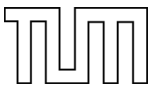
Technische Universität München

Fakultät für Mathematik
Lehrstuhl für Algebra

Arithmetic Invariant Rings of Finite Groups

David Mundelius



Technische Universität München

Fakultät für Mathematik
Lehrstuhl für Algebra

Arithmetic Invariant Rings of Finite Groups

David Mundelius

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation

Vorsitzender:		Prof. Dr. Daniel Matthes
Prüfer der Dissertation:	1.	Prof. Dr. Gregor Kemper
	2.	Prof. Dr. Peter Symonds University of Manchester

Die Dissertation wurde am 11.09.2019 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 26.12.2019 angenommen.

Summary

This thesis studies rings of invariants for linear actions of finite groups over Dedekind domains. This means, for a Dedekind domain R and a finite group $G \subseteq Gl_n(R)$ we consider the ring of invariants $R[x_1, \ldots, x_n]^G$. We study different structural properties of these rings and thereby generalize the corresponding well-known results for rings of invariants over fields.

First we prove that under certain conditions the ring of invariants of a pseudoreflection group over R is regular, and, that under the same conditions it is isomorphic to a polynomial ring over R if R is a principal ideal domain; this is a generalization of classical results of Shephard, Todd, and Chevalley. Furthermore, in this context we characterize all finitely generated regular graded R-algebras. Next we determine all finite subgroups of $Gl_n(R)$ for which the ring of invariants is factorial and those for which it is a quasi-Gorenstein ring; this generalizes results of Nakajima and Broer over fields.

Finally we prove that for certain points $x \in R_n$, many structural properties of the invariant ring of G are inherited by the invariant ring of the stabilizer subgroup G_x.

Zusammenfassung

Diese Arbeit befasst sich mit den Invariantenringen für lineare Operationen endlicher Gruppen über Dedekindringen. Das heißt, wir betrachten für einen Dedekindring R und eine endliche Gruppe $G \subseteq Gl_n(R)$ den Invariantenring $R[x_1, \ldots, x_n]^G$. Wir untersuchen verschiedene Struktureigenschaften dieser Ringe und verallgemeinern damit die entsprechenden bekannten Resultate für Invariantenringe über Körpern.

Zuerst zeigen wir, dass unter bestimmten Voraussetzungen der Invariantenring einer Spiegelungsgruppe über R regulär ist, und, dass er unter den gleichen Voraussetzungen isomorph ist zu einem Polynomring über R, falls R ein Hauptidealring ist. Das ist eine Verallgemeinerung klassischer Resultate von Shephard, Todd und Chevalley. Außerdem charakterisieren wir in diesem Zusammenhang alle endlich erzeugten regulären graduierten R-Algebren. Danach bestimmen wir alle endlichen Untergruppen von $Gl_n(R)$, für die der Invariantenring faktoriell ist, sowie diejenigen, für die der Invariantenring ein Quasi-Gorensteinring ist. Das verallgemeinert Resultate von Nakajima und Broer über Körpern.

Schließlich zeigen wir für bestimmte Punkte $x \in R^n$, dass sich viele Struktureigenschaften des Invariantenringes von G auf den des Stabilisators G_x übertragen.

Contents

1 Introduction

Invariant theory is one of the classical applications of commutative algebra; in fact, several of the early results in commutative algebra such as Hilbert's basis theorem have originally been developed in the context of invariant theory. While in its most general setting, invariant theory studies the ring of invariants S^G of any group G which acts by automorphisms on a ring S, most of the classical theory is developed for the following setting: let K be a field and let G be a group acting linearly on K^n; this induces an action on the polynomial ring $S \coloneqq K[x_1, \ldots, x_n]$. Then one studies the subring $K[x_1, \ldots, x_n]^G$ consisting of all polynomials which are invariant under this action of G. Among the many references for this theory we especially mention the books by Benson [4] and Derksen and Kemper [16].

If the group G is finite, then it was proved by Noether [47] that in the above setting $K[x_1, \ldots, x_n]^G$ is a finitely generated K-algebra; however, in general not much can be said about the structure of this ring, so it became an important part of invariant theory to analyze for which groups G the ring of invariants $K[x_1, \ldots, x_n]^G$ has certain ring-theoretic properties. The first main result in this direction is due to Shephard and Todd [54] and states that in the case $K = \mathbb{C}$ the ring of invariants is isomorphic to a polynomial ring if and only if G is generated by pseudoreflections; later this has been generalized to arbitrary fields K in which $|G|$ is invertible. Under the same assumption on $|G|$ Hochster and Eagon [29] proved that the ring of invariants is always a Cohen-Macaulay ring.

Also several other properties of rings of invariants have been studied; a summary of those results which are important for us is given in Section 2.3. Furthermore, it has been noticed that the ring of invariants of the stabilizer subgroup G_x of a point $x \in K^n$ inherits many properties from the ring of invariants of G; for a systematic account on results of this kind see Kemper [34].

Although Noether's finiteness theorem holds for actions of finite groups on rings in a much more general setting than just linear actions on polynomial rings over fields, most of the work on the structure of the ring of invariants has been done only in this special situation. The goal of this thesis is to generalize some of the classical structure theorems for rings of invariants over fields to the case of an action of a finite group G on $R[x_1, \ldots, x_n]$ induced by a linear action on R^n, where R is a sufficiently nice ring; these are what I call arithmetic invariant rings. What "sufficiently nice" precisely means differs between the sections of this thesis, but all main results are applicable if R is a Dedekind domain.

Previous work

To the best of my knowledge, no systematic account on invariant theory over rings is yet available in the literature. Several results on invariant rings appear in the literature which are formulated over arbitrary rings where this does not require much extra work; an important example are Göbel's results on invariant rings of permutation groups [22, 23]. Kemper [37] gave an algorithm for computing arithmetic invariant rings in the case where Gröbner basis computations are possible over the base ring R. For example, this is the case if R is Euclidean. Furthermore, in [36] Kemper proved a result on the Cohen-Macaulay defect of rings of invariants which does not need a base field. Notbohm [48] studied the question of when the ring of invariants of an irreducible pseudoreflection group over the p-adic integers for an odd prime p is isomorphic to a polynomial ring.

The Cohen-Macaulay property and some related properties of rings of invariants over $\mathbb{Z}$ have been studied recently by Almuhaimeed [1]; a summary of her results along with some other earlier results is given in Section 3.3. The approach of Almuhaimeed is complementary to the one used in this thesis in the following sense: most of Almuhaimeed's main results are useful mainly when one wants to know whether a ring of invariants for which an explicit set of generators is already given has certain properties; on the other hand, the main goal in this thesis is to prove these properties for the invariant rings of certain classes of subgroups of $Gl_n(R)$ so that one can decide whether a ring of invariants has a certain property without computing a set of generators.

Outline of the thesis

After recalling some basics from invariant theory and commutative algebra in Chapter 2 we begin our investigation of rings of arithmetic invariants in Chapter 3 by proving some elementary general results on these rings and providing several examples emphasizing different phenomena we will study in detail in later chapters. Chapter 3 ends with a detailed summary of some previous results on the structure of rings of arithmetic invariants.

Chapter 4 studies a first important property of rings of arithmetic invariants: we discuss the question of when a ring of arithmetic invariants is regular and closely related the question of when it is isomorphic to a polynomial ring, so the goal of this chapter is a generalization of the classical theorem of Shephard, Todd, and Chevalley to arithmetic invariant rings. Along the way we prove a general result on the structure of finitely generated regular graded algebras over Dedekind domains. The main results of Chapter 4 already appeared in [43].

The discussion of further properties of rings of arithmetic invariants requires some special knowledge on several related topics in commutative algebra which we introduce in Chapter 5: reflexive modules, divisorial ideals, divisor class groups, and Picard groups.

The theory of divisor class groups is used in Chapter 6 in order to answer the question under which conditions a ring of arithmetic invariants is factorial; moreover, we compute the Picard groups of rings of arithmetic invariants in this chapter. Chapter 7 contains a discussion of the question under which conditions a ring of arithmetic invariants is a

quasi-Gorenstein ring. We begin this chapter with a summary of the basic properties of canonical modules of local rings and a discussion of the quasi-Gorenstein property for graded rings. In Section 7.5 we prove the existence of homogeneous systems of parameters in rings of arithmetic invariants for certain classes of base rings; this is a result which might be interesting in its own right. This is then used to compute the graded canonical module of a ring of invariants over a local ring. Finally we prove our main result on the quasi-Gorenstein property by putting the previous results together and hereby removing the assumption that the base ring is local.

Finally in Chapter 8 we prove a result which shows that if the ring of arithmetic invariants of some group has a certain property, then the rings of invariants of certain stabilizer subgroups have the same property. This requires some basic results on étale morphisms of schemes which are summarized at the beginning of that chapter.

Main results

The first main new result of this thesis (Theorem 4.22) says that for the ring of invariants $R[x_1, \ldots, x_n]^G$ of a finite group $G \subseteq Gl_n(R)$ over a principal ideal domain R the following two statements are equivalent:

(i) *$R[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring over R and G acts faithfully on $(R/\mathfrak{p})^n$ for every maximal ideal $\mathfrak{p} \subset R$ which contains $|G|$.*

(ii) *The rings of invariants of G over $\mathrm{Quot}(R)$ and over all $R/\mathfrak{p}$ where $\mathfrak{p} \subset R$ is a prime ideal are all isomorphic to polynomial rings and the homogeneous generators of all these rings of invariants have the same degrees.*

In particular, if the assumption on faithfullness in (i) is given, the theorem completely characterizes those rings of invariants over principal ideal domains which are isomorphic to polynomial rings. The theorem also contains a generalization of this result to the case where R is only a Dedekind domain, although in this case the precise statement becomes much more technical.

Our second main result is Theorem 6.5, which answers the question of when a ring of invariants is factorial:

A ring of invariants $R[x_1, \ldots, x_n]^G$ with a finite group $G \subseteq Gl_n(R)$ and a Noetherian normal domain R is factorial if and only if both R and $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$ are factorial.

More precisely, we will see that the divisor class group of $R[x_1, \ldots, x_n]^G$ is the direct product of the divisor class groups of R and $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$; the divisor class group of $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$ is known by a classical result of Nakajima [45], see Theorem 2.19. Moreover, in this context we prove that under the same assumptions on R as above the Picard groups of R and $R[x_1, \ldots, x_n]^G$ are isomorphic, see Theorem 6.11; note that the Picard group of $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$ is always trivial by a result of Kang [31].

In Chapter 7 we prove a similar result for the quasi-Gorenstein property, see Definition 7.7. The main result here is Theorem 7.56:

A ring of invariants $R[x_1, \ldots, x_n]^G$ with a finite group $G \subseteq Gl_n(R)$ and a Dedekind domain R is a quasi-Gorenstein ring if and only if $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$ is a quasi-Gorenstein ring.

In fact, the result holds for a more general class of base rings R which we call allowed base rings, see Definition 7.51. Again, the question of when $\mathrm{Quot}(R)[x_1,\ldots,x_n]^G$ is quasi-Gorenstein is answered already; this is a result of Broer [8], see Theorem 7.30. Moreover, we shall see that if $|G|$ is invertible in R, then we can replace "quasi-Gorenstein" by "Gorenstein" in the above statement. Along the way towards these results we also prove that for a certain class of base rings R including all Noetherian local domains a ring of invariants $R[x_1,\ldots,x_n]^G$ always contains a homogeneous system of parameters (Corollary 7.38).

In the last main result of this thesis (Theorem 8.20) we consider an arbitrary Noetherian domain R, a finite group $G \subseteq Gl_n(R)$, and a point $x \in R^n$ such that for every maximal ideal $\mathfrak{m} \subset R$ the stabilizer subgroups in G of x and of the ideal

$$\{f \in R[x_1,\ldots,x_n] | f(x) - x \in \mathfrak{m}\} \subseteq R[x_1,\ldots,x_n]$$

coincide. Moreover let $\mathcal{P}$ be one of the following ring-theoretic properties: regularity, the Gorenstein property, and the Cohen-Macaulay property. The theorem then states the following:

If $R[x_1,\ldots,x_n]^G$ satisfies $\mathcal{P}$, then $R[x_1,\ldots,x_n]^{G_x}$ also satisfies $\mathcal{P}$.

If R is an allowed base ring in the same sense as mentioned above, this also holds if $\mathcal{P}$ is the quasi-Gorenstein property. Moreover, we prove that under the above assumptions we have $\mathrm{cmdef}(R[x_1,\ldots,x_n]^{G_x}) \leq \mathrm{cmdef}(R[x_1,\ldots,x_n]^G)$, where cmdef denotes the Cohen-Macaulay defect.

We finally mention that Section 9.1 contains a summary on how the different ring-theoretic properties of an arithmetic invariant ring considered in this thesis behave under certain changes of the base ring and the group.

Conventions

In this thesis "ring" always means "commutative ring with one". If R is a ring and $G \subseteq Gl_n(R)$ is a group and we consider an action of G on $R[x_1,\ldots,x_n]$ then this always means the induced action on the symmetric algebra of the module $(R^n)^*$ which is isomorphic to $R[x_1,\ldots,x_n]$. So for $\sigma \in G$, $f \in R[x_1,\ldots,x_n]$, $x \in R^n$ we have $\sigma(f)(x) = f(\sigma^{-1}(x))$. By a graded ring we always mean a positively graded ring. If R is a ring, then by a graded R-algebra $S = \bigoplus_{d\in\mathbb{N}_0} S_d$ we always mean a graded ring S with $S_0 \cong R$.

Acknowledgements

First of all I want to thank my supervisor Prof. Gregor Kemper for proposing this topic and for his continuous support. Moreover, I thank all the other members of the unit M11 at the faculty of mathematics at TUM for many interesting conversations. This thesis has been written within the graduate program TopMath within the Elite Network of Bavaria and the TUM Graduate School. I want to thank Agnieszka Baumgärtel, Dr. Carl-Friedrich Kreiner, and Dr. Katja Kröss who in a great way tackled all organizational issues within this program and all other TopMath students for many inspiring events.

2 Basics from invariant theory and commutative algebra

This chapter is a summary of several basic results from invariant theory and commutative algebra which will be used throughout this thesis. In later chapters we also need the theory of reflexive modules and divisor class groups; however, in order to avoid this chapter to become overly long, the introduction of these concepts is postponed to Chapter 5. Furthermore, the theory of canonical modules is postponed to the beginning of Chapter 7.

2.1 Rings of invariants

This section contains some basic definitions and results from invariant theory. We begin by recalling the definition of the ring of invariants.

Definition 2.1. *Let S be a ring. For a subgroup $G \subseteq \mathrm{Aut}(S)$ we define the ring of invariants as*

$$S^G := \{f \in S | \forall \sigma \in G : \sigma(f) = f\}.$$

In this thesis we shall mostly consider the special case where $S = R[x_1, \ldots, x_n]$ for some ring R and G is a subgroup of $Gl_n(R)$; we then define the action of G on S as follows: G acts on the dual M^* of the free R-module $M := R^n$ via the dual representation, i.e. for $\sigma \in G, f \in M^*, m \in m$ we set $(\sigma(f))(m) := f(\sigma^{-1}(m))$. Now we can identify $S = R[x_1, \ldots, x_n]$ with the symmetric algebra $S(M^*)$ and thus naturally extend the G-action to S. So for $\sigma \in G, f \in S, m \in R^n$ we have $\sigma(f)(m) = f(\sigma^{-1}(m))$; if R is infinite, we could also use this to define the action. In the following we only consider finite groups G for which we have the following basic result due to Noether [47], see also Derksen and Kemper [16, Proposition 3.0.1].

Theorem 2.2. (Noether's finiteness theorem) *Let R be a Noetherian ring, S a finitely generated R-algebra and $G \subseteq \mathrm{Aut}_R(S)$ a finite subgroup. Then S^G is again a finitely generated R-algebra.*

Proof. We can write $S = R[a_1, \ldots, a_n]$. Then a_i is a zero of the polynomial $h_i := \prod_{\sigma \in G}(x - \sigma(a_i)) \in S^G[x]$. Let $A \subseteq S^G$ be the R-subalgebra generated by all coefficients of the h_i; by construction S is integral over A and hence a finitely generated A-module. As it is a finitely generated R-algebra, A is Noetherian, so $S^G \subseteq S$ is also finitely generated as an A-module. Since A is a finitely generated R-algebra, the claim follows. □

The above proof also shows the following:

Proposition 2.3. *Let R, S, and G be as in Theorem 2.2. Then $S^G \subseteq S$ is an integral ring extension; in particular,* $\dim(S^G) = \dim(S)$.

If S is an integral domain and $G \subseteq \mathrm{Aut}(S)$ a subgroup, then G also acts on $\mathrm{Quot}(S)$. If G is finite, then for $\frac{a}{b} \in \mathrm{Quot}(S)^G$ we have

$$\frac{a}{b} = \frac{a \prod_{\sigma \in G \setminus \{\mathrm{id}\}} \sigma(b)}{\prod_{\sigma \in G} \sigma(b)} \in \mathrm{Quot}(S^G),$$

so $\mathrm{Quot}(S^G) = \mathrm{Quot}(S)^G$. We also immediately obtain the following:

Lemma 2.4. *Let S be an integral domain and let $G \subseteq \mathrm{Aut}(S)$ be a finite group. Then $S^G = S \cap \mathrm{Quot}(S^G)$.*

An important question in invariant theory is under which conditions a ring of invariants S^G inherits certain ring-theoretic properties from S. The following theorem is a first step in this direction.

Theorem 2.5. (see Derksen and Kemper [16, Proposition 2.4.4]) *Let S be a normal domain and let $G \subseteq \mathrm{Aut}(S)$ be a finite group. Then S^G is again normal.*

Proof. Let $f \in \mathrm{Quot}(S^G) \subseteq \mathrm{Quot}(S)$ be integral over S^G. Since S is normal, we have $f \in S$. So $f \in S \cap \mathrm{Quot}(S^G)$; by Lemma 2.4 this implies $f \in S^G$. Hence S^G is normal. □

We end this section by introducing two important maps which can often be used to construct elements in a ring of invariants.

Definition 2.6. *Let S be a ring and let $G \subseteq \mathrm{Aut}(S)$ be a finite group.*
a) The transfer Tr^G is the map $S \to S^G, f \mapsto \sum_{\sigma \in G} \sigma(f)$.
b) If $|G|$ is invertible in S, then the Reynolds operator $\mathcal{R}^G$ is the map $S \to S^G, f \mapsto \frac{1}{|G|}\mathrm{Tr}^G(f)$.

Both Tr^G and $\mathcal{R}^G$ are homomorphisms of S^G-modules; the Reynolds operator has the additional advantage that it is a projection map, i.e. for $f \in S^G$ we have $\mathcal{R}^G(f) = f$.

2.2 Ramification and pseudoreflections

In this section we collect several basic facts concerning ramification of prime ideals which will be needed several times in this thesis. As a general reference for this we mention Broué [9, Chapter 3]. For a ring A we define $X^{(1)}(A) := \{\mathfrak{p} \in \mathrm{Spec}(A) | \mathrm{ht}(\mathfrak{p}) = 1\}$.

We fix a finite extension of normal domains $A \subseteq B$, where finite means that B is finitely generated as an A-module. Let $\mathfrak{q} \in X^{(1)}(B)$ and $\mathfrak{p} := \mathfrak{q} \cap A$. Then $B_\mathfrak{q}$ is a discrete valuation ring and hence there is an $e(\mathfrak{q}, \mathfrak{p}) \in \mathbb{N}$ such that $\mathfrak{p}B_\mathfrak{q} = \mathfrak{q}^{e(\mathfrak{q},\mathfrak{p})}B_\mathfrak{q}$.

Definition 2.7. *Let A, B, $\mathfrak{q}$, and $\mathfrak{p}$ be as above. The number $e(\mathfrak{q}, \mathfrak{p})$ is called the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$. The ideal $\mathfrak{q}$ is called unramified over A if $e(\mathfrak{q}, \mathfrak{p}) = 1$ and the field extension $\mathrm{Quot}(B/\mathfrak{q}) \supseteq \mathrm{Quot}(A/\mathfrak{p})$ is separable; otherwise, it is called ramified.*

The following lemma is an immediate consequence of the definition of the ramification index:

Lemma 2.8. *Let $A \subseteq B \subseteq C$ be finite extensions of Noetherian normal domains, $\mathfrak{p} \in X^{(1)}(C)$, $\mathfrak{p}' := \mathfrak{p} \cap B$, and $\mathfrak{p}'' := \mathfrak{p} \cap A$. Then we have $e(\mathfrak{p}, \mathfrak{p}'') = e(\mathfrak{p}, \mathfrak{p}')e(\mathfrak{p}', \mathfrak{p}'')$.*

Proof. We have

$$\begin{aligned}\mathfrak{p}''C_{\mathfrak{p}} &= (\mathfrak{p}''B_{\mathfrak{p}'})C_{\mathfrak{p}} = ((\mathfrak{p}')^{e(\mathfrak{p}',\mathfrak{p}'')}B_{\mathfrak{p}'})C_{\mathfrak{p}} = (\mathfrak{p}')^{e(\mathfrak{p}',\mathfrak{p}'')}C_{\mathfrak{p}} \\ &= (\mathfrak{p}'C_{\mathfrak{p}})^{e(\mathfrak{p}',\mathfrak{p}'')} = (\mathfrak{p}^{e(\mathfrak{p},\mathfrak{p}')}C_{\mathfrak{p}})^{e(\mathfrak{p}',\mathfrak{p}'')} = \mathfrak{p}^{e(\mathfrak{p},\mathfrak{p}')\cdot e(\mathfrak{p}',\mathfrak{p}'')}C_{\mathfrak{p}}.\end{aligned}$$

Now the lemma follows from the definition of the ramification index. □

From now on we set $L := \mathrm{Quot}(B)$ and $K := \mathrm{Quot}(A)$ and assume that the field extension L/K is Galois with Galois group G. Since B is normal, G acts on B and since A is also normal and B is integral over A we have $A = B \cap K = B^G$ by Lemma 2.4.

Definition 2.9. *The inertia group of a prime ideal $\mathfrak{q} \in X^{(1)}(B)$ is the subgroup of G consisting of all $\sigma \in G$ for which $\sigma(\mathfrak{q}) = \mathfrak{q}$ and σ acts trivially on $B/\mathfrak{q}$; it is written as $G^i(\mathfrak{q})$.*

The next lemma connects the inertia group and the notion of unramified primes.

Lemma 2.10. *Let $\mathfrak{q} \in X^{(1)}(B)$ and $\mathfrak{p} := \mathfrak{q} \cap A$. The ramification index $e(\mathfrak{q}, \mathfrak{p})$ divides $|G^i(\mathfrak{q})|$. In particular, if $G^i(\mathfrak{q}) = \{\mathrm{id}\}$, then $e(\mathfrak{q}, \mathfrak{p}) = 1$.*

Proof. See [9, Proposition 3.4]. □

We give one further result on inertia groups here which we will need later:

Lemma 2.11. *Let $\mathfrak{q} \in X^{(1)}(B)$ and $\mathfrak{q}' := \mathfrak{q} \cap B^{G^i(\mathfrak{q})} \in X^{(1)}(B^{G^i(\mathfrak{q})})$. Then $G^i(\mathfrak{q}') = \{\mathrm{id}\}$.*

The following proof is an adaption of standrad arguments in algebraic number theory, see Neukirch [46, Chapter I, §9].

Proof. Let $\sigma \in G^i(\mathfrak{q}') \subseteq \mathrm{Gal}(L^{G^i(\mathfrak{q})}/K)$; we need to show that $\sigma = \mathrm{id}$. There is a $\tau_1 \in \mathrm{Gal}(L/K)$ such that $\tau_1|_{L^{G^i(\mathfrak{q})}} = \sigma$; set $\mathfrak{q}_1 := \tau_1(\mathfrak{q})$, so we have $\mathfrak{q}_1 \cap B^{G^i(\mathfrak{q})} = \tau_1(\mathfrak{q} \cap B^{G^i(\mathfrak{q})}) = \tau_1(\mathfrak{q}') = \sigma(\mathfrak{q}') = \mathfrak{q}' = \mathfrak{q} \cap B^{G^i(\mathfrak{q})}$. Then there is a $\tau_2 \in \mathrm{Gal}(L/L^{G^i(\mathfrak{q})}) \subseteq \mathrm{Gal}(L/K)$ with $\tau_2(\mathfrak{q}_1) = \mathfrak{q}$ (see [9, Theorem 3.2]) and for $\tau := \tau_2 \circ \tau_1 \in \mathrm{Gal}(L/K)$ we have $\tau|_{L^{G^i}(\mathfrak{q})} = \sigma$ and $\tau(\mathfrak{q}) = \mathfrak{q}$. We now prove that τ acts trivially on $B/\mathfrak{q}$; then we have $\tau \in G^i(\mathfrak{q})$ and hence $\sigma = \tau|_{L^{G^i(\mathfrak{q})}} = \mathrm{id}$ as desired.

We define $F := \mathrm{Quot}(B^{G^i(\mathfrak{q})}/\mathfrak{q}')$ and $\hat{F} := \mathrm{Quot}(B/\mathfrak{q})$. Since we know that σ acts trivially on $B^{G^i(\mathfrak{q})}/\mathfrak{q}'$, it is sufficient to prove that the finite field extension $\hat{F}/F$ has no nontrivial automorphisms. Let F^s be the maximal separable extension of F in $\hat{F}$ and let $\overline{\theta}$ be a primitive element of the field extension F^s/F. Since $B^{G^i(\mathfrak{q})}/\mathfrak{q}' \subseteq B/\mathfrak{q}$ is an integral extension, there is an $a \in B^{G^i(\mathfrak{q})}/\mathfrak{q}'$ such that $a\overline{\theta} \in B/\mathfrak{q}$. But $a \in F$, so $a\overline{\theta}$ is again a primitive element of $\hat{F}/F$ and therefore we may assume that $\overline{\theta} \in B/\mathfrak{q}$. Let

$\overline{g} \in F[t]$ be the minimal polynomial of $\overline{\theta}$ over F; let $\theta \in B$ be a representative of $\overline{\theta}$. We define $f \in B^{G^i(\mathfrak{q})}[t]$ to be the minimal polynomial of θ over $B^{G^i(\mathfrak{q})}$; since $B^{G^i(\mathfrak{q})} \subseteq B$ is integral, f is monic and in particular the class $\overline{f} \in F[t]$ of f is not zero. We have $\overline{f}(\overline{\theta}) = 0$, so $\overline{g}$ divides $\overline{f}$. Now let δ be an automorphism of $\hat{F}/F$. Then $\delta(\overline{\theta})$ is a zero of $\overline{g}$ and hence of $\overline{f}$, so there is a zero $\theta' \in B$ of f such that $\overline{\theta'} = \delta(\overline{\theta})$ (f can be written as a product of linear factors in $B[t]$ because $L/L^{G^i(\mathfrak{q})}$ is a normal field extension and B is a normal domain). Since f is irreducible, there is a $\rho \in G^i(\mathfrak{q}) = \mathrm{Gal}(L/L^{G^i(\mathfrak{q})})$ such that $\rho(\theta) = \theta'$. By the definition of the inertia group, the induced automorphism $\overline{\rho}$ of $\hat{F}/F$ is the identity, so $\delta(\overline{\theta}) = \overline{\theta'} = \overline{\rho(\theta)} = \overline{\rho}(\overline{\theta}) = \overline{\theta}$. Since $\overline{\theta}$ generates the field extension F^s/F, this implies $\delta|_{F^s} = \mathrm{id}$. But then $\delta = \mathrm{id}$ because $\hat{F}/F^s$ is purely inseparable and therefore does not have any non-trivial automorphisms. □

We now introduce pseudoreflections. These will play an essential role in several of the theorems on ring-theoretic properties of rings of invariants in the next section. From now on, we fix a field F. We discuss generalizations of this concept to rings in Section 3.1.

Definition 2.12.
a) A matrix $\sigma \in Gl_n(F)$ is called a pseudoreflection if $\sigma \neq \mathrm{id}$, σ is of finite order and σ fixes some $(n-1)$-dimensional subspace of F^n elementwise.
b) A finite subgroup $G \subseteq Gl_n(F)$ is called a pseudoreflection group if G is generated by pseudoreflections.

A pseudoreflection in $Gl_n(\mathbb{R})$ is simply called a reflection and pseudoreflection groups over $\mathbb{R}$ are usually called Coxeter groups. A diagonalizable matrix σ is a pseudoreflection if and only if all but one eigenvalue of σ is equal to 1 and the remaining eigenvalue is a root of unity. Over fields of characteristic zero every pseudoreflection is diagonalizable; in positive characteristic this is not true as here for example the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is a pseudoreflection which is not diagonalizable. Non-diagonalizable pseudoreflections are called transvections. In the previous section we defined an action of $Gl_n(F)$ on $F[x_1, \ldots, x_n]$. Using this we can characterize pseudoreflections as follows:

Lemma 2.13. *Let $\sigma \in Gl_n(F)$. Then σ is a pseudoreflection if and only if the height of the ideal in $F[x_1, \ldots, x_n]$ generated by $(\sigma - \mathrm{id})(F[x_1, \ldots, x_n])$ is one.*

This motivates the following definition (see Nakajima [45]):

Definition 2.14. *Let S be an F-algebra. An automorphism $\sigma \in \mathrm{Aut}_F(S)$ is called a generalized reflection if the height of the ideal in S generated by $(\sigma - \mathrm{id})(S)$ is one.*

For later use, we also note the following:

Lemma 2.15. *Let $\sigma, \tau \in Gl_n(K)$ and assume that σ is a pseudoreflection. Then $\tau^{-1}\sigma\tau$ is again a pseudoreflection. In particular, if $G \subseteq Gl_n(K)$ is a subgroup and $N \subseteq G$ is the subgroup of G generated by all pseudoreflections in G, then N is a normal subgroup of G.*

The next proposition gives a connection between ramification and pseudoreflections:

Proposition 2.16. *Let $S := F[x_1, \ldots, x_n]$ be the polynomial ring in n variables over F and let $G \subseteq Gl_n(F)$ be a finite group; again, we view the elements of G as automorphisms of S. Let $\mathfrak{q} \in X^{(1)}(S)$ and $\sigma \in G^i(\mathfrak{q}) \backslash \{\mathrm{id}\} \subseteq G$. Then σ is a pseudoreflection.*

Proof. See Broué [9, Proposition 3.7]. □

2.3 Properties of invariant rings over fields

Let F be a field and let $G \subseteq Gl_n(F)$ be a finite group. In this section we collect some results answering the question under which conditions the ring of invariants $F[x_1, \ldots, x_n]^G$ has certain nice properties; these questions form one of the main branches of invariant theory of finite groups. The main goal of this thesis is to develop analogous results in the case where the field F is replaced by some ring R. Invariant theory over F often becomes much simpler when $\mathrm{char}(F)$ does not divide $|G|$; this is called the nonmodular case. The more complicated case where $\mathrm{char}(F)$ divides $|G|$ is called the modular case.

The simplest possible structure $F[x_1, \ldots, x_n]^G$ can have is that it is isomorphic to a polynomial ring over F or, equivalently, that it is generated by n algebraically independent elements; note that $\dim(F[x_1, \ldots, x_n]^G) = n$ by Proposition 2.3. In the nonmodular case we have the following theorem:

Theorem 2.17. *Assume that* $\mathrm{char}(F) \nmid |G|$. *Then the following two statements are equivalent:*
(i) $F[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring.
(ii) G is a pseudoreflection group.
If $\mathrm{char}(F)$ *divides $|G|$, then the implication $(i) \implies (ii)$ still holds.*

This has first been proved by Shephard and Todd [54] in the case $F = \mathbb{C}$ and then by Chevalley [12] in the case $F = \mathbb{R}$; it was noted later that Chevalley's proof works for arbitrary fields with $\mathrm{char}(F) \nmid |G|$. Another proof of this result has been given by Smith [55]. The implication $(i) \implies (ii)$ for arbitrary fields is due to Serre [52]. A proof of the whole theorem can also be found in Benson's book [4, Theorem 7.2.1].

For the next result, we need the notion of a character:

Definition 2.18. *Let G be a group and let R be a ring. An (R-valued) character of G is a group homomorphism $G \to R^\times$.*

Now we can formulate the following theorem due to Nakajima [45] which fully answers the question under which conditions $F[x_1, \ldots, x_n]^G$ is factorial.

Theorem 2.19. *Let $N \subseteq G$ be the subgroup generated by all pseudoreflections in G. The ring of invariants $F[x_1, \ldots, x_n]^G$ is factorial if and only if every F-valued character of G is uniquely determined by its restriction to N or, equivalently, if and only if every F-valued character which takes the value one on every pseudoreflection takes the value one on all elements of G.*

In the nonmodular case, the question of when a ring of invariants is a Cohen-Macaulay ring is answered by the following theorem by Hochster and Eagon [29]:

Theorem 2.20. *Let F be a field and let $G \subseteq Gl_n(F)$ be a finite group such that* $\mathrm{char}(F) \nmid |G|$. *Then the ring of invariants $F[x_1, \ldots, x_n]^G$ is a Cohen-Macaulay ring.*

The question under which conditions $F[x_1, \ldots, x_n]^G$ is a Gorenstein ring has been studied by several people. The following theorem answeres this under the assumption that G contains no pseudoreflections. It is due to Watanabe [59, 60] in the nonmodular case and due to Braun [6] in the modular case.

Theorem 2.21. *Assume that G does not contain a pseudoreflection. Then the following two conditions are equivalent:*
(i) $F[x_1, \ldots, x_n]^G$ is a Gorenstein ring.
(ii) $F[x_1, \ldots, x_n]^G$ is a Cohen-Macaulay ring and $G \subseteq Sl_n(F)$.

This result has been generalized to the case where G may contain pseudoreflections by Broer [8] and Fleischmann and Woodcock [18]. Since their result requires some more terminology, we postpone its statement to Chapter 7, see Theorem 7.30.

2.4 Dedekind domains

Dedekind domains will play a crucial role throughout this thesis, so it may be helpful to briefly recall some important results about them here; as a standard reference for this topic we use Neukirch [46]. We begin with the definition.

Definition 2.22. *A Dedekind domain is a Noetherian normal integral domain of Krull dimension at most one.*

Example 2.23.
a) Every principal ideal domain is a Dedekind domain.
b) If K is an algebraic number field, then the ring of algebraic integers $\mathcal{O}_K$ is a Dedekind domain.
c) More generally, if R is a Dedekind domain, $K := \mathrm{Quot}(R)$, and L/K is a finite field extension, then the integral closure of R in L is again a Dedekind domain (see [46, Chapter I, Proposition 12.8]).
d) Let K be an algebraically closed field and let C be an irreducible smooth affine curve over K. Then the coordinate ring $K[C]$ is a Dedekind domain.

In a factorial domain, every ideal of height one is principal (see Bruns and Herzog [11, Lemma 2.2.17]), so we obtain the following lemma:

Lemma 2.24. *A Dedekind domain is factorial if and only if it is a principal ideal domain.*

We will also frequently use the following local characterization of Dedekind domains.

Proposition 2.25. ([46, Chapter I, Proposition 11.5]) *A Noetherian integral domain R is a Dedekind domain if and only if for every prime ideal $\mathfrak{p} \subset R$ the localization $R_\mathfrak{p}$ is either a field or a discrete valuation ring. In particular, every local Dedekind domain is either a field or a discrete valuation ring and hence a principal ideal domain.*

An immediate consequence of this is the following:

Proposition 2.26. *Every Dedekind domain is a regular ring and hence also a Gorenstein ring and a Cohen-Macaulay ring.*

Next we introduce fractional ideals; for later use we define them for arbitrary Noetherian domains, not just for Dedekind domains.

Definition 2.27. *Let R be a Noetherian domain.*
a) A fractional ideal of R is a nonzero finitely generated R-submodule of $\mathrm{Quot}(R)$.
b) For two fractional ideals I and J their product is defined as

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in I, b_i \in J \right\}.$$

c) A fractional ideal is called principal if it is generated by one element as an R-module.
d) For a fractional ideal I, the inverse of I is defined as

$$I^{-1} = \{a \in \mathrm{Quot}(R) | aI \subseteq R\}$$

and I is called invertible if $II^{-1} = R$.

One important property of a Dedekind domain R is that the set of all fractional ideals of R forms an abelian group J_R with respect to the product defined above ([46, Chapter I, Proposition 3.8]); in particular, in a Dedekind domain every fractional ideal is invertible. The principal fractional ideals form a subgroup $P_R \subseteq J_R$ and the factor group $\mathrm{Cl}(R) := J_R/P_R$ is called the ideal class group of R. Now Lemma 2.24 says that R is factorial of and only if $\mathrm{Cl}(R) = \{1\}$. In Section 5.3 we discuss a generalization of the ideal class group to a larger class of domains.

Over a principal ideal domain every finitely generated torsion-free module is free. This is not true anymore over a Dedekind domain; however, there is still a nice description of such modules.

Theorem 2.28. *Let R be a Dedekind domain and let M be a finitely generated torsion-free R-module. Then the following holds:*
a) M is projective.
b) If $M \neq \{0\}$, then there exist an $n \in \mathbb{N}_0$ and a nonzero ideal $I \subseteq R$ such that $M \cong R^n \oplus I$. The number n is uniquely determined and the class of the ideal I in $\mathrm{Cl}(R)$ *is uniquely determined by M. In particular, I is a principal ideal if and only if M is free.*

Proof. See for example Curtis and Reiner [14, Theorem 4.13]. □

2.5 Graded rings

This section contains some basic results about graded rings which will be needed throughout this thesis. As a general reference we mention Bruns and Herzog [11, Section 1.5]. For us a graded ring is always a positively graded ring, that is, a ring S which can be written as $S = \bigoplus_{d\in\mathbb{N}_0} S_d$ (direct sum of additive groups) such that $S_d \cdot S_e \subseteq S_{d+e}$ for all $d, e \in \mathbb{N}_0$. If R is any ring, then by a graded R-algebra we always mean a graded ring $S = \bigoplus_{d\in\mathbb{N}_0} S_d$ with $S_0 \cong R$. An ideal I in a graded ring S is called homogeneous if for $f = \sum_{d\in\mathbb{N}_0} f_d \in I$ with $f_d \in S_d$ for all d each f_d is again in I. Moreover we define $S_+ := \bigoplus_{d>0} S_d$.

Lemma 2.29. *Let S be a graded ring. The homogeneous maximal ideals in S are precisely the ideals of the form $(\mathfrak{n}, S_+)_S$ where $\mathfrak{n}$ is a maximal ideal in S_0. Moreover, every homogeneous ideal in S is contained in a homogeneous maximal ideal.*

Proof. Let $\mathfrak{n} \subset S_0$ be a maximal ideal and set $\mathfrak{m} := (\mathfrak{n}, S_+)_S$. Then $S/\mathfrak{m} \cong S_0/\mathfrak{n}$, so $\mathfrak{m}$ is indeed a maximal ideal. Conversely, let $\mathfrak{m}'$ be a homogeneous maximal ideal in S. Then $\mathfrak{m}' \cap S_0$ is a proper ideal in S_0, so there exists a maximal ideal $\mathfrak{n} \subset S_0$ such that $\mathfrak{m}' \cap S_0 \subseteq \mathfrak{n}$. Since $\mathfrak{m}'$ is a homogeneous ideal, we obtain $\mathfrak{m}' \subseteq \mathfrak{m} := (\mathfrak{n}, S_+)_S$ and since $\mathfrak{m}'$ is maximal, this implies $\mathfrak{m}' = \mathfrak{m}$ and hence $\mathfrak{m}'$ is of the desired form.

For the second statement, let I be any homogeneous ideal. Then there is a maximal ideal $\mathfrak{n} \subset S_0$ such that $I \cap S_0 \subseteq \mathfrak{n}$, so every homogeneous element of I is contained in $\mathfrak{m} := (\mathfrak{n}, S_+)_S$ and hence $I \subseteq \mathfrak{m}$ because I is homogeneous. By the first statement $\mathfrak{m}$ is a homogeneous maximal ideal, so the second statement follows. □

The literature on graded rings often focuses on graded rings S for which S_0 is a field. When we want to do invariant theory over rings, then we obviously need more general graded rings; it turns out that there is a particularly nice theory for so-called *local graded rings.

Definition 2.30. *A graded ring is called *local if it contains only one homogeneous maximal ideal.*

By Lemma 2.29 a graded ring $S = \bigoplus_{n\in\mathbb{N}_0} S_n$ is *local if and only if S_0 is a local ring. In this case, the unique homogeneous maximal ideal in S is $(\mathfrak{m}, S_+)_S$ where $\mathfrak{m}$ is the unique maximal ideal in S_0.

For a graded ring S and an S_0-algebra A we can define a natural grading on $S' := S \otimes_{S_0} A$ by setting $(S')_d := S_d \otimes_{S_0} A$ for each d. In particular, for a prime ideal $\mathfrak{p} \subset S_0$ $S \otimes_{S_0} (S_0)_\mathfrak{p}$ becomes a *local graded ring. This often allows us to reduce to the case of *local graded rings and is the main reason why *local rings are important for us. We can also describe this ring as a localization: $S \otimes_{S_0} (S_0)_\mathfrak{p} \cong (S_0 \backslash \mathfrak{p})^{-1} S$.

Next we discuss homogeneous prime ideals.

Definition 2.31. *Let S be a graded ring and let $I \subset S$ be any ideal. Then we define I^* to be the homogeneous ideal in S generated by all homogeneous elements of I.*

Clearly if I is a homogeneous ideal, then $I^* = I$. Now let $\mathfrak{p}$ be a prime ideal in a graded ring S. Then $\mathfrak{p}^*$ is again a prime ideal ([11, Lemma 1.5.6]); moreover, we have the following:

Lemma 2.32. (Matijevic and Roberts [40, Lemma 1], see also [11, Theorem 1.5.8]) *Let S be a graded ring and let $\mathfrak{p} \subset S$ be a non-homogeneous prime ideal in S. Then* $\mathrm{ht}(\mathfrak{p}^*) = \mathrm{ht}(\mathfrak{p}) - 1$.

This lemma has the following consequence, see also Eisenbud [17, Corollary 13.7].

Lemma 2.33. *Let S be a graded ring with* $\dim S < \infty$. *Then there is a homogeneous maximal ideal $\mathfrak{m} \subset S$ with* $\mathrm{ht}(\mathfrak{m}) = \dim(S)$.

Proof. Let $\mathfrak{m}_0$ be any maximal ideal in S with $\mathrm{ht}(\mathfrak{m}_0) = \dim(S)$. If $\mathfrak{m}_0$ is already homogeneous, we are done. Otherwise, by Lemma 2.32 $\mathfrak{m}_0^*$ is a homogeneous prime ideal with $\mathrm{ht}(\mathfrak{m}_0^*) = \dim(S) - 1$. Since $\mathfrak{m}_0^* \subsetneq \mathfrak{m}_0$, $\mathfrak{m}_0^*$ is not a maximal ideal, so by Lemma 2.29 there is a homogeneous maximal ideal $\mathfrak{m} \subset S$ such that $\mathfrak{m}_0^* \subsetneq \mathfrak{m}$ and hence $\mathrm{ht}(\mathfrak{m}) > \mathrm{ht}(\mathfrak{m}_0^*) = \dim(S) - 1$, so $\mathrm{ht}(\mathfrak{m}) = \dim(S)$. □

We will often need to check whether a graded ring has certain ring-theoretic properties. For many properties this can be checked at localizations at graded prime ideals. Here we give a slight reformulation of these results which will turn out to be the most useful version for our purposes.

Proposition 2.34. *Let S be a Noetherian graded ring. Then the following statements are equivalent.*

(i) S is regular.

(ii) For every homogeneous maximal ideal $\mathfrak{m} \subset S$ the localization $S_{\mathfrak{m}}$ is regular.

(iii) For every maximal ideal $\mathfrak{p} \subset S_0$ the ring $S \otimes_{S_0} (S_0)_{\mathfrak{p}} \cong (S_0 \backslash \mathfrak{p})^{-1} R$ is regular.

Proof. It is well known that (i) implies (iii) (see [11, Corollary 2.2.9]). Next we prove that (iii) implies (ii): let $\mathfrak{m} \subset R$ be a homogeneous maximal ideal, then $\mathfrak{m} = (\mathfrak{p}, S_+)_S$ for some maximal ideal $\mathfrak{p} \subset S_0$ by Lemma 2.29. Since $S_0 \backslash \mathfrak{p} \subseteq S \backslash \mathfrak{m}$, $S_{\mathfrak{m}}$ is a localization of $(S_0 \backslash \mathfrak{p})^{-1} S$ and hence regular by (iii). Finally, we prove that (ii) implies (i). In order to prove that S is regular, it is sufficient to prove that $S_{\mathfrak{q}}$ is regular for every homogeneous prime ideal $\mathfrak{q} \subset S$ (see [11, Exercise 2.2.24]). By Lemma 2.29 there is a homogeneous maximal ideal $\mathfrak{m} \subset S$ with $\mathfrak{q} \subseteq \mathfrak{m}$. Then $S_{\mathfrak{m}}$ is regular by assumption. But since $\mathfrak{q} \subset \mathfrak{m}$, $S_{\mathfrak{q}}$ can be viewed as a localization of $S_{\mathfrak{m}}$, so $S_{\mathfrak{q}}$ is also regular (see [11, Corollary 2.2.9]). The claim follows. □

Similarly, we can prove the following two results; instead of [11, Exercise 2.2.24] we use [11, Exercise 2.1.27] and [11, Exercise 3.6.20].

Proposition 2.35. *Let S be a Noetherian graded ring. Then the following statements are equivalent.*

(i) S is a Cohen-Macaulay ring.

(ii) *For every homogeneous maximal ideal $\mathfrak{m} \subset S$ the localization $S_{\mathfrak{m}}$ is a Cohen-Macaulay ring.*
(iii) *For every maximal ideal $\mathfrak{p} \subset S_0$ the ring $S \otimes_{S_0} (S_0)_{\mathfrak{p}} \cong (S_0 \backslash \mathfrak{p})^{-1} S$ is a Cohen-Macaulay ring.*

Proposition 2.36. *Let S be a Noetherian graded ring. Then the following statements are equivalent.*
(i) *S is a Gorenstein ring.*
(ii) *For every homogeneous maximal ideal $\mathfrak{m} \subset S$ the localization $S_{\mathfrak{m}}$ is a Gorenstein ring.*
(iii) *For every maximal ideal $\mathfrak{p} \subset S_0$ the ring $S \otimes_{S_0} (S_0)_{\mathfrak{p}} \cong (S_0 \backslash \mathfrak{p})^{-1} S$ is a Gorenstein ring.*

We end this section by giving some results on graded modules, see for example Brodmann and Sharp [7, Section 13.1]. Let S be a graded ring; a graded S-module is an S-module M which, as an abelian group, can be written as $M = \bigoplus_{e \in \mathbb{Z}} M_e$ such that for all $d \in \mathbb{N}_0, e \in \mathbb{Z}$ we have $S_d \cdot M_e \subseteq M_{d+e}$. For a graded module M and $m \in \mathbb{Z}$ let $M(m)$ be the graded module given by $M(m)_e := M_{m+e}$.

Definition 2.37. *Let S be a graded ring and let M and N be graded S-modules. A homomorphism $\varphi : M \to N$ is called homogeneous of degree $d \in \mathbb{Z}$ if for every $e \in \mathbb{Z}$ we have $\varphi(M_e) \subseteq N_{d+e}$. The set of all such homomorphisms is written as* $\mathrm{Hom}_d(M, N)$. *We define* ${}^*\mathrm{Hom}_S(M, N) := \bigoplus_{d \in \mathbb{Z}} \mathrm{Hom}_d(M, N)$.

Each $\mathrm{Hom}_d(M, N)$ is an abelian group and ${}^*\mathrm{Hom}_S(M, N)$ is a graded S-module. A homomorphism of graded modules is simply called homogeneous if it is homogeneous of degree zero. We define the category ${}^*\mathcal{C}(S)$ whose objects are graded S-modules and whose morphisms are homogeneous homomorphisms (of degree zero) of S-modules. Then ${}^*\mathcal{C}(S)$ is an abelian category ([7, 13.1.7(i)]); for every graded S-module M there is a surjective homogeneous homomorphism $P \to M$ for some graded free S-module P, so M has a free resolution in ${}^*\mathcal{C}(S)$; we call such a resolution a graded free resolution of M. We can use this to define a graded version of the Ext-functor: for a fixed graded module N the functor ${}^*\mathrm{Hom}(\cdot, N) : {}^*\mathcal{C}(S) \to {}^*\mathcal{C}(S)$ is left exact ([7, Exercise 13.1.8(ii)]), so we can make the following definition.

Definition 2.38. *The functor* ${}^*\mathrm{Ext}^r_S(\cdot, N)$ *is the r-th right derived functor of* ${}^*\mathrm{Hom}(\cdot, N)$. *More concretely, let $P_\bullet$ be a graded free resolution of M. Then* ${}^*\mathrm{Ext}^r_S(M, N)$ *is the r-th cohomology module of the cochain complex* ${}^*\mathrm{Hom}(P_\bullet, M)$.

In many situations, the graded *Ext-module and the usual Ext-module are the same object:

Lemma 2.39. ([7, Exercise 13.1.8(iv)]) *Let S be a graded ring and let M and N be graded S-modules. Assume that S is Noetherian and M is finitely generated. Then for every $r \geq 0$ we have* ${}^*\mathrm{Ext}^r_S(M, N) \cong \mathrm{Ext}^r_S(M, N)$; *in particular* ${}^*\mathrm{Hom}_S(M, N) \cong \mathrm{Hom}_S(M, N)$.

3 Arithmetic invariants: first steps

In this chapter we begin the investigation of rings of arithmetic invariants, i.e. rings of invariants of the form $R[x_1, \ldots, x_n]^G$ where R need not be a field. The first section contains some elementary properties of these rings. The second section gives several examples of rings of invariants over the integers which show the different behaviour that can occur for these rings. The third section is a collection of several results concerning properties of rings of arithmetic invariants which can be found in the literature.

3.1 Basic properties

Let R be a ring and let $G \subseteq Gl_n(R)$ be a finite group. As usual, G acts on the polynomial ring $S := R[x_1, \ldots, x_n]$ via the dual representation on $(R^n)^* \subseteq S((R^n)^*) \cong R[x_1, \ldots, x_n]$. The goal of this thesis is to study the properties of the ring of invariants S^G. In this section we begin with some basic properties. First of all Theorem 2.2 and Proposition 2.3 yield the following:

Proposition 3.1. *Let R be a Noetherian ring and let S and G be as above. Then the following holds:*
a) S^G is finitely generated as an R-algebra.
b) The ring extension $S^G \subseteq S$ is integral.

We now want to study what happens when we change the base ring R. Let R' be any R-algebra. Then we get a canonical homomorphism $Gl_n(R) \to Gl_n(R')$ and hence a natural R'-representation of $G \subseteq Gl_n(R)$, although this representation need not be faithful. We write $S_{R'} := S \otimes_R R' = R'[x_1, \ldots, x_n]$. We have a canonical map $S \to S_{R'}$ which is compatible with the G-action, so we obtain a canonical homomorphism $S^G \to S_{R'}^G$ the image of which is $S^G \otimes_R R'$. In general, this map will not be surjective even if G acts faithfully on $(R')^n$, as Example 3.10 in the next section shows. The situation becomes much better if we consider the special case that R is an integral domain and R' is a localization of R. In this case we have the following:

Proposition 3.2. *Let R be an integral domain and let $U \subseteq R \backslash \{0\}$ be a multiplicative subset. Then with S and G as above, the following statements hold:*
a) $U^{-1}(S^G) = (U^{-1}S)^G$. In particular, every set of generators of S^G as an R-algebra also generates $(U^{-1}S)^G$ as an $U^{-1}R$-algebra.
b) $S^G = (U^{-1}S)^G \cap S$.

Proof. Since G acts trivially on R and hence on U, we have $U^{-1}(S^G) \subseteq (U^{-1}S)^G$. On the other hand, if $\frac{f}{a} \in (U^{-1}S)^G$ where $f \in S$ and $a \in U$, then $a \in R \subseteq S^G$, so we must

also have $f \in S^G$. Hence $\frac{f}{a} \in U^{-1}(S^G)$, so the proof of *a)* is complete. For part *b)* we now have $(U^{-1}S)^G \cap S = U^{-1}(S^G) \cap S = S^G$, where the second equality again follows from the fact that G acts trivially on U. □

The next proposition provides a relation between generators of the invariant ring over R and generators of the invariant rings over $R_\mathfrak{m}$ for maximal ideals $\mathfrak{m} \subset R$.

Proposition 3.3. *Let R be an integral domain. Assume that there are $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]^G$ such that $R_\mathfrak{m}[x_1, \ldots, x_n]^G = R_\mathfrak{m}[f_1, \ldots, f_m]$ for every maximal ideal $\mathfrak{m} \subset R$. Then $R[x_1, \ldots, x_n]^G = R[f_1, \ldots, f_m]$.*

Proof. We claim that for arbitrary $g_1, \ldots, g_r \in R[x_1, \ldots, x_r]$ we have

$$R[g_1, \ldots, g_r] = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\max}(R)} R_\mathfrak{m}[g_1, \ldots, g_r].$$

It is clear that the left hand side is contained in the right, so let f be an element of the right hand side. We define $I := \{a \in R | af \in R[g_1, \ldots, g_r]\}$. Certainly I is an ideal in R and we need to show that $I = R$. Assume the contrary: then there is a maximal ideal $\mathfrak{m} \subset R$ such that $I \subseteq \mathfrak{m}$. We have $f \in R_\mathfrak{m}[g_1, \ldots, g_r] = (R \backslash \mathfrak{m})^{-1} R[g_1, \ldots, g_r]$, so there is a $b \in R \backslash \mathfrak{m}$ such that $bf \in R[g_1, \ldots, g_r]$. But then $b \in I$, contradicting the assumption that $I \subseteq \mathfrak{m}$.

As a special case we have $R[x_1, \ldots, x_n] = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\max}(R)} R_\mathfrak{m}[x_1, \ldots, x_n]$ and hence also $R[x_1, \ldots, x_n]^G = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\max}(R)} R_\mathfrak{m}[x_1, \ldots, x_n]^G$. So by using the assumption and the above equality we obtain:

$$R[f_1, \ldots, f_m] = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\max}(R)} R_\mathfrak{m}[f_1, \ldots, f_m] = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\max}(R)} R_\mathfrak{m}[x_1, \ldots, x_n]^G = R[x_1, \ldots, x_n]^G.$$

□

The first part of Proposition 3.2 shows that if we know the ring of invariants over one base ring R, then we also know it over every localization of R. On the contrary, if we pass from R to a quotient ring R/I for some ideal $I \subset R$, then there is no easy connection between the invariants over R and over R/I. In particular, the natural homomorphism $R[x_1, \ldots, x_n]^G \to (R/I)[x_1, \ldots, x_n]^G$ need not be surjective, see Example 3.10. The situation becomes much better if $|G|$ is a unit in R:

Lemma 3.4. *Let R be a ring and let $I \subset R$ be a prime ideal. Let $G \subseteq Gl_n(R)$ be a finite group such that $|G|$ is a unit in R. Then the canonical projection map $p : R[x_1, \ldots, x_n] \to (R/I)[x_1, \ldots, x_n]$ restricts to a surjective homomorphism*

$$R[x_1, \ldots, x_n]^G \to (R/I)[x_1, \ldots, x_n]^G.$$

Proof. Let $g \in (R/I)[x_1, \ldots, x_n]^G$ and let $f_0 \in R[x_1, \ldots, x_n]$ with $p(f_0) = g$. Since $|G|$ is a unit in R, we have the Reynolds operator

$$\mathcal{R}_G : R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]^G, f \mapsto \sum_{\sigma \in G} \sigma(f).$$

We define $f := \mathcal{R}_G(f_0) \in R[x_1, \ldots, x_n]^G$. Then we have $p(f) = \frac{1}{|G|}\sum_{\sigma\in G} p(\sigma(f_0)) = \frac{1}{|G|}\sum_{\sigma\in G} \sigma(p(f_0)) = \frac{1}{|G|}\sum_{\sigma\in G} \sigma(g) = g$ where in the last step we used that g is an invariant. Hence g is indeed in the image of $p|_{R[x_1,\ldots,x_n]^G}$. □

We will see in Lemma 3.9 below that for certain groups $G \subseteq Gl_n(R)$ the projection map p as in Lemma 3.4 is always surjective even if $|G|$ is not a unit in R.

In order to formulate arithmetic analogues for the theorems from Section 2.3 in later chapters, we will need the notion of a pseudoreflection over rings.

Definition 3.5. *Let R be an integral domain and $K := \mathrm{Quot}(R)$. We call a matrix $A \in Gl_n(R)$ a pseudoreflection if it is a pseudoreflection in $Gl_n(K)$.*

Remark 3.6. The analogue of Lemma 2.13 is false over rings. Consider the matrix $\sigma := -\mathrm{id} \in Gl_n(\mathbb{Z})$ for some $n > 1$. Then σ is clearly not a pseudoreflection in $Gl_n(\mathbb{Q})$, but $(\sigma - \mathrm{id})(S) \subseteq (2)_S$ where $S := \mathbb{Z}[x_1, \ldots, x_n]$ and hence $\mathrm{ht}(((\sigma - \mathrm{id})(S))_S) = 1$ by Krull's principal ideal theorem.

We immediately get the following result:

Proposition 3.7. *Let R be an integral domain and let $G \subseteq Gl_n(R)$ be a finite group such that the ring of invariants $R[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring. Then G is a pseudoreflection group.*

Proof. Let $K := \mathrm{Quot}(R)$. Then $K[x_1, \ldots, x_n]^G$ is also isomorphic to a polynomial ring by Proposition 3.2. Now the claim follws from Theorem 2.17. □

The type of examples of arithmetic invariant rings we are mainly interested in is the following. Let $G \subseteq Gl_n(\mathbb{C})$ be a finite group such that the entries of all matrices in G are algebraic integers. Then there is some number field K with ring of integers R such that $G \subseteq Gl_n(R)$. In this situation we want to study the ring of invariants $R[x_1, \ldots, x_n]^G$ and compare it to $K[x_1, \ldots, x_n]^G$. This naturally determines the class of base rings we are mainly interested in: the ring of integers in a number field is always a Dedekind domain, so our main goal is to study rings of invariants $R[x_1, \ldots, x_n]^G$ where R is a Dedekind domain. However, whenever this is possible without too much extra effort, we formulate our results in greater generality.

3.2 Examples

In this section we present several examples of arithmetic invariants rings, some of which we will use again as counterexamples in later chapters.

Example 3.8. Let R be any ring and let S_n be the symmetric group viewed as the group of all permutation matrices in $Gl_n(R)$. Then the fundamental theorem on symmetric polynomials (see for example Lang [39, Chapter IV, Theorem 6.1]) tells us that the ring of invariants $R[x_1, \ldots, x_n]^{S_n}$ is generated by the elementary symmetric polynomials

$$s_k := \sum_{1\le i_1<\ldots<i_k\le n} \prod_{j=1}^{n} x_{i_j} \qquad (k = 1, \ldots, n).$$

So in this example, the generators of the invariant ring do not depend on R; in particular, for every R-algebra R' we have $R'[x_1,\dots,x_n]^{S_n} \cong R'[x_1,\dots,x_n]^{S_n} \otimes_R S$. This holds in a more general situation:

Lemma 3.9. *Let R be a ring and let $G \subseteq Gl_n(R)$ be a permutation group, i.e. every element of G just permutes the standard basis of R^n. Then for every R-algebra R' we have $R'[x_1,\dots,x_n]^G \cong R[x_1,\dots,x_n]^G \otimes_R R'$.*

Proof. Göbel [22] proved that the ring of invariants of a permutation group G over an arbitrary ring A is generated by all orbit sums of monomials in $A[x_1,\dots,x_n]$, that is, all sums of the form $\sum_{u\in\{\sigma(t)|\sigma\in G\}} u$ where $t \in A[x_1,\dots,x_n]$ is a monomial. In particular, this holds both for $A = R$ and for $A = R'$, so $R[x_1,\dots,x_n]^G$ generates $R'[x_1,\dots,x_n]^G$ as an R'-algebra. From this, the lemma follows. □

The following example shows that there really are new phenomena in arithmetic invariant theory which do not occur over fields.

Example 3.10. We consider the local ring $R := \mathbb{Z}_{(3)}$ as a base ring and the group $G \subseteq Gl_2(R)$ generated be the two matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

This is a finite group isomorphic to the symmetric group S_3, so $|G| = 6$. We first consider the ring of invariants of this group over $\mathbb{Q} = \mathrm{Quot}(R)$. It contains the two polynomials $f_1 := x^2 - xy + y^2, f_2 := 2x^3 - 3x^2y - 3xy^2 + 2y^3$. Since the Jacobian determinant of f_1 and f_2 is $27xy(y-x) \neq 0$ and $|G| = \deg(f_1)\cdot\deg(f_2)$ it follows that $\mathbb{Q}[x,y]^G = \mathbb{Q}[f_1,f_2]$, see Kemper [32, Proposition 16]. We can also consider the ring of invariants over the residue field $\mathbb{F}_3 = R/(3)$; it contains the two polynomials $g_1 := x+y, g_2 := x^4y^2 + x^3y^3 + x^2y^4$ with Jacobian determinant $xy^4 + x^2y^3 - x^3y^2 - x^4y$ and as above we obtain $\mathbb{F}_3[x,y]^G = \mathbb{F}_3[g_1,g_2]$. So the rings of invariants over $\mathbb{Q}$ and $\mathbb{F}_3$ are both isomorphic to polynomial rings. However, we shall see now that $R[x,y]^G$ is not isomorphic to a polynomial ring. Assume there exist invariants $h_1, h_2 \in R[x,y]^G$ such that $R[x,y]^G = R[h_1,h_2]$. Since $\dim(R[x,y]^G) = \dim(R[x,y]) = 3 = \dim(R)+2$, h_1 and h_2 are algebraically independent over R, so by Lemma 3.11 below we may assume that h_1 and h_2 are homogeneous. Then we also have $\mathbb{Q}[x,y]^G = \mathbb{Q}[h_1,h_2]$ and since by the above $\mathbb{Q}[x,y]^G$ contains elements of degrees 2 and 3, but no elements of degree 1, this is only possible if the degrees of h_1 and h_2 are 2 and 3. Since $\mathbb{Q}[x,y]^G = \mathbb{Q}[f_1,f_2]$, every invariant of degree 2 is a scalar multiple of f_1. So $h_1 = c_1 f_1$ for some $c_1 \in R$ and since $f_1 \in R[h_1,h_2]$ and h_1 and h_2 must be algebraically independent we have $c_1 \in R^\times$. Similarly there is a $c_2 \in R^\times$ such that $c_2 f_2 = h_2$, so $R[h_1,h_2] = R[f_1,f_2]$ and hence if $R[x,y]^G$ is isomorphic to a polynomial ring, then $R[x,y]^G = R[f_1,f_2]$. But this is not the case: $k := \frac{1}{27}(4f_1^3 - f_2^2)$ is in $R[x,y]^G$, but since f_1 and f_2 are algebraically independent and $\frac{1}{27} \notin R$, we have $k \notin R[f_1,f_2]$. This proves that $R[x,y]^G$ is not isomorphic to a polynomial ring. We will revisit this example in Chapter 4 and will there be able to give a better explanation of what happens here.

In the above example we used the following lemma:

Lemma 3.11. *Let R be a principal ideal domain and let S be a graded R-algebra generated by elements $f_1, \ldots, f_n$ which are algebraically independent over R. Then there exist homogeneous elements $g_1, \ldots, g_n \in S$ such that $S = R[g_1, \ldots, g_n]$.*

Proof. By assumption, S is isomorphic to the polynomial ring in n variables over R, so S is a regular ring, see Bruns and Herzog [11, Theorem 2.2.13]; hence the lemma is a special case of Corollary 4.11 in the next chapter. However, for this special case we can also give a more elementary proof.

Since $S_0 = R$ we may assume that $f_1, \ldots, f_n \in S_+$. Then $f_1, \ldots, f_n$ generate S_+ as an ideal in S and their classes generate $M := S_+/S_+^2$ as an R-module. Next we show that M is a free R-module: since $f_1, \ldots, f_n$ are algebraically independent over R, $B := \{f_1^{e_1} \cdots f_n^{e_n} | e_1, \ldots, e_n \in \mathbb{N}_0\}$ is a basis of S as an R-module. Then $B \backslash \{1\}$ is a basis of S_+ as an R-module and $B \backslash \{1, f_1, \ldots, f_n\}$ is a basis of S_+^2 as an R-module. This shows that we have $S_+ = S_+^2 \oplus (f_1, \ldots, f_n)_R$ and hence $M = S_+/S_+^2 \cong (f_1, \ldots, f_n)_R$ is free of rank n.

Furthermore, M is a graded S-module since S_+ and S_+^2 are homogeneous ideals, so we can write $M = \bigoplus_{d=1}^{r} M_d$. Each M_d is a direct summand of M as an R-module, M is free, and R is a principal ideal domain, so each M_d is again free and hence M has a basis $\{\overline{g_1}, \ldots, \overline{g_n}\}$ consisting of homogeneous elements. We can choose representatives $g_1, \ldots, g_n \in S_+$ of these classes which are homogeneous in S. By the graded version of Nakayama's lemma (see Derksen and Kemper [16, Lemma 3.7.1]; they state the result only for graded rings S in which S_0 is a field, but this assumption is not needed in their proof) we obtain that $g_1, \ldots, g_n$ generate S_+ as an ideal in S. Then we also have $S = R[g_1, \ldots, g_n]$, see Bruns and Herzog [11, Proposition 1.5.4]. □

The following example taken from Almuhaimeed [1, Example 6.2.23] shows that similar phenomena as in the previous example for the question of being a polynomial ring can also occur for the Cohen-Macaulay property.

Example 3.12. We consider the following matrix in $Gl_3(\mathbb{Z})$:

$$U := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then the group $G := \langle U \rangle$ is of order 4. Almuhaimeed calculated the ring of invariants $\mathbb{Z}[x_1, x_2, x_3]^G$ explicitly and proved that it is not Cohen-Macaulay. However, $\mathbb{Q}[x_1, x_2, x_3]^G$ is Cohen-Macaulay by Theorem 2.20 and by a result of Smith [56] also the ring of invariants of G over $\mathbb{F}_p$ is Cohen-Macaulay for every prime p.

It is proven in [1] that up to conjugation the group G given in the previous example is the only finite subgroup of $Gl_3(\mathbb{Z})$ with a non-Cohen-Macaulay invariant ring. Furthermore, in [1, Example 6.2.26] an example of a finite subgroup of $Gl_4(\mathbb{Z})$ which also has a non-Cohen-Macaulay ring of invariants is given. In both examples, it follows from Theorem 2.21 that the ring of invariants over $\mathbb{Q}$ is not Gorenstein. Here is an example, where the ring of invariants over $\mathbb{Z}$ is not Cohen-Macaulay, while the one over $\mathbb{Q}$ is Gorenstein.

Example 3.13. Let $G = \{\iota, \sigma\}$ be the cyclic group of order 2. Then we define a $\mathbb{Z}$-linear action of G on $M := \mathbb{Z}^2$ where σ acts by interchanging the two components of an element of M. This induces an action of G on $M^n \cong \mathbb{Z}^{2n}$ for all $n \in \mathbb{N}$. With $S^{(n)} := \mathbb{Z}[x_1, \ldots, x_{2n}]$ we can now study the ring of invariants $(S^{(n)})^G$ given by this action of G on M^n. We claim that for a suitable choice of n, $(S^{(n)})^G \otimes_{\mathbb{Z}} \mathbb{Q}$ is Gorenstein while $(S^{(n)})^G$ is not Cohen-Macaulay.

For $n > 1$, σ does not act as a pseudoreflection on M^n, so by Watanabe's Theorem 2.21, $(S^{(n)})^G \otimes_{\mathbb{Z}} \mathbb{Q}$ is Gorenstein if and only if the determinant of σ as an element of $Gl_{2n}(\mathbb{Z})$ is one. But σ acts on M via the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so this determinant is $(-1)^n$ and hence $(S^{(n)})^G \otimes_{\mathbb{Z}} \mathbb{Q}$ is Gorenstein for all even n.

Now assume that $(S^{(n)})^G$ is Cohen-Macaulay. Then $(S^{(n)})^G \otimes_{\mathbb{Z}} \mathbb{F}_2 \cong (S^{(n)})^G/(2)$ is again Cohen-Macaulay (see Bruns and Herzog, [11, Theorem 2.1.3(a)]). Since G acts on M^n as a permutation group, $(S^{(n)})^G \otimes_{\mathbb{Z}} \mathbb{F}_2$ is isomorphic to $(S^{(n)} \otimes_{\mathbb{Z}} \mathbb{F}_2)^G$ by Lemma 3.9. It follows from Kemper [33, Corollary 2.4] that this ring of invariants is not Cohen-Macaulay for sufficiently large n. Hence the same is true for $(S^{(n)})^G$; so if n is sufficiently large and even, then indeed we have both desired properties. In fact, it follows from [33, Remark 2.5] that we can choose $n = 4$.

3.3 Previous results

In this section we collect some results on arithmetic invariant rings available in the literature which address questions related to those we discuss in the subsequent chapters. We begin with the following generalization of Theorem 2.20. Already in Hochster's and Eagon's article [29, Proposition 13] it is proven that whenever a finite group G acts by automorphisms on a Cohen-Macaulay ring S in which $|G|$ is invertible, then the ring of invariants S^G is again a Cohen-Macaulay ring; see Kemper [36, Theorem 1.1] for a generalization of this result. In our setting, it implies the following:

Theorem 3.14. *Let R be a Cohen-Macaulay ring and let $G \subseteq Gl_n(R)$ be a finite group such that $|G|$ is a unit in R. Then $R[x_1, \ldots, x_n]^G$ is again a Cohen-Macaulay ring.*

Further results concerning the Cohen-Macaulay property for rings of invariants over $\mathbb{Z}$ have been obtained by Almuhaimeed [1]. Although we will not use these theorems in this thesis, they address questions similar to those discussed in this thesis, so it seems appropriate to mention these results here. Perhaps the most important result of Almuhaimeed is the following:

Theorem 3.15. (Almuhaimeed [1, Corollary 6.2.12 and Theorem 6.2.15]) *Let $G \subseteq Gl_n(\mathbb{Z})$ be a finite group.*

a) $\mathbb{Z}[x_1, \ldots, x_n]^G$ is Cohen-Macaulay if and only if for every prime number p which divides $|G|$ the ring $\mathbb{Z}[x_1, \ldots, x_n]^G/(p)$ is Cohen-Macaulay.

b) If for every Sylow subgroup $P \subseteq G$ the ring of invariants $\mathbb{Z}[x_1, \ldots, x_n]^P$ is Cohen-Macaulay, then $\mathbb{Z}[x_1, \ldots, x_n]^G$ is also Cohen-Macaulay.

Note that the ring $\mathbb{Z}[x_1,\ldots,x_n]^G/(p)$ occurring in Theorem 3.15 is in general not the same as the invariant ring $\mathbb{F}_p[x_1,\ldots,x_n]^G$. Furthermore, Almuhaimeed proved a result similar to Theorem 3.15a) for the Gorenstein property:

Theorem 3.16. (Almuhaimeed [1, Theorem 6.3.2]) *Let $G \subseteq Gl_n(\mathbb{Z})$ be a finite group. Then the following statements are equivalent.*

(i) $\mathbb{Z}[x_1,\ldots,x_n]^G$ *is Gorenstein.*

(ii) For every prime number p, the ring $\mathbb{Z}[x_1,\ldots,x_n]^G/(p)$ is Gorenstein.

(iii) For every prime number p which divides $|G|$, the rings $\mathbb{Z}[x_1,\ldots,x_n]^G/(p)$ and $\mathbb{Q}[x_1,\ldots,x_n]^G$ are Gorenstein.

Remark 3.17. In [1] in statement *(iii)* of the previous theorem instead of the condition that $\mathbb{Q}[x_1,\ldots,x_n]^G$ is Gorenstein one finds the condition that the Hilbert series H of $\mathbb{Q}[x_1,\ldots,x_n]^G$ satisfies $H(\frac{1}{t}) = (-1)^n t^\rho H(t)$ for some $\rho \in \mathbb{Z}$. By a result of Stanley [57, Theorem 4.4] these two conditions are equivalent.

Moreover, Almuhaimeed proved the following result concerning the question of when a ring of invariants over the integers is isomorphic to a polynomial ring.

Theorem 3.18. (Almuhaimeed [1, Theorem 6.4.2 (ii)]) *Let $G \subseteq Gl_n(\mathbb{Z})$ be a finite group and let $f_1,\ldots,f_n$ be a homogeneous system of parameters in $\mathbb{Z}[x_1,\ldots,x_n]^G$ (see Definition 7.31) such that $\prod_{i=1}^n \deg(f_i) = |G|$. If G acts faithfully on $\mathbb{F}_p^n$ for every prime number p or $\mathbb{Z}[x_1,\ldots,x_n]^G$ is Cohen-Macaulay, then $\mathbb{Z}[x_1,\ldots,x_n]^G = \mathbb{Z}[f_1,\ldots,f_n]$.*

Note that Example 3.10 is not a contradiction to Theorem 3.18 as in that example f_1 and f_2 do not form a system of parameters in $R[x,y]^G$ because the invariant k occurring in the example is not integral over $R[f_1,f_2]$.

4 Regularity of arithmetic invariant rings

By the Chevalley-Shephard-Todd theorem (Theorem 2.17) the ring of invariants of a finite group G over a field in the nonmodular case is isomorphic to a polynomial ring if and only if G is a pseudoreflection group. Smith's proof [55] of this result is based on the fact that a finitely generated graded algebra over a field is isomorphic to a polynomial ring if and only if it is regular, or equivalently, if and only if its global dimension is finite.

The goal of this chapter is to generalize these results to invariant rings over Dedekind domains. In the first section we prove criteria which in many cases allow to decide whether a ring of invariants over a discrete valuation ring is isomorphic to a polynomial ring (and hence regular) once we know the rings of invariants over the quotient field and over the residue field. In order to extend these results to general Dedekind domains, we need a characterization of regular graded algebras over Dedekind domains. This is the content of Section 4.2. It turns out that regular graded algebras over principal ideal domains are always isomorphic to polynomial rings while over Dedekind domains the situation is slightly more complicated. In the last section of this chapter the previous results are put together in order to analyze the structure of invariant rings of pseudoreflection groups over Dedekind domains.

The main results of this chapter have already appeared in [43].

4.1 Invariants of pseudoreflection groups over discrete valuation rings

In this section we always assume that R is a discrete valuation ring with maximal ideal (π), quotient field $K := \mathrm{Quot}(R)$, and residue field $F := R/(\pi)$. We define $S := R[x_1, \ldots, x_n]$, $S_K := S \otimes_R K \cong K[x_1, \ldots, x_n]$, and $S_F := S \otimes_R F \cong F[x_1, \ldots, x_n]$ and consider a finite subgroup $G \subseteq Gl_n(R)$. The object we are interested in is the ring of invariants S^G. Assume we have homogeneous invariants $f_1, \ldots, f_n \in S^G$ such that $S_K^G = K[f_1, \ldots, f_n]$; these are then necessarily algebraically independent over K because $\dim(S_K^G) = \dim(S_K) = n$. The following lemma answers the question of whether we also have $S^G = R[f_1, \ldots, f_n]$.

Lemma 4.1. *With the notation as above we have $S^G = R[f_1, \ldots, f_n]$ if and only if the classes of $f_1, \ldots, f_n$ in S_F are algebraically independent over F.*

Proof. Let $\overline{f_i}$ be the class of f_i in $F[x_1, \ldots, x_n]$. First assume that $S^G = R[f_1, \ldots, f_n]$ and suppose that there is a polynomial $\overline{p} \in F[y_1, \ldots, y_n] \backslash \{0\}$ such that $\overline{p}(\overline{f_1}, \ldots, \overline{f_n}) = 0$. Choose a $p \in R[y_1, \ldots, y_n]$ such that $\overline{p}$ is the class of p in $F[y_1, \ldots, y_n]$. Then $\pi \nmid p$, but $\pi | p(f_1, \ldots, f_n)$, so $g := \frac{1}{\pi} p(f_1, \ldots, f_n) \in S^G$, but $\frac{1}{\pi} p \notin R[y_1, \ldots, y_n]$ and hence $g \notin$

$R[f_1, \ldots, f_n]$ because $f_1, \ldots, f_n$ are algebraically independent over K. This contradicts $S^G = R[f_1, \ldots, f_n]$, so $\overline{f_1}, \ldots, \overline{f_n}$ are algebraically independent over F.

Now we assume that $\overline{f_1}, \ldots, \overline{f_n}$ are algebraically independent and prove that we then have $S^G = R[f_1, \ldots, f_n]$. So let $g \in S^G$; then $g \in S_K^G = K[f_1, \ldots, f_n]$ and hence there is a polynomial $p \in K[y_1, \ldots, y_n]$ such that $g = p(f_1, \ldots, f_n)$. Assume that $p \notin R[y_1, \ldots, y_n]$ and let $l \in \mathbb{N}$ be minimal such that $\pi^l p \in R[y_1, \ldots, y_n]$; by our assumption we have $l > 0$. Hence, the class of $\pi^l g = \pi^l p(f_1, \ldots, f_n)$ in $F[x_1, \ldots, x_n]$ is zero and since $\overline{f_1}, \ldots, \overline{f_n}$ are algebraically independent over F, this proves that the class of $\pi^l p$ in $F[y_1, \ldots, y_n]$ is zero. But then π divides $\pi^l p$ in $R[y_1, \ldots, y_n]$ and we obtain a contradiction to the minimality of l. So we must have $l = 0$, so $p \in R[y_1, \ldots, y_n]$ and hence $g \in R[f_1, \ldots, f_n]$. □

Example 4.2. Let $R = \mathbb{Z}_{(2)}$; then we have $K = \mathrm{Quot}(R) = \mathbb{Q}$ and $F = R/(2) = \mathbb{F}_2$. We consider the symmetric group $G = S_2$ acting on R^2 by permuting the two components. Then the ring of invariants over K is $K[x_1, x_2]^G = K[x_1 + x_2, x_1 x_2] = K[x_1 + x_2, x_1^2 + x_2^2]$. While $x_1 + x_2$ and $x_1 x_2$ are algebraically independent over F, $x_1 + x_2$ and $x_1^2 + x_2^2$ are not as $x_1^2 + x_2^2 = (x_1 + x_2)^2 \in F[x_1, x_2]$. So by Lemma 4.1 we have $R[x_1, x_2]^G = R[x_1 + x_2, x_1 x_2] \neq R[x_1 + x_2, x_1^2 + x_2^2]$. Indeed,

$$x_1 x_2 = \frac{1}{2}((x_1 + x_2)^2 - (x_1^2 + x_2^2)) \notin R[x_1 + x_2, x_1^2 + x_2^2]$$

because $x_1 + x_2$ and $x_1^2 + x_2^2$ are algebraically independent over R.

We now want to use Lemma 4.1 to prove sufficient conditions for S^G to be a polynomial ring. For this we need the following lemma on invariant rings over fields.

Lemma 4.3. *Let $\tilde{K}$ be any field and let $G \subseteq Gl_n(\tilde{K})$ be a finite group such that $\tilde{K}[x_1, \ldots, x_n]^G$ is a polynomial ring. Furthermore let $f_1, \ldots, f_n \in \tilde{K}[x_1, \ldots, x_n]^G$ be homogeneous polynomials which are algebraically independent over $\tilde{K}$. Then the following statements are equivalent:*

(i) $\tilde{K}[x_1, \ldots, x_n]^G = \tilde{K}[f_1, \ldots, f_n]$.
(ii) $\deg(f_1) \cdots \deg(f_n) = |G|$.
(iii) $\deg(f_1) \cdots \deg(f_n) \leq |G|$.

Proof. The equivalence of *(i)* and *(ii)* is a result of Kemper [32, Proposition 16] and it is clear that *(ii)* implies *(iii)*. It remains to prove that *(iii)* implies *(ii)*. For this we need to show that $\deg(f_1) \cdots \deg(f_n) < |G|$ is impossible. By assumption there exist homogeneous invariants $g_1, \ldots, g_n$ such that $\tilde{K}[x_1, \ldots, x_n]^G = \tilde{K}[g_1, \ldots, g_n]$. We change the order of the f_i and g_i in such a way that $\deg(f_i) \leq \deg(f_j)$ and $\deg(g_i) \leq \deg(g_j)$ for all $i < j$. Since we already know that *(i)* implies *(ii)*, we obtain that $\deg(g_1) \cdots \deg(g_n) = |G|$. Now assume $\deg(f_1) \cdots \deg(f_n) < |G|$; then there must be an index i such that $d := \deg(f_i) < \deg(g_i)$. Let A be the $\tilde{K}$-subalgebra of $\tilde{K}[x_1, \ldots, x_n]^G$ generated by all elements of degree at most d; then A is contained in the $\tilde{K}$-algebra generated by $g_1, \ldots, g_{i-1}$; in particular, the transcendence degree of A is at most $i-1$. But $f_1, \ldots, f_i \in A$, so $f_1, \ldots, f_i$ cannot be algebraically independent, a contradiction to the assumption. □

Now we can prove the desired sufficient condition for S^G to be a polynomial ring:

Proposition 4.4. *Assume that both S_K^G and S_F^G are isomorphic to polynomial rings over K and F, respectively and that they are generated by homogeneous invariants of the same degrees, i.e. we have $S_K^G = K[f_1, \ldots, f_n]$ and $S_F^G = F[g_1, \ldots, g_n]$ such that all f_i and g_i are homogeneous and $\deg(f_i) = \deg(g_i)$ for each i. Then S^G is isomorphic to a polynomial ring over R.*

Proof. Let $d \in \mathbb{N}_0$. From the assumptions we immediately get that

$$\dim_K (S_K^G)_d = \dim_F (S_F^G)_d.$$

Here $(S_K^G)_d$ denotes the degree-d-part of the graded ring S_K^G and similarly for $(S_F^G)_d$. Since R is a discrete valuation ring and hence a principal ideal domain, S_d^G is a finitely generated free R-module; let $B = \{p_1, \ldots, p_m\}$ be a basis; then B is also a basis of the K-vector space $(S_K^G)_d$. Let $\overline{p_i}$ be the image of p_i under the canonical map $S^G \to S_F^G$ and $\overline{B} := \{\overline{p_1}, \ldots, \overline{p_m}\}$. We claim that $\overline{B}$ is F-linearly independent. For this we need to show that if we have $\lambda_1, \ldots, \lambda_m \in R$ such that $\lambda_1 p_1 + \ldots + \lambda_m p_m$ is divisible by π, then each λ_i is divisible by π. We have

$$\sum_{i=1}^{m} \frac{\lambda_i}{\pi} p_i \in S_d^G = \langle p_1, \ldots, p_m \rangle_R$$

and hence indeed $\frac{\lambda_i}{\pi} \in R$ since $p_1, \ldots, p_m$ are K-linearly independent, so the claim follows. The equality of dimensions above now shows that $\overline{B}$ is a basis of $(S_F^G)_d$. Overall we have now proved that the canonical map $\varphi : S^G \to S_F^G$ is surjective. By assumption there are homogeneous $g_1, \ldots, g_n \in S_F^G$ such that $S_F^G = F[g_1, \ldots, g_n]$. Choose homogeneous $h_i \in S^G$ such that $\varphi(h_i) = g_i$. Furthermore by assumption there are homogeneous $f_1, \ldots, f_n \in S_K^G$ such that $S_K^G = K[f_1, \ldots, f_n]$ and $\deg(h_i) = \deg(g_i) = \deg(f_i)$ for each i. So we have $\deg(h_1) \cdots \deg(h_n) = \deg(f_1) \cdots \deg(f_n) = |G|$ by Lemma 4.3. Using Lemma 4.3 again we obtain $S_K^G = K[h_1, \ldots, h_n]$. Since $\varphi(h_1) = g_1, \ldots, \varphi(h_n) = g_n$ are algebraically independent over F, Lemma 4.1 shows that $S^G = R[h_1, \ldots, h_n]$. □

An important special case of Proposition 4.4 is the following:

Corollary 4.5. *If G is generated by pseudoreflections and $|G|$ is invertible in R, then S^G is a polynomial ring over R.*

Proof. Since $|G|$ is invertible in R, it is also invertible in K and in F, so both S_K^G and S_F^G are isomorphic to polynomial rings by Theorem 2.17. Let $g_1, \ldots, g_n$ be homogeneous generators of S_F^G. By Lemma 4.3 we have $\deg(g_1) \cdots \deg(g_n) = |\tilde{G}| \leq |G|$, where $\tilde{G}$ is the image of G in $Gl_n(F)$. Let φ denote the projection map $S \to S_F$ and for $i = 1, \ldots, n$ we choose homogeneous $f_i \in S^G$ such that $\varphi(f_i) = g_i$ (such elements exist by Lemma 3.4). Then the f_i are algebraically independent over R and thus also over K. Furthermore we have $\deg(f_i) = \deg(g_i)$, so $\deg(f_1) \cdots \deg(f_n) \leq |G|$. Lemma 4.3 now implies that $S_K^G = K[f_1, \ldots, f_n]$. Using Proposition 4.4 we obtain that S^G is indeed isomorphic to a polynomial ring. □

For the proof of the next theorem we need that if a graded algebra over a field is isomorphic to a polynomial ring, then the degrees of the homogeneous generators are uniquely determined. Since this does not cause any extra difficulties, we prove this over rings.

Lemma 4.6. *Let $B = \bigoplus_{d\in\mathbb{N}_0} B_d$ be a graded ring and $A := B_0$. Let $f_1, \dots, f_n, g_1, \dots, g_n$ be homogeneous elements of S such that the set of all f_i and the set of all g_i are both algebraically independent over A. Assume that for $i \le j$ we have $\deg(f_i) \le \deg(f_j)$ and $\deg(g_i) \le \deg(g_j)$. Then if $A[f_1, \dots, f_n] = A[g_1, \dots, g_n]$ we have $\deg(f_i) = \deg(g_i)$ for each i.*

Proof. For $d \in \mathbb{N}$ let C_d be the subalgebra of B generated by all elements of degree at most d. Let m_d be the largest $m \in \mathbb{N}$ such that $\deg(f_m) \le d$ and let m'_d be the largest $\deg(g_m) \le d$. Then we have $C_d = A[f_1, \dots, f_{m_d}] = A[g_1, \dots, g_{m'_d}]$ because the f_i and g_i are homogeneous. Because of the algebraic independence of the f_i and the g_i we then obtain that both m_d and m'_d are equal to the transcendence degree of C_d over A; in particular $m_d = m'_d$. Since this is true for all d, the lemma follows. □

We can now prove a partial converse of Proposition 4.4. Note that F^n becomes a representation of G via the canonical map $Gl_n(R) \to Gl_n(F)$.

Theorem 4.7. *Assume that $S_K^G = K[f_1, \dots, f_n]$ for certain homogeneous elements $f_1, \dots, f_n$. Then the following two statements are equivalent.*

(i) There are homogeneous elements $g_1, \dots, g_n \in S_F^G$ such that $S_F^G = F[g_1, \dots, g_n]$ and $\deg(g_i) = \deg(f_i)$ for each i.

(ii) S^G is isomorphic to a polynomial ring and G acts faithfully on F^n.

So if we assume that G acts faithfully on F^n, then the converse of Proposition 4.4 is true.

Proof. We first prove that (i) implies (ii). So suppose that (i) holds; then the first part of (ii) follows from Proposition 4.4. Let $\alpha : G \to Gl_n(F)$ be the canonical map. By Lemma 4.3 we have $|G| = \deg(f_1) \cdots \deg(f_n)$ and $|\mathrm{im}(\alpha)| = \deg(g_1) \cdots \deg(g_n)$, so by (i) we have $|G| = |\mathrm{im}(\alpha)|$; hence α is injective and this just means that the action of G on F^n is faithful.

Now we assume that (ii) holds. Then $S^G = R[h_1, \dots, h_n]$ for certain homogeneous $h_i \in S^G$. Since the h_i then also generate S_K^G, by Lemma 4.6 we can change the order of the h_i in such a way that $\deg(h_i) = \deg(f_i)$ for each i. Let g_i be the class of h_i in S_F^G. Using Lemma 4.3 we get $\deg(g_1) \cdots \deg(g_n) = \deg(h_1) \cdots \deg(h_n) = |G|$. By Lemma 4.1 the g_i are algebraically independent over F, so $S_F^G = F[g_1, \dots, g_n]$ by Lemma 4.3; note that G acts faithfully on F^n by assumption. By construction we have $\deg(g_i) = \deg(h_i) = \deg(f_i)$, so (i) follows. □

Example 4.8. We can now also understand better what happens in Example 3.10. There we have the base ring $R = \mathbb{Z}_{(3)}$ which is a discrete valuation ring with quotient field $K = \mathbb{Q}$ and residue field $F = \mathbb{F}_3$. As we have seen, although the rings of invariants over

K and F are both polynomial rings, their generators do not have the same degrees, so statement (i) of Theorem 4.7 is not satisfied, but the action of G on F^2 is faithful. So Theorem 4.7 shows that indeed the ring of invariants over R cannot be a polynomial ring. By looking at the proof of Proposition 4.4 we see that really the reason for this is that the classes in $F[x,y]$ of f_1 and f_2 as defined in Example 3.10 are not algebraically independent. Indeed, $\overline{f_1} = g_1^2$ and $\overline{f_2} = 2g_1^3$.

4.2 A characterization of regular graded algebras

As mentioned at the beginning of this chapter, every finitely generated regular graded algebra over a field is isomorphic to a polynomial ring. This is not true anymore for graded algebras over Dedekind domains; in order to give a counterexample, the following definition is useful.

Definition 4.9. *Let R be a ring and let $I \subseteq R$ be a nonzero ideal. The blowup algebra of I in R is the graded algebra*

$$B_I R := \bigoplus_{d \in \mathbb{N}_0} I^d.$$

If I is a principal ideal, then $B_I R \cong R[x]$. Now let R be a Dedekind domain which is not a principal ideal domain and let $(0) \neq I \subseteq R$ be an ideal; Lemma 4.14c) below shows that the blowup algebra $B_I R$ is always regular; however, if I is not a principal ideal, then $B_I R$ is not isomorphic to a polynomial ring, so we have the desired counterexample. The main goal of this section is to prove that this is essentially the only kind of counterexample that can occur; more precisely, we prove the following:

Theorem 4.10. *Let R be a Dedekind domain and let S be a finitely generated regular graded R-algebra. Then there exist nonzero ideals $I_1, \dots, I_n \subseteq R$ such that*

$$S \cong B_{I_1} R \otimes_R \cdots \otimes_R B_{I_n} R$$

where $n = \dim S - \dim R$.

In the case where R is a principal ideal domain this theorem immediately implies the following:

Corollary 4.11. *Let R be a principal ideal domain and let S be a finitely generated regular graded R-algebra. Then S is isomorphic to a polynomial ring over R.*

In general, a necessary condition for a graded algebra $S = \bigoplus_{d \in \mathbb{N}_0} S_d$ to be isomorphic to a polynomial ring is that S_d is a free R-module for each d. The next theorem shows that this is also sufficient.

Theorem 4.12. *Let R be a Dedekind domain and let $S = \bigoplus_{d \in \mathbb{N}_0} S_d$ be a finitely generated regular graded R-algebra. Then S is isomorphic to a polynomial ring over R if and only if S_d is a free R-module for every $d \in \mathbb{N}_0$.*

The remainder of this section is devoted to the proof of Theorems 4.10 and 4.12. In order to simplify the notation, we make the following definition:

Definition 4.13. *Let R be a ring and let $I_1, \dots, I_n$ be nonzero ideals in R. Then we write*

$$B_{I_1,\dots,I_n}R := B_{I_1}R \otimes_R \cdots \otimes_R B_{I_n}R.$$

Before we go on, we make some remarks on the algebras $B_{I_1,\dots,I_n}R$. If we choose an embedding $I_i \to R$ for each I_i, these give an embedding of $B_{I_1,\dots,I_n}R$ to the n-fold tensor product $R[x] \otimes_R \dots \otimes_R R[x]$ which is the same as the polynomial ring $R[x_1, \dots, x_n]$. So if I_i is generated by elements $a_{ij} \in R, j \in J_i$ for some index sets $J_1, \dots, J_n$, then we can identify $B_{I_1,\dots,I_n}R$ with the subalgebra of $R[x_1, \dots, x_n]$ generated by all the $a_{ij}x_i$. Now we choose natural numbers $d_1, \dots, d_n$ and turn $R[x_1, \dots, x_n]$ into a graded ring by setting $\deg(x_i) = d_i$. Then all the $a_{ij}x_i$ are homogeneous, so $B_{I_1,\dots,I_n}$ becomes a graded subalgebra; this is the same as the tensor product of the algebras $B_{I_i}R$ viewed as graded algebras with the grading given by $\det(a) = d_i$ for all $a \in I_i$. The proof of Theorem 4.10 will show that in this way we can define a grading on $B_{I_1,\dots,I_n}R$ such that the isomorphism in the theorem is homogeneous.

We first prove some basic properties of the algebras $B_{I_1,\dots,I_n}R$:

Lemma 4.14. *Let R be a ring and let $I_1, \dots, I_n \subseteq R$ be nonzero ideals.*
a) For a multiplicative subset $U \subset R$ we have $U^{-1}(B_{I_1,\dots,I_n}R) \cong B_{U^{-1}I_1,\dots,U^{-1}I_n}U^{-1}R$.
b) If $I_1, \dots, I_n$ are principal ideals, then $B_{I_1,\dots,I_n}R \cong R[x_1, \dots, x_n]$.
c) If R is a Dedekind domain, then $B_{I_1,\dots,I_n}R$ is regular.

Proof. For $i = 1, \dots, n$ we have

$$U^{-1}B_{I_i}R = U^{-1}\left(\bigoplus_{d\in\mathbb{N}_0} I_i^d\right) \cong \bigoplus_{d\in\mathbb{N}_0} U^{-1}I_i^d = \bigoplus_{d\in\mathbb{N}_0} (U^{-1}I_i)^d = B_{U^{-1}I_i}U^{-1}R.$$

From this we obtain

$$\begin{aligned} U^{-1}(B_{I_1,\dots,I_n}R) &= U^{-1}\left(B_{I_1}R \otimes_R \dots \otimes_R B_{I_n}R\right) \\ &\cong (U^{-1}B_{I_1}R) \otimes_{U^{-1}R} \dots \otimes_{U^{-1}R} (U^{-1}B_{I_n}R) \\ &\cong (B_{U^{-1}I_1}U^{-1}R) \otimes_{U^{-1}R} \dots \otimes_{U^{-1}R} (B_{U^{-1}I_n}U^{-1}R) \\ &= B_{U^{-1}I_1,\dots,U^{-1}I_n}U^{-1}R. \end{aligned}$$

This proves part *a)* and *b)* is clear. For part *c)*, by Proposition 2.34 we need to show that for every maximal ideal $\mathfrak{p} \subset R$ the ring $(R\backslash\mathfrak{p})^{-1}B_{I_1,\dots,I_n}R$ is regular. We set $U := R\backslash\mathfrak{p}$. Then $U^{-1}R = R_\mathfrak{p}$ is a discrete valuation ring, so each $U^{-1}I_i$ is a principal ideal. Hence by *a)* and *b)* $U^{-1}B_{I_1,\dots,I_n}R \cong R_\mathfrak{p}[x_1, \dots, x_n]$ and this ring is regular because R is regular. □

In Theorems 4.10 and 4.12 we did not assume that S is an integral domain. We need this generality, although the invariant rings we are interested in are always integral

domains, because our proof of the main theorems is by induction on $\dim S$ and it is not obvious that the rings we consider remain integral domains after the induction step. On the other hand, the algebras $B_{I_1,\dots,I_n}R$ are always integral domains, so the first main step in our proof is the following lemma.

Lemma 4.15. *Let R and S be as in Theorem 4.10. Then S is an integral domain.*

Proof. We first show that S is torsion-free as an R-module. So let $f \in S\backslash\{0\}$ and $I_f := \{a \in R | af = 0\}$; we want to show that $I_f = \{0\}$. We may assume that f is homogeneous. I_f is a proper ideal in R, so there is a maximal ideal $\mathfrak{n}_f \subset R$ with $I_f \subseteq \mathfrak{n}_f$. We define $\mathfrak{m}_f := (\mathfrak{n}_f, S_+)_S$; by Lemma 2.29 this is a maximal ideal in S. The localization $S_{\mathfrak{m}_f}$ is a regular local ring and hence an integral domain; let ε denote the canonical map $S \to S_{\mathfrak{m}_f}$. For $a \in I_f$ we have $\varepsilon(a) \cdot \varepsilon(f) = 0$ and hence either $\varepsilon(a) = 0$ or $\varepsilon(f) = 0$. So there exists $c \in R\backslash\mathfrak{m}_f$ such that $c \cdot a = 0$ or $c \cdot f = 0$; let c_0 denote the degree-0-part of c. We have $c_0 \cdot a = 0$ or $c_0 \cdot f = 0$ because a and f are homogeneous. Since $c \notin S_+ \subseteq \mathfrak{m}_f$, we have $c_0 \neq 0$. But R is an integral domain, so $c_0 \cdot a = 0$ implies $a = 0$ as desired. It remains to show that the case $c_0 \cdot f = 0$ cannot occur. Indeed this would imply $c_0 \in I_f \subseteq \mathfrak{m}_f$ and since $c - c_0 \in S_+ \subseteq \mathfrak{m}_f$ we would obtain $c \in \mathfrak{m}_f$, a contradiction. So we have shown that $I_f = \{0\}$ for every f and hence S is a torsion-free R-module.

Now we prove that S is indeed an integral domain. So assume we have $s, t \in S\backslash\{0\}$ such that $s \cdot t = 0$. S_+ is a prime ideal in S and since S is regular, the localization S_{S_+} is a regular local ring and hence an integral domain; let η denote the canonical map $S \to S_{S_+}$, so we have $\eta(s) \cdot \eta(t) = 0$ and hence either $\eta(s) = 0$ or $\eta(t) = 0$. Without loss of generality, we assume $\eta(s) = 0$; then there is a $u \in S\backslash S_+$ such that $u \cdot s = 0$. We write $s = \sum_{m \in \mathbb{N}_0} s_m$ with $s_m \in S_m$ for every m. Let $d \in \mathbb{N}_0$ be minimal such that $s_d \neq 0$ and let u_0 be the degree-0-part of u; since $u \notin S_+$ we have $u_0 \neq 0$. The degree-d-part of $u \cdot s$ is $u_0 \cdot s_d$ and this is zero since $u \cdot s = 0$. But we already proved that S is torsion-free as an $R = S_0$-module and hence $u_0 \neq 0$ implies $s_d = 0$, a contradiction. □

Using this we can prove a simple special case of Theorem 4.10 which will later serve as the starting point for our proof by induction.

Lemma 4.16. *Let R and S be as in Theorem 4.10 and assume that* $\dim(S) = \dim(R)$. *Then $S = S_0 = R$.*

Proof. We have $\mathrm{ht}(S_+) \leq \dim(S) - \dim(S/S_+) = \dim(S) - \dim(R) = 0$ and, since S is an integral domain by Lemma 4.15, this implies $S_+ = (0)$, so $S = S_0$ as claimed. □

The next step is the computation of the Krull dimension of the algebras $B_{I_1,\dots,I_n}R$:

Lemma 4.17. *Let R be a Dedekind domain and let $I_1, \dots, I_n$ be nonzero ideals in R. Then*

$$\dim(B_{I_1,\dots,I_n}R) = n + \dim R.$$

In the special case of a polynomial ring over R this is a well-known result. Our proof here is a direct generalization of this standard proof; it uses the concept of a fiber ring. Recall that for a ring homomorphism $\varphi : S \to T$ and a prime ideal $\mathfrak{p} \subset S$ the fiber ring of $\mathfrak{p}$ is the ring $\kappa(\mathfrak{p}) \otimes_S T$ where $\kappa(\mathfrak{p}) := \mathrm{Quot}(S/\mathfrak{p})$. If S and T are Noetherian and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ for some prime ideal $\mathfrak{q} \subset T$, then $\dim(\kappa(\mathfrak{p}) \otimes_S T) \geq \mathrm{ht}(\mathfrak{q}) - \mathrm{ht}(\mathfrak{p})$ (see Kemper [35, Theorem 7.12]).

Proof. Let $P \subset R$ be a prime ideal with $\mathrm{ht}(P) = \dim(R)$. Then using Lemma 4.14 and the fact that R_P is a principal ideal domain we obtain

$$\dim(B_{I_1,\ldots,I_n}R) \geq \dim((R\backslash P)^{-1}B_{I_1,\ldots,I_n}R) = \dim(R_P[x_1,\ldots,x_n]) = n + \dim R$$

In order to prove the reverse inequality we use induction on n. The case $n = 0$ is clear, so we assume $n > 0$ and define $S := B_{I_1,\ldots,I_{n-1}}R$, $T := B_{I_1,\ldots,I_n}R$, and $\varphi : S \to T = S \otimes_R B_{I_n}R, f \mapsto f \otimes 1$. By induction we have $\dim(S) \leq n - 1 + \dim(R)$ and we want to show $\dim(T) \leq n + \dim(R)$. Let $\mathfrak{q} \subset T$ be a prime ideal and $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$; the claim follows if we prove that $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p}) + 1$. We prove this inequality using the fiber ring $\kappa(\mathfrak{p}) \otimes_S T$. We have

$$\begin{aligned}\kappa(\mathfrak{p}) \otimes_S T &= \kappa(\mathfrak{p}) \otimes_S (S \otimes_R B_{I_n}R) \\ &\cong \kappa(\mathfrak{p}) \otimes_R B_{I_n}R \cong \bigoplus_{d\in\mathbb{N}_0} (\kappa(\mathfrak{p}) \otimes_R I_n^d).\end{aligned}$$

As an algebra over $\kappa(\mathfrak{p})$, this is generated by $\kappa(\mathfrak{p}) \otimes_R I_n$ which is isomorphic to a subvectorspace of $\kappa(\mathfrak{p}) \otimes_R R \cong \kappa(\mathfrak{p})$. Hence $\kappa(\mathfrak{p}) \otimes_S T$ is generated by one element as an $\kappa(\mathfrak{p})$-algebra, so its dimension is indeed at most one. The claim follows using the formula for fiber dimension mentioned before this proof. □

The central part of the proof of Theorems 4.10 and 4.12 is now the following lemma, which may seem rather technical at first glance.

Lemma 4.18. *Let R be a Dedekind domain and let S be a finitely generated regular graded R-algebra such that $S_0 \neq S$. Let $d \in \mathbb{N}_{>0}$ be minimal such that $S_d \neq \{0\}$. Using Theorem 2.28 we can write $S_d = I \oplus M$ where I is isomorphic to some ideal $(0) \neq I \subseteq R$ and M is a free R-module; set $J := (I)_S$. Then the following holds:*
a) $T := S/J$ is again a regular ring.
b) If S_i is a free R-module for each $i \in \mathbb{N}_0$, then also T_i is a free R-module for each i.
c) If $T \cong B_{I_1,\ldots,I_n}R$, then $S \cong B_{I_1,\ldots,I_n,I}R$.

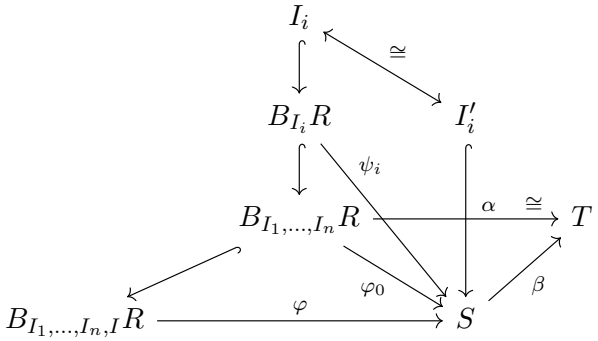
Proof.
a) By Proposition 2.34 it is sufficient to show that $T_\mathfrak{n}$ is regular for every homogeneous maximal ideal $\mathfrak{n} \subset T$, so fix such an ideal $\mathfrak{n}$. By Lemma 2.29 $\mathfrak{n} = (\mathfrak{p}, T_+)_T$ for some maximal ideal $\mathfrak{p} \subset R$. Let $\mathfrak{m} := (\mathfrak{p}, S_+)_S$; then $\mathfrak{n} = \mathfrak{m}/J$ (note that $J \subseteq S_+ \subseteq \mathfrak{m}$). Hence we have $T_\mathfrak{n} \cong S_\mathfrak{m}/J_\mathfrak{m}$ and $S_\mathfrak{m}$ is regular. We prove that $J_\mathfrak{m}$ is a principal ideal generated by some element $g \in I$ such that $g \notin (\mathfrak{m}_\mathfrak{m})^2$. Then the regularity of $T_\mathfrak{n}$ follows, see Bruns and Herzog [11, Proposition 2.2.4].

Let $U_0 := R\backslash\mathfrak{p}$. Then $U_0^{-1}S$ is a graded ring with $(U_0^{-1}S)_0 \cong U_0^{-1}R = R_\mathfrak{p}$, which is a discrete valuation ring. We have $(U_0^{-1}S)_d = I_\mathfrak{p} \oplus M_\mathfrak{p}$, where $I_\mathfrak{p}$ is isomorphic to an ideal in $R_\mathfrak{p}$, hence a principal ideal. Let g be a generator of this ideal; we may choose g in such a way that $g \in I$. Then $U_0^{-1}J = (g)_{U_0^{-1}S}$ and since we can view $S_\mathfrak{m}$ as a localization of $U_0^{-1}S$, we find $J_\mathfrak{m} = (g)_{S_\mathfrak{m}}$.
It remains to prove that $g \notin (\mathfrak{m}_\mathfrak{m})^2$. Assume the contrary; then there is an $h \in S\backslash\mathfrak{m}$ such that $gh \in \mathfrak{m}^2$. We write $h = \sum_{i\in\mathbb{N}_0} h_i$ with $h_i \in S_i$; since $S_+ \subseteq \mathfrak{m}$ we have $h_0 \notin \mathfrak{p}$, in particular $h_0 \neq 0$. Since gh_0 is the degree-d-part of gh and $\mathfrak{m}^2$ is a homogeneous ideal, we have $gh_0 \in \mathfrak{m}^2$, so $gh_0 = \sum_j \gamma_j\delta_j$ for certain $\gamma_j, \delta_j \in \mathfrak{m}$. We may assume that all γ_j, δ_j are homogeneous and $\deg(\gamma_j\delta_j) = d$ for each j. By the choice of d we may assume without loss of generality that $\deg(\gamma_j) = 0$ and $\deg(\delta_j) = d$ for every j. So $\delta_j \in S_d = I \oplus M$ and we can write $\delta_j = \lambda_j + \mu_j$ with $\lambda_j \in I, \mu_j \in M$. So we have $gh_0 = \sum_j \gamma_j\lambda_j + \sum_j \gamma_j\mu_j$. Since $h_0 \in R$ and $g \in I$, we have $gh_0 \in I$ and hence $gh_0 = \sum_j \gamma_j\lambda_j$. By our choice of g and the fact that $\lambda_j \in I$ there are $\eta_j \in R_\mathfrak{p}$ such that $\lambda_j = \eta_j g$. We thus have $gh_0 = g \cdot \left(\sum_j \gamma_j\eta_j\right)$ and hence $h_0 = \sum_j \gamma_j\eta_j$ since S is an integral domain by Lemma 4.15. There are elements $\theta_j \in R, \omega \in R\backslash\mathfrak{p}$ such that $\eta_j = \frac{\theta_j}{\omega}$ for each j. We obtain $h_0\omega = \sum_j \gamma_j\theta_j$, a contradiction: the left hand side is not an element of $\mathfrak{p}$, but the right hand side is an element of $R \cap \mathfrak{m} = \mathfrak{p}$ since $\gamma_j \in \mathfrak{p}$ for each j.

b) Since S_d is free, $I \cong R$ by Theorem 2.28b), so $J_i \cong S_{i-d}$ for all $i \geq d$. If $T_i = \{0\}$, then there is nothing to show, so assume $T_i \neq \{0\}$; in particular $i \geq d$. By part *a)* and Lemma 4.15 T is an integral domain and hence T_i is torsion-free. So by Theorem 2.28b) we have $T_i \cong R^l \oplus I'$ for some $l \geq 0$ and some nonzero ideal $I' \subseteq R$. The canonical projection $S \to T$ restricts to a surjective homomorphism of R-modules $S_i \to T_i$ with kernel J_i. Since T_i is a projective R-module by Theorem 2.28a) we obtain $S_i \cong T_i \oplus J_i \cong R^l \oplus I' \oplus S_{i-d}$. Since S_i and S_{i-d} are free by assumption, I' is a principal ideal by Theorem 2.28b) and hence $T_i \cong R^l \oplus I'$ is a free R-module.

c) Let $\alpha : B_{I_1,\ldots,I_n}R \to T$ be an isomorphism and let $\beta : S \to T$ be the canonical projection map; then β is a homogeneous homomorphism of R-modules. By part *a)* and Lemma 4.15 T is an integral domain; hence each T_i is a projective R-module by Theorem 2.28a). Thus there is an injective homogeneous homomorphism of R-modules $\beta' : T \to S$ with $\beta \circ \beta' = \mathrm{id}$. We can view each $B_{I_i}R$ as a subalgebra of $B_{I_1,\ldots,I_n}R$, so we can also view $I_i \subset B_{I_i}R$ as an R-submodule of $B_{I_1,\ldots,I_n}R$. We define $I_i' := \beta'(\alpha(I_i)) \subseteq S$; since α and β' are injective, this is isomorphic to I_i and hence we can define a homomorphism of R-algebras $\psi_i : B_{I_i}R \to S$ such that for $a \in I_i \subseteq B_{I_i}R$ we have $\psi_i(a) = \beta'(\alpha(a))$ and hence $\beta(\psi_i(a)) = \alpha(a)$. Since I_i generates $B_{I_i}R$ as an R-algebra, we have $\beta \circ \psi_i = \alpha|_{B_{I_i}R}$. Since I is also an R-submodule of S we can similarly define a ring homomorphism $\psi_{n+1} : B_IR \to S$. We obtain ring homomorphisms $\varphi_0 := \psi_1 \otimes \ldots \otimes \psi_n : B_{I_1,\ldots,I_n}R \to S$ and $\varphi := \varphi_0 \otimes \psi_{n+1} : B_{I_1,\ldots,I_n,I}R \to S$. Since we have $\beta \circ \psi_i = \alpha|_{B_{I_i}R}$, we obtain $\beta \circ \varphi_0 = \alpha$.
It remains to prove that φ is an isomorphism. We first prove that it is surjective. So let $t \in S$ be homogeneous; we use induction on $\deg(t)$ to prove that $t \in \mathrm{im}\varphi$. The case

$\deg t = 0$ is clear, so we assume $\deg t > 0$ and define $s := \varphi_0(\alpha^{-1}(\beta(t))) \in \mathrm{im}\varphi_0 \subseteq \mathrm{im}\varphi$. Since $\beta \circ \varphi_0 = \alpha$, we have $\beta(s) = \beta(t)$ and thus $s - t \in \ker\beta = J$. Since J is generated by $I \subseteq S_d$ we find elements $a_j \in S, r_j \in I$ such that $s - t = \sum_j a_j r_j$ and $\deg a_j = \deg t - d$ for each j. Then for each j we have $a_j \in \mathrm{im}\varphi$ by induction and $r_j \in \mathrm{im}\psi_{n+1} \subseteq \mathrm{im}\varphi$. So $t = s + \sum_j a_j r_j \in \mathrm{im}\varphi$ and hence φ is indeed surjective. Therefore $\mathrm{ht}(\ker\varphi) = 0$ since $\dim S \geq \dim T + 1 = n + \dim R + 1 = \dim(B_{I_1,\ldots,I_n,I}R)$ by Lemma 4.17. But $B_{I_1,\ldots,I_n,I}R$ is an integral domain by Lemma 4.14c) and Lemma 4.15, so $\ker\varphi = \{0\}$ and hence φ is injective.



□

Now we have everything that we need for the proof of the main theorems.

Proof of Theorem 4.10. We use induction on $\delta := \dim(S) - \dim(R)$; $\delta \geq 0$ since $R \cong S/S_+$. If $\delta = 0$, then the theorem follows from Lemma 4.16. So assume that $\delta > 0$. Then $R \subsetneq S$; let d, I, and T be as in Lemma 4.18. Since S is an integral domain by Lemma 4.15, we have $\dim(T) < \dim(S)$ and T is regular by Lemma 4.18a), so we can apply induction and obtain $T \cong B_{I_1,\ldots,I_n}R$ for nonzero ideals $I_1, \ldots, I_n \subseteq R$. Now the theorem follows from Lemma 4.18c). □

Proof of Theorem 4.12. It is clear that $S \cong R[x_1, \ldots, x_n]$ implies that each S_i is free. For the converse we again use induction on $\delta := \dim(S) - \dim(R)$. If $\delta = 0$ then the result follows from Lemma 4.16. So assume that $\delta > 0$ and let d, I, and T be as in Lemma 4.18. Since S_d is free, I is principal by Theorem 2.28b). We have $\dim(T) < \dim(S)$, T is regular and each T_i is free by Lemma 4.18b), so we can apply induction and obtain $T \cong R[x_1, \ldots, x_n] \cong B_{I_1,\ldots,I_n}R$ with $I_1 = \ldots = I_n = (1)$. Hence by Lemma 4.18c) and Lemma 4.14b) we obtain $S \cong B_{I_1,\ldots,I_n,I}R \cong R[x_1, \ldots, x_{n+1}]$. □

4.3 Invariants of pseudoreflection groups over Dedekind domains

In this section we analyze rings of invariants of pseudoreflection groups over Dedekind domains. The first step is the following proposition which shows that the question of

whether such a ring of invariants is regular can be reduced to the case of pseudoreflection groups over discrete valuation rings which we discussed in Section 4.1.

Proposition 4.19. *Let R be a Dedekind domain and let $G \subseteq Gl_n(R)$ be a finite group. Then the following statements are equivalent:*

(i) $R[x_1, \ldots, x_n]^G$ *is regular.*

(ii) For every maximal ideal $\mathfrak{p} \subset R$ the ring $R_\mathfrak{p}[x_1, \ldots, x_n]^G$ is regular.

(iii) For every maximal ideal $\mathfrak{p} \subset R$ the ring $R_\mathfrak{p}[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring.

Proof. The equivalence of (i) and (ii) follows from Proposition 2.34. Since polynomial rings over regular rings are regular ([11, Theorem 2.2.13]), (iii) implies (ii). The implication $(ii) \implies (iii)$ follows from Corollary 4.11 and the fact that each $R_\mathfrak{p}$ is a discrete valuation ring. □

The easiest case in which this result can be applied is if the group order is invertible in the base ring.

Theorem 4.20. *Let R be a Dedekind domain and let $G \subseteq Gl_n(R)$ be a finite pseudoreflection group such that $|G| \in R^\times$. Then $R[x_1, \ldots, x_n]^G$ is regular.*

Proof. Let $\mathfrak{p} \subset R$ be a maximal ideal. Then $|G| \in R_\mathfrak{p}^\times$ and hence $R_\mathfrak{p}[x_1, \ldots, x_n]^G$ is a polynomial ring over $R_\mathfrak{p}$ by Corollary 4.5. Now the theorem follows from Proposition 4.19. □

Using the theory developed in Section 4.2, we can now prove results concerning the question of whether a ring of arithmetic invariants is a polynomial ring. The following result is basically a direct arithmetic analogue of the Chevalley-Shepard-Todd theorem.

Corollary 4.21. *Let R be a principal ideal domain and let $G \subseteq Gl_n(R)$ be a finite pseudoreflection group such that $|G| \in R^\times$. Then $R[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring over R.*

Proof. This follows immediately from Theorem 4.20 and Corollary 4.11. □

The most general result I managed to obtain for regularity of rings of arithmetic invariants is the following.

Theorem 4.22. *Let R be a Dedekind domain with $K := \mathrm{Quot}(R)$ and let $G \subseteq Gl_n(R)$ be a finite pseudoreflection group such that there are homogeneous invariants $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]^G$ with $K[x_1, \ldots, x_n]^G = K[f_1, \ldots, f_n]$. Then the following statements are equivalent:*

(i) For every maximal ideal $\mathfrak{p} \subset R$ with $|G| \in \mathfrak{p}$ there are homogeneous $g_1, \ldots, g_n \in (R/\mathfrak{p})[x_1, \ldots, x_n]^G$ such that $(R/\mathfrak{p})[x_1, \ldots, x_n]^G = (R/\mathfrak{p})[g_1, \ldots, g_n]$ and $\deg(g_i) = \deg(f_i)$ for each i.

(ii) $R[x_1, \ldots, x_n]^G$ is regular and G acts faithfully on $(R/\mathfrak{p})^n$ for every maximal ideal $\mathfrak{p} \subset R$ with $|G| \in \mathfrak{p}$.

(iii) *There are nonzero ideals* $I_1, \dots, I_n \subseteq R$ *such that* $R[x_1, \dots, x_n]^G \cong B_{I_1,\dots,I_n} R$ *and* G *acts faithfully on* $(R/\mathfrak{p})^n$ *for every maximal ideal* $\mathfrak{p} \subset R$ *with* $|G| \in \mathfrak{p}$.

If R *is a principal ideal domain, then these statements are also equivalent to the following:*

(iv) $R[x_1, \dots, x_n]^G$ *is isomorphic to a polynomial ring over* R *and* G *acts faithfully on* $(R/\mathfrak{p})^n$ *for every maximal ideal* $\mathfrak{p} \subset R$ *with* $|G| \in \mathfrak{p}$.

Proof. We begin with the proof that (i) implies (ii). By Proposition 4.19 we only need to show that $R_\mathfrak{p}[x_1, \dots, x_n]^G$ is isomorphic to a polynomial ring over $R_\mathfrak{p}$ for every maximal ideal $\mathfrak{p} \subset R$ and that if $|G| \in \mathfrak{p}$, then G acts faithfully on $(R/\mathfrak{p})^n$. If $|G| \in \mathfrak{p}$, both properties follow from (i) and Theorem 4.7. If $|G| \notin \mathfrak{p}$, then $|G| \in R_\mathfrak{p}^\times$ and hence $R_\mathfrak{p}[x_1, \dots, x_n]^G$ is isomorphic to a polynomial ring by Corollary 4.5. The converse implication $(ii) \implies (i)$ follows directly from Theorem 4.7 and Proposition 2.34.

The implication $(ii) \implies (iii)$ follows from Theorem 4.10 and $(iii) \implies (ii)$ follows from Lemma 4.14c).

Now we assume that R is a principal ideal domain. Then $(iii) \implies (iv)$ follows from Lemma 4.14b) and $(iv) \implies (iii)$ is clear. □

Since I do not know any example of a pseudoreflection group over a Dedekind domain where the ring of invariants is an algebra of the form $B_{I_1,\dots,I_n} R$ where not all the ideals $I_1, \dots, I_n$ are principal, I make the following conjecture.

Conjecture 4.23. *Let* R *be a Dedekind domain and let* $G \subseteq Gl_n(R)$ *be a finite pseudoreflection group such that* $R[x_1, \dots, x_n]^G$ *is regular. Then* $R[x_1, \dots, x_n]^G$ *is isomorphic to a polynomial ring over* R.

We end this chapter with a result which relates invariants over a Dedekind domain R to invariants over residue fields $R/\mathfrak{p}$ in the case that $|G|$ is invertible in R.

Proposition 4.24. *Let* R *be a Dedekind domain and let* $G \subseteq Gl_n(R)$ *be a finite group. If* $R[x_1, \dots, x_n]^G$ *is regular, then for every maximal ideal* $\mathfrak{p} \subset R$ *with* $|G| \notin \mathfrak{p}$ *the ring of invariants* $(R/\mathfrak{p})[x_1, \dots, x_n]^G$ *is isomorphic to a polynomial ring over* $R/\mathfrak{p}$.

Proof. Since $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ and $R_\mathfrak{p}[x_1, \dots, x_n]^G$ is again regular by Proposition 4.19 we may replace R by $R_\mathfrak{p}$ and hence assume that $|G| \in R^\times$. Let $K := \mathrm{Quot}(R)$; then $K[x_1, \dots, x_n]^G$ is also regular and hence a polynomial ring. So G is a pseudoreflection group in $Gl_n(R)$ by Theorem 2.17. Let $\sigma \in G$ be a pseudoreflection; the image of σ in $Gl_n(R/\mathfrak{p})$ is either again a pseudoreflection or the identity, so G acts as a pseudoreflection group on $(R/\mathfrak{p})^n$. Since $|G| \notin \mathfrak{p}$ we get that $|G|$ is invertible in $R/\mathfrak{p}$. But $R/\mathfrak{p}$ is a field and hence $(R/\mathfrak{p})[x_1, \dots, x_n]^G$ is isomorphic to a polynomial ring by Theorem 2.17. □

5 Reflexive modules, divisors, and Picard groups

In this chapter we introduce several related concepts from commutative algebra which we will need in the next two chapters. None of the material in this chapter is new; the main references are the books by Fossum [20] and Benson [4, Chapter 3]. We begin in Section 5.1 with reflexive modules and the reflexive closure of modules. In Sections 5.2 and 5.3 we introduce divisorial ideals and the divisor class group of a Noetherian normal domain which will be the main tool in Chapter 6 to determine when a ring of invariants is factorial. Finally, in Section 5.4 we define the Picard group of a Noetherian ring, a concept closely related to the divisor class group.

5.1 Reflexive modules

In this section, we fix a Noetherian normal domain A and a finitely generated torsion-free A-module M. For the definition of reflexive modules we need the dual module $M^* := \mathrm{Hom}_A(M, A)$. For our purposes a slightly different description is more useful: we define $K := \mathrm{Quot}(A)$ and $V := M \otimes_A K$; note that the canonical map $M \to V$ is injective since we assumed M to be torsion-free. Then we have $M^* \cong \{f \in \mathrm{Hom}_K(V, K) | f(M) \subseteq A\}$ where $\mathrm{Hom}_K(V, K)$ is of course just the dual vectorspace V^*. For the definition of reflexive modules we need the dual of the dual, the module M^{**}. By the above, we view this as a subset of V^{**} and since M is finitely generated, we can identify V^{**} with V. Hence we can view M^{**} as an A-submodule of V which contains M. Now we can make the following definition.

Definition 5.1. *Let $K := \mathrm{Quot}(A)$ and $V := M \otimes_A K$.*
a) The module $\overline{M} := M^{**}$, viewed as a subset of V, is called the reflexive closure of M.
b) M is called reflexive if $\overline{M} = M$.

So M is reflexive if and only if every homomorphism of A-modules $M^* \to A$ is of the form $\varphi \mapsto \varphi(m)$ for some $m \in M$. We have the following explicit characterization of the reflexive closure, which shows the advantage of viewing M^{**} as a subset of V. Recall from Chapter 2 that $X^{(1)}(A)$ denotes the set of all prime ideals of height one in A.

Lemma 5.2. (Fossum [20, Proposition 5.2(c)]) *We have*

$$\overline{M} = \bigcap_{\mathfrak{p} \in X^{(1)}(A)} M_{\mathfrak{p}} \subseteq V.$$

This lemma immediately implies the following:

Lemma 5.3. *Let M, N be finitely generated torsion-free A-modules and let $\varphi : M \to N$ be a homomorphism of A-modules. Then $\varphi_K(\overline{M}) \subseteq \overline{N}$, where $\varphi_K := \varphi \otimes \mathrm{id} : M \otimes_A K \to N \otimes_A K$.*

The next lemma provides some basic examples of reflexive modules:

Lemma 5.4.
a) Every finitely generated free module is reflexive.
b) For every finitely generated torsion-free module M and for every reflexive module N, the module $\mathrm{Hom}_A(M, N)$ is again reflexive; in particular, the dual module M^* is reflexive.

Proof. Part *a)* is clear, for *b)* we refer to [20, Proposition 2.6]. □

Furthermore, we have the following criterion for reflexivity, see Bourbaki [5, Chapter VII, §4.8, Proposition 19].

Lemma 5.5. *Let $A \subseteq B$ be a finite extension of Noetherian normal domains, i.e. B is finitely generated as an A-module, and let M be a finitely generated torsion-free B-module. Then the reflexive closure of M as an A-module equals the reflexive closure of M as a B-module. In particular, M is reflexive as an A-module if and only if it is reflexive as a B-module.*

5.2 Divisorial ideals and divisors

In this section we collect some results on divisorial ideals. We mainly follow the book by Fossum [20], see also Benson [4, Chapter 3]. In this section A always stands for a Noetherian normal domain.

Definition 5.6. *A fractional ideal $\mathfrak{a}$ of A is called divisorial if it is reflexive as an A-module. The set of all divisorial fractional ideals is written as $D(A)$.*

Remark 5.7. For a fractional ideal $\mathfrak{a}$ we have $\mathfrak{a}^* \cong \mathfrak{a}^{-1}$ and $\overline{\mathfrak{a}} = (\mathfrak{a}^{-1})^{-1}$. In particular, $\mathfrak{a}^{-1}$ is divisorial by Lemma 5.4b).

It can be proved (see [20, §3]) that $D(A)$ becomes an abelian group with the multiplication defined by $(\mathfrak{a}, \mathfrak{b}) \mapsto \overline{\mathfrak{ab}}$. Next we define a second abelian group associated to A.

Definition 5.8. *The group of divisors is the free abelian group generated by $X^{(1)}(A)$; it is written as* $\mathrm{Div}(A)$.

Our next goal is to relate the two groups $D(A)$ and $\mathrm{Div}(A)$. First we note that for $\mathfrak{p} \in X^{(1)}(A)$ the localization $A_\mathfrak{p}$ is a discrete valuation ring because A is normal; let $v_\mathfrak{p} : \mathrm{Quot}(A) \to \mathbb{Z}$ denote the corresponding discrete valuation. For a fractional ideal $\mathfrak{a}$ of A, we define $v_\mathfrak{p}(\mathfrak{a}) := \inf\{v_\mathfrak{p}(a) | a \in \mathfrak{a}\}$. Then it can be proved that $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ and that

for a fixed fractional ideal $\mathfrak{a}$ the value $v_{\mathfrak{p}}(\mathfrak{a})$ is nonzero for only finitely many $\mathfrak{p} \in X^{(1)}(A)$ (see [20, §5]). Thus we can define the divisor

$$\operatorname{div}(\mathfrak{a}) \coloneqq \sum_{\mathfrak{p} \in X^{(1)}(A)} v_{\mathfrak{p}}(\mathfrak{a})\mathfrak{p} \in \operatorname{Div}(A).$$

Proposition 5.9. ([20, Proposition 5.9]) *The map*

$$\operatorname{div} : D(A) \to \operatorname{Div}(A), \mathfrak{a} \mapsto \operatorname{div}(\mathfrak{a})$$

is an isomorphism of abelian groups.

Proposition 5.9 is equivalent to saying that every divisorial fractional ideal can be written uniquely as $\overline{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}}$ with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in X^{(1)}(A)$ and $e_1, \ldots, e_r \in \mathbb{Z}$. We end this section with an important class of examples of divisorial ideals.

Definition 5.10. *Let R be a Noetherian ring, let S be a finitely generated R-algebra which is a normal domain, and let $G \subseteq \operatorname{Aut}_R(S)$ be a finite group. Furthermore, let χ be an R-valued character of G, that is, a group homomorphism $G \to R^\times$. Then we define the module of semi-invariants as*

$$S_\chi^G := \{f \in S | \forall \sigma \in G : \sigma(f) = \chi(\sigma)f\}.$$

This is an S^G-module.

Lemma 5.11. (Nakajima [45, Lemma 2.1]) *Let R, S, G, and χ be as in the definition. Then S_χ^G is isomorphic to a divisorial fractional ideal of S^G.*

Note that S^G is again a finitely generated R-algebra and thus Noetherian by Theorem 2.2 and that it is normal by Theorem 2.5, so it makes sense to talk about divisorial ideals in S^G.

5.3 Divisor class groups

Let A be a Noetherian normal domain. The group of divisors $\operatorname{Div}(A)$ can be used to define the divisor class group of A, an important tool to check whether a ring is factorial. The main reference for this section is again Fossum [20].

Definition 5.12. *A divisor in* $\operatorname{Div}(A)$ *is called principal if it is of the form* $\operatorname{div}(\mathfrak{a})$ *for a principal fractional ideal $\mathfrak{a} \in D(A)$. The principal divisors form a subgroup of* $\operatorname{Div}(A)$*, written as* $\operatorname{Prin}(A)$*. Now we define the divisor class group of A as*

$$\operatorname{Cl}(A) := \operatorname{Div}(A)/\operatorname{Prin}(A).$$

Example 5.13. Let A be a Dedekind domain. Then every fractional ideal is divisorial ([20, Theorem 13.1]), so the divisor class group of A is just its ideal class group. Therefore it is justified that we use the same notation for the divisor class group and the ideal class group.

The main reason why we are interested in divisor class groups is the following theorem:

Theorem 5.14. ([20, Proposition 6.1]) *Let A be a Noetherian normal domain. Then A is factorial if and only if* $\mathrm{Cl}(A) = \{0\}$.

From now on let B be a second Noetherian normal domain. Unfortunately, it is not possible to attach to an arbitrary ring homomorphism $A \to B$ a homomorphism of divisor class groups $\mathrm{Cl}(A) \to \mathrm{Cl}(B)$. A quite general setting in which this is possible has been described by Sather-Wagstaff and Spiroff [51], see also Remark 5.21. For us it is sufficient to develop this theory for a certain class of injective ring homomorphisms for which it is quite elementary. So in the following we shall always assume that A is a subring of B; the inclusion $i : A \to B$ then induces a group homomorphism

$$\mathrm{Div}(i) : \mathrm{Div}(A) \to \mathrm{Div}(B), \mathfrak{p} \mapsto \sum_{\substack{\mathfrak{P} \in X^{(1)}(B), \\ \mathfrak{P} \cap A = \mathfrak{p}}} e(\mathfrak{P}, \mathfrak{p})\mathfrak{P}.$$

Note that in Definition 2.7 we defined the ramification index only for finite ring extensions and in the situation here the extension $A \subseteq B$ need not be finite; however, we can use precisely the same definition to define $e(\mathfrak{P}, \mathfrak{p})$ for any extension of Noetherian normal domains $A \subseteq B$ with prime ideals $\mathfrak{p} \in X^{(1)}(A)$ and $\mathfrak{P} \in X^{(1)}(B)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$.

Definition 5.15. *We say that the inclusion $i : A \to B$ satisfies condition (PDE)*[1] *if for every $\mathfrak{P} \in X^{(1)}(B)$ we have* $\mathrm{ht}(\mathfrak{P} \cap A) \leq 1$.

Now the map $\mathrm{Div}(i) : \mathrm{Div}(A) \to \mathrm{Div}(B)$ induces a homomorphism $\mathrm{Cl}(A) \to \mathrm{Cl}(B)$ if and only if the inclusion $A \to B$ satisfies condition (PDE) (see [20, §6]). There are several classes of inclusions of rings for which condition (PDE) is always satisfied. In the next three propositions we study some of these situations; we begin with the case that B is a localization of A.

Proposition 5.16. ([20, Corollary 7.2]) *If $B = U^{-1}A$ for some multiplicatively closed subset $U \subseteq A \backslash \{0\}$, then the inclusion $A \hookrightarrow B$ satisfies (PDE), the induced homomorphism* $\mathrm{Cl}(A) \to \mathrm{Cl}(B)$ *is surjective, and its kernel is generated by the classes of all prime ideals $\mathfrak{p} \in X^{(1)}(A)$ for which $\mathfrak{p} \cap U \neq \emptyset$.*

The second case we consider is that B is a polynomial ring over A:

Proposition 5.17. ([20, Proposition 8.8]) *If B is the polynomial ring $A[x_1, \ldots, x_n]$, then the inclusion $A \hookrightarrow B$ satisfies (PDE) and the induced homomorphism* $\mathrm{Cl}(A) \to \mathrm{Cl}(B)$ *is an isomorphism.*

Finally, we study the situation that A is the ring of invariants of a finite group of automorphisms of B.

[1] This is the terminology used in Fossum's book - (PDE) is an abbreviation for the french "pas d'éclatement"; Samuel [50] calls this condition (NBU) for "no blowing up".

Proposition 5.18. ([20, Theorem 16.1]) *Let S be any Noetherian normal domain and let $G \subseteq \mathrm{Aut}(S)$ be a finite group such that S^G is again Noetherian. The inclusion $i : S^G \to S$ satisfies (PDE) and the kernel of the induced homomorphism $\varphi : \mathrm{Cl}(S^G) \to \mathrm{Cl}(S)$ can be embedded into the first cohomology group $H^1(G, S^\times)$.*

Remark 5.19. In the situation of Proposition 5.18 the assumption that S is Noetherian in general does not imply that S^G is also Noetherian, see Nagata [44]. However, if S is a finitely generated algebra over a Noetherian ring R and the elements of G are R-algebra automorphisms, then S^G is again a finitely generated R-algebra and hence Noetherian by Theorem 2.2. The assumption that S^G is Noetherian is needed in Proposition 5.18 because we defined the divisor class group only for Noetherian normal domains (S^G is normal by Theorem 2.5). Alternatively it would also be possible to define the divisor class group more generally for so-called Krull domains, see [20, §1]. A Noetherian domain is a Krull domain if and only if it is normal, but there also exist non-Noetherian Krull domains; in particular, for a Krull domain S and a finite group $G \subseteq \mathrm{Aut}(S)$ the ring of invariants S^G is again a Krull domain, see [20, Proposition 1.2].

Since we will need this later, we sketch the construction of the embedding $\ker \varphi \hookrightarrow H^1(G, S^\times)$ in Proposition 5.18; for the details we refer to [20]. We define $K := \mathrm{Quot}(S^G)$ and $L := \mathrm{Quot}(S)$. The group G acts naturally on $\mathrm{Div}(S)$ and $\mathrm{Prin}(S)$ and hence also on $\mathrm{Cl}(S)$. We have a short exact sequence of G-modules

$$0 \to S^\times \to L^\times \to \mathrm{Prin}(S) \to 0.$$

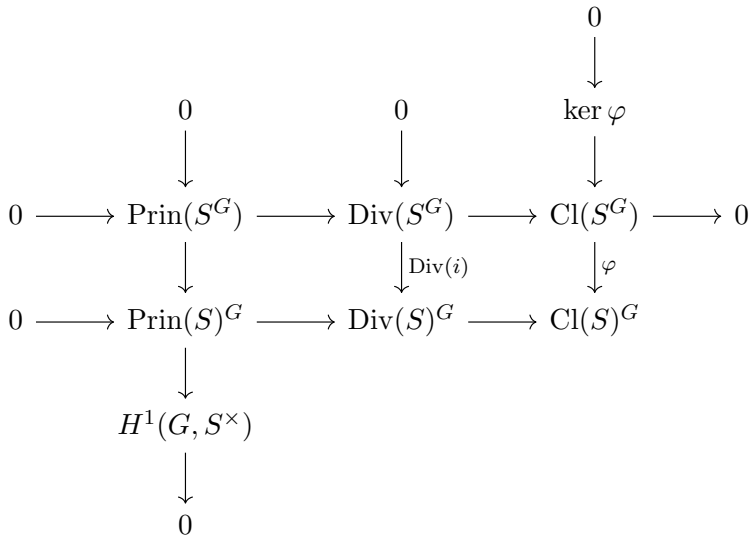
By applying the long exact sequence for group cohomology to this we obtain the following exact sequence (note that $H^1(G, L^\times) = 0$ be Hilbert's theorem 90, see Serre [53, Chapter X, Proposition 2]):

$$0 \to (S^G)^\times \to K^\times \to \mathrm{Prin}(S)^G \to H^1(G, S^\times) \to 0.$$

We have $\mathrm{Prin}(S^G) \cong K^\times/(S^G)^\times$, so we obtain an exact sequence

$$0 \to \mathrm{Prin}(S^G) \to \mathrm{Prin}(S)^G \to H^1(G, S^\times) \to 0.$$

The map $K^\times \to \mathrm{Prin}(S)^G$ in the previous sequence is given by $a \mapsto \mathrm{div}((a))$, so the map $\mathrm{Prin}(S^G) \to \mathrm{Prin}(S)^G$ in this sequence is the restriction of $\mathrm{Div}(i)$ to $\mathrm{Prin}(S^G)$. Since S is integral over S^G, the map $\mathrm{Div}(i)$ is injective and its image is contained in $\mathrm{Div}(S)^G$, so we obtain the following commutative diagram with exact rows and columns:



By applying the snake lemma we now get an exact sequence

$$0 \to \ker \varphi \to H^1(G, S^\times)$$

which gives the desired injective map $\ker \varphi \to H^1(G, S^\times)$.

We end this section by giving one more result on the induced homomorphisms on divisor class groups.

Lemma 5.20. *Let $A \subseteq B \subseteq C$ be Noetherian normal domains and let $i_{AB} : A \to B$, $i_{BC} : B \to C$, and $i_{AC} : A \to C$ be the respective inclusions. Assume that all these inclusions satisfy condition (PDE).*
a) We have $\mathrm{Div}(i_{AC}) = \mathrm{Div}(i_{BC}) \circ \mathrm{Div}(i_{AB})$.
b) Let $\varphi_{AB} : \mathrm{Cl}(A) \to \mathrm{Cl}(B)$, $\varphi_{BC} : \mathrm{Cl}(B) \to \mathrm{Cl}(C)$, and $\varphi_{AC} : \mathrm{Cl}(A) \to \mathrm{Cl}(C)$ be the induced maps on divisor class groups. Then we have $\varphi_{AC} = \varphi_{BC} \circ \varphi_{AB}$.

Proof. Let $\mathfrak{p} \in X^{(1)}(A)$ and $\mathfrak{P} \in X^{(1)}(C)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$. Since $B \subseteq C$ satisfies (PDE) and $(0) \neq \mathfrak{p} \subseteq \mathfrak{P} \cap B$ we have $\mathfrak{P} \cap B \in X^{(1)}(B)$. Then we have $e(\mathfrak{P}, \mathfrak{p}) = e(\mathfrak{P}, \mathfrak{P} \cap B) \cdot e(\mathfrak{P} \cap B, \mathfrak{p})$: if all extensions are finite this is Lemma 2.8 and the general case can be proved precisely in the same way. Now part *a)* follows from the definition of the maps $\mathrm{Div}(i)$ and part *b)* is then clear. □

Remark 5.21. It is natural to ask whether it is possible and perhaps even easier to define the maps $\mathrm{Div}(i)$ directly on the group of divisorial ideals $D(A)$ instead of the group of divisors $\mathrm{Div}(A)$. This is indeed possible and one can even do this in a much more general context, see Sather-Wagstaff and Spiroff [51]: if A and B are Noetherian normal domains and $\varphi : A \to B$ is a ring homomorphism of finite flat dimension, i.e. B has a finite flat resolution as an A-module, then the map $D(A) \to D(B), \mathfrak{a} \mapsto \overline{\mathfrak{a} \otimes_A B}$ induces a homomorphism on divisor class groups. However, due to the reflexive closure involved in the definition, many arguments become much more complicated with this definition. For

example, the proof of the generalization of Lemma 5.20 to this situation in [51, Theorem 1.14] is rather involved, while the proof given above is almost trivial.

5.4 Picard groups

An object closely related to the divisor class group of a Noetherian normal domain is its Picard group. This group can be defined for arbitrary rings and even for schemes. For Noetherian normal domains there is then an embedding of the Picard group into the divisor class group. Here we summarize the basic facts on Picard groups which we need in the next chapters. Our main reference for this is Fossum [20, Section 18]. We fix a Noetherian ring A (for simplicity, we only consider Noetherian rings in this section).

Definition 5.22. *An A-module L is called invertible if it is locally free of rank one, that is, if for every prime ideal $\mathfrak{p} \subset A$ we have $L_\mathfrak{p} \cong A_\mathfrak{p}$.*

Lemma 5.23. *Let L and L' be invertible A-modules. Then $L \otimes_A L'$ and $L^* := \mathrm{Hom}_A(L, A)$ are again invertible A-modules.*

The set of isomorphism classes of invertible A-modules is a group with respect to the tensor product; the inverse of the isomorphism class of a module L is the isomorphism class of L^*.

Definition 5.24. *The group of isomorphism classes of invertible A-modules with the group structure indicated above is called the Picard group of A and written as* $\mathrm{Pic}(A)$.

It is clear from the definition that the Picard group of a local ring is always trivial. We will see below that the Picard group of a Dedekind domain is isomorphic to its ideal class group.

Now let A be a Noetherian normal domain with quotient field K. Then an invertible A-module L can be embedded into $L \otimes_A K \cong K$ and hence is isomorphic to an invertible fractional ideal $\mathfrak{a}$ of A, see [20, Proposition 18.2]. It is clear that invertible fractional ideals are divisorial, so in this way we can associate a divisorial ideal to every invertible A-module. Using this, one can prove the following result, see [20, Corollary 18.3].

Proposition 5.25. *Let A be a Noetherian normal domain. Then* $\mathrm{Pic}(A)$ *is isomorphic to a subgroup of* $\mathrm{Cl}(A)$.

The next proposition, see [20, Corollary 18.5], shows in which cases this embedding is in fact an isomorphism.

Proposition 5.26. *Let A be a Noetherian normal domain. The injective homomorphism $\mathrm{Pic}(A) \to \mathrm{Cl}(A)$ given by Proposition 5.25 is an isomorphism if and only if A is locally factorial.*

In particular this implies the result announced above that the Picard group of a Dedekind domain is isomorphic to the ideal class group: Dedekind domains are always

locally factorial by Proposition 2.25 and the divisor class group of a Dedekind domain is precisely the ideal class group by Example 5.13.

Next we want to associate to a homomorphism $\varphi : A \to B$ of Noetherian rings a group homomorphism $\mathrm{Pic}(A) \to \mathrm{Pic}(B)$. While for the divisor class group we only achieved this for injective homomorphisms satisfying condition (PDE), for the Picard group we can really do this for arbitrary ring homomorphisms: if L is an invertible A-module, then $L \otimes_A B$ is an invertible B-module: for $\mathfrak{q} \in \mathrm{Spec}(B)$ and $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$ we have

$$(L \otimes_A B)_{\mathfrak{q}} \cong (L \otimes_A B) \otimes_B B_{\mathfrak{q}} \cong L \otimes_A B_{\mathfrak{q}} \cong (L \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \cong L_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \cong A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \cong B_{\mathfrak{q}}.$$

Using this we can define the desired group homomorphism $\mathrm{Pic}(\varphi) : \mathrm{Pic}(A) \to \mathrm{Pic}(B)$ by mapping the isomorphism class of L to the isomorphism class of $L \otimes_A B$.

Lemma 5.27. *With the above definition* Pic *becomes a functor from the category of Noetherian commutative rings to the category of abelian groups.*

We finally mention the following result which in many cases allows us to describe the Picard group of a polynomial ring.

Proposition 5.28. (Gilmer and Heitmann [24, Theorem 1.6]) *Let A be a Noetherian normal domain. Then the map* $\mathrm{Pic}(A) \to \mathrm{Pic}(A[x])$ *induced by the inclusion $A \hookrightarrow A[x]$ is an isomorphism.*

6 Factoriality of rings of arithmetic invariants

The goal of this chapter is a generalization of Nakajima's theorem on factorial rings of invariants (Theorem 2.19) to the arithmetic case. Our proof as well as the proof of Nakajima's theorem uses the theory of divisor class groups summarized in Chapter 5 which provides a useful characterization of factorial rings (Theorem 5.14). The first section of this chapter contains a general result on divisor class groups of rings of invariants in general algebras. In the second section we prove the main result of this chapter, which fully answeres the question under which conditions a ring of invariants $R[x_1, \ldots, x_n]^G$ is factorial (Theorem 6.5) for a Noetherian normal domain R and a finite group $G \subseteq Gl_n(R)$. In the final section we compute the Picard group of such a ring of invariants.

6.1 Group actions on algebras

Let R and S be Noetherian normal domains with $R \subseteq S$. Furthermore, let G be a finite subgroup of $\mathrm{Aut}_R(S)$. We define $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$. We want to know whether S^G is factorial. The best result we could hope for would be the following:

$$S^G \text{ is factorial if and only if both } S \text{ and } S_K^G \text{ are factorial.} \tag{6.1}$$

This statement however is not true in general, as the following example shows.

Example 6.1. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[\sqrt{-5}]$. We recall some basic facts about S from algebraic number theory. S is the ring of integers in the number field $L = \mathbb{Q}(\sqrt{-5})$; in particular, S is normal. But S is not factorial since the class number of L is not 1 (see Neukirch [46, Page 37]). Furthermore, let $G := \mathrm{Gal}(L/\mathbb{Q})$ be the Galois group. Then $S^G = \mathbb{Z}$ is factorial, contradicting (6.1).

From now on we assume that $S^\times = S \cap R^\times$ and $S_K^\times = S_K \cap K^\times$; see Remark 6.4 for a discussion of these assumptions. Then the factoriality of S_K^G can be checked using a generalized version of Nakajima's Theorem 2.19, see Nakajima [45, Theorem 2.11].

In the next section we shall see that (6.1) is indeed true in the particularly interesting case that S is a polynomial ring over R. In this section we prove the simpler result that under the above assumptions on groups of units (6.1) holds if S is factorial; in particular, the "if"-part of (6.1) holds under these assumptions. More precisely, we prove that if S is factorial, the divisor class groups of S^G and S_K^G coincide.

We begin with a lemma for which we do not need that S is factorial but only that S_K is factorial. This lemma will be used again in the next section.

Lemma 6.2. *With the notation as above, the inclusion $S^G \subseteq (R\backslash\{0\})^{-1}S^G = S_K^G$ induces a homomorphism $\alpha : \mathrm{Cl}(S^G) \to \mathrm{Cl}(S_K^G)$ by Proposition 5.16. Furthermore, by Proposition 5.18, the inclusion $S^G \subseteq S$ induces a homomorphism $\varphi : \mathrm{Cl}(S^G) \to \mathrm{Cl}(S)$. If S_K is factorial and $S_K^\times = K^\times$ and $S^\times = R^\times$, then the restriction of α to $\ker(\varphi)$ is injective.*

Proof. Since $S^\times = R^\times$ and G acts trivially on R, by Proposition 5.18 there is an injective homomorphism $\theta : \ker\varphi \to H^1(G, S^\times) = \mathrm{Hom}(G, R^\times)$. Let $\varphi_K : \mathrm{Cl}(S_K^G) \to \mathrm{Cl}(S_K)$ be the map given by Proposition 5.18 applied to the inclusion $S_K^G \subseteq S_K$. Since we assumed S_K to be factorial, $\mathrm{Cl}(S_K) = \{0\}$ and hence $\ker\varphi_K = \mathrm{Cl}(S_K^G)$, so Proposition 5.18 gives an embedding $\theta_K : \mathrm{Cl}(S_K^G) \to H^1(G, S_K^\times) = \mathrm{Hom}(G, K^\times)$ since $S_K^\times = K^\times$ by assumption. R is normal, so every root of unity in K is already in R, and hence $\mathrm{Hom}(G, R^\times) = \mathrm{Hom}(G, K^\times)$ because G is finite. So we have the following diagram:

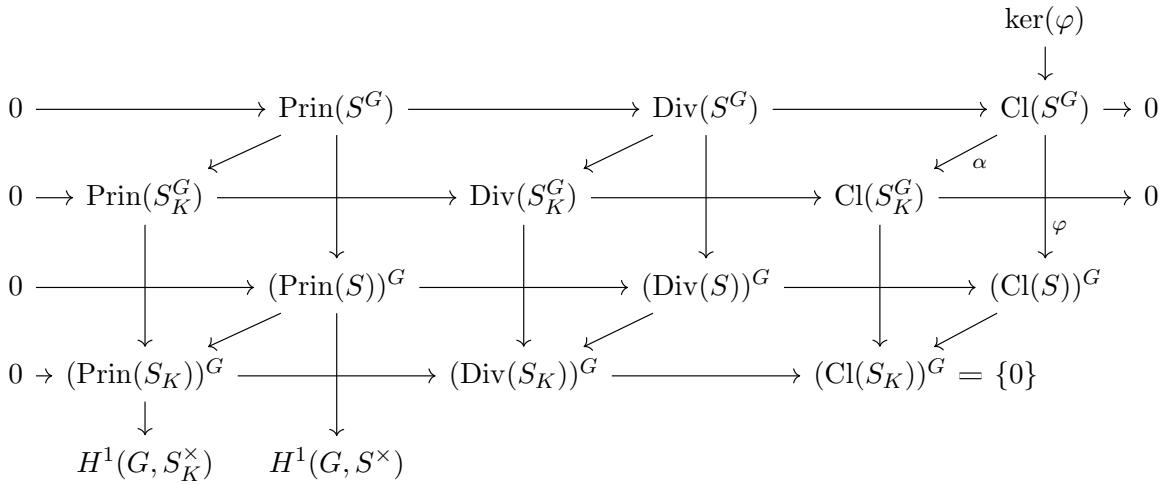
$$\begin{array}{ccc} \ker(\varphi) & \xrightarrow{\theta} & \mathrm{Hom}(G, R^\times) \\ \downarrow{\scriptstyle \alpha|_{\ker(\varphi)}} & & \downarrow{\scriptstyle =} \\ \mathrm{Cl}(S_K^G) & \xrightarrow{\theta_K} & \mathrm{Hom}(G, K^\times) \end{array}$$

Since θ is injective, the claim follows if we prove that this diagram commutes.

The inclusion $S \subseteq S_K$ satisfies condition (PDE) by Proposition 5.16 and hence we obtain a map $\mathrm{Cl}(S) \to \mathrm{Cl}(S_K)$ which fits into the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Prin}(S) & \longrightarrow & \mathrm{Div}(S) & \longrightarrow & \mathrm{Cl}(S) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Prin}(S_K) & \longrightarrow & \mathrm{Div}(S_K) & \longrightarrow & \mathrm{Cl}(S_K) & \longrightarrow & 0 \end{array}$$

The inclusion $S^G \hookrightarrow S_K^G$ gives a similar commutative diagram and as in the discussion after Remark 5.19 we obtain the following diagram with exact rows and columns:



The front and back part of this diagram commute by the discussion after Remark 5.19 and the top and bottom parts commute by the above. Furthermore the mid part of the diagram, that is, the part with the groups of divisors, commutes since both possible paths are just the map on divisor class groups induced by the inclusion $S^G \subseteq S_K$ (see Lemma 5.20); then it follows immediately that the left and right parts also commute. Now by the construction of θ and the naturality of the connecting homomorphism in the snake lemma we obtain a commutative diagram

$$\begin{array}{ccc} \ker(\varphi) & \xrightarrow{\theta} & H^1(G, R^\times) \\ \downarrow{\scriptstyle \alpha|_{\ker(\varphi)}} & & \downarrow \\ \mathrm{Cl}(S_K^G) & \xrightarrow{\theta_K} & H^1(G, K^\times) \end{array}$$

It remains to show that in the last diagram the map on the right is really the identity on $\mathrm{Hom}(G, R^\times) = \mathrm{Hom}(G, K^\times)$. Again the discussion after Remark 5.19 shows that by the naturality of the long exact sequence in group cohomology this map is the map on $H^1(G, \cdot)$ induced by the inclusion $R^\times \hookrightarrow K^\times$ which indeed is the identity $\mathrm{Hom}(G, R^\times) = \mathrm{Hom}(G, K^\times)$. □

Now we prove the desired result on the factoriality of S^G for factorial rings S.

Theorem 6.3. *Let R and S be Noetherian normal domains with $R \subseteq S$. Define $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$ and assume that $S^\times = R^\times$ and $S_K^\times = K^\times$. Let $G \subseteq \mathrm{Aut}_R(S)$ be a finite subgroup. If S is factorial, then $\mathrm{Cl}(S^G) \cong \mathrm{Cl}(S_K^G)$. In particular, if both S and S_K^G are factorial, then S^G is also factorial.*

Proof. We continue with the notation from Lemma 6.2. By Proposition 5.16, α is surjective and since S is factorial, $\mathrm{Cl}(S) = \{1\}$ and hence $\ker \varphi = \mathrm{Cl}(S^G)$. So by Lemma 6.2, α is also injective and hence an isomorphism. □

Remark 6.4. Here are some comments on the assumptions $S^\times = R^\times$ and $S_K^\times = K^\times$ in Theorem 6.3. First of all, these assumptions are certainly satisfied if S is a graded R-algebra, so in particular they always hold if S is a polynomial ring over R. On the other hand, the second assumption is not satisfied in Example 6.1; we have $S_K = L$ and hence $S_K^\times = L \backslash \{0\} \neq K^\times$ there. So it may be questioned whether Example 6.1 really shows that the converse of the last statement in Theorem 6.3 does not hold or rather that the assumptions on the groups of units are necessary. The main goal of this remark is to demonstrate that the first answer fits better. Example 6.1 also shows that $S_K^\times = K^\times$ does not follow automatically if we have $S^\times = R^\times$: it is easy to see that in this example we have $S^\times = \{1, -1\} = R^\times$.

First of all, it is easy to see that it is possible to replace the assumption $S_K^\times = K^\times$ in Theorem 6.3 by a weaker one: we used it only to prove that $\mathrm{Hom}(G, S^\times) = H^1(G, S_K^\times)$ in the proof of Lemma 6.2 and a closer look to that proof shows that we really only need the weaker statement that the homomorphism on group cohomology $H^1(G, S^\times) \to H^1(G, S_K^\times)$ induced by the inclusion $S^\times \hookrightarrow S_K^\times$ is injective. Using the long exact sequence

for group cohomology, we see that this is the same as saying that the projection $S_K^\times \to S_K^\times/S^\times$ restricts to a surjective homomorphism $(S_K^\times)^G \to (S_K^\times/S^\times)^G$. So we can replace the above assumption by this one. Even this weaker assumption is not satisfied in Example 6.1: there the class of $\sqrt{-5} \in S_K^\times$ in $(S_K^\times/S^\times)$ consists of $\sqrt{-5}$ and $-\sqrt{-5}$, so it is invariant under the action of G, because the nontrivial element of G interchanges $\sqrt{-5}$ and $-\sqrt{-5}$. On the other hand, this also shows that neither $\sqrt{-5}$ nor $-\sqrt{-5}$ are G-invariant, so the class of $\sqrt{-5}$ is not in the image of the restricted map $(S_K^\times)^G \to (S_K^\times/S^\times)^G$ which is therefore not surjective. However, this assumption is still more than what we really need: the proof of Theorem 6.3 shows that it is possible to write the theorem in the following form:

Let R and S be Noetherian normal domains with $R \subseteq S$. Define $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$. Let $G \subseteq \mathrm{Aut}_R(S)$ be a finite subgroup. If S is factorial and $\alpha|_{\ker\varphi}$ is injective, where α and φ are defined as in Lemma 6.2, then $\mathrm{Cl}(S^G) \cong \mathrm{Cl}(S_K^G)$. In particular, if both S and S_K^G are factorial, then S^G is also factorial.

And it turns out that $\alpha|_{\ker\varphi}$ is injective in the situation of Example 6.1: since $S^G = \mathbb{Z}$ is factorial, we have $Cl(S^G) = \{0\}$ and thus also $\ker\varphi = \{0\}$, so a homomorphism from $\ker\varphi$ to any group must always be injective. Nevertheless, the converse of the last statement in the theorem does not hold in this example, so the converse is really not true in this general version.

6.2 Group actions on polynomial rings

One situation in which Theorem 6.3 can be applied is when R is a Noetherian normal domain and S is a polynomial ring over R; in this case, statement (6.1) from the previous section is indeed true as the following theorem shows. This is the main result of this chapter.

Theorem 6.5. *Let R be a Noetherian normal domain, $S := R[x_1, \ldots, x_n]$, and $G \subseteq \mathrm{Aut}_R(S)$ a finite subgroup. Further define $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$. Then*

$$\mathrm{Cl}(S^G) \cong \mathrm{Cl}(R) \times \mathrm{Cl}((S_K)^G).$$

In particular S^G is factorial if and only if both R and $(S_K)^G$ are factorial.

In the special case where G acts linearly on R^n we obtain the following generalization of Nakajima's Theorem 2.19:

Corollary 6.6. *Let R be a Noetherian normal domain and let $G \subseteq Gl_n(R)$ be a finite subgroup. Then $R[x_1, \ldots, x_n]^G$ is factorial if and only if R is factorial and every R-valued character of G is uniquely determined by its restriction to the subgroup of G generated by all pseudoreflections. In particular, if G is a pseudoreflection group, then $R[x_1, \ldots, x_n]^G$ is factorial if and only if R is factorial.*

Proof. Let $K := \mathrm{Quot}(R)$ and let χ be a K-valued character of G. For every $\sigma \in G$, $\chi(\sigma)$ is a root of unity in K since G is finite; therefore $\chi(\sigma) \in R$ because R is normal. This shows that the R-valued characters and the K-valued characters of G are the same, so the result follows from Theorem 6.5 and Theorem 2.19. □

Now we aim to prove Theorem 6.5; we need two lemmas. As in the theorem we take a Noetherian normal domain R and set $S := R[x_1, \ldots, x_n]$. We already know from Propositions 5.18 and 5.17 that the inclusions $S^G \subseteq S$ and $R \subseteq S$ satisfy condition (PDE). The next lemma shows that the same holds for $R \subseteq S^G$.

Lemma 6.7. *Under the assumptions of Theorem 6.5 the inclusion $R \subseteq S^G$ satisfies (PDE).*

Proof. Let $\mathfrak{P} \in X^{(1)}(S^G)$. The extension $S^G \subseteq S$ is integral, so by lying-over there exists a $\mathfrak{Q} \in X^{(1)}(S)$ with $\mathfrak{Q} \cap S^G = \mathfrak{P}$. Then we have $\mathfrak{P} \cap R = (\mathfrak{Q} \cap S^G) \cap R = \mathfrak{Q} \cap R$ and $\mathrm{ht}(\mathfrak{Q} \cap R) \leq 1$ since the inclusion $R \subseteq S$ satisfies (PDE) by Proposition 5.17. □

In the situation of Theorem 6.5 we now have several inclusions of rings which satisfy condition (PDE). These induce the following canonical maps of divisor class groups: $\varphi : \mathrm{Cl}(S^G) \to \mathrm{Cl}(S)$ exists by Proposition 5.18; $\psi : \mathrm{Cl}(R) \to \mathrm{Cl}(S)$ exists by Proposition 5.17; $\psi' : \mathrm{Cl}(R) \to \mathrm{Cl}(S^G)$ exists by Lemma 6.7; $\alpha : \mathrm{Cl}(S^G) \to \mathrm{Cl}(S^G_K)$ exists by Proposition 5.16. Lemma 5.20 shows that $\psi = \varphi \circ \psi'$, so we obtain the following commutative diagram:

$$\begin{array}{ccccc} & & \mathrm{Cl}(S) & & \\ & \overset{\psi}{\nearrow} & \uparrow{\scriptstyle \varphi} & & \\ \mathrm{Cl}(R) & \xrightarrow{\psi'} & \mathrm{Cl}(S^G) & \xrightarrow{\alpha} & \mathrm{Cl}(S^G_K) \end{array}$$

The next lemma contains several properties of these maps:

Lemma 6.8. *With the notation as above, the following holds.*
a) $\mathrm{im}\psi' \cong \mathrm{Cl}(R)$.
b) $\mathrm{Cl}(S^G) = \ker\varphi \times \mathrm{im}\psi'$.
c) The restriction of α to $\ker\varphi$ is surjective.

Proof.
a) Since ψ is an isomorphism by Proposition 5.17 and $\psi = \varphi \circ \psi'$, ψ' must be injective. This implies $\mathrm{im}\psi' \cong \mathrm{Cl}(R)$.
b) With the same argument as in the proof of a) we see that φ must be surjective, so we have a short exact sequence

$$0 \to \ker\varphi \to \mathrm{Cl}(S^G) \xrightarrow{\varphi} \mathrm{Cl}(S) \to 0.$$

Since ψ is an isomorphism, $\psi = \varphi \circ \psi'$ implies $\mathrm{id}_{\mathrm{Cl}(S)} = \varphi \circ (\psi' \circ \psi^{-1})$, so $\psi' \circ \psi^{-1}$ is a right inverse of φ with $\mathrm{im}(\psi' \circ \psi^{-1}) = \mathrm{im}\psi'$. Hence the above exact sequence splits and we obtain $\mathrm{Cl}(S^G) = \ker\varphi \times \mathrm{im}(\psi' \circ \psi^{-1}) = \ker\varphi \times \mathrm{im}\psi'$.
c) By part b) we have $\mathrm{Cl}(S^G) = \mathrm{im}\psi' \times \ker\varphi$. We prove that $\alpha|_{\mathrm{im}\psi'} = 0$; then the claim follows since α is surjective by Proposition 5.16. So let $\mathfrak{p} \in X^{(1)}(R)$. By definition we have

$$\psi'([\mathrm{div}(\mathfrak{p})]) = \sum_{\substack{\mathfrak{P} \in X^{(1)}(S^G), \\ \mathfrak{P} \cap R = \mathfrak{p}}} e(\mathfrak{P}, \mathfrak{p})[\mathrm{div}(\mathfrak{P})]$$

where $[\mathrm{div}(\mathfrak{p})]$ denotes the class of $\mathrm{div}(\mathfrak{p})$ in $\mathrm{Cl}(R)$ and similarly for $[\mathrm{div}(\mathfrak{P})]$. For every prime ideal $\mathfrak{P} \in X^{(1)}(S^G)$ with $\mathfrak{P} \cap R = \mathfrak{p} \neq (0)$ we have $\alpha([\mathrm{div}(\mathfrak{P})]) = 0$ by Proposition 5.16, so we also have $\alpha(\psi'([\mathrm{div}(\mathfrak{p})])) = 0$. This shows that indeed $\alpha|_{\mathrm{im}\psi'} = 0$.

□

Now we can easily proof our main theorem:

Proof of Theorem 6.5. By Lemmas 6.2 and 6.8c) α restricts to an isomorphism $\ker\varphi \to \mathrm{Cl}(S_K^G)$. By combining this with Lemma 6.8a) and b) we obtain

$$\mathrm{Cl}(S^G) = \ker\varphi \times \mathrm{im}\psi' \cong \mathrm{Cl}(S_K^G) \times \mathrm{Cl}(R).$$

The second statement now follows from Theorem 5.14. □

We end this section by considering the question of whether factoriality of the ring of invariants over some ring R implies factoriality of the ring of invariants over a factor ring R/P for a prime ideal $P \subset R$. The following example shows that this need not be true, even in the case where $|G| \notin P$.

Example 6.9. Let $R = \mathbb{Z}$. We consider the cyclic subgroup G of $Gl_3(\mathbb{Z})$ generated by the following matrix:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Then $|G| = 3$ and since $\mathbb{Z}$ does not contain any nontrivial third root of unity, there are no nontrivial $\mathbb{Z}$-valued characters of G. Hence $\mathbb{Z}[x, y, z]^G$ is factorial by Corollary 6.6. Now we study the invariants of G over $\mathbb{F}_7 = \mathbb{Z}/(7)$. Since $\mathbb{F}_7^\times$ is cyclic of order 6, there are nontrivial $\mathbb{F}_7$-valued characters of G. But G viewed as a subgroup of $Gl_3(\mathbb{F}_7)$ does not contain any pseudoreflections, and hence $\mathbb{F}_7[x, y, z]^G$ is not factorial by Theorem 2.19.

6.3 The Picard group of rings of invariants

After having computed the divisor class group of a ring of invariants one may ask whether it is also possible to compute the Picard group. Over fields, this has been done by Kang [31]; his result is the following:

Theorem 6.10. ([31, Theorem 5.3]) *Let K be a field and let $G \subseteq Gl_n(K)$ be a finite subgroup. Then* $\mathrm{Pic}(K[x_1, \ldots, x_n]^G) = \{0\}$.

In this section we prove the following arithmetic generalization of Kang's theorem:

Theorem 6.11. *Let R be a Noetherian normal domain and let $G \subseteq Gl_n(R)$ be a finite subgroup. Then* $\mathrm{Pic}(R[x_1, \ldots, x_n]^G) \cong \mathrm{Pic}(R)$.

The proof of this result turns out to be much simpler than the discussion of the divisor class group of $R[x_1,\dots,x_n]^G$ in the previous section: a large part of the proof for the divisor class group was related to the kernel of the canonical map $\mathrm{Cl}(R[x_1,\dots,x_n]^G) \to \mathrm{Cl}(R[x_1,\dots,x_n])$. The following result of Kang [31] shows that this is not necessary for the Picard group.

Proposition 6.12. (Kang [31, Corollary 2.2]) *Let R be a normal domain, $S := R[x_1,\dots,x_n]$, and $G \subseteq \mathrm{Aut}_R(S)$ a subgroup such that $\sigma(S_+) = S_+$ for all $\sigma \in G$. Then the homomorphism $\mathrm{Pic}(S^G) \to \mathrm{Pic}(S)$ induced by the embedding $S^G \hookrightarrow S$ is injective.*

Using this we can now prove Theorem 6.11. The basic idea of the proof is the same as for Theorem 6.5.

Proof of Theorem 6.11. We consider the embeddings

$$\alpha : R \hookrightarrow R[x_1,\dots,x_n]^G, \beta : R[x_1,\dots,x_n]^G \hookrightarrow R[x_1,\dots,x_n], \gamma : R \hookrightarrow R[x_1,\dots,x_n]$$

and the induced maps on Picard groups; we need to show that $\mathrm{Pic}(\alpha)$ is an isomorphism. We have $\gamma = \beta \circ \alpha$ and thus $\mathrm{Pic}(\gamma) = \mathrm{Pic}(\beta) \circ \mathrm{Pic}(\alpha)$ since Pic is a functor. By Proposition 5.28 $\mathrm{Pic}(\gamma)$ is an isomorphism, so $\mathrm{Pic}(\alpha)$ must be injective. Let $b \in \mathrm{Pic}(S^G)$; since $\mathrm{Pic}(\gamma)$ is an isomorphism, there is an $a \in \mathrm{Pic}(R)$ such that $\mathrm{Pic}(\gamma)(a) = \mathrm{Pic}(\beta)(b)$, so with $\mathrm{Pic}(\gamma) = \mathrm{Pic}(\beta) \circ \mathrm{Pic}(\alpha)$ we obtain $\mathrm{Pic}(\beta)(\mathrm{Pic}(\alpha)(a)) = \mathrm{Pic}(\beta)(b)$. Since $\mathrm{Pic}(\beta)$ is injective by Proposition 6.12, this shows $b = \mathrm{Pic}(\alpha)(a)$ and hence $\mathrm{Pic}(\alpha)$ is surjective. □

Theorem 6.11 has the following remarkable consequence which in the case where R is a field is essentially due to Kang [31, Corollary 5.4].

Corollary 6.13. *Let R be a Noetherian and factorial domain and let $G \subseteq Gl_n(R)$ be a finite subgroup. Then the following statements are equivalent.*
(i) $R[x_1,\dots,x_n]^G$ is factorial.
(ii) $R[x_1,\dots,x_n]^G_{\mathfrak{p}}$ is factorial for every prime ideal $\mathfrak{p} \subset R[x_1,\dots,x_n]^G$.

Proof. Since localizations of factorial domains are again factorial, (i) implies (ii). For the converse we first note that since R is factorial, we have $\mathrm{Cl}(R) = \{0\}$ by Theorem 5.14, so $\mathrm{Pic}(R) = \{0\}$ by Proposition 5.25. By Theorem 6.11 this implies $\mathrm{Pic}(R[x_1,\dots,x_n]^G) = \{0\}$. Hence by (ii) and Proposition 5.26 we have $\mathrm{Cl}(R[x_1,\dots,x_n]^G) = \{0\}$, so we obtain that $R[x_1,\dots,x_n]^G$ is factorial by Theorem 5.14. □

7 The quasi-Gorenstein property for rings of arithmetic invariants

Broer [8] generalized the results of Watanabe and Braun (see Theorem 2.21) on the Gorenstein property for rings of invariants to groups which may contain pseudoreflections. He gives a complete answer to the question of when the ring of invariants $K[x_1, \ldots, x_n]^G$ of a finite group $G \subseteq Gl_n(K)$ over an arbitrary field K is a quasi-Gorenstein ring. Quasi-Gorenstein rings are a concept due to Aoyama and others generalizing the Gorenstein property to rings which need not be Cohen-Macaulay: a Cohen-Macaulay ring is quasi-Gorenstein if and only if it is Gorenstein, but there are quasi-Gorenstein rings which are not Cohen-Macaulay. The goal of this chapter is to generalize Broer's theorem to the arithmetic case. We begin by recalling the definition of a quasi-Gorenstein ring and then we study the quasi-Gorenstein property for graded rings in some more detail. After that we introduce Dedekind differents and give the precise statement of Broer's theorem (Theorem 7.30). As a further tool in Section 7.5 we introduce systems of parameters and prove an existence theorem which might be interesting not only in the context of the quasi-Gorenstein property. In the last two sections of this chapter we finally prove the generalization of Broer's theorem to the arithmetic case (Theorem 7.56).

7.1 The quasi-Gorenstein property for local rings

In this section we briefly recall the definitions and some basic properties of the canonical module of a local ring and local quasi-Gorenstein rings. All rings in this section are assumed to be Noetherian. Before we define canonical modules we need the definition of the injective hull of a module (see Lam [38, Definition 3.31]).

Definition 7.1. *Let A be a ring and let M be an A-module.*

a) A minimal injective extension of M is an injective A-module I together with an injective homomorphism of A-modules $i : M \to I$ such that for every other injective module J with an injective homomorphism $j : M \to J$ there is an injective homomorphism $k : I \to J$ such that $j = k \circ i$.

b) It can be proved that every module M has a minimal injective extension (see [38, Lemma 3.29]) and that it is unique up to an isomorphism which restricts to the identity on M (see [38, Corollary 3.32]). This unique minimal injective extension is called the injective hull of M and is written as $E_A(M)$.

Furthermore, we briefly recall the definition of local cohomology (see Brodmann and Sharp [7, Chapter 1]): Let I be an ideal in a ring A and let M be an A-module. We

define $\Gamma_I(M) \coloneqq \bigcup_{i\in\mathbb{N}}(0 :_M I^i) = \{m \in M | \exists i \in \mathbb{N} : I^i \cdot m = 0\}$. The association $M \mapsto \Gamma_I(M)$ is a left-exact functor called the I-torsion functor. Then one defines the n-th local cohomology functor with support in I as the n-th right derived functor of $\Gamma_I(\cdot)$; it is written as $H^n_I(\cdot)$. We have an isomorphism

$$H^n_I(M) \cong \varinjlim_{i\in\mathbb{N}} \operatorname{Ext}^n_A(A/I^i, M).$$

Now we can give the definition of the canonical module of a local ring due to Herzog and Kunz [28, Definition 5.6].

Definition 7.2. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and $d := \dim A$. If A is complete, then the canonical module of A is $K_A := \operatorname{Hom}(H^d_\mathfrak{m}(A), E_A(A/\mathfrak{m}))$. If A is not necessarily complete, then an A-module K_A is called a canonical module of A if $K_A \otimes_A \hat{A} \cong K_{\hat{A}}$, where $\hat{A}$ denotes the completion of A and $K_{\hat{A}}$ denotes the canonical module of $\hat{A}$.*

Not every local ring has a canonical module, but if a canonical module exists, then it is unique up to isomorphism ([28, Bemerkung 5.7]). The canonical module of a local ring A (if it exists) is written as K_A.

Remark 7.3. Although we do not need this later, it seems appropriate to give some motivation for the definition of the canonical module, see Brodmann and Sharp [7] for more details. Let A be a complete Noetherian local ring of dimension d with maximal ideal $\mathfrak{m}$. The local cohomology module $H^d_\mathfrak{m}(A)$ plays a particularly important role as it is always nonzero while $H^n_\mathfrak{m}(A) = 0$ for all $n > d$ (Grothendieck's vanishing theorem, see [7, Theorems 6.1.2 and 6.1.4]). However, it is rather hard to work with $H^d_\mathfrak{m}(A)$ directly as it is in general not a finitely generated A-module. But it turns out that $H^d_\mathfrak{m}(A)$ is always an Artinian A-module (see [7, Theorem 7.1.3]), so we can use a tool called Matlis duality: for an A-module M we define the Matlis dual of M as the module $D(M) := \operatorname{Hom}_A(M, E_A(A/\mathfrak{m}))$. As usual, we have a canonical map $M \to D(D(M))$. If now M is either Noetherian (that is, finitely generated) or Artinian, then this canonical map is an isomorphism, so in these cases the module M can be reconstructed from its Matlis dual. Moreover, the Matlis dual of an Artinian module is noetherian and vice versa (see [7, Theorem 10.2.12]). Hence instead of the Artinian module $H^d_\mathfrak{m}(A)$ we can also study its Matlis dual which is then finitely generated; this Matlis dual is precisely the canonical module.

In many cases we have an explicit description of the canonical module. This is the content of the following theorem (see [28, Satz 5.12]).

Theorem 7.4. *Let A and B be Noetherian local rings and let $\varphi : A \to B$ be a local homomorphism, i.e. for the maximal ideals $\mathfrak{m} \subset A$ and $\mathfrak{n} \subset B$ we have $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$, such that B becomes a finitely generated A-module. Assume that A is Cohen-Macaulay and has a canonical module K_A. Then $\operatorname{Ext}^r_A(B, K_A)$ is a canonical module of B where $r := \dim A - \dim B$.*

In the context of the theorem $\mathrm{Ext}^r_A(B, K_A)$ becomes a B-module as follows. For $b \in B$ the multiplication map $\mu_b : B \to B, c \mapsto bc$ is a homomorphism of A-modules, so it induces a homomorphism $\mu_b^* : \mathrm{Ext}^r_A(B, K_A) \to \mathrm{Ext}^r_A(B, K_A)$ and we define the B-module structure on $\mathrm{Ext}^r_A(B, K_A)$ by setting $b \cdot s := \mu_b^*(s)$ for $b \in B$ and $s \in \mathrm{Ext}^r_A(B, K_A)$.

A local ring A is a Gorenstein ring if and only if it is a Cohen-Macaulay ring which has a canonical module K_A and $K_A \cong A$, see [28, Satz 5.9]. This motivates the definition of a local quasi-Gorenstein ring due to Platte and Storch [49, §3] and Aoyama [2, Definition 2.1]:

Definition 7.5. *A local ring A is called a quasi-Gorenstein ring if the canonical module K_A of A exists and $A \cong K_A$ as A-modules.*

We end this section by giving some basic properties of local quasi-Gorenstein rings, see Aoyama [2, Section 2].

Lemma 7.6. *Let A be a local ring.*
a) A is quasi-Gorenstein if and only if its completion $\hat{A}$ is quasi-Gorenstein.
b) A is Gorenstein if and only if it is quasi-Gorenstein and Cohen-Macaulay.
c) Let $\mathfrak{p} \subset A$ be a prime ideal. If A is quasi-Gorenstein, then $A_\mathfrak{p}$ is also quasi-Gorenstein.

7.2 The quasi-Gorenstein property for graded rings

In this section we study the quasi-Gorenstein property for graded rings; again we assume that all rings are Noetherian. We begin with the general definition of a quasi-Gorenstein ring due to Aoyama and Goto [3, Definition 0.4].

Definition 7.7. *A ring A is called quasi-Gorenstein if $A_\mathfrak{p}$ is a quasi-Gorenstein local ring for every prime ideal $\mathfrak{p} \subset A$.*

The following result follows immediately from Lemma 7.6b).

Lemma 7.8. *Let A be a ring. Then A is Gorenstein if and only if A is quasi-Gorenstein and Cohen-Macaulay.*

In the rest of this section we study quasi-Gorenstein rings S which are *local graded rings. In this case we can define graded canonical modules; this notion is due to Goto and Watanabe [25] in the case that S_0 is a field and due to Ikeda [30] in the general case.

We first need to study injective objects in the category ${}^*\mathcal{C}(S)$ of graded S-modules, see Brodmann and Sharp [7, Section 13.2]. A graded S-module M is called *injective if it is an injective object in ${}^*\mathcal{C}(S)$.

Definition 7.9. *Let S be a graded ring, L a graded S-module, and $M \subseteq L$ a graded submodule.*
*a) L is called an *essential extension of M if $B \cap M \neq \{0\}$ for every graded submodule $\{0\} \neq B \subseteq L$.*
*b) L is called an *injective hull of M if L is *injective and an *essential extension of M.*

Similar as for minimal injective extensions in the ungraded case, we have the following existence and uniqueness result for *injective hulls:

Theorem 7.10. *Let S be a graded ring and let M be a graded S-module.*
a) M has an *injective hull; in particular, the category $^*\mathcal{C}(S)$ has enough injectives.
b) If L and L' are two *injective hulls of M, then there is a homogeneous isomorphism $f : L \to L'$ with $f|_M = \mathrm{id}$.

Proof. See [7, Theorem 13.2.4]. □

We write $^*E_S(M)$ for an *injective hull of a graded S-module M.

Definition 7.11. *a) Let S be a *local graded ring and let M be a graded S-module. Let $\mathfrak{m}$ be the unique homogeneous maximal ideal in S. We define the n-th graded local cohomology of M as $^*H^n_{\mathfrak{m}}(M) \coloneqq \varinjlim_{i\in\mathbb{N}} {}^*\mathrm{Ext}^n_S(S/\mathfrak{m}^i, M)$. Note that $^*H^n_{\mathfrak{m}}(M) \cong H^n_{\mathfrak{m}}(M)$ as S-modules for all n by Lemma 2.39.*
b) If S_0 is a complete local ring, then we define the graded canonical module of S as $^*K_S \coloneqq {}^*\mathrm{Hom}_S({}^*H^d_{\mathfrak{m}}(S), {}^*E_S(S/\mathfrak{m}))$.
c) If S_0 is not necessarily complete, then a graded S-module $^*K_S$ is called a graded canonical module of S if we have an isomorphism of graded $\hat{S}$-modules $^*K_S \otimes_S \hat{S} \cong {}^*K_{\hat{S}}$ where $\hat{S} \coloneqq S \otimes_{S_0} \hat{S}_0$ and $\hat{S}_0$ is the completion of the local ring S_0.

As in the local case, the graded canonical module is unique up to isomorphism if it exists; moreover, it is always finitely generated (see Ikeda [30, Proposition 1.7]). Furthermore, we have the following analogue of Theorem 7.4 (see [30, Proposition 1.10]).

Theorem 7.12. *Let S and T be *local graded rings with $S_0 = T_0$ and let $\varphi : S \to T$ be a homogeneous homomorphism such that T is finitely generated as an S-module. Assume that S is Cohen-Macaulay with graded canonical module $^*K_S$. Then $^*K_T \coloneqq {}^*\mathrm{Ext}^r_S(T, {}^*K_S)$ with $r \coloneqq \dim S - \dim T$ is the graded canonical module of T.*

Corollary 7.13. *Let S be a *local graded ring such that S_0 is Gorenstein. Then S has a graded canonical module.*

Proof. Since S is Noetherian by our general assumption, it is finitely generated as an S_0-algebra, see Bruns and Herzog [11, Proposition 1.5.4]. So we can write $S = S_0[f_1, \ldots, f_s]$ with homogeneous elements $f_1, \ldots, f_s \in S$. Next we define $T \coloneqq S_0[y_1, \ldots, y_s]$ with indeterminates $y_1, \ldots, y_s$. We define a grading on T by setting $\deg(y_i) \coloneqq \deg(f_i)$ for each i. Then we get a surjective homogeneous homomorphism $T \to S$. Since S_0 is Gorenstein, T is also Gorenstein, so $T(m)$ is a graded canonical module of T for some $m \in \mathbb{Z}$, see [30, Proposition 1.9] and hence with $r \coloneqq \dim(T) - \dim(S)$ Theorem 7.12 shows that $^*\mathrm{Ext}^r_T(S, T(m))$ is a graded canonical module of S. □

Theorem 7.12 has the following proposition as a consequence, which is mentioned without proof in [30]. For completeness and because we will need similar arguments again later we give a proof of it here.

Proposition 7.14. *Let R be a Gorenstein local ring and let S be a finitely generated graded R-algebra with graded canonical module ${}^*K_S$. Then for every prime ideal $\mathfrak{p} \subset S$, $({}^*K_S)_\mathfrak{p}$ is a canonical module of the local ring $S_\mathfrak{p}$.*

Proof. Let $f_1, \ldots, f_m$ be homogeneous generators of S as an R-algebra. Set $T := R[y_1, \ldots, y_m]$ and define a homomorphism of R-algebras $g : T \to S$ via $g(y_i) := f_i$. Since g is surjective, S becomes a finitely generated T-module. We define a grading on T by setting $\deg(y_i) := \deg(f_i)$. T is Gorenstein, so $T(m)$ is the graded canonical module of T for some $m \in \mathbb{Z}$ by [30, Proposition 1.9]. Thus by Theorem 7.12 and Lemma 2.39 we have ${}^*K_S \cong \operatorname{Ext}^r_T(S,T)$ as ungraded S-modules with $r := \dim(T) - \dim(S)$. Now let $\mathfrak{p} \subset S$ be a prime ideal and $\mathfrak{q} := g^{-1}(\mathfrak{p})$. The S-module $({}^*K_S)_\mathfrak{p} \cong \operatorname{Ext}^r_T(S,T)_\mathfrak{p}$ and the T-module $\operatorname{Ext}^r_T(S,T)_\mathfrak{q}$ coincide since g is surjective; the latter one is isomorphic to $\operatorname{Ext}^r_{T_\mathfrak{q}}(S_\mathfrak{p}, T_\mathfrak{q})$, see Weibel [61, Proposition 3.3.10], so we need to show that $\operatorname{Ext}^r_{T_\mathfrak{q}}(S_\mathfrak{p}, T_\mathfrak{q})$ is the canonical module of $S_\mathfrak{p}$. Since the map $T_\mathfrak{q} \to S_\mathfrak{p}$ induced by g is surjective, by Theorem 7.4 this follows if we prove that $\dim(T_\mathfrak{q}) - \dim(S_\mathfrak{p}) = r$.

Let $I := \ker(g)$. Then $S \cong T/I$ and $S_\mathfrak{p} \cong T_\mathfrak{q}/I_\mathfrak{q}$. Let $\mathfrak{m}$ be the homogeneous maximal ideal in the *local graded ring T. Then up to isomorphism $\mathfrak{m}/I$ is the homogeneous maximal ideal of S. By Lemma 2.33 we have $\dim(T) = \operatorname{ht}(\mathfrak{m}) = \dim(T_\mathfrak{m})$ and $\dim(S) = \dim(T/I) = \operatorname{ht}(\mathfrak{m}/I) = \dim((T/I)_{\mathfrak{m}/I}) = \dim(T_\mathfrak{m}/I_\mathfrak{m})$. Since R is Cohen-Macaulay, T and $T_\mathfrak{m}$ are also Cohen-Macaulay and hence $\dim(T_\mathfrak{m}) - \dim(T_\mathfrak{m}/I_\mathfrak{m}) = \operatorname{ht}(I_\mathfrak{m})$, see Bruns and Herzog [11, Corollary 2.1.4]. So we have $r = \dim(T) - \dim(S) = \dim(T_\mathfrak{m}) - \dim(T_\mathfrak{m}/I_\mathfrak{m}) = \operatorname{ht}(I_\mathfrak{m}) = \operatorname{ht}(I)$ where the last equality follows since I is a homogeneous ideal in T and thus $I \subseteq \mathfrak{m}$. By using the fact that $T_\mathfrak{q}$ is Cohen-Macaulay, we also obtain $\dim(T_\mathfrak{q}) - \dim(S_\mathfrak{p}) = \dim(T_\mathfrak{q}) - \dim(T_\mathfrak{q}/I_\mathfrak{q}) = \operatorname{ht}(I_\mathfrak{q})$ using [11, Corollary 2.1.4] again. Since $\mathfrak{q} = g^{-1}(\mathfrak{p}) \supseteq g^{-1}(\{0\}) = I$ we have $\operatorname{ht}(I_\mathfrak{q}) = \operatorname{ht}(I)$. Hence $r = \operatorname{ht}(I) = \operatorname{ht}(I_\mathfrak{q}) = \dim(T_\mathfrak{q}) - \dim(S_\mathfrak{p})$. This finishes the proof. □

We can now prove the main result of this section which relates graded canonical modules and the quasi-Gorenstein property.

Proposition 7.15. *Let S be a *local graded ring with homogeneous maximal ideal $\mathfrak{m}$ and graded canonical module ${}^*K_S$. Assume that S_0 is Gorenstein. Then the following statements are equivalent:*

(i) S is quasi-Gorenstein.
(ii) $S_\mathfrak{p}$ is quasi-Gorenstein for every $\mathfrak{p} \in \operatorname{Spec}(R)$.
(iii) $S_\mathfrak{m}$ is quasi-Gorenstein.
(iv) There is a homogeneous isomorphism ${}^*K_S \cong S(m)$ for some $m \in \mathbb{Z}$.
(v) ${}^*K_S$ is a free S-module of rank one.

Proof. Statements *(i)* and *(ii)* are equivalent by definition and it is clear that *(ii)* implies *(iii)*. Next we assume that *(iii)* holds. Then by Proposition 7.14 we have $({}^*K_S)_\mathfrak{m} \cong S_\mathfrak{m}$. In particular, $({}^*K_S)_\mathfrak{m}$ is a free $S_\mathfrak{m}$-module and hence its projective dimension is zero. As ${}^*K_S$ is a finitely generated graded S-module, this implies that the projective dimension of ${}^*K_S$ is zero ([11, Proposition 1.5.15(e)]), so ${}^*K_S$ is projective and hence free ([11, Proposition 1.5.15(d)]). Furthermore $\operatorname{rank}({}^*K_S) = \operatorname{rank}({}^*K_S)_\mathfrak{m} = 1$, so ${}^*K_S$ is a graded

free module of rank one. That proves that (iii) implies (iv). It is clear that (iv) implies (v); finally (v) implies (ii) by Proposition 7.14. □

7.3 The Dedekind different

The Dedekind different is a classical tool in algebraic number theory. In his article [8] Broer defines a generalization of the Dedekind different which he calls the twisted different. Broer introduces the twisted different only for extensions $S \supseteq S^G$ where S is the polynomial ring in n variables over a field K and G is a finite subgroup of $Gl_n(K)$. All results on twisted differents given in [8] are direct generalizations of well-known results for the Dedekind different and therefore Broer often does not give proofs. In this section we define twisted differents in the generality needed for what follows and for convenience we give full proofs. At the end of this section we recall a classical result on the Dedekind different; there we only give a reference for the proof. As a general reference for the classical theory of Dedekind differents we mention Benson [4, Section 3.10].

Throughout this section let B be a Noetherian normal domain and let G be a finite group of automorphisms of B. We set $L := \mathrm{Quot}(B)$, $A := B^G$, and $K := \mathrm{Quot}(A) = L^G$ and we assume that A is again Noetherian, see also Remark 5.19. Moreover, we fix a character $\nu : G \to A^\times$; recall that we write B_ν^G or A_ν for the module of ν-semiinvariants.

Definition 7.16. *The twisted transfer is the map*

$$\mathrm{Tr}_\nu^G : L \to L_\nu^G, a \mapsto \sum_{\sigma \in G} \nu(\sigma^{-1})\sigma(a).$$

The twisted transfer is a homomorphism of K-vector spaces which restricts to a homomorphism of A-modules $B \to A_\nu$. Of course, in the case $\nu = 1$ the twisted transfer is the same as the usual transfer $\mathrm{Tr}^G : L \to L^G$. The map $L \times L \to K_\nu, (a, b) \mapsto \mathrm{Tr}_\nu^G(ab)$ is K-bilinear; by Lemma 5.11 we have $K_\nu \cong K$ and we now prove that the above bilinear form is non-degenerate. G is linearly independent as a subset of the L-vector space of all maps $L \to L$, see Lang [39, Chapter VI, Theorem 4.1]. So $\mathrm{Tr}_\nu^G \neq 0$ as it is a nontrivial linear combination of the elements of G and therefore also for every $a \in L\backslash\{0\}$ we have $\mathrm{Tr}_\nu^G(aL) \neq 0$. Hence indeed the above bilinear form is non-degenerate, so it induces an isomorphism of K-vector spaces

$$L \to \mathrm{Hom}_K(L, K_\nu), a \mapsto (b \mapsto \mathrm{Tr}_\nu^G(ab)).$$

If we make $\mathrm{Hom}_K(L, K_\nu)$ into an L-vectorspace by setting $(a\alpha)(b) = \alpha(ab)$ for $\alpha \in \mathrm{Hom}_K(L, K)$ and $a, b \in L$ then this also becomes an isomorphism of L-vector spaces. Since $(A\backslash\{0\})^{-1}B = L$, every homomorphism of A-modules $B \to A_\nu$ extends uniquely to a K-linear homomorphism $L \to K_\nu$, so we can view $\mathrm{Hom}_A(B, A_\nu)$ as a B-submodule of $\mathrm{Hom}_K(L, K_\nu)$. We define an action of the group G on $\mathrm{Hom}_A(B, A_\nu)$ as follows: for $\sigma \in G, \alpha \in \mathrm{Hom}_A(B, A_\nu), b \in B$ we set $\sigma(\alpha)(b) := \sigma(\alpha(\sigma^{-1}(b)))$. Now we make the following definition:

Definition 7.17. *We define the twisted inverse different as the module* $\mathcal{D}^{-1}_{B/A,\nu} := \{b \in \mathrm{Quot}(B) | \mathrm{Tr}^G_\nu(bB) \subseteq A_\nu\}$.

In the case $\nu = 1$ the twisted inverse different is simply called the inverse different and written as $\mathcal{D}^{-1}_{B/A}$.

Lemma 7.18. *Let* $\nu : G \to R^\times$ *be a character. Then the map*

$$\Phi : \mathcal{D}^{-1}_{B/A,\nu} \to \mathrm{Hom}_A(B, A_\nu), a \mapsto (b \mapsto \mathrm{Tr}^G_\nu(ab))$$

is an isomorphism of B*-modules compatible with the* G*-action.*

Proof. The fact that Φ is an isomorphism follows from the discussion preceding the definition of the twisted inverse different. Now let $\sigma \in G, a \in \mathcal{D}^{-1}_{B/A,\nu}, b \in B$. Then we have

$$\begin{aligned}\Phi(\sigma(a))(b) = \mathrm{Tr}^G_\nu(\sigma(a)b) = \sum_{\tau\in G} \nu(\tau^{-1})\tau(\sigma(a\sigma^{-1}(b))) = \sum_{\tau\in G} \nu(\sigma)\nu((\tau\sigma)^{-1})(\tau\sigma)(a\sigma^{-1}(b)) \\ = \nu(\sigma)\mathrm{Tr}^G_\nu(a\sigma^{-1}(b)) = \sigma(\mathrm{Tr}^G_\nu(a\sigma^{-1}(b))) = \sigma(\Phi(a)(\sigma^{-1}(b))) = \sigma(\Phi(a))(b)\end{aligned}$$

where for the fifth equality we use that $\mathrm{Tr}^G_\nu(B) \subseteq A_\nu$. This implies $\Phi(\sigma(a)) = \sigma(\Phi(a))$. □

The twisted inverse different is a fractional ideal of B, so we can consider its inverse.

Definition 7.19. *We define the twisted different as* $\mathcal{D}_{B/A,\nu} := (\mathcal{D}^{-1}_{B/A,\nu})^{-1}$.

In the case $\nu = 1$ the twisted different is the usual Dedekind different and written as $\mathcal{D}_{B/A}$. Since $B \subseteq \mathcal{D}^{-1}_{B/A,\nu}$, the twisted different is an integral ideal. The following lemma follows immediately from the definitions.

Lemma 7.20. *Let* $U \subseteq A\backslash\{0\}$ *be a multiplicatively closed subset. Then* $\mathcal{D}^{-1}_{U^{-1}B/U^{-1}A,\nu} = U^{-1}\mathcal{D}^{-1}_{B/A,\nu}$ *and* $\mathcal{D}_{U^{-1}B/U^{-1}A,\nu} = U^{-1}\mathcal{D}_{B/A,\nu}$.

The next lemma gives a further important property of $\mathcal{D}^{-1}_{B/A,\nu}$ and $\mathcal{D}_{B/A,\nu}$.

Lemma 7.21. *The twisted inverse different* $\mathcal{D}^{-1}_{B/A,\nu}$ *and the twisted different* $\mathcal{D}_{B/A,\nu}$ *are divisorial fractional ideals of* B.

Proof. The twisted inverse different is a reflexive A-module by Lemmas 7.18, 5.11, and 5.4b), so it is a reflexive B-module by Lemma 5.5. The twisted different is divisorial by Remark 5.7. □

Since $\mathcal{D}^{-1}_{B/A,\nu}$ is divisorial, by Remark 5.7 $\mathcal{D}^{-1}_{B/A,\nu}$ is really the inverse of $\mathcal{D}_{B/A,\nu}$.

Lemma 7.22. *Let* C *be a Noetherian normal domain,* $G \subseteq \mathrm{Aut}(C)$ *a finite subgroup and* $N \subseteq G$ *a normal subgroup. Assume that* $A := S^G$ *and* $B := S^N$ *are again Noetherian. Then for every character* $\nu : G \to A^\times$ *which is trivial on* N *we have* $\mathcal{D}_{C/A,\nu} = \overline{\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu}}$. *Here* $\overline{\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu}}$ *denotes the reflexive closure of* $\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu}$ *as a* C*-module.*

Proof. By Remark 5.7 and Lemma 7.21 this follows if we prove $\mathcal{D}_{C/A,\nu}^{-1} = (\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu})^{-1}$. For this, let $a \in \mathrm{Quot}(C)$; then we have

$$\begin{aligned} a \in \mathcal{D}_{C/A,\nu}^{-1} &\Leftrightarrow \mathrm{Tr}_\nu^G(aC) \subseteq A_\nu \Leftrightarrow Tr_\nu^{G/N}(\mathrm{Tr}^N(aC)) \subseteq A_\nu \\ &\Leftrightarrow \mathrm{Tr}_\nu^{G/N}(B \cdot Tr^N(aC)) \subseteq A_\nu \Leftrightarrow \mathrm{Tr}^N(aC) \subseteq \mathcal{D}_{B/A,\nu}^{-1} \\ &\Leftrightarrow \mathrm{Tr}^N(a\mathcal{D}_{B/A,\nu}C) \subseteq B \Leftrightarrow a\mathcal{D}_{B/A,\nu} \subseteq \mathcal{D}_{C/B}^{-1} \\ &\Leftrightarrow a\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu} \subseteq C \Leftrightarrow a \in (\mathcal{D}_{C/B}\mathcal{D}_{B/A,\nu})^{-1}. \end{aligned}$$

□

Remark 7.23. Let A, B, and C be as above and let $\mathfrak{P} \in X^{(1)}(C)$ and $\mathfrak{p} := \mathfrak{P} \cap B$. Then Lemma 7.22 and Proposition 5.9 imply that

$$v_{\mathfrak{P}}(\mathcal{D}_{C/A,\nu}) = v_{\mathfrak{P}}(\mathcal{D}_{C/B,\nu}) + v_{\mathfrak{P}}(\mathcal{D}_{B/A,\nu}C) = v_{\mathfrak{P}}(\mathcal{D}_{C/B,\nu}) + e(\mathfrak{P},\mathfrak{p})v_{\mathfrak{p}}(\mathcal{D}_{B/A,\nu}).$$

Here $v_{\mathfrak{P}}$ and $v_{\mathfrak{p}}$ as usual denote the discrete valuations corresponding to the valuation rings $C_{\mathfrak{P}}$ and $B_{\mathfrak{p}}$.

We end this section by giving some important properties of the Dedekind different which we will also need in the next section and which relate the Dedekind different to the material on ramification from Section 2.2.

Proposition 7.24. (see Benson, [4, Theorem 3.10.2]) *Let $\mathfrak{q} \in X^{(1)}(B)$ and $\mathfrak{p} := \mathfrak{q} \cap A$. Then we have $e(\mathfrak{q},\mathfrak{p}) > 1$ if and only if $\mathcal{D}_{B/A} \subseteq \mathfrak{q}$; here $e(\mathfrak{q},\mathfrak{p})$ is the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$.*

We can now prove a further proposition, which relates the Dedekind different to the notion of pseudoreflections.

Proposition 7.25. *Let F be a field, let $S := F[x_1,\ldots,x_n]$ be the polynomial ring in n variables over F, and let $G \subseteq Gl_n(F)$ be a finite group; as usual we view the elements of G as automorphisms of S. Let $N \subseteq G$ be the subgroup generated by all pseudoreflections. Then $\mathcal{D}_{S^N/S^G} = (1)$.*

Proof. Let $\mathfrak{P} \in X^{(1)}(S^N)$. Since $S^N \subseteq S$ is an integral extension, there is a $\mathfrak{Q} \in X^{(1)}(S)$ such that $\mathfrak{P} = \mathfrak{Q} \cap S^N$. By Proposition 2.16, $G^i(\mathfrak{Q}) \subseteq N$ and hence $S^N \subseteq S^{G^i(\mathfrak{Q})}$. By Lemma 2.11 and Lemma 2.10 we have $e(\mathfrak{Q} \cap S^{G^i(\mathfrak{Q})}, \mathfrak{P} \cap S^G) = 1$, so $e(\mathfrak{P},\mathfrak{P} \cap S^G) = 1$ by Lemma 2.8 and hence $\mathcal{D}_{S^N/S^G} \not\subseteq \mathfrak{P}$ by Proposition 7.24, so $v_{\mathfrak{P}}(\mathcal{D}_{S^N/S^G}) = 0$; this implies $\mathrm{div}(\mathcal{D}_{S^N/S^G}) = 0$. Since $\mathcal{D}_{S^N/S^G}$ is divisorial, we thus have $\mathcal{D}_{S^N/S^G} = (1)$ by Proposition 5.9. □

7.4 The differential character and Broer's theorem

In this section we formulate Broer's [8] generalization of Theorem 2.21 to groups which may contain pseudoreflections. The main goal of this chapter is then to generalize this further to arithmetic invariants.

For the statement of Broer's theorem we need the notion of the differential character, see Broer [8, Section 2.1]. Let R be a Noetherian factorial domain, $S := R[x_1, \ldots, x_n]$, and $G \subseteq Gl_n(R)$ a finite group. We need the following lemma:

Lemma 7.26. *With the notation as above, the Dedekind different $\mathcal{D}_{S/S^G}$ is a principal ideal in S.*

Proof. By Lemma 7.21 $\mathcal{D}_{S/S^G}$ is a divisorial ideal in S. Since we assumed R to be factorial, S is also factorial, so $\mathrm{Cl}(S) = \{0\}$ by Theorem 5.14. But this implies that every divisorial ideal in S is principal, so the lemma follows. □

Let $\theta \in S$ be a generator of $\mathcal{D}_{S/S^G}$. Since $\mathcal{D}_{S/S^G}$ is invariant under the action of G, for every $\sigma \in G$ we obtain that $\sigma(\theta)$ also generates $\mathcal{D}_{S/S^G}$ and hence $\sigma(\theta) = \chi(\sigma)\theta$ for some $\chi(\sigma) \in S^\times = R^\times$. The map $\chi : G \to R^\times$ is a group homomorphism which is independent of the choice of θ.

Definition 7.27. *The character $\chi : G \to R^\times$ defined above is called the differential character of G.*

The following result is implicitly used several times in Broer's article [8].

Proposition 7.28. *Let R, S, and G be as above and let χ be the differential character of G. If G is a pseudoreflection group, then $\chi = \det$.*

Since Broer does not give a proof for this proposition, for convenience we prove it here. We need the following lemma for the field case which is proven in [8, Lemma 5]. Formally this lemma is a consequence of Broer's main theorem which we state below; however, as it is used in the proof of that theorem in [8], it should really be stated separately.

Lemma 7.29. *Let K be a field, $S := K[x_1, \ldots, x_n]$, and $G \subseteq Gl_n(R)$ a finite group. Let $\mathcal{F} \subseteq S^G$ be a graded K-subalgebra which is Gorenstein such that S^G is finitely generated as an $\mathcal{F}$-module. Then ${}^*\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}(m)) \cong S$ for some $m \in \mathbb{Z}$ as a graded S-module and for a generator α of ${}^*\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}(m))$ we have $\sigma(\alpha) = \det(\sigma)^{-1}\alpha$ for all $\sigma \in Gl_n(K)$. Here the G-action on ${}^*\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}(m))$ is defined in the same way as before Definition 7.17.*

Note that in the situation of the lemma ${}^*\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}(m))$ is a graded canonical module of S for some $m \in \mathbb{N}$, so the first part of the lemma follows from Proposition 7.15.

Proof of Proposition 7.28. Let θ be a generator of $\mathcal{D}_{S/S^G}$. With $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$ we obtain from Lemma 7.20 that θ also generates $\mathcal{D}_{S_K/S_K^G}$, so we may assume that R is a field.

Let $\sigma \in G$ be a pseudoreflection. If σ is a transvection, then $\mathrm{ord}(\sigma) = \mathrm{char}R =: p$ and hence we have $\chi(\sigma)^p = 1 \in R$. In a field of characteristic p, this is only possible if $\chi(\sigma) = 1$ and by the same argument we get $\det(\sigma) = 1$.

So from now on we assume that σ is diagonalizable; hence there is a basis B of R^n with respect to which σ is given by a matrix of the form

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

Let $B^* = \{f_1, \dots, f_n\}$ be the dual basis of $(R^n)^* \subseteq S$. Then with $H \coloneqq \langle \sigma \rangle \subseteq G$ we obtain $S^H = R[f_1^{|H|}, f_2, \dots, f_n]$; since we assumed that R is a field, this follows from Lemma 4.3. Let θ_1 be a generator of $\mathcal{D}_{S/S^H}$, which is principal by Lemma 7.26. Then $\frac{1}{\theta_1}$ generates $\mathcal{D}_{S/S^H}^{-1}$ and S^H is isomorphic to a polynomial ring over R by the above, hence Gorenstein. By Lemma 7.18 we have $\mathcal{D}_{S/S^H}^{-1} \cong \mathrm{Hom}_{S^H}(S, S^H)$; therefore by Lemmas 7.29 and 2.39 we have $\sigma(\theta_1) = \det(\sigma)\theta_1$. Since S^H is isomorphic to a polynomial ring, it is factorial, so $\mathcal{D}_{S^H/S^G}$ is a principal ideal; let θ_2 be a generator. Since $\theta_2 \in S^H$ we have $\sigma(\theta_2) = \theta_2$. Now Lemma 7.22 implies that $\theta_1\theta_2$ is a generator of $\mathcal{D}_{S/S^G}$. We have $\sigma(\theta_1\theta_2) = \sigma(\theta_1)\sigma(\theta_2) = \det(\sigma)\theta_1\theta_2$ and hence $\chi(\sigma) = \det(\sigma)$. As G is generated by pseudoreflections, this finishes the proof. □

In Broer's article [8] the definition of the differential character appears only in the case that R is a field. For this case we can now state Broer's theorem on the quasi-Gorenstein property of rings of invariants.

Theorem 7.30. (Broer [8]) *Let K be a field, $S \coloneqq K[x_1, \dots, x_n]$, and let $G \subseteq Gl_n(K)$ be a finite group. Then the ring of invariants S^G is quasi-Gorenstein if and only if the differential character $\chi : G \to K^\times$ is equal to the determinant.*

Assume that G does not contain any pseudoreflections. Then by Proposition 7.25 we obtain $\mathcal{D}_{S/S^G} = (1)$ and hence $\chi = 1$. In this case Broer's theorem states that S^G is quasi-Gorenstein if and only if $\det|_G = 1$, so we get back Theorem 2.21 as a special case.

7.5 Systems of parameters

An important object in Broer's discussion of the quasi-Gorenstein property and also in invariant theory in general is a homogeneous system of parameters. In this section we prove a general existence theorem for such systems of parameters. This is basically a reformulation of recent results in algebraic geometry.

Definition 7.31. *Let R be a ring and let S be a finitely generated graded R-algebra. A homogeneous system of parameters in S is a sequence of homogeneous elements $f_1, \dots, f_m \in S$ which are algebraically independent over R such that S is finitely generated as a module over $R[f_1, \dots, f_m]$.*

The importance of systems of parameters for us comes from the following: let R and S be as in the definition; the object we are interested in is the graded canonical module of S. In order to apply Theorem 7.12 we need a graded R-algebra $\mathcal{F}$ which is Cohen-Macaulay and for which we know the graded canonical module together with a finite homogeneous homomorphism $\mathcal{F} \to S$. If R is Gorenstein, we can try to take $\mathcal{F}$ to be a polynomial ring over R; then $\mathcal{F}$ is again Gorenstein, so the graded canonical module of $\mathcal{F}$ is just $\mathcal{F}(m)$ for some $m \in \mathbb{Z}$. This is always possible: since S is finitely generated as an R-algebra, we can always find a surjective homogeneous homomorphism $\mathcal{F}_1 := R[x_1, \ldots, x_s] \to S$ for some $s \in \mathbb{N}$ with suitable choices for the degrees of the x_i. However, the description of the canonical module of S given in Theorem 7.12 becomes particularly simple if $\dim \mathcal{F} = \dim S$ and we cannot expect this to happen with $\mathcal{F} = \mathcal{F}_1$. On the other hand, if S contains a homogeneous system of parameters $f_1, \ldots, f_m$ and we set $\mathcal{F}_2 := R[f_1, \ldots, f_m]$, then the inclusion $\mathcal{F}_2 \to S$ certainly has the desired properties and we have $\dim \mathcal{F}_2 = \dim S$ because S is then finitely generated as an $\mathcal{F}_2$-module.

If R is a field then every finitely generated graded R-algebra has a system of parameters by the Noether normalization lemma, see Derksen and Kemper [16, Corollary 2.5.8]. But Noether normalization is not available over rings, so we cannot use this here. In the case $R = \mathbb{Z}$, recent work of Bruce and Erman [10, Corollary 7.5] provides the following result:

Theorem 7.32. *Let S be a graded ring which is finitely generated as an algebra over $S_0 = \mathbb{Z}$. Assume that there exists a $d \in \mathbb{N}$ such that $\dim(S \otimes_{\mathbb{Z}} \mathbb{F}_p) = d$ for all primes $p \in \mathbb{Z}$. Then there exist homogeneous elements $f_1, \ldots, f_d \in S$ such that $\mathbb{Z}[f_1, \ldots, f_d] \subseteq S$ is a finite extension.*

We now want to prove a similar result for more general base rings. Theorem 7.32 appears in [10] as a corollary of a geometric result ([10, Corollary 1.3]). This geometric result has been proved over more general rings independently by Gabber et al. [21] and Chinburg et al. [13]; in order to state their result, we need the following definition.

Definition 7.33. (Gabber et al. [21, Definition 0.3]) *A ring R is called a pictorsion ring if for every R-algebra R' which is finitely generated as an R-module the Picard group $\mathrm{Pic}(R')$ is a torsion group.*

We are mainly interested in the case where R is local and local rings are always pictorsion; nevertheless, systems of parameters may also be interesting in their own right, so we give some more examples of pictorsion rings.

Example 7.34.

(a) Every semilocal ring is a pictorsion ring; this is mentioned in [21] right after the definition of a pictorsion ring.

(b) The ring of integers in a number field is always a pictorsion ring; this follows from [21, Lemma 8.10(2)].

(c) The next example shows that a Dedekind domain with finite ideal class group need not be pictorsion; recall that the Picard group of a Dedekind domain is isomorphic to its ideal class group. Let $E/\mathbb{Q}$ be an elliptic curve of rank greater than zero. Then the affine coordinate ring $R = \mathbb{Q}[E]$ is finitely generated as a module over the

polyomial ring $\mathbb{Q}[x]$ and the Picard group of E is isomorphic to E with the usual group structure of an elliptic curve; by assumption, this is not a torsion group. Hence $\mathbb{Q}[x]$ is not pictorsion.

(d) On the other hand, for a prime number p let $\overline{\mathbb{F}_p}$ be an algebraic closure of the finite field $\mathbb{F}_p$. Then $\overline{\mathbb{F}_p}[x]$ is pictorsion, see [21, Example 8.15].

Theorem 7.35. (Gabber et al. [21, Theorem 8.1]) *Let R be a pictorsion ring, let X be a scheme, and let $g : X \to \operatorname{Spec}(R)$ be a projective morphism of schemes. Assume that there exists a $d \in \mathbb{N}$ such that $\dim X_s = d$ for every $s \in \operatorname{Spec}(R)$ where X_s denotes the fiber of g at s. Then there is a finite surjective R-morphism $r : X \to \mathbb{P}^d_R$.*

Remark 7.36. The proof of Theorem 7.35 given in [21] shows that in fact the following more precise statement holds: let R, X, and g be as in the theorem. For simplicity, we assume that R is Noetherian and g is of finite type. Since g is projective, we can view X as a closed subscheme of $P \coloneqq \mathbb{P}^n_R$ for some $n \in \mathbb{N}$. Then there are an integer $m \in \mathbb{N}$ and global sections $f_1, \ldots, f_d \in \Gamma(P, \mathcal{O}_P(m))$ which induce a morphism $\hat{r} : P \to \mathbb{P}^{d-1}_R$ such that $r \coloneqq \hat{r}|_X$ is a finite surjective morphism $X \to \mathbb{P}^{d-1}_R$.

Now we can prove the desired generalization of Theorem 7.32. For simplicity, we only consider the case where S is an integral domain.

Corollary 7.37. *Let R be a Noetherian pictorsion ring and let S be a finitely generated graded R-algebra which is an integral domain. Assume that there exists a number $d \in \mathbb{N}$ such that for all $\mathfrak{p} \in \operatorname{Spec}(R)$ we have $\dim(S \otimes_R \operatorname{Quot}(R/\mathfrak{p})) = d$. Then S contains a homogeneous system of parameters consisting of d elements.*

The following proof is basically the same as the proof of Theorem 7.32 given in [10].

Proof. Let $f_1, \ldots, f_n \in S$ be homogemeous elements which generate S as an R-algebra; the case $n = 0$ is clear, so we may assume $n > 0$. We define $e \coloneqq \operatorname{lcm}(\deg(f_1), \ldots, \deg(f_n))$ and $f'_i \coloneqq f_i^{\frac{e}{\deg(f_i)}}$. Then $\deg(f'_i) = e$ for each i and S is integral over $S' \coloneqq R[f'_1, \ldots, f'_n]$. We can change the grading on S' in such a way that each f'_i is of degree one and therefore we get a closed immersion $\iota : X \coloneqq \operatorname{Proj} S' \to P \coloneqq \mathbb{P}^{n-1}_R$ (see Hartshorne [27, Chapter II, Exercise 3.12]). Moreover, there is a canonical projective morphism $g : X \to \operatorname{Spec}(R)$ (see [27, Chapter II, Example 4.8.1]); by assumption all fibers of g are of dimension $d-1$. Then by Remark 7.36 there are $m \in \mathbb{N}$ and $h_1, \ldots, h_d \in \Gamma(P, \mathcal{O}_P(m))$ which induce a morphism $\hat{r} : P \to \mathbb{P}^{d-1}_R$ such that $r \coloneqq \hat{r}|_X$ is a finite surjective morphism $X \to \mathbb{P}^{d-1}_R$; hence with $\mathbb{P}^{d-1}_R = \operatorname{Proj}(R[z_1, \ldots, z_d])$ we have $h_i = \hat{r}^*(z_i)$. We set $h'_i \coloneqq \iota^*(h_i) = (\hat{r} \circ \iota)^*(z_i) = r^*(z_i)$; then r is induced by $h'_1, \ldots, h'_d \in \Gamma(X, \iota^*(\mathcal{O}_P(m))) = \Gamma(X, \mathcal{O}_X(m)) \cong S'_m$ (see [27, Chapter II, Propositions 5.12 and 5.15]). Since S' is an integral domain it is the homogeneous coordinate ring of X, so r induces a ring homomorphism $R[x_1, \ldots, x_d] \to S'$ mapping x_i to h'_i such that S' is a finitely generated $R[x_1, \ldots, x_d]$-module. Hence S' and thus also S is a finitely generated $R[h'_1, \ldots, h'_d]$-module. Then also $S \otimes_R \operatorname{Quot}(R)$ is a finitely generated $\operatorname{Quot}(R)[h'_1, \ldots, h'_d]$-module and hence $\dim(\operatorname{Quot}(R)[h'_1, \ldots, h'_d]) = \dim(S \otimes_R \operatorname{Quot}(R)) = d$ by assumption. This shows that $h'_1, \ldots, h'_d$ indeed form a system of parameters. □

In the special case where S is a ring of invariants we obtain the following result:

Corollary 7.38. *Let R be a Noetherian pictorsion ring which is an integral domain, $S := R[x_1, \ldots, x_n]$ and let $G \subseteq Gl_n(R)$ be a finite group. Then S^G contains a homogeneous system of parameters consisting of n elements.*

Proof. Since R is Noetherian, S^G is a finitely generated R-algebra. By Corollary 7.37 the only thing we need to show is that for every $\mathfrak{p} \in \operatorname{Spec}(R)$ we have $\dim(S^G \otimes_R \operatorname{Quot}(R/\mathfrak{p})) = n$. We can view $S^G \otimes_R \operatorname{Quot}(R/\mathfrak{p})$ as a subring of $(S \otimes_R \operatorname{Quot}(R/\mathfrak{p}))^G = \operatorname{Quot}(R/\mathfrak{p})[x_1, \ldots, x_n]^G$; the latter is of dimension n, so it is sufficient to prove that $S^G \otimes_R \operatorname{Quot}(R/\mathfrak{p}) \subseteq \operatorname{Quot}(R/\mathfrak{p})[x_1, \ldots, x_n]^G$ is an integral extension. For this let $f \in \operatorname{Quot}(R/\mathfrak{p})[x_1, \ldots, x_n]^G$ and choose $a \in (R/\mathfrak{p}) \backslash \{0\}$ such that $af \in (R/\mathfrak{p})[x_1, \ldots, x_n]^G$. Then there is a $g \in S$ such that af is obtained from g be reducing all coefficients modulo $\mathfrak{p}$. We define $h := \prod_{\sigma \in G} \sigma(g) \in S^G$. Since f is already invariant, reducing the coefficients of h modulo $\mathfrak{p}$ just gives $(af)^{|G|}$. So $f^{|G|} = \frac{1}{a^{|G|}}(af)^{|G|} \in S^G \otimes_R \operatorname{Quot}(R/\mathfrak{p})$ and hence f is integral over $S^G \otimes_R \operatorname{Quot}(R/\mathfrak{p})$. □

At this point, we can already give a first application in invariant theory:

Theorem 7.39. *Let R be a Dedekind domain, $\mathfrak{m} \subset R$ a maximal ideal, and $F := R/\mathfrak{m}$. Furthermore, let $G \subseteq Gl_n(R)$ be a finite group such that $|G| \notin \mathfrak{m}$ and $R[x_1, \ldots, x_n]^G$ is quasi-Gorenstein. Then $F[x_1, \ldots, x_n]^G$ is a Gorenstein ring.*

Proof. Since $F \cong R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}$, we may restrict ourselves to the case where R is local with maximal ideal $\mathfrak{m}$ and hence a discrete valuation ring, so $\mathfrak{m} =: (p)$ is a principal ideal; then $|G|$ is invertible in R and in F. We define $S := R[x_1, \ldots, x_n]$ and $S_F := F[x_1, \ldots, x_n]$; by Theorems 2.20 and 3.14, S_F^G and S^G are Cohen-Macaulay. By Corollary 7.38, there is a homogeneous system of parameters $f_1, \ldots, f_n$ in S^G; we define $\mathcal{F} := R[f_1, \ldots, f_n]$. Let $\mathfrak{q} \subset S^G$ be a prime ideal and set $\mathfrak{p} := \mathfrak{q} \cap \mathcal{F}$. Since $\mathcal{F} \subseteq S^G$ is a finite extension, we have $\dim(\mathcal{F}_{\mathfrak{p}}) = \dim(S^G_{\mathfrak{q}})$ and $\dim(S^G_{\mathfrak{q}}/\mathfrak{p}S^G_{\mathfrak{q}}) = 0$. Furthermore, $\mathcal{F}$ is regular and S^G is Cohen-Macaulay, so $S^G_{\mathfrak{q}}$ is a flat $\mathcal{F}_{\mathfrak{p}}$-module (see Matsumura [41, Theorem 23.1]) and hence S^G is a flat $\mathcal{F}$-module (see [41, Theorem 7.1]). Since S^G is a finitely generated module over the Noetherian ring $\mathcal{F}$, it is therefore projective and hence free since it is a graded $\mathcal{F}$-module and $\mathcal{F}$ is *local (see Bruns and Herzog [11, Proposition 1.5.15(d)]). Let $g_1, \ldots, g_m$ be a basis of S^G as an $\mathcal{F}$-module. For a polynomial $f \in S$ let $\overline{f}$ denote the class of f in S_F; we write $\mathcal{F}_F := F[\overline{f_1}, \ldots, \overline{f_n}] \cong \mathcal{F} \otimes_R F$. Since the projection map $S^G \to S_F^G$ is surjective by Lemma 3.4, S_F^G is generated by $\overline{g_1}, \ldots, \overline{g_m}$ as an $\mathcal{F}_F$-module; in particular, $\overline{f_1}, \ldots, \overline{f_n}$ form a system of parameters in S_F^G.

Since we already know that S_F^G is Cohen-Macaulay, we need to show that it is quasi-Gorenstein. By Theorem 7.12 we obtain that $\operatorname{Hom}_{\mathcal{F}_F}(S_F^G, \mathcal{F}_F(m))$ is a graded canonical module of S_F^G for some $m \in \mathbb{Z}$, so by Proposition 7.15 it is sufficient to prove that $\operatorname{Hom}_{\mathcal{F}_F}(S_F^G, \mathcal{F}_F) \cong S_F^G$ as a non-graded S_F^G-module. We prove that $\operatorname{Hom}_{\mathcal{F}_F}(S_F^G, \mathcal{F}_F) \cong \operatorname{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \otimes_{S^G} S_F^G$. Then the claim follows since $\operatorname{Hom}_{\mathcal{F}}(S^G, \mathcal{F}(m'))$ is a graded canonical module of S^G for some $m' \in \mathbb{Z}$ and S^G is quasi-Gorenstein by assumption.

We have a canonical homomorphism of S^G-modules

$$\psi : \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \otimes_{S^G} S_F^G \to \mathrm{Hom}_{\mathcal{F}_F}(S_F^G, \mathcal{F}_F)$$

given by $\psi(\beta \otimes \overline{s})(\overline{t}) := \overline{\beta(st)}$ for all $\beta \in \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ and $s, t \in S^G$. Every element of $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \otimes_{S^G} S_F^G$ is of the form $\beta \otimes \overline{1}$ for some $\beta \in \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$. If $\psi(\beta \otimes \overline{1}) = 0$, this means that $\overline{\beta(f)} = 0$ for all $f \in S^G$, so every $\beta(f)$ is divisible by p; hence β is divisible by p in $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$, so $\beta \otimes \overline{1} = 0$. This shows that ψ is injective. Now let $\alpha \in \mathrm{Hom}_{\mathcal{F}_F}(S_F^G, \mathcal{F}_F)$ and write $\alpha(\overline{g_i}) = \overline{h_i}$ for all $i = 1, \ldots, m$ with $h_i \in \mathcal{F}$. Since S^G is a free $\mathcal{F}$-module with basis $g_1, \ldots, g_m$, we can define a $\beta \in \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ via $\beta(g_i) = h_i$. Then $\psi(\beta \otimes \overline{1}) = \alpha$, so ψ is also surjective. □

7.6 The canonical module of a ring of invariants over a local ring

In this section let R always be a local domain which is Gorenstein and factorial and let $S := R[x_1, \ldots, x_n]$. As usual, we set $K := \mathrm{Quot}(R)$ and $S_K := S \otimes_R K$. Moreover we fix a finite subgroup $G \subseteq Gl_n(R)$. The goal of this section is to compute the graded canonical module of S^G. This has been done by Broer [8] in the case where R is a field and we mainly follow his approach here. We start with the following technical lemma:

Lemma 7.40. *Let $A \subseteq S^G$ be a normal graded R-subalgebra of S^G such that S^G is a finitely generated A-module and let $\mathfrak{p} \in X^{(1)}(A)$. Then $(S^G)_{\mathfrak{p}}$ is a direct summand of $S_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module.*

Proof. S^G and hence also S are finitely generated A-modules, so $(S^G)_{\mathfrak{p}}$ and $S_{\mathfrak{p}}$ are finitely generated $A_{\mathfrak{p}}$-modules. Furthermore, they are clearly torsion-free as $A_{\mathfrak{p}}$-modules. Since A is normal and $\mathrm{ht}(\mathfrak{p}) = 1$, $A_{\mathfrak{p}}$ is a discrete valuation ring and in particular a principal ideal domain. So $S_{\mathfrak{p}}$ and $(S^G)_{\mathfrak{p}}$ are finitely generated free $A_{\mathfrak{p}}$-modules and hence there exist a basis $b_1, \ldots, b_l$ of $S_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module and $\alpha_1, \ldots, \alpha_k \in A_{\mathfrak{p}}$ $(k \leq l)$ such that $\alpha_1 b_1, \ldots, \alpha_k b_k$ is a basis of $(S^G)_{\mathfrak{p}}$. For $1 \leq i \leq k$ b_i is G-invariant since α_i and $\alpha_i b_i$ are G-invariant, so $b_i \in (S_{\mathfrak{p}})^G = (S^G)_{\mathfrak{p}}$ (see Bourbaki [5, Chapter V, §1.9, Proposition 23]); hence we have $b_i \in \langle \alpha_1 b_1, \ldots, \alpha_k b_k \rangle_{A_{\mathfrak{p}}}$. Since $b_1, \ldots, b_k$ are linearly independent over $A_{\mathfrak{p}}$, this implies $\alpha_i \in A_{\mathfrak{p}}^{\times}$. Hence $(S^G)_{\mathfrak{p}} = \langle b_1, \ldots, b_k \rangle$, so we have $S_{\mathfrak{p}} = (S^G)_{\mathfrak{p}} \oplus \langle b_{k+1}, \ldots, b_l \rangle$. □

Remark 7.41. In the special case where R is a field and $A = S^G$ the above lemma is contained in the proof of [8, Lemma 3(i)]. However, Broer's proof of this seems to be wrong: he considers the transfer $\mathrm{Tr}^G : S_{\mathfrak{p}} \to (S^G)_{\mathfrak{p}}$. Since $(S^G)_{\mathfrak{p}}$ is a discrete valuation ring, the image of this map is a principal ideal (a) in $(S^G)_{\mathfrak{p}}$. Now he claims that the map $\frac{1}{a}\mathrm{Tr}^G$ is a projection map from $S_{\mathfrak{p}}$ to $(S^G)_{\mathfrak{p}}$. But if $|G|$ divides $\mathrm{char}(R)$, then Tr^G maps every element of $(S^G)_{\mathfrak{p}}$ to zero and hence the same is true for $\frac{1}{a}\mathrm{Tr}^G$, which therefore cannot be a projection. The proof given above avoids this problem.

By Corollary 7.38 there are homogeneous elements $f_1, \ldots, f_n \in S^G$ which form a homogeneous system of parameters; we define $\mathcal{F} := R[f_1, \ldots, f_n]$. Then by Theorem 7.12 ${}^*\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}(m))$ is the graded canonical module of the graded ring S^G for some $m \in \mathbb{Z}$. In the following we will ignore the grading on this module; we can do this as we are only interested in the quasi-Gorenstein property of S^G and therefore by Proposition 7.15 we only need to check when the graded canonical module is free of rank one and this does not depend on the grading. So we want to find an easy description of the S^G-module $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}(m)) \cong \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$, see Lemma 2.39. Here we define the S^G-module structure on $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ in the usual way: for $a, b \in S^G$ and $\alpha \in \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ we set $(a\alpha)(b) := \alpha(ab)$. Now let $\iota : S^G \to S$ be the inclusion and let $\iota^* : \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}) \to \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ be its dual map. Then ι^* is a homomorphism of S^G-modules.

Lemma 7.42. *We have* $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) = \overline{\mathrm{im}(\iota^*)}$ *where* $\overline{\mathrm{im}(\iota^*)}$ *denotes the reflexive closure of* $\mathrm{im}(\iota^*)$ *as an* S^G*-module.*

Proof. By Lemma 5.2 we have

$$\overline{\mathrm{im}(\iota^*)} = \bigcap_{\mathfrak{q} \in X^{(1)}(S^G)} (\mathrm{im}(\iota^*))_{\mathfrak{q}}.$$

For every $\mathfrak{q} \in X^{(1)}(S^G)$ we have $(\mathrm{im}(\iota^*))_{\mathfrak{q}} = \mathrm{im}(\iota^*_{\mathfrak{q}})$ where $\iota^*_{\mathfrak{q}}$ denotes the localized map $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})_{\mathfrak{q}} \to \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})_{\mathfrak{q}}$. We claim that $\iota^*_{\mathfrak{q}}$ is surjective. Let $\mathfrak{p} := \mathcal{F} \cap \mathfrak{q}$. Then $(S^G)_{\mathfrak{p}}$ is a direct summand of $S_{\mathfrak{p}}$ as an $\mathcal{F}_{\mathfrak{p}}$-module by Lemma 7.40, so the induced map $\mathrm{Hom}_{\mathcal{F}_{\mathfrak{p}}}(S_{\mathfrak{p}}, \mathcal{F}_{\mathfrak{p}}) \to \mathrm{Hom}_{\mathcal{F}_{\mathfrak{p}}}(S^G_{\mathfrak{p}}, \mathcal{F}_{\mathfrak{p}})$ is surjective. This implies that the map $\iota^*_{\mathfrak{p}} : \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})_{\mathfrak{p}} \to \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})_{\mathfrak{p}}$ is also surjective (see Eisenbud [17, Proposition 2.10]). This is in fact a homomorphism of $(S^G)_{\mathfrak{p}} = (\mathcal{F} \backslash \mathfrak{p})^{-1} S^G$-modules, so localizing it at the prime ideal $(\mathcal{F} \backslash \mathfrak{p})^{-1}\mathfrak{q}$ gives the claimed surjectivity of $\iota^*_{\mathfrak{q}}$. So we have proved:

$$\overline{\mathrm{im}(\iota^*)} = \bigcap_{\mathfrak{q} \in X^{(1)}(S^G)} \mathrm{im}(\iota^*_{\mathfrak{q}}) = \bigcap_{\mathfrak{q} \in X^{(1)}(S^G)} \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})_{\mathfrak{q}} = \overline{\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})},$$

where the last step again follows from Lemma 5.2. But $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ is reflexive as an $\mathcal{F}$-module by Lemma 5.4b) and hence also as an S^G-module by Lemma 5.5, so the statement follows. □

Using the twisted transfer introduced in the previous section, we can formulate the next lemma:

Lemma 7.43. *Let* $\iota^* : \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}) \to \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ *be as above. Then* $\mathrm{im}(\iota^*) \cong \mathrm{im}(\mathrm{Tr}^G_{\det})$ *as* S^G*-modules.*

For the proof of this we also need the usual transfer $\mathrm{Tr}^G : S \to S^G$ and its dual map $(\mathrm{Tr}^G)^* : \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \to \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ for which we have the following result due to Broer:

Lemma 7.44. (Broer) $(\mathrm{Tr}^G)^* : \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \to \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ *is injective.*

This result apparently appeared first in a preprint by Broer which does not seem to be publicly available and the only other reference for it I am aware of is the first edition of Derksen's and Kemper's book [15, Lemma 3.9.7]. So for convenience I include the proof taken from that book here.

Proof of Lemma 7.44. We have $\mathrm{Quot}(S^G) = \mathrm{Quot}(S)^G$, so $\mathrm{Quot}(S)/\mathrm{Quot}(S^G)$ is a Galois extension with Galois group G. We can extend Tr^G to the trace map $\mathrm{Quot}(S) \to \mathrm{Quot}(S)^G = \mathrm{Quot}(S^G)$. Since $\mathrm{Quot}(S)/\mathrm{Quot}(S^G)$ is separable, $\mathrm{Tr}^G : \mathrm{Quot}(S) \to \mathrm{Quot}(S^G)$ is surjective, see Lang [39, Chapter VI, Theorem 5.2], and hence there are $f, g \in S, g \neq 0$ such that $\mathrm{Tr}^G(\frac{f}{g}) = 1$. Since $\mathcal{F} \subseteq S$ is an integral extension, we have $\mathrm{Quot}(S) = (\mathcal{F}\backslash\{0\})^{-1}S$, so we may assume that $g \in \mathcal{F}$. Then we have $1 = \frac{1}{g}\mathrm{Tr}^G(f)$ since $g \in \mathcal{F} \subseteq S^G$ and hence $g = \mathrm{Tr}^G(f)$. Now let $\varphi \in \mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ such that $(\mathrm{Tr}^G)^*(\varphi) = 0$. Then for every $h \in S^G$ we have

$$0 = (\mathrm{Tr}^G)^*(\varphi)(fh) = \varphi(\mathrm{Tr}^G(fh)) = \varphi(h\mathrm{Tr}^G(f)) = \varphi(hg) = g\varphi(h).$$

Since $g \neq 0$, this implies $\varphi = 0$ and hence $(\mathrm{Tr}^G)^*$ is indeed injective. □

Proof of Lemma 7.43. Since $(\mathrm{Tr}^G)^*$ is injective by Lemma 7.44, we have $\mathrm{im}(\iota^*) \cong \mathrm{im}((\mathrm{Tr}^G)^* \circ \iota^*)$ and we now compute the image of $(\mathrm{Tr}^G)^* \circ \iota^* : \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}) \to \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$. Here $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ is the graded canonical module of S except that we ignore the grading by Theorem 7.12 and $S = R[x_1, \ldots, x_n]$ is Gorenstein since R is Gorenstein, so $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}) \cong S$ by Proposition 7.15. Let $\phi \in \mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ be a generator. Then the way we defined the S-module structure on $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ shows that every element of $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ is of the form $g \mapsto \phi(fg)$ for some $f \in S$. Following Broer, we write $\phi \circ f$ for this map. Then we have for all $f, f' \in S$:

$$\begin{aligned}(\mathrm{Tr}^G)^*(\iota^*(\phi \circ f))(f') &= ((\phi \circ f) \circ \iota \circ \mathrm{Tr}^G)(f') = (\phi \circ f)(\mathrm{Tr}^G(f')) \\ &= \phi(f\mathrm{Tr}^G(f')) = \phi(f(\sum_{\sigma \in G} \sigma f')) = \sum_{\sigma \in G} \phi(f \cdot \sigma f').\end{aligned}$$

Using the G-action on $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ as defined before Definition 7.17 and the fact that $\mathcal{F} \subseteq S^G$ we have

$$\sum_{\sigma \in G} \phi(f \cdot \sigma f') = \sum_{\sigma \in G} (\sigma^{-1}\phi)(\sigma^{-1}(f \cdot \sigma f')) = \sum_{\sigma \in G} (\sigma^{-1}\phi)(\sigma^{-1}f \cdot f').$$

But we know what $\sigma^{-1}\phi$ is: we set $\mathcal{F}_K \coloneqq \mathcal{F} \otimes_R K$; then ϕ also generates $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F}) \otimes_R K \cong \mathrm{Hom}_{\mathcal{F}_K}(S_K, \mathcal{F}_K)$ and thus $\sigma^{-1}\phi = \det(\sigma) \cdot \phi$ by Lemma 7.29. So with the above calculations we obtain

$$\begin{aligned}(\mathrm{Tr}^G)^*(\iota^*(\phi \circ f))(f') &= \sum_{\sigma \in G} \phi(f \cdot \sigma f') = \sum_{\sigma \in G} \det\sigma \cdot \phi(\sigma^{-1}f \cdot f') \\ &= \phi\left(\left(\sum_{\sigma \in G} \det\sigma \cdot \sigma^{-1}f\right) \cdot f'\right) = \phi\left(\left(\sum_{\sigma \in G} \det\sigma^{-1} \cdot \sigma f\right) \cdot f'\right) \\ &= \phi(\mathrm{Tr}^G_{\det}(f) \cdot f') = (\phi \circ \mathrm{Tr}^G_{\det}(f))(f').\end{aligned}$$

This proves that $(\mathrm{Tr}^G)^*(\iota^*(\phi \circ f)) = \phi \circ \mathrm{Tr}^G_{\det}(f)$ for every $f \in S$ and hence

$$\mathrm{im}(\iota^*) \cong \mathrm{im}((\mathrm{Tr}^G)^* \circ \iota^*) = \{\phi \circ \mathrm{Tr}^G_{\det}(f) | f \in S\}.$$

But $\mathrm{Hom}_{\mathcal{F}}(S, \mathcal{F})$ is a free S-module generated by ϕ, so this is isomorphic to $\{\mathrm{Tr}^G_{\det}(f) | f \in S\} = \mathrm{im}(\mathrm{Tr}^G_{\det})$. □

So it remains to compute the reflexive closure of the image of the twisted transfer $\mathrm{Tr}^G_{\det} : S \to S^G$. From now on let N be the subgroup of G generated by all pseudoreflections in G. Instead of computing the image of $\mathrm{Tr}^G_{\det}$ directly, we first consider the image of $\mathrm{Tr}^N_{\det}$. This is the content of the next lemma. We use the Dedekind different $\mathcal{D}_{S/S^N}$ which is a principal ideal in S by Lemma 7.26.

Lemma 7.45. *Let θ_N be a generator of $\mathcal{D}_{S/S^N}$. Then we have $\overline{\mathrm{im}(\mathrm{Tr}^N_{\det})} = S^N \cdot \theta_N$. Here $\overline{\mathrm{im}(\mathrm{Tr}^N_{\det})}$ denotes the reflexive closure of $\mathrm{im}(\mathrm{Tr}^N_{\det})$ as an S^N-module.*

Proof. The inclusion $\iota_N : S^N \to S$ induces a homomorphism of S^N-modules $\iota_N^* : \mathrm{Hom}_{S^N}(S, S^N) \to \mathrm{Hom}_{S^N}(S^N, S^N)$. By Lemma 7.40 $S^N_{\mathfrak{p}}$ is a direct summand of $S_{\mathfrak{p}}$ for every $\mathfrak{p} \in X^{(1)}(S^N)$ and hence as in the proof of Lemma 7.42 we get that $(\iota_N^*)_{\mathfrak{p}} : \mathrm{Hom}_{S^N}(S, S^N)_{\mathfrak{p}} \to \mathrm{Hom}_{S^N}(S^N, S^N)_{\mathfrak{p}}$ is surjective. Together with Lemma 5.2 this implies $\overline{\mathrm{im}(\iota_N^*)} = \mathrm{Hom}_{S^N}(S^N, S^N)$.

We consider the natural isomorphism $\eta : S^N \to \mathrm{Hom}_{S^N}(S^N, S^N), a \mapsto f_a$ with $f_a(b) = ab$ for all $a, b \in S^N$. $\mathrm{Hom}_{S^N}(S, S^N)$ is generated by $\phi : S \to S^N, x \mapsto \mathrm{Tr}^N(\frac{x}{\theta_N})$ as an S-module (see Lemma 7.18). Thus for every $\alpha \in \mathrm{im}(\iota_N^*) \subseteq \mathrm{Hom}_{S^N}(S^N, S^N)$ there is an $a \in S$ such that $\alpha(b) = \phi(ab) = b\phi(a)$ for all $b \in S^N$, so $\mathrm{im}(\iota_N^*) = \{f_{\phi(a)} | a \in S\} = \eta(\mathrm{Tr}^N(\frac{1}{\theta_N} S))$. Since η is an isomorphism, we obtain

$$\overline{\mathrm{Tr}^N\left(\frac{1}{\theta_N} S\right)} = \eta^{-1}(\overline{\mathrm{im}(\iota_N^*)}) = \eta^{-1}(\mathrm{Hom}_{S^N}(S^N, S^N)) = S^N.$$

Furthermore, Proposition 7.28 implies that $\sigma(\theta_N) = \det(\sigma) \cdot \theta_N$ for every $\sigma \in G$. From this it follows that $\theta_N \cdot \mathrm{Tr}^N(\frac{1}{\theta_N} S) = \mathrm{Tr}^N_{\det}(S)$ and hence

$$\overline{\mathrm{im}(\mathrm{Tr}^N_{\det})} = \overline{\mathrm{Tr}^N\left(\frac{1}{\theta_N} S\right)} \cdot \theta_N = S^N \cdot \theta_N.$$

□

For the final step of the computation we need to study the image of the twisted transfer $\mathrm{Tr}^{G/N}_{\nu} : S^N \to S^G_{\nu}$ for a character $\nu : G/N \to R^\times$. This is the content of the next proposition.

Proposition 7.46. *Let $\nu : G/N \to R^\times$ be a character. Then we have an isomorphism of S^G-modules $\overline{\mathrm{Tr}^{G/N}_{\nu}(S^N)} \cong S^G_{\nu}$. Here $\overline{\mathrm{Tr}^{G/N}_{\nu}(S^N)}$ is the reflexive closure of $\mathrm{Tr}^{G/N}_{\nu}(S^N)$ as an S^G-module.*

The proof needs some preparations:

Lemma 7.47. *The Dedekind different $\mathcal{D}_{S^N/S^G}$ is a principal ideal in S^N generated by an element r of R.*

Proof. By Corollary 6.6, S^N is factorial. By Lemma 7.21, $\mathcal{D}_{S^N/S^G}$ is a divisorial ideal in S^N, so it is indeed a principal ideal, say $\mathcal{D}_{S^N/S^G} = (r)$: we need to show that $r \in R$. By Lemma 7.20 we also have $\mathcal{D}_{S_K^N/S_K^G} = (r)$, but $\mathcal{D}_{S_K^N/S_K^G} = S_K^N$, see Fleischmann and Woodcock [18, Lemma 5.3]. So $r \in (S_K^N)^\times \cap S^N = K^\times \cap S^N \subseteq R$.

For convenience we also give a proof which is independent of [18]; however, it should be said that really the strategy of this proof is the same as in [18]. As above we see that $\mathcal{D}_{S^N/S^G}$ is a principle ideal (r) in S^N. Let $p \in S^N$ be a prime element which is not in R; we need to show that p does not divide r or equivalently that $v_{(p)}(\mathcal{D}_{S^N/S^G}) = 0$; here again we use that S^N is factorial by Corollary 6.6. Let $q \in S$ be a prime divisor of p. Then $(q) \cap S^N = (p)$, so by Remark 7.23 we need to show $v_{(q)}(\mathcal{D}_{S/S^G}) = v_{(q)}(\mathcal{D}_{S/S^N})$. Let $G^i((q)) \coloneqq \{\sigma \in G | (\sigma - \mathrm{id})(S) \subseteq (q)\}$ be the inertia group of (q). Since p is prime, $p \notin R$, and $q|p$, we have $q \notin R$. Hence q is prime in $S_K = K[x_1, \ldots, x_n]$ and thus $G^i((q)) \subseteq N$ by Proposition 2.16. We have $G^i((q) \cap S^{G^i(q)}) = \{\mathrm{id}\}$ by Lemma 2.11, so $e((q) \cap S^{G^i(q)}, (q) \cap S^G) = 1$ by Lemma 2.10 and hence $v_{(q)\cap S^{G^i((q))}}(\mathcal{D}_{S^{G^i((q))}/S^G}) = 0$ by Proposition 7.24. By applying Remark 7.23 to the extensions $S^G \subseteq S^{G^i((q))} \subseteq S$ we obtain $v_{(q)}(\mathcal{D}_{S/S^G}) = v_{(q)}(\mathcal{D}_{S/S^{G^i((q))}})$. By replacing G by N and using that $G^i((q)) \subseteq N$ we obtain in the same way that $v_{(q)}(\mathcal{D}_{S/S^N}) = v_{(q)}(\mathcal{D}_{S/S^{G^i((q))}})$. Putting both equalities together finishes the proof. □

Using Lemma 7.47 we can generalize it to the twisted different.

Lemma 7.48. *Let $\nu : G/N \to R^\times$ be a character. Then $\mathcal{D}_{S^N/S^G,\nu}$ is a principal ideal in S^N generated by an element of R.*

Proof. S^N is factorial by Corollary 6.6; let θ_N and $\theta_{N,\nu}$ be generators of the divisorial and hence principal ideals $\mathcal{D}_{S^N/S^G}$ and $\mathcal{D}_{S^N/S^G,\nu}$, respectively. By Lemma 7.47 we have $\theta_N \in R$. We will show that there is an $r \in K$ such that $r\theta_N = \theta_{N,\nu}$; then $\theta_{N,\nu} \in R$ follows since $\mathcal{D}_{S^N/S^G,\nu}$ is an integral ideal. We can also view ν as a character of G which is trivial on N; then we have $\mathcal{D}_{S_K/S_K^G} = \mathcal{D}_{S_K/S_K^G,\nu}$ (see Broer [8, Proposition 10]; this needs the assumption that ν is trivial on pseudoreflections). Let θ and θ_ν be generators of $\mathcal{D}_{S/S^G}$ and $\mathcal{D}_{S/S^G,\nu}$, respectively. Then by Lemma 7.20 we obtain $r_0\theta = \theta_\nu$ for some $r_0 \in K$.

Now let $p \in S^N$ be a prime element such that $p \notin R$ and let $q \in S$ be a prime divisor of p in S; since $R \subseteq S^N$ we also have $q \notin R$. Let again $v_{(p)}$ and $v_{(q)}$ be the discrete valuations corresponding to the valuation rings $S^N_{(p)}$ and $S_{(q)}$, respectively. Since we have seen above that θ and θ_ν only differ by factors in R we have $v_{(q)}(\mathcal{D}_{S/S^G}) = v_{(q)}(\mathcal{D}_{S/S^G,\nu})$. Using Remark 7.23 we obtain $v_{(p)}(\mathcal{D}_{S^N/S^G}) = v_{(p)}(\mathcal{D}_{S^N/S^G,\nu})$. This shows that also θ_N and $\theta_{N,\nu}$ only differ by factors in R, so the claim follows. □

By combining this with Lemma 7.18 we obtain:

Lemma 7.49. *Let $\nu : G/N \to R^\times$ be a character and let $r \in R$ be a generator of $\mathcal{D}_{S^N/S^G,\nu}$. For every $f \in S^N$, the map $\alpha_f : S^N \to S^G_\nu, g \mapsto \mathrm{Tr}^{G/N}_\nu(\frac{1}{r}fg) = \frac{1}{r}\mathrm{Tr}^{G/N}_\nu(fg)$ is a well-defined homomorphism of S^G-modules and the map $S^N \to \mathrm{Hom}_{S^G}(S^N, S^G_\nu), f \mapsto \alpha_f$ is an isomorphism of S^N-modules.*

Using this we can finally prove Proposition 7.46:

Proof of Proposition 7.46. Let $r \in R$ be as in Lemma 7.49. Then Lemma 7.49 shows that

$$\psi : \mathrm{Hom}_{S^G}(S^N, S^G_\nu) \to \mathrm{Tr}^{G/N}_\nu(S^N), \alpha \mapsto r \cdot \alpha(1)$$

is a well-defined and surjective homomorphism of S^N-modules. The embedding $\hat{\imath} : S^G \to S^N$ induces a homomorphism of S^G-modules

$$\hat{\imath}^* : \mathrm{Hom}_{S^G}(S^N, S^G_\nu) \to \mathrm{Hom}_{S^G}(S^G, S^G_\nu), \alpha \mapsto \alpha|_{S^G}.$$

For $\alpha \in \mathrm{Hom}_{S^G}(S^N, S^G_\nu)$ we have

$$\psi(\alpha) = 0 \iff \alpha(1) = 0 \iff \forall f \in S^G : \alpha(f) = 0 \iff \hat{\imath}^*(\alpha) = 0,$$

so $\ker\psi = \ker\hat{\imath}^*$. Hence $\hat{\imath}^*$ induces an injective homomorphism

$$\begin{aligned}\varphi : \mathrm{Tr}^{G/N}_\nu(S^N) = \mathrm{im}\psi &\cong \mathrm{Hom}_{S^G}(S^N, S^G_\nu)/\ker\psi = \mathrm{Hom}_{S^G}(S^N, S^G_\nu)/\ker\hat{\imath}^* \\ &\cong \mathrm{im}\hat{\imath}^* \hookrightarrow \mathrm{Hom}_{S^G}(S^G, S^G_\nu) \cong S^G_\nu.\end{aligned}$$

Now let $\mathfrak{p} \in X^{(1)}(S^G)$; as in Lemma 7.40 we obtain that $(S^G)_\mathfrak{p}$ is a direct summand of $(S^N)_\mathfrak{p}$ and hence the localized map $(\hat{\imath}^*)_\mathfrak{p}$ is surjective, so $\varphi_\mathfrak{p}$ is also surjective. As φ is injective, this implies that we obtain an isomorphism of reflexive closures $\overline{\mathrm{Tr}^{G/N}_\nu(S^N)} \cong \overline{S^G_\nu}$ by Lemma 5.2. By Lemma 5.11, S^G_ν is reflexive, so the proposition follows. □

Now we are ready to state the main result of this section:

Theorem 7.50. *Let $f_1, \ldots, f_n$ be a system of parameters in S^G and $\mathcal{F} := R[f_1, \ldots, f_n]$. Let furthermore χ be the differential character of G. Then we have $\mathrm{Hom}_\mathcal{F}(S^G, \mathcal{F}) \cong S^G_{\det/\chi}$.*

For the proof of this we need some more notation: let $\nu : G \to R^\times$ be a character and let $\nu_0 := \nu|_N$. We want to define a twisted transfer $\mathrm{Tr}^{G/N}_\nu : S^N_{\nu_0} \to S^G_\nu$. If $\nu_0 = 1$, then we can just view ν as a character $G/N \to R^\times$ and use the usual twisted transfer. In general let $\sigma_1, \ldots, \sigma_r$ be representatives of the cosets of N in G (N is a normal subgroup, so we do not need to distinguish between left and right cosets). Then we define $\mathrm{Tr}^{G/N}_\nu$ as follows:

$$\mathrm{Tr}^{G/N}_\nu : S^N_{\nu_0} \to S^G_\nu, f \mapsto \sum_{i=1}^{r} \nu(\sigma_i^{-1})\sigma_i(f).$$

It follows directly from the definition of $S^N_{\nu_0}$ that this does not depend on the choice of $\sigma_1, \ldots, \sigma_r$. It is clear that $\mathrm{Tr}^G_\nu = \mathrm{Tr}^{G/N}_\nu \circ \mathrm{Tr}^N_{\nu_0}$.

Proof of Theorem 7.50. By Lemmas 7.42 and 7.43 $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F})$ is isomorphic to the reflexive closure of $\mathrm{im}(\mathrm{Tr}^G_{\det})$ as an S^G-module; hence by Lemma 5.3 it is isomorphic to the reflexive closure of $\mathrm{Tr}^{G/N}_{\det}(\overline{\mathrm{Tr}^N_{\det}(S)})$ where by Lemma 5.5 we may also take the inner reflexive closure as an S^N-module. By Lemma 7.45 we then obtain $\mathrm{Hom}_{\mathcal{F}}(S^G, \mathcal{F}) \cong \overline{\mathrm{Tr}^{G/N}_{\det}(S^N \cdot \theta_N)}$, where θ_N is a generator of $\mathcal{D}_{S/S^N}$. As $\mathcal{D}_{S^N/S^G}$ is generated by an $r \in R$ (see Lemma 7.47), $\mathcal{D}_{S/S^G}$ is generated by $r\theta_N$ (see Lemma 7.22), so $r\theta_N$ is a χ-semiinvariant by the definition of the differenial character. Since $r \in R \subseteq S^G$, θ_N is also a χ-semiinvariant and hence with a set of representatives $\sigma_1, \ldots, \sigma_r$ of the cosets of N in G we have for $f \in S^N$:

$$\begin{aligned}
\mathrm{Tr}^{G/N}_{\det}(f\theta_N) &= \sum_{i=1}^{r} \det(\sigma_i^{-1})\sigma_i(f\theta_N) = \sum_{i=1}^{r} \det(\sigma_i^{-1})\sigma_i(f)\sigma_i(\theta_N) \\
&= \sum_{i=1}^{r} \det(\sigma_i^{-1})\sigma_i(f)\chi(\sigma_i)\theta_N = \left(\sum_{i=1}^{r} (\det/\chi)(\sigma_i^{-1})\sigma_i(f)\right)\theta_N \\
&= \mathrm{Tr}^{G/N}_{\det/\chi}(f) \cdot \theta_N,
\end{aligned}$$

so we obtain $\overline{\mathrm{Tr}^{G/N}_{\det}(S^N \cdot \theta_N)} = \overline{\mathrm{Tr}^{G/N}_{\det/\chi}(S^N)} \cdot \theta_N$. This is isomorphic to $S^G_{\det/\chi}$ by Proposition 7.46; note that $\det/\chi$ is trivial on N by Proposition 7.28. □

7.7 The main result

In this section we use Theorem 7.50 to derive a criterion for the quasi-Gorenstein property of arithmetic invariant rings. We begin by defining the class of rings we want to allow as base rings; this is an ad hoc definition.

Definition 7.51. *We call a ring R an allowed base ring if it satisfies the following conditions:*

(i) R is Gorenstein,
(ii) R is an integral domain,
(iii) for every prime ideal $\mathfrak{p} \subset R$, the localization $R_{\mathfrak{p}}$ is factorial,
(iv) for every maximal ideal $\mathfrak{m} \subset R$, we have $\mathrm{ht}(\mathfrak{m}) = \dim(R)$.

The following properties of allowed base rings are immediate from the definition:

Lemma 7.52.
a) Every Dedekind domain is an allowed base ring.
b) Every allowed base ring is Noetherian, Cohen-Macaulay, and normal.
c) If R is an allowed base ring and $\mathfrak{p} \subset R$ is a prime ideal, then $R_{\mathfrak{p}}$ is again an allowed base ring; in particular, $R_{\mathfrak{p}}$ is factorial and Gorenstein.

The following proposition gives a criterion for a graded algebra over an allowed base ring to be a quasi-Gorenstein ring.

Proposition 7.53. *Let R be an allowed base ring and let S be a finitely generated graded R-algebra which is an integral domain. Then the following statements are equivalent:*

(i) S is quasi-Gorenstein.

(ii) For every prime ideal $\mathfrak{p} \subset R$ the ring $S \otimes_R R_\mathfrak{p}$ is quasi-Gorenstein.

(iii) For every homogeneous surjective homomorphism $T := R[x_1, \ldots, x_m] \to S$ of R-algebras $\operatorname{Ext}^r_T(S, T)$ is a projective S-module of rank 1 where $r := \dim(T) - \dim(S)$.

For the proof we need two lemmas:

Lemma 7.54. *Let R and S be as in the proposition, let M be a finitely generated graded S-module, and let $\mathfrak{p} \subset R$ be a prime ideal such that there is a homogeneous isomorphism $M \otimes_R R_\mathfrak{p} \cong S \otimes_R R_\mathfrak{p}$. Then there is an $f \in R \backslash \mathfrak{p}$ such that $M \otimes_R R_f \cong S \otimes_R R_f$. Here R_f means the localization $U^{-1}R$ with $U := \{f^i | i \in \mathbb{N}_0\}$.*

In the special case $S = R$ this is a classical result in commutative algebra, see Bourbaki [5, Chapter II, §5.1, Prop. 2(ii)] and the proof given here reduces the general result to this special case.

Proof. We write $S_\mathfrak{p} := S \otimes_R R_\mathfrak{p}$ and $M_\mathfrak{p} := M \otimes_R R_\mathfrak{p}$. By assumption there is an $a \in M$ which is homogeneous of degree zero such that $M_\mathfrak{p} = (a)_{S_\mathfrak{p}}$. We consider the homogeneous homomorphism $\varphi : S \to M, b \mapsto ba$. Then the induced homomorphism $\varphi_\mathfrak{p} : S_\mathfrak{p} \to M_\mathfrak{p}$ is an isomorphism.

We choose a $d \in \mathbb{N}$ such that M is generated as an S-module by elements of degree at most d. Since S is a finitely generated graded R-algebra, the R-modules $\tilde{M} := M_{\leq d}$ and $\tilde{S} := S_{\leq d}$ are finitely generated. Since φ is homogeneous, it restricts to a homomorphism $\tilde{\varphi} : \tilde{S} \to \tilde{M}$ and $\varphi_\mathfrak{p}$ restricts to an isomorphism $\tilde{S}_\mathfrak{p} \to \tilde{M}_\mathfrak{p}$ where $\tilde{S}_\mathfrak{p} := (S_\mathfrak{p})_{\leq d}$ and $\tilde{M}_\mathfrak{p} := (M_\mathfrak{p})_{\leq d}$. Since $\tilde{S}$ and $\tilde{M}$ are finitely generated R-modules, we now get that there is an $f \in R \backslash \mathfrak{p}$ such that the restriction $\tilde{\varphi}_f : \tilde{S}_f \to \tilde{M}_f$ of the homomorphism $S_f \to M_f$ induced by φ is an isomorphism (see Bourbaki [5, Chapter II, §5.1, Prop. 2 (ii)]) where $S_f := S \otimes_R R_f$, $M_f := M \otimes_R R_f$, $\tilde{S}_f := (S_f)_{\leq d}$, and $\tilde{M}_f := (M_f)_{\leq d}$. We show that φ_f is also an isomorphism.

First of all φ_f is certainly injective since we can view it as a restriction of $\varphi_\mathfrak{p}$ which is an isomorphism. By the choice of d there are elements $m_1, \ldots, m_l \in \tilde{M}$ such that $M = (m_1, \ldots, m_l)_S$. Since $\tilde{\varphi}_f$ is surjective, $m_1, \ldots, m_l$ are in $\operatorname{im}(\tilde{\varphi}_f) \subseteq \operatorname{im}(\varphi_f)$ and hence φ_f is surjective because $m_1, \ldots, m_l$ generate M and therefore also M_f. □

The second lemma we need is a stronger version of Lemma 2.33.

Lemma 7.55. *Let R be an allowed base ring and let T be a finitely generated graded R-algebra which is an integral domain. Then for every homogeneous maximal ideal $\mathfrak{m} \subset T$ we have $\operatorname{ht}(\mathfrak{m}) = \dim(T)$.*

Proof. We define $\mathfrak{n} := \mathfrak{m} \cap R$. Then $\mathfrak{n}$ is a maximal ideal in R, so $\operatorname{ht}(\mathfrak{n}) = \dim(R)$ because R is an allowed base ring. Also R is universally catenary, see Bruns and Herzog [11, Theorem 2.1.12], so T is catenary and hence there is a chain of prime ideals

$$(0) = P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_{r-1} \subsetneq P_r = \mathfrak{m}$$

with $r = \mathrm{ht}(\mathfrak{m})$ and $P_i = T_+$ for some index i; note that $T_+ \subseteq \mathfrak{m}$ by Lemma 2.29. We have $i = \mathrm{ht}(T_+)$ and $r - i = \mathrm{ht}(\mathfrak{m}/T_+) = \mathrm{ht}(\mathfrak{n}) = \dim(R)$. This implies $\mathrm{ht}(\mathfrak{m}) = r = \mathrm{ht}(T_+) + \dim(R)$, so all homogeneous maximal ideals have the same height. Now the lemma follows from Lemma 2.33. □

Proof of Proposition 7.53. It is clear that (i) implies (ii). Now we assume that (ii) holds and fix a T as in (iii). We write $M := {}^*\mathrm{Ext}^r_T(S,T)$; this is isomorphic to $\mathrm{Ext}^r_T(S,T)$ by Lemma 2.39. Let $\mathfrak{p} \subset R$ be a prime ideal. $T \otimes_R R_\mathfrak{p}$ is Gorenstein, so $M(m) \otimes_R R_\mathfrak{p}$ is the graded canonical module of $S \otimes_R R_\mathfrak{p}$ for some $m \in \mathbb{Z}$; hence there is a homogeneous isomorphism $M(m) \otimes_R R_\mathfrak{p} \cong S \otimes_R R_\mathfrak{p}$ by Proposition 7.15 because $S \otimes_R R_\mathfrak{p}$ is quasi-Gorenstein. By Lemma 7.54 there is an $f \in R \backslash \mathfrak{p}$ such that $M(m) \otimes_R R_f \cong S \otimes_R R_f$. Since this holds for every prime ideal $\mathfrak{p}$ and R is Noetherian, there are $f_1, \ldots, f_s \in R$ such that $(f_1, \ldots, f_s)_R = R$ and $M \otimes_R R_{f_i} \cong S \otimes_R R_{f_i}$ as ungraded $S \otimes_R R_f$-modules for each i. This implies that M is a projective S-module, see Bourbaki [5, Chapter II, §5.2, Theorem 1]. Finally $M \otimes_R R_\mathfrak{p} \cong S \otimes_R R_\mathfrak{p}$ implies that $M \otimes_R R_\mathfrak{p}$ is of rank one and hence the same holds for M. So we proved that (ii) implies (iii).

It remains to prove that (iii) implies (i). The argument for this is similar to the proof of Proposition 7.14. Fix a T as in (iii), let again $M := {}^*\mathrm{Ext}^r_T(S,T) \cong \mathrm{Ext}^r_T(S,T)$ and let $\mathfrak{m} \subset S$ be a maximal ideal. Then $M_\mathfrak{m}$ is a projective $S_\mathfrak{m}$-module of rank one and hence $M_\mathfrak{m} \cong S_\mathfrak{m}$ since projective modules over local rings are free. So it is sufficient to prove that $M_\mathfrak{m}$ is the canonical module of $S_\mathfrak{m}$. Let g be the given map $T \to S$ and let $\mathfrak{n} := g^{-1}(\mathfrak{m})$. As in the proof of Proposition 7.14 we have $M_\mathfrak{m} \cong \mathrm{Ext}_{T_\mathfrak{n}}(S_\mathfrak{m}, T_\mathfrak{n})$ and g induces a surjective homomorphism $T_\mathfrak{n} \to S_\mathfrak{m}$. So by Theorem 7.4 it suffices to show that $r = \dim(T_\mathfrak{n}) - \dim(S_\mathfrak{m})$. For this again we use the same argument as in the proof of Proposition 7.14; we only need to replace Lemma 2.33 by Lemma 7.55. □

By putting all the major results on the quasi-Gorenstein property we have obtained so far together, we obtain the follwing theorem, which is the main result of this chapter:

Theorem 7.56. *Let R be an allowed base ring, $S := R[x_1, \ldots, x_n]$, and let $G \subseteq Gl_n(R)$ be a finite group. Then the following statements are equivalent:*

(i) S^G *is quasi-Gorenstein.*
(ii) $(S \otimes_R R_\mathfrak{p})^G$ *is quasi-Gorenstein for every prime ideal* $\mathfrak{p} \subset R$.
(iii) $(S \otimes_R \mathrm{Quot}(R))^G$ *is quasi-Gorenstein.*
(iv) The differential character $G \to R^\times$ *is equal to the determinant.*
(v) For every prime ideal $\mathfrak{p} \subset R$ *we have* ${}^*K_{(S \otimes_R R_\mathfrak{p})^G} \cong (S \otimes_R R_\mathfrak{p})^G$.

Proof. Using Proposition 3.2 we get $(S \otimes_R R_\mathfrak{p})^G \cong S^G \otimes_R R_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R$. Now the equivalence of (i) and (ii) is Proposition 7.53 and (iii) is the special case $\mathfrak{p} = (0)$ in (ii). The equivalence of (iii) and (iv) is Broer's Theorem 7.30 and (iv) implies (v) by Theorem 7.50 and Theorem 7.12. Finally (v) implies (ii) by Proposition 7.15 □

In the case where $|G|$ is invertible in R we can give a criterion for S^G to be a Gorenstein ring.

Corollary 7.57. *Let R, S, and G be as in Theorem 7.56 and assume that $|G|$ is invertible in R. Then S^G is Gorenstein if and only if $(S \otimes_R \mathrm{Quot}(R))^G$ is Gorenstein.*

Proof. Since a ring is Gorenstein if and only if it is quasi-Gorenstein and Cohen-Macaulay, this follows from Theorem 3.14 and Theorem 7.56. □

Example 3.13 shows that the assumption that $|G|$ is invertible cannot be omitted in Corollary 7.57. Since in that example $(S^{(n)} \otimes_R \mathbb{Q})^G$ is Gorenstein, $(S^{(n)})^G$ is quasi-Gorenstein by Theorem 7.56, so this also gives an example of a ring of invariants which is quasi-Gorenstein but not Gorenstein.

8 Invariants of point stabilizers

An important observation in invariant theory over a field K is that many properties of a ring of invariants imply the same property for the ring of invariants of the stabilizer subgroup of a point $y \in K^n$. Kemper [34] identifies a general class of properties, which he calls "local properties", for which this is always true. In this chapter, we prove similar results over rings; however, in oder to carry over Kemper's approach we need a more restrictive definition of a local property and also our proofs only work under some condition on the point y. In Section 8.1 we recall some results on étale morphisms of schemes which we need for the proof of the main result. Then in Section 8.2 we introduce the notion of a local property in the way we need it and give some examples of such properties. Section 8.3 contains the main results on invariant rings of stabilizer subgroups.

8.1 Étale Morphisms

In this section we briefly summarize the definition and some basic properties of étale morphisms; for proofs and more details, we refer to the book by Milne [42]. For simplicity, we assume in the following that all our schemes are Noetherian.

Definition 8.1. *Let X and Y be schemes and let $f : X \to Y$ be a morphism which is locally of finite type.*

a) The morphism f is called unramified at a point $x \in X$ if with $y := f(x)$ and $\mathfrak{m}_y$ the maximal ideal of $\mathcal{O}_{Y,y}$ we have that $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x}$ is a finite and separable field extension of $\kappa(y)$; in particular, it is part of the condition that $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x}$ is a field. Here $\mathcal{O}_{Y,y}$ denotes the stalk of the structure sheaf $\mathcal{O}_Y$ at y and $\kappa(y) \coloneqq \mathcal{O}_{Y,y}/\mathfrak{m}_y$ denotes the residue field of Y at y.

b) The morphism f is called unramified if it is unramified at every point $x \in X$.

c) The morphism f is called flat if for every $x \in X$ the induced ring homomorphism $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is flat.

d) The morphism f is called étale if it is flat and unramified.

Remark 8.2. The notion of an unramified morphism can be viewed as a generalization of the notion of an unramified ring extension introduced in Section 2.2: let $A \subseteq B$ be a finite extension of Noetherian normal domains and $\mathfrak{q} \in X^{(1)}(B)$. Then the extension is unramified at $\mathfrak{q}$ if and only if the induced morphism $f : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is unramified at $\mathfrak{q}$.

The first result on étale morphisms we need is the following lemma which describes the set of those points in X at which a morphism $f : X \to Y$ is unramified.

Lemma 8.3. ([42, Remark 3.7]) *Let $f : X \to Y$ be a morphism of schemes which is locally of finite type. The set of all points in X at which f is unramified is open in X.*

The next theorem will allow us to prove that certain unramified morphisms are étale.

Theorem 8.4. ([42, Theorem 3.20]) *Let $f : X \to Y$ be a morphism of schemes. Assume that f is unramified and Y is normal. Then f is étale if and only if for every $x \in X$ the induced map $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is injective.*

The notion of an unramified map has its origin in the theory of Riemann surfaces. An unramified holomorphic map between Riemann surfaces is locally an isomorphism, see Forster [19, Theorem 4.4]. This is not true for unramified morphisms of schemes; for example, every closed immersion is unramified. This is the reason why the more restrictive notion of étale maps is introduced. However, it is still not true that an étale morphism is locally an isomorphism, but at least we have the following theorem. As usual we write $\hat{A}$ for the completion of a local ring A.

Theorem 8.5. ([42, Remark 4.7]) *Let $f : X \to Y$ be an étale morphism of schemes. Let $x \in X$, $y := f(x)$ and assume that $\kappa(x) = \kappa(y)$. Then the induced map $\hat{\mathcal{O}}_{Y,y} \to \hat{\mathcal{O}}_{X,x}$ is an isomorphism.*

8.2 Local properties

In this section we introduce the class of properties of Noetherian rings for which we prove the main result in the next section. A similar definition has been given by Kemper [34, Definition 1.4], and he calls these properties local. Although our definition is slightly more complicated than Kemper's as he only wants to consider graded algebras over fields, we also use the term "local property".

Definition 8.6. *Let $\mathcal{P}$ be a property of Noetherian commutative rings. Then we call $\mathcal{P}$ local if it satisfies the following conditions:*

(i) If A is a Noetherian local ring with completion $\widehat{A}$, then $\mathcal{P}(A)$ holds if and only if $\mathcal{P}(\widehat{A})$ holds.

*(ii) If S is a Noetherian *local graded ring with homogeneous maximal ideal $\mathfrak{m}$, then $\mathcal{P}(S)$ holds if and only if $\mathcal{P}(S_{\mathfrak{m}})$ holds.*

*(iii) If S is a Noetherian *local graded ring, $\mathfrak{n} \subset S_0$ the maximal ideal in S_0, and $\mathfrak{m} \subset S$ a maximal ideal such that $\mathfrak{m} \cap S_0 = \mathfrak{n}$, then $\mathcal{P}(S)$ implies $\mathcal{P}(S_{\mathfrak{m}})$.*

(iv) If S is a Noetherian graded ring, then $\mathcal{P}(S)$ holds if and only if $\mathcal{P}(S \otimes_{S_0} (S_0)_{\mathfrak{n}})$ holds for every maximal ideal $\mathfrak{n} \subset S_0$.

*We call the property $\mathcal{P}$ R-local for a Noetherian ring R if (i) holds, (iv) holds for graded rings S with $S_0 \cong R$ and (ii) and (iii) hold for *local graded rings S with $S_0 \cong R_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R$.*

Proposition 8.7. *The following properties of Noetherian commutative rings are local properties: regularity, the Gorenstein property, and the Cohen-Macaulay property. The quasi-Gorenstein property is R-local for every allowed base ring R (in the sense of Definition 7.51).*

Proof. For regularity, Gorenstein, and Cohen-Macaulay statements (*i*), (*ii*), and (*iii*) are well-known results, see for example Bruns and Herzog [11]; for statement (*iv*) see Propositions 2.34, 2.35, and 2.36. All the results on the quasi-Gorenstein property have been proved in Chapter 7: (*i*) is Lemma 7.6a). For (*ii*) we note that S has a graded canonical module by Corollary 7.13; hence (*ii*) follows from Proposition 7.15. Statement (*iii*) follows directly from the definition of quasi-Gorenstein rings, and (*iv*) is Proposition 7.53. □

Factoriality is not a local property: if R is a Dedekind domain which is not a principal ideal domain, then $R[x]$ is not factorial but $R[x] \otimes_R R_\mathfrak{n}$ is factorial for every maximal ideal $\mathfrak{n} \subset R_0$, so statement (*iv*) does not hold.

We want to introduce a further family of local properties which is also discussed in [34] for invariant rings over fields. For this, we first need the following definition (see for example Kemper [36]:

Definition 8.8. *Let A be a Noetherian ring. The Cohen-Macaulay defect of A is*

$$\operatorname{cmdef}(A) := \sup_{\mathfrak{p} \in \operatorname{Spec}(A)} (\dim(A_\mathfrak{p}) - \operatorname{depth}(A_\mathfrak{p})).$$

For local rings, we have the following result, see Grothendieck and Dieudonné [26, Proposition 6.11.5]:

Lemma 8.9. *Let A be a Noetherian local ring and let $\mathfrak{p} \in \operatorname{Spec}(A)$ be a prime ideal. Then $\dim(A_\mathfrak{p}) - \operatorname{depth}(A_\mathfrak{p}) \leq \dim(A) - \operatorname{depth}(A)$. In particular, $\operatorname{cmdef}(A) = \dim(A) - \operatorname{depth}(A)$.*

The next proposition facilitates the computation of the Cohen-Macaulay defect of a graded ring.

Proposition 8.10. *Let A be a Noetherian graded ring. Then $\operatorname{cmdef}(S)$ is the supremum over all $\operatorname{cmdef}(S_\mathfrak{n})$ where $\mathfrak{n}$ is a homogeneous maximal ideal in S.*

The proof of this proposition uses the following lemma:

Lemma 8.11. *Let S be a Noetherian graded ring and let $\mathfrak{m}$ be a non-homogeneous maximal ideal in S. As in Definition 2.31 we define $\mathfrak{m}^*$ to be the ideal generated by all homogeneous elements in $\mathfrak{m}$. Then we have $\operatorname{depth}(S_\mathfrak{m}) = \operatorname{depth}(S_{\mathfrak{m}^*}) + 1$.*

Proof. This is a special case of Bruns and Herzog [11, Theorem 1.5.9]. □

Proof of Proposition 8.10. By Lemma 8.9 it is sufficient to show that for every maximal ideal $\mathfrak{m} \subset S$ there is a homogeneous maximal ideal $\mathfrak{n} \subset S$ such that $\operatorname{cmdef}(S_\mathfrak{n}) \geq \operatorname{cmdef}(S_\mathfrak{m})$. If $\mathfrak{m}$ is homogeneous, we just take $\mathfrak{n} = \mathfrak{m}$. Otherwise let $\mathfrak{n}$ be a homogeneous maximal ideal such that $\mathfrak{m}^* \subseteq \mathfrak{n}$; such an ideal exists by Lemma 2.29. Using Lemma 8.9, Lemma 2.32, and Lemma 8.11 we obtain

$$\operatorname{cmdef}(S_{\mathfrak{m}^*}) = \operatorname{ht}(\mathfrak{m}^*) - \operatorname{depth}(S_{\mathfrak{m}^*}) = \operatorname{ht}(\mathfrak{m}) - 1 - (\operatorname{depth}(S_\mathfrak{m}) - 1) = \operatorname{cmdef}(S_\mathfrak{m})$$

and hence $\operatorname{cmdef}(S_\mathfrak{n}) \geq \operatorname{cmdef}(S_{\mathfrak{m}^*}) = \operatorname{cmdef}(S_\mathfrak{m})$. □

Proposition 8.12. *Let $n \in \mathbb{N}$. We say that a Noetherian ring R has the property $\mathcal{P}_n$ if* $\operatorname{cmdef}(R) \leq n$. *Then $\mathcal{P}_n$ is a local property.*

Proof. For a Noetherian local ring R we have $\dim(R) = \dim(\hat{R})$ and $\operatorname{depth}(R) = \operatorname{depth}(\hat{R})$, see Eisenbud [17, Corollary 10.12 and the proof of Proposition 18.8]. Hence we have $\operatorname{cmdef}(R) = \operatorname{cmdef}(\hat{R})$ by Lemma 8.9 and statement (i) from the definition of a local property follows. Statement (ii) follows from Proposition 8.10 and (iii) is clear from the definition of the Cohen-Macaulay defect. In order to prove (iv), let S be a Noetherian graded ring. For every maximal ideal $\mathfrak{n} \subset S_0$ $\mathcal{P}_n(S \otimes_{S_0} (S_0)_\mathfrak{n})$ implies $\mathcal{P}_n(S_\mathfrak{m})$ where $\mathfrak{m} := (\mathfrak{n}, S_+)$ because $S \otimes_{S_0} (S_0)_\mathfrak{n} \cong (S_0 \backslash \mathfrak{n})^{-1} S$. Now (iv) follows from Lemma 2.29 and Proposition 8.10. □

8.3 The main result

Let R be a Noetherian normal domain, $S := R[x_1, \ldots, x_n]$, and $G \subseteq Gl_n(R)$ a finite group. Furthermore, let $y \in R^n$ be any point and $G_y := \{\sigma \in G | \sigma(y) = y\}$ its stabilizer subgroup. If R is a field, then Kemper [34] proved for every local property $\mathcal{P}$ that $\mathcal{P}(S^G)$ implies $\mathcal{P}(S^{G_y})$. Our goal here is to generalize this to the case where R need not be a field. I achieved this only for some points y: for an ideal $\mathfrak{a} \subseteq S$ we define the stabilizer subgroup $G_\mathfrak{a} := \{\sigma \in G | \sigma(\mathfrak{a}) \subseteq \mathfrak{a}\}$. Now let $I \subseteq R$ be an ideal and $y \in R^n$ a point; we consider $\mathfrak{a} := \{f \in S | f(y) \in I\}$, which is an ideal in S. Then we have $G_y \subseteq G_\mathfrak{a}$. The points we want to consider are those where these two groups coincide:

Definition 8.13. *Let R be a ring, $S := R[x_1, \ldots, x_n]$, and $G \subseteq Gl_n(R)$ a finite group. Let $y \in R^n$ and let $I \subseteq R$ be an ideal; define $\mathfrak{a} := \{f \in S | f(y) \in I\}$. We say that y has I-stable stabilizer if the stabilizer subgroups G_y and $G_\mathfrak{a}$ coincide.*

Remark 8.14. In the context of the definition we can view $G_\mathfrak{a}$ as the stabilizer of the residue class of y in $(R/I)^n$; in particular, if G is a permutation group and all components of y are either 0 or 1, then y has I-stable stabilizer for every proper ideal $I \subsetneq R$.

Next we give an easy example of a point which is not I-stable.

Example 8.15. Let $R = \mathbb{Z}_{(2)}$, $I = (2)_R$, $n = 1$, and $G := \{1, -1\} \subseteq Gl_1(\mathbb{Z}_{(2)})$. Then for $y = 1 \in \mathbb{Z}$ we have $(x-1)(y) = 0$, but for $\sigma = -1 \in G$ we obtain $\sigma(x-1)(y) = (-x-1)(y) = -2 \neq 0$. This shows that $\sigma \notin G_y$. On the other hand, as $1 \equiv -1 \mod 2$, we have $f(1) \in (2)$ if and only if $f(-1) \in (2)$ for each $f \in R[x]$ and hence $f \in \mathfrak{a}$ if and only if $\sigma(f) \in \mathfrak{a}$, so $\sigma \in G_\mathfrak{a}$.

In order to analyze the invariant ring S^{G_y} we can use the ideas from Kemper's article [34]. The main technical step is the following theorem.

Theorem 8.16. *Let R be a local Noetherian normal domain with maximal ideal $\mathfrak{m}$ and let $G \subseteq Gl_n(R)$ be a finite group. Let $y \in R^n$ be a point with $\mathfrak{m}$-stable stabilizer and let $S := R[x_1, \ldots, x_n]$, $\mathfrak{p} := \{f \in S | f(y) \in \mathfrak{m}\}$, $\mathfrak{p}' := \mathfrak{p} \cap S^G$, and $\mathfrak{p}'' := \mathfrak{p} \cap S^{G_y}$. Then the inclusion $S^G \hookrightarrow S^{G_y}$ induces an isomorphism*

$$\widehat{(S^G)_{\mathfrak{p}'}} \cong \widehat{(S^{G_y})_{\mathfrak{p}''}}$$

where as usual $\widehat{\ }$ denotes the completion of a local ring with respect to its maximal ideal.

The proof requires a lemma:

Lemma 8.17. *In the situation of the theorem, we have the following:*
a) $\mathfrak{p}'_{\mathfrak{p}'}(S^{G_y})_{\mathfrak{p}''} = \mathfrak{p}''_{\mathfrak{p}''}$.
b) The inclusion $S^G \hookrightarrow S^{G_x}$ *induces an isomorphism* $S^G/\mathfrak{p}' \cong S^{G_y}/\mathfrak{p}''$.

Proof. We first prove part b). The kernel of the canonical map $S^G \hookrightarrow S^{G_y} \to S^{G_y}/\mathfrak{p}''$ is $\mathfrak{p}'' \cap S^G = \mathfrak{p}'$, so we obtain an injective map $S^G/\mathfrak{p}' \to S^{G_y}/\mathfrak{p}''$. Since every $f \in S^{G_y}$ can be written as $f = f(y) + (f - f(y))$ with $f(y) \in R \subseteq S^G$ and $f - f(y) \in \mathfrak{p}''$, this map is also surjective.

For the proof of a) we use an idea of Kemper [34, Proposition 1.1]. Assume that $\mathfrak{p} \subseteq \bigcup_{\sigma \in G \backslash G_y} \sigma(\mathfrak{p})$. Then by the prime avoidance lemma we have $\mathfrak{p} \subseteq \sigma(\mathfrak{p})$ for some $\sigma \in G \backslash G_y$. This would imply $\sigma(\mathfrak{p}) = \mathfrak{p}$ as σ is an automorphism. But then $\sigma \in G_{\mathfrak{p}} = G_y$ since y has $\mathfrak{m}$-stable stabilizer; this contradicts $\sigma \notin G_y$. So there is an $f \in \mathfrak{p}$ such that f is not an element of $\sigma(\mathfrak{p})$ for any $\sigma \in G \backslash G_y$. For $g := \prod_{\tau \in G_y} \tau(f)$ we have $g \in \mathfrak{p} \cap S^{G_y} = \mathfrak{p}''$ and $g \notin \sigma(\mathfrak{p})$ for all $\sigma \in G \backslash G_y$.

Let $J \subseteq \mathfrak{p}''$ be the subideal generated by all elements of $\mathfrak{p}''$ which are not in $\bigcup_{\sigma \in G \backslash G_y} \sigma(\mathfrak{p})$. Then $\mathfrak{p}'' \subseteq J \cup \bigcup_{\sigma \in G \backslash G_y} (\sigma(\mathfrak{p}) \cap S^{G_y})$. Since $\mathfrak{p}$ is a prime ideal in S, $\sigma(\mathfrak{p}) \cap S^{G_y}$ is a prime ideal in S^{G_y} and hence we can apply prime avoidance again: since g is in $\mathfrak{p}''$ but not in $\sigma(\mathfrak{p})$ for any $\sigma \in G \backslash G_y$, we obtain $\mathfrak{p}'' \subseteq J$ and hence $\mathfrak{p}'' = J$ as J was defined to be a subideal of $\mathfrak{p}''$. This shows that there are $f_1, \ldots, f_n \in \mathfrak{p}'' \backslash \bigcup_{\sigma \in G \backslash G_y} \sigma(\mathfrak{p})$ such that $\mathfrak{p}'' = (f_1, \ldots, f_n)_{S^{G_y}}$.

Let $\sigma_1, \ldots, \sigma_r \in G$ be a set of left coset representatives of G_y in G with $\sigma_1 \in G_y$. For $i = 1, \ldots, n$ we define $g_i := \prod_{j=2}^{r} \sigma_j(f_i)$. By the choice of the f_i we have $g_i \in S^{G_y} \backslash \mathfrak{p}''$ and hence $g_1, \ldots, g_n$ are units in $S^{G_y}_{\mathfrak{p}''}$. Then the ideal $\mathfrak{p}''_{\mathfrak{p}''}$ in $S^{G_y}_{\mathfrak{p}''}$ is generated by $f_1 g_1, \ldots, f_n g_n$. As $f_i \in S^{G_y}$ we obtain that $f_i g_i = \prod_{j=1}^{r} \sigma_j(f_i) \in S^G \cap \mathfrak{p}'' = \mathfrak{p}'$, so $\mathfrak{p}''_{\mathfrak{p}''} \subseteq \mathfrak{p}'_{\mathfrak{p}'}(S^{G_y})_{\mathfrak{p}''}$. The other inclusion is clear. □

Kemper [34, Lemma 1.2] states that every inclusion of Noetherian local rings satisfying the two properties proven in Lemma 8.17 induces an isomorphism of completions. However, the proof for this given in [34] is wrong; it uses a result from Eisenbud's book [17, Theorem 7.2(a)] which only holds for inclusions of local rings $R \hookrightarrow S$ for which S is finitely generated as an R-module. So we give an alternative proof of Theorem 8.16 here which does not need this argument. For this we use the material on étale morphisms developed in the previous section. The special case where R is a field in the following proof also shows that Theorem 1.1 of Kemper's article [34] is nevertheless true.

Proof of Theorem 8.16. The inclusion $S^G \hookrightarrow S^{G_y}$ induces a morphism of affine schemes $h : \operatorname{Spec}(S^{G_y}) \to \operatorname{Spec}(S^G)$. Lemma 8.17 implies that h is unramified at the point $\mathfrak{p}'' \in \operatorname{Spec}(S^{G_y})$. Then Lemma 8.3 implies that there is an open subscheme $U \subseteq \operatorname{Spec}(S^{G_y})$ with $\mathfrak{p}'' \in U$ such that $h|_U$ is unramified. Since $\operatorname{Spec}(S^G)$ is normal by Theorem 2.5 and for every $\mathfrak{q} \in U$ the induced map $(S^G)_{h(\mathfrak{q})} \to (S^{G_y})_{\mathfrak{q}}$ of local rings is a restriction of the

inclusion $\mathrm{Quot}(S^G) \to \mathrm{Quot}(S^{G_y})$ and therefore injective, Theorem 8.4 implies that $h|_U$ is étale. By Lemma 8.17b) and Theorem 8.5 it follows that h induces an isomorphism $\widehat{(S^G)_{\mathfrak{p}'}} \cong \widehat{(S^{G_y})_{\mathfrak{p}''}}$. □

Corollary 8.18. *In the situation of Theorem 8.16 we additionally define* $\mathfrak{p}_0 := \{f \in S | f(0) \in \mathfrak{m}\}$ *and* $\mathfrak{p}_0'' := \mathfrak{p}_0 \cap S^{G_x}$. *Then*

$$\widehat{(S^G)_{\mathfrak{p}'}} \cong \widehat{(S^{G_y})_{\mathfrak{p}_0''}}.$$

Proof. We show that $(S^{G_y})_{\mathfrak{p}''} \cong (S^{G_y})_{\mathfrak{p}_0''}$; then the corollary follows from Theorem 8.16. The map $\varphi : S \to S$ which maps a polynomial $f \in S = R[x_1, \ldots, x_n]$ to the polynomial $f((x_1, \ldots, x_n) + y)$ is an automorphism of S which is compatible with the action of G_y, so it restricts to an automorphism of S^{G_y}. Furthermore we have $\mathfrak{p}_0 = \varphi(\mathfrak{p})$ and hence $\mathfrak{p}_0'' = \varphi(\mathfrak{p}'')$. Thus the claimed isomorphism follows. □

Theorem 8.19. *Let R be a Noetherian ring and let $G \subseteq Gl_n(R)$ be a finite group and $y \in R^n$ a point with $\mathfrak{m}$-stable stabilizer for every maximal ideal $\mathfrak{m} \subset R$. Then for every local property $\mathcal{P}$ we have*

$$\mathcal{P}(R[x_1, \ldots, x_n]^G) \implies \mathcal{P}(R[x_1, \ldots, x_n]^{G_x}).$$

Proof. By part (iv) of the definition of a local property we may assume that R is local and hence $S = R[x_1, \ldots, x_n]$ is *local. We use the notation from Theorem 8.16 and Corollary 8.18. $\mathcal{P}(S^G)$ implies $\mathcal{P}((S^G)_{\mathfrak{p}'})$ by statement (iii) from the definition of a local property. Hence by (i) we have $\mathcal{P}(\widehat{(S^G)_{\mathfrak{p}'}})$ and by Corollary 8.18 also $\mathcal{P}(\widehat{(S^{G_y})_{\mathfrak{p}_0''}})$. Now (i) implies $\mathcal{P}((S^{G_y})_{\mathfrak{p}_0''})$ and since $\mathfrak{p}_0''$ is the homogeneous maximal ideal in the *local ring S^{G_y} statement (ii) implies $\mathcal{P}(S^{G_y})$. □

We are now ready to prove the main result of this chapter.

Theorem 8.20. *Let R be a Noetherian ring and let $G \subseteq Gl_n(R)$ be a finite group and $y \in R^n$ a point with $\mathfrak{m}$-stable stabilizer for every maximal ideal $\mathfrak{m} \subset R$.*

a) If $R[x_1, \ldots, x_n]^G$ is regular, a Gorenstein ring, or a Cohen-Macaulay ring, then the same holds for $R[x_1, \ldots, x_n]^{G_y}$.

b) If R is an allowed base ring and $R[x_1, \ldots, x_n]^G$ is a quasi-Gorenstein ring, then $R[x_1, \ldots, x_n]^{G_y}$ is also a quasi-Gorenstein ring.

c) We have $\mathrm{cmdef}(R[x_1, \ldots, x_n]^{G_y}) \leq \mathrm{cmdef}(R[x_1, \ldots, x_n]^G)$.

Proof. Parts (a) and (b) directly from Theorem 8.19 and Proposition 8.7. For part (c) let $n \coloneqq \mathrm{cmdef}(R[x_1, \ldots, x_n]^G)$; then $R[x_1, \ldots, x_n]^G$ satisfies the property $\mathcal{P}_n$ defined in Proposition 8.12. So by Theorem 8.19 and Proposition 8.12, $R[x_1, \ldots, x_n]^{G_y}$ also satisfies $\mathcal{P}_n$; the statement follows. □

The fact that $R[x_1, \ldots, x_n]^G$ is factorial does not imply that $R[x_1, \ldots, x_n]^{G_y}$ is factorial, not even if R is a field. This is shown by the following example.

Example 8.21. Let R be a Noetherian normal domain with $\mathrm{char}(R) \neq 2$ which contains no nontrivial third root of unity; for example, this holds for $R = \mathbb{Q}$ or for every R with $\mathrm{char}(R) = 3$. Let $S := R[x_1, \ldots, x_4]$ and $G := A_4$ viewed as a group of permutation matrices in $Gl_4(R)$. Furthermore we define $y := (1, 1, 0, 0) \in R^4$; since G is a permutation group, y has $\mathfrak{m}$-stable stabilizer for every maximal ideal $\mathfrak{m} \subset R$ by Remark 8.14. We claim that S^G is factorial but S^{G_y} is not. First of all, G contains no pseudoreflections because a permutation matrix is a pseudoreflection if and only if the corresponding permutation is a transposition. Hence S^G is factorial if and only if there is no nontrivial R-valued character of G, similar for S^{G_y}. G_y is cyclic of order two, generated by $\sigma := (1\ 2)(3\ 4)$, so there is a nontrivial character $G_y \to R^\times$ sending σ to -1. Hence S^{G_y} is not factorial. On the other hand, let χ be any character $G \to R^\times$. Since R contains no nontrivial third root of unity, χ maps every 3-cycle to 1. But the alternating groups are generated by 3-cycles, so we obtain that χ must be the trivial character. Hence S^G is factorial.

9 Conclusion

9.1 Summary of the main results

We begin this summary with the three main results of this thesis concerning the question of when a ring of arithmetic invariants has certain properties. Let always R be a ring and $G \subseteq Gl_n(R)$ a finite group.

1. Theorem 4.22: Assume that R is a Dedekind domain. If $\mathrm{Quot}(R)[x_1, \ldots, x_n]^G$ and all $(R/\mathfrak{p})[x_1, \ldots, x_n]^G$ where $\mathfrak{p} \subset R$ is a maximal ideal with $|G| \in \mathfrak{p}$ are polynomial rings generated by homogeneous elements of the same degrees, then $R[x_1, \ldots, x_n]^G$ is regular. If G acts faithfully on $(R/\mathfrak{p})^n$ for all $\mathfrak{p}$ as above, then the converse also holds. Moreover, under the same assumptions, if R is a principal ideal domain, then $R[x_1, \ldots, x_n]^G$ is isomorphic to a polynomial ring.

2. Corollary 6.6: Assume that R is a Noetherian normal domain. Then $R[x_1, \ldots, x_n]^G$ is factorial if and only if R is factorial and every character $\chi : G \to R^\times$ which takes the value 1 on every pseudoreflection takes the value 1 on every element of G.

3. Theorem 7.56: Assume that R is an allowed base ring in the sense of Definition 7.51. Then $R[x_1, \ldots, x_n]^G$ is quasi-Gorenstein if and only if the differential character of G is equal to the determinant.

Next we want to consider the question of whether some ring-theoretic property of the invariant ring remains valid under certain changes of the base ring or the group. For simplicity, we assume that R is a Dedekind domain. Let $G \subseteq Gl_n(R)$ be a finite group and $K := \mathrm{Quot}(R)$. Furthermore, let $\mathcal{P}$ be a ring theoretic property which $R[x_1, \ldots, x_n]^G$ may or may not satisfy. We consider the following statements.

1. If $K[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$, then $R[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$.

2. If $K[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$ and $|G|$ is invertible in R, then $R[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$.

3. If $R[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$, then for every prime ideal $\mathfrak{p} \subset R$ with $|G| \notin \mathfrak{p}$, $(R/\mathfrak{p})[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$.

4. If $R[x_1, \ldots, x_n]^G$ satisfies $\mathcal{P}$, then $R[x_1, \ldots, x_n]^{G_y}$ satisfies $\mathcal{P}$ for every $y \in R^n$ which has $\mathfrak{m}$-stable stabilizer, see Definition 8.13, for every maximal ideal $\mathfrak{m} \subset R$.

The following table collects all results on the question of whether these statements are true for the following properties: regularity, Cohen-Macaulay, Gorenstein, quasi-Gorenstein, factoriality. In the case of factoriality, we make the stronger assumption that R is a principal ideal domain (PID). The table also contains the places where the respective results can be found in this thesis.

$\mathcal{P}$	Statement 1	Statement 2	Statement 3	Statement 4
Regularity	False, Example 3.10	True, Theorem 4.20	True, Theorem 8.20	True, Proposition 4.24
Cohen-Macaulay	False, Example 3.12	True, Theorem 3.14	True, Theorem 8.20	True, see below
Gorenstein	False, Example 3.13	True, Corollary 7.57	True, Theorem 8.20	True, Theorem 7.39
quasi-Gorenstein	True, Theorem 7.56	True, Theorem 7.56	True, Theorem 8.20	True, Theorem 7.39
Factoriality (with R a PID)	True, Theorem 6.5	True, Theorem 6.5	False, Example 8.21	False, Example 6.9

We did not consider Statement 4 for the Cohen-Macaulay property before, but this is almost trivial: there is nothing to show in Statement 4 if $\mathfrak{p} = 0$, so as R is a Dedekind domain, we may assume that $\mathfrak{p}$ is maximal. Then $R/\mathfrak{p}$ is a field and by assumption $\mathrm{char}R/\mathfrak{p}$ does not divide $|G|$, so $(R/\mathfrak{p})[x_1, \ldots, x_n]^G$ is always a Cohen-Macaulay ring by Theorem 2.20 even if $R[x_1, \ldots, x_n]^G$ is not.

9.2 Outlook

Here are some open problems which arise in the context of the topics considered in this thesis:

1. Prove or disprove conjecture Conjecture 4.23.
2. What can be said about the invariants of a pseudoreflection group $G \subseteq Gl_n(R)$ over a discrete valuation ring R with maximal ideal $\mathfrak{m}$ if G does not act faithfully on $(R/\mathfrak{m})^n$. This is the case where Theorem 4.7 is not applicable.
3. Is it possible to generalize parts of the results of Chapter 4 to base rings which are not necessarily Dedekind domains? In particular, it might be possible to generalize the results of Section 4.1 to invariants over regular local rings of dimension greater than one.
4. Does Theorem 8.20 hold also without the assumption that y has $\mathfrak{m}$-stable stabilizer for all maximal ideals $\mathfrak{m} \subset R$? While at first it seems natural to assume that this

should be true, a closer look shows that the equality of the stabilizers over R and $R/\mathfrak{m}$ is really essential for our proof, so I suppose that if this is true, then the proof requires a different strategy than the one used in [34] and in this thesis.

5. Can one prove analogous results to Theorem 8.20c) for other parameters than the Cohen-Macaulay defect, e.g. the polynomial defect, the complete intersection defect, or the Gorenstein defect? This has been done by Kemper [34] over fields and thus it seems natural to hope that similar results also hold over rings.

6. It might also be worthwhile to study algorithmic aspects of arithmetic invariant theory. An algorithm which computes the ring of invariants $R[x_1, \ldots, x_n]$ using Gröbner bases over R has been given by Kemper [37], but it might be possible to avoid Gröbner bases over R and instead first compute generators for the invariant ring over $K := \mathrm{Quot}(R)$ and then add some additional generators to obtain a generating set of the invariant ring over R.

7. Another important topic in invariant theory not covered in this thesis are degree bounds: for this we consider a ring of invariants $R[x_1, \ldots, x_n]^G$ where R is Noetherian and G is finite. Then the ring of invariants is finitely generated as an R-algebra, so there is a number $\beta \in \mathbb{N}$ such that $R[x_1, \ldots, x_n]^G$ can be generated as an R-algebra by elements of degree at most β. A classical result, see Derksen and Kemper [16, Theorem 3.2.2], says that if R is a field and $|G| \in R^\times$, then we can choose $\beta = |G|$. If R is an arbitrary field, then Symonds [58] proved that we can choose $\beta = (|G|-1)n$ and it might be interesting to also consider this question in the case where R is not a field; some special cases of this have been handled by Almuhaimeed [1, Section 4.2].

Some more open problems on arithmetic invariant rings, in particular concerning the Cohen-Macaulay property, have been collected by Almuhaimeed [1, Chapter 8].

Bibliography

[1] Areej Almuhaimeed. *Group Actions on Rings*. PhD thesis, University of Manchester, 2018.

[2] Yoichi Aoyama. Some basic results on canonical modules. *Journal of Mathematics of Kyoto University*, 23-1:85–94, 1983.

[3] Yoichi Aoyama and Shiro Goto. On the endomorphism ring of the canonical module. *Journal of Mathematics of Kyoto University*, 25-1:21–30, 1985.

[4] David Benson. *Polynomial Invariants of Finite Groups*. Cambridge University Press, Cambridge, 1993.

[5] Nicolas Bourbaki. *Commutative Algebra, Chapters 1-7*. Springer-Verlag, New York, 1989.

[6] Amiram Braun. On the Gorenstein property for modular invariants. *Journal of Algebra*, 345:81–99, 2011.

[7] M. P. Brodmann and R. Y. Sharp. *Local Cohomology. An Algebraic Introduction with Geometric Applications*. Cambridge University Press, Cambridge, 2nd edition, 2013.

[8] Abraham Broer. The direct summand property in modular invariant theory. *Transformation groups*, 10:5–27, 2005.

[9] Michel Broué. *Introduction to Complex Reflection Groups and Their Braid Groups*. Springer-Verlag, Berlin, 2010.

[10] Juliette Bruce and Daniel Erman. A probabilistic approach to systems of parameters and noether normalization. preprint, available at https://arxiv.org/abs/1604.01704, 2016.

[11] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*. Cambridge University Press, Cambridge, 1993.

[12] Claude Chevalley. Invariants of finite groups generated by reflections. *American Journal of Mathematics*, 77:778–782, 1955.

[13] Ted Chinburg, Laurent Moret-Bailly, Georgios Pappas, and Martin Taylor. Finite morphisms to projective space and capacity theory. *Journal für die reine und angewandte Mathematik*, 727:69–84, 2017.

[14] Charles W. Curtis and Irving Reiner. *Methods of Representation Theory, volume 1.* Wiley, New York, 1981.

[15] Harm Derksen and Gregor Kemper. *Computational Invariant Theory.* Springer-Verlag, Berlin, Heidelberg, 1st edition, 2002.

[16] Harm Derksen and Gregor Kemper. *Computational Invariant Theory.* Springer-Verlag, Berlin, Heidelberg, 2nd edition, 2015.

[17] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, New York, 1995.

[18] Peter Fleischmann and Chris Woodcock. Relative invariants, ideal classes and quasi-canonical modules of modular rings of invariants. *Journal of Algebra*, 348:110–134, 2011.

[19] Otto Forster. *Lectures on Riemann Surfaces.* Springer-Verlag, New York, 1981.

[20] Robert M. Fossum. *The Divisor Class Group of a Krull Domain.* Springer-Verlag, Berlin, 1973.

[21] Ofer Gabber, Qing Liu, and Dino Lorenzini. Hypersurfaces in projective schemes and a moving lemma. *Duke Mathematical Journal*, 164:1187–1270, 2015.

[22] Manfred Göbel. Computing Bases for Rings of Permutation-invariant Polynomials. *Journal of Symbolic Computation*, 19:285–291, 1995.

[23] Manfred Göbel. On the Number of Special Permutation-Invariant Orbits and Terms. *Applicable Algebra in Engineering, Communication, and Computing*, 8:505–509, 1997.

[24] Robert Gilmer and Raymond C. Heitmann. On $\mathrm{Pic}(R[x])$ for R seminormal. *Journal of Pure and Applied Algebra*, 16:251–257, 1980.

[25] Shiro Goto and Keiichi Watanabe. On graded rings, I. *Journal of the Mathematical Society of Japan*, 30-2:179–213, 1978.

[26] Alexander Grothendieck and Jean Dieudonné. *Éléments de géométrie algébrique, IV.* Inst. Hautes Études Sci. Publ. Math., 1964-1967.

[27] Robin Hartshorne. *Algebraic Geometry.* Springer, New York, 1977.

[28] Jürgen Herzog and Ernst Kunz, editors. *Der kanonische Modul eines Cohen-Macaulay-Rings*, volume 238 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1971.

[29] Melvin Hochster and John A. Eagon. Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci. *American Journal of Mathematics*, 93:1020–1058, 1971.

[30] Shin Ikeda. On the Gorensteinness of Rees algebras over local rings. *Journal of Mathematics of Kyoto University*, 102:135–154, 1986.

[31] Ming-Chang Kang. Picard groups of some rings of invariants. *Journal of Algebra*, 58:455–461, 1979.

[32] Gregor Kemper. Calculating Invariant Rings of Finite Groups over Arbitrary Fields. *Journal of Symbolic Computation*, 21:351–366, 1996.

[33] Gregor Kemper. On the Cohen-Macaulay Property of Modular Invariant Rings. *Journal of Algebra*, 215:330–351, 1999.

[34] Gregor Kemper. Loci in Quotients by Finite Groups, Pointwise Stabilizers and the Buchsbaum Property. *Journal für die reine und angewandte Mathematik*, 547:69–96, 2002.

[35] Gregor Kemper. *A Course in Commutative Algebra.* Springer, New York, 2011.

[36] Gregor Kemper. The Cohen-Macaulay Property and Depth in Invariant Theory. In *Proceedings of the 33rd Symposium on Commutative Algebra in Japan*, pages 53–63, 2012.

[37] Gregor Kemper. Using Extended Derksen Ideals in Computational Invariant Theory. *Journal of Symbolic Computation*, 72:161–181, 2016.

[38] Tsit-Yuen Lam. *Lectures on Modules and Rings.* Springer, New York, 1999.

[39] Serge Lang. *Algebra.* Springer, New York, 2002.

[40] Jacob Matijevic and Paul Roberts. A conjecture of Nagata on graded Cohen-Macaulay rings. *Journal of Mathematics of Kyoto University*, 14-1:125–128, 1974.

[41] Hideyuki Matsumura. *Commutative Ring Theory.* Cambridge University Press, Cambridge, 1987.

[42] James S. Milne. *Étale Cohomology.* Princeton University Press, Princeton, 1980.

[43] David Mundelius. Arithmetic invariants of pseudoreflection groups over Dedekind domains and regular graded algebras. preprint, available at https://arxiv.org/abs/1711.08201, 2017.

[44] Masayoshi Nagata. Some questions on rational actions of groups. In *Algebraic geometry. Papers presented at the Bombay colloquium, 1968*, pages 323–334, London, 1969. Oxford University Press.

[45] Haruhisa Nakajima. Relative Invariants of Finite Groups. *Journal of Algebra*, 79:218–234, 1982.

[46] Jürgen Neukirch. *Algebraic Number Theory.* Springer, Berlin, 1999.

[47] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, pages 28–35, 1926.

[48] D. Notbohm. For Which Pseudo Reflection Groups Are the p-adic Polynomial Invariants Again a Polynomial Algebra. *Journal of Algebra*, 214:553–570, 1999.

[49] Erich Platte and Uwe Storch. Invariante reguläre Differentialformen auf Gorenstein-Algebren. *Mathematische Zeitschrift*, 157:1–11, 1977.

[50] Pierre Samuel. *Lectures on Unique Factorization Domains*. Tata Institute, Bombay, 1964.

[51] Sean Sather-Wagstaff and Sandra Spiroff. Maps on Divisor Class Groups Induced by Ring Homomorphisms of Finite Flat Dimension. *Journal of Commutative Algebra*, 1:567–590, 2009.

[52] Jean-Pierre Serre. Groupes finis d'automorphismes d'anneaux locaux régulieres. In *Colloque d'Algebre*, pages 8–01 – 8–11, Paris, 1968. Secrétariat mathématique.

[53] Jean-Pierre Serre. *Local Fields*. Springer, New York, 1979.

[54] Geoffrey Colin Shephard and John Arthur Todd. Finite Unitary Reflection Groups. *Canadian Journal of Mathematics*, 6:274–304, 1954.

[55] Larry Smith. On the invariant theory of finite pseudo reflection groups. *Archiv der Mathematik*, 44:225–228, 1985.

[56] Larry Smith. Some Rings of Invariants that are Cohen-Macaulay. *Canadian Mathematical Bulletin*, 39:238–240, 1996.

[57] Richard P. Stanley. Hilbert functions of graded algebras. *Advances in Mathematics*, 28:57–83, 1978.

[58] Peter Symonds. On the Castelnuovo-Mumford regularity of rings of polynomial invariants. *Annals of Mathematics*, 174:499–517, 2011.

[59] Keiichi Watanabe. Certain invariant subrings are Gorenstein I. *Osaka Journal of Mathematics*, 11:1–8, 1974.

[60] Keiichi Watanabe. Certain invariant subrings are Gorenstein II. *Osaka Journal of Mathematics*, 11:379–388, 1974.

[61] Charles Weibel. *An introduction to homological algebra*. Cambridge University Press, Cambridge, 2003.

List of symbols

$\hat{A}$ Completion of the local ring A. 76

$B_I R$ Blowup algebra of I in R. 27

$B_{I_1,\ldots,I_n} R$ Tensor product of blowup algebras. 28

${}^*\mathcal{C}(S)$ Category of graded S-modules. 14

$\mathrm{Cl}(R)$ Ideal class group of the Dedekind domain R. 11

$\mathrm{Cl}(A)$ Divisor class group of A. 37

$\mathrm{cmdef}(A)$ Cohen-Macaulay defect of A. 77

$D(A)$ Group of all divisorial ideals of A. 36

$\mathcal{D}_{B/A}$ Dedekind different of B over A. 57

$\mathcal{D}_{B/A}^{-1}$ Inverse different of B over A. 57

$\mathcal{D}_{B/A,\nu}$ Twisted different of B over A. 57

$\mathcal{D}_{B/A,\nu}^{-1}$ Twisted inverse different of B over A. 57

$\mathrm{Div}(A)$ Group of divisors of A. 36

$\mathrm{div}(\mathfrak{a})$ Divisor associated to the fractional ideal $\mathfrak{a}$. 37

$\mathrm{Div}(i)$ Map on groups of divisors induced by the inclusion $i : A \to B$. 38

$e(\mathfrak{q}, \mathfrak{p})$ Ramification index of $\mathfrak{p}$ in $\mathfrak{q}$. 6

$E_A(M)$ Injective hull of the A-module M. 51

${}^*E_S(M)$ *Injective hull of the graded S-module M. 54

${}^*\mathrm{Ext}_S^r(M, N)$ r-th graded Ext-module. 14

$G_{\mathfrak{a}}$ Stabilizer subgroup of the ideal $\mathfrak{a} \subseteq S$ in $G \subseteq \mathrm{Aut}(S)$. 78

$G^i(\mathfrak{q})$ Inertia group of $\mathfrak{q}$. 7

List of symbols

G_y Stabilizer subgroup of $y \in R^n$ in $G \subseteq Gl_n(R)$. 78

$H^n_I(M)$ n-th local cohomology of M with support in I. 52

${}^*H^n_{\mathfrak{m}}(M)$ Graded local cohomology of M. 54

${}^*\mathrm{Hom}_S(M,N)$ Module of graded homomorphisms $M \to N$. 14

$\kappa(\mathfrak{p})$ Quotient field of $S/\mathfrak{p}$. 30

K_A Canonical module of the local ring A. 52

${}^*K_S$ Graded canonical module of S. 54

$\kappa(y)$ Residue field of a scheme Y at the point $y \in Y$. 75

M^* Dual of the module M. 35

$\overline{M}$ Reflexive closure of the module M. 35

$M(m)$ Graded module M with degrees shifted by $m \in \mathbb{Z}$. 14

$\mathcal{O}_{Y,y}$ Stalk of the sheaf $\mathcal{O}_Y$ at y. 75

$\mathrm{Pic}(A)$ Picard group of A. 41

$\mathrm{Pic}(\varphi)$ Map on Picard groups induced by φ. 42

$\mathrm{Prin}(A)$ Group of principal divisors of A. 37

$\mathcal{R}^G$ Reynolds operator. 6

S_+ Homogeneous ideal $\bigoplus_{d>0} S_d$ in a graded ring S. 12

S^G_χ Module of semi-invariants. 37

S^G Ring of invariants of $G \subseteq \mathrm{Aut}(S)$. 5

$S(M)$ Symmetric algebra over the module M. 5

Tr^G Transfer map. 6

Tr^G_ν Twisted transfer map. 56

$v_{\mathfrak{p}}$ Discrete valuation associated to the valuation ring $A_{\mathfrak{p}}$. 36

$X^{(1)}(A)$ Set of all prime ideals in A of height one. 6

Index