Bbbk$ so that x belongs to the image of $H^1(F, G) \to H^1(K, G)$. Then $\operatorname{ed}(G)$ is the supremum of all $\operatorname{ed}(x)$ for varying K and x.

The value of $\operatorname{ed}(G)$ is an interesting invariant of G, albeit generally very difficult to determine. The essential dimension of $G = \mathrm{PGL}_n$, for example, is the minimum positive integer d such that every central division K-algebra D of degree n with $\Bbbk \subseteq K$ can be defined over a field K_0 with $\operatorname{trdeg}_{\Bbbk} K_0 \leq d$, that is, $D = D_0 \otimes_{K_0} K$ for some division K_0-algebra D_0. Only the following exact values of $\operatorname{ed}(\mathrm{PGL}_n)$ are known: $\operatorname{ed}(\mathrm{PGL}_n) = 2$ for $n = 2, 3$ or 6 (assuming $\Bbbk$ contains all n^{th} roots of unity) and $\operatorname{ed}(\mathrm{PGL}_4) = 5$, the latter being a recent result of Rost [173]. For a finite group $\mathcal{G}$, the value of $\operatorname{ed}(\mathcal{G})$ is a lower bound for (and conjecturally equal to) the minimum number of parameters in any generic polynomial for $\mathcal{G}$ over $\Bbbk$ (see §9.1.2) if such a polynomial exists; cf. Jensen et al. [98, Sect. 8.5].

The connection with the material in this book comes from the fact that upper bounds for the essential dimensions of certain algebraic groups can be obtained by using lattice techniques. The following proposition is implicit in Lorenz and Reichstein [126]. A more general version can be found in Lemire [116, Prop. 2.1]. Recall that the character lattice of an algebraic torus T is denoted by $X(T)$; so $X(T) = \mathrm{Hom}(T, \mathbb{G}_\mathrm{m})$.

Proposition 10.4.1. *Let H be an algebraic group of the form $H = T \rtimes \mathcal{G}$, where T is an algebraic torus and $\mathcal{G}$ a finite group. Given a map of $\mathcal{G}$-lattices*

$$f\colon L \to X(T)\ ,$$

put $X_f = \operatorname{Spec} \Bbbk[L]$. Then X_f is an irreducible H-variety with the following properties:

(a) *Functoriality: A commutative diagram of $\mathcal{G}$-lattices*

$$\begin{tikzcd} L \arrow[dr, "f"] & \\ & X(T) \\ L_0 \arrow[uu, "\mu"] \arrow[ur, "f_0"'] & \end{tikzcd} \tag{10.2}$$

leads to a morphism of H-varieties $X_\mu\colon X_f \to X_{f_0}$. The morphism X_μ is dominant if and only if μ is injective.

(b) $\dim X_f/H = \operatorname{rank} \operatorname{Ker} f$.

(c) *The H-variety X_f is generically free if and only if f is surjective and* $\operatorname{Ker} f$ *is a faithful $\mathcal{G}$-lattice.*

(d) *If L is a permutation $\mathcal{G}$-lattice then the H-variety X_f is birationally equivalent to a linear H-variety V_f.*

Corollary 10.4.2. *If there is a diagram of $\mathcal{G}$-lattices*

$$\begin{tikzcd} L \arrow[dr, "f"] & \\ & X(T) \\ L_0 \arrow[uu, hook] \arrow[ur, two heads, "f_0"'] & \end{tikzcd} \tag{10.3}$$

with L permutation and $\operatorname{Ker} f_0$ *faithful then* $\mathrm{ed}(H) \leq \operatorname{rank} \operatorname{Ker} f_0$.

The corollary follows from the compression $V_f \overset{\sim}{\dashrightarrow} X_f \to X_{f_0}$.

Proof of Proposition 10.4.1. Composing the evaluation map $T \to \mathrm{Hom}(X(T), \Bbbk^*)$ with the restriction map $f^*\colon \mathrm{Hom}(X(T), \Bbbk^*) \to \mathrm{Hom}(L, \Bbbk^*)$ along f one obtains a homomorphism $\varphi\colon T \to \mathrm{Hom}(L, \Bbbk^*) \hookrightarrow \mathrm{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L]) = \mathrm{Hom}(L, \Bbbk^*) \rtimes \mathrm{GL}(L)$; see (3.22). The corresponding action of T on $\Bbbk[L]$ is explicitly given by

$$t(\mathbf{x}^m) = f(m)(t)\mathbf{x}^m$$

for $t \in T$ and $m \in L$. The map φ is $\mathcal{G}$-equivariant. Thus, φ and the structure map $\mathcal{G} \to \mathrm{GL}(L)$ combine to given an action $H = T \rtimes \mathcal{G} \to \mathrm{Aut}_{\Bbbk\text{-alg}}(\Bbbk[L])$, thereby giving $X_f = \operatorname{Spec} \Bbbk[L]$ the structure of an H-variety.

For (a), note that the given diagram leads to an H-equivariant algebra map $\Bbbk[L_0] \to \Bbbk[L]$, and hence to a morphism of H-varieties $X_\mu \colon X_f \to X_{f_0}$.

Part (b) follows from the equalities $\dim X_f/H = \dim X_f/T = \operatorname{trdeg}_{\Bbbk} \Bbbk(L)^T$ and $\Bbbk(L)^T = \Bbbk(\operatorname{Ker} f)$; see Lemma 9.8.1.

To prove (c), we remark that X_f is generically free as H-variety if and only if X_f is generically free as T-variety and X_f/T is generically free for $\mathcal{G} = H/T$. The former is equivalent to surjectivity of f; c.f., e.g., Onishchik and Vinberg [144, Theorem 3.2.5]. Moreover, as we have seen above, $\mathcal{K}(X_f/T) = \Bbbk(L)^T = \Bbbk(\operatorname{Ker} f)$. Thus, $\operatorname{Ker} f$ is a faithful $\mathcal{G}$-lattice if and only if $\mathcal{G}$ acts faithfully on X_f/T or, equivalently, the $\mathcal{G}$-action on X_f/T is generically free (the two notions coincide for finite groups).

Finally, assume that L is a permutation lattice and fix a $\mathbb{Z}$-basis $m_1, \ldots, m_r$ that is permuted by $\mathcal{G}$. Then $\mathcal{K}(X_f) = \Bbbk(L) = \Bbbk(m_1, \ldots, m_r)$. Thus, putting $V_f = \sum_i \Bbbk m_i$ we obtain an H-invariant $\Bbbk$-subspace of $\mathcal{K}(X_f)$ with $\mathcal{K}(X_f) = \mathcal{K}(V_f)$. This shows that X_f is birationally linearizable. □

Example 10.4.3 (Essential dimension estimates for PGL_n)**.** As in the proof of Theorem 9.8.2, let T_{n-1} denote the maximal torus of PGL_n corresponding to the diagonal matrices. Recall that the normalizer $N(T_{n-1})$ of T_{n-1} in PGL_n is the semidirect product $T_{n-1} \rtimes \mathcal{S}_n$, with $\mathcal{S}_n$ acting on T_{n-1} by permuting the entries of diagonal matrices. We claim that

$$\operatorname{ed}(\mathrm{PGL}_n) \le \operatorname{ed}(N(T_{n-1})) \,. \tag{10.4}$$

This is a consequence of the $(\mathrm{PGL}_n, N(T_{n-1}))$-section $S = \mathrm{D}_n \oplus \mathrm{M}_n \subseteq X = \mathrm{M}_n^2$ that was constructed in the proof of Theorem 9.8.2. Recall that X and S are generically free linear varieties for PGL_n and $N(T_{n-1})$, respectively. The asserted inequality therefore follows from Reichstein [158, Definition 3.5 and Lemma 4.1].

Next, we use Corollary 10.4.2 above to show that

$$\operatorname{ed}(N(T_{n-1})) \le \; n^2 - 3n + 1 \quad \text{for } n \ge 4. \tag{10.5}$$

This result is due to Lemire [116]; combined with (10.4), it yields the best general estimate for $\operatorname{ed}(\mathrm{PGL}_n)$ known to date. To prove (10.5), let $U_n = \bigoplus_{i=1}^n \mathbb{Z}e_i$ denote the standard permutation lattice for $\mathcal{S}_n$ and A_{n-1} its root sublattice; see §1.3.3. Recall from (9.12) that $X(T_{n-1}) \cong A_{n-1}$ as $\mathcal{S}_n$-lattices. Further, recall from the proof of Theorem 9.8.2 that there is an exact sequence of $\mathcal{S}_n$-lattices

$$0 \to A_{n-1}^{\otimes 2} \longrightarrow P = \bigoplus_{r \neq s} \mathbb{Z}(e_r \otimes e_s) \xrightarrow{\;f\;} A_{n-1} \to 0$$

with $f(e_r \otimes e_s) = e_s - e_r$. Define $g \colon P \longrightarrow U_n$ by $g(e_r \otimes e_s) = e_s$ and put $L_0 = \operatorname{Ker} g$. We claim that $f(L_0) = A_{n-1}$ if $n \ge 3$. Indeed, if $\{r, s, t\}$ are all distinct then the element $e_r \otimes e_s - e_t \otimes e_s$ belongs to P_0 and maps to $e_t - e_r$ under f. Therefore, we obtain a commutative diagram of $\mathcal{S}_n$-lattices

$$\begin{tikzcd}
P \arrow[dr, "f"] & \\
& X(T_{n-1}) = A_{n-1} \\
L_0 \arrow[uu, hook] \arrow[ur, two heads, "f_0"'] &
\end{tikzcd} \tag{10.6}$$

with P a permutation lattice and $f_0 = f\big|_{L_0}$. Note that $\operatorname{rank}\operatorname{Ker} f_0 = \operatorname{rank} P - \operatorname{rank} U_n - \operatorname{rank} A_{n-1} = n^2 - 3n + 1$. Thus, the estimate (10.5) will follow form Corollary 10.4.2 if we can show that $\operatorname{Ker} f_0$ is a faithful $\mathcal{S}_n$-lattice for $n \geq 4$. For this, let $1 \neq s \in \mathcal{S}_n$, say $s(i) \neq i$. Choose $j \notin \{i, s(i)\}$ and choose two distinct elements $r, s \notin \{i, j\}$. Then the element $m = (e_s - e_r) \otimes (e_i - e_j) \in P$ satisfies $f(m) = 0$, $g(m) = 0$ and $s(m) \neq m$. Therefore, $\operatorname{Ker} f_0$ is faithful, as desired.

For odd values of n, one can improve upon (10.5):

$$\operatorname{ed}(N(T_{n-1})) \leq \binom{n-1}{2} \quad \text{for odd } n \geq 5. \tag{10.7}$$

This estimate, due to Lorenz and Reichstein [126], also follows from Corollary 10.4.2 by constructing a diagram of $\mathcal{S}_n$-lattices like (10.6), with the same permutation lattice P but a different L_0 so that $\operatorname{Ker} f_0 \cong \bigwedge^2 A_{n-1}$. For details, see [126, Proposition 4.4].

Problem 10. *Can the estimate* (10.7) *be further improved for large enough n? Is there analogous estimate for even values of n improving upon* (10.5)*? Is there a bound for* $\operatorname{ed}(\mathrm{PGL}_n)$ *that is linear in n?*

In a similar fashion, bounds for the essential dimensions of other semisimple algebraic groups G can be obtained from lattices for the Weyl group of G. In detail, let T be a maximal torus in G, $N = N_G(T)$ its normalizer in G, and $\mathcal{W} = N/T$ the Weyl group. If G is connected with trivial center then

$$\operatorname{ed}(G) \leq \operatorname{ed}(N)\ ; \tag{10.8}$$

see Reichstein [158, Proposition 4.3]. The proof involves a relative section due to Popov [152] which generalizes the one used in Example 10.4.3 above. Thus we may focus on constructing upper bounds for $\operatorname{ed}(N)$. (We remark, however, that the inequality (10.8) is often strict.) The problem with the approach used above is that the group extension $1 \to T \to N \to \mathcal{W} \to 1$ is usually not split, and so Proposition 10.4.1 and Corollary 10.4.2 do not apply as stated. However, using a construction of Saltman [180], Lemire [116] has generalized Corollary 10.4.2 to the non-split case. In this way, several interesting essential dimension bounds have been derived in [116] by finding suitable epimorphisms of $\mathcal{W}$-lattices

$$L \overset{f}{\twoheadrightarrow} X(T)\ , \tag{10.9}$$

where L is a permutation lattice of smallest possible rank such that $\operatorname{Ker} f$ is faithful. The issue of looking for further “compressions” L_0 as in (10.3) still needs to be more systematically addressed. Thus we propose, somewhat vaguely:

Problem 11. *Use lattice techniques to find good upper bounds for the essential dimension* $\operatorname{ed}(G)$ *of semisimple algebraic groups G.*

10.5 Rationality Problems

The basic problem is the multiplicative Noether problem:

Problem 12. *Find criteria for $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ to be rational (stably rational, retract rational).*

In this generality, the problem is presumably out of reach for now. It might be worthwhile to investigate more systematically the effect of replacing the lattice L by suitable related lattices. To a certain extent, this has been addressed in the no-name lemma (Proposition 9.4.4) and in Proposition 9.6.1, but more needs to be done. For instance, I do not know how sensitive rationality properties of $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ are to variation of L within its $\mathbb{Q}$-class. Note that Theorems 9.6.2 and 9.6.4 only depend on $L_{\mathbb{Q}}$.

We now turn to certain special cases of Problem 12 and related problems. First and foremost, there is the rationality problem for the field of matrix invariants:

Problem 13. *Is $\mathcal{K}(\mathrm{M}_n^r)^{\mathrm{PGL}_n}$ rational (stably rational, retract rational) over $\Bbbk$ for all n?*

This problem can be treated as a special case of Problem 12, as was explained in Section 9.8. The current state of knowledge has essentially been described there. Subsequent work of Beneish [10], [11], [13] further explores the approach to Problem 13 via multiplicative invariant theory. This has resulted in a number of reductions without, thus far, fully settling the problem for any additional values of n. The first open case is still $n = 8$. For a well-written survey on the generic division algebra $\mathrm{UD}(\Bbbk, n, r)$ and its connection with Problem 13, see Formanek [66]. Currently the main motivation for studying Problem 13, and potentially a new approach to its solution, comes from results of Schofield. In [189], it is proved that the moduli space of representations of a quiver Q with fixed dimension vector α is birationally isomorphic to $\mathrm{M}_n^r \,/\, \mathrm{PGL}_n$. (Here, n is the greatest common divisor of the components of α and r is determined from α/n and the Euler form of Q.) Article [190] gives a similar result for the moduli space of vector bundles on the projective plane $\mathbb{P}^2$ with given Hilbert polynomial. Once the rationality problem for these moduli spaces is settled, Problem 13 will also be resolved.

Turning to a problem of more modest scope, recall that the $\mathcal{S}_4$-invariant field of the signed root lattice $\mathbb{Z}^- \otimes_{\mathbb{Z}} A_3$ is the only multiplicative invariant field of transcendence degree at most 3 whose rationality was left undecided in Hajja and Kang [84] (group $W_{10}(198)$); all others were shown to be rational. Thus, in order to clean up the rationality problem for $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ with $\operatorname{rank} L \leq 3$, we ask:

Problem 14. *Is $\Bbbk(\mathbb{Z}^- \otimes_{\mathbb{Z}} A_3)^{\mathcal{S}_4}$ rational over $\Bbbk$?*

Here is another problem, for linear invariant fields, aiming to clarify a borderline situation left undecided by previous work.

Problem 15. *Let $\mathcal{G}$ be a group of order p^5 for some prime p and let $\mathcal{G} \to \mathrm{GL}(V)$ be a linear representation over a field $\Bbbk$ containing all e^{th} roots of unity, where e is the exponent of $\mathcal{G}$. Is $\mathsf{K}(V)^{\mathcal{G}}$ rational over $\Bbbk$?*

The corresponding problem for groups of order dividing p^4 has been affirmatively solved by Chu and Kang [38], improving on earlier work of Beneish [12] for p^3. The answer is negative in general for groups of order p^6; see Bogomolov [18]. Some cases of Problem 15 are consequences of the following general result due to Miyata [134] and Vinberg [216]. Recall that a flag in a finite-dimensional vector space V is a chain of subspaces $V_1 \subseteq \cdots \subseteq V_i \subseteq V_{i+1} \subseteq \cdots \subseteq V_n = V$ with $\dim V_i = i$.

Theorem 10.5.1 (Miyata, Vinberg). *Let $G \to \mathrm{GL}(V)$ be a linear representation of the (arbitrary) group G over $\Bbbk$. If G stabilizes some flag in V then $\mathsf{K}(V)^{\mathcal{G}}/\Bbbk$ is rational.*

A nice exposition of this theorem can be found in Kervaire and Vust [111]. It covers in particular an earlier result of Kuniyoshi [112] and Gaschütz [72], asserting rationality of $\mathsf{K}(V)^{\mathcal{G}}/\Bbbk$ for any finite p-group $\mathcal{G}$ if $\operatorname{char} \Bbbk = p$, and a classical result of Fischer [63] proving rationality of $\mathsf{K}(V)^{\mathcal{G}}/\Bbbk$ for finite abelian groups $\mathcal{G}$ provided the field $\Bbbk$ contains all e^{th} roots of unity, where e is the exponent of $\mathcal{G}$. Therefore, in Problem 15 one can assume that $\mathcal{G}$ is non-abelian and $\operatorname{char} \Bbbk \neq p$. For the classification of all groups of order p^5, see Szekeres [213] and Levy [119].

Recall from Section 9.4 that, in order to prove the existence of a generic polynomial for $\mathcal{G}$ over $\Bbbk$, it suffices to show that $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational for just one faithful $\mathcal{G}$-lattice L. To the best of my knowledge, the smallest group for which the existence of a generic polynomial over $\mathbb{Q}$ remains to be settled is the special linear group $\mathrm{SL}_2(\mathbb{F}_3)$ of order 24. Moreover, for $n > 5$ it is unknown whether the alternating group $\mathcal{A}_n$ has a generic polynomial (over any field); see Jensen et al. [98] Thus, the following problem seems worthwhile if admittedly again stated somewhat vaguely.

Problem 16. *For certain interesting groups $\mathcal{G}$ (such as $\mathrm{SL}_2(\mathbb{F}_3)$, $\mathcal{A}_6, \ldots$), find one particular faithful $\mathcal{G}$-lattice L such that $\Bbbk(L)^{\mathcal{G}}/\Bbbk$ is retract rational.*

References

1. E. Ascher and H. Grimmer, *Comment on a paper by Tahara on the finite subgroups of* $\mathrm{GL}(3, \mathbf{Z})$, Nagoya Math. J. **48** (1972), 203. MR 47 #3564
2. Peter Bardsley and Roger W. Richardson, *Étale slices for algebraic transformation groups in characteristic* p, Proc. London Math. Soc. (3) **51** (1985), no. 2, 295–317. MR 86m:14034
3. Jean Barge, *Cohomologie des groupes et corps d'invariants multiplicatifs*, Math. Ann. **283** (1989), no. 3, 519–528. MR 90c:12006
4. Jean Barge, *Cohomologie des groupes et corps d'invariants multiplicatifs tordus*, Comment. Math. Helv. **72** (1997), no. 1, 1–15. MR 98g:12006
5. Hyman Bass, *Algebraic K-theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 40 #2736
6. Hyman Bass and M. Pavaman Murthy, *Grothendieck groups and Picard groups of abelian group rings*, Ann. of Math. (2) **86** (1967), 16–73. MR 36 #2671
7. Esther Beneish, *Failure of Krull-Schmidt for invertible lattices*, preprint.
8. Esther Beneish, *Induction theorems on the stable rationality of the center of the ring of generic matrices*, Trans. Amer. Math. Soc. **350** (1998), no. 9, 3571–3585. MR 98k:16034
9. Esther Beneish, *Noether settings for central extensions of groups with zero Schur multiplier*, J. Algebra Appl. **1** (2002), no. 1, 107–112. MR 2003c:12007
10. Esther Beneish, *The center of the generic division ring and twisted multiplicative group actions*, J. Algebra **259** (2003), no. 2, 313–322. MR 2003i:16027
11. Esther Beneish, *Monomial actions of the symmetric group*, J. Algebra **265** (2003), no. 2, 405–419. MR 2004b:20008
12. Esther Beneish, *Stable rationality of certain invariant fields*, J. Algebra **269** (2003), no. 2, 373–380. MR 2 015 282
13. Esther Beneish, *Lattice invariants and the center of the generic division ring*, Trans. Amer. Math. Soc. **356** (2004), no. 4, 1609–1622 (electronic). MR 2004h:20007
14. David J. Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series, vol. 190, Cambridge University Press, Cambridge, 1993. MR 94j:13003
15. George M. Bergman, *The logarithmic limit-set of an algebraic variety*, Trans. Amer. Math. Soc. **157** (1971), 459–469. MR 43 #6209
16. Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic). MR 2004m:11056

17. Christine Bessenrodt and Lieven Le Bruyn, *Stable rationality of certain* PGL_n*-quotients*, Invent. Math. **104** (1991), no. 1, 179–199. MR 92m:14060
18. F. A. Bogomolov, *The Brauer group of quotient spaces of linear representations*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 3, 485–516, 688. MR 88m:16006
19. Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 92d:20001
20. Wieb Bosma, John J. Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265, software available at `http://magma.maths.usyd.edu.au/magma/`.
21. Nicolas Bourbaki, *Algèbre commutative. Chapitre 3: Graduations, filtrations et topologies. Chapitre 4: Idéaux premiers associés et décomposition primaire*, Actualités Scientifiques et Industrielles, No. 1293, Hermann, Paris, 1961. MR 30 #2027
22. Nicolas Bourbaki, *Algèbre commutative. Chapitre 5: Entiers. Chapitre 6: Valuations*, Actualités Scientifiques et Industrielles, No. 1308, Hermann, Paris, 1964. MR 33 #2660
23. Nicolas Bourbaki, *Algèbre commutative. Chapitre 7: Diviseurs*, Actualités Scientifiques et Industrielles, No. 1314, Hermann, Paris, 1965. MR 41 #5339
24. Nicolas Bourbaki, *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. MR 39 #1590
25. Nicolas Bourbaki, *Algèbre, Chapitres 1 à 3*, Hermann, Paris, 1970. MR 43 #2
26. Nicolas Bourbaki, *Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*, Actualités Scientifiques et Industrielles, No. 1364, Hermann, Paris, 1975.
27. Nicolas Bourbaki, *Algèbre, chapitres 4 à 7*, Masson, Paris, 1981. MR 84d:00002
28. Nicolas Bourbaki, *Algèbre commutative. Chapitre 8: Dimension. Chapitre 9: Anneaux locaux noethériens complets*, Masson, Paris, 1983.
29. Markus P. Brodmann and Rodney Y. Sharp, *Local cohomology: an algebraic introduction with geometric applications*, Cambridge Studies in Advanced Mathematics, vol. 60, Cambridge University Press, Cambridge, 1998. MR 99h:13020
30. Harold Brown, Rolf Bülow, Joachim Neubüser, Hans Wondratschek, and Hans Zassenhaus, *Crystallographic groups of four-dimensional space*, Wiley-Interscience [John Wiley & Sons], New York, 1978, Wiley Monographs in Crystallography. MR 58 #4109
31. Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1982. MR 83k:20002
32. Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay rings*, revised ed., Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1998. MR 95h:13020
33. J. Buhler and Zinovy Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179. MR 98e:12004
34. *CARAT: Crystallographic AlgoRithms And Tables*, software and further information available at `http://wwwb.math.rwth-aachen.de/carat/`.
35. Henri Cartan and Samuel Eilenberg, *Homological algebra*, Princeton Mathematical Series, vol. 19, Princeton University Press, Princeton, N. J., 1956. MR 17,1040e
36. S. U. Chase, D. K. Harrison, and Alex Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. **52** (1965), 15–33. MR 33 #4118
37. Claude Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782. MR 17,345d
38. Huah Chu and Ming-chang Kang, *Rationality of p-group actions*, J. Algebra **237** (2001), no. 2, 673–690. MR 2001k:13008

39. C. L. Chuang and Pjek Hwee Lee, *Noetherian rings with involution*, Chinese J. Math. **5** (1977), no. 1, 15–19. MR 56 #12053
40. Jean-Louis Colliot-Thélène and Manuel Ojanguren, *Variétés unirationnelles non rationnelles: au-delà de l'exemple d'Artin et Mumford*, Invent. Math. **97** (1989), no. 1, 141–158. MR 90m:14012
41. Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 175–229. MR 56 #8576
42. Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *Principal homogeneous spaces under flasque tori: applications*, J. Algebra **106** (1987), no. 1, 148–205. MR 88j:14059
43. Anne Cortella and Boris Kunyavskiĭ, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000), no. 2, 771–793. MR 2001c:14070
44. Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR 82i:20001
45. Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 88f:20002
46. Everett C. Dade, *The maximal finite groups of* 4×4 *integral matrices*, Illinois J. Math. **9** (1965), 99–122. MR 30 #1192
47. V. I. Danilov, *The geometry of toric varieties*, Uspekhi Mat. Nauk **33** (1978), no. 2(200), 85–134, 247 (Russian), English translation: Russian Math. Surveys **33** (1978), 97–154. MR 80g:14001
48. Frank DeMeyer and Thomas McKenzie, *On generic polynomials*, J. Algebra **261** (2003), no. 2, 327–333. MR 2003m:12007
49. Harm Derksen and Gregor Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, Encyclopaedia of Mathematical Sciences, 130. MR 2003g:13004
50. Warren Dicks and M. J. Dunwoody, *Groups acting on graphs*, Cambridge Studies in Advanced Mathematics, vol. 17, Cambridge University Press, Cambridge, 1989. MR 91b:20001
51. Igor V. Dolgachev, *Rationality of fields of invariants*, Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., vol. 46, Amer. Math. Soc., Providence, RI, 1987, pp. 3–16. MR 89b:14064
52. Stephen Donkin, *Invariants of several matrices*, Invent. Math. **110** (1992), no. 2, 389–401. MR 93j:20090
53. Andreas W. M. Dress, *The permutation class group of a finite group*, J. Pure Appl. Algebra **6** (1975), 1–12. MR 50 #13220
54. David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 97a:13001
55. Geir Ellingsrud and Tor Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compositio Math. **41** (1980), no. 2, 233–244. MR 82c:13015
56. Shizuo Endô and Takehiko Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973), 7–26. MR 47 #316
57. Shizuo Endô and Takehiko Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975), 85–104. MR 51 #458
58. Shizuo Endô and Takehiko Miyata, *On the projective class group of finite groups*, Osaka J. Math. **13** (1976), no. 1, 109–122. MR 53 #13315
59. Daniel R. Farkas, *Multiplicative invariants*, Enseign. Math. (2) **30** (1984), no. 1-2, 141–157. MR 85h:16042

60. Daniel R. Farkas, *Toward multiplicative invariant theory*, Group actions on rings (Brunswick, Maine, 1984), Contemp. Math., vol. 43, Amer. Math. Soc., Providence, RI, 1985, pp. 69–80. MR 87b:16013
61. Daniel R. Farkas, *Reflection groups and multiplicative invariants*, Rocky Mountain J. Math. **16** (1986), no. 2, 215–222. MR 87k:20085
62. Walter Feit, *Orders of finite linear groups*, preprint.
63. Ernst Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen*, Gött. Nachr. (1915), 77–80.
64. Edward Formanek, *The center of the ring of* 3×3 *generic matrices*, Linear and Multilinear Algebra **7** (1979), no. 3, 203–212. MR 80h:16019
65. Edward Formanek, *The center of the ring of* 4×4 *generic matrices*, J. Algebra **62** (1980), no. 2, 304–319. MR 81g:15032
66. Edward Formanek, *The ring of generic matrices*, J. Algebra **258** (2002), no. 1, 310–320, Special issue in celebration of Claudio Procesi's 60th birthday. MR 2004a:16039
67. Robert M. Fossum, *The divisor class group of a Krull domain*, Springer-Verlag, New York, 1973, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74. MR 52 #3139
68. Shmuel Friedland, *The maximal orders of finite subgroups in* $\mathrm{GL}_n(\mathbf{Q})$, Proc. Amer. Math. Soc. **125** (1997), no. 12, 3519–3526. MR 98b:20064
69. William Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, vol. 131, Princeton University Press, Princeton, NJ, 1993, The William H. Roever Lectures in Geometry. MR 94g:14028
70. William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics. MR 93a:20069
71. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002, software and further information available at `http://www.gap-system.org`.
72. Wolfgang Gaschütz, *Fixkörper von p-Automorphismengruppen rein-transzendener Körpererweiterungen von p-Charakteristik*, Math. Z. **71** (1959), 466–468. MR 22 #12104
73. Robert Gilmer, *Commutative semigroup rings*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1984. MR 85e:20058
74. Manfred Göbel, *Computing bases for rings of permutation-invariant polynomials*, J. Symbolic Comput. **19** (1995), no. 4, 285–291. MR 96f:13006
75. Nikolai Gordeev, *Coranks of elements of linear groups and the complexity of algebras of invariants*, Algebra i Analiz **2** (1990), no. 2, 39–64 (Russian), English translation: Leningrad Math. J. **2** (1991), 245–267.
76. Nikolai Gordeev and Gregor Kemper, *On the branch locus of quotients by finite groups and the depth of the algebra of invariants*, J. Algebra **268** (2003), no. 1, 22–38. MR 2004h:13010
77. Alexandre Grothendieck, *Sur quelques points d'algèbre homologique*, Tôhoku Math. J. (2) **9** (1957), 119–221. MR 21 #1328
78. Alexandre Grothendieck et. al., *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris), 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61, directed by A. Grothendieck, with two papers by M. Raynaud, updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin]. MR 2004g:14017
79. Joseph Gubeladze, *The Anderson conjecture and a maximal class of monoids over which projective modules are free*, Mat. Sb. (N.S.) **135(177)** (1988), no. 2, 169–185, 271 (Russian), translation in Math. USSR-Sb. **63** (1989), no. 1, 165–180. MR 89d:13010

80. Joseph Gubeladze, *The elementary action on unimodular rows over a monoid ring*, J. Algebra **148** (1992), no. 1, 135–161. MR 93e:19001
81. Robert M. Guralnick and Jan Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), no. 2, 519–571. MR 2009321
82. Mowaffaq Hajja, *A minimal example of a nonrational monomial automorphism*, Comm. Algebra **18** (1990), no. 8, 2423–2431. MR 91i:12005
83. Mowaffaq Hajja and Ming Chang Kang, *Finite group actions on rational function fields*, J. Algebra **149** (1992), no. 1, 139–154. MR 93d:12009
84. Mowaffaq Hajja and Ming-chang Kang, *Three-dimensional purely monomial group actions*, J. Algebra **170** (1994), no. 3, 805–860. MR 95k:12008
85. Mowaffaq Hajja and Ming-chang Kang, *Some actions of symmetric groups*, J. Algebra **177** (1995), no. 2, 511–535. MR 96i:20013
86. Mowaffaq Hajja and Ming-chang Kang, *Twisted actions of symmetric groups*, J. Algebra **188** (1997), no. 2, 626–647. MR 98b:13003
87. P. J. Hilton and U. Stammbach, *A course in homological algebra*, second ed., Graduate Texts in Mathematics, vol. 4, Springer-Verlag, New York, 1997. MR 97k:18001
88. Peter Hindman, Lee Klingler, and Charles J. Odenthal, *On the Krull-Schmidt-Azumaya theorem for integral group rings*, Comm. Algebra **26** (1998), no. 11, 3743–3758. MR 99i:16012
89. Melvin Hochster, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*, Ann. of Math. (2) **96** (1972), 318–337. MR 46 #3511
90. Melvin Hochster and John A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020–1058. MR 46 #1787
91. W. Cary Huffman, *Linear groups containing an element with an eigenspace of codimension two*, J. Algebra **34** (1975), 260–287. MR 53 #5762
92. W. Cary Huffman and David B. Wales, *Linear groups containing an element with an eigenspace of codimension two*, Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975), Academic Press, New York, 1976, pp. 425–429. MR 55 #8199
93. James E. Humphreys, *Introduction to Lie algebras and representation theory*, Springer-Verlag, New York, 1972, Graduate Texts in Mathematics, Vol. 9. MR 48 #2197
94. James E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, vol. 29, Cambridge University Press, Cambridge, 1990. MR 92h:20002
95. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 92e:11001
96. I. Martin Isaacs, *Character theory of finite groups*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976, Pure and Applied Mathematics, No. 69. MR 57 #417
97. H. Jacobinski, *Unique decomposition of lattices over orders*, Proceedings of the International Conference on Representations of Algebras (Carleton Univ., Ottawa, Ont., 1974), Paper No. 15, Carleton Univ., Ottawa, 1974, pp. 9 pp. Carleton Math. Lecture Notes, No. 9. MR 51 #589
98. Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem. MR 2004d:12007
99. Alfredo Jones, *Indecomposable integral representations*, Ph.D. thesis, University of Illinois, Urbana, 1962.

100. Alfredo Jones, *Groups with a finite number of indecomposable integral representations*, Michigan Math. J. **10** (1963), 257–261. MR 27 #3698

101. Camille Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, J. Reine Angew. Math. **84** (1878), 89–215.

102. Camille Jordan, *Mémoire sur l'équivalence des formes*, J. Ecole Polytech. **48** (1880), 112–150.

103. Victor G. Kac, *Infinite-dimensional Lie algebras*, third ed., Cambridge University Press, Cambridge, 1990. MR 92k:17038

104. Ming-chang Kang, *Picard groups of some rings of invariants*, J. Algebra **58** (1979), no. 2, 455–461. MR 82m:14004

105. Pavel I. Katsylo, *Rationality of orbit spaces of irreducible representations of the group* SL_2, Izv. Akad. Nauk SSSR Ser. Mat. **47** (1983), no. 1, 26–36. MR 85g:14057

106. Pavel I. Katsylo, *Stable rationality of fields of invariants of linear representations of the groups* PSL_6 *and* PSL_{12}, Mat. Zametki **48** (1990), no. 2, 49–52, 159 (Russian), English translation: Math. Notes **48** (1991), 751–753.

107. Yonatan R. Katznelson, *On the orders of finite subgroups of* $\mathrm{GL}(n, \mathbb{Z})$, Exposition. Math. **12** (1994), 453–457.

108. Gregor Kemper, *Die Cohen-Macaulay Eigenschaft in der modularen Invariantentheorie*, Habilitationsschrift, Universität Heidelberg, 1999.

109. Gregor Kemper, *The depth of invariant rings and cohomology*, J. Algebra **245** (2001), no. 2, 463–531, With an appendix by Kay Magaard. MR 2002h:13009

110. Gregor Kemper, Elmar Körding, Gunter Malle, B. Heinrich Matzat, Denis Vogel, and Gabor Wiese, *A database of invariant rings*, Experiment. Math. **10** (2001), no. 4, 537–542. MR 2002k:13011

111. Michel Kervaire and Thierry Vust, *Fractions rationnelles invariantes par un groupe fini: quelques exemples*, Algebraische Transformationsgruppen und Invariantentheorie, DMV Sem., vol. 13, Birkhäuser, Basel, 1989, pp. 157–179. MR 1 044 591

112. Hideo Kuniyoshi, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 65–67. MR 16,993d

113. T. Y. Lam, *Serre's conjecture*, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 635. MR 58 #5644

114. Lieven Le Bruyn, *Centers of generic division algebras, the rationality problem 1965–1990*, Israel J. Math. **76** (1991), no. 1-2, 97–111. MR 93f:16024

115. Nicole Lemire, *Reduction in the rationality problem for multiplicative invariant fields*, J. Algebra **238** (2001), no. 1, 51–81. MR 2002b:13009

116. Nicole Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transformation Groups **9** (2004), no. 4, 337–379.

117. Nicole Lemire and Martin Lorenz, *On certain lattices associated with generic division algebras*, J. Group Theory **3** (2000), no. 4, 385–405. MR 2001h:16018

118. Hendrik W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325. MR 50 #289

119. Lawrence S. Levy, *Modules over Dedekind-like rings*, J. Algebra **93** (1985), no. 1, 1–116. MR 87k:20017a

120. Martin Lorenz, *On the Cohen-Macaulay property of multiplicative invariants*, to appear in Trans. Amer. Math. Soc.; arXiv: math.AC/0312302.

121. Martin Lorenz, *Class groups of multiplicative invariants*, J. Algebra **177** (1995), no. 1, 242–254. MR 96j:16036

122. Martin Lorenz, *Regularity of multiplicative invariants*, Comm. Algebra **24** (1996), no. 3, 1051–1055. MR 96m:13007

123. Martin Lorenz, *Picard groups of multiplicative invariants*, Comment. Math. Helv. **72** (1997), no. 3, 389–399. MR 98m:13019

124. Martin Lorenz, *Multiplicative invariants and semigroup algebras*, Algebr. Represent. Theory **4** (2001), no. 3, 293–304. MR 2002i:13003

125. Martin Lorenz and Jawahar Pathak, *On Cohen-Macaulay rings of invariants*, J. Algebra **245** (2001), no. 1, 247–264. MR 2002h:13010

126. Martin Lorenz and Zinovy Reichstein, *Lattices and parameter reduction in division algebras*, arXiv-preprint math.RA/0001026, 2000.

127. Martin Lorenz, Zinovy Reichstein, Louis Rowen, and David Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670. MR 2 009 442

128. Domingo Luna, *Slices étales*, Sur les groupes algébriques, Soc. Math. France, Paris, 1973, pp. 81–105. Bull. Soc. Math. France, Paris, Mémoire 33. MR 49 #7269

129. Saunders Mac Lane, *Homology*, 3rd corrected printing ed., Grundlehren der mathematischen Wissenschaften, vol. 114, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

130. Katsuhiko Masuda, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 59–63. MR 16,993c

131. Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR 82i:13003

132. Alexander Merkurjev, *Essential dimension*, unpublished notes, University of California - Los Angeles, 1999.

133. Hermann Minkowski, *Zur Theorie der positiven quadratische Formen*, J. reine angew. Math. **101** (1887), 196–202.

134. Takehiko Miyata, *Invariants of certain groups. I*, Nagoya Math. J. **41** (1971), 69–73. MR 42 #7804

135. Susan Montgomery, *Fixed rings of finite automorphism groups of associative rings*, Lecture Notes in Mathematics, vol. 818, Springer, Berlin, 1980. MR 81j:16041

136. Haruhisa Nakajima, *Invariants of finite abelian groups generated by transvections*, Tokyo J. Math. **3** (1980), no. 2, 201–214. MR 82e:14058

137. Gabriele Nebe, *Finite subgroups of* $\mathrm{GL}_{24}(\mathbf{Q})$, Experiment. Math. **5** (1996), no. 3, 163–195. MR 98b:20080

138. Gabriele Nebe, *Finite subgroups of* $\mathrm{GL}_n(\mathbf{Q})$ *for* $25 \leq n \leq 31$, Comm. Algebra **24** (1996), no. 7, 2341–2397. MR 97e:20066

139. Gabriele Nebe and Wilhelm Plesken, *Finite rational matrix groups*, Mem. Amer. Math. Soc. **116** (1995), no. 556, viii+144. MR 95k:20081

140. Morris Newman, *Integral matrices*, Academic Press, New York, 1972, Pure and Applied Mathematics, Vol. 45. MR 49 #5038

141. Emmy Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1918), 221–229.

142. Tadao Oda, *Convex bodies and algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 15, Springer-Verlag, Berlin, 1988, An introduction to the theory of toric varieties, Translated from the Japanese. MR 88m:14038

143. Robert Oliver, *G-actions on disks and permutation representations*, J. Algebra **50** (1978), no. 1, 44–62. MR 58 #18508

144. A. L. Onishchik and È. B. Vinberg, *Lie groups and algebraic groups*, Springer Series in Soviet Mathematics, Springer-Verlag, Berlin, 1990, Translated from the Russian and with a preface by D. A. Leites. MR 91g:22001

145. J. Opgenorth, W. Plesken, and T. Schulz, *Crystallographic algorithms and tables*, Acta Cryst. Sect. A **54** (1998), no. 5, 517–531. MR 99h:20082

146. Dmitri I. Panyushev, *Orbit spaces of finite and connected linear groups*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 1, 95–99, 191 (Russian), English translation: Math. USSR Izv. **20** (1983), 97–101. MR 83i:14039

147. Donald S. Passman, *Infinite group rings*, Marcel Dekker Inc., New York, 1971, Pure and Applied Mathematics, 6. MR 47 #3500

148. Jawahar Pathak, *The Cohen-Macaulay property of multiplicative invariants*, Ph.D. thesis, Temple University, 2003.

149. Wilhelm Plesken, *Some applications of representation theory*, Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991), Progr. Math., vol. 95, Birkhäuser, Basel, 1991, pp. 477–496. MR 92k:20019

150. Wilhelm Plesken and Tilman Schulz, *Counting crystallographic groups in low dimensions*, Experiment. Math. **9** (2000), no. 3, 407–411. MR 1795312

151. Vladimir L. Popov, *Divisor class groups of the semigroups of the highest weights*, J. Algebra **168** (1994), no. 3, 773–779. MR 95h:20056

152. Vladimir L. Popov, *Sections in invariant theory*, The Sophus Lie Memorial Conference (Oslo, 1992), Scand. Univ. Press, Oslo, 1994, pp. 315–361. MR 98d:14058

153. Vladimir L. Popov and Ernest B. Vinberg, *Invariant theory*, Algebraic Geometry IV (A. N. Parshin and I. R. Shafarevich, eds.), Encyclopaedia of Mathematical Sciences, vol. 55, Springer-Verlag, Berlin-Heidelberg, 1994.

154. Claudio Procesi, *Non-commutative affine rings*, Atti Accad. Naz. Lincei, VIII. Ser., v. VIII **6** (1967), 239–255.

155. Claudio Procesi, *The invariant theory of $n \times n$ matrices*, Advances in Math. **19** (1976), no. 3, 306–381. MR 54 #7512

156. Michel Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics, Vol. 169, Springer-Verlag, Berlin, 1970. MR 43 #3252

157. D. Rees, *A theorem of homological algebra*, Proc. Cambridge Philos. Soc. **52** (1956), 605–610. MR 18,277g

158. Zinovy Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304. MR 2001j:20073

159. Zinovy Reichstein, *SAGBI bases in rings of multiplicative invariants*, Comment. Math. Helv. **78** (2003), no. 1, 185–202. MR 2004c:13005

160. Zinovy Reichstein, *A note on retracts and lattices*, unpublished note, 2004.

161. Irving Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003, corrected reprint of the 1975 original, with a foreword by M. J. Taylor. MR 2004c:16026

162. Marc Renault, *Computing generators for rings of multiplicative invariants*, Ph.D. thesis, Temple University, 2002, available at `www.ship.edu/~msrena/`.

163. Philippe Revoy, *Anneau des invariants du groupe alterné*, Bull. Sci. Math. (2) **106** (1982), no. 4, 427–431. MR 84m:13007

164. Philippe Revoy, *Invariants de deux matrices carrées d'ordre 3*, C. R. Acad. Sci. Paris Sér. I Math. **323** (1996), no. 1, 1–6. MR 97e:15028

165. Roger W. Richardson, *The conjugating representation of a semisimple group*, Invent. Math. **54** (1979), no. 3, 229–245. MR 81a:14023

166. Roger W. Richardson, *Orbits, invariants, and representations associated to involutions of reductive groups*, Invent. Math. **66** (1982), no. 2, 287–312. MR 83i:14042

167. Lorenzo Robbiano and Moss Sweedler, *Subalgebra bases*, Commutative algebra (Salvador, 1988), Lecture Notes in Math., vol. 1430, Springer, Berlin, 1990, pp. 61–87. MR 91f:13027

168. Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 96f:20001

169. A. V. Roĭter, *Integer-valued representations belonging to one genus*, Izv. Akad. Nauk SSSR Ser. Mat. **30** (1966), 1315–1324 (Russian), English translation: Amer. Math. Soc. Transl. (2) **71** (1968), 49 – 59.

170. James E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc. (3) **36** (1978), no. 3, 385–447, Corrigenda: Proc. London Math. Soc. (3) **38** (1979), no. 3, 216–218. MR 58 #10996a

171. Maxwell Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443. MR 18,514a

172. Maxwell Rosenlicht, *A remark on quotient spaces*, An. Acad. Brasil. Ci. **35** (1963), 487–489. MR 30 #2009

173. Markus Rost, *Computation of some essential dimensions*, preprint, 2000, available at `http://www.mathematik.uni-bielefeld.de/~rost/ed.html`.

174. S. S. Ryškov and Z. D. Lomakina, *A proof of the theorem on maximal finite groups of integral* 5×5 *matrices*, Trudy Mat. Inst. Steklov. **152** (1980), 204–215, 238, Geometry of positive quadratic forms. MR 82e:20058

175. David J. Saltman, *Generic structures and field theory*, Algebraists' Hommage: Papers in Ring Theory and Related Topics (S. A. Amitsur et. al., ed.), Contemp. Math., vol. 13, Amer. Math. Soc., Providence, RI, 1982, pp. 127–134.

176. David J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), no. 1, 71–84. MR 85m:13006

177. David J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), no. 2-3, 165–215. MR 85j:13008

178. David J. Saltman, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985), no. 1, 53–67. MR 87a:13005

179. David J. Saltman, *Multiplicative field invariants*, J. Algebra **106** (1987), no. 1, 221–238. MR 88f:12007

180. David J. Saltman, *Invariant fields of linear groups and division algebras*, Perspectives in ring theory (Antwerp, 1987) (F. van Oystaeyen and L. le Bruyn, eds.), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 233, Kluwer Acad. Publ., Dordrecht, 1988, pp. 279–297. MR 91f:20053

181. David J. Saltman, *Multiplicative field invariants and the Brauer group*, J. Algebra **133** (1990), no. 2, 533–544. MR 91h:12016

182. David J. Saltman, *Twisted multiplicative field invariants, Noether's problem, and Galois extensions*, J. Algebra **131** (1990), no. 2, 535–558. MR 91f:12005

183. David J. Saltman, *A note on generic division algebras*, Abelian groups and noncommutative rings, Contemp. Math., vol. 130, Amer. Math. Soc., Providence, RI, 1992, pp. 385–394. MR 93i:12002

184. David J. Saltman, H^3 *and generic matrices*, J. Algebra **195** (1997), no. 2, 387–422. MR 99b:12003

185. David J. Saltman, *Ramification and lattices*, J. Algebra **195** (1997), no. 2, 423–464. MR 99b:12004

186. David J. Saltman, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, vol. 94, Published by American Mathematical Society, Providence, RI, 1999. MR 2000f:16023

187. Pierre 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. MR 35 #5428

188. Aidan Schofield, *Matrix invariants of composite size*, J. Algebra **147** (1992), no. 2, 345–349. MR 93e:16038

189. Aidan Schofield, *Birational classification of moduli spaces of representations of quivers*, Indag. Math. (N.S.) **12** (2001), no. 3, 407–432. MR 2003k:16028
190. Aidan Schofield, *Birational classification of moduli spaces of vector bundles over* $\mathbb{P}^2$, Indag. Math. (N.S.) **12** (2001), no. 3, 433–448. MR 2003g:14057
191. Issai Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen*, Sitzungsber. Preuss. Akad. Wiss. (1905), 77–91.
192. Jean-Pierre Serre, *Algèbre locale, multiplicités*, troisième ed., Lecture Notes in Mathematics, vol. 11, Springer-Verlag, Berlin-Heidelberg-New York, 1975.
193. Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 82e:12016
194. Jean-Pierre Serre, *Trees*, Springer-Verlag, Berlin, 1980, Translated from the French by John Stillwell. MR 82c:20083
195. Jean-Pierre Serre, *Sous-groupes finis des groupes de Lie*, Astérisque (2000), no. 266, Exp. No. 864, 5, 415–430, Séminaire Bourbaki, Vol. 1998/99. MR 2001j:20075
196. G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304. MR 15,600b
197. Balwant Singh, *Invariants of finite groups acting on local unique factorization domains*, J. Indian Math. Soc. (N.S.) **34** (1970), 31–38 (1971). MR 44 #6669
198. Peter Slodowy, *Der Scheibensatz für algebraische Transformationsgruppen*, Algebraische Transformationsgruppen und Invariantentheorie (H. Kraft, P. Slodowy, and T. A. Springer, eds.), DMV Sem., vol. 13, Birkhäuser, Basel, 1989, Appendix by F. Knop, pp. 89–113. MR 1044587
199. Larry Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995. MR 96f:13008
200. A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeitschrift **5** (1919), 1–6.
201. Tonny A. Springer, *Invariant theory*, Springer-Verlag, Berlin, 1977, Lecture Notes in Mathematics, Vol. 585. MR 56 #5740
202. Richard P. Stanley, *Combinatorics and commutative algebra*, second ed., Progress in Mathematics, vol. 41, Birkhäuser Boston Inc., Boston, MA, 1996. MR 98h:05001
203. Robert Steinberg, *Differential equations invariant under finite reflection groups*, Trans. Amer. Math. Soc. **112** (1964), 392–400. MR 29 #4807
204. Robert Steinberg, *On a theorem of Pittie*, Topology **14** (1975), 173–177. MR 51 #9101
205. Elisabetta Strickland, *The divisor class group of some semigroups associated to root systems*, J. Algebra **170** (1994), no. 1, 300–306. MR 95k:20070
206. Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996. MR 97b:13034
207. Richard G. Swan, *Induced representations and projective modules*, Ann. of Math. (2) **71** (1960), 552–578. MR 25 #2131
208. Richard G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158. MR 39 #5532
209. Richard G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982) (B. Srinivasan and J. Sally, eds.), Springer, New York, 1983, pp. 21–40. MR 84k:12013
210. Richard G. Swan, *Gubeladze's proof of Anderson's conjecture*, Azumaya algebras, actions, and modules (Bloomington, IN, 1990), Contemp. Math., vol. 124, Amer. Math. Soc., Providence, RI, 1992, pp. 215–250. MR 92m:13012
211. Richard G. Swan and E. Graham Evans, *K-theory of finite groups and orders*, Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 149. MR 46 #7310

212. J. J. Sylvester, *On the involution of two matrices of the second order*, British Assoc. Report (Southport), 1883, reprinted in: Collected Mathematical Papers, Vol. 4, Chelsea, 1973, pp. 115–117, pp. 430–432.

213. G. Szekeres, *Determination of a certain family of finite metabelian groups*, Trans. Amer. Math. Soc. **66** (1949), 1–43. MR 11,320i

214. Ken-Ichi Tahara, *On the finite subgroups of* $\mathrm{GL}(3, \mathbf{Z})$, Nagoya Math. J. **41** (1971), 169–209. MR 42 #7791

215. Mohammed Tesemma, *Reflection groups and semigroup algebras in multiplicative invariant theory*, Ph.D. thesis, Temple University, 2004.

216. È. B. Vinberg, *Rationality of the field of invariants of a triangular group*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. (1982), no. 2, 23–24, 115. MR 83k:14044

217. V. E. Voskresenskiĭ, *Birational properties of linear algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 3–19 (Russian), English translation: Math. USSR-Izv. **4** (1970), 1–17.

218. V. E. Voskresenskiĭ, *On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field* $Q(x_1, \cdots, x_n)$, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 366–375 (Russian), English translation: Math. USSR-Izv. **4** (1970), 371–380.

219. V. E. Voskresenskiĭ, *The birational invariants of algebraic tori*, Uspehi Mat. Nauk **30** (1975), no. 2(182), 207–208 (Russian). MR 58 #5701

220. V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998, translated from the Russian manuscript by Boris È. Kunyavskiĭ. MR 99g:20090

221. David B. Wales, *Linear groups of degree* n *containing an involution with two eigenvalues* -1. *II*, J. Algebra **53** (1978), no. 1, 58–67. MR 58 #921

222. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 97h:11130

223. Charles A. Weibel, *Pic is a contracted functor*, Invent. Math. **103** (1991), no. 2, 351–377. MR 92c:19002

224. Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 95f:18001

225. Boris Weisfeiler, *On the size and structure of finite linear groups*, preprint.

226. Boris Weisfeiler, *Post-classification version of Jordan's theorem on finite linear groups*, Proc. Nat. Acad. Sci. U.S.A. **81** (1984), no. 16, Phys. Sci., 5278–5279. MR 85j:20041

227. Joseph A. Wolf, *Spaces of constant curvature*, fifth ed., Publish or Perish Inc., Houston, TX, 1984. MR 88k:53002

Index