Technische Universität München
Zentrum Mathematik

Algorithms for the Computation of Invariant Rings

Tobias Michael Kamke

Technische Universität München
Zentrum Mathematik

Algorithms for the Computation of Invariant Rings

Tobias Michael Kamke

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:		Univ.-Prof. Dr. Bernd Simeon
Prüfer der Dissertation:	1.	Univ.-Prof. Dr. Gregor Kemper
	2.	apl. Prof. Dr. Friedrich Roesler
	3.	Prof. Dr. Harm Derksen University of Michigan, USA (schriftliche Beurteilung)

Die Dissertation wurde am 03. Februar 2009 bei der Technischen Universität eingereicht und durch die Fakultät für Mathematik am 18. Mai 2009 angenommen.

Für meine Eltern.

Abstract

In this thesis, we present algorithms for the computation of invariant rings. In the first part, we consider the case where a finite group G acts on an affine algebra A via K-algebra automorphisms. We give an algorithm which works for arbitrary affine algebras A, including the case where A is not reduced.
In the second part, we consider a linear algebraic group G acting regularly on an irreducible affine variety and examine the relationship of the quotient field of the invariant ring and the invariant field. This leads to an algorithm for the computation of invariant rings of certain group actions. In particular, this algorithm works for unipotent groups.
In the third part, we study invariants of linear algebraic groups acting regularly on quasi-affine varieties. We present algorithms for the cases where the group is finite or unipotent. We also briefly discuss the case where the group is reductive. Finally, an outline is given of how the problem of computing invariants of arbitrary linear algebraic groups acting regularly on factorial varieties can be reduced to the problem of computing invariants of one-dimensional tori.

Zusammenfassung

Die Arbeit untersucht Algorithmen zur Berechnung von Invariantenringen. Im ersten Teil geht es um die Berechnung von Invarianten endlicher Gruppen, die auf affinen Algebren mittels K-Algebra-Automorphismen operieren. Der hier entwickelte Algorithmus funktioniert für beliebige affine Algebren A, also auch für nicht reduzierte affine Algebren.
Der zweite Teil behandelt reguläre Operationen von linearen algebraischen Gruppen auf irreduziblen affinen Varietäten. Es wird zunächst der Zusammenhang zwischen dem Quotientenkörper des Invariantenrings und dem Invariantenkörper untersucht. Daraus ergibt sich ein Algorithmus zur Berechnung von Invariantenringen gewisser Gruppenoperationen. Insbesondere ist dieser Algorithmus für unipotente Gruppen anwendbar.
Im dritten Teil werden reguläre Operationen von linearen algebraischen Gruppen auf quasi-affinen Varietäten untersucht. Es werden Algorithmen zur Berechnung von Invarianten endlicher und unipotenter Gruppen entwickelt, außerdem wird auch kurz der Fall reduktiver Gruppen diskutiert. Schließlich wird noch ein Verfahren skizziert, welches das Problem der Berechnung von Invarianten beliebiger linearer algebraischer Gruppenoperationen auf faktoriellen Varietäten zurückführt auf das Problem der Berechnung von Invarianten eindimensionaler Tori.

Contents

Introduction

Invariant theory. Invariant theory is a mathematical discipline with a long tradition. It was about 150 years ago that mathematicians started to work in this field. In its very beginnings, it consisted more or less of a loose collection of normal form principles describing various attempts to classify algebraic objects. Today, it is an important branch of mathematics which links to a variety of other fields such as algebraic geometry, representation theory and commutative algebra. Important theorems of algebra, like Hilbert's Basis Theorem and the Syzygy Theorem, have its roots in invariant theory.

Problem setting. Before we can give a short overview of invariant theory, we have to specify the problem setting. The classical situation of invariant theory is the following.* Let K be an algebraically closed field and let G be a linear algebraic group acting regularly on an affine variety $X \subset K^n$. This induces an action of G on the coordinate ring $K[X]$. A regular function $f \in K[X]$ is called invariant if it is a fixed point under this action. The invariant ring, denoted by $K[X]^G$, is defined as the set of all invariants. It has the structure of a K-algebra.

Historical notes. In the 19th century, great effort has been put into the development of tools for the computation of the invariant ring in order to get a comprehensive understanding of its structure. At that time, Gordan was known as the expert in this field. His work concentrated on the cases where G is a classical group. For example, several important results about the special linear group $\mathrm{SL}_n(K)$ are due to him.
It was Hilbert who contributed to this field with radically new ideas. In contrast to most of his predecessors, he used non-constructive methods which were not concerned with concrete computations of the invariant ring. It therefore comes as no surprise that initially, he encountered resistance from the old school invariant theorists. Gordan's first reaction to his work was "Das ist nicht Mathematik. Das ist Theologie."†.
In his well-known papers ([Hil90] and [Hil93]), Hilbert proved that the invariant ring is finitely generated as a K-algebra for an important class of groups, the so-called linearly reductive groups. He raised the question whether this finiteness property can be generalized to arbitrary groups in his famous 14th problem. The latter was open for around 60 years until Nagata succeeded in finding a counter-example, i. e. a regular action of a group G on an affine variety X such that the invariant ring $K[X]^G$ is not finitely generated (cf. [Nag59]). Moreover, Nagata could generalize Hilbert's finite generation result to the class of reductive groups (cf. [Nag64]).
With the appearance of Gröbner bases in the 1960s, a new mathematical branch, computational algebra, entered the field which in turn initiated a revival of the computational

*For a precise treatment of the terms and definitions, see the next chapter.
†"This is theology and not mathematics."

aspect of invariant theory. Eventually, it was the book [Stu93] of Sturmfels which caused a broad interest of the mathematical community in this area. Over the last two decades, computational invariant theory has made significant progress. Naturally, it has been one of the important goals to find an algorithm for computing generators of the invariant ring $K[X]^G$. It comes as no surprise that this has turned out to be extremely difficult in this generality. Therefore, several important special cases have been investigated first.

Achievements in computational invariant theory. In the following, we list the most important achievements in this area in chronological order. In the book of Sturmfels, algorithms can be found for the computation of invariant rings of finite groups. Unfortunately, these methods do not work for arbitrary ground fields K since they depend on a construction which only can be done if the characteristic of the ground field K does not divide the order of the group G.
In [vdE93], van den Essen published a method for the computation of $K[X]^{G_a}$ where X is an irreducible affine variety and $G_a = (K, +)$ is the additive group. Note that since G_a is not reductive, it may happen that $K[X]^{G_a}$ is not finitely generated. In this case, van den Essen's method yields an infinite sequence of generators of the invariant ring.
Later, especially Kemper and Derksen achieved outstanding results in computational invariant theory. They deeply examined the algorithmic aspects of the computation of generators of the invariant ring $K[X]^G$ for various classes of groups.
In [Kem96], Kemper developed an algorithm for the case that G is a finite group. Unlike the work of Sturmfels and others, his method works for arbitrary characteristic of the ground field. In particular, this includes the case, where the characteristic divides the order of the group. Today, there exist high performace implementations of his ideas within the computer algebra system Magma.
In [Der99], Derksen found an algorithm for the computation of $K[X]^G$ in case that X is a vector space and G is a linearly reductive group acting linearly on X. Furthermore, his ideas provide the possibility to compute $K[X]^G$ for arbitrary regular actions of linearly reductive groups on arbitrary affine varieties. Derksen's methods are implemented in Magma, too.
In [Kem03], Kemper could generalize Derksen's work, he succeeded in an algorithm for computing invariants of reductive groups acting linearly on affine space.
Finally, in [DK08], Derksen and Kemper gave a further generalization of their methods to arbitrary actions of reductive groups on arbitrary affine varieties. Moreover, they entered fresh territory and examined non-reductive cases, too. They could generalize van den Essen's algorithm to arbitrary characteristic. Having this as a tool, they could finally construct a method for the computation of $K[X]^G$ if G is a connected unipotent group and X is an irreducible affine variety. Similarly to Essen's construction, their algorithms terminate if and only if the invariant ring is finitely generated. Otherwise, they return an infinite sequence of generators.

An interesting variant of the problem of computing invariant rings is the computation of invariant fields. If X is an irreducible variety, then the invariant field, denoted by $K(X)^G$, is defined as the set of all rational functions which are invariant under the induced group action of G on $K(X)$. It has the structure of a field.

In [MQB99], Müller-Quade and Beth provided an algorithm for the computation of generators of the invariant field for arbitrary linear algebraic groups acting linearly on a vector space X. Later, Kemper generalized their algorithm to arbitrary actions of linear algebraic groups on arbitrary irreducible (algebraic) varieties X (cf. [Kem07]).

Main results

Despite this impressive progress, there are still a lot of open problems in computational invariant theory today. I want to mention two of them which are related to this thesis. First and foremost, there does not exist an algorithm yet for the computation of invariant rings for the general case that an arbitrary linear algebraic group acts on an arbitrary affine variety. Although there is some progress in this direction (see [DK08] and Chapter 4 of this thesis), this problem is still unsolved.
For a solution of this problem it is helpful to examine computational methods for regular group actions on quasi-affine varieties. Up to now – to the best of my knowledge – there has not been any computational treatment of this generalized situation. In this thesis, various algorithms concerning this quasi-affine case will be developed. This includes algorithms for the computation of invariant rings of finite and unipotent groups. Furthermore – corresponding to the original motivation for considering the quasi-affine situation – a sketch of a method is given for reducing the problem of computing invariants of arbitrary linear algebraic groups acting on factorial varieties to the problem of computing invariants of one-dimensional tori acting on quasi-affine varieties.
Another open problem is motivated by the paper [Nag64] of Nagata. As mentioned earlier, he proved that the invariant ring of a reductive group acting on an affine variety is always finitely generated. In fact, he proved the more general result that the invariant ring of a reductive group acting algebraically on an arbitrary affine algebra is always finitely generated. In particular, this includes non-reduced affine algebras which do not occur as coordinate rings of affine varieties. Therefore, the non-reduced case is not covered by the existing algorithms of Derksen and Kemper. In this thesis, an algorithm for the case of finite group actions will be developed which works for non-reduced algebras, too.
Finally, it is always a matter of interest to optimize the already known algorithms of computational invariant theory. In this spirit, an alternative algorithm for computing invariants of unipotent groups acting on irreducible affine varieties will be constructed. This algorithm has been implemented in the computer algebra system Magma. This thesis includes both the source code as well as a basic runtime examination.

Structure of the thesis

The (basic) requisites on algebraic geometry, on invariant theory and on computational algebra are treated in the first chapter. It contains a precise treatment of the terms and definitions which have been used in this preface in a somewhat sloppy way. Moreover, for the lack of adequate references, this chapter includes the proofs of some minor elementary results. Most of the material presented here should be well-known for invariant theorists

with a computational background.

An investigation of computational aspects of reductive groups acting on non-reduced affine algebras is done in the second chapter. As mentioned above, this leads to an algorithm for computing invariants of finite groups. Furthermore, this chapter includes a discussion about the computational difficulties which arise for infinite group actions on non-reduced affine algebras.

The third chapter starts with an examination of the relation of the quotient field of the invariant ring and the invariant field of linear algebraic groups acting on irreducible affine varieties. This leads to an algorithm for computing invariants of certain group actions. In particular, this algorithm works for unipotent group actions giving an alternative to a method of Derksen and Kemper for this case. This chapter also includes a basic runtime examination of an implementation of this algorithm.

A generalization of computational invariant theory to a wider class of varieties, the quasi-affines, is the content of chapter four. In the course of this chapter, various algorithms are developed for this case. The chapter closes with a discussion about how an investigation of quasi-affine varieties might be helpful for the construction of an algorithm for computing invariant rings of arbitrary linear algebraic groups acting on factorial varieties.

Finally, a listing of the source code of an implementation of the algorithms which have been developed in chapter three can be found in the appendix.

Acknowledgements

I would like to thank my advisor Prof. Dr. Gregor Kemper for his supervision, for his help during research and with the manuscript as well as for his many useful suggestions. I very much enjoyed the fruitful discussions with him. He always kept me on the right track but also gave me plenty of time to work on my own.
Special thank also goes to Dr. Frank Himstedt for his support concerning questions of representation theory of groups.
It was a privilege for me to write this thesis within the programme "TopMath – Angewandte Mathematik mit Promotion". In this context, I would like to thank Dr. Christian Kredler, Dr. Ralf Franken und Andrea Echtler who took care that organizational matters concerning this programme went smoothly.
Finally, I gratefully acknowledge the Konrad-Adenauer-Stiftung for supporting this work financially.

1 Preliminaries

In this chapter, we give a short introduction to algebraic geometry, invariant theory and computational algebra. It covers some basic material which will be necessary for the understanding of the thesis. The selection of the material is mainly driven by what will be used in the following chapters, by no means should the content of the sections be considered as a comprehensive introduction to the three theories. We assume that the reader is familiar with the fundamental concepts of commutative algebra, we do not give a survey of the relevant aspects here. An (advanced) introduction to commutative algebra can be found in the book [Eis95].
We have not included the proofs of standard results in this chapter. They can be found in the books which are mentioned at the beginning of the respective sections.

All rings in this thesis are assumed to be commutative with 1.

1.1 Algebraic geometry

This section covers some facts about algebraic geometry. We try to use this theory with as little machinery as possible, thus the material presented here is rather basic and somewhat simplified in the sense that it is not carried out in the usual generality of abstract algebraic geometry. Note that in this section all proofs have been omitted. For an advanced introduction to algebraic geometry (including all the proofs of the basic facts presented here), see [Har77].

Throughout this section, let K be a fixed algebraically closed field and let $n \in \mathbb{N}$ be a natural number. Moreover, let $x_1, \ldots, x_n$ be indeterminates over K.
The ***n*-dimensional affine space** is defined as the set $K^n = \{(\xi_1, \ldots, \xi_n);\ \xi_1, \ldots, \xi_n \in K\}$. Every polynomial $f \in K[x_1, \ldots, x_n]$ defines a function on K^n in the natural way, i. e.

$$K^n \longrightarrow K,\ (\xi_1, \ldots, \xi_n) \longmapsto f(\xi_1, \ldots, \xi_n).$$

A function $K^n \longrightarrow K$ which can be written in this way for a suitable polynomial f is called a polynomial function.

Definition 1.1. *Let $I \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal. Then*

$$\mathrm{Var}(I) := \{(\xi_1, \ldots, \xi_n) \in K^n;\ f(\xi_1, \ldots, \xi_n) = 0 \text{ for all } f \in I\}$$

is called the **affine variety** *defined by I.*

Remarks. (i) Let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. The ideal generated by $f_1, \ldots, f_m$ in $K[x_1, \ldots, x_n]$ will be denoted by $(f_1, \ldots, f_m)_{K[x_1,\ldots,x_n]}$ or simply $(f_1, \ldots, f_m)$ if no misunderstanding can arise. The affine variety defined by $(f_1, \ldots, f_m)$ will be written as $\mathrm{Var}(f_1, \ldots, f_m)$.

(ii) With the notation of the preceding definition, let $X = \mathrm{Var}(I)$ be the affine variety defined by I. If it is not desired to refer specifically to the defining ideal I, the set X is just called an affine variety. To make the field K explicit in this case, i. e. to explicitly mention that X is contained in K^n for some $n \in \mathbb{N}$, it is common to say that X is an affine variety over K.

(iii) When there is no danger of confusion, we sometimes omit the word 'affine' and simply speak of a variety.

Throughout this section, all varieties are over K.

Lemma 1.2. *The union of finitely many affine varieties and the intersection of affine varieties is an affine variety, again. Moreover, the empty set $\emptyset \subset K^n$ and the whole affine space K^n are affine varieties.* ∎

By this lemma, the n-dimensional affine space can be given the structure of a topological space.

Definition 1.3. *The* **Zariski topology** *on K^n is the topology where the closed sets are given by the set of all affine varieties contained in K^n. More explicitely, a subset $X \subset K^n$ is called Zariski-closed if there exists an ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ such that $X = \mathrm{Var}(I)$.*
Let $X \subset K^n$ be an affine variety. The Zariski topology on K^n induces the subspace topology on X which is also called Zariski topology. In particular, every affine variety has the structure of a topological space.

Definition 1.4. *Let $X \subset K^n$. Then the vanishing ideal of X is defined as*

$$\mathrm{Id}(X) := \{f \in K[x_1, \ldots, x_n];\ f(\xi_1, \ldots, \xi_n) = 0 \text{ for all } (\xi_1, \ldots, \xi_n) \in X\} \trianglelefteq K[x_1, \ldots, x_n].$$

Theorem 1.5 (Hilbert's Nullstellensatz). *There is an inclusion-reversing one-to-one correspondence between affine varieties contained in K^n and radical ideals of $K[x_1, \ldots, x_n]$ given by*

$$\begin{aligned} \{\text{affine varieties } \subset K^n\} &\longrightarrow \{\text{radical ideals of } K[x_1, \ldots, x_n]\} \\ X &\longmapsto \mathrm{Id}(X) \end{aligned}$$

and

$$\begin{aligned}\{\textit{radical ideals of } K[x_1,\dots,x_n]\} &\longrightarrow \{\textit{affine varieties } \subset K^n\}\\ I &\longmapsto \mathrm{Var}(I)\end{aligned}$$

■

Definition 1.6. *Let $X \subset K^n$ be an affine variety. A function $f : X \longrightarrow K$ is called* **regular on X** *if for every $p \in X$ there exists an open neighbourhood $V \subset X$ of p and polynomials $N, D \in K[x_1,\dots,x_n]$ such that $0 \notin D(V)$ and $f(v) = N(v)/D(v)$ for all $v \in V$. The set of regular functions on X has the structure of a K-algebra (resp. is the zero ring if $X = \emptyset$) and is denoted by $K[X]$. It is called the* **ring of regular functions** *of X.*

Remark 1.7. Let $X \subset K^n$ be an affine variety. Then $K[x_1,\dots,x_n]/\operatorname{Id}(X)$ is isomorphic to the ring of regular functions $K[X]$ via the following map

$$K[x_1,\dots,x_n]/\operatorname{Id}(X) \longrightarrow K[X],\ f + \operatorname{Id}(X) \longmapsto ((\xi_1,\dots,\xi_n) \mapsto f(\xi_1,\dots,\xi_n))\,.$$

The ring $K[x_1,\dots,x_n]/\operatorname{Id}(X)$ is called the **coordinate ring** of X. Because of the above isomorphism, the coordinate ring and the ring of regular functions are usually identified.♢

For ease of notation, we sometimes use the following relative forms of the definitions of Var and Id. Let X be an affine variety and let $L \trianglelefteq K[X]$ be an ideal. Then, similarly to the above, this corresponds to a Zariski-closed subset of X in the following way

$$\mathrm{Var}_X(L) := \{(\xi_1,\dots,\xi_n) \in X;\ f(\xi_1,\dots,\xi_n) = 0 \text{ for all } f \in L\} \subset X.$$

Conversely, let $Y \subset X$ be a subset of X. Then the vanishing ideal of Y in $K[X]$ is defined as

$$\mathrm{Id}_X(Y) := \{f \in K[X];\ f(\xi_1,\dots,\xi_n) = 0 \text{ for all } (\xi_1,\dots,\xi_n) \in Y\} \trianglelefteq K[X].$$

Definition and Proposition 1.8. *An affine variety X is called* **irreducible** *if it is irreducible as a topological space. The empty set is not considered to be irreducible. An affine variety $X \subset K^n$ is irreducible if and only if $\operatorname{Id}(X) \trianglelefteq K[x_1,\dots,x_n]$ is a prime ideal, which in turn is equivalent to $K[X]$ being a domain.*
Let X be an arbitrary non-empty affine variety. A maximal irreducible affine variety contained in X is called an **irreducible component** *of X. The set of irreducible components of X is finite. If $X_1,\dots,X_s$ are the irreducible components of X, then $X = \bigcup_{i=1}^{s} X_i$. This union is called the* **decomposition of X into irreducible components**. ■

Definition 1.9. *Let $X \subset K^n$ be an affine variety. The* **dimension of X**, *denoted by*

$\dim(X)$, *is defined to be the Krull dimension of* $K[X]$.

Definition 1.10. *A* **morphism** *between two affine varieties* X *and* $X' \subset K^{n'}$ *is a map*

$$\phi = (\phi_1, \ldots, \phi_{n'}) : X \longrightarrow X'$$

such that all components $\phi_1, \ldots, \phi_{n'} : X \longrightarrow K$ *of* ϕ *are regular functions on* X. *Equivalently,* ϕ *is a morphism if and only if* $\phi_1, \ldots, \phi_{n'} : X \longrightarrow K$ *are polynomial functions.*
The morphism ϕ *is called an* **isomorphism** *if there exists a morphism* $\psi : X' \longrightarrow X$ *such that* $\phi \circ \psi = \mathrm{id}_{X'}$ *and* $\psi \circ \phi = \mathrm{id}_X$. *In this case, the affine varieties* X *and* X' *are said to be isomorphic.*

Proposition 1.11. *Let* X *and* X' *be non-empty affine varieties and* $\phi : X \longrightarrow X'$ *be a morphism. Then*

$$\phi^* : K[X'] \longrightarrow K[X],\ f \longmapsto f \circ \phi$$

is a homomorphism of K*-algebras. Conversely, if* $\alpha : K[X'] \longrightarrow K[X]$ *is a homomorphism of* K*-algebras, then there is a unique morphism* $\phi : X \longrightarrow X'$ *such that* $\alpha = \phi^*$.
In fact, there is a bijection

$$\begin{aligned}&\{\textit{set of morphisms } X \longrightarrow X'\}\\ &\quad\xrightarrow{\cong} \{\textit{set of homomorphisms of } K\textit{-algebras } K[X'] \longrightarrow K[X]\}\end{aligned}$$

which is given by the $*$*-operator.* ∎

Proposition 1.12. *Let* $X \subset K^n$ *and* $X' \subset K^{n'}$ *be non-empty affine varieties. Then the product*

$$X \times X' := \{(p, p') \in K^{n+n'};\ p \in X, p' \in X'\}$$

of X *and* X' *is again an affine variety. The coordinate ring* $K[X \times X']$ *is isomorphic to* $K[X] \otimes_K K[X']$ *and this isomorphism is given by*

$$K[X] \otimes_K K[X'] \longrightarrow K[X \times X'],\ \sum_{i=1}^{s} f_i \otimes f_i' \longmapsto \left((p, p') \mapsto \sum_{i=1}^{s} f_i(p) f_i'(p')\right).$$ ∎

Definition 1.13. *Let* X *be an irreducible affine variety. The* **field of rational functions of** $\boldsymbol{X}$, *denoted by* $K(X)$, *is defined as* $K(X) := \mathrm{Quot}(K[X])$, *the quotient field of* $K[X]$.
The elements of $K(X)$ *are called* **rational functions**. *They can be interpreted as functions which are defined on a non-empty open subset of* X. *More explicitely, if* $f/g \in K(X)$ *with* $f \in K[X], g \in K[X] \setminus \{0\}$ *is a rational function, then it defines a function on* $X \setminus \mathrm{Var}_X(g)$ *in the usual way, i. e.* $X \setminus \mathrm{Var}_X(g) \longrightarrow K,\ p \longmapsto f(p)/g(p)$.

1.2 Invariant theory

This section covers some basic facts about invariant theory which will be required in the following chapters. For a more detailed introduction to this theory, see the book [DK02]. Besides the coverage of the important definitions and theorems of invariant theory, this book has a strong emphasize on computational aspects which is very useful as a background for this thesis. For alternatives with a more geometric flavour, see for example [MFK94] or [Kra84].
Throughout this section, let K be a fixed algebraically closed field. Again, all varieties are over K.

Before we can start with invariant theory, we have to make a brief digression to the theory of algebraic groups.

Definition 1.14. *A* **linear algebraic group** *G (over K) is a group that is an affine variety (over K) such that the multiplication map $m : G \times G \longrightarrow G$ and the inversion map $i : G \longrightarrow G$ are morphisms of affine varieties.*

Definition and Proposition 1.15. *A linear algebraic group G is* **connected** *if it is irreducible as an affine variety. If G is not connected, then the irreducible components of G are disjoint. The component containing the identity element 1_G is a normal subgroup of G of finite index. It is called the* **identity component** *of G and denoted by G^0. Moreover, the decomposition of G into irreducible components is given by the cosets of G^0 in G (for details, see [Hum75], Chapter 7, Section 3).* ∎

Let G be the general linear group $\mathrm{GL}_n(K)$. It can be seen with linear algebra methods that every element $\sigma \in G$ can be written as $\sigma = \sigma_s\sigma_u$ where $\sigma_s, \sigma_u \in G$ such that σ_s is diagonalizable (as a homomorphism $K^n \longrightarrow K^n$ of K-vector spaces) and the only eigenvalue of σ_u is 1. Moreover, σ_s and σ_u are unique with respect to this properties. They are called the **semisimple** resp. the **unipotent part** of σ.
This decomposition of elements generalizes to arbitrary linear algebraic groups G: Every element $\sigma \in G$ can be written uniquely as a product of a semisimple part σ_s and a unipotent part σ_u. The element σ is called **semisimple** if $\sigma = \sigma_s$. Similarly, σ is called **unipotent** if $\sigma = \sigma_u$. For more details, see Chapter 15 of [Hum75].

Definition 1.16. *A linear algebraic group G is called* **unipotent** *if all its elements are unipotent. It can be shown that every linear algebraic group G possesses a largest connected normal unipotent subgroup which is called the* **unipotent radical** *of G (cf. [Hum75], Chapter 19, Section 5). A linear algebraic group G is called* **reductive** *if its unipotent radical is trivial.*

Examples of reductive groups include all the classical groups, for example $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{Sp}_{2n}(K)$, just to name a few. Important examples for unipotent groups are the additive group $G_a := (K, +)$ and $U_n(K)$, the group of upper triangular matrices with all diagonal entries 1.

Proposition 1.17. *Let G be a linear algebraic group and $N \trianglelefteq G$ be a closed normal subgroup of G. Then the factor group G/N can be given the structure of a linear algebraic group (for details, see [Hum75], Chapter 12).* ∎

Remark. In case that N is the unipotent radical of some linear algebraic group G, the factor group G/N is reductive. In some sense this means that unipotent resp. reductive groups are the building blocks of every linear algebraic group (cf. [Hum75], Chapter 19, Section 5). ♢

Definition 1.18. *Let G be a group and X be a set. We say that G acts on X if there is a map $\mu : G \times X \longrightarrow X$ such that*

(i) $\mu(1_G, p) = p$ *for all* $p \in X$

(ii) $\mu(\sigma, \mu(\tau, p)) = \mu(\sigma\tau, p)$ *for all* $\sigma, \tau \in G$ *and* $p \in X$.

When there is no danger of confusion, we write $\sigma(p)$ instead of $\mu(\sigma, p)$.

Let now G be a linear algebraic group and X be an affine variety. Furthermore, let G act on X via $\mu : G \times X \longrightarrow X$. We say that G acts **regularly** *on X if the map $\mu : G \times X \longrightarrow X$ is a morphism of affine varieties. In this case, we call X an affine* ***G*-variety**.
If the G-variety X is the whole affine space $X = K^n$ for some $n \in \mathbb{N}_0$ and the action of G on X is linear, i. e. $\sigma(-) : X \longrightarrow X$ is linear for all $\sigma \in G$, then X is called a ***G*-module**.

Let G be a linear algebraic group acting regularly on an affine variety X via $\mu : G \times X \longrightarrow X$. Since by definition, the morphism $\mu : G \times X \longrightarrow X$ is given by polynomial data, it follows that for every $\sigma \in G$ the map $\mu(\sigma, -) : X \longrightarrow X$ is a morphism, too. Hence the action of G on X induces an action of G on $K[X]$ via

$$\sigma(f) := f \circ \mu(\sigma^{-1}, -) \qquad \text{for all } \sigma \in G, f \in K[X].$$

It is an easy verification that $\sigma(-) : K[X] \longrightarrow K[X]$ is an automorphism of K-algebras for every $\sigma \in G$. Accordingly, $K[X]$ is also called a G-algebra in this case. In a more general form, this notion is contained in the following definition.

Definition 1.19. *Let A be a K-algebra and let G act on A via K-algebra automorphisms. Then A is called a* ***G*-algebra**.
Let X, X' be sets and let G act on both X and X'. A map $\alpha : X \longrightarrow X'$ is said to be ***G*-equivariant** *if it commutes with the action of G, i. e. if*

$$\alpha(\sigma(p)) = \sigma(\alpha(p)) \qquad \text{for all } \sigma \in G, p \in X.$$

If $\alpha : A \longrightarrow A'$ is a G-equivariant homomorphism between two G-algebras A and A', we also say that α is a ***G*-homomorphism**. *A subset $B \subset A$ of the G-algebra A is called* ***G*-stable** *if it is stable under the action of G, i. e. if*

$$\sigma(b) \in B \qquad \text{for all } \sigma \in G, b \in B.$$

Finally, for a subset $C \subset A$ of the G-algebra A, the ***G*-closure** *of C in A is defined as the smallest (with respect to inclusion) G-stable K-vector space $\widetilde{C}$ such that $C \subset \widetilde{C} \subset A$.*

Definition 1.20. *Let the linear algebraic group G act regularly on the affine variety X. The set*

$$K[X]^G := \{f \in K[X];\ \sigma(f) = f \text{ for all } \sigma \in G\} \subset K[X]$$

is called the **invariant ring** *(with respect to the action of G on X). It has the structure of a K-algebra. Let X be irreducible. The set*

$$K(X)^G = \left\{ \frac{f}{g};\ f \in K[X], g \in K[X] \setminus \{0\} \text{ such that } \frac{\sigma(f)}{\sigma(g)} = \frac{f}{g} \text{ for all } \sigma \in G \right\} \subset K(X)$$

is called the **invariant field** *(with respect to the action of G on X). It has the structure of a field.*

For what follows, we need the concept of a graded algebra.

Definition 1.21. *A* **graded *K*-algebra** *is a K-algebra S together with a decomposition $S = \bigoplus_{d=0}^{\infty} S_d$ as a direct sum of K-vector spaces $S_0, S_1, \ldots$ such that*

(i) $S_0 = K$

(ii) $S_i S_j \subset S_{i+j}$ *for all* $i, j \in \mathbb{N}_0$.

An element $s \in S \setminus \{0\}$ is said to be **homogeneous of degree *d*** *if $s \in S_d$. If the degree d of s is not relevant, we simply say that s is* **homogeneous**. *In case that S is a polynomial algebra, we implicitly assume that S is graded by the usual degree function for polynomials.*

We can now define a special case of reductivity which is important for invariant theory.

Definition 1.22. *A linear algebraic group G is called* **linearly reductive** *if for every G-module V and every non-zero invariant vector $v \in V^G := \{v \in V;\ \sigma(v) = v \text{ for all } \sigma \in G\}$, there exists a non-zero invariant* $f \in (V^*)^G \setminus \{0\}$ such that $f(v) \neq 0$.*

Remark. There is also another notion of reductivity. A linear algebraic group G is called **geometrically reductive** if for every G-module V and every non-zero invariant vector $v \in V^G \setminus \{0\}$, there exists a non-zero homogeneous invariant $f \in K[X]^G \setminus \{0\}$ such that $f(v) \neq 0$. Nagata and Miyata have shown in [NM64] that geometrically reductive groups are reductive. The proof of the converse – which has been conjectured by Mumford – is due to Haboush (cf. [Hab75]).
Note that by the equivalence of reductive and geometrically reductive, every linearly reductive group is reductive. Moreover, Nagata and Miyata have shown in [NM64] that if the characteristic of K is zero, then linearly reductive and reductive mean the same. ♢

A central problem of invariant theory is the examination of the structure of the invariant ring. Of course, it depends both on the group G and on the affine algebra $K[X]$. An important result in this context is the following.

Theorem 1.23 (Hilbert ([Hil90], [Hil93]), Nagata ([Nag59]), Popov ([Pop79])). *Let the reductive group G act regularly on the affine variety X. Then $K[X]^G$ is finitely generated (as a K-algebra). In fact, a linear algebraic group G is reductive if and only if $K[X]^G$ is finitely generated for all G-varieties X.* ∎

Apart from the finite generation property, there are many other interesting structural questions about the invariant ring.

Definition 1.24. *Let S be a graded K-algebra. The sequence $s_1, \ldots, s_n$ is called a* **system of homogeneous parameters of S** *if*

(i) $s_1, \ldots, s_n \in S$ *are homogeneous*

(ii) $s_1, \ldots, s_n$ *are algebraically independent over K*

(iii) S *is integral over $K[s_1, \ldots, s_n]$.*

Note that by the Noether Normalization Lemma (cf. [Eis95], Chapter 13, Theorem 13.3), systems of homogeneous parameters exist for every finitely generated graded K-algebra S.

*Note that $K[V]^G$ is a graded algebra. We write $(V^*)^G$ for the set of G-invariant linear combinations of the coordinate functions on V, i. e. $(V^*)^G := K[V]^G_1$.

Definition 1.25. *Let G be a linear algebraic group and let X be a G-module. Note that the natural grading on $K[X]$ induces a grading on the invariant ring $K[X]^G$. A system of homogeneous parameters of $K[X]^G$ is called a* **system of primary invariants** *for the action of G on X. In this context,* **secondary invariants** *are defined to be generators of the invariant ring regarded as a module over the K-algebra which is generated by the primary invariants, i. e. generators of the $K[s_1, \ldots, s_n]$-module $K[X]^G$.*

Definition 1.26. *A graded algebra S is called* **Cohen-Macaulay** *if there exists a system of homogeneous parameters $s_1, \ldots, s_n \in S$ such that S is free as a module over $K[s_1, \ldots, s_n]$.*

Hochster and Roberts have proved the following important theorem about the Cohen-Macaulayness of invariant rings of linearly reductive groups.

Theorem 1.27 (Hochster and Roberts [HR74]). *Let G be a linearly reductive group and let X be a G-module. Then $K[X]^G$ is Cohen-Macaulay.* ∎

The next lemma gives an explicit description of the induced action of G on $K[X]$. We include a proof since in the following this construction will be used several times.

Lemma 1.28. *Let the linear algebraic group G act regularly on the affine variety X. Then there exists a homomorphism of algebras*

$$\tilde{\mu} : K[X] \longrightarrow K[G] \otimes_K K[X]$$

which describes the action of G on $K[X]$ in the following way. If $\tilde{\mu}(f) = \sum_{i=1}^{s} g_i \otimes a_i$ with $g_1, \ldots, g_s \in K[G]$ and $a_1, \ldots, a_s \in K[X]$, then $\sigma(f)$ is given by $\sigma(f) = \sum_{i=1}^{s} g_i(\sigma) \cdot a_i$ for all $\sigma \in G$.

Proof. Consider the morphism $\mu : G \times X \longrightarrow X$ and the induced homomorphism of algebras

$$\mu^* : K[X] \longrightarrow K[G] \otimes_K K[X],\ f \longmapsto f \circ \mu.$$

Moreover, let $i : G \longrightarrow G$ be the inversion in G and $i^* : K[G] \longrightarrow K[G]$ be the corresponding homomorphism of algebras. Set

$$\tilde{\mu} := (i^* \otimes_K \mathrm{id}_{K[X]}) \circ \mu^* : K[X] \longrightarrow K[G] \otimes_K K[X].$$

By construction, $\tilde{\mu}$ is a homomorphism of algebras and it describes the action of G on $K[X]$ in the sense as described in the statement of this lemma. ∎

One may ask if conversely every action of G on $K[X]$ which can be described by a homomorphism $\tilde{\mu} : K[X] \longrightarrow K[G] \otimes_K K[X]$ (in the sense of the previous lemma) originates

from a regular action of G on the affine variety X. A positive answer to this question is given in the next proposition. For the lack of a reference, we give a proof.

Proposition 1.29. *Let A be a reduced, affine K-algebra and G a linear algebraic group. Let $\tilde{\mu} : A \longrightarrow K[G] \otimes_K A$ be a homomorphism of K-algebras such that*

$$\sigma(a) := \tilde{\mu}(a)(\sigma) \quad \text{for all } a \in A, \sigma \in G$$

defines an action of G on A. Then there exists an affine G-variety X such that $K[X]$ and A are G-isomorphic.

Proof. Let $x_1, \ldots, x_n$ be indeterminates over K. We may assume that $A = K[x_1, \ldots, x_n]/I$ where $I \trianglelefteq K[x_1, \ldots, x_n]$ is a radical ideal. With this notation, A can be identified with the coordinate ring of the affine variety $X := \mathrm{Var}(I) \subset K^n$. Let $i : G \longrightarrow G$ be the inversion in G and $i^* : K[G] \longrightarrow K[G],\ g \longmapsto g \circ i$ be the corresponding homomorphism of algebras. Consider the homomorphism $\mu^* := (i^* \otimes_K \mathrm{id}_A) \circ \tilde{\mu} : A \longrightarrow K[G] \otimes_K A$. It corresponds to the morphism $\mu : G \times X \longrightarrow X$ which is given by

$$\mu : G \times X \longrightarrow X,\ (\sigma, p) \longmapsto (\mu^*(x_1 + I)(\sigma, p), \ldots, \mu^*(x_n + I)(\sigma, p)) \tag{1.1}$$

(cf. the previous section or [Har77], Chapter I, Proposition 3.5 & Exercise 3.15). We will show that

$$\sigma(p) := \mu(\sigma, p) \quad \text{for all } \sigma \in G, p \in X$$

defines an action of G on X and that the induced action on the coordinate ring $A = K[X]$ is exactly the action which is given on A already.
Since $\tilde{\mu}$ defines an action of G on A, it follows that

$$\begin{aligned} \mu(1_G, p) &= (\mu^*(x_1 + I)(1_G, p), \ldots, \mu^*(x_n + I)(1_G, p)) \\ &= (\mu^*(x_1 + I)(1_G)(p), \ldots, \mu^*(x_n + I)(1_G)(p)) \\ &= ((x_1 + I)(p), \ldots, (x_n + I)(p)) = p \end{aligned}$$

for all $p \in X$. Thus 1_G induces the identity morphism on X, as desired.
Now let $\sigma, \tau \in G$ and $p \in X$ be arbitrary. For μ to be an action, it remains to show that $\mu(\sigma, \mu(\tau, p)) = \mu(\sigma\tau, p)$. Let $i \in \{1, \ldots, n\}$ and let $g_1, \ldots, g_s \in K[G],\ a_1 + I, \ldots, a_s + I \in K[X]$ such that $\tilde{\mu}(x_i + I) = \sum_{j=1}^{s} g_j \otimes (a_j + I)$. Then

$$\begin{aligned} \tilde{\mu}(x_i + I)(\sigma\tau, p) &= ((\sigma\tau)(x_i + I))\,(p) = \sigma(\tau(x_i + I))(p) \\ &= \sigma(\tilde{\mu}(x_i + I)(\tau, -))(p) = \tilde{\mu}(\tilde{\mu}(x_i + I)(\tau, -))(\sigma, p) \\ &= \tilde{\mu}\left(\sum_{j=1}^{s} g_j(\tau) \cdot (a_j + I)\right)(\sigma, p) \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{j=1}^{s} g_j(\tau) \cdot a_j \left(\tilde{\mu}(x_1 + I), \ldots, \tilde{\mu}(x_n + I) \right) \right) (\sigma, p) \\
&= \left(\sum_{j=1}^{s} g_j(\tau) \cdot a_j \left(\tilde{\mu}(x_1 + I)(\sigma, p), \ldots, \tilde{\mu}(x_n + I)(\sigma, p) \right) \right) \\
&= \tilde{\mu}(x_i + I) \left(\tau, (\tilde{\mu}(x_1 + I)(\sigma, p), \ldots, \tilde{\mu}(x_n + I)(\sigma, p)) \right).
\end{aligned}
$$

Since this calculation can be done for all $i \in \{1, \ldots, n\}$, it follows

$$
\begin{aligned}
\mu(\sigma, \mu(\tau, p)) &= \mu \left(\sigma, \left(\tilde{\mu}(x_1 + I)(\tau^{-1}, p), \ldots, \tilde{\mu}(x_n + I)(\tau^{-1}, p) \right) \right) \\
&= \left(\tilde{\mu}(x_i + I) \left(\sigma^{-1}, \left(\tilde{\mu}(x_1 + I)(\tau^{-1}, p), \ldots, \tilde{\mu}(x_n + I)(\tau^{-1}, p) \right) \right) \right)_{i=1,\ldots,n} \\
&= \left(\tilde{\mu}(x_i + I)(\tau^{-1}\sigma^{-1}, p) \right)_{i=1,\ldots,n} \\
&= \mu(\sigma\tau, p),
\end{aligned}
$$

which we wanted to prove. But this means that μ defines an action of G on X, indeed. Finally, observe that by construction, the induced action of G on $K[X]$ coincides with the action which is already given on $A = K[X]$. ∎

The group actions on K-algebras which we have considered so far, i. e. those that are induced from group actions on affine varieties, all have an important finiteness property. The following definition makes this more precise.

Definition 1.30. *Let G be a linear algebraic group and let A be a G-algebra. The action of G on A is said to be* **locally finite** *if for every $a \in A$ there exists a finite dimensional K-vector space $V \subset A$ such that*

(i) $a \in V$ and

(ii) V is stable under the action of G.

As indicated above, the actions on coordinate rings which are induced from regular actions on affine varieties are locally finite. This will be shown in the following. In fact, we will show this property for a wider class of group actions which include the "variety cases".

Proposition 1.31. *Let G be a linear algebraic group acting on a K-algebra A via a homomorphism of algebras $\tilde{\mu} : A \longrightarrow K[G] \otimes_K A$. Then we have the following properties.*

(a) The action of G on A is locally finite.

(b) Let $B \subset A$ be a G-stable subalgebra of A. Then $\tilde{\mu}(B) \subset K[G] \otimes_K B$.

Proof. We first prove (a). Let $a \in A$. By definition of locally finite, we have to show that there is a finite dimensional G-stable vector space $V \subset A$ containing a. Let $\tilde{\mu}(a) = \sum_{i=1}^{s} g_i \otimes a_i$ for some $g_1, \ldots, g_s \in K[G]$ and $a_1, \ldots, a_s \in A$. Without loss of generality, we may assume that $g_1, \ldots, g_s$ are linearly independent over K. We claim that

$$V := \sum_{i=1}^{s} K \cdot a_i \subset A$$

is a G-stable vector space containing a. Clearly $a \in V$, since $a = 1_G(a) = \sum_{i=1}^{s} g_i(1_G) \cdot a_i \in V$. It remains to show that V is stable under the action of G. Let $\tau \in G$. Since $\tilde{\mu}$ defines an action of G on A, it follows that

$$\tilde{\mu}(a)(\tau\sigma) = \tau(\tilde{\mu}(a)(\sigma)) = \sum_{i=1}^{s} g_i(\sigma)\tau(a_i) \in V \quad \text{for all } \sigma \in G. \tag{1.2}$$

By assumption, $g_1, \ldots, g_s$ are linearly independent over K, hence – by an easy induction argument – there exist $\sigma_1, \ldots, \sigma_s \in G$ such that the matrix $(g_i(\sigma_j))_{i,j=1,\ldots,s} \in K^{s \times s}$ is regular. By equation (1.2), it follows

$$(\tau(a_1), \ldots, \tau(a_s)) \cdot (g_i(\sigma_j))_{i,j=1,\ldots,s} \in V^s$$

and this implies

$$(\tau(a_1), \ldots, \tau(a_s)) = (\tau(a_1), \ldots, \tau(a_s)) \cdot (g_i(\sigma_j))_{i,j=1,\ldots,s} \cdot (g_i(\sigma_j))^{-1}_{i,j=1,\ldots,s} \in V^s. \tag{1.3}$$

Since τ was chosen arbitrarily, this shows that V is G-stable, as desired.

For the proof of (b), let $a \in B$ and – as above – let $\tilde{\mu}(a) = \sum_{i=1}^{s} g_i \otimes a_i$ for some $g_1, \ldots, g_s \in K[G]$ and $a_1, \ldots, a_s \in A$. Again, we may assume that $g_1, \ldots, g_s$ are linearly independent over K. By the proof of (a), it follows that $V := \sum_{i=1}^{s} K \cdot a_i \subset A$ is a G-stable vector space containing a. Moreover, setting $\tau = 1_G$ in equation (1.3) above shows that $\sum_{i=1}^{s} K \cdot a_i$ is in fact the smallest G-stable vector space containing a in the sense that for every G-stable vector space $V' \subset A$ with $a \in V'$, it follows $V \subset V'$. Since B is G-stable, this implies $V \subset B$. In particular, $a_1, \ldots, a_s \in B$ and therefore $\tilde{\mu}(a) \in K[G] \otimes_K B$ which we wanted to prove. ∎

Remark 1.32. It can be shown that – with the notation of the previous proposition – every G-stable finite dimensional vector space $V \subset A$ is in fact a G-module. ♢

Corollary 1.33. *Let the linear algebraic group G act regularly on the affine variety X. Then the induced action of G on $K[X]$ is locally finite.* ∎

We close this section with the definition of separating invariants.

Definition 1.34. *Let the linear algebraic group G act regularly on the affine variety X. We say that $p, p' \in X$ can be* **separated** *by invariants if there exists $f \in K[X]^G$ such that $f(p) \neq f(p')$. A subset $S \subset K[X]^G$ is said to be* **separating** *if for all points $p, p' \in X$ which can be separated by invariants there exists $g \in S$ such that $g(p) \neq g(p')$.*

1.3 Computational algebra

This section gives a very rough introduction to computational algebra. A detailed treatment of this theory can be found in [BW93]. For a more practical approach, see the book [CLO07].

As before, let K be a field, let $n \in \mathbb{N}$ and let $x_1, \ldots, x_n$ be indeterminates over K. For the theory of this section to be transformable to algorithms on a computer, it is necessary that the occuring data, i. e. the coefficients of the involved polynomials, are contained in a computable field. In simple terms, a field is called **computable** if it can be represented on a computer and the operations addition, subtraction, multiplication and division can be computed effectively. Examples for computable fields include the field of rational numbers $\mathbb{Q}$ and the Galois fields $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ for $p \in \mathbb{Z}$ a prime number. We will also see that finitely generated field extensions of computable fields, such as $\mathbb{Q}(x_1, \ldots, x_n)$, are computable again.
We do not require K itself to be a computable field, we only require the coefficients of the occuring polynomials to be contained in a computable field. For example, it is common to consider ideals in a polynomial ring over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Even though $\overline{\mathbb{Q}}$ is not a computable field, such ideals can be handled with algorithms of computational algebra if the coefficients of the generators are contained in $\mathbb{Q}$.
Note that this computability condition will not be mentioned explicitly at the various places in this thesis.

Definition 1.35. *A* **monomial** *in $x_1, \ldots, x_n$ is a product of powers of $x_1, \ldots, x_n$. More explicitly, a monomial is a polynomial $f \in K[x_1, \ldots, x_n]$ of the form $f = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ be the tuple of exponents of f. Abbreviatory, we often write x^α for $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$.*

Obviously, every polynomial $f \in K[x_1, \ldots, x_n]$ can be written as a K-linear combination of monomials. More precisely, there exist coefficients $c_\alpha \in K$ for $\alpha \in \mathbb{N}_0^n$ such that $f = \sum_\alpha c_\alpha x^\alpha$. Note that by the definition of a polynomial, only finitely many coefficients c_α for $\alpha \in \mathbb{N}_0^n$ are non-zero. Thus, whenever we write a polynomial in the form $\sum_\alpha c_\alpha x^\alpha$, we implicitly assume that almost all coefficients c_α are zero.

Definition 1.36. *A relation $\leq$ on the set of monomials $\{x^\alpha;\ \alpha \in \mathbb{N}_0^n\}$ is called a* **monomial order** *if the following conditions are satisfied:*

(i) $\leq$ is a total order on $\{x^\alpha;\ \alpha \in \mathbb{N}_0^n\}$

(ii) *If* $x^\alpha \leq x^\beta$ *then* $x^{\alpha+\gamma} \leq x^{\beta+\gamma}$ *for all* $\alpha, \beta, \gamma \in \mathbb{N}_0^n$

(iii) $1 \leq x^\alpha$ *for all* $\alpha \in \mathbb{N}_0^n$

Example 1.37. An important example for a monomial order is the **lexicographic order** specified by $x_n \leq \ldots \leq x_1$. It is defined as follows: $x^\alpha \leq x^\beta$ if and only if the left-most non-zero entry of $\beta - \alpha \in \mathbb{Z}^n$ is positive. The name "lexicographic" may become clearer if this order is defined recursively as: $x^\alpha \leq x^\beta$ if and only if

- $\alpha_1 < \beta_1$ or
- $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \leq x_2^{\beta_2} \cdot \ldots \cdot x_n^{\beta_n}$. ◁

Definition 1.38. *Let* $\leq$ *be a monomial order on* $x_1, \ldots, x_n$ *and let* $f = \sum_\alpha c_\alpha x^\alpha$ *be a non-zero polynomial. The* **leading monomial** *of* f *with respect to* $\leq$ *is defined as*

$$\mathrm{LM}_\leq(f) := \max\{x^\alpha;\ c_\alpha \neq 0\}.$$

For the zero polynomial we define $\mathrm{LM}_\leq(0) := 0$. *If the monomial order* $\leq$ *is clear from the context, we sometimes omit the* $\leq$*-symbol and simply write* $\mathrm{LM}(f)$.

The central notion of computational algebra is that of a Gröbner basis of an ideal $I \trianglelefteq K[x_1, \ldots, x_n]$. It was first introduced by Buchberger in [Buc65]. Roughly speaking, it is a special generating set for I which allows various problems concerning I to be solved algorithmically. For example, algorithms for a membership test for I, for a primary decomposition of I, and for the computation of unique normal forms of elements in $K[x_1, \ldots, x_n]/I$ can be realized with Gröbner basis techniques.

Definition 1.39. *Let* $\leq$ *be a monomial order on* $x_1, \ldots, x_n$ *and let* $I \trianglelefteq K[x_1, \ldots, x_n]$ *be an ideal. A set* $\{h_1, \ldots, h_s\}$ *with* $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ *is called a* **Gröbner basis** *of* I *(with respect to* $\leq$*) if*

(i) $I = (h_1, \ldots, h_s)_{K[x_1,\ldots,x_n]}$

(ii) $(\mathrm{LM}(h_1), \ldots, \mathrm{LM}(h_s))_{K[x_1,\ldots,x_n]} = (\mathrm{LM}(f);\ f \in I)_{K[x_1,\ldots,x_n]}$.

Theorem 1.40. *Let* $\leq$ *be a monomial order on* $x_1, \ldots, x_n$ *and let* $I \trianglelefteq K[x_1, \ldots, x_n]$ *be an ideal. Then there exists a Gröbner basis of* I. *Moreover, it can be computed effectively.* ■

Remark. The standard algorithm for computing Gröbner bases is Buchberger's Algorithm (cf. [Buc65]). ♢

In general, there exist many different Gröbner bases of a given ideal I with respect to a given monomial order. It will turn out that a unique Gröbner basis can be singled out quite easily.

Definition 1.41. *Let $\leq$ be a monomial order on $x_1, \ldots, x_n$ and let $I \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal. A Gröbner basis $\{h_1, \ldots, h_s\}$ of I is* **reduced** *if*

(i) $0 \notin \{h_1, \ldots, h_s\}$

(ii) The coefficient of the leading monomial in h_i is equal to 1 for $i = 1, \ldots, s$

(iii) No monomial of h_i is divisible by any monomial in $\{\mathrm{LM}(h_j) : \ j = 1, \ldots, i-1, i+1, \ldots, s\}$ for $i = 1, \ldots, s$.

Theorem 1.42. *Let $\leq$ be a monomial order on $x_1, \ldots, x_n$ and let $I \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal. Then there exists a reduced Gröbner basis of I. Moreover, it is unique and can be computed effectively.* ∎

As mentioned above, Gröbner bases can be used to define unique normal forms of elements of $K[x_1, \ldots, x_n]/I$.

Proposition and Definition 1.43. *Let $\leq$ be a monomial order on $x_1, \ldots, x_n$, let $\mathcal{G}$ be a Gröbner basis of an ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ and let $f \in K[x_1, \ldots, x_n]$ be a polynomial. Then there exists a unique polynomial $r \in K[x_1, \ldots, x_n]$ such that*

(i) $f - r \in I$

(ii) No monomial of r is divisible by any monomial in $\{\mathrm{LM}(f);\ f \in \mathcal{G}\}$.

The polynomial r is called the **normal form** *of f with respect to $\mathcal{G}$. It is denoted by* $\mathrm{NF}_{\mathcal{G}}(f)$. ∎

Remarks 1.44. As before, let $\mathcal{G}$ be a Gröbner basis of $I \trianglelefteq K[x_1, \ldots, x_n]$. The following properties of the normal form operator $\mathrm{NF}_{\mathcal{G}}$ will be needed in the next chapters.

(a) For all $f \in K[x_1, \ldots, x_n]$ we have $\mathrm{NF}_{\mathcal{G}}(f) = 0 \iff f \in I$.

(b) For all $f, f' \in K[x_1, \ldots, x_n]$ we have $f + I = f' + I \iff \mathrm{NF}_{\mathcal{G}}(f) = \mathrm{NF}_{\mathcal{G}}(f')$.

(c) $\mathrm{NF}_{\mathcal{G}} : K[x_1, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]$ is a K-linear map.

(d) Let $\mathcal{G}$ be a reduced Gröbner basis of I. Moreover, let $R \subset K$ be a subring of the field K and assume that the coefficients of the elements of $\mathcal{G}$ are contained in R. Then $\mathrm{NF}_{\mathcal{G}}(R[x_1, \ldots, x_n]) \subset R[x_1, \ldots, x_n]$. ♢

With the availability of the normal form operator, it can be seen that finitely generated field extensions over a computable field K are computable, again. For, let $L = \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ be a finitely generated field extension over K. An element of this field – more precisley, representations of its numerator and its denominator – can be described by a pair of polynomials in $K[x_1, \ldots, x_n]$. Then, addition, subtraction, multiplication, and division of elements can be realized in the obvious way. Moreover, the normal form operator NF provides a test for equality in $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)$.

Another important application of Gröbner bases is the computation of elimination ideals.

Definition 1.45. *Let $I \trianglelefteq K[x_1, \ldots, x_n]$. The ith* **elimination ideal** *I_i of I is defined as*

$$I_i := I \cap K[x_{i+1}, \ldots, x_n] \trianglelefteq K[x_{i+1}, \ldots, x_n].$$

Theorem 1.46. *Let $I \trianglelefteq K[x_1, \ldots, x_n]$. The ith elimination ideal I_i of I can be computed effectively. More precisely, let $\leq$ be a monomial order on $x_1, \ldots, x_n$ where any monomial involving one of $x_1, \ldots, x_i$ is greater than all monomials in $x_{i+1}, \ldots, x_n$. Let $\mathcal{G}$ be a Gröbner basis of I. Then a Gröbner basis of I_i (with respect to the restriction of the monomial order $\leq$ to $x_{i+1}, \ldots, x_n$) is given by $\mathcal{G} \cap K[x_{i+1}, \ldots, x_n]$.* ∎

Remark 1.47. A monomial order with the properties of the previous theorem is called an **elimination order** for $x_1, \ldots, x_i$. ♢

The last application of Gröbner bases which we want to present here is the computation of syzygies.

Definition 1.48. *Let $m_1, \ldots, m_s \in K[x_1, \ldots, x_n]$. A tuple of polynomials $(f_1, \ldots, f_s) \in K[x_1, \ldots, x_n]^s$ is called a* **syzygy** *of $m_1, \ldots, m_s$ if $f_1 m_1 + \ldots + f_s m_s = 0$. The set*

$$\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s) := \{(f_1, \ldots, f_s) \in K[x_1, \ldots, x_n]^s : \ f_1 m_1 + \ldots + f_s m_s = 0\}$$

of all syzygies of $m_1, \ldots, m_s$ is a submodule of $K[x_1, \ldots, x_n]^s$. It is called the **module of syzygies** *of $m_1, \ldots, m_s$. Note that since $K[x_1, \ldots, x_n]$ is a noetherian ring, the module $\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s)$ is finitely generated over $K[x_1, \ldots, x_n]$.*

Theorem 1.49. *Let $m_1, \ldots, m_s \in K[x_1, \ldots, x_n]$. Then generators of the $K[x_1, \ldots, x_n]$-module $\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s)$ can be computed effectively.* ∎

The notion of a syzygy can be generalized to the case of free $K[x_1, \ldots, x_n]$-modules in the following way.

Definition 1.50. *Let $t \in \mathbb{N}$ and let $m_1, \ldots, m_s$ be elements of the free $K[x_1, \ldots, x_n]$-module $K[x_1, \ldots, x_n]^t$. A tuple of polynomials $(f_1, \ldots, f_s) \in K[x_1, \ldots, x_n]^s$ is called a* **syzygy** *of $m_1, \ldots, m_s$ if $f_1 m_1 + \ldots + f_s m_s = 0$. The set*

$$\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s) := \{(f_1, \ldots, f_s) \in K[x_1, \ldots, x_n]^s : \ f_1 m_1 + \ldots + f_s m_s = 0\}$$

of all syzygies of $m_1, \ldots, m_s$ is a submodule of $K[x_1, \ldots, x_n]^s$. It is called the **module of syzygies** *of $m_1, \ldots, m_s$. Again, the module $\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s)$ is finitely generated over $K[x_1, \ldots, x_n]$.*

Similarly as in the polynomial case, it would be nice to have an algorithm for the computation of syzygies in the module case, too, i. e. the case where the value of t (from the previous definition) is greater than 1. This case can be handled with **Gröbner bases for modules** over a polynomial ring, which is a generalization of the theory of Gröbner bases for ideals. We do not go into the details of this theory here. An introduction to modules over polynomial rings from a computational point of view is given for example in [CLO05], Chapter 5. Detailed instructions about the computation of syzygies can be found there, too. We can therefore state the following theorem.

Theorem 1.51. *Let $t \in \mathbb{N}$ and let $m_1, \ldots, m_s \in K[x_1, \ldots, x_n]^t$. Then generators of the $K[x_1, \ldots, x_n]$-module $\mathrm{Syz}_{K[x_1,\ldots,x_n]}(m_1, \ldots, m_s)$ can be computed effectively.* ∎

2 Computing invariants of reductive groups acting on non-reduced affine algebras

The examination of G-modules and their invariant rings has always been a central aspect of invariant theory. A G-module corresponds to an action of a group on a polynomial ring where the action can be described by a linear substitution of variables. As we have seen, the notion of a G-module can be generalized to that of a G-variety, i. e. to the situation where a linear algebraic group G acts regularly on an affine variety X. Similarly as for G-modules, this algebraically corresponds to an action of G on the coordinate ring $K[X]$ of X. The action of G on $K[X]$ can then be described by a homomorphism of algebras $\tilde{\mu} : K[X] \longrightarrow K[G] \otimes_K K[X]$ in the sense that $\sigma(f) = \tilde{\mu}(f)(\sigma)$ for all $f \in K[X]$ and $\sigma \in G$. Nagata has shown that if a reductive group G acts on an affine algebra A via a homomorphism of algebras $\tilde{\mu} : A \longrightarrow K[G] \otimes_K A$, then the invariant ring

$$A^G := \{f \in A;\ \sigma(f) = f \text{ for all } \sigma \in G\}$$

is finitely generated as a K-algebra (cf. [Nag64]). In particular, this shows that $K[X]^G$ is finitely generated for every G-variety X if G is a reductive group. But in fact, his result includes even more, namely the cases where A is a non-reduced affine algebra. Unlike to A being reduced – which always geometrically corresponds to an affine G-variety – a non-reduced affine G-algebra does not have a geometric counterpart in classical algebraic geometry. Nonetheless, it is interesting for its own sake to examine the non-reduced case more closely.
Derksen and Kemper have developed various algorithms for the computation of $K[X]^G$ if X is an affine variety and G is a reductive group (cf. [Der99], [Kem03], [DK02] and [DK08]). The correctness of their algorithms heavily relies on the fact that the underlying algebra, i. e. the algebra $K[X]$, is reduced. Therefore, the invariant ring A^G cannot be calculated with the existing algorithms if A is a non-reduced affine algebra.
In this chapter, we give an algorithm for the computation of the invariant ring A^G if G is a finite group. Moreover, we point out some computational difficulties which arise if G is an infinite reductive group.

2.1 Finite groups

As a motivation, we start with an example.

Example 2.1. Let $K = \mathbb{F}_2$ be the finite field with two elements and let x_1, x_2 be indetermi-

nates over K. Moreover, let the cyclic group* $G = \langle\sigma\rangle$ of order 2 act on the non-reduced affine algebra

$$A := K[x_1, x_2]/I \quad \text{where} \quad I := (x_1^2) \trianglelefteq K[x_1, x_2]$$

by the following rules

$$\sigma(x_1 + I) := x_1 + I, \quad \sigma(x_2 + I) := x_1 + x_2 + I.$$

What is the invariant ring A^G in this case? Note that the algebra A is the image of the polynomial ring $K[x_1, x_2]$ under the homomorphism

$$\alpha : K[x_1, x_2] \longrightarrow A,\ x_1 \longmapsto x_1 + I, x_2 \longmapsto x_2 + I.$$

The polynomial ring can be given the structure of a G-algebra by

$$\sigma(x_1) := x_1, \quad \sigma(x_2) := x_1 + x_2.$$

Then obviously the homomorphism α commutes with the action of G. It is not hard to see that the invariant ring $K[x_1, x_2]^G$ is given by $K[x_1, x_2]^G = K[x_1, x_1x_2 + x_2^2]$. In particular, both $x_1 + I$ and $x_1x_2 + x_2^2 + I$ are invariant elements of A. But does there exist another invariant which is not contained in $K[x_1+I, x_1x_2+x_2^2+I]$? The answer is yes, the element x_1x_2+I for example happens to be a "new" invariant. (Note that $x_1x_2 \in K[x_1, x_2]$ is certainly not invariant.) But it is still not clear at this point whether $x_1+I, x_1x_2+x_2^2+I$ and $x_1x_2 + I$ is already a generating system of A^G or not. Do there exist further "hidden" invariants? Later in this section, we will be able to solve this problem algorithmically. $\triangleleft$

Throughout this section, let K be an arbitrary field and let $x_1, \ldots, x_n$ be indeterminates over K. Let A be an affine algebra over K and let G act on A via K-algebra automorphisms. Needless to say, the formulation of the algorithm for the computation of A^G requires a specification of how the algebra A, the group G and the action of G on A are given.

Convention 2.2.
Let $G = \{\sigma_1, \ldots, \sigma_m\}$ be a finite group, let A be a (possibly non-reduced) affine algebra and let G act on A via automorphisms of K-algebras. We assume that these data are given as follows:

(1) Generators of the ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ such that $A = K[x_1, \ldots, x_n]/I$.

(2) For $i = 1, \ldots, n$ and $j = 1, \ldots, m$:
A polynomial $g_{ij} \in K[x_1, \ldots, x_n]$ such that

$$\sigma_j(x_i + I) = g_{ij} + I.$$

*We write $\langle\sigma\rangle$ for the group generated by σ.

Before we can formulate the algorithm for the computation of A^G, we have to discuss an auxiliary algorithmic construction which will be used therein. As we will see, it will be necessary to compute a polynomial ring P with a linear G-action such that A is a G-homomorphic image of P. This can be done as follows. First, compute a G-module V which contains the generators $x_1 + I, \ldots, x_n + I$ of A. The vector space V can be chosen for example as the K-linear span of the union of the orbits of $x_1 + I, \ldots, x_n + I$. Then clearly $P := S(V)$, the symmetric algebra of V, together with the induced action of G on P and the obvious homomorphism $P \longrightarrow A$ has the required properties.
Although this seems to be pretty obvious, we include a concrete algorithmic formulation of this method.

Algorithm 2.3. (Computing a polynomial ring P with a G-action such that A is a G-homomorphic image of P)

Input: A finite group G, an affine algebra A and an action of G on A according to Convention 2.2.

Output: A polynomial ring $P = K[y_1, \ldots, y_{n'}]$ (with $y_1, \ldots, y_{n'}$ new indeterminates), an action of G on P and an epimorphism $\alpha : P \longrightarrow A$ which commutes with the action of G. More precisely, the output is given by homogeneous polynomials $g'_{ij} \in P$ $(i = 1, \ldots, n',\ j = 1, \ldots, m)$ of degree one and polynomials $a_1, \ldots, a_{n'} \in K[x_1, \ldots, x_n]$ which stand for the following: The polynomials g'_{ij} describe the action of G on P, i. e.

$$\sigma_j(y_i) = g'_{ij} \quad \text{for all } i = 1, \ldots, n' \text{ and } j = 1, \ldots, m.$$

Moreover, the epimorphism α is given by $\alpha : P \longrightarrow A,\ y_i \longmapsto a_i + I$ for $i = 1, \ldots, n'$.

(1) Compute a K-basis $a_1 + I, \ldots, a_{n'} + I$ of the vector space generated by the elements in the set

$$\{\sigma_j(x_i + I);\ i = 1, \ldots, n,\ j = 1, \ldots, m\}.$$

(For details about how basic linear algebra can be done within the residue class ring $K[x_1, \ldots, x_n]/I$, see Remark 2.4(b))

(2) Let $y_1, \ldots, y_{n'}$ be indeterminates over K and set $P := K[y_1, \ldots, y_{n'}]$.

(3) For $i = 1, \ldots, n'$:
For $j = 1, \ldots, m$:

Compute $\beta_{ij1}, \ldots, \beta_{ijn'} \in K$ such that

$$\sigma_j(a_i + I) = \sum_{k=1}^{n'} \beta_{ijk}(a_k + I).$$

Set $g'_{ij} := \sum_{k=1}^{n'} \beta_{ijk} y_k$.
(For details about how basic linear algebra can be done within the residue class ring

$K[x_1, \ldots, x_n]/I$, see Remark 2.4(b))

(4) Return P, $(g'_{ij})_{i=1,\ldots,n',\ j=1,\ldots,m}$ and $(a_i)_{i=1,\ldots,n'}$.

Remark 2.4. (a) For better clarity, we have written $\sigma_j(x_i + I)$ resp. $\sigma_j(a_i + I)$ in the expression of step (1) resp. step (3). By Convention 2.2, this obviously should be replaced by $g_{ij} + I$ resp. $a_i(g_{1j}, \ldots, g_{nj}) + I$ for concrete computations.

(b) Let $I \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal and let $\mathcal{G}$ be a Gröbner basis of I with respect to an arbitrary monomial order on $x_1, \ldots, x_n$. By the K-linearity of the $\mathrm{NF}_{\mathcal{G}}$-operator, it follows that the elements $(b + I;\ b \in B)$ are linear independent over K if and only if the polynomials $(\mathrm{NF}_{\mathcal{G}}(b);\ b \in B)$ are linearly independent over K. This is the key for doing linear algebra in $K[x_1, \ldots, x_n]/I$. The various operations in this residue class ring such as choosing a linear independent subset or testing linear independence of a set of elements can thus be reduced to doing the very same operations in the polynomial ring $K[x_1, \ldots, x_n]$. Computations in this latter polynomial ring are usually done by comparing coefficients and then solving the resulting systems of linear equations. ♢

Proof of Correctness. The correctness should be clear from the outline preceding this algorithm. ∎

Remark. If A is a reduced algebra, the construction of Algorithm 2.3 can be interpreted geometrically as a G-equivariant embedding of the G-variety corresponding to A into a G-module (see also [DK08], Algorithm 1.2). ♢

We can now state the algorithm for the computation of A^G.

Algorithm 2.5. (Computing invariants of finite groups actions)

Input: A finite group G, an affine algebra A and an action of G on A according to Convention 2.2.

Output: Polynomials $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ such that $A^G = K[f_1 + I, \ldots, f_s + I]$.

(1) Use Algorithm 2.3 to define a polynomial ring P with a linear G-action such that A is a G-homomorphic image of P. More precisely, obtain the polynomial ring $P = K[y_1, \ldots, y_{n'}]$ (with $y_1, \ldots, y_{n'}$ new indeterminates), homogeneous polynomials $g'_{ij} \in P$ of degree one and elements $a_1, \ldots, a_{n'} \in K[x_1, \ldots, x_n]$. By the specification of Algorithm 2.3, these data mean the following. The polynomial ring P has the

structure of a G-algebra via

$$\sigma_j(y_i) := g'_{ij} \qquad \text{for all } i = 1, \ldots, n' \text{ and } j = 1, \ldots, m.$$

Moreover, A is the image of P under the G-equivariant epimorphism defined by $\alpha : P \longrightarrow A,\ y_i \longrightarrow a_i + I$ for $i = 1, \ldots, n'$.

(2) Compute a homogeneous system of parameters $c_1, \ldots, c_{n'}$ of the invariant ring P^G. Set $R := K[c_1, \ldots, c_{n'}]$.
(For details about the computation of this and the next step, see Remark 2.6(b))

(3) Compute $d_1, \ldots, d_t \in P$ such that $P = \bigoplus_{i=1}^{t} Rd_i$.

(4) Compute generators $l_1, \ldots, l_r \in P$ of $\ker \alpha$.
(For details, see Remark 2.6(c))

(5) Denote the standard basis vectors of the free P-module P^m by $e_1 := (1, 0, \ldots, 0), \ldots, e_m := (0, \ldots, 0, 1)$. Compute generators of the module of syzygies

$$M := \mathrm{Syz}_P\left(\begin{pmatrix}(\sigma_1 - \mathrm{id})(d_1)\\ \vdots \\ (\sigma_m - \mathrm{id})(d_1)\end{pmatrix}, \ldots \begin{pmatrix}(\sigma_1 - \mathrm{id})(d_t)\\ \vdots \\ (\sigma_m - \mathrm{id})(d_t)\end{pmatrix}, \right.$$
$$\left. l_1e_1, \ldots, l_1e_m, l_2e_1, \ldots, l_2e_m, \ldots, l_re_1, \ldots, l_re_m\right) \subset P^{t+m\cdot r}.$$

(For details, see Theorem 1.51)

(6) Let $M' \subset P^t$ be the projection of M on the first t components. Compute generators $m_1, \ldots, m_{s'}$ of the R-module $M' \cap R^t$.
(For details, see Remark 2.6(d))

(7) Set

$$f_1 + I := \alpha(c_1), \ldots, f_{n'} + I := \alpha(c_{n'}),$$
$$f_{n'+1} + I := \alpha\left(\sum_{i=1}^{t}(m_1)_i \cdot d_i\right), \ldots, f_s + I := \alpha\left(\sum_{i=1}^{t}(m_{s'})_i \cdot d_i\right)$$

and return $f_1, \ldots, f_s$.

Remarks 2.6. (a) For better clarity, we have written $(\sigma_j - \mathrm{id})(d_i)$ in the expression of step (5). By Convention 2.2 and step (1) of the algorithm, this obviously should be replaced by $d_i(g'_{1j}, \ldots, g'_{n'j}) - d_i$ for concrete computations.

(b) In short, the algorithmic realization of steps (2) and (3) can be done as follows. Step (2) can be performed with an algorithm for the computation of a system of primary invariants for the action of G on P (see below). An implementation of step (3) can

be obtained by an algorithm for computing secondary invariants (with respect to the system of primary invariants $c_1, \ldots, c_{n'}$) for the trivial action of the trivial group on P (see below).
First examinations of the computational aspects of finding a system of primary invariants go back to Hilbert (cf. [Hil93]). An explicit algorithm can be found in the book of Sturmfels (see [Stu93], Algorithm 2.5.8). Later, Kemper has developed a highly optimized method for the computation of primary invariants. Details can be found in [Kem96], [KS99] and [Kem99].
For the implementation of step (3) as suggested above to make sense, we first have to check whether $c_1, \ldots, c_{n'} \in P$ – which by construction is a system of primary invariants for the action of G on P – is a system of primary invariants for the trivial action of the trivial group on P, too. For this, it is enough to show that P is integral over $K[c_1, \ldots, c_{n'}]$. By step (2), we know that P^G is integral over $K[c_1, \ldots, c_{n'}]$. Moreover, the ring P is integral over P^G, since every $p \in P$ satisfies a monic polynomial with coefficients in P^G. This polynomial can be given explicitly by

$$F_p := \prod_{\sigma \in G} \sigma(T - p) \in P^G[T]$$

where T is an indeterminate over P and G acts trivially on T. It follows by [AM69], Chapter 5, Corollary 5.4 that P is integral over $K[c_1, \ldots, c_{n'}]$, as desired. (In particular, it is perfectly valid to assume that the homogeneous system of parameters for P^G in step (2) is of length n'.)
Secondly, observe that the trivial group is certainly linearly reductive. Therefore, by the theorem of Hochster and Roberts (cf. Theorem 1.27), the invariant ring $P^{\{1\}} = P$ of the trivial group is Cohen-Macaulay. This means that elements $d_1, \ldots, d_t$ as requested in step (3) of Algorithm 2.5 exist.
Concrete algorithms for the computation of secondary invariants in the Cohen-Macaulay case can be found for example in [Kem94] and [KS99].

(c) Generators of $\ker(\alpha)$ in step (4) can be obtained with an algorithm for the computation of the ideal of relations of the elements $a_1 + I, \ldots, a_{n'} + I$. A possibility for computing this is as follows. Let $Z_1, \ldots, Z_{n'}$ be indeterminates over $K[x_1, \ldots, x_n]$ and form the ideal

$$D_0 := (Z_1 - a_1, \ldots, Z_{n'} - a_{n'}) + (I) \trianglelefteq K[x_1, \ldots, x_n, Z_1, \ldots, Z_{n'}].$$

Then the ideal of relations of $a_1 + I, \ldots, a_{n'} + I$ is given by the elimination ideal $D_0 \cap K[Z_1, \ldots, Z_{n'}] \trianglelefteq K[Z_1, \ldots, Z_{n'}]$. We do not prove this identity here, since similar (and to some extent more general) considerations with detailed proofs are carried out in Remark 4.23 and [CLO07], Chapter 7, Section 4.
Details about the computation of elimination ideals can be found in Section 1.3.

(d) An algorithm for the computation of the intersection $M' \cap R^t$ can be found in [Kem96]. ♢

Proof of Correctness. We have to show that

$$A^G = K[f_1 + I, \ldots, f_s + I]. \tag{2.1}$$

It is clear by the G-equivariance of α that $\alpha(c_1), \ldots, \alpha(c_{n'}) \in A^G$. Hence for the right hand side of (2.1) to be contained in the left hand side, it remains to prove that

$$\sigma_j\left(\alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right)\right) = \alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right) \quad \text{for all } j = 1, \ldots, m,\ k = 1, \ldots, s'$$

Let $k \in \{1, \ldots, s'\}$. Since $m_k \in M'$, there are polynomials $q_{11}, \ldots, q_{1m}, \ldots, q_{r1}, \ldots, q_{rm} \in P$ such that

$$\sum_{i=1}^{t}(m_k)_i \cdot \begin{pmatrix}(\sigma_1 - \mathrm{id})(d_i)\\ \vdots \\ (\sigma_m - \mathrm{id})(d_i)\end{pmatrix} + \sum_{i=1}^{m} q_{1i} \cdot l_1 e_i + \ldots + \sum_{i=1}^{m} q_{ri} \cdot l_r e_i = 0,$$

where – as in step (5) – we write e_i for the ith standard basis vector of the free module P^m. It follows that $\sum_{i=1}^{t}(m_k)_i \cdot (\sigma_j - \mathrm{id})(d_i) \in \ker \alpha$ for all $j \in \{1, \ldots, m\}$. But this implies that

$$\begin{aligned}\sigma_j\left(\alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right)\right) - \alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right) &= \alpha\left(\sigma_j\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right) - \sum_{i=1}^{t}(m_k)_i \cdot d_i\right)\\ = \alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot (\sigma_j - \mathrm{id})(d_i)\right) &= 0 \quad \text{for all } j \in \{1, \ldots, m\}\end{aligned}$$

and hence $\alpha\left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right) \in A^G$. Since this is true for all $k = 1, \ldots, s'$, it follows that $K[f_1 + I, \ldots, f_s + I] \subset A^G$, as desired.
For the reverse conclusion, let $f + I \in A^G$. By the surjectivity of α, there exists $F \in P$ such that $\alpha(F) = f$. We may write F in the form

$$F = \sum_{i=1}^{t} r_i d_i$$

for some $r_1, \ldots, r_t \in R$. In the following we show that F is contained in the R-module

$$\sum_{k=1}^{s'} R \cdot \left(\sum_{i=1}^{t}(m_k)_i \cdot d_i\right), \tag{2.2}$$

which then obviously implies that $f = \alpha(F) \in K[f_1 + I, \ldots, f_s + I]$.
Since $\alpha(F)$ is invariant under G and α commutes with the action of G, it follows that

$$\alpha\left(\sigma_j\left(\sum_{i=1}^{t} r_i d_i\right) - \sum_{i=1}^{t} r_i d_i\right) = 0 \quad \text{for all } j = 1, \ldots, m$$

and thus

$$\sum_{i=1}^{t} r_i \cdot (\sigma_j - \mathrm{id})(d_i) \in \ker \alpha \quad \text{for all } j = 1, \ldots, m.$$

Writing this in one equation for all $j = 1, \ldots, m$ yields

$$\sum_{i=1}^{t} r_i \cdot \begin{pmatrix} (\sigma_1 - \mathrm{id})(d_i) \\ \vdots \\ (\sigma_m - \mathrm{id})(d_i) \end{pmatrix} \in \sum_{i=1}^{m} P \cdot l_1 e_i + \ldots + \sum_{i=1}^{m} P \cdot l_r e_i$$

and hence there exist $q_{11}, \ldots, q_{1m}, \ldots, q_{r1}, \ldots, q_{rm} \in P$ such that

$$\sum_{i=1}^{t} r_i \cdot \begin{pmatrix} (\sigma_1 - \mathrm{id})(d_i) \\ \vdots \\ (\sigma_m - \mathrm{id})(d_i) \end{pmatrix} + \sum_{i=1}^{m} q_{1i} \cdot l_1 e_i + \ldots + \sum_{i=1}^{m} q_{ri} \cdot l_r e_i = 0.$$

But this means that $(r_1, \ldots, r_t, q_{11}, \ldots, q_{rm}) \in M$ and therefore certainly $(r_1, \ldots, r_t) \in M' \cap R^t$. By definition of $m_1, \ldots, m_{s'}$, there exist elements $b_1, \ldots, b_{s'} \in R$ such that $(r_1, \ldots, r_t) = \sum_{k=1}^{s'} b_k m_k$. It follows that

$$F = \sum_{i=1}^{t} r_i d_i = \sum_{i=1}^{t} \left(\sum_{k=1}^{s'} b_k m_k \right)_i \cdot d_i = \sum_{k=1}^{s'} b_k \left(\sum_{i=1}^{t} (m_k)_i \cdot d_i \right)$$

and thus F is contained in the module (2.2), which finishes the proof. ∎

Remark. Note that by the preceding proof, the algorithm not just gives generators of A^G as a K-algebra. In fact – with the notation of the proof – we have shown that

$$A^G = \sum_{i=1}^{s'} K[f_1 + I, \ldots, f_{n'} + I] \cdot (f_{n'+i} + I).$$

We close this section with an application of Algorithm 2.5 to a concrete example.

Example 2.7. In the following, we present a step-by-step application of Algorithm 2.5 to the situation of Example 2.1.
For step (1), observe that the vector space generated by $x_1 + I, x_2 + I$ is stable under the action of G. Hence we can set $P := K[y_1, y_2]$ where the G-action is given by

$$\sigma(y_1) := y_1, \quad \sigma(y_2) := y_1 + y_2.$$

Moreover, A is a homomorphic image of P under the G-equivariant homomorphism $\alpha : P \longrightarrow A,\ y_i \longmapsto x_i + I$ for $i = 1, 2$. As we have seen in Example 2.1, a homogeneous

system of parameters for P^G is given by

$$c_1 := y_1,\ c_2 := y_1y_2 + y_2^2$$

It can be checked without difficulties that for step (3), we can set $t := 2$ and

$$d_1 := 1,\ d_2 := y_2.$$

Obviously $\ker(\alpha)$ is equal to I and therefore we set $r := 1$ and $l_1 := y_1^2$. Corresponding to step (5) of the algorithm, we have to compute the modules of syzygies

$$M := \mathrm{Syz}_P\left(\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\y_1\end{pmatrix}, \begin{pmatrix}y_1^2\\0\end{pmatrix}, \begin{pmatrix}0\\y_1^2\end{pmatrix}\right) \subset P^4.$$

(where we have set $\sigma_1 := 1_G$ and $\sigma_2 := \sigma$). It is immediate that the module of syzygies of the elements of the first row, i. e. of $0, 0, y_1^2, 0$, is given by $P \times P \times \{0\} \times P \subset P^4$. The syzygies of the second row can be seen as $\{(p_1, p_2, p_3, p_4) \in P^4 : p_4 \cdot y_1 = p_2\}$. It follows that M is generated (as a P-module) by $(0, y_1, 0, 1)$ and $(1, 0, 0, 0)$.
By step (6), it remains to intersect the P-module generated by $(0, y_1)$ and $(1, 0)$ with $K[y_1, y_1y_2 + y_2^2]^2 = (P^G)^2$. Let $p_1, p_2 \in P$. It is clear that if $p_1 \cdot (0, y_1) + p_2 \cdot (1, 0) \in (P^G)^2$, then $p_2 \in P^G$. Moreover, since $p_1 \cdot y_1 \in P^G$ is invariant, it follows by the invariance of y_1 that p_1 is invariant, too, i. e. $p_1 \in P^G$. But this means that $(P \cdot (0, y_1) + P \cdot (1, 0)) \cap (P^G)^2$ is generated as a P^G-module by $(0, y_1)$ and $(1, 0)$. Therefore, we set $m_1 := (0, y_1)$ and $m_2 := (1, 0)$. It follows that A^G is generated by

$$\alpha(y_1) = x_1 + I,\ \alpha(y_1y_2 + y_2^2) = x_1x_2 + x_2^2 + I,\ \alpha(y_1y_2) = x_1x_2 + I,\ \alpha(1) = 1. \qquad \lhd$$

As mentioned above, there exist several algorithms for the computation of invariant rings of finite groups acting linearly on polynomial rings. For these, various optimizations have been suggested by Kemper and Steel in [KS99]. Since the "non-reduced" methods presented in this section use similar constructions as the algorithms for the polynomial cases, one might think that these optimizations could be applied to Algorithm 2.5, too. It can be checked that in principle some of the optimizations are applicable, indeed. Nevertheless, it seems that – unless to the polynomial case – this brings new computational difficulties and complexity and hence does not improve the performance of the non-reduced case.

2.2 Some remarks about infinite groups

Throughout this section, let K be an algebraically closed field and let $x_1, \ldots, x_n$ be indeterminates over K. Moreover, let $A := K[x_1, \ldots, x_n]/I$ with $I \trianglelefteq K[x_1, \ldots, x_n]$ be a (possibly non-reduced) affine algebra and let the reductive group G act on A via a homomorphism of algebras $\tilde{\mu} : A \longrightarrow K[G] \otimes_K A$.

If G is a linearly reductive group, then the invariant ring A^G can be computed with Derksen's algorithm (cf. [Der99]) by carrying out the following well-known construction

(cf. Algorithm 2.3). Let $V \subset A$ be a G-module containing $x_1 + I, \ldots, x_n + I$. Note that such a V always exists since G acts locally finite on A by Proposition 1.31(a). Let $S(V)$ denote the symmetric algebra. It is a G-algebra in a natural way and obviously there exists a G-equivariant, surjective homomorphism $\alpha : S(V) \longrightarrow A$. Since $S(V)$ is a polynomial algebra, the invariant ring $S(V)^G$ can be computed with Derksen's algorithm. But then the invariant ring of A is given by $A^G = \alpha(S(V)^G)$. This latter conclusion – which is only true if G is a linearly reductive group – is a standard result about G-equivariant epimorphisms. For details, see [DK02], Chapter 2, Section 2.2.

In case that G is reductive, the restriction of the homomorphism α to $S(V)^G$ does not map surjectively onto A^G anymore. But at least we know by [MFK94], Appendix, Lemma A.1.2 that $\alpha(S(V)^G)$ and A^G only differ by pth roots, i. e. for all $a \in A^G$ there exists $n \in \mathbb{N}$ such that $a^{p^n} \in \alpha(S(V)^G)$.

Example 2.8. In Example 2.1, we have constructed a G-equivariant homomorphism α mapping from a polynomial ring P to a non-reduced affine algebra A. As we have seen, the restriction of this homomorphism to the invariant ring of P does not map surjectively onto the invariant ring A^G since for example $x_1x_2 + I \notin \alpha(P^G)$ but $x_1x_2 + I \in A^G$. According to the result about pth roots, we have $(x_1x_2 + I)^2 = 0 \in A^G$. ◁

If A is a reduced algebra, Kemper and Derksen have found a method to bridge the gap between $\alpha(S(V)^G)$ and A^G algorithmically. They have developed an algorithm for computing (finitely many) generators of the B-module $\sqrt[p]{B} := \{a \in A;\ a^p \in B\}$ of pth roots, where B is an arbitrary finitely generated subalgebra of A. Roughly speaking, the invariant ring A^G can then be calculated by applying this algorithm successively until there are no pth roots left (cf. [DK08], Algorithms 1.4 & 1.7).
In the non-reduced case, this does not work anymore. In fact, the module of pth-roots of a subalgebra B of A may not be finitely generated. Neither is it true that a pth root of an invariant is again an invariant. This is illustrated in the following example.

Example 2.9. Let $K = \overline{\mathbb{F}_2}$ be the algebraic closure of the field with two elements, let x_1, x_2 be indeterminates over K and let the multiplicative group $G = K^\times := K \setminus \{0\}$ act on the algebra $A := K[x_1, x_2]/(x_1^2)$ via multiplication, i. e.

$$\lambda(x_1 + I) := \lambda x_1 + I,\ \lambda(x_2 + I) := \lambda x_2 + I \quad \text{for all } \lambda \in G.$$

Note that the vector space V generated by $x_1 + I$ and $x_2 + I$ is G-stable and generates A (as a K-algebra). Following the above construction, the symmetric algebra $S(V)$ is given by $S(V) = K[x_1, x_2]$, the action of G on $S(V)$ is given by

$$\lambda(x_1) := \lambda x_1,\ \lambda(x_2) := \lambda x_2 \quad \text{for all } \lambda \in G.$$

and moreover, the homomorphism α is defined by

$$K[x_1, x_2] \longrightarrow A,\ x_i \longmapsto x_i + I \quad \text{for } i = 1, 2.$$

An easy argument shows that $S(V)^G = K$ (cf. Example 3.1). Hence it follows that $\alpha(S(V)^G) = K$, too. One can check that the module of square roots of K in A is given by

$$K + (x_1 + I)_{K[x_1+I, x_2+I]} = K[x_1 + I, x_1x_2 + I, x_1x_2^2 + I, x_1x_2^3 + I, \ldots]$$

It is not finitely generated as a module over K. In fact, there does not even exist a finite generating set as an algebra over K. Moreover, there are obviously non-invariant elements in this algebra. $\lhd$

It thus seems to be the wrong way to compute A^G by some sort of closure operation of $\alpha(S(V)^G)$. In any case, it is still open how to compute the invariant ring of a reductive group acting on a non-reduced affine algebra.

3 Computing invariants of unipotent groups acting on affine varieties

In [vdE93], van den Essen has found an algorithm for the computation of the invariant ring of the additive group G_a acting regularly on an irreducible affine variety X. His algorithm works in the case that the underlying field K has characteristic zero. It relies heavily on a well-known correspondence of regular G_a-actions and so-called locally nilpotent derivations which does not hold any more in positive characteristic.
Until recently, there was no method known for the computation of additive group invariants in characteristic p. It was in 2008 that Derksen and Kemper succeeded in a generalization of van den Essen's work to this case (cf. [DK08]). Furthermore, based on this result, they developed an algorithm for the computation of invariant rings of arbitrary connected unipotent groups acting on irreducible affine varieties which works in arbitrary characteristic. Essentially, the idea was the following. Every connected unipotent group possesses a finite composition series whose factors are isomorphic (as algebraic groups) to the additive group G_a. This can be used to inductively compute invariants of unipotent group actions by repeatedly applying the "base algorithm" for the computation of the invariant ring of the additive group. It is necessary for the applicability of their method to have a composition series of the unipotent group. Moreover, the isomorphisms of the factor groups and the additive group must be given explicitly.
In this chapter, we give an algorithm for the computation of the invariant ring of a unipotent group G acting on an irreducible affine variety X which works in arbitrary characteristic. Apart from the group G, the variety X and the action of G on X, no additional input data or structural knowledge about the group – as for example a composition series etc. – is required. Moreover, it turns out that this algorithm not only works for unipotent groups but also for certain other situations.
Note that by a theorem of Nagata (cf. [Nag59]), it may happen that the invariant ring $K[X]^G$ is not finitely generated (as a K-algebra). In this case the algorithm* for the computation of generators cannot terminate. In fact, it terminates if and only if the invariant ring $K[X]^G$ is finitely generated.

Before we start with the algorithmic details, we examine the relation of the field of fractions of the invariant ring $\mathrm{Quot}(K[X]^G)$ and the invariant field $K(X)^G$. Recall that the invariant field $K(X)^G$ is given by the set of rational functions which are invariant

*Some people do not like to use the term algorithm if termination after a finite number of steps is not guaranteed. Nonetheless, we will call the resulting recipe for the computation of the invariant ring an algorithm and we will do so for all following algorithms regardless of whether they terminate or not.

under G, the so-called rational invariants, that is

$$K(X)^G = \left\{ \frac{n}{d};\ n \in K[X], d \in K[X] \setminus \{0\} \text{ such that } \frac{\sigma(n)}{\sigma(d)} = \frac{n}{d} \text{ for all } \sigma \in G \right\}.$$

This examination turns out to be very fruitful for the algorithms. Apart from that it provides some insights which are interesting for their own sake.

Unless otherwise stated, let K be an algebraically closed field, let X be an irreducible affine variety over K and let G be a linear algebraic group over K acting regularly on X. Note that G does not have to be unipotent for now.

3.1 Some remarks about the relation of the field of fractions of the invariant ring and the invariant field

It is obvious that the field of fractions of the invariant ring, i. e. $\mathrm{Quot}(K[X]^G)$, is contained in the invariant field $K(X)^G$. In general, this inclusion is strict, as the following example shows.

Example 3.1. Let $G = K^\times := K \setminus \{0\}$ act on $X = K^2$ via multiplication, i. e. $\lambda(\xi_1, \xi_2) := (\lambda\xi_1, \lambda\xi_2)$. The orbits of this action are the origin and all lines through the origin with the origin removed. From this it follows that the origin is contained in the closure of every orbit and hence $K[X]^G = K$.
Let x_1, x_2 denote the coordinate functions on K^2. Then obviously x_1/x_2 is a rational invariant and therefore $K = \mathrm{Quot}(K[X]^G) \neq K(X)^G$.
Generalizing this example to higher dimensions shows that there does not even exist a bound for the difference of the transcendental degrees of $\mathrm{Quot}(K[X]^G)$ and $K(X)^G$. $\lhd$

In the sequel, we will examine various situations where we can actually show that the equality $\mathrm{Quot}(K[X]^G) = K(X)^G$ holds. Apart from that we will give several examples where this equality fails along with geometric interpretations why this is the case.
As we will see, the equality of the field of fractions of the invariant ring and the invariant field can be proved for certain types of algebraic groups G, for varieties X with special properties and for some types of actions of G on X.

Before we can start with this programme, we have to digress briefly to some basic considerations about colon ideals. Recall the definition of a colon ideal. If $I, I' \trianglelefteq R$ are ideals of some ring R, then the set

$$I : I' := \{r \in R;\ r \cdot I' \subset I\}$$

is an ideal of R. It is called the **colon ideal** of I by I'.
Let $n/d = \tilde{n}/\tilde{d} \in K(X)$ be two representations of the same rational function. We claim

that

$$(d)_{K[X]} : (n)_{K[X]} = (\tilde{d})_{K[X]} : (\tilde{n})_{K[X]}.$$

If $n/d = \tilde{n}/\tilde{d} = 0$, then obviously $(d)_{K[X]} : (n)_{K[X]} = (\tilde{d})_{K[X]} : (\tilde{n})_{K[X]} = K[X]$. In case that $n/d \neq 0$, we show that the left hand side of the above equation is contained in the right hand side. By symmetry, this implies equality. So let $d' \in (d)_{K[X]} : (n)_{K[X]}$. By definition of the colon ideal, there exist $n' \in K[X]$ such that $d' \cdot n = n' \cdot d$. The equality $n/d = \tilde{n}/\tilde{d}$ implies that $\tilde{n} \cdot d = n \cdot \tilde{d}$. Multiplying these two equations yields $d' \cdot n \cdot \tilde{n} \cdot d = n' \cdot d \cdot n \cdot \tilde{d}$. Both n and d being non-zero and $K[X]$ being a domain, it follows that $d' \cdot \tilde{n} = n' \cdot \tilde{d}$. But this means $d' \in (\tilde{d})_{K[X]} : (\tilde{n})_{K[X]}$, as desired.

For a rational invariant $n/d \in K(X)^G$ we can thus define

$$\mathfrak{a}(n/d) := (d)_{K[X]} : (n)_{K[X]} = \{d' \in K[X];\ d' \cdot n \in (d)_{K[X]}\}.$$

It will turn out in the following proposition that this ideal is closely related to the question whether n/d can be written as a quotient of regular invariants or not.

Proposition 3.2. *Let the linear algebraic group G act regularly on the irreducible affine variety X and let $n/d \in K(X)^G$ be a rational invariant. Then*

(a) $\mathfrak{a}(n/d)$ is a G-stable ideal.

(b) $n/d \in \mathrm{Quot}(K[X]^G) \iff \mathfrak{a}(n/d) \cap K[X]^G \neq \{0\}$.

Proof. (a) Since $\sigma \in G$ defines an automorphism of $K[X]$, we have

$$\begin{aligned}\sigma(\mathfrak{a}(n/d)) &= \{\sigma(d');\ d' \in K[X] \text{ and } d' \cdot n \in (d)\} \\ &= \{\sigma(d');\ d' \in K[X] \text{ and } \sigma(d') \cdot \sigma(n) \in (\sigma(d))\} \\ &= \mathfrak{a}(\sigma(n)/\sigma(d) \\ &= \mathfrak{a}(n/d).\end{aligned}$$

(b) Assume first that $n/d \in \mathrm{Quot}(K[X]^G)$. Then there are $n', d' \in K[X]^G$ with $d' \neq 0$ such that $n/d = n'/d'$. But this means $n \cdot d' = n' \cdot d$ and hence $d' \in \mathfrak{a}(n/d) \cap K[X]^G$. Conversely, let $d' \in \mathfrak{a}(n/d) \cap K[X]^G$ with $d' \neq 0$. By definition of the colon ideal, there exists $n' \in K[X]$ such that $d' \cdot n = d \cdot n'$. This means that $n/d = n'/d'$. Since n/d is a rational invariant and $d' \in K[X]^G$, it follows that n' is invariant, too. But this says that $n/d \in \mathrm{Quot}(K[X]^G)$.

Remark 3.3. One can think of $\mathfrak{a}(n/d) \setminus \{0\}$ as the set of all possible denominators of representations of the rational function n/d as a quotient of regular functions. With this in mind, the validity of Proposition 3.2 is obvious. ♢

For finite groups we have the following well-known result.

Proposition 3.4. *Let the finite group G act regularly on the irreducible affine variety X. Then* $\mathrm{Quot}(K[X]^G) = K(X)^G$.

Proof. Let $n/d \in K(X)^G$ be a rational invariant. Then $0 \neq \prod_{\sigma\in G} \sigma(d) \in \mathfrak{a}(n/d) \cap K[X]^G$. So by Proposition 3.2, it follows that $n/d \in \mathrm{Quot}(K[X]^G)$. ∎

Remark 3.5. Note that for the proof of this proposition we do not need the geometric setting of a finite group G acting regularly on an irreducible affine variety X. In fact, if we replace $K[X]$ by an arbitrary integral domain R and G by a finite group of automorphisms of R, then we still have $\mathrm{Quot}(R^G) = \mathrm{Quot}(R)^G$. ♢

For infinite groups we have seen that in general, the field of fractions of the invariant ring differs from the invariant field. However, in case that G is a unipotent group, we have equality, as will be shown in the following proposition.

Proposition 3.6. *Let the linear algebraic group G act regularly on the irreducible affine variety X. If the identity component G^0 of G is unipotent, then* $\mathrm{Quot}(K[X]^G) = K(X)^G$.

Proof. Assume first that G is a connected, unipotent group and let $n/d \in K(X)^G$ be a rational invariant. By Corollary 1.33, the group G acts locally finite on $K[X]$. Since the ideal $\mathfrak{a}(n/d)$ is G-stable (cf. Proposition 3.2), we can find a non-zero finite dimensional G-stable vector space $V \subset \mathfrak{a}(n/d)$. As G is unipotent, it follows that $V^G \neq 0$ (see [Hum75], Chapter 17, Theorem 17.5) and hence $\mathfrak{a}(n/d)^G \neq 0$. Now Proposition 3.2 implies that $n/d \in \mathrm{Quot}(K[X]^G)$.
For the case where G is not connected, recall that the identity component G^0 is a normal subgroup of finite index in G (cf. Definition and Proposition 1.15). Therefore, by Remark 3.5, it follows

$$\begin{aligned}\mathrm{Quot}(K[X]^G) &= \mathrm{Quot}((K[X]^{G^0})^{G/G^0}) = \mathrm{Quot}(K[X]^{G^0})^{G/G^0} \\ &= (K(X)^{G^0})^{G/G^0} = K(X)^G,\end{aligned}$$

which proves the proposition. ∎

Definition 3.7. *Let G be a linear algebraic group. A* **rational character** *of G is a homomorphism $\chi : G \longrightarrow K^\times$ of algebraic groups. Let G act regularly on the affine variety X and let χ be a rational character of G. An element $f \in K[X]$ is said to be a* **semi-invariant of weight** χ *if*

$$\sigma(f) = \chi(\sigma)f \qquad \text{for all } \sigma \in G.$$

Example 3.8. Let $G = K^\times$ act on $X = K^2$ as in Example 3.1. Then both x_1 and x_2 are semi-invariants of weight $G \longrightarrow K^\times,\ \lambda \longmapsto \lambda$. In particular, the rational invariant x_1/x_2 is a quotient of semi-invariants. It can be shown that every rational invariant of this action can be written as a quotient of semi-invariants (necessarily of the same weight). For details, see Proposition 3.11 below. $\triangleleft$

If $n, d \in K[X]$ are semi-invariants of the same weight, then clearly n/d is a rational invariant. As in the preceding example, one might hope that conversely every rational invariant can be written as a quotient of semi-invariants. This would clarify the relation of the quotient field of the invariant ring and the invariant field. But this is not true in general, as the example below shows. To be more precise, we will give an example of an action of the linear algebraic group $\mathrm{SL}_2(K)$ where the quotient field of the invariant ring is not equal to the invariant field. Since $\mathrm{SL}_2(K)$ is a perfect group, it does not have any rational characters. Hence it follows that there are rational invariants which cannot be written as quotients of semi-invariants.
In some sense this example is geometrically analogous to Example 3.1 – again, the orbits of the action are the origin and linear subspaces with the origin removed.

Example 3.9. Let K be an algebraically closed field, let x_1, x_2, x_3, x_4 be indeterminates over K, let $X := \mathrm{Var}(I) \subset K^4$ with $I := (x_1x_4 - x_2x_3) \trianglelefteq K[x_1, x_2, x_3, x_4]$ and let $G := \mathrm{SL}_2 := \mathrm{SL}_2(K)$ act on X by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (\xi_1, \xi_2, \xi_3, \xi_4) := (\alpha\xi_1 + \beta\xi_3, \alpha\xi_2 + \beta\xi_4, \gamma\xi_1 + \delta\xi_3, \gamma\xi_2 + \delta\xi_4)$$
$$\text{for all } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2, (\xi_1, \xi_2, \xi_3, \xi_4) \in X.$$

One can think of X as the set of all 2×2-matrices $\begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix}$ with determinant 0. It is then clear that the action of SL_2 on X comes from the multiplication with SL_2 from the left. For $M = \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix} \in X$ we define the kernel of M in the usual way as

$$\ker(M) := \left\{ \begin{pmatrix} \upsilon_1 \\ \upsilon_2 \end{pmatrix} \in K^2;\ \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix} \begin{pmatrix} \upsilon_1 \\ \upsilon_2 \end{pmatrix} = 0 \right\}.$$

We claim that $M, M' \in X$ are contained in the same SL_2-orbit if and only if $\ker(M) = \ker(M')$. It is obvious that all elements of an SL_2-orbit have the same kernel. For the converse, let $M, M' \in X$ with $\ker(M) = \ker(M')$. If $\ker(M) = K^2$, that is $M = 0$, then $M' = 0$, too. Otherwise, let $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \notin \ker(M)$. Then there is a linear transformation σ of

K^2 such that

$$\sigma\left(M\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) = M'\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}.$$

Moreover, since K^2 is two-dimensional we can choose σ to be an element of SL_2 which proves the claim.
It follows that the orbits of SL_2 on X are given by the origin

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

and for each $\begin{pmatrix}\upsilon_1\\ \upsilon_2\end{pmatrix} \neq 0$ the linear subspace with the origin removed

$$\left\{\begin{pmatrix}\xi_1 & \xi_2\\ \xi_3 & \xi_4\end{pmatrix};\ \begin{pmatrix}\xi_1 & \xi_2\\ \xi_3 & \xi_4\end{pmatrix}\begin{pmatrix}\upsilon_1\\ \upsilon_2\end{pmatrix} = 0\right\} \setminus \{0\}.$$

Since the origin is in the closure of every orbit, it follows that $K[X]^{\mathrm{SL}_2} = K$. But on the other hand Rosenlicht's Theorem (cf. [Ros56]) says that there is a dense G-stable open subset U of X such that all orbits contained in U can be separated by rational invariants. Since no orbit is dense in X, it follows that non-constant rational invariants must exist. It can be checked easily that for example $(x_3 + I)/(x_4 + I) \in K(X)^{\mathrm{SL}_2}$. So $\mathrm{Quot}(K[X]^{\mathrm{SL}_2}) \neq K(X)^{\mathrm{SL}_2}$. ◁

Nonetheless, for special types of varieties – for so-called factorial varieties – it is true that every rational invariant can be written as a quotient of semi-invariants. An irreducible affine variety X is called **factorial** if the coordinate ring $K[X]$ is a unique factorization domain. For the case that X is a finite dimensional vector space this result seems to be folklore. For the proof of the more general case where $K[X]$ is a factorial but not necessarily a polynomial ring, special care has to be taken of the units of $K[X]$.
In [Ros57], Rosenlicht proved the following useful result about the structure of $K[X]^\times$, the group of units of $K[X]$.

Proposition 3.10. *Let X be an irreducible affine variety over K. Then $K[X]^\times/K^\times$ is a free abelian group of finite rank.* ■

Equipped with this, we can prove

Proposition 3.11. *Let the linear algebraic group G act regularly on the factorial affine variety X. Then every rational invariant can be written as a quotient of semi-invariants of the same weight. In particular, if G does not have any rational characters, then $\mathrm{Quot}(K[X]^G) = K(X)^G$.*

Remarks 3.12. (a) For every perfect linear algebraic group G acting on a factorial

variety X it follows that $\mathrm{Quot}(K[X]^G) = K(X)^G$, since a perfect group obviously does not have any rational characters. Examples for perfect groups include the classical groups $\mathrm{SL}_n(K)$ and $\mathrm{Sp}_{2n}(K)$.

(b) From the proof of the proposition it will follow that if a connected group G acts regularly on an irreducible affine variety X, then $K[X]^\times$ consists of semi-invariants. In particular, if G has no rational characters then $K[X]^\times \subset K[X]^G$.
In general, this is false if G is not connected. Let x_1, x_2 be indeterminates over K and let the cyclic group with two elements, $G = \langle\sigma\rangle$, act on $X = \mathrm{Var}(x_1x_2 - 1) \subset K^2$ by

$$\sigma(\xi_1, \xi_2) := (\xi_2, \xi_1) \qquad \text{for all } (\xi_1, \xi_2) \in X.$$

Since $K[X]$ is a localization of a polynomial ring, it follows that $K[X]$ is a unique factorization domain. Observe that $x_1 + (x_1x_2 - 1)_{K[x_1,x_2]}$ is mapped to $x_2 + (x_1x_2 - 1)_{K[x_1,x_2]}$ under σ. Therefore, the unit $x_1 + (x_1x_2 - 1)_{K[x_1,x_2]}$ is not a semi-invariant.

(c) Although the proof of the proposition takes a slightly different approach, it can be shown that if $n/d \in K(X)^G$ is a rational invariant of a connected group G acting on a factorial variety X with n and d coprime, then both n and d are necessarily semi-invariants of the same weight.
On the first sight this seems to be a convenient way to find an expression of a rational invariant n/d as a quotient of semi-invariants by simply cancelling out common factors of n and d. Nonetheless, it may be very hard to actually find common factors of n and d algorithmically. For more details about algorithmic aspects, see the next section. ♢

For the simplification of the proof of Proposition 3.11 we need the following auxiliary lemma.

Lemma 3.13. *Let the linear algebraic group G act regularly on the affine variety X. Let $\chi : G \longrightarrow K^\times$ be a homomorphism of groups and let $f \in K[X] \setminus \{0\}$ be an element such that*

$$\sigma(f) = \chi(\sigma)f \qquad \text{for all } \sigma \in G.$$

Then χ is a rational character. In particular, it follows that f is a semi-invariant.

Proof. We have to prove that χ is a morphism of algebraic groups. In short, this follows from the fact that G acts regularly on X. To be more explicit, recall that the induced action of G on $K[X]$ can be described by a homomorphism of algebras $\tilde{\mu} : K[X] \longrightarrow K[G] \otimes_K K[X]$ (cf. Lemma 1.28). Let $\tilde{\mu}(f) = \sum_{i=1}^{s} g_i \otimes a_i$ with $g_i \in K[G], a_i \in K[X]$. We may assume that $a_1, \ldots, a_s \in K[X]$ are linearly independent over K. Apparently, there exists $i_0 \in \{1, \ldots, s\}$ with $g_{i_0}(1_G) \neq 0$. It then can be verified that $\chi = g_{i_0}/g_{i_0}(1_G)$, so χ is a rational character, indeed. ∎

Proof (of Proposition 3.11). We start with the proof of the proposition for the special case that G is a connected linear algebraic group. First, we show that every unit of $K[X]$ is a semi-invariant. The action of G on $K[X]$ induces an action of G on $K[X]^\times/K^\times$. Since by Rosenlicht's Proposition 3.10, the latter group is isomorphic to $\mathbb{Z}^r$ for some $r \in \mathbb{N}_0$, this action in turn corresponds to a homomorphism of groups $\phi : G \longrightarrow \mathrm{GL}_r(\mathbb{Z})$. We claim that ϕ is trivial. Let $p \in \mathbb{Z}$ be a prime number. Then the composition of ϕ and the componentwise reduction modulo p yields a homomorphism $G \longrightarrow \mathrm{GL}_r(\mathbb{F}_p)$ which must be trivial by the connectedness of G. Since p was chosen arbitrarily, this implies that ϕ itself must be trivial.
Let $\epsilon \in K[X]^\times$ be a unit. By the above, it makes sense to define the map $\chi_\epsilon : G \longrightarrow K^\times$, $\sigma \longmapsto \sigma(\epsilon)/\epsilon$. Let $\sigma, \tau \in G$ be arbitrary. Then

$$\begin{aligned}\chi_\epsilon(\sigma\tau) &= \frac{(\sigma\tau)(\epsilon)}{\epsilon} = \frac{\sigma(\tau(\epsilon))}{\epsilon} \cdot \frac{\tau(\epsilon)}{\tau(\epsilon)} = \frac{\sigma(\chi_\epsilon(\tau)\epsilon)}{\chi_\epsilon(\tau)\epsilon} \cdot \frac{\tau(\epsilon)}{\epsilon} \\ &= \chi_\epsilon(\sigma) \cdot \chi_\epsilon(\tau),\end{aligned}$$

and so χ_ϵ is a homomorphism of groups. By Lemma 3.13, the homomorphism χ_ϵ is a rational character and therefore every unit in $K[X]$ is a semi-invariant, indeed.
Let now $n/d \in K(X)^G \setminus \{0\}$ be a rational invariant. We show that $\mathfrak{a}(n/d)$ contains a semi-invariant. By Remark 3.3, it then follows that n/d can be written as n'/d' where the denominator d' is a semi-invariant. As $n/d = n'/d'$ is a rational invariant, this implies that the numerator n' is a semi-invariant, too.
Since $K[X]$ is a unique factorization domain, it is immediate that

$$\mathfrak{a}(n/d) = \left(\frac{d}{\gcd(n,d)}\right),$$

where we write $\gcd(n,d)$ for the greatest common divisor of n and d. In particular, $\mathfrak{a}(n/d)$ is a principal ideal. Let $h := d/\gcd(n,d)$. Then $\mathfrak{a}(n/d) = (h)$ is G-stable by Proposition 3.2 and hence it follows that for all $\sigma \in G$ there exists $\epsilon_\sigma \in K[X]^\times$ such that $\sigma(h) = \epsilon_\sigma \cdot h$. We claim that the map $\eta : G \longrightarrow K[X]^\times$, $\sigma \longmapsto \epsilon_\sigma$ is a homomorphism of groups. Let χ_ϵ be the character belonging to the unit ϵ (see a few lines above). Then

$$\begin{aligned}\eta(\sigma\tau) &= \frac{(\sigma\tau)(h)}{h} = \frac{\sigma(\tau(h))}{h} = \frac{\sigma(\eta(\tau)\cdot h)}{h} \\ &= \frac{\sigma(\eta(\tau))\cdot\sigma(h)}{h} = \frac{\chi_{\eta(\tau)}(\sigma)\cdot\eta(\tau)\cdot\sigma(h)}{h} \\ &= \chi_{\eta(\tau)}(\sigma)\cdot\eta(\tau)\cdot\eta(\sigma).\end{aligned} \tag{3.1}$$

Applying Rosenlicht's Proposition 3.10 to the composition of η with the natural epimorphism $K[X]^\times \longrightarrow K[X]^\times/K^\times$ yields a homomorphism $G \longrightarrow \mathbb{Z}^r$. Similarly to the argument above, this homomorphism must by trivial by the connectedness of G, which shows that η maps into $K^\times$. But this implies $\chi_{\eta(\tau)} = 1$ and it follows from (3.1) that η is a homomorphism of groups. By Lemma 3.13, the map $\eta : G \longrightarrow K^\times$ is a homomorphism of algebraic groups, i. e. η is a rational character.
We have shown that h is a semi-invariant of weight η which is contained in $\mathfrak{a}(n/d)$. There-

fore, the proposition is proved for the special case that G is a connected algebraic group.

Let now G be an arbitrary linear algebraic group and – as above – let $n/d \in K(X)^G \setminus \{0\}$ be a rational invariant. Let $N := G^0$ be the identity component of G. Then obviously n/d is invariant under N, too, and by what we have proved before, we may assume that n and d are semi-invariants for the action of the group N on $K[X]$, say of weight $\chi : N \longrightarrow K^\times$. Let $T \subset G$ be a set of representatives for the residue classes of G mod N. We claim that

$$\prod_{\tau \in T} \tau(n)$$

is a semi-invariant for the action of G on $K[X]$. Let $\sigma \in G$. By construction, every element of G can be written uniquely as a product of an element of T and an element of N. More explicitly, if $\sigma \in G$, then

$$\sigma = \sigma_T \sigma_N \qquad \text{for } \sigma_T \in T, \sigma_N \in N.$$

The notation $-_T$ resp. $-_N$ will be used in the following computations. Before going into the details, observe that $\{(\sigma\tau)_T;\ \tau \in T\} = T$ for all $\sigma \in G$ which can be seen by an easy argument. Keeping this in mind, one calculates

$$\begin{aligned}\sigma\left(\prod_{\tau\in T}\tau(n)\right) &= \prod_{\tau\in T}((\sigma\tau)_T(\sigma\tau)_N)(n) = \prod_{\tau\in T}\chi((\sigma\tau)_N)\cdot(\sigma\tau)_T(n)\\ &= \lambda\cdot\prod_{\tau\in T}(\sigma\tau)_T(n) = \lambda\cdot\prod_{\tau\in T}\tau(n)\end{aligned}$$

for some $\lambda \in K$. An easy verification together with Lemma 3.13 shows that the map

$$\chi' : G \longrightarrow K^\times,\ \sigma \longmapsto \sigma\left(\prod_{\tau\in T}\tau(n)\right) \Big/ \prod_{\tau\in T}\tau(n)$$

is a rational character. It follows that $\prod_{\tau\in T}\tau(n)$ is a semi-invariant for the action of G on $K[X]$, as claimed.
We may assume that $1_G \in T$. Since

$$n/d = \frac{\prod_{\tau\in T}\tau(n)}{d\cdot\prod_{\tau\in T,\tau\neq 1_G}\tau(n)} \in K(X)^G$$

is a rational invariant, it follows that the denominator $d\cdot\prod_{\tau\in T,\tau\neq 1_G}\tau(n)$ is a semi-invariant, too, necessarily of the same weight $\chi' : G \longrightarrow K^\times$ as the numerator. Hence n/d can be written as a quotient of semi-invariants, as we wanted to show. ∎

Corollary 3.14. *Let the linear algebraic group G act regularly on the factorial affine variety X. If the identity component of G does not have any rational characters, then* $\mathrm{Quot}(K[X]^G) = K(X)^G$.

Proof. By the previous proposition, the assertion is true for connected groups. Then – similarly as in the proof of Proposition 3.6 – an application of Remark 3.5 yields the desired result for possibly non-connected groups. ∎

It is tempting to hope that the previous proposition might even be true if X is only assumed to be a normal variety, i. e. if $K[X]$ is a normal ring. But this is not the case for general normal varieties, as the following example shows.

Example 3.15. We show that the variety X of Example 3.9 is a normal variety. In short, X is a so-called determinantal variety and varieties of this type are always normal (see [HE71]). Determinantal varieties can be quite complicated, however, for the simple case here, it is easy to give a proof of normality explicitly.
Let $V = K^4$ and consider the action of $G = K^\times$ on V given by

$$\lambda(v_1, v_2, v_3, v_4) := (\lambda v_1, \lambda v_2, \lambda^{-1} v_3, \lambda^{-1} v_4) \qquad \text{for all } (v_1, v_2, v_3, v_4) \in V,\ \lambda \in G.$$

The coordinate ring of V is a polynomial ring and hence a normal domain. It is a well-known fact that the invariant ring of a group acting on a normal domain is again normal (see for example [DK02], Chapter 2, Proposition 2.3.11). Hence the normality of X follows if we can show that $K[V]^G = K[X]$. Let y_1, y_2, y_3, y_4 denote the coordinate functions on V. Then the invariant ring $K[V]^G$ is given by

$$K[V]^G = K[y_1y_3, y_1y_4, y_2y_3, y_2y_4].$$

Let $T_1, \ldots, T_4$ be indeterminates over K and consider the homomorphism of rings

$$\phi : K[T_1, T_2, T_3, T_4] \longmapsto K[V]^G,\ T_1 \longmapsto y_1y_3, T_2 \longmapsto y_1y_4, T_3 \longmapsto y_2y_3, T_4 \longmapsto y_2y_4.$$

Obviously, $T_1T_4 - T_2T_3$ lies in the kernel of ψ. Since $(T_1T_4 - T_2T_3) \trianglelefteq K[T_1, T_2, T_3, T_4]$ is a prime ideal of height one and the dimension of $K[V]^G$ is equal to 3, it follows that $K[X] \cong K[T_1, T_2, T_3, T_4]/(T_1T_4 - T_2T_3) \cong K[V]^G$. ◁

In Example 3.1 and Example 3.9 we have seen that the quotient field of the invariant ring can be properly contained in the invariant field. As mentioned earlier, the geometries of the respective actions are similar in the sense that in both cases the origin is contained in the closure of every orbit. In fact, the origin may be thought of as a "pivotal point" posing an obstacle for the equality of $\mathrm{Quot}(K[X]^G)$ and $K(X)^G$. For, if we had $\mathrm{Quot}(K[X]^G) = K(X)^G$, then by Rosenlicht's Theorem (cf. [Ros56]), it would follow that the orbits of the points contained in some dense open subset of X could be separated by invariants. In both examples the special property of the origin forces the invariant ring to be trivial. But on the other hand, there does not exist a dense orbit in neither of the two cases, which is obviously a contradiction.
Roughly speaking, for the equality $\mathrm{Quot}(K[X]^G) = K(X)^G$ to be true, it is necessary that the invariant ring has strong separating properties.

If we impose the additional restriction on the action of G on X that all orbits of G are closed in X, then there are at least no topological reasons why orbits cannot be separated by invariants. In fact, if G is a reductive group, then this additional property implies that the field of fractions of the invariant ring is equal to the invariant field.

Proposition 3.16. *Let the reductive group G act regularly on the irreducible affine variety X and assume that all orbits of G in X are closed. Then* $\mathrm{Quot}(K[X]^G) = K(X)^G$.

Proof. Let $n/d \in K(X)^G$ be a rational invariant. The set $Y := \mathrm{Var}_X(\mathfrak{a}(n/d))$ is a proper closed subset of X which is G-stable by Proposition 3.2. Let $p \in X \setminus Y$ be arbitrary. By assumption, the orbit $Z := G \cdot p$ is closed in X, hence there exists an invariant $f \in K[X]^G$ which vanishes on Y and is not zero on Z (see [New78], Chapter 3, Lemma 3.3). By Hilbert's Nullstellensatz (cf. Theorem 1.5), it follows that $f^s \in \mathfrak{a}(n/d)$ for some $s \in \mathbb{N}$. But this implies that $\mathfrak{a}(n/d) \cap K[X]^G \neq \{0\}$, and so we are done by Proposition 3.2. ∎

3.2 Algorithms

As mentioned at the beginning of this chapter, van den Essen and later Derksen and Kemper have constructed algorithms for the computation of the invariant ring of the additive group acting on an irreducible affine variety. Since the additive group is not reductive, it may happen that the invariant ring is not finitely generated (cf. [Nag59], [Pop79]). Algorithmically, they handled this problem as follows. If the invariant ring is finitely generated, then their algorithms terminate. Otherwise, they return an infinite sequence $f_1, f_2, \ldots \in K[X]^G$ of invariants which generate the invariant ring in the usual sense: If $f \in K[X]^G$ is an invariant, then there exists $s \in \mathbb{N}$ such that $f \in K[f_1, \ldots, f_s]$.
The approaches for the computation of the invariant ring of van den Essen as well as Derksen and Kemper can roughly be described as follows. First, an non-zero invariant $f \in K[X]^G \setminus \{0\}$ is chosen with the property that $K[X]^G_f$ is finitely generated and generators of $K[X]^G_f$ can be calculated. Then the intersection $K[X]^G_f \cap K[X]$ is computed. Note that the invariant ring $K[X]^G$ is equal to this intersection.
The method we present here for the computation of invariant rings of certain group actions – including unipotent ones – uses a similar approach.

First we give the definition of the so-called colon operation which will be needed for the algorithm.

Definition 3.17. *Let S be an algebra over K, $R \subset S$ be a subalgebra and let $\mathfrak{a} \trianglelefteq R$ be an ideal of R. We define*

$$(R : \mathfrak{a})_S := \{s \in S;\ s \cdot \mathfrak{a} \subset R\}$$

and

$$(R : \mathfrak{a}^\infty)_S := \bigcup_{i=1}^{\infty} (R : \mathfrak{a}^i)_S = \{s \in S;\ \exists i \in \mathbb{N} : s \cdot \mathfrak{a}^i \subset R\}.$$

Note that we have used the notion of the ith power of an ideal which is defined recursively as $\mathfrak{a}^0 := (1) \trianglelefteq R$ *and for* $i \in \mathbb{N}$ *as* $\mathfrak{a}^i := (r_1 r_2 :\ r_1 \in \mathfrak{a}, r_2 \in \mathfrak{a}^{i-1}) \trianglelefteq R$.
(For a more general definition of the concept of the colon operation, see [DK08])

Remarks 3.18. (a) Using the notation of the definition, if the ideal $\mathfrak{a}$ is generated by one element, say $\mathfrak{a} = (f)_R$, then we also write $(R : f)_S$ resp. $(R : f^\infty)_S$ instead of $(R : \mathfrak{a})_S$ resp. $(R : \mathfrak{a}^\infty)_S$.

(b) Let S be an affine domain, $R \subset S$ be a finitely generated subalgebra and $\mathfrak{a} \trianglelefteq R$. If $\mathfrak{a} \neq (0)$, then $(R : \mathfrak{a})_S$ has the structure of a finitely generated R-module. For, let $f \in \mathfrak{a} \setminus \{0\}$. By definition, we have $f \cdot (R : \mathfrak{a}) \subset R$. So we may identify $(R : \mathfrak{a})_S$ with a submodule of R. In particular, it follows that $(R : \mathfrak{a})_S$ is finitely generated as an R-module. The union $(R : \mathfrak{a}^\infty)_S = \bigcup_{i=1}^{\infty} (R : \mathfrak{a}^i)_S$ is a subalgebra of S. In general, this subalgebra is not finitely generated (cf. [DK08], Section 2).

(c) Let S be an affine domain, say $S := K[x_1, \ldots, x_n]/I$ with $x_1, \ldots, x_n$ indeterminates over K and $I \trianglelefteq K[x_1, \ldots, x_n]$ a prime ideal. Furthermore, let $R \subset S$ be a finitely generated K-algebra and $\mathfrak{a} \trianglelefteq R$. Derksen and Kemper have developed an algorithm for the computation of $(R : \mathfrak{a})_S$. Their algorithm returns finitely many generators of $(R : \mathfrak{a})_S$ as an R-module. In case that $(R : \mathfrak{a})_S = R$, it returns the empty set. Furthermore, they showed that $(R : \mathfrak{a}^\infty)_S = R$ if and only if $(R : \mathfrak{a})_S = R$. This leads to an algorithm for the computation of $(R : \mathfrak{a}^\infty)_S$:

> First, output generators of $(R : \mathfrak{a})_S$, then – if $(R : \mathfrak{a})_S \neq R$ – replace R by the algebra generated by R and the generators of $(R : \mathfrak{a})_S$ and start again.

In fact, this algorithm terminates if and only if $(R : \mathfrak{a}^\infty)_S$ is finitely generated as a K-algebra. Otherwise, the output will be an infinite sequence of generators. For details, see [DK08], Algorithms 2.6 & 2.7. ♢

As before, let $x_1, \ldots, x_n$ and $t_1, \ldots, t_m$ be indeterminates over K. For the algorithms, let the input data be given as in the following convention.

Convention 3.19.
Let G be a linear algebraic group, X be an irreducible affine variety and let G act regularly on X. We assume that these data are given as follows:

(1) Generators of the radical ideal $J \trianglelefteq K[t_1, \ldots, t_m]$ defining the linear algebraic group G as an affine variety in K^m.

(2) Generators $p_1, \ldots, p_r$ of the prime ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ such that $X = \mathrm{Var}(I) \subset K^n$.

(3) Polynomials $N_1, \ldots, N_n \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ such that

$$\mu(\sigma, p) = (N_1(\sigma, p), \ldots, N_n(\sigma, p)) \text{ for all } \sigma \in G, p \in X,$$

where $\mu : G \times X \longrightarrow X$ is the morphism corresponding to the action of G on X.

As mentioned before, the following algorithm does not only work for the important case of unipotent groups. Actually, it works in every case where the equality of the field of fractions of the invariant ring and the invariant field holds. In the previous section this special property has been proved for various cases, see Propositions 3.4, 3.6, 3.11 & 3.16. Note that – following the approach of van den Essen, Derksen and Kemper – the algorithm does not compute the invariant ring itself but a certain localization thereof. With generators of this localization in hand it is not a hard task to compute a (possibly infinite) sequence of generators of $K[X]^G$, as we will see in Remark 3.21(b).

Algorithm 3.20. (Computing invariants of certain group actions)

Input: A linear algebraic group G, an irreducible affine variety X and an action μ of G on X according to Convention 3.19 such that $\mathrm{Quot}(K[X]^G) = K(X)^G$.

Output: Polynomials $f, f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ with $f \notin I$ such that

$$K[X]^G_{f+I} = K[f_1 + I, \ldots, f_s + I, f + I, 1/(f + I)].$$

(1) Let $Z_1, \ldots, Z_n$ be indeterminates over $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ and let α be the composition of the natural homomorphisms

$$\begin{aligned}\alpha : K[t_1, \ldots, t_m, x_1, \ldots, x_n] &\longrightarrow \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m] \\ &\longrightarrow \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m, Z_1, \ldots, Z_n].\end{aligned}$$

Set

$$\begin{aligned}D_0 := \big(J, Z_1 - \alpha(N_1), \ldots, Z_n - \alpha(N_n)\big) \\ \trianglelefteq \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m, Z_1, \ldots, Z_n].\end{aligned}$$

(See Remark 3.21(c) for an explanation of this notation)

(2) Compute the elimination ideal

$$D := D_0 \cap \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[Z_1, \ldots, Z_n].$$

(For details, see Remark 3.21(d))

(3) Let $\mathcal{G}$ be the reduced Gröbner basis of D with respect to an arbitrary monomial

order on $Z_1, \ldots, Z_n$ and let

$$\frac{n_1 + I}{d_1 + I}, \ldots, \frac{n_s + I}{d_s + I}$$

with $n_1, \ldots, n_s, d_1, \ldots, d_s \in K[x_1, \ldots, x_n]$ be the non-zero coefficients of the elements of $\mathcal{G}$.

(4) For $i = 1, \ldots, s$:
Set

$$L_i := ((d_i)_{K[x_1,\ldots,x_n]} + I) : (n_i)_{K[x_1,\ldots,x_n]} \trianglelefteq K[x_1, \ldots, x_n]$$

and choose $h_i \in L_i$ with $h_i + I \in (L_i/I)^G \setminus \{0\}$.
(See Remark 3.21(d) and the discussion after the following proof of correctness for methods of how this can be done)

(5) Set $f := \prod_{i=1}^{s} h_i$.

(6) For $i = 1, \ldots, s$:
Compute $f_i \in K[x_1, \ldots, x_n]$ such that

$$(f + I) \cdot (n_i + I) = (f_i + I) \cdot (d_i + I). \tag{3.2}$$

(For details, see Remark 3.21(f))

(7) Return $f, f_1, \ldots, f_s$.

Remarks 3.21. (a) Note that an algorithm with a similar functionality as Algorithm 3.20 has been developed by Kemper and Derksen. For details, see [DK08].

(b) For the actual computation of generators of $K[X]^G$ observe that the invariant ring is given by

$$K[X]^G = K[X]^G_{f+I} \cap K[X] = K[f_1 + I, \ldots, f_s + I, f + I, 1/(f + I)] \cap K[X].$$

This intersection in turn is equal to $(K[f_1 + I, \ldots, f_s + I, f + I] : (f + I)^\infty)_{K[X]}$. As mentioned above, this colon algebra can be computed by [DK08], Algorithm 2.7. Note that this computation terminates if and only if the invariant ring is finitely generated. Otherwise, it returns an infinite sequence of generators of $K[X]^G$.

(c) In step (1) we have loosely written J in the list of generators of the ideal D_0. It should be clear what is meant here. It stands for the set J regarded as a subset of $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m, Z_1, \ldots, Z_n]$ via the natural embedding $K[t_1, \ldots, t_m] \longrightarrow \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m, Z_1, \ldots, Z_n]$.

(d) Algorithms for the computation of elimination and colon ideals can be found in Section 1.3 and [BW93], Chapter 6, Section 2. For computations in polynomial rings over fields of rational functions, see Section 1.3.

(e) It can be seen without difficulties that for $i = 1, \ldots, s$ the ideal L_i of step (4) is the preimage of the ideal $\mathfrak{a}((n_i + I)/(d_i + I)) = (d_i + I)_{K[X]} : (n_i + I)_{K[X]}$ under the natural epimorphism $K[x_1, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]/I$. As we will see in the following proof, the rational function $(n_i + I)/d_i + I)$ is an invariant. By the assumption $\mathrm{Quot}(K[X]^G) = K(X)^G$, it follows that the ideal $\mathfrak{a}((n_i + I)/(d_i + I))$ contains a non-zero invariant. Therefore, step (4) of the algorithm makes sense and the h_i with the required properties exist.

(f) Step (6) of the algorithm can be computed for example with the Extended Buchberger Algorithm (cf. [BW93], Chapter 5, Section 5.6). To be more precise, the latter algorithm can be used to compute coordinates of the ideal membership

$$f \cdot n_i \in (d_i, p_1, \ldots, p_r)_{K[x_1,\ldots,x_n]}$$

where – according to Convention 3.19 – the polynomials $p_1, \ldots, p_r$ are generators of the ideal I. Then f_i is given by the coordinate correspoding to d_i. Note that $f \in \bigcap_{i=1}^{s} L_i$ by steps (4) and (5). Therefore, polynomials f_i with the required properties exist.

(g) In the first two steps of the algorithm, the Derksen ideal, as Kemper calls it in [Kem07], is computed. For computational purposes this ideal – or variants thereof – seems to occur quite frequently (see for example [Der99], [MQB99], [Kem07]). In [MQB99], Müller-Quade and Beth showed that it can be used to compute invariant fields of algebraic groups acting linearly on vector spaces. Later Kemper generalized their work to arbitrary algebraic groups acting rationally on algebraic varieties.
The following proof is self-contained in the sense that it does not assume any knowledge about the theory which has been developed in [MQB99] and [Kem07]. ♢

Proof of Correctness. We have to prove that

$$K[X]^G_{f+I} = K[f_1 + I, \ldots, f_s + I, f + I, 1/(f + I)]. \tag{3.3}$$

For the right hand side to be contained in the left hand side, it is enough to show that $f + I, f_1 + I, \ldots, f_s + I$ are invariants. For $f + I$ this is clear by definition. The invariance of $f_1 + I, \ldots, f_s + I$ requires a bit more work.
Observe that the action of G on $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ can be extended to an action on $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)[Z_1, \ldots, Z_n]$ where G acts on $Z_1, \ldots, Z_n$ trivially. We claim that the ideal D is G-stable under this action. To see this, we prove that

$$D = D' := \bigcap_{\sigma \in G} (Z_1 - \sigma(x_1 + I), \ldots, Z_n - \sigma(x_n + I)). \tag{3.4}$$

As a preliminary consideration, we show that $\sigma^{-1}(x_i + I) = \alpha(N_i)(\sigma)$ for all $i = 1, \ldots, n$

and all $\sigma \in G$. Let $i \in \{1, \dots, n\}$. Then

$$\begin{aligned}\sigma^{-1}(x_i + I)(p) &= (x_i + I)(\sigma(p)) = (x_i + I)(N_1(\sigma, p), \dots, N_n(\sigma, p)) \\ &= N_i(\sigma, p)\end{aligned}$$

for all $\sigma \in G$ and all $p \in X$. It follows that

$$\sigma^{-1}(x_i + I) = \alpha(N_i)(\sigma) \quad \text{for all } \sigma \in G.$$

For the proof of equality (3.4), let $h \in D$. By definition of D, there exist $t \in \mathbb{N}$, $b_1, \dots, b_t,\ c_1, \dots, c_n \in \mathrm{Quot}(K[x_1, \dots, x_n]/I)[t_1, \dots, t_m, Z_1, \dots, Z_n]$ and $j_1, \dots, j_t \in J$ such that

$$h = \sum_{i=1}^{t} b_i \cdot j_i + \sum_{i=1}^{n} c_i \cdot (Z_i - \alpha(N_i)).$$

Note that h does not contain any $t_1, \dots, t_m$-variables. We may thus replace $t_1, \dots, t_m$ on the right hand side of the above equation by arbitrary values. Let $\sigma = (\zeta_1, \dots, \zeta_m) \in G$. Substituting $t_1 = \zeta_1, \dots, t_m = \zeta_m$, it then follows that

$$h = \sum_{i=1}^{n} \tilde{c}_i \cdot (Z_i - \alpha(N_i)(\sigma))$$

for some $\tilde{c}_1, \dots \tilde{c}_n \in \mathrm{Quot}(K[x_1, \dots, x_n]/I)[Z_1, \dots, Z_n]$ which implies that

$$h \in (Z_1 - \alpha(N_1)(\sigma), \dots, Z_n - \alpha(N_n)(\sigma)) = (Z_1 - \sigma^{-1}(x_1 + I), \dots, Z_n - \sigma^{-1}(x_n + I)).$$

Since $\sigma \in G$ was chosen arbitrarily, it follows that $h \in D'$, as desired.
For the reverse inclusion, let $h \in D'$. Then

$$\begin{aligned}h &- h(\alpha(N_1), \dots, \alpha(N_n)) \\ &= h(Z_1 - \alpha(N_1) + \alpha(N_1), \dots, Z_n - \alpha(N_n) + \alpha(N_n)) - h(\alpha(N_1), \dots, \alpha(N_n)) \\ &= h(\alpha(N_1), \dots, \alpha(N_n)) + \left(\sum_{i=1}^{n} d_i \cdot (Z_i - \alpha(N_i)) \right) - h(\alpha(N_1), \dots, \alpha(N_n))\end{aligned}$$

for some $d_1, \dots, d_n \in \mathrm{Quot}(K[x_1, \dots, x_n]/I)[t_1, \dots, t_m, Z_1, \dots, Z_n]$. But this means that

$$h - h(\alpha(N_1), \dots, \alpha(N_n)) \in (Z_1 - \alpha(N_1), \dots, Z_n - \alpha(N_n)) \subset D_0. \tag{3.5}$$

On the other hand, since h is contained in D', it follows that

$$h(\alpha(N_1)(\sigma), \dots, \alpha(N_n)(\sigma)) = h(\sigma^{-1}(x_1 + I), \dots, \sigma^{-1}(x_n + I)) = 0 \tag{3.6}$$

for all $\sigma \in G$. The polynomial $h(\alpha(N_1), \dots, \alpha(N_n))$ can be written as

$$h(\alpha(N_1), \dots, \alpha(N_n)) = \sum_{i=1}^{t} g_j \cdot a_j$$

for some $t \in \mathbb{N}$, $a_1, \ldots, a_t \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ and $g_1, \ldots, g_t \in K[t_1, \ldots, t_m]$. We may assume that $a_1, \ldots, a_t$ are linearly independent over K. By equation (3.6), we have

$$0 = \sum_{i=1}^{t} g_i(\sigma) \cdot a_i$$

and by the linear independence of $a_1, \ldots, a_t$, this means that $g_1(\sigma) = \ldots = g_t(\sigma) = 0$. Since this is true for all $\sigma \in G$, it follows that $g_i \in J$. This in turn implies that $h(\alpha(N_1), \ldots, \alpha(N_n)) \in D_0$. Combining this with (3.5) shows that $h \in D$, as desired.

We can now show that $f_1 + I, \ldots, f_s + I$ are invariant under the action of G. The G-stability of D together with the uniqueness of the reduced Gröbner basis implies that $\mathcal{G}$ is G-stable, too. By definition, the leading monomials of a reduced Gröbner basis are pairwise distinct, hence it follows that $\mathcal{G}$ consists of G-invariant polynomials. Since G acts trivially on $Z_1, \ldots, Z_n$, this in turn implies that

$$\frac{n_1 + I}{d_1 + I}, \ldots, \frac{n_s + I}{d_s + I} \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)^G.$$

Let $i \in \{1, \ldots, s\}$. Equation (3.2) yields

$$\frac{f_i + I}{f + I} = \frac{n_i + I}{d_i + I} \tag{3.7}$$

and since both $(n_i + I)/(d_i + I) \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)^G$ and $f + I \in (K[x_1, \ldots, x_n]/I)^G$ are invariants, it follows that $f_i + I$ is invariant, too. To sum up, we have shown that the right hand side of equation (3.3) is contained in the left hand side.
For the reverse inclusion, let $g + I \in K[X]^G$. We will show that if we regard $g + I = g(x_1 + I, \ldots, x_n + I)$ as an element of $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)[Z_1, \ldots, Z_n]$, then

$$g(Z_1, \ldots, Z_n) - g(x_1 + I, \ldots, x_n + I) \in D. \tag{3.8}$$

Assume for a moment that this is true. Then $g(Z_1, \ldots, Z_n) - g(x_1 + I, \ldots, x_n + I)$ reduces to zero with respect to an arbitrary Gröbner basis of D. In particular, this holds for $\mathcal{G}$ which is computed in step (3). Because of the $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)$-linearity of the normal form operator $\mathrm{NF}_{\mathcal{G}}$ (cf. Remark 1.44), it follows

$$\begin{aligned} &\mathrm{NF}_{\mathcal{G}}(g(Z_1, \ldots, Z_n) - g(x_1 + I, \ldots, x_n + I)) \\ &\quad = \mathrm{NF}_{\mathcal{G}}(g(Z_1, \ldots, Z_n)) - \mathrm{NF}_{\mathcal{G}}(g(x_1 + I, \ldots, x_n + I)) \\ &\quad = \mathrm{NF}_{\mathcal{G}}(g(Z_1, \ldots, Z_n)) - g(x_1 + I, \ldots, x_n + I) = 0 \end{aligned}$$

and hence

$$\mathrm{NF}_{\mathcal{G}}(g(Z_1, \ldots, Z_n)) = g(x_1 + I, \ldots, x_n + I). \tag{3.9}$$

By equation (3.7), we have $\mathcal{G} \subset (K[f_1 + I, \ldots, f_s + I, f + I]_{f+I})[Z_1, \ldots, Z_n]$. Together

with Remark 1.44 this implies

$$\begin{aligned} g(x_1+I,\ldots,x_n+I) &= \mathrm{NF}_{\mathcal{G}}(g(Z_1,\ldots,Z_n)) \\ &\in (K[f_1+I,\ldots,f_s+I,f+I]_{f+I})[Z_1,\ldots,Z_n], \end{aligned}$$

which finally proves (3.3).
It remains to show the validity of (3.8). Let $\sigma \in G$. By the invariance of $g+I$, we have

$$\begin{aligned} &g(Z_1,\ldots,Z_n) - g(x_1+I,\ldots,x_n+I) \\ &\quad= g(Z_1-\sigma(x_1+I)+\sigma(x_1+I),\ldots,Z_n-\sigma(x_n+I)+\sigma(x_n+I)) \\ &\qquad\quad - g(x_1+I,\ldots,x_n+I) \\ &\quad= g(\sigma(x_1+I),\ldots,\sigma(x_n+I)) - g(x_1+I,\ldots,x_n+I) + \sum_{i=1}^{n} c_i\cdot(Z_i-\sigma(x_i+I)) \\ &\quad= \sigma(g(x_1+I,\ldots,x_n+I)) - g(x_1+I,\ldots,x_n+I) + \sum_{i=1}^{n} c_i\cdot(Z_i-\sigma(x_i+I)) \\ &\quad= \sum_{i=1}^{n} c_i\cdot(Z_i-\sigma(x_i+I)), \end{aligned}$$

for some $c_1,\ldots,c_n \in \mathrm{Quot}(K[x_1,\ldots,x_n]/I)[Z_1,\ldots,Z_n]$. Since σ was chosen arbitrarily, it follows from equation (3.4) that $g(Z_1,\ldots,Z_n) - g(x_1+I,\ldots,x_n+I) \in D$, as desired. ∎

As promised above, we give some details about how step (4) of the previous algorithm can be computed. So let the linear algebraic group G act regularly on X and assume that $L \trianglelefteq K[X]$ is a G-stable ideal with $L^G \neq \{0\}$. Our aim is to find a non-zero invariant $f \in L^G \setminus \{0\}$. A possible way of doing this could be as follows.
Let $(f_i)_{i\in\mathbb{N}}$ be a sequence such that $K[X]^G = K[f_i;\ i \in \mathbb{N}]$. Since we have assumed $L^G \neq \{0\}$, there is an index i_0 such that $L \cap K[f_1,\ldots,f_{i_0}] \neq \{0\}$. Hence $f \in L^G \setminus \{0\}$ can be found algorithmically by simply computing $L\cap K[f_1], L\cap K[f_1,f_2],\ldots$ until the intersection contains a non-zero element. Some hints about the computation of this intersection are given in Remark 4.35(b) below.
But how can such a sequence $(f_i)_{i\in\mathbb{N}}$ be constructed? If

$$K[X] = \bigoplus_{d\in\mathbb{N}_0} K[X]_d$$

is a graded ring and the action of G on $K[X]$ preserves this grading, then the invariant ring $K[X]^G$ is graded, too, and a successive computation of the K-bases of $K[X]_0^G, K[X]_1^G,\ldots$ yields a sequence with the desired properties. Note that the bases of $K[X]_d^G$ can be obtained for example by simply writing down the invariance conditions for the elements of $K[X]_d$ as a system of linear equations and solving this.
For arbitrary $K[X]$, we can replace the grading of $K[X]$ by an ascending chain of finite

dimensional subspaces

$$K := K[X]_0 \subset K[X]_1 \subset K[X]_2 \subset \dots$$

with the property that $K[X] = \bigcup_{d\in\mathbb{N}_0} K[X]_d$. Similarly to the graded case, bases of $K[X]_0^G, K[X]_1^G, \dots$ (as K-vector spaces) can then be computed, thereby constructing the desired sequence $(f_i)_{i\in\mathbb{N}}$.

Another, slightly different approach is realized in the following algorithm. In fact, it does not compute a chain of subspaces of $K[X]$, but an ascending chain of subspaces of the ideal L which then provides – similarly to the above – a way of systematically searching for invariants.

Algorithm 3.22. (Computing step (4) of Algorithm 3.20)

Input: A linear algebraic group G, an irreducible affine variety X, an action μ of G on X according to Convention 3.19 and polynomials $q_1, \dots, q_t \in K[x_1, \dots, x_n]$ such that the ideal $L := (q_1 + I, \dots, q_t + I) \trianglelefteq K[x_1, \dots, x_n]/I$ contains a non-zero invariant.

Output: A polynomial $f \in K[x_1, \dots, x_n]$ such that $f + I \in L^G \setminus \{0\}$.

(1) Compute a Gröbner basis $\mathcal{M}$ of the ideal $J \trianglelefteq K[t_1, \dots, t_m]$ with respect to an arbitrary monomial order $\leq$ on $t_1, \dots, t_m$.

(2) Compute a Gröbner basis $\mathcal{N}$ of the ideal $I \trianglelefteq K[x_1, \dots, x_n]$ with respect to an arbitrary monomial order $\leq'$ on $x_1, \dots, x_n$.

(3) Set $B := \{q_1, \dots, q_t\}$.

(4) Choose a maximal linearly independent subset B' of $\{b + I;\ b \in B\}$, say $B' = \{b'_1 + I, \dots, b'_{t'} + I\}$ where $t' \in \mathbb{N}$ and $b'_1, \dots, b'_{t'} \in K[x_1, \dots, x_n]$. Set $B := \{b'_1, \dots, b'_{t'}\}$. (For details about how basic linear algebra can be done within the residue class ring $K[x_1, \dots, x_n]/I$, see Remark 2.4(b))

(5) Check if there is a non-zero solution[†] $(\alpha_b;\ b \in B) \in K^{|B|}$ of the linear equation

$$\sum_{b\in B} \alpha_b \operatorname{NF}_{\mathcal{M}\cup\mathcal{N}}(b(N_1, \dots, N_n) - b(x_1, \dots, x_n)) = 0.$$

(For details, see Remark 3.23)
If this is the case, set

$$f := \sum_{b\in B} \alpha_b b$$

and return f.

[†]We write $|B|$ for the number of elements of B and $K^{|B|}$ for a tuple of elements of K of length $|B|$.

(6) Set

$$B := B \cup \bigcup_{b \in B} \{x_1 b, \ldots, x_n b\}.$$

and go back to step (4).

Remark 3.23. Note that in the linear equation of step (5) both $b(N_1, \ldots, N_n)$ and $b(x_1, \ldots, x_n)$ for $b \in B$ are regarded as elements of $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. From Buchberger's First Criterion (see [BW93], Chapter 5, Lemma 5.66) it follows that the set $\mathcal{M} \cup \mathcal{N}$ is a Gröbner basis of $(I, J) \trianglelefteq K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ with respect to the block order on the monomials in $t_1, \ldots, t_m, x_1, \ldots, x_n$ defined by $\leq$ (first block) and $\leq'$ (second block) (for the definition of block order, see e. g. [BW93], Chapter 4). Because of this it is clear what is meant by $\mathrm{NF}_{\mathcal{M} \cup \mathcal{N}}$. ♢

Proof of Correctness. We claim that $f + I \in K[x_1, \ldots, x_n]/I$ is invariant under G if and only if

$$\mathrm{NF}_{\mathcal{M} \cup \mathcal{N}}(f(N_1, \ldots, N_n) - f(x_1, \ldots, x_n)) = 0. \tag{3.10}$$

Assume first that $f + I$ is invariant. Then

$$\begin{aligned} f(N_1(\sigma, p), \ldots, N_n(\sigma, p)) - f(p) &= f(\sigma(p)) - f(p) \\ &= \sigma^{-1}(f + I)(p) - (f + I)(p) \\ &= 0 \qquad \text{for all } \sigma \in G, p \in X. \end{aligned}$$

Since the vanishing ideal of $G \times X$ is given by $(I, J)_{K[t_1, \ldots, t_m, x_1, \ldots, x_n]}$ (see for example [Eis95], Chapter 13, Exercise 13.13), this shows that $f(N_1, \ldots, N_n) - f(x_1, \ldots, x_n) \in (I, J)_{K[t_1, \ldots, t_m, x_1, \ldots, x_n]}$. Therefore, $f(N_1, \ldots, N_n) - f(x_1, \ldots, x_n)$ reduces to 0 with respect to $\mathcal{M} \cup \mathcal{N}$, the latter being a Gröbner basis of $(I, J)_{K[t_1, \ldots, t_m, x_1, \ldots, x_n]}$ (cf. Remark 3.23). For the reverse conclusion, let $f \in K[x_1, \ldots, x_n]$ such that

$$\mathrm{NF}_{\mathcal{M} \cup \mathcal{N}}(f(N_1, \ldots, N_n) - f(x_1, \ldots, x_n)) = 0.$$

We have to show that $f + I \in K[X]$ is an invariant. Clearly, $f(N_1, \ldots, N_n) - f(x_1, \ldots, x_n)$ is contained in the ideal $(I, J)_{K[t_1, \ldots, t_m, x_1, \ldots, x_n]}$. This implies that

$$\begin{aligned} \sigma(f + I)(p) - (f + I)(p) &= f(\sigma^{-1}(p)) - f(p) \\ &= f(N_1(\sigma^{-1}, p), \ldots, N_n(\sigma^{-1}, p)) - f(p) \\ &= 0 \qquad \text{for all } \sigma \in G, p \in X. \end{aligned}$$

But this means that $f + I = \sigma(f + I)$. Since this is true for all $\sigma \in G$, it follows that $f + I \in K[X]^G$, as claimed.

The heart of the algorithm is the loop comprising steps (4)-(6). Let B_j denote the set

B in the jth iteration of step (5). It can be shown with an easy induction that

$$\langle b+I;\ b\in B_j\rangle_K = L_j := \left\{ \sum_{i=1}^{t} a_i q_i + I;\ a_i \in K[x_1,\ldots,x_n] \text{ with } \deg a_i \leq j-1 \right\},$$

where $\langle b+I;\ b\in B_j\rangle_K$ stands for the K-linear span of the elements $b+I,\ b\in B_j$. By (3.10) and the linear independence of $(b+I;\ b\in B_j)$, it follows that

$$\begin{aligned} L_j^G \neq \{0\} \Longleftrightarrow \exists\, (\alpha_b \in K;\ b\in B_j) \neq 0 \text{ such that} \\ \sum_{b\in B_j} \alpha_b \,\mathrm{NF}_{\mathcal{M}\cup\mathcal{N}}(b(N_1,\ldots,N_n) - b(x_1,\ldots,x_n)) = 0. \end{aligned}$$

Therefore, if $L_j^G \neq \{0\}$, then non-trivial coordinates $(\alpha_b \in K;\ b\in B_j)$ satisfying the linear equation of step (5) exist. In this case, the algorithm returns $f := \sum_{b\in B_j} \alpha_b b$ with $f+I \in L_j^G \setminus \{0\} \subset L^G \setminus \{0\}$, as desired.
Finally, by definition of L_j, it follows that $L = \bigcup_{j\in\mathbb{N}} L_j$ and since $L^G \neq \{0\}$, there is an index j with $L_j^G \neq \{0\}$. Hence the algorithm terminates after a finite number of steps. ∎

For the special and most important case that G is a unipotent group this algorithm can be simplified as follows. Note that in step (3) of the following algorithm we need to compute the G-closure of a vector space. An explicit method of how this can be done is given below.

Algorithm 3.24. (Computing step (4) of Algorithm 3.20 if G is unipotent)

Input: A unipotent linear algebraic group G, an irreducible affine variety X, an action μ of G on X according to Convention 3.19 and polynomials $q_1,\ldots,q_t \in K[x_1,\ldots,x_n]$ such that $L := (q_1+I,\ldots,q_t+I) \trianglelefteq K[x_1,\ldots,x_n]/I$ is a non-zero G-stable ideal.

Output: A polynomial $f \in K[x_1,\ldots,x_n]$ such that $f+I \in L^G \setminus \{0\}$.

(1) Compute a Gröbner basis $\mathcal{M}$ of the ideal $J \trianglelefteq K[t_1,\ldots,t_m]$ with respect to an arbitrary monomial order $\leq$ on $t_1,\ldots,t_m$.

(2) Compute a Gröbner basis $\mathcal{N}$ of the ideal $I \trianglelefteq K[x_1,\ldots,x_n]$ with respect to an arbitrary monomial order $\leq'$ on $x_1,\ldots,x_n$.

(3) We may assume that $q_1+I \neq 0$. Use Algorithm 3.25 below to compute a basis $h_1+I,\ldots,h_s+I$ of a G-module $V \subset L$ which contains q_1+I.

(4) Set $B := \{h_1,\ldots,h_s\}$.

(5) Compute a non-zero solution $(\alpha_b;\ b \in B) \in K^{|B|}$ of the linear equation

$$\sum_{b \in B} \alpha_b \operatorname{NF}_{\mathcal{M} \cup \mathcal{N}}(b(N_1, \ldots, N_n) - b(x_1, \ldots, x_n)) = 0,$$

set

$$f := \sum_{b \in B} \alpha_b b.$$

and return f.

Proof of Correctness. By the correctness of Algorithm 3.25, the vector space $V = \langle b + I;\ b \in B \rangle_K$ is G-stable and contains $q_1 + I$. Moreover, it is minimal with this property in the sense that V is contained in any G-stable vector space containing $q_1 + I$ (see Remark 3.26). Since L is a G-stable ideal, this implies that $V \subset L$. From the unipotency of G it follows that $V^G \neq \{0\}$ (cf. [Hum75], Theorem 17.5). Equivalently, this means that there exist coordinates $(\alpha_b;\ b \in B) \neq 0$ not all zero such that $\sum_{b \in B} \alpha_b (b + I)$ is an invariant. By equation (3.10) of the preceding proof, this in turn is equivalent to the existence of $\alpha_1, \ldots, \alpha_{|B|} \in K$ not all zero such that

$$\sum_{b \in B} \alpha_b \operatorname{NF}_{\mathcal{M} \cup \mathcal{N}}(b(N_1, \ldots, N_n) - b(x_1, \ldots, x_n)) = 0.$$

This shows the correctness of the algorithm, since scalars $\alpha_b,\ b \in B$ with exactly this property are computed in step (5). ∎

Before we demonstrate an application of Algorithm 3.20 to a concrete example, we give a method for computing the G-closure of a vector space contained in the G-algebra $K[X]$ (which is needed for step (3) of the previous algorithm). Although a very similar method can be found in [DK08], we include an explicit algorithm in this section for the benefit of being self-contained. Moreover, the situation examined here is slightly different from that of Derksen and Kemper.

Algorithm 3.25. (Computing the G-closure)

Input: A linear algebraic group G, an affine variety X, an action μ of G on X according to Convention 3.19 and polynomials $q_1, \ldots, q_t \in K[x_1, \ldots, x_n]$.

Output: A finite subset $B \subset K[x_1, \ldots, x_n]$ of polynomials such that $(b + I;\ b \in B)$ is a basis of a G-module $V \subset K[x_1, \ldots, x_n]/I$ with $q_1 + I, \ldots, q_t + I \in V$.

(1) Compute a Gröbner basis $\mathcal{M}$ of the ideal $J \trianglelefteq K[t_1, \ldots, t_m]$ with respect to an arbitrary monomial order $\leq$ on $t_1, \ldots, t_m$.

(2) Compute a Gröbner basis $\mathcal{N}$ of the ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ with respect to an arbitrary monomial order $\leq'$ on $x_1, \ldots, x_n$.

(3) Set $H_i := \mathrm{NF}_{\mathcal{M}\cup\mathcal{N}}(q_i(N_1, \ldots, N_n))$ for $i = 1, \ldots, t$.

(4) Let $C \subset K[x_1, \ldots, x_n]$ be the set of all coefficients occurring in the H_i considered as polynomials in $t_1, \ldots, t_m$.

(5) Return a maximal K-linearly independent subset B of C.

Remark. This algorithm makes the proof of Proposition 1.31(a) constructive. ♢

Proof of Correctness. Let $i \in \{1, \ldots, t\}$. Since a polynomial in $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ regarded as a function on $G \times X$ does not change when it is replaced by its normal form with respect to $\mathcal{M} \cup \mathcal{N}$, it follows that

$$\begin{aligned} H_i(\sigma, p) &= q_i(N_1(\sigma, p), \ldots, N_n(\sigma, p)) \\ &= q_i(\sigma(p)) = \sigma^{-1}(q_i + I)(p) \qquad \text{for all } \sigma \in G, p \in X. \end{aligned} \tag{3.11}$$

The polynomial H_i can be written as $H_i = \sum_{j=1}^{s} g_j \cdot a_j$ where $g_1, \ldots, g_s$ are pairwise distinct monomials in $t_1, \ldots, t_m$ and $a_1, \ldots, a_s \in K[x_1, \ldots, x_n]$. We claim that

$$\widetilde{V} := \langle a_1 + I, \ldots, a_s + I \rangle_K \subset K[x_1, \ldots, x_n]/I$$

is a G-module containing $q_i + I$. Let $\tau \in G$. We have to show that $\tau(a_i + I) \in \widetilde{V}$, again (cf. Remark 1.32). By construction, the monomials $g_1, \ldots, g_s$ are pairwise distinct monomials which are in normal form with respect to $\mathcal{M}$. This implies that $g_1 + J, \ldots, g_s + J$ are linearly independent as regular functions on G (see [BW93], Chapter 6, Proposition 6.52). Hence there exist $\sigma_1, \ldots, \sigma_s \in G$ such that $(g_j(\sigma_k))_{j,k=1,\ldots,s} \in K^{s\times s}$ is regular. By equation (3.11), it follows that

$$\begin{aligned} (\tau(a_1 + I), \ldots, \tau(a_s + I)) \cdot (g_j(\sigma_k))_{j,k=1,\ldots,s} &= ((\tau\sigma_1^{-1})(q_i + I), \ldots, (\tau\sigma_s^{-1})(q_i + I)) \\ &= \left(\sum_{j=1}^{s} g_j(\sigma_1\tau^{-1}) \cdot a_j + I, \ldots, \sum_{j=1}^{s} g_j(\sigma_s\tau^{-1}) \cdot a_j + I \right) \in \widetilde{V}^s \end{aligned}$$

and thus

$$\begin{aligned} &(\tau(a_1 + I), \ldots, \tau(a_s + I)) \\ &\quad = (\tau(a_1 + I), \ldots, \tau(a_s + I)) \cdot (g_j(\sigma_k))_{j,k=1,\ldots,s} \cdot (g_j(\sigma_k))^{-1}_{j,k=1,\ldots,s} \in \widetilde{V}^s. \end{aligned}$$

But this means that $\tau(a_1 + I), \ldots, \tau(a_s + I) \in \widetilde{V}$, as desired.
Moreover, since $q_i + I = \sum_{j=1}^{s} g_j(1_G) \cdot (a_j + I)$, it follows that $q_i + I \in \widetilde{V}$ and so $\widetilde{V}$ is a G-module containing $q_i + I$, indeed.
Note also that $\widetilde{V}$ is the smallest G-module containing $q_i + I$ in the sense that $\widetilde{V}$ is contained in every G-module $\widetilde{V}'$ with $q_i + I \in \widetilde{V}'$. This follows by setting $\tau = 1_G$ in the equations a few lines above.
Applying these arguments to $i = 1, \ldots, t$ shows that $(b + I;\ b \in B)$ is a basis of a G-

module $V \subset K[X]$ containing $q_1 + I, \ldots, q_t + I$, as claimed (for the linear independence of $(b + I;\ b \in B)$, see Remark 2.4(b)). ∎

Remark 3.26. By the previous proof, the G-module V which is computed by Algorithm 3.25 is minimal in the sense that V is contained in every other G-module V' with $q_1 + I, \ldots, q_t + I \in V'$. ♢

We close this section with an example of the application of Algorithm 3.20.

Example 3.27. Let $K = \overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. The unipotent group

$$G := \left\{ \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} ;\ \alpha, \beta, \gamma \in K \right\}$$

of upper triangular matrices with 1's on the diagonal acts on the vector space $X := K^3$ via left multiplication, i. e.

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} := \begin{pmatrix} \xi_1 + \alpha\xi_2 + \beta\xi_3 \\ \xi_2 + \gamma\xi_3 \\ \xi_3 \end{pmatrix}$$

$$\text{for all } \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \in G, \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} \in X.$$

Even though it might be obvious that the invariant ring is generated by the third coordinate function of X, we want to demonstrate step-by-step how Algorithm 3.20 can be used for the computation of $K[X]^G$.
Before we can start, we have to specify the input data according to Convention 3.19. The unipotent group G can be realized as $G = \mathrm{Var}(J) \subset K^3$ with $J := (0) \trianglelefteq K[t_1, t_2, t_3]$. Note that t_1, t_2 and t_3 correspond to the entries α, β and γ above.
Similarly, let $X = \mathrm{Var}(I) \subset K^3$ with $I := (0) \trianglelefteq K[x_1, x_2, x_3]$. The action of G on X can then be described by $\mu = (N_1, N_2, N_3)$ with

$$N_1 = x_1 + t_1x_2 + t_2x_3,\ N_2 = x_2 + t_3x_3,\ N_3 = x_3.$$

By step (1) of the algorithm, the ideal D_0 is defined as

$$D_0 := \big(Z_1 - (x_1 + t_1x_2 + t_2x_3), Z_2 - (x_2 + t_3x_3), Z_3 - x_3\big) \trianglelefteq \mathrm{Quot}(K[x_1, x_2, x_3])[t_1, t_2, t_3, Z_1, Z_2, Z_3].$$

Note that we do not distinguish notationally between elements of the polynomial ring $K[x_1, x_2, x_3]$ and the isomorphic ring $K[x_1, x_2, x_3]/I$. By Buchberger's First Criterion (see [BW93], Chapter 5, Lemma 5.66), this generating set of D_0 is a Gröbner basis of D_0 with respect to the lexicographic order $Z_3 \leq Z_2 \leq Z_1 \leq t_3 \leq t_2 \leq t_1$. It follows by

Theorem 1.46 that a reduced Gröbner basis $\mathcal{G}$ of the elimination ideal D of step (2) (with respect to the induced lexicographic order $Z_3 \leq Z_2 \leq Z_1$) is given by

$$\mathcal{G} = \{Z_3 - x_3\}.$$

Obviously, 1 and x_3 are the only coefficients of the single polynomial in $\mathcal{G}$. Applying step (4) to these data yields $h_1 := 1$ and $h_2 := 1$. This leads to $f := 1$ and $f_1 := 1$, $f_2 := x_3$. But this means that $K[X]^G = K[x_3]$, as predicted. ◁

3.2.1 Some remarks about the running time of Algorithm 3.20

We have used a preliminary implementation of Algorithm 3.20 to compute a series of invariant rings of unipotent groups. This implementation has been done in the computer algebra system Magma (cf. [BCP97]), some code can be found in the appendix. Note that – as the term "preliminary" suggests – the implementation is not yet comprehensive enough for everyday use. For instance, there is only a minimal amount of error processing. Apart from that there is possibly also much room for optimizations. In any case, the implementation provides an insight into the capabilities of the algorithm – i. e. whether it is able to produce new and interesting results in reasonable time or if it is merely of theoretical interest.

Most likely, the invariant rings computed in the following are already known and have been examined by others – nonetheless, as indicated above, we have calculated these invariants to get a feeling for the practicability of Algorithm 3.20.
Consider the following situation. Let $n \in \mathbb{N}$ and let K be an algebraically closed field. Furthermore, let the unipotent group $G \subset K^{n\times n}$ of upper triangular matrices with 1's on the diagonal act on the vector space $X = K^{n\times n}$ of $n \times n$-matrices via left multiplication. How does Algorithm 3.20 applied to this situation perform for different values of n?

Table 3.1 summarizes the computing time for the cases where $n \in \{1, \ldots, 7\}$ and K is one of $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}_2}$, $\overline{\mathbb{F}_3}$ or $\overline{\mathbb{F}_5}$ (as usual, the bar denotes the algebraic closure of the respective fields). All computations have been done with Magma V.2.14-17 running under Solaris 10 6/06 on a Sun Fire 880 with 8 UltraSparc-III+ processors (1.2 GHz) and 32 GB RAM. A dash in the table means that the algorithm has been aborted by the user after 24 hours of running time.

It comes as no surprise that the most time consuming steps of Algorithm 3.20 are the computation of the elimination ideal D in step (2), the computation of the product f in step (5) and the computation of $f_1, \ldots, f_s$ in step (6). For $n \leq 5$, the computation of D seems to be the dominating part, for $n \in \{6, 7\}$, the computation of $f_1, \ldots, f_s$ has turned out to be the most time consuming operation. However, this might be an implementation artefact.

n	$K = \overline{\mathbb{Q}}$	$K = \overline{\mathbb{F}_2}$	$K = \overline{\mathbb{F}_3}$	$K = \overline{\mathbb{F}_5}$
1	0.00 sec	0.01 sec	0.01 sec	0.00 sec
2	0.00 sec	0.01 sec	0.00 sec	0.01 sec
3	0.02 sec	0.13 sec	0.5 sec	0.32 sec
4	0.54 sec	0.13 sec	0.13 sec	0.13 sec
5	20.5 sec	5.91 sec	10.62 sec	10.99 sec
6	235 min	83 min	178 min	214 min
7	–	–	–	–

Table 3.1: Running times of Algorithm 3.20.

4 Computing invariants of group actions on quasi-affine varieties

In the previous chapters, we have studied invariants of algebraic groups acting on affine algebras. In the case that the affine algebra is reduced, this geometrically corresponds to algebraic groups acting on affine varieties, as we have seen in Proposition 1.29. In fact, most of the progress which has been made in computational invariant theory so far took place in this setting. In the present chapter we will investigate the more general situation where a linear algebraic group G acts on a quasi-affine variety U. Similarly to the affine case, this leads to a situation where G acts on an algebra via automorphisms. Again, we are interested in those elements of this algebra which are invariant under the action of G. One might think at first sight that the examination of such "quasi-affine invariants" is rather special. But this situation evolves naturally: Nagata proved in [Nag65] that the invariant ring of an algebraic group acting on a normal affine variety geometrically corresponds to a quasi-affine variety U in the sense that the invariant ring is isomorphic to the ring of regular functions of U. Therefore, quasi-affine varieties occur – at least implicitly – in some of the algorithms found in invariant theory today. For example, Derksen and Kemper suggested in [DK08] to compute invariant rings of arbitrary algebraic groups G acting on a factorial affine variety X by first computing the invariant ring of the unipotent radical N of G and then calculating $(K[X]^N)^{G/N} = K[X]^G$. As mentioned above, the "intermediate invariant ring" $K[X]^N$ corresponds to a quasi-affine variety U, and $(K[X]^N)^{G/N}$ is the invariant ring of the (reductive) group G/N acting on the algebra belonging to the quasi-affine variety U.
But the quasi-affine case is interesting not only as an auxiliary construction for the algorithmic solution of the affine case. It is a natural generalization and interesting for the sake of its own. A variety of publications has been made by Magid and Fauntleroy (e. g. [FM76], [FM78] and [Mag79]) in which they investigated invariants of group actions on quasi-affine varieties.
In this chapter, we develop algorithms to compute invariants of several important classes of algebraic groups acting on quasi-affine varieties. Algorithmically, this tends to be rather complicated since quite often non-finitely generated algebras occur. To deal with those, we use the framework which has been introduced by Derksen and Kemper in [DK08].
The theory of quasi-affine varieties is very similar to the affine case. Nonetheless, we start with a short survey on the concepts which are needed for the algorithms. In the literature, the facts given below are often formulated and proved for general algebraic varieties or schemes. The proofs given here are very concrete, which turns out to be helpful for the construction and the understanding of the algorithms.

Throughout this chapter, let K denote an algebraically closed field. As in the previous

chapters, $x_1, \ldots, x_n$ and $t_1, \ldots, t_m$ shall denote indeterminates over K. Unless otherwise stated, let X be an affine variety and G be a linear algebraic group. All varieties and algebraic groups are over K.

4.1 Quasi-affine varieties

Definition 4.1. *A Zariski-open subset U of an affine variety X is called a* **quasi-affine variety**. *The Zariski topology on X induces the subspace tolopogy on U, which we also refer to as the* **Zariski topology on U**.
A non-empty quasi-affine variety U is called **irreducible** *if it is irreducible as a topological space. The empty set is not considered to be irreducible.*
Let $U \subset X \subset K^n$ be embedded in the affine space K^n. A function $f : U \longrightarrow K$ is called **regular on U** *if for every $u \in U$ there exists an open neighbourhood $V \subset U$ of u and polynomials $N, D \in K[x_1, \ldots, x_n]$ such that $0 \notin D(V)$ and $f(v) = N(v)/D(v)$ for all $v \in V$. The set of regular functions on U has the structure of a K-algebra (resp. is the zero ring if $U = \emptyset$) and is denoted by $K[U]$.*
A **morphism** *between two quasi-affine varieties U' and U is a map*

$$\phi = (\phi_1, \ldots, \phi_n) : U' \longrightarrow U$$

such that all components $\phi_1, \ldots, \phi_n : U' \longrightarrow K$ of ϕ are regular functions on U'. The morphism ϕ is called an **isomorphism** *if there is a morphism $\psi : U \longrightarrow U'$ such that $\phi \circ \psi = \mathrm{id}_U$ and $\psi \circ \phi = \mathrm{id}_{U'}$. In this case, the quasi-affine varieties U and U' are said to be isomorphic.*

Remarks 4.2. (a) Every affine variety can be regarded as a quasi-affine variety. In this case, all the concepts as defined above coincide with those known from the affine case. Of course, there are quasi-affine varieties which are not affine. Nagata showed in [Nag65] that – in contrast to affine coordinate rings – the ring of regular functions of a quasi-affine variety need not be finitely generated. We will deal with a quasi-affine variety whose ring of regular functions is not finitely generated in Example 4.40 below.

(b) It can be shown that every regular function $f : U \longrightarrow K$ on the quasi-affine variety U is continuous if we regard K as an affine variety together with its Zariski topology (cf. [Har77], Chapter I, Section 3).

(c) Similarly, it can be shown that every morphism $\phi : U \longrightarrow U'$ between quasi-affine varieties U and U' is continuous (cf. [Har77], Chapter I, Section 3).

(d) Let X be an irreducible affine variety and let $U \subset X$ be a non-empty open subset, i. e. U is quasi-affine. It can be shown that $K[U]$ is a subset of $\mathrm{Quot}(K[X])$. More precisely,

$$K[U] = \bigcap_{u \in U} K[X]_{\mathfrak{m}_u},$$

where $\mathfrak{m}_u \trianglelefteq K[X]$ is the maximal ideal corresponding to the point $u \in U$ and $K[X]_{\mathfrak{m}_u}$ stands for the localization of $K[X]$ at $\mathfrak{m}_u$ (cf. [Har77], Chapter I, Section 3). ♢

In [DK08], Derksen and Kemper gave a method to compute the ring of regular functions of an irreducible quasi-affine variety $U \subset X$ where X is an irreducible affine variety. To be more explicit, assume that $X := \mathrm{Var}(I) \subset K^n$ is given by a prime ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ and let $L \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal such that $U := X \setminus \mathrm{Var}(L)$. Then they showed that

$$K[U] = (K[x_1, \ldots, x_n]/I : ((L + I)/I)^\infty)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)}. \tag{4.1}$$

For the definition of the colon notation used in this equation, see Definition 3.17. The expression (4.1) can be handled algorithmically, e. g. if $K[U]$ is known to be finitely generated, then $K[U]$ can be computed in finitely many steps (for details, see [DK08]). Even if $K[U]$ is not finitely generated, it may be possible to do certain operations with the above expression. Later, for example, we will give an algorithm to compute certain invariants of $K[U]$ which works for arbitrary irreducible quasi-affine varieties.
The quasi-affine variety U may be irreducible even if X is reducible, that is if $I \trianglelefteq K[x_1, \ldots, x_n]$ is a radical ideal which is not prime. For this case, the above formula can be easily generalized: Note first that the Zariski closure $\overline{U}$ of U in X is irreducible. So we have

Lemma 4.3. *Let U be an irreducible quasi-affine variety. Then there is an irreducible affine variety $Y \supset U$ such that U is an open subset of Y.*

In fact, the closure $\overline{U}$ can be given explicitly by $\overline{U} = \mathrm{Var}(I : L)$ (see [CLO07], Chapter 4, § 4, Theorem 7). By the irreducibility of $\overline{U}$, it follows that the ideal $\tilde{I} := \sqrt{I : L}$, the radical of $I : L$, is a prime ideal. Hence we have

$$K[U] = (K[x_1, \ldots, x_n]/\tilde{I} : ((L + \tilde{I})/\tilde{I})^\infty)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/\tilde{I})}.$$

Note that because of this, we may always assume that an irreducible quasi-affine variety is given as an open subset of an irreducible affine variety.

Next, we will give the definition of normality in the quasi-affine case. Later we will see that the invariant rings of groups acting on normal quasi-affine varieties have particularly nice properties.

Definition 4.4. *An irreducible affine variety X is called* **normal** *if $K[X]$ is normal, i. e. integrally closed in its quotient field* $\mathrm{Quot}(K[X])$. *An irreducible quasi-affine variety U is* **normal** *if every point of U has an open neighbourhood which is isomorphic to a normal affine variety.*

Note that there is also another equivalent definition of normality which can sometimes

be found in the literature, see Proposition 4.6.
The definition of normality in the quasi-affine case is – because of its local nature – not really handy for algorithmic purposes. But as in the affine case, normality corresponds to the normality of the ring of regular functions. Before we can prove this, we need the concept of the local ring at a point.

Definition and Proposition 4.5. *Let U be a quasi-affine variety and let $u \in U$. The* **local ring at u** *is defined to be the set of equivalence classes*

$$O_{U,u} := \{(\mathcal{O}, f);\ u \in \mathcal{O} \subset U \text{ open and } f \in K[\mathcal{O}]\}/\sim,$$

where $(\mathcal{O}, f) \sim (\mathcal{O}', f')$ if and only if $f_{|\mathcal{O}\cap\mathcal{O}'} = f'_{|\mathcal{O}\cap\mathcal{O}'}$. As the name suggests, this set has the structure of a ring: addition and multiplication are defined pointwise, i. e. $(\mathcal{O}, f) + (\mathcal{O}', f') := (\mathcal{O} \cap \mathcal{O}', f + f')$ and $(\mathcal{O}, f) \cdot (\mathcal{O}', f') := (\mathcal{O} \cap \mathcal{O}', f \cdot f')$. Moreover, this ring is local.
Let $\mathfrak{m}_u \trianglelefteq K[U]$ be the maximal ideal corresponding to u. Then $O_{U,u}$ is isomorphic to the localized ring $K[U]_{\mathfrak{m}_u}$. Furthermore, if $V \subset U$ is an open subset of U, then $O_{V,u} \cong O_{U,u}$ for all $u \in V$.

Proof. For the verification of the details, we refer the reader to [Har77], Chapter I. ∎

Proposition 4.6. *Let U be an irreducible quasi-affine variety. The following statements are equivalent.*

(i) U is normal.

(ii) The local ring $O_{U,u}$ is a normal ring for all $u \in U$.

(iii) The ring of regular functions $K[U]$ is a normal ring.

Proof. By Lemma 4.3, we may assume that U is an open subset of an irreducible affine variety X.
For the proof of (i) $\Longrightarrow$ (ii), let U be normal. We have to show that $O_{U,u}$ is normal for all $u \in U$. Let $u \in U$. By definition of normality, u has a normal affine neighbourhood V. Let $\mathfrak{n}_u \trianglelefteq K[V]$ be the maximal ideal corresponding to the point $u \in V$. By the Definition and Proposition above, $O_{U,u} \cong O_{V,u} \cong K[V]_{\mathfrak{n}_u}$ which implies that $O_{U,u}$ is normal, since localization and normalization commute (see [Eis95], Chapter 4, Proposition 4.13). As $u \in U$ was chosen arbitrarily, this shows that (i) implies (ii).
For the proof of the reverse conclusion (ii) $\Longrightarrow$ (i), take $u \in U$. We have to show that there is an affine neighbourhood V of u which is normal as an affine variety. Since U can be covered by open irreducible affine sets ([Har77], Chapter I, Proposition 4.3), we can find an open irreducible affine set $V \subset U$ containing u. It remains to show that $K[V]$ is normal. By Remark 4.2(d), we have $K[V] = \bigcap_{v\in V} K[V]_{\mathfrak{n}_v}$, where $\mathfrak{n}_v \trianglelefteq K[V]$ is the maximal ideal corresponding to the point $v \in V$. The isomorphism $O_{U,v} \cong O_{V,v} \cong K[V]_{\mathfrak{n}_v}$ implies that all rings in this intersection are normal and hence – since they all have the

same quotient field – $K[V]$ is normal, too. It follows that (i) and (ii) are equivalent.
For the proof of implication (ii) $\Longrightarrow$ (iii), let $u \in U$. Regarding u as a point of the affine variety X, we have $O_{U,u} \cong O_{X,u} \cong K[X]_{\mathfrak{o}_u}$, where $\mathfrak{o}_u \trianglelefteq K[X]$ is the maximal ideal corresponding to u. It follows by assumption that $K[X]_{\mathfrak{o}_u}$ is normal. Note that this holds for all $u \in U$. By Remark 4.2(d), we have $K[U] = \bigcap_{u \in U} K[X]_{\mathfrak{o}_u}$, and thus $K[U]$ is normal, too.
For the reverse implication (iii) $\Longrightarrow$ (ii), observe that since $K[U]$ is normal, all of its localizations are again normal. In particular, this is the case for $K[U]_{\mathfrak{m}_u}$, where as usual $\mathfrak{m}_u \trianglelefteq K[U]$ stands for the ideal corresponding to a point $u \in U$. By the Definition and Proposition 4.5 above, $K[U]_{\mathfrak{m}_u} \cong O_{U,u}$, and so the local rings $O_{U,u}$ with $u \in U$ arbitrary are all normal rings. This shows that (ii) and (iii) are equivalent, and the proposition is proved. ∎

Since normality is a local property, it follows immediately that an open subset of a normal affine variety is normal, too. But note that a normal quasi-affine variety may be contained in a non-normal affine variety. Let K be the algebraic closure of $\mathbb{Q}$. Consider the algebraic curve $X \subset K^2$ given by $x_2^2 = x_1^2 + x_1^3$. Since regularity and normality is the same for plane curves (see [Eis95], Chapter 11) and $(0,0)$ is a singular point of X, it follows that X is not normal. But evidently, $X \setminus (0,0)$ is quasi-affine and normal.

Nevertheless, it is always possible to find a normal affine variety in which a normal quasi-affine variety can be embedded.

Proposition 4.7. *Let U be a normal quasi-affine variety embedded as an open subset in a possibly non-normal irreducible affine variety X. Then there exists a normal affine variety $\hat{X}$ and an open subset $\hat{U} \subset \hat{X}$ such that $\hat{U}$ is isomorphic to U.*

Proof (Sketch). In the next section we prove a more general version of this proposition. Hence we only sketch the proof here.
By definition of a regular function, it follows that $K[X] \subset K[U]$. Since $K[X]$ is affine, its integral closure S is again affine (see [Eis95], Chapter 13, Corollary 13.13). Therefore, there is a normal affine variety $\hat{X}$ with $K[\hat{X}] \cong S$. The normality of $K[U]$, which follows from Proposition 4.6, implies that $S \subset K[U]$. Let $\widetilde{L} := \mathrm{Id}_{K[X]}(X \setminus U) \trianglelefteq K[X]$. It then can be shown that U is isomorphic to the open subset $\hat{U} := \hat{X} \setminus \mathrm{Var}_{\hat{X}}((\widetilde{L})_{K[\hat{X}]}) \subset \hat{X}$. For details, see Proposition 4.20. ∎

The proof of the previous proposition can easily be turned into an algorithm.

Algorithm 4.8. (Normal affine embedding of a normal quasi-affine variety)

Input: A prime ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ and an ideal $L \trianglelefteq K[x_1, \ldots, x_n]$ such that the normal quasi-affine variety $U \subset K^n$ is given by $U = \mathrm{Var}(I) \setminus \mathrm{Var}(L)$.

Output: A prime ideal $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ (with $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ new indeterminates) and an

ideal $\hat{L} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ such that $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ is a normal affine variety and $\hat{U} := \mathrm{Var}(\hat{I}) \setminus \mathrm{Var}(\hat{L}) \subset \hat{X}$ is isomorphic to U.

(1) Compute the normalization $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ of $K[x_1, \ldots, x_n]/I$ together with an embedding $\alpha : K[x_1, \ldots, x_n]/I \longrightarrow K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$.

(2) Let $\hat{L}$ be the preimage of $(\alpha((L+I)/I))_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]/\hat{I}}$ under the natural epimorphism $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}] \longrightarrow K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$.

(3) Return $\hat{I}$ and $\hat{L}$.

Remarks. (a) Step (1) of this algorithm can be computed by an algorithm of de Jong, which was given in [dJ98].

(b) By definition of normalization, we have

$$K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \subset \mathrm{Quot}\left(\alpha(K[x_1, \ldots, x_n]/I)\right).$$

In particular, there exist $a_1, \ldots, a_{\hat{n}}, b_1, \ldots, b_{\hat{n}} \in K[x_1, \ldots, x_n]$ with $b_1+I, \ldots, b_{\hat{n}}+I \neq 0$ such that

$$\hat{x}_1 + \hat{I} = \frac{\alpha(a_1 + I)}{\alpha(b_1 + I)}, \ldots, \hat{x}_{\hat{n}} + \hat{I} = \frac{\alpha(a_{\hat{n}} + I)}{\alpha(b_{\hat{n}} + I)}.$$

Then – as we will see in Proposition 4.20 – the map

$$U \longrightarrow \hat{U}, u \longmapsto (a_1(u)/b_1(u), \ldots, a_{\hat{n}}(u)/b_{\hat{n}}(u))$$

for all u of a dense open subset of U defines an isomorphism of the quasi-affine varieties U and $\hat{U}$.

Example 4.9. Let K be the algebraic closure of $\mathbb{Q}$ and let $X := \mathrm{Var}(x_2^2 - x_1^2 - x_1^3) \subset K^2$. As we have seen above, the normal quasi-affine variety $U := X \setminus \{(0,0)\}$ is an open subset of the non-normal affine variety X. Applying the construction of the algorithm shows that U can be embedded into the normal affine variety $\hat{X} := \mathrm{Var}(\hat{x}_2^2 - \hat{x}_1 - 1) \subset K^2$ via the isomorphism

$$U \longrightarrow \hat{X} \setminus \mathrm{Var}(\hat{x}_1, \hat{x}_1\hat{x}_2),\ (\xi_1, \xi_2) \longmapsto (\xi_1, \xi_2/\xi_1). \qquad \lhd$$

4.2 Invariant theory for quasi-affine varieties

We are now prepared to study invariants of group actions on quasi-affine varieties. Formally, the theory of algebraic group actions on quasi-affine varieties looks quite similar to

the theory in the affine case. But things get harder since the description of a morphism between quasi-affine varieties, so in particular the description of the action of a group on a quasi-affine variety, can no longer by given by polynomials. In fact, we have to work with rational functions.

Similarly as in the affine case we define a quasi-affine G-variety.

Definition 4.10. *Let G be a linear algebraic group and let U be a quasi-affine variety. We say that G acts* **regularly** *on U if there exists a morphism $\mu : G \times U \longrightarrow U$ such that*

$$\sigma(u) := \mu(\sigma, u) \qquad \text{for all } \sigma \in G, u \in U$$

defines an action of G on U. In this case, we call U a **quasi-affine G-variety**.

The Cartesian product $G \times U$ with $U \subset X$ open has again the structure of a quasi-affine variety since $G \times U = G \times X \setminus (G \times (X \setminus U))$. Therefore it is clear what is meant by μ to be a morphism.

Examples 4.11. (a) Let X be an affine variety with a regular G-action. Then every G-stable open subset of X is a quasi-affine G-variety.

(b) Let $K = \overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and consider the affine line $X := \overline{\mathbb{Q}}$. Moreover, let the cyclic group with two elements, $G = \langle\sigma\rangle$, act on the open subset $U := X \setminus \{0\}$ by

$$\sigma(u) := 1/u \qquad \text{for all } u \in U.$$

It is not hard to see that this indeed defines a regular action of G on the quasi-affine variety U. This means that U is a quasi-affine G-variety. For details, see Example 4.24. ◁

As in the affine case, the action of G on U induces an action of G on the ring of regular functions $K[U]$.

Lemma 4.12. *Let $\mu : G \times U \longrightarrow U$ be a regular action of the linear algebraic group G on the quasi-affine variety U. Then for every $\sigma \in G$*

$$\mu(\sigma, -) : U \longrightarrow U,\ u \longmapsto \mu(\sigma, u)$$

defines an automorphism of U.

Proof. Let $\sigma \in G$ be a fixed element of G. It is enough to show that $\mu(\sigma, -)$ defines a morphism $U \longrightarrow U$. The one-point set $\{\sigma\} \subset G$ has the structure of an affine variety.

Moreover, the inclusion map $\iota : \{\sigma\} \longmapsto G$ is a morphism. It follows that the product map $\iota \times \mathrm{id}_U : \{\sigma\} \times U \longrightarrow G \times U$ is a morphism, too. This proves the lemma, since $\mu(\sigma, -) = \mu \circ (\iota \times \mathrm{id}_U)$ and the composition of morphisms is again a morphism. ∎

Because of the previous proposition, we see that

$$\sigma(f) := f \circ \mu(\sigma^{-1}, -) \qquad \text{for all } \sigma \in G,\ f \in K[U]$$

defines an action of G on $K[U]$. We aim to compute the **invariant ring**

$$K[U]^G = \{f \in K[U] : \sigma(f) = f \text{ for all } \sigma \in G\}.$$

Obviously, $K[U]^G$ cannot be finitely generated in general, since even $K[U]$ may not be finitely generated. But in fact it may happen that, although $K[U]$ is not finitely generated, the invariant ring $K[U]^G$ is finitely generated. An example which illustrates this is given below (cf. Example 4.40).

Since we want to handle group actions on quasi-affine varieties algorithmically, we have to choose a "data format", how to describe the morphism μ. By the definition of a morphism, this in turn amounts to the description of a regular function on a quasi-affine variety.
In the affine case, this is not a big problem: a regular function can be described by a single polynomial. For the concrete situation of a linear algebraic group acting on an affine variety this means that if G and X are given by $G := \mathrm{Var}(J)$ with $J \trianglelefteq K[t_1, \ldots, t_m]$ radical and $X := \mathrm{Var}(I)$ with $I \trianglelefteq K[x_1, \ldots, x_n]$ radical, then the components $\mu_1, \ldots, \mu_n$ of the morphism $\mu : G \times X \longrightarrow X$ can be written as polynomials in the variables $t_1, \ldots, t_m, x_1, \ldots, x_n$. In general, for the quasi-affine variety $U := X \setminus \mathrm{Var}(L)$, where $L \trianglelefteq K[x_1, \ldots, x_n]$ is an arbitrary ideal, a regular function $f : U \longrightarrow K$ can no longer be described by a polynomial. By the definition of regularity, it is possible to write f locally as a quotient of polynomials. So we need several pieces of information to describe f globally.

Example 4.13. Consider the quasi-affine variety $U = \mathrm{Var}(x_1 \cdot x_2) \setminus \{(0,0)\} \subset K^2$. The map $f : U \longrightarrow K$ which equals 0 on the x_1-axis and 1 on the x_2-axis is clearly regular at every point of U, hence $f \in K[U]$. But obviously, there is no single quotient of polynomial functions a/b with $a, b \in K[x_1, x_2]$ which describes this map uniquely. ◁

If U is assumed to be irreducible, it is enough to know the regular function f on an non-empty open subset of U. This is because f is continuous (cf. Remark 4.2(b)) and every non-empty open subset of U is automatically dense in U. Hence for irreducible quasi-affine varieties, a regular function f can indeed be represented by a single quotient of polynomials.
We are interested in a description of the morphism $\mu = (\mu_1, \ldots, \mu_n) : G \times U \longrightarrow U$, that is we want to specify $\mu_1, \ldots, \mu_n$ which are by definition regular functions on $G \times U$. Unfortunately, the quasi-affine variety $G \times U$ is irreducible only in the case that G

is assumed to be connected. Nonetheless, because of the special form of $G \times U$, it is still possible to describe regular functions on that variety by only one single quotient of polynomials. This will be shown in the next proposition. Before we can actually start, though, we need a preparatory lemma.

Lemma 4.14. *Let $Y \subset K^m$ be a non-empty affine variety and let $U \subset K^n$ be a non-empty quasi-affine variety. Then the map*

$$\alpha : K[Y] \otimes_K K[U] \longrightarrow K[Y \times U],\ \alpha\left(\sum_{i=1}^{s} g_i \otimes f_i\right) : (p,u) \longmapsto \sum_{i=1}^{s} g_i(p) f_i(u)$$

is a well-defined isomorphism of K-algebras.

Proof. It is easy to see that

$$\alpha : K[Y] \otimes_K K[U] \longrightarrow \mathrm{Func}(Y \times U, K),\ \alpha\left(\sum_{i=1}^{s} g_i \otimes f_i\right) : (p,u) \longmapsto \sum_{i=1}^{s} g_i(p) f_i(u),$$

where $\mathrm{Func}(Y \times U, K)$ denotes the K-algebra of functions from $Y \times U$ to K, is a well-defined homomorphism of K-algebras. We have to check first that α maps into $K[Y \times U]$. So let $\sum_{i=1}^{s} g_i \otimes f_i \in K[Y] \otimes_K K[U]$. Let $t_1, \ldots, t_m$ resp. $x_1, \ldots, x_n$ be the coordinate functions on K^m resp. K^n. Both $g_1, \ldots, g_s \in K[Y]$ and $f_1, \ldots, f_s \in K[U]$ can be written locally as polynomial functions in $t_1, \ldots, t_m$ resp. as quotients of polynomial functions in $x_1, \ldots, x_n$. Hence it follows by the definition of α that $\alpha\left(\sum_{i=1}^{s} g_i \otimes f_i\right)$ can be written locally as a quotient of polynomial functions in $t_1, \ldots, t_m, x_1, \ldots, x_n$, too, showing that $\alpha(\sum_{i=1}^{s} g_i \otimes f_i)$ is a regular function on $Y \times U$. Note that we have used the fact that the product $V_1 \times V_2$ of two open subsets $V_1 \subset Y$, $V_2 \subset U$ is again open in $Y \times U$. Since $\sum_{i=1}^{s} g_i \otimes f_i \in K[Y] \otimes_K K[U]$ was chosen arbitrarily, it follows that α maps into $K[Y \times U]$, as desired.
Let $(g_\nu;\ \nu \in C)$ be a K-basis of $K[Y]$, where C denotes a suitable index set. Obviously, every element of $K[Y] \otimes_K K[U]$ can be written as

$$\sum_{\nu \in C} g_\nu \otimes f_\nu$$

where almost all of the f_ν, $\nu \in C$ are zero. In the sequel, whenever we write sums over the index set C, we implicitly assume this finiteness condition.
Suppose that $\alpha\left(\sum_{\nu \in C} g_\nu \otimes f_\nu\right) = 0$. Let $u \in U$. Then the regular function

$$Y \longrightarrow K,\ p \longmapsto \sum_{\nu \in C} g_\nu(p) f_\nu(u)$$

is zero on Y and the linear independence of $(g_\nu;\ \nu \in C)$ implies that $f_\nu(u) = 0$ for all $\nu \in C$. It follows that $f_\nu = 0$ for all $\nu \in C$ and hence $\sum_{\nu \in C} g_\nu \otimes f_\nu = 0$. This shows that α is injective.
For the proof of surjectivity, let $h \in K[Y \times U]$ be an arbitrary regular function. It is required to prove that there exists $\sum_{\nu \in C} g_\nu \otimes f_\nu \in K[Y] \otimes_K K[U]$ such that $\alpha\left(\sum_{\nu \in C} g_\nu \otimes f_\nu\right)$

$= h$. Note that if U is affine, then the assertion of the proposition is well-known. In particular, α is surjective in this case.
If U is quasi-affine, let $U = \bigcup_{j \in E} U_j$ be an affine open covering of U, where E denotes a suitable index set. Observe that – by the local nature of the definition of regularity – $h_{|Y \times U_j}$ is regular on $Y \times U_j$ for all $j \in E$. Let $j \in E$. By the affineness of Y and U_j, it follows by the remark a few lines above that there exist $f_{\nu,j} \in K[U_j]$, $\nu \in C$ such that

$$h_{|Y \times U_j}(p,u) = \sum_{\nu \in C} g_\nu(p) f_{\nu,j}(u) \quad \text{for all } (p,u) \in Y \times U_j.$$

The linear independence of $(g_\nu;\ \nu \in C)$ implies that

$$(f_{\nu,j})_{|U_k \cap U_j} = (f_{\nu,k})_{|U_j \cap U_k} \quad \text{for all } \nu \in C, j,k \in E$$

and by the local nature of the definition of a regular function, it follows that there exist global regular functions $f_\nu \in K[U]$ for all $\nu \in C$ such that

$$(f_\nu)_{|U_j} = f_{\nu,j} \quad \text{for all } j \in E.$$

In particular, this means that $h(p,u) = \sum_{\nu \in C} g_\nu(p) f_\nu(u)$ for all $(p,u) \in Y \times U$ and hence $\alpha\left(\sum_{\nu \in C} g_\nu \otimes f_\nu\right) = h$, as desired. ∎

Proposition 4.15. *Let $U \subset K^n$ be an irreducible quasi-affine variety and $G \subset K^m$ be a linear algebraic group. The coordinate functions on K^n shall be denoted by $x_1, \ldots, x_n$, those on K^m by $t_1, \ldots, t_m$. Let $\mu = (\mu_1, \ldots, \mu_n) : G \times U \longrightarrow U$ be a morphism. Then there exist a dense open subset $V \subset G \times U$, polynomials $N_1, \ldots, N_n \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ and $D_1, \ldots, D_n \in K[x_1, \ldots, x_n] \subset K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ such that $0 \notin D_1(V), \ldots, D_n(V)$ and*

$$\mu(v) = (N_1(v)/D_1(v), \ldots, N_n(v)/D_n(v)) \qquad \text{for all } v \in V.$$

In particular, the data $N_1, \ldots, N_n, D_1, \ldots, D_n$ describe the morphism μ uniquely.

Proof. Let $G = \bigcup_{i=1}^s G_i$ be the decomposition of G into irreducible components. As the product of irreducible varieties is again irreducible (cf. [Har77], Ex. 3.16), the decomposition of $G \times U$ into irreducible components is given by

$$G \times U = \bigcup_{i=1}^{s} G_i \times U.$$

Let f be a regular function on $G \times U$. Setting $Y := G$ in the preceding lemma, it follows that we may identify f with an element of $K[G] \otimes_K K[U]$. Moreover, by the explicit isomorphism given there, we can find polynomials $N \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ and $D \in K[x_1, \ldots, x_n]$ such that the open set $V := (G \times U) \setminus \mathrm{Var}(D)$ is non-empty and $f = N/D$ as functions on that open set. Obviously, we have $V \cap (G_i \times U) \neq \emptyset$ for $i = 1, \ldots, s$, which implies that V is dense in $G \times U$. Note that this construction only works if U is an irreducible quasi-affine variety. As we have seen, it is not possible in

general to write the regular function f as a quotient of two polynomials N and D on a dense open subset of $G \times U$ if U is a reducible quasi-affine variety.
The components of the morphism $\mu = (\mu_1, \ldots, \mu_n)$ are regular functions. Hence, by the preceding discussion, there exist $N_1, \ldots, N_n \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$, $D_1, \ldots, D_n \in K[x_1, \ldots, x_n] \subset K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ and open sets $V_1, \ldots, V_n \subset G \times U$ such that for $i = 1, \ldots, n$ the function N_i/D_i is defined on V_i and $\mu_i(v) = N_i(v)/D_i(v)$ for all $v \in V_i$. The open sets V_i are non-empty and dense, hence $V := \bigcap_{i=1}^{n} V_i$ is non-empty and dense, too. Moreover, $0 \notin D_1(V), \ldots, D_n(V)$ and $\mu(v) = (N_1(v)/D_1(v), \ldots, N_n(v)/D_n(v))$ for all $v \in V$. Finally, since V is dense, the data $N_1, \ldots, N_n, D_1, \ldots, D_n$ describe the morphism μ uniquely. ∎

Because of the previous proposition, we make the following convention for the description of a linear algebraic group G, a quasi-affine variety U and an action of G on U.

Convention 4.16.
Let G be a linear algebraic group, U be an irreducible quasi-affine variety and let G act regularly on U. We assume that these data are given as follows:

(1) Generators of the radical ideal $J \trianglelefteq K[t_1, \ldots, t_m]$ defining the linear algebraic group G as an affine variety in K^m.

(2) Generators $p_1, \ldots, p_r$ of the prime ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ and generators $q_1, \ldots, q_t$ of the ideal $L \trianglelefteq K[x_1, \ldots, x_n]$ such that $U = \mathrm{Var}(I) \setminus \mathrm{Var}(L) \subset K^n$.

(3) Polynomials $N_1, \ldots, N_n \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ and $D_1, \ldots, D_n \in K[x_1, \ldots, x_n] \subset K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ such that there is a dense open subset $V \subset G \times U$ with $0 \notin D_1(V), \ldots, D_n(V)$ and

$$\mu(v) = (N_1(v)/D_1(v), \ldots, N_n(v)/D_n(v)) \qquad \text{for all } v \in V,$$

where $\mu : G \times U \longrightarrow U$ is the morphism corresponding to the action of G on U.

Now that we have gained some clarity about the description of the action of G on U, we want to close this section with an examination of the extensibility of this action to the affine variety X in which U is embedded as an open subset.
First note that in general G does not act on X, as can be seen in the following example.

Example 4.17. Recall Example 4.11(b) where the generator σ of the cyclic group with two elements acts on $\overline{\mathbb{Q}} \setminus \{0\}$ by multiplicative inversion. Clearly, this action cannot be extended to $X = \overline{U}$, since otherwise the polynomial function $\mu(\sigma, -) : X \longrightarrow X$ would have a pole at the origin which is impossible. ◁

We will see in the following proposition that U may always be embedded G-equivariantly into an affine G-variety. This will turn out to be quite useful for algorithmic purposes.

But first, we need a preparatory lemma about the action of G on $K[U]$. As in the affine case, the action of G on $K[U]$ can be described by a homomorphism $K[U] \longrightarrow K[G] \otimes_K K[U]$.

Lemma 4.18. *Let the linear algebraic group G act regularly on the quasi-affine variety U. Then there exists a homomorphism of algebras*

$$\tilde{\mu} : K[U] \longrightarrow K[G] \otimes_K K[U]$$

which describes the action of G on $K[U]$ in the following way. If $\tilde{\mu}(f) = \sum_{i=1}^{s} g_i \otimes a_i$ with $g_1, \ldots, g_s \in K[G]$ and $a_1, \ldots, a_s \in K[U]$, then $\sigma(f)$ is given by $\sigma(f) = \sum_{i=1}^{s} g_i(\sigma) \cdot a_i$ for all $\sigma \in G$. In particular, G acts locally finite on $K[U]$.

Proof. The construction of $\tilde{\mu}$ is identical to the case where G acts on an affine variety (cf. Lemma 1.28). ∎

Remark 4.19. Note that – as a variant of the above – there always exists a homomorphism of algebras

$$\mu^* : K[U] \longrightarrow K[G] \otimes_K K[U]$$

with the slightly different property that if $\mu^*(f) = \sum_{i=1}^{s} g_i \otimes a_i$, then $\sigma^{-1}(f)$ is given by $\sigma^{-1}(f) = \sum_{i=1}^{s} g_i(\sigma) \cdot a_i$ for all $\sigma \in G$. ♢

Proposition 4.20. *Let the linear algebraic group G act regularly on the irreducible quasi-affine variety U. Then there is an irreducible affine G-variety $\hat{X}$ and a G-equivariant embedding of U as an open subset in $\hat{X}$. Moreover, if U is normal, $\hat{X}$ can be chosen to be normal, too.*

Proof. We assume that the linear algebraic group G, the quasi-affine variety U and the action of G on U are given as in Convention 4.16. By Lemma 4.18, G acts locally finite on $K[U]$. In particular, we can find G-modules $V_1, \ldots, V_n \subset K[U]$ such that $x_i + I \in V_i$ for $i = 1, \ldots, n$. Let S be the subalgebra of $K[U]$ generated by the elements of $V_1, \ldots, V_n$, that is

$$S := K\left[v;\ v \in \bigcup_{i=1}^{n} V_i\right] \subset K[U].$$

As $V_1, \ldots, V_n$ are finitely generated vector spaces, it follows that S is finitely generated as a K-algebra.
By a theorem of Noether, the normalization of S is again affine (see [Eis95], Chapter 13, Corollary 13.13). We may thus replace S by its normalization in case U is normal and we want $\hat{X}$ to be normal, too. Observe that in this case, we still have $S \subset K[U]$ by the normality of $K[U]$.
Note that the algebra S is stable under G, which is obvious from the construction in case we did not normalize, and follows easily in the "normalization case" since the normalization

of a G-stable algebra is again G-stable.
By Proposition 1.31(b), the action of G on S can be described by a homomorphism of algebras $\tilde{\mu}_{|S} : S \longrightarrow K[G] \otimes_K S$. As S is an affine algebra, we may represent S as follows. There exists an isomorphism

$$\gamma : K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \longrightarrow S$$

where $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ are indeterminates over K and $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ is a prime ideal. Apparently, the action of G on S given by $\tilde{\mu}_{|S}$ can be carried over via γ to an action of G on $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$, then given by $\hat{\mu} : K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \longrightarrow K[G] \otimes_K K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$, say. More precisely, if $i \in \{1, \ldots, \hat{n}\}$ and $\tilde{\mu}_{|S}(\gamma(\hat{x}_i + \hat{I})) = \sum_{j=1}^{s} g_j \otimes a_j$ for some $g_1, \ldots, g_s \in K[G]$ and $a_1, \ldots, a_s \in S$, then

$$\hat{\mu}(\hat{x}_i + \hat{I}) = \sum_{j=1}^{s} g_j \otimes \gamma^{-1}(a_j). \tag{4.2}$$

By Proposition 1.29, there is an action of G on the affine variety $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$, whose induced action on the coordinate ring $K[\hat{X}] = K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ is exactly the action we have already given on $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ by $\hat{\mu}$.
In what follows, we will show that U is G-isomorphic to the quasi-affine variety $\hat{U} := \hat{X} \setminus \mathrm{Var}_{\hat{X}}(\gamma^{-1}(((L + I)/I)_S))$ via the following two morphisms

$$\begin{aligned} &\phi : U \longrightarrow \hat{U},\ u \longmapsto (\gamma(\hat{x}_1 + \hat{I})(u), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})(u)) \quad \text{and} \\ &\psi : \hat{U} \longrightarrow U,\ \hat{u} \longmapsto (\gamma^{-1}(x_1 + I)(\hat{u}), \ldots, \gamma^{-1}(x_n + I)(\hat{u})). \end{aligned}$$

Note that $\gamma(\hat{x}_1 + \hat{I}), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I}) \in K[U]$ are regular functions and thus defined for every point of U. Our aim is to show that the image of ϕ resp. ψ is contained in $\hat{U}$ resp. U and that $\psi \circ \phi = \mathrm{id}_U$ and $\phi \circ \psi = \mathrm{id}_{\hat{U}}$.
It is clear that ϕ maps into $\hat{X}$ since $\hat{I}$ is the ideal of relations of $\gamma(\hat{x}_1 + \hat{I}), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})$. Let $u \in U$. By definition of U, there is $f + I \in (L + I)/I$ with $(f + I)(u) \neq 0$. The element $\gamma^{-1}(f + I)$ is contained in $\gamma^{-1}(((L + I)/I)_S)$ and

$$\begin{aligned} (\gamma^{-1}(f + I))(\phi(u)) &= \gamma^{-1}(f + I)(\gamma(\hat{x}_1 + \hat{I})(u), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})(u)) \\ &= \gamma^{-1}(f + I)(\gamma(\hat{x}_1 + \hat{I}), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I}))(u) \\ &= \gamma(\gamma^{-1}(f + I)(\hat{x}_1 + \hat{I}, \ldots, \hat{x}_{\hat{n}} + \hat{I}))(u) \\ &= (f + I)(u) \neq 0, \end{aligned}$$

which implies that $\phi(U) \subset \hat{U}$. Since $\gamma(\hat{x}_1 + \hat{I}), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})$ are regular functions on U, the map $\phi : U \longrightarrow \hat{U}$ is a morphism, indeed.
We do the same for ψ. The image of ψ is clearly contained in X. Let $\hat{u} \in \hat{U}$. By definition of $\hat{U}$, there exists $\hat{f} + \hat{I} \in \gamma^{-1}(((L + I)/I)_S)$ with $(\hat{f} + \hat{I})(\hat{u}) \neq 0$. We may assume that

$\hat{f} + \hat{I} \in \gamma^{-1}((L+I)/I)$. But then $\gamma(\hat{f} + \hat{I}) \in (L+I)/I$ and

$$\begin{aligned}\gamma(\hat{f} + \hat{I})(\psi(\hat{u})) &= \gamma(\hat{f} + \hat{I})(\gamma^{-1}(x_1 + I)(\hat{u}), \ldots, \gamma^{-1}(x_n + I)(\hat{u})) \\ &= \gamma(\hat{f} + \hat{I})(\gamma^{-1}(x_1 + I), \ldots, \gamma^{-1}(x_n + I))(\hat{u}) \\ &= \gamma^{-1}(\gamma(\hat{f} + \hat{I})(x_1 + I, \ldots, x_n + I))(\hat{u}) \\ &= (\hat{f} + \hat{I})(\hat{u}) \neq 0,\end{aligned}$$

which implies that $\psi(\hat{U}) \subset U$. Finally, the components of ψ are regular on $\hat{U}$ and hence $\psi : \hat{U} \longrightarrow U$ is a morphism, too.
Let $u = (u_1, \ldots, u_n) \in U$ and $\hat{u} = (\hat{u}_1, \ldots, \hat{u}_{\hat{n}}) \in \hat{U}$. Then

$$\begin{aligned}\psi(\phi(u)) &= \psi\left(\gamma(\hat{x}_1 + \hat{I})(u), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})(u)\right) \\ &= \left(\gamma^{-1}(x_i + I)\left(\gamma(\hat{x}_1 + \hat{I})(u), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})(u)\right)\right)_{i=1,\ldots,n} \\ &= \left(\gamma^{-1}(x_i + I)\left(\gamma(\hat{x}_1 + \hat{I}), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})\right)(u)\right)_{i=1,\ldots,n} \\ &= \left(\gamma\left(\gamma^{-1}(x_i + I)\left(\hat{x}_1 + \hat{I}, \ldots, \hat{x}_{\hat{n}} + \hat{I}\right)\right)(u)\right)_{i=1,\ldots,n} \\ &= (u_1, \ldots, u_n)\end{aligned}$$

and similarly

$$\begin{aligned}\phi(\psi(\hat{u})) &= \phi\left(\gamma^{-1}(x_1 + I)(\hat{u}), \ldots, \gamma^{-1}(x_n + I)(\hat{u})\right) \\ &= \left(\gamma(\hat{x}_i + \hat{I})\left(\gamma^{-1}(x_1 + I)(\hat{u}), \ldots, \gamma^{-1}(x_n + I)(\hat{u})\right)\right)_{i=1,\ldots,\hat{n}} \\ &= \left(\gamma^{-1}\left(\gamma(\hat{x}_i + \hat{I})\left(x_1 + I, \ldots, x_n + I\right)\right)(\hat{u})\right)_{i=1,\ldots,\hat{n}} \\ &= (\hat{u}_1, \ldots, \hat{u}_{\hat{n}}).\end{aligned}$$

It follows that the quasi-affine varieties U and $\hat{U}$ are isomorphic.
It remains to show that ϕ commutes with the action of G. Let $\sigma \in G$ and $u \in U$. Applying σ first and evaluating ϕ afterwards yields

$$\begin{aligned}\phi(\sigma(u)) &= (\gamma(\hat{x}_1 + \hat{I})(\sigma(u)), \ldots, \gamma(\hat{x}_{\hat{n}} + \hat{I})(\sigma(u))) \\ &= (\sigma^{-1}(\gamma(\hat{x}_1 + \hat{I}))(u), \ldots, \sigma^{-1}(\gamma(\hat{x}_{\hat{n}} + \hat{I}))(u)).\end{aligned} \tag{4.3}$$

Let $i \in \{1, \ldots, \hat{n}\}$ and take $g_1, \ldots, g_s \in K[G]$, $a_1, \ldots, a_s \in S$ such that $\hat{\mu}(\hat{x}_i + \hat{I}) = \sum_{j=1}^{s} g_j \otimes \gamma^{-1}(a_j)$ (cf. equation (4.2)). Similar considerations as in the previous calcula-

tions yield

$$\begin{aligned}\hat{\mu}(\hat{x}_i + \hat{I})(\sigma^{-1}, \phi(u)) &= \sum_{j=1}^{s} g_j(\sigma^{-1}) \cdot \gamma^{-1}(a_j)(\phi(u)) \\ &= \sum_{j=1}^{s} g_j(\sigma^{-1}) \cdot a_j(u) = \sigma^{-1}(\gamma(\hat{x}_i + \hat{I}))(u).\end{aligned}$$

Recall definition (1.1) of the action of G on $\hat{X}$. Letting σ act on $\phi(u)$ and applying the result of the preceding equation for all $i \in \{1, \ldots, \hat{n}\}$ gives

$$\begin{aligned}\sigma(\phi(u)) &= \Big(\hat{\mu}(\hat{x}_1 + \hat{I})(\sigma^{-1}, \phi(u)), \ldots, \hat{\mu}(\hat{x}_{\hat{n}} + \hat{I})(\sigma^{-1}, \phi(u))\Big) \\ &= (\sigma^{-1}(\gamma(\hat{x}_1 + \hat{I}))(u), \ldots, \sigma^{-1}(\gamma(\hat{x}_{\hat{n}} + \hat{I}))(u)).\end{aligned}$$

Comparing this with equation (4.3) shows that $\phi(\sigma(u)) = \sigma(\phi(u))$. Since this is true for arbitrary $u \in U$ and $\sigma \in G$, the result follows. ∎

Remarks 4.21. (a) With the notation of the proof, the isomorphism $U \longrightarrow \hat{U}$ induces an isomorphism of algebras $K[\hat{U}] \longrightarrow K[U]$ which is given by $\hat{x}_i + \hat{I} \longmapsto \phi_i$ for $i = 1, \ldots, \hat{n}$. Note that by construction, this isomorphism commutes with the action of G. For future reference, observe that – identifying $K[\hat{X}]$ and $K[\hat{U}]$ with their images in $K[U]$ – we have the inclusions

$$K[X] \subset K[\hat{X}] \subset K[U] = K[\hat{U}].$$

(b) Note that the proof of the previous proposition remains correct if the concrete definition of S is replaced by setting S to be any G-stable affine algebra such that $K[X] \subset S \subset K[U]$. In particular, if $K[U]$ is finitely generated (as a K-algebra) then it is perfectly valid to set $S := K[U]$. In this case, $\hat{X}$ and $\hat{U}$ have isomorphic rings of regular functions. ♢

The proof of the previous proposition can be turned into an algorithm. Although the basic idea of the construction is simple, the algorithm becomes quite lengthy when it is worked out in all its details.

Algorithm 4.22. (Embedding a quasi-affine G-variety into an affine G-variety)

Input: A linear algebraic group G, an irreducible quasi-affine variety U and a regular action μ of G on U according to Convention 4.16.

Output: An irreducible affine variety $\hat{X}$, an action $\hat{\mu}$ of G on $\hat{X}$, a G-stable open subset $\hat{U} \subset \hat{X}$ and a G-morphism $\phi : U \longrightarrow \hat{X}$ which induces a G-isomorphism of U and $\hat{U}$.

More precisely, the output is given by a prime ideal $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ (with $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ new indeterminates), an ideal $\hat{L} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$, polynomials $\hat{N}_1, \ldots, \hat{N}_{\hat{n}} \in K[t_1, \ldots, t_m, \hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ and rational functions $\phi_1, \ldots, \phi_{\hat{n}} \in K[U] \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ which stand for the following: The group G acts on $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ via $\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X}$, where $\hat{\mu}$ is defined by

$$\hat{\mu}(v) = (\hat{N}_1(v), \ldots, \hat{N}_{\hat{n}}(v))$$

for all $v \in G \times \hat{X}$, the open subset $\hat{U} := \hat{X} \setminus \mathrm{Var}(\hat{L})$ is G-stable under this action and $\phi : U \longrightarrow \hat{U}$ is a G-isomorphism given by $(\phi_1, \ldots, \phi_{\hat{n}})$ in the sense that

$$\phi(u) = (\phi_1(u), \ldots, \phi_{\hat{n}}(u))$$

for all $u \in U$.

(1) Compute a Gröbner basis $\mathcal{G}$ of the ideal $(J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]}$ with respect to an arbitrary monomial order on $t_1, \ldots, t_m$.

(2) Let α be the natural homomorphism

$$\alpha : K[t_1, \ldots, t_m, x_1, \ldots, x_n] \longrightarrow \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m].$$

Set

$$H_1 := \mathrm{NF}_{\mathcal{G}}(\alpha(N_1)/\alpha(D_1)), \ldots, H_n := \mathrm{NF}_{\mathcal{G}}(\alpha(N_n)/\alpha(D_n)).$$

(3) Let $C \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ be the set of coefficients occuring in the polynomials $H_1, \ldots, H_n$.

(4) Choose a maximal K-linearly independent subset of C, say $\{\phi_1, \ldots, \phi_{\hat{n}}\}$.

(5) Let $n_1, \ldots, n_{\hat{n}}, d_1, \ldots, d_{\hat{n}} \in K[x_1, \ldots, x_n]$ such that

$$\phi_1 = \frac{n_1 + I}{d_1 + I}, \ldots, \phi_{\hat{n}} = \frac{n_{\hat{n}} + I}{d_{\hat{n}} + I}$$

(6) For $i = 1, \ldots, \hat{n}$:

(i) Find $R_i \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ such that

$$n_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) - R_i \cdot d_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) \in (J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]}. \tag{4.4}$$

(see Remark 4.23(c) for details about how this can be computed)

(ii) Replace R_i by $\mathrm{NF}_{\mathcal{G}}(R_i)$.

(iii) Find $\alpha_{i1}, \ldots, \alpha_{i\hat{n}} \in K[t_1, \ldots, t_m]$ such that

$$R_i = \sum_{j=1}^{\hat{n}} \alpha_{ij}\phi_j.$$

(a hint on how this can be calculated is given in the following proof of correctness)

(7) Compute the ideal of relations of $\phi_1, \ldots, \phi_{\hat{n}}$ over K, say $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$. (For details, see Remark 4.23(d))

(8) Compute polynomials $\hat{q}_1, \ldots, \hat{q}_t \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ such that

$$q_i + I = \hat{q}_i(\phi_1, \ldots, \phi_{\hat{n}}).$$

(For details, see Remark 4.23(e))

(9) Set $\hat{N}_1 := \sum_{j=1}^{\hat{n}} \alpha_{1j}\hat{x}_j, \ldots, \hat{N}_{\hat{n}} := \sum_{j=1}^{\hat{n}} \alpha_{\hat{n}j}\hat{x}_j$ and

$$\hat{L} := (\hat{q}_1, \ldots, \hat{q}_t) \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}].$$

(10) Return $\hat{I}, \hat{L}, (\hat{N}_1, \ldots, \hat{N}_{\hat{n}}), (\phi_1, \ldots, \phi_{\hat{n}})$.

Remarks 4.23. (a) As seen in Remark 4.21(a), the isomorphism $U \longrightarrow \hat{U}$ induces an isomorphism of algebras $K[\hat{U}] \longrightarrow K[U]$ which is given by $\hat{x}_i + \hat{I} \longmapsto \phi_i$ for $i = 1, \ldots, \hat{n}$. Note that by construction, this isomorphism commutes with the action of G.

(b) According to Proposition 4.20, a normal quasi-affine G-variety can be embedded G-equivariantly as an open subset in a normal affine G-variety. In this algorithm, we have not included a special treatment of this normal case. However, it is not hard to modify Algorithm 4.22 such that it can handle this case, too (cf. Algorithm 4.7).

(c) As indicated for a similar situation in the last section, step (6)(i) of the algorithm can be computed for example with the Extended Buchberger Algorithm (cf. [BW93], Chapter 5, Section 5.6). To be more precise, it can be used to compute coordinates of the ideal membership

$$\begin{aligned} &n_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) \\ &\qquad \in (d_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)), J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]}. \end{aligned}$$

It is then clear that R_i is given by the coordinate corresponding to the generator $d_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n))$.

(d) In step (7) it is required to compute the ideal of relations of the rational functions $\phi_1, \ldots, \phi_{\hat{n}}$. The standard method for the computation of relation ideals cannot be applied here, since the elements $\phi_1, \ldots, \phi_{\hat{n}}$ are rational and not – as usual –

polynomial functions. One possibility for the computation of $\hat{I}$ is the following. Let $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ be additional indeterminates over K. Set $d := \prod_{j=1}^{\hat{n}} d_j$ and define

$$D := \big((n_1 - \hat{x}_1 \cdot d_1, \ldots, n_{\hat{n}} - \hat{x}_{\hat{n}} \cdot d_{\hat{n}})_{K[x_1,\ldots,x_n,\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]} + (I)_{K[x_1,\ldots,x_n,\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]}\big) : (d)^\infty \trianglelefteq K[x_1, \ldots, x_n, \hat{x}_1, \ldots, \hat{x}_{\hat{n}}].$$

Then the desired ideal of relations is given by

$$\hat{I} := D \cap K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}] \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]. \tag{4.5}$$

In the following, we prove that every $F \in \hat{I}$ is a relation of $\phi_1, \ldots, \phi_{\hat{n}}$. We omit the proof of the converse here, since it is very similar to what will be done in (e) below. Let $F \in \hat{I}$. We have to show that $F(\phi_1, \ldots, \phi_{\hat{n}}) = 0$. By definition of D, there exist $M \in \mathbb{N}$, $a_1, \ldots, a_{\hat{n}} \in K[x_1, \ldots, x_n, \hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ and $b \in (I)_{K[x_1,\ldots,x_n,\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]}$ such that

$$F \cdot d^M = \sum_{j=1}^{\hat{n}} a_j \cdot (n_j - \hat{x}_j \cdot d_j) + b.$$

Applying the natural homomorphism

$$\delta : K[x_1, \ldots, x_n, \hat{x}_1, \ldots, \hat{x}_{\hat{n}}] \longrightarrow (K[x_1, \ldots, x_n]/I)[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$$

to this equation and setting $\hat{x}_1 := \phi_1, \ldots, \hat{x}_{\hat{n}} := \phi_{\hat{n}}$ yields

$$F(\phi_1, \ldots, \phi_{\hat{n}}) \cdot (d + I)^M = \sum_{j=1}^{\hat{n}} \delta(a_j) \cdot ((n_j + I) - \phi_j \cdot (d_j + I)) + 0 = 0.$$

Since $(d + I)^M \neq 0$, it follows that $F(\phi_1, \ldots, \phi_{\hat{n}}) = 0$, as desired.

(e) At first sight, the computation of $\hat{q}_1, \ldots, \hat{q}_t$ of step (8) seems to be a simple constructive algebra membership test (cf. [BW93], Chapter 6, Section 6.2). But similarly as in (d) above, the problem here is that the generators of the algebra, i. e. $\phi_1, \ldots, \phi_{\hat{n}}$, are rational and not – as usual – polynomial functions. Therefore, we have to modify the standard algebra membership test.
With the same notation as in (d), let $\mathcal{H}$ be a Gröbner basis of D with respect to an elimination order on the variables $x_1, \ldots, x_n, \hat{x}_1, \ldots, \hat{x}_n$ where any monomial involving one of $x_1, \ldots, x_n$ is greater than all monomials in $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$. Let $i \in \{1, \ldots, t\}$. We claim that a representation of $q_i + I$ in the generators $\phi_1, \ldots, \phi_{\hat{n}}$ can be found by simply reducing q_i with respect to $\mathcal{H}$.
So let $\hat{q}_i \in K[\hat{x}_1, \ldots, \hat{x}_n]$ be a representation of $q_i + I$, that is $q_i + I = \hat{q}_i(\phi_1, \ldots, \phi_{\hat{n}})$. It will become clear in the following proof of correctness that such a polynomial $\hat{q}_i$ always exists. We may assume without loss of generality that $\hat{q}_i$ is in normal form with respect to $\mathcal{H}$. For, otherwise we can replace $\hat{q}_i$ by $\mathrm{NF}_{\mathcal{H}}(\hat{q}_i)$. Note that $\mathrm{NF}_{\mathcal{H}}(\hat{q}_i)$ is a polynomial only in $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$, again since we have assumed the monomial order to be an elimination order for $x_1, \ldots, x_n$. Furthermore by (d) above, this replacement preserves the property $q_i + I = \hat{q}_i(\phi_1, \ldots, \phi_{\hat{n}})$. We now show that $\mathrm{NF}_{\mathcal{H}}(q_i) = \hat{q}_i$.

The following calculation takes place in $(K[x_1,\dots,x_n]/I)_{d+I}[\hat{x}_1,\dots,\hat{x}_{\hat{n}}]$. We have

$$\begin{aligned} q_i + I = \hat{q}_i(\phi_1,\dots,\phi_{\hat{n}}) &= \hat{q}_i(\hat{x}_1+\phi_1-\hat{x}_1,\dots,\hat{x}_{\hat{n}}+\phi_{\hat{n}}-\hat{x}_{\hat{n}}) \\ &= \hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}}) + \sum_{j=1}^{\hat{n}} a_j\cdot(\phi_j-\hat{x}_j) \end{aligned}$$

for certain $a_1,\dots,a_{\hat{n}} \in (K[x_1,\dots,x_n]/I)_{d+I}[\hat{x}_1,\dots,\hat{x}_{\hat{n}}]$. Multipliying this equation by a common denominator $d^M + I$ for $M \in \mathbb{N}$ large enough yields

$$d^M\cdot q_i + I = (d^M+I)\cdot\hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}}) + \sum_{j=1}^{\hat{n}} \widetilde{a}_j\cdot((n_j+I)-\hat{x}_j\cdot(d_j+I))$$

for certain $\widetilde{a}_1,\dots,\widetilde{a}_{\hat{n}} \in (K[x_1,\dots,x_n]/I)[\hat{x}_1,\dots,\hat{x}_{\hat{n}}]$. Let $a'_1,\dots a'_{\hat{n}} \in K[x_1,\dots,x_n, \hat{x}_1,\dots,\hat{x}_{\hat{n}}]$ be arbitrary preimages of $\widetilde{a}_1,\dots,\widetilde{a}_{\hat{n}}$ under the natural homomorphism δ from (d). Since $\sum_{j=1}^{\hat{n}} a'_j\cdot(n_j-\hat{x}_j\cdot d_j)$ is clearly contained in D, it follows that

$$d^M\cdot q_i - d^M\cdot\hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}}) \in D$$

and by the definition of D, this implies

$$q_i - \hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}}) \in D.$$

Since, by assumption, $\hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}})$ is in normal form with respect to $\mathcal{H}$, it follows that $\mathrm{NF}_{\mathcal{H}}(q_i) = \hat{q}_i(\hat{x}_1,\dots,\hat{x}_{\hat{n}})$.

To sum up, this means that the polynomials $\hat{q},\dots,\hat{q}_t$ can be found algorithmically by first computing a Gröbner basis $\mathcal{H}$ of the colon ideal D for an adequate monomial order (which has already been calculated for the implementation of step (7)) and then reducing $q_1,\dots,q_t$ with respect to $\mathcal{H}$. ♢

Proof of Correctness. In steps (1)-(4), a G-module $V \subset K[U]$ with $x_1+I,\dots,x_n+I \in V$ is computed. We first show that $\phi_1,\dots,\phi_{\hat{n}}$ is a K-basis of such a V. The proof for this is very similar to parts of the proof of Proposition 1.31(a) and Algorithm 3.25. Nonetheless, we repeat it here for the sake of completeness. Let $i \in \{1,\dots,n\}$. Then

$$\begin{aligned} \sigma^{-1}(x_i+I)(u) = (x_i+I)(\sigma(u)) &= (x_i+I)(N_1(\sigma,u)/D_1(u),\dots,N_n(\sigma,u)/D_n(u)) \\ &= N_i(\sigma,u)/D_i(u) \end{aligned}$$

for all $\sigma \in G$ and all u in a dense open subset of U. It follows that

$$\sigma^{-1}(x_i+I) = \frac{\alpha(N_i)(\sigma)}{\alpha(D_i)} \quad \text{for all } \sigma \in G. \tag{4.6}$$

Since a reduction of $\alpha(N_i)/\alpha(D_i)$ modulo $\mathcal{G}$ does not change the validity of the previous equation, this implies

$$\sigma^{-1}(x_i + I) = H_i(\sigma) \quad \text{for all } \sigma \in G. \tag{4.7}$$

The polynomial H_i can be written as $H_i = \sum_{j=1}^{s} a_j \cdot g_j$ where $g_1, \ldots, g_s$ are pairwise distinct monomials in $t_1, \ldots, t_m$ and $a_1, \ldots, a_s \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$. We claim that

$$\widetilde{V} := \langle a_1, \ldots, a_s \rangle_K \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$$

is a G-module containing $x_i + I$. Let $\tau \in G$. We have to show that $\tau(a_i) \in \widetilde{V}$, again. Since H_i is in normal form with respect to $\mathcal{G}$, it follows that $g_1 + J, \ldots, g_s + J$ are linearly independent as regular functions on G (see [BW93], Chapter 6, Proposition 6.52). Hence there exist $\sigma_1, \ldots, \sigma_s \in G$ such that $(g_j(\sigma_k))_{j,k=1,\ldots,s} \in K^{s \times s}$ is regular. By equation (4.7), it follows that

$$\begin{aligned}(\tau(a_1), \ldots, \tau(a_s)) \cdot (g_j(\sigma_k))_{j,k=1,\ldots,s} &= ((\tau\sigma_1^{-1})(x_i + I), \ldots, (\tau\sigma_s^{-1})(x_i + I)) \\ &= \left(\sum_{j=1}^{s} a_j \cdot g_j(\sigma_1\tau^{-1}), \ldots, \sum_{j=1}^{s} a_j \cdot g_j(\sigma_s\tau^{-1}) \right) \in \widetilde{V}^s\end{aligned}$$

and thus

$$(\tau(a_1), \ldots, \tau(a_s)) = (\tau(a_1), \ldots, \tau(a_s)) \cdot (g_j(\sigma_k))_{j,k=1,\ldots,s} \cdot (g_j(\sigma_k))^{-1}_{j,k=1,\ldots,s} \in \widetilde{V}^s.$$

But this means that $\tau(a_1), \ldots, \tau(a_s) \in \widetilde{V}$, as desired.
Moreover, as $x_i + I = \sum_{j=1}^{s} a_j \cdot g_j(1_G)$, it follows that $x_i + I \in \widetilde{V}$ and so $\widetilde{V}$ is a G-module containing $x_i + I$, indeed.
Note also that $\widetilde{V}$ is the smallest G-module containing $x_i + I$ in the sense that $\widetilde{V}$ is contained in every G-module $\widetilde{V}'$ with $x_i + I \in \widetilde{V}'$. This follows by setting $\tau = 1_G$ in the equations a few lines above. In particular, we have $\widetilde{V} \subset K[U]$.
Applying these arguments to $i = 1, \ldots, n$ shows that $\phi_1, \ldots, \phi_{\hat{n}}$ is a basis of a G-module $V \subset K[U]$ containing $x_1 + I, \ldots, x_n + I$, as claimed.

In steps (5) & (6), an explicit description of the induced action of G on V is computed. Let $i \in \{1, \ldots, n\}$. We will first show that in (4.4) a polynomial R_i with the desired properties exists. Since G acts regularly on U, there exists $\mu^* : K[U] \longrightarrow K[G] \otimes_K K[U]$ such that $\mu^*(\phi_i)(\sigma) = \sigma^{-1}(\phi_i)$ for all $\sigma \in G$ (see Remark 4.19). Let $g_1 + (J), \ldots, g_s + (J) \in K[G]$, $a_1, \ldots, a_s \in K[U] \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ such that

$$\mu^*(\phi_i) = \sum_{j=1}^{s} (g_j + (J)) \otimes a_j.$$

We claim that $R_i := \sum_{j=1}^{s} g_j \cdot a_j \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ satisfies equation

(4.4) of step (6)(i). By (4.6), it follows

$$\sigma^{-1}(n_i + I) = n_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) \qquad \text{and}$$
$$\sigma^{-1}(d_i + I) = d_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma)$$

for all $\sigma \in G$. Since $\phi_i = (n_i + I)/(d_i + I)$ and $R_i(\sigma) = \sigma^{-1}(\phi_i)$ by construction, this implies that

$$n_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) - R_i(\sigma) \cdot d_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) = 0 \quad \text{for all } \sigma \in G$$

and hence

$$n_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right) - R_i \cdot d_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right) \in (J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]}.$$

This proves that a polynomial R_i satisfying (4.4) exists. We now show that conversely, every R_i satisfying equation (4.4) has the property that

$$\sigma^{-1}(\phi_i) = R_i(\sigma) \quad \text{for all } \sigma \in G. \tag{4.8}$$

This is not hard to see since by (4.4),

$$n_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) - R_i(\sigma) \cdot d_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) = 0$$

for all $\sigma \in G$. But this means that

$$R_i(\sigma) = n_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma)/d_i\left(\frac{\alpha(N_1)}{\alpha(D_1)}, \ldots, \frac{\alpha(N_n)}{\alpha(D_n)}\right)(\sigma) = \sigma^{-1}(\phi_i)$$

for all $\sigma \in G$, which we wanted to show.
Note that replacing R_i by its normal form $\mathrm{NF}_{\mathcal{G}}(R_i)$ in step (6)(ii) does not change the validity of (4.8).

A remark is in order about the existence of a solution $\alpha_{i1}, \ldots, \alpha_{i\hat{n}}$ of the equation in step (6)(iii). As R_i is in normal form with respect to $\mathcal{G}$, it can be shown similarly to the methods above that the coefficients of R_i as a polynomial in $\mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ span a G-module V_i containing ϕ_i. Furthermore, it is not hard to see that V_i is minimal in the sense that it is contained in every G-module containing ϕ_i. This implies that $V_i \subset \langle \phi_1, \ldots, \phi_{\hat{n}} \rangle_K$, and hence every coefficient of R_i can be expressed as a K-linear combination of $\phi_1, \ldots, \phi_{\hat{n}}$. Substituting these coefficients by the respective linear combinations of $\phi_1, \ldots, \phi_{\hat{n}}$ and rearranging the terms of R_i with respect to $\phi_1, \ldots, \phi_{\hat{n}}$ then yields the desired polynomials $\alpha_{i1}, \ldots, \alpha_{i\hat{n}} \in K[t_1, \ldots, t_m]$.

It follows by equation (4.8) that

$$\sigma^{-1}(\phi_i) = \sum_{j=1}^{\hat{n}} \alpha_{ij}(\sigma) \cdot \phi_j \quad \text{for all } \sigma \in G.$$

Recall that $\hat{N}_1 := \sum_{j=1}^{\hat{n}} \alpha_{1j}\hat{x}_j, \ldots, \hat{N}_{\hat{n}} := \sum_{j=1}^{\hat{n}} \alpha_{\hat{n}j}\hat{x}_j$. Let G act on $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ by

$$\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X},\ (\sigma, p) \longmapsto (\hat{N}_1(\sigma, p), \ldots, \hat{N}_{\hat{n}}(\sigma, p)).$$

Obviously, we have $K[\hat{X}] \cong K[\phi_1, \ldots, \phi_{\hat{n}}]$. More explicitly, this isomorphism is given by

$$\gamma : K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \longrightarrow K[\phi_1, \ldots, \phi_{\hat{n}}],\ \hat{x}_i \longmapsto \phi_i.$$

Note that by construction, this isomorphism commutes with the action of G. The proof of Proposition 4.20 now shows that the quasi-affine variety U is G-isomorphic to $\hat{U} := \hat{X} \setminus \mathrm{Var}_{\hat{X}}(\gamma^{-1}(((L+I)/I)_S))$ via $\phi = (\phi_1, \ldots, \phi_{\hat{n}}) : U \longrightarrow \hat{U}$.
Finally, observe that the isomorphism γ exactly maps $\hat{q}_i + \hat{I}$ to $q_i + I$ for $i = 1, \ldots, t$. Hence $\hat{U}$ is given by $\hat{X} \setminus \mathrm{Var}(\hat{L})$, as claimed. ∎

As an example, we demonstrate the application of the algorithm to the quasi-affine G-variety of Example 4.11(b).

Example 4.24. All computations in this example have been done with the computer algebra system Magma (cf. [BCP97]). Needless to say, before we can start with a concrete application of the algorithm to Example 4.11(b), we have to specify the input data adequately.
Recall that $K = \overline{\mathbb{Q}}$. Let $m = n = 1$. The finite group G can be realized as an algebraic group via the ideal $J := (t_1^2 - 1) \trianglelefteq K[t_1]$ where we assume that $1 \in \overline{\mathbb{Q}}$ corresponds to the neutral element 1_G of G. Set $I := (0) \trianglelefteq K[x_1]$ and $L := (x_1) \trianglelefteq K[x_1]$. Then $U = \overline{\mathbb{Q}} \setminus \{0\}$ is obviously given by $\mathrm{Var}(I) \setminus \mathrm{Var}(L)$.
Moreover, the action of G on U – as defined in Example 4.11(b) – can be described by the quotient N_1/D_1 where $N_1 := (1 + t_1) \cdot x_1^2 + 1 - t_1 \in K[t_1, x_1]$ and $D_1 := 2x_1 \in K[x_1]$. Hence according to Convention 4.16, the situation of Example 4.11(b) is given by $J \trianglelefteq K[t_1]$, $I, L \trianglelefteq K[x_1]$ and $N_1 \in K[x_1, t_1], D_1 \in K[x_1]$.
We can now apply the steps of Algorithm 4.22. Since J is a principal ideal, it follows that a Gröbner basis $\mathcal{G}$ of $(J)_{K(x_1)[t_1]}$ is given by the single generator $t_1^2 - 1$. Note that we do not have to specify a monomial order on the powers of t_1 since there is only one possibility for doing this. We have

$$\frac{\alpha(N_1)}{\alpha(D_1)} = \frac{(1 + t_1) \cdot x_1^2 + 1 - t_1}{2x_1} = \frac{x_1^2 - 1}{2x_1} \cdot t_1 + \frac{x_1^2 + 1}{2x_1}$$

and as the right hand side of this equation is already in reduced form with respect to $\mathcal{G}$, we can set $\phi_1 := 1/2 \cdot (x_1^2 - 1)/x_1$ and $\phi_2 := 1/2 \cdot (x_1^2 + 1)/x_1$.

It can be verified easily that

$$\sigma(\phi_1) = -\phi_1 \quad \text{and} \quad \sigma(\phi_2) = \phi_2.$$

By equation (4.8), it follows that we can set $R_1 := \phi_1 \cdot t_1$ and $R_2 := \phi_2$. Of course, the very same result about R_1 and R_2 can be achieved by executing step (6) of the algorithm. To be more explicit, applying the Extended Buchberger Algorithm to the ideal membership problem

$$\frac{1}{2} \cdot \left(\left(\frac{(1+t_1) \cdot x_1^2 + 1 - t_1}{2x_1} \right)^2 - 1 \right) \in \left(\frac{(1+t_1) \cdot x_1^2 + 1 - t_1}{2x_1}, t_1^2 - 1 \right)_{K(x_1)[t_1]}$$

yields (as described in Remark 4.23(c))

$$\begin{aligned} R_1 = {} & \frac{-x_1^6 + 3x_1^4 - 3x_1^2 + 1}{16x_1^3} \cdot t_1^3 + \frac{-x_1^6 + x_1^4 + x_1^2 - 1}{16x_1^3} \cdot t_1^2 \\ & + \frac{x_1^6 + 5x_1^4 - 5x_1^2 - 1}{16x_1^3} \cdot t_1 + \frac{x_1^6 - x_1^4 - x_1^2 + 1}{16x_1^3} \end{aligned}$$

The normal form of R_1 with respect to $\mathcal{G}$ is $1/2 \cdot (x_1^2 - 1)/x_1 \cdot t_1$. By step (6)(iii), this means $R_1 := \phi_1 \cdot t_1$, as expected. An analogous computation for ϕ_2 shows that $R_2 = \phi_2$. Finally, a simple application of the methods as outlined in Remarks 4.23(d) & (e) gives

$$\hat{I} := (\hat{x}_1^2 - \hat{x}_2^2 + 1) \trianglelefteq K[\hat{x}_1, \hat{x}_2]$$

and $\hat{q}_1 = \hat{x}_1 + \hat{x}_2 \in K[\hat{x}_1, \hat{x}_2]$. Thus $\hat{L}$ is given by

$$\hat{L} := (\hat{x}_1 + \hat{x}_2) \trianglelefteq K[\hat{x}_1, \hat{x}_2].$$

To sum this up, we have found an affine variety $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^2$ together with a regular G-action

$$\mu : G \times \hat{X} \longrightarrow \hat{X},\ (\sigma, (\hat{\xi}_1, \hat{\xi}_2)) \longmapsto (-\hat{\xi}_1, \hat{\xi}_2).$$

Note that $\mathrm{Var}(\hat{L}) \cap \hat{X} = \emptyset$ which implies that $\hat{U} = \hat{X}$. By construction, U is G-isomorphic to $\hat{U} = \hat{X}$ and this isomorphism is given by

$$U \longrightarrow \hat{U},\ \xi \longmapsto \left(\frac{\xi^2 - 1}{2\xi}, \frac{\xi^2 + 1}{2\xi} \right). \qquad \triangleleft$$

4.3 Algorithms for computing invariants of group actions on quasi-affine varieties

With the same notation as in the previous section, let G be a linear algebraic group and U be an irreducible quasi-affine G-variety. Our aim is to compute the invariant ring $K[U]^G$.

If the ring of regular functions $K[U]$ is finitely generated, this can be reduced to the affine case, where several algorithms are known. The actual problem is that in most of the cases, it is not known whether $K[U]$ is finitely generated or not. Up to now – to the best of my knowledge – there is no method to decide this algorithmically. For the computation of $K[U]^G$, it is therefore necessary to give an algorithm which does not involve any steps which depend on questions about finite generation of $K[U]$.

It is clear that the invariant ring $K[U]^G$ is not always finitely generated. However, we can deal with non-finitely generated invariant rings similarly as in the affine case. As before, our algorithms terminate with a finite generating set of $K[U]^G$ if and only if $K[U]^G$ is finitely generated. Otherwise they return an infinite sequence $f_1, f_2, f_3, \ldots \in K[U]$ which generate $K[U]^G$ in the usual sense.

We start with the examination of an important class of quasi-affine varieties and show that their rings of regular functions are always finitely generated. In particular, this means that for quasi-affine varieties of this type, invariant rings can be calculated with the computational methods known from the affine case. Next, we try to compute invariant rings (for arbitrary quasi-affine varieties) with a quite naive approach. It turns out that this leads to an algorithm for the computation of invariant rings for finite groups and in some cases also for reductive groups. We then develop an algorithm for computing invariants of unipotent groups acting on quasi-affine varieties. For the special case that G acts on a normal quasi-affine variety, a variant of this algorithm will be given. Interestingly enough, the theory which comes out of this construction enables us to generalize a result of Nagata and Winkelmann. Finally, we conclude this section with an outline of how computational methods for the quasi-affine case can be used for the computation of invariants of arbitrary linear algebraic groups acting on factorial varieties.

4.3.1 An algorithm for computing invariants of groups acting on open subsets of factorial varieties

In this subsection, we do not develop new algorithms for the computation of invariant rings in the quasi-affine case, but show that for a certain class of quasi-affine varieties the ring of regular functions is always finitely generated. For these quasi-affine varieties we thus can calculate invariant rings with the existing algorithms for affine varieties, as we will see below.

Recall that an irreducible affine variety X is called **factorial** if the coordinate ring $K[X]$ is a unique factorization domain. An important example for the occurrence of factorial varieties is the common case that X is a finite-dimensional K-vector space.

Theorem 4.25. *Let U be an open subset of a factorial variety X. Then $K[U]$ is a finitely generated K-algebra.*

Proof. We may assume that $U \neq X$. Let M be the finite set of all prime ideals of $K[X]$ which are minimal over $\widetilde{L} := \mathrm{Id}_{K[X]}(X \setminus U)$. Then $\widetilde{L} = \bigcap_{\mathfrak{p} \in M} \mathfrak{p}$ is the (unique) minimal

decomposition of $\widetilde{L}$ into distinct primes (see [Eis95], Chapter 3). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be those primes of M which are of height one and set $L' := \bigcap_{i=1}^{s} \mathfrak{p}_i$. (In case that there are no primes of height one in M, set $L' := K[X]$.) We claim that

$$(K[X] : \widetilde{L}^{\infty})_{\mathrm{Quot}(K[X])} = (K[X] : L'^{\infty})_{\mathrm{Quot}(K[X])}. \tag{4.9}$$

By (4.1), this means that the rings of regular functions of the quasi-affine varieties U and $U' := X \setminus \mathrm{Var}_X(L')$ are isomorphic.
Since $\widetilde{L} \subset L'$, it is clear that the right hand side of (4.9) is contained in the left hand side. For the reverse inclusion, let $a/b \in (K[X] : \widetilde{L}^{\infty})_{\mathrm{Quot}(K[X])}$. By definition, there is an $m \in \mathbb{N}_0$ such that $(a/b) \cdot (\widetilde{L})^m \subset K[X]$. We have to show that there exists $m' \in \mathbb{N}_0$ such that $(a/b) \cdot (L')^{m'} \subset K[X]$. The coordinate ring $K[X]$ is factorial, hence normal (see [Eis95], Chapter 4, Proposition 4.10) and thus $K[X]$ is the intersection of its localizations at primes of height one (see [Eis95], Chapter 11, Corollary 11.4), i. e.

$$K[X] = \bigcap_{\substack{\mathfrak{p} \trianglelefteq K[X] \text{ prime} \\ \mathrm{height}(\mathfrak{p})=1}} K[X]_{\mathfrak{p}}.$$

So it is enough to show that there exists $m' \in \mathbb{N}_0$ such that $(a/b) \cdot (L')^{m'} \subset K[X]_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of $K[X]$ of height one.
We first prove that $a/b \in K[X]_{\mathfrak{p}}$ for all height one prime ideals $\mathfrak{p}$ with $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. So let $\mathfrak{p}$ be a prime ideal of $K[X]$ of height one which is not contained in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Then there exists $l \in \widetilde{L} \setminus \mathfrak{p}$ and it follows that $(a/b) \cdot l^m \in K[X]$. But this means that $a/b = ((a/b) \cdot l^m)/l^m \in K[X]_{\mathfrak{p}}$.
Let now $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Since $K[X]$ is normal, it follows that $K[X]_{\mathfrak{p}}$ is a discrete valuation ring (see [Eis95], Chapter 11, Theorem 11.2). In particular, the maximal ideal $\mathfrak{p}_{\mathfrak{p}} \trianglelefteq K[X]_{\mathfrak{p}}$ is a principal ideal, $\mathfrak{p}_{\mathfrak{p}} = (r_{\mathfrak{p}})_{K[X]_{\mathfrak{p}}}$ with $r_{\mathfrak{p}} \in K[X]$, say.
We can write a/b as $a/b = r_{\mathfrak{p}}^l \cdot q'$ with $l \in \mathbb{Z}$ and $q' \in K[X]_{\mathfrak{p}}^{\times}$. In case that $l \geq 0$, it follows that $a/b \in K[X]_{\mathfrak{p}}$. In case that $l < 0$ we have

$$\begin{aligned}(a/b) \cdot (L')^{-l} \subset (a/b) \cdot (L'_{\mathfrak{p}})^{-l} \subset (a/b) \cdot \mathfrak{p}_{\mathfrak{p}}^{-l} &= (a/b) \cdot r_{\mathfrak{p}}^{-l} \cdot K[X]_{\mathfrak{p}} \\ &= r_{\mathfrak{p}}^{l} \cdot r_{\mathfrak{p}}^{-l} \cdot K[X]_{\mathfrak{p}} = K[X]_{\mathfrak{p}}.\end{aligned}$$

Since $\mathfrak{p}$ was chosen arbitrarily among $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, it follows that there exists $m' \in \mathbb{N}_0$ such that $(a/b) \cdot (L')^{m'} \subset K[X]_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of $K[X]$ of height one. Hence equation (4.9) is proved.

If $L' = K[X]$, then $K[U'] = K[X]$ is obviously finitely generated. Otherwise, note that by construction, the ideal $L' \trianglelefteq K[X]$ is the intersection of the height one prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Since every height one prime ideal of a unique factorization domain is principal (see [Eis95], Chapter 10, Corollary 10.6), there exist prime elements $p_1, \ldots, p_s \in K[X]$ such that $\mathfrak{p}_i = (p_i)_{K[X]}$ for $i = 1, \ldots, s$. By construction, the prime elements $p_1, \ldots, p_s$ are pairwise coprime and it follows that $L' = (\prod_{i=1}^{s} p_i)_{K[X]}$. Hence the ring of regular functions of U' is given by the localization $K[U'] = K[X]_{\prod_{i=1}^{s} p_i}$. In particular, $K[U']$ is finitely generated. Combining this with (4.9) proves the theorem. ∎

Remark 4.26. From the previous proof, the following useful fact about normal varieties can be extracted: Let X be a normal affine variety and let $\widetilde{L} \trianglelefteq K[X]$ be a non-zero ideal. Then every function which is regular on $X \setminus \mathrm{Var}_X(\widetilde{L})$ can be extended to a function which is regular on the complement of the codimension one components of $\mathrm{Var}_X(\widetilde{L})$.
By symmetry, it follows that if $\bar{L} \trianglelefteq K[X]$ is another non-zero ideal such that the set of all primes of height one which are minimal over $\bar{L}$ is equal to the set of all primes of height one which are minimal over $\widetilde{L}$, then

$$(K[X] : \widetilde{L}^\infty)_{\mathrm{Quot}(K[X])} = (K[X] : \bar{L}^\infty)_{\mathrm{Quot}(K[X])}.$$

In other words, the rings of regular functions of the quasi-affine varieties $X \setminus \mathrm{Var}_X(\widetilde{L})$ and $X \setminus \mathrm{Var}_X(\bar{L})$ are isomorphic. ♢

As mentioned in the outline above, the previous theorem enables us to compute the invariant ring of certain classes of groups acting on open subsets of factorial varieties.

Theorem 4.27. *Let U be an open subset of the factorial variety X and let the linear algebraic group G act regularly on U. Then there is an algorithm for the computation of $K[U]^G$ for the case that*

(a) G is a finite group.

(b) G is a reductive group.

(c) G is a unipotent group.

The rough idea for proving this theorem is as follows. Since $K[U]$ is an affine algebra, there exists an affine variety $\hat{X}$ such that the coordinate ring $K[\hat{X}]$ is isomorphic to $K[U]$. Moreover, the action of G on $K[U]$ can be described by $\tilde{\mu} : K[U] \longrightarrow K[G] \otimes_K K[U]$ (see Proposition 4.20) and hence the isomorphism of $K[U]$ and $K[\hat{X}]$ induces an action $K[\hat{X}] \longrightarrow K[G] \otimes_K K[\hat{X}]$ of G on $K[\hat{X}]$. By Proposition 1.29, this in turn comes from a regular action of G on the affine variety $\hat{X}$. We can therefore apply the algorithms which are known for affine varieties.
The unsatisfactory part of this argumentation is the fact that it is purely algebraic – in general, it is not clear, how the geometry of the affine G-variety $\hat{X}$ is related to the geometry of the quasi-affine G-variety U. In the following, we therefore present a geometric version of this construction which clarifies the relation of $\hat{X}$ and U better. For this, we need the following result about quasi-affine G-varieties with a finitely generated ring of regular functions.

Proposition 4.28. *Let U be an irreducible quasi-affine variety such that the ring of regular functions $K[U]$ is finitely generated (as a K-algebra). Moreover, let the linear algebraic group G act regularly on U. Then there is an irreducible affine G-variety $\hat{X}$ and a G-equivariant embedding of U as an open subset in $\hat{X}$ such that every regular function on*

U can be extended to a regular function on $\hat{X}$. In fact, every invariant regular function on U can be extended to an invariant regular function on $\hat{X}$.

Remark. Note that the algebras $K[\hat{U}]$ and $K[\hat{X}]$ of the proposition are G-isomorphic, as intended. ♢

Proof. By Proposition 4.20, the quasi-affine variety U can be embedded G-equivariantly as an open subset in an irreducible affine G-variety $\hat{X}$. Moreover, by Remark 4.21(b), $\hat{X}$ can be chosen in such a way that $K[\hat{X}] = K[U]$. In other words this means that every function which is regular on U can be extended to a regular function on $\hat{X}$. Finally, since G acts on $K[U]$ in the very same way as on $K[\hat{X}] = K[U]$, it follows that every invariant of $K[U]$ is an invariant of $K[\hat{X}]$. ∎

Proof (of Theorem 4.27). By Theorem 4.25, the ring of regular functions $K[U]$ is finitely generated. Moreover, by Proposition 4.28, there exists an affine G-variety $\hat{X}$ such that $K[\hat{X}]$ is G-isomorphic to $K[U]$. We will see below that the construction of $\hat{X}$ can be done algorithmically.
This proves the theorem since algorithms are known for the calculation of the invariant ring $K[\hat{X}]^G$ if G is contained in one of the classes listed under (a), (b) and (c). For details, see [Kem96], [Der99], [DK02], [Kem03] and Chapter 3 above. ∎

To complete the previous proof, we give an algorithm which makes the proof of Proposition 4.28 constructive. By construction, this algorithm can be applied to all quasi-affine varieties U where $K[U]$ is finitely generated. So in particular, it is applicable to the case considered above where U is an open subset of a factorial variety.

Algorithm 4.29. (Embedding a quasi-affine G-variety G-equivariantly in an affine G-variety such that the respective rings of regular functions are G-isomorphic)

Input: A linear algebraic group G, an irreducible quasi-affine variety U such that $K[U]$ is finitely generated, and a regular action μ of G on U according to Convention 4.16.

Output: An irreducible affine variety $\hat{X}$, an action $\hat{\mu}$ of G on $\hat{X}$ and a G-equivariant embedding $\phi : U \longrightarrow \hat{X}$ of U as an open subset in $\hat{X}$ such that ϕ induces a G-isomorphism $K[\hat{X}] \longrightarrow K[U]$.
More precisely, the output is given by a prime ideal $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ (with $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ new indeterminates), polynomials $\hat{N}_1, \ldots, \hat{N}_{\hat{n}} \in K[t_1, \ldots, t_m, \hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ and rational functions $\phi_1, \ldots, \phi_{\hat{n}} \in K[U] \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ which stand for the following: The group G acts on $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ via $\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X}$, where $\hat{\mu}$ is defined by

$$\hat{\mu}(v) = (\hat{N}_1(v), \ldots, \hat{N}_{\hat{n}}(v))$$

for all $v \in G \times \hat{X}$. Moreover, the morphism $\phi : U \longrightarrow \hat{X}$ is given by $(\phi_1, \ldots, \phi_{\hat{n}})$ in the sense that $\phi(u) = (\phi_1(u), \ldots, \phi_{\hat{n}}(u))$ for all $u \in U$.

(1) Compute generators

$$\frac{a_1 + I}{b_1 + I}, \ldots, \frac{a_s + I}{b_s + I} \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$$

of the algebra $(K[x_1, \ldots, x_n]/I : ((L + I)/I)^\infty)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)}$.
(For details, see [DK08], Algorithms 2.6 and 2.7)

(2) Compute a Gröbner basis $\mathcal{G}$ of the ideal $(J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]}$ with respect to an arbitrary monomial order on $t_1, \ldots, t_m$.

(3) Let α be the natural homomorphism

$$\alpha : K[t_1, \ldots, t_m, x_1, \ldots, x_n] \longrightarrow \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m].$$

(4) For $i = 1, \ldots, s$:
   (i) Find $H_i \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ such that

$$a_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) - H_i \cdot b_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) \in (J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]} \tag{4.10}$$

   (For details, see Remarks 4.23(c))
   (ii) Replace H_i by $\mathrm{NF}_{\mathcal{G}}(H_i)$.

(5) Let $C \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ be the set of coefficients occuring in the polynomials $H_1, \ldots, H_s$.

(6) Choose a maximal K-linearly independent subset of C, say $\{\phi_1, \ldots, \phi_{\hat{n}}\}$.

(7) Let $n_1, \ldots, n_{\hat{n}}, d_1, \ldots, d_{\hat{n}} \in K[x_1, \ldots, x_n]$ such that

$$\phi_1 = \frac{n_1 + I}{d_1 + I}, \ldots, \phi_{\hat{n}} = \frac{n_{\hat{n}} + I}{d_{\hat{n}} + I}$$

(8) For $i = 1, \ldots, \hat{n}$:
   (i) Find $R_i \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ such that

$$n_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) - R_i \cdot d_i(\alpha(N_1)/\alpha(D_1), \ldots, \alpha(N_n)/\alpha(D_n)) \in (J)_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)[t_1,\ldots,t_m]} \tag{4.11}$$

   (For details, see Remarks 4.23(c))

(ii) Replace R_i by $\mathrm{NF}_{\mathcal{G}}(R_i)$.
(iii) Find $\alpha_{i1}, \ldots, \alpha_{i\hat{n}} \in K[t_1, \ldots, t_m]$ such that

$$R_i = \sum_{j=1}^{\hat{n}} \alpha_{ij}\phi_j.$$

(9) Compute the ideal of relations of $\phi_1, \ldots, \phi_{\hat{n}}$ over K, say $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$. (For details, see Remarks 4.23(d))

(10) Set $\hat{N}_1 := \sum_{j=1}^{\hat{n}} \alpha_{1j}\hat{x}_j, \ldots, \hat{N}_{\hat{n}} := \sum_{j=1}^{\hat{n}} \alpha_{\hat{n}j}\hat{x}_j$.

(11) Return $\hat{I}, (\hat{N}_1, \ldots, \hat{N}_{\hat{n}}), (\phi_1, \ldots, \phi_{\hat{n}})$.

Remarks. (1) The homomorphism $K[\hat{X}] \longrightarrow K[U]$ which is induced by ϕ can be given explicitly as

$$\beta : K[\hat{X}] \longrightarrow K[U],\ \hat{x}_i + \hat{I} \longmapsto \phi_i.$$

By the specification of the algorithm, β is a G-isomorphism.

(2) This algorithm can be streamlined to a shorter version. Nonetheless, we have tried to reuse as much code from Algorithm 4.22 as possible – on the one hand to make it easier for the reader being already familiar with Algorithm 4.22, on the other hand to be able to reuse parts of the proof of correctness of Algorithm 4.22.

Proof of Correctness (Sketch). As mentioned in the remark above, this algorithm uses the same ideas and constructions as Algorithm 4.22. We therefore only sketch the following proof.
By (4.1), the ring of regular functions on U is given by

$$K[U] = (K[x_1, \ldots, x_n]/I : ((L + I)/I)^{\infty})_{\mathrm{Quot}(K[x_1,\ldots,x_n]/I)}.$$

Hence the elements $(a_1 + I)/(b_1 + I), \ldots, (a_s + I)/(b_s + I)$ of step (1) are just generators of $K[U]$ (which is finitely generated by assumption).
In steps (2)-(6), a basis $\phi_1, \ldots, \phi_{\hat{n}}$ of a G-module $V \subset K[U]$ is computed such that

$$\frac{a_1 + I}{b_1 + I}, \ldots, \frac{a_s + I}{b_s + I} \in V.$$

Note first that a polynomial $H_i \in \mathrm{Quot}(K[x_1, \ldots, x_n]/I)[t_1, \ldots, t_m]$ satisfies (4.10) if and only if

$$H_i(\sigma) = \sigma^{-1}\left(\frac{a_i + I}{b_i + I}\right) \qquad \text{for all } \sigma \in G. \tag{4.12}$$

A proof for this can be carried over almost word by word from the discussion around (4.8) of the proof of Algorithm 4.22. (Simply replace a_i by n_i, b_i by d_i and R_i by H_i.) Moreover,

it is clear by the very same proof that a polynomial H_i with property (4.12) always exists. The coefficients of H_i (in reduced form) span a G-module which contains $(a_i + I)/(b_i + I)$. This has been proven for similar cases in Proposition 1.31(a) and Algorithm 4.22 and will not be repeated here. Therefore, a linear independent subset of the coefficients of $H_1, \ldots, H_s$ – that is $\phi_1, \ldots, \phi_{\hat{n}}$ – is a basis of a G-module $V \subset K[U]$ with $(a_1 + I)/(b_1 + I), \ldots, (a_s + I)/(b_s + I) \in V$, as claimed. Note that in particular, $K[U]$ is generated by $\phi_1, \ldots, \phi_{\hat{n}}$.
By the specification of the algorithm, we have to construct an affine variety $\hat{X} \subset K^{\hat{n}}$ together with a regular action of G on $\hat{X}$ such that U can be embedded G-equivariantly as an open subset in $\hat{X}$ and moreover, every function which is regular on U can be extended to a regular function on $\hat{X}$. The embedding of U in an irreducible affine variety $\hat{X}$ is done in steps (7)-(11). These steps are almost identical to the steps (6)-(10) of Algorithm 4.22 and the respective parts of the proof given for Algorithm 4.22 apply here, too. By construction, we have $K[\hat{X}] \cong K[\phi_1, \ldots, \phi_{\hat{n}}] = K[U]$. Hence every regular function on U extends to a regular function on $\hat{X}$, indeed. ∎

Before we have a closer look at finite group actions on quasi-affine varieties, we give an example for the application of the methods which have been developed in this section.

Example 4.30. Let $K = \overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and let $X = K^2$ be the two-dimensional affine space over K. Apparently, X is a factorial variety. Moreover, let U be the open subset $X \setminus \mathrm{Var}(x_1(x_1 - 1), x_1x_2)$ where as usual x_1, x_2 denote the coordinate functions on K^2. The cyclic group with two elements, $G = \langle\sigma\rangle$, acts on U via

$$\sigma(\xi_1, \xi_2) := (1/\xi_1, \xi_2) \quad \text{for all } (\xi_1, \xi_2) \in U.$$

Our aim is to compute generators of the invariant ring $K[U]^G$. As indicated above, we do this by first invoking Algorithm 4.29, thereby realizing $K[U]$ as the coordinate ring of an affine G-variety. After that we can apply one of Kemper's algorithms for the computation of invariant rings of finite groups to this well-understood affine situation.
The interesting part of this action is the fact that U is a quasi-affine variety which is not isomorphic to an affine variety. Hence the existing algorithms in invariant theory cannot be applied here. Moreover, the action of G on U does not extend to an action of G on X.
A remark is in order about the non-affineness of U. It can be seen without difficulties (for example with Algorithms 2.6 & 2.7 of [DK08]) that $K[U]$ is given by

$$K[U] = K\left[x_1, x_2, \frac{1}{x_1}\right].$$

Consider the ideal $(x_1 - 1, x_2) \trianglelefteq K[U]$. Obviously, it is proper. But $\mathrm{Var}_U(x_1 - 1, x_2) = \emptyset$ and therefore U cannot be isomorphic to an affine variety (see [Har77], Chapter I, Theorem 3.2).
In addition to the non-affineness of U, we have claimed above that the action of G on U does not extend to a regular action of G on X. To see this, consider the automorphism $\mu(\sigma, -) : U \longrightarrow U$. Then $|\mu(\sigma, -)|$ (where $|\cdot|$ denotes the usual norm in the complex

numbers) is not bounded on $\mathcal{O} \cap K^2$ where $\mathcal{O}$ is any open neighbourhood of $(0,0)$ in the usual topology of $\overline{\mathbb{Q}}^2$. Therefore $\mu(\sigma, -)$ cannot be regular at $(0,0)$. In particular, the action of G on U cannot be the restriction of a regular action of G on X.
Before we can start with an application of Algorithm 4.29 to this example, we have to specify the input data appropriately. In accordance to Convention 4.16, it can be given by $n := 2, m := 1, J := (t_1^2 - 1) \trianglelefteq K[t_1], I := (0) \trianglelefteq K[x_1, x_2], L := (x_1(x_1 - 1), x_1 x_2) \trianglelefteq K[x_1, x_2]$ and $\mu := (N_1/D_1, N_2/D_2)$ where $N_1 := (1 + t_1) \cdot x_1^2 + 1 - t_1 \in K[t_1, x_1, x_2], D_1 := 2x_1 \in K[x_1, x_2], N_2 := x_2 \in K[t_1, x_1, x_2]$ and $D_2 := 1 \in K[x_1, x_2]$.
As we have remarked above, the ring of regular functions on U is given by $K[U] = (K[x_1, x_2] : (x_1(x_1 - 1), x_1 x_2)^\infty)_{K(x_1, x_2)} = K[x_1, x_2, 1/x_1]$. We therefore define $s := 3$ and

$$a_1 := x_1, b_1 := 1,\ a_2 := x_2, b_2 := 1,\ a_3 := 1, b_3 := x_1.$$

Next, a Gröbner basis of $(J)_{K(x_1,x_2)[t_1]}$ with respect to the unique monomial ordering on the powers of t_1 is given by $\mathcal{G} = \{t_1^2 - 1\}$. Since $b_1 = b_2 = 1$, we can set

$$H_1 := 1/2 \cdot ((1 + t_1) \cdot x_1^2 + 1 - t_1)/x_1 = \frac{x_1^2 - 1}{2x_1} \cdot t_1 + \frac{x_1^2 + 1}{2x_1} \quad \text{and}$$
$$H_2 := x_2.$$

Moreover by (4.12), H_3 can be set to

$$H_3 := \frac{-x_1^2 + 1}{2x_1} \cdot t_1 + \frac{x_1^2 + 1}{2x_1}.$$

(Recall that this is because $H_3(1) = 1/x_1$ and $H_3(-1) = x_1$.) Note that H_1, H_2 and H_3 are in normal form with respect to $\mathcal{G}$. Hence we define

$$\phi_1 := \frac{x_1^2 - 1}{2x_1}, \phi_2 := \frac{x_1^2 + 1}{2x_1}, \phi_3 := x_2.$$

Since $\sigma(\phi_1) = -\phi_1$, $\sigma(\phi_2) = \phi_2$ and $\sigma(\phi_3) = \phi_3$, we can set

$$R_1 := \phi_1 \cdot t_1,\ R_2 := \phi_2,\ R_3 := \phi_3.$$

Finally, a simple application of the methods as outlined in Remark 4.23(d) gives

$$\hat{I} := (\hat{x}_1^2 - \hat{x}_2^2 + 1) \trianglelefteq K[\hat{x}_1, \hat{x}_2, \hat{x}_3].$$

To sum this up, Algorithm 4.29 has returned an affine variety $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^3$ together with a regular G-action

$$\mu : G \times \hat{X} \longrightarrow \hat{X},\ (\sigma, (\hat{\xi}_1, \hat{\xi}_2, \hat{\xi}_3)) \longmapsto (-\hat{\xi}_1, \hat{\xi}_2, \hat{\xi}_3).$$

Moreover, the quasi-affine variety U can be embedded G-equivariantly in $\hat{X}$ via (ϕ_1, ϕ_2, ϕ_3)

and $K[\hat{X}]$ is G-isomorphic to $K[U]$ via

$$\beta : K[\hat{X}] \longrightarrow K[U],\ \hat{x}_i \longmapsto \phi_i \quad \text{for } i = 1, 2, 3.$$

But now $K[\hat{X}]^G$ can be seen to be equal to $K[\hat{x}_1^2+\hat{I}, \hat{x}_2+\hat{I}, \hat{x}_3+\hat{I}]/\hat{I}$. (For more complicated situations where the invariant ring cannot be "seen", there are a lot of computational methods for calculating $K[\hat{X}]^G$, see for example [Stu93], [Kem96], [Der99], [Kem03] and [DK02].) Translating this back to $K[U]$ via the isomorphism β finally yields

$$K[U]^G = K\left[\frac{(x_1^2-1)^2}{4x_1^2}, \frac{x_1^2+1}{2x_1}, x_2\right]. \qquad \lhd$$

4.3.2 An algorithm for computing invariants of finite groups acting on quasi-affine varieties

Let X be an irreducible affine variety, let $U \subset X$ be a non-empty open subset and let the linear algebraic group G act regularly on U. For the moment, G does not have to be a finite group. By Proposition 4.20, we may assume for the subsequent discussion that the action of G on U extends to a regular action of G on X.
Let $L' \trianglelefteq K[X]$ be any ideal such that $U = X \setminus \mathrm{Var}_X(L')$. By (4.1), the ring of regular functions on U is given by

$$K[U] = (K[X] : (L')^\infty)_{\mathrm{Quot}(K[X])}.$$

If – up to taking radicals – the ideal L' is generated by invariants, then the invariant ring $K[U]^G$ can be written as a colon expression quite easily. More precisely*,

$$\begin{aligned} &\sqrt{(L'^{\,G})_{K[X]}} = \sqrt{L'} \Longrightarrow \\ &\qquad \big((K[X] : (L')^\infty)_{\mathrm{Quot}(K[X])}\big)^G = (K[X]^G : (L'^{\,G})^\infty)_{\mathrm{Quot}(K[X]^G)}. \end{aligned} \tag{4.13}$$

We first show that the left hand side of this last equation is contained in the right hand side. Let $a/b \in \big((K[X] : (L')^\infty)_{\mathrm{Quot}(K[X])}\big)^G$. By definition, there exists $m \in \mathbb{N}$ such that $a/b \cdot (L')^m \subset K[X]$. But then obviously $a/b \cdot (L'^{\,G})^m \subset K[X]^G$ and moreover, it follows that a/b is contained in $\mathrm{Quot}(K[X]^G)$.
For the reverse inclusion, let $a/b \in (K[X]^G : (L'^{\,G})^\infty)_{\mathrm{Quot}(K[X]^G)}$. By definition, there exists $m \in \mathbb{N}$ such that $(a/b) \cdot (L'^{\,G})^m \subset K[X]^G$. It follows that $a/b \cdot ((L'^{\,G})_{K[X]})^m \subset K[X]$. Moreover, since $\sqrt{(L'^{\,G})_{K[X]}} = \sqrt{L'}$, there exists $m' \in \mathbb{N}$ such that $(L')^{m'} \subset (L'^{\,G})_{K[X]}$. This implies that $a/b \cdot (L')^{m \cdot m'} \subset K[X]$ and hence a/b is contained in $\big((K[X] : (L')^\infty)_{\mathrm{Quot}(K[X])}\big)^G$.

It is very tempting to guess that the equation in (4.13) can even be deduced if only

*We write $L'^{\,G}$ for $L' \cap K[X]^G$.

$L'^{G} \neq \{0\}$. This would be nice, since for example for G unipotent this is always the case. But this is not true as the following example shows.

Example 4.31. Let $K := \overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$, let $X := K^2$ and let $U := X \setminus \{(0,1)\}$. With the above notation, we can set $L' := (x_1, x_2 - 1) \trianglelefteq K[x_1, x_2]$ where x_1, x_2 denote the coordinate functions on K^2. A regular action of the additive group $G_a = (K, +)$ on X is given by

$$\lambda(\xi_1, \xi_2) := (\xi_1, \xi_2 + \lambda\xi_1).$$

Since the point $(0,1)$ is a fixed point, this induces an action of G_a on the quasi-affine variety U. The invariant ring $K[X]^G$ is given by $K[X]^G = K[x_1]$ which can be seen for example from the orbit structure of the G-action on X: the orbits are just the x_1-translates of the x_2-axis together with all the points on the x_2-axis.
Since X is normal and $(0,1)$ has codimension 2 in X, it follows that $K[U] = K[X]$ (see [Eis95], Chapter 11, Corollary 11.4) and hence $K[U]^G = K[X]^G$.
In contrary to the guess preceding this example, we have the inequality

$$\begin{aligned} K[U]^G &= K[x_1] \\ &\neq (K[x_1] : ((x_1, x_2 - 1)_{K[x_1,x_2]} \cap K[x_1])^\infty)_{\mathrm{Quot}(K[x_1])} = (K[X]^G : (L'^{G})^\infty)_{\mathrm{Quot}(K[X]^G)}, \end{aligned}$$

which is not very hard to see, since for example $1/x_1$ is certainly not regular on U but is contained in $(K[x_1] : ((x_1, x_2 - 1)_{K[x_1,x_2]} \cap K[x_1])^\infty)_{\mathrm{Quot}(K[x_1])}$. ◁

In the following, we will show that (4.13) can be used to compute invariant rings of finite groups. For this, we need the following well-known result about separation of orbits.

Theorem 4.32. *Let X be an affine variety and assume that the finite group G acts regularly on X. Then all orbits of G can be separated by invariants, i. e. if $p, p' \in X$ and $f(p) = f(p')$ for all $f \in K[X]^G$, then there exists $\sigma \in G$ such that $p = \sigma(p')$.*

Proof. Let $p, p' \in X$ with $G(p) := \{\sigma(p);\ \sigma \in G\} \neq G(p') := \{\sigma(p');\ \sigma \in G\}$. We will show that there exists $f \in K[X]^G$ with $f(p) \neq f(p')$. Choose for each $q \in G(p')$ a regular function $f_q \in K[X]$ such that

$$f_q(G(p) \cup G(p') \setminus \{q\}) = \{0\} \text{ and } f_q(q) \neq 0.$$

Note that such a function exists since the finite set $G(p) \cup G(p') \setminus \{q\}$ is closed in the Zariski topology. Set

$$f := \prod_{\sigma \in G} \sigma \left(\sum_{q \in G(p')} f_q \right).$$

Each factor of the expression above vanishes on $G(p)$ and does not vanish on any point of $G(p')$, hence this is also true for f. Moreover, f is invariant under G. ∎

Proposition 4.33. *Let X be an irreducible affine variety, $U \subset X$ be a non-empty open subset and assume that the finite group G acts regularly on the quasi-affine variety U. Then there exists an affine algebra S with $S \subset K[U]^G$ and an ideal $\mathfrak{a} \trianglelefteq S$ of S such that the invariant ring $K[U]^G$ is given by*

$$K[U]^G = (S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)}.$$

In particular, this shows that the invariant ring of a finite group acting on an irreducible quasi-affine variety is isomorphic to the ring of regular functions of a quasi-affine variety.

Proof. By Proposition 4.20, there is an irreducible affine G-variety $\hat{X}$ such that U is G-isomorphic to an open G-stable subset $\hat{U}$ of $\hat{X}$. Let $L' \trianglelefteq K[\hat{X}]$ be any ideal such that $\hat{U} = \hat{X} \setminus \mathrm{Var}_{\hat{X}}(L')$. We first prove that

$$K[\hat{U}]^G = (K[\hat{X}]^G : (L'^G)^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)}. \tag{4.14}$$

Note that by (4.13), for this it is enough to show that

$$\sqrt{(L'^G)_{K[\hat{X}]}} = \sqrt{L'}.$$

Clearly the left hand side of this latter equation is contained in the right hand side. For the reverse inclusion, let $\mathfrak{m}$ be a maximal ideal of $K[\hat{X}]$ with $\mathfrak{m} \supset (L'^G)_{K[\hat{X}]}$. The ring $K[\hat{X}]$ is integral over $K[\hat{X}]^G$, since every $f \in K[\hat{X}]$ satisfies a monic polynomial with coefficients in $K[\hat{X}]^G$. This polynomial can be given explicitly by

$$F_f := \prod_{\sigma \in G} \sigma(T - f) \in K[\hat{X}]^G[T]$$

where T is an indeterminate over $K[\hat{X}]$ and G acts trivially on T. Hence by the Lying Over Theorem (see [Eis95], Chapter 4, Proposition 4.15), there exists a prime ideal $\mathfrak{m}' \trianglelefteq K[\hat{X}]$ with $\mathfrak{m}' \supset L'$ and $\mathfrak{m}' \cap K[\hat{X}]^G = \mathfrak{m} \cap K[\hat{X}]^G$. We may assume that $\mathfrak{m}'$ is a maximal ideal of $K[\hat{X}]$. Both $\mathfrak{m}$ and $\mathfrak{m}'$ correspond to a point on the affine variety $\hat{X}$. Since $\mathfrak{m}^G = (\mathfrak{m}')^G$, these two points cannot be separated by invariants. Hence, by the previous theorem, there exists $\sigma \in G$ with $\mathfrak{m} = \sigma(\mathfrak{m}')$. Note that by the G-stability of $\hat{U}$, the ideal $\sqrt{L'} = \mathrm{Id}_{K[\hat{X}]}(\hat{X} \setminus \hat{U})$ is G-stable. It follows that $\mathfrak{m} = \sigma(\mathfrak{m}') \supset \sigma(\sqrt{L'}) = \sqrt{L'}$.
As the maximal ideal $\mathfrak{m}$ was chosen arbitrarily among the maximal ideals containing $(L'^G)_{K[\hat{X}]}$, equation (4.14) is proved.
By Remark 4.21(a), the G-equivariant embedding $U \longrightarrow \hat{U}$ induces a G-isomorphism of $K[\hat{U}]$ and $K[U]$, say $\beta : K[\hat{U}] \longrightarrow K[U]$. Set $S := \beta(K[\hat{X}]^G)$ and $\mathfrak{a} := \beta(L'^G)$. Then $S \subset K[U]^G$ (cf. Remark 4.21(a)) and it follows by equation (4.14) that

$$K[U]^G = (S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)},$$

as desired. ∎

Remark. From the proof of the previous proposition, the following generalization of Theorem 4.32 can be deduced: If G is a finite group acting regularly on an irreducible quasi-affine variety, then all orbits can be separated by invariants. ♢

Combining ideas of this proof with Algorithm 4.22, we can give an algorithm for the computation of the invariant ring of a finite group acting on a quasi-affine variety.

Algorithm 4.34. (Computing invariants of finite group actions)

Input: A finite group G, an irreducible quasi-affine variety U and an action μ of G on U according to Convention 4.16.

Output: An affine algebra $S \subset K[U]^G$ and an ideal $\mathfrak{a} \trianglelefteq S$ such that the invariant ring $K[U]^G$ is given by $K[U]^G = (S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)}$.

(1) Use Algorithm 4.22 to compute a G-equivariant embedding of U as an open subset $\hat{U}$ of an irreducible affine G-variety $\hat{X}$. More precisely, compute ideals $\hat{I}, \hat{L} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ such that $\hat{X}$ resp. $\hat{U}$ is given by $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ and $\hat{U} := \hat{X} \setminus \mathrm{Var}(\hat{L})$. Moreover, compute a morphism $\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X}$ which describes the action of G on $\hat{X}$, and rational functions $\phi_1, \ldots, \phi_{\hat{n}} \in K[U] \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ such that $\phi := (\phi_1, \ldots, \phi_{\hat{n}}) : U \longrightarrow \hat{U}$ defines a G-isomorphism of U and $\hat{U}$.

(2) Compute generators $h_1 + \hat{I}, \ldots, h_s + \hat{I}$ of the algebra $K[\hat{X}]^G$ (see Remark 4.35(a)). Let $S \subset K[U]^G$ be the affine algebra generated by $h_1(\phi_1, \ldots, \phi_{\hat{n}}), \ldots, h_s(\phi_1, \ldots, \phi_{\hat{n}})$.

(3) Compute generators $\widetilde{q}_1 + \hat{I}, \ldots, \widetilde{q}_{t'} + \hat{I}$ of the ideal $(\hat{L} + \hat{I})/\hat{I} \cap K[\hat{X}]^G$ (see Remark 4.35(b)). Let $\mathfrak{a} \trianglelefteq S$ be the ideal generated by $\widetilde{q}_1(\phi_1, \ldots, \phi_{\hat{n}}), \ldots, \widetilde{q}_{t'}(\phi_1, \ldots, \phi_{\hat{n}})$.

(4) Return S and $\mathfrak{a}$.

Proof of Correctness. The correctness of the algorithm follows directly from the proof of Proposition 4.33. ∎

Remarks 4.35. (a) Several algorithms are known for the computation of the invariant ring $K[\hat{X}]^G$ in step (2). Details can be found for example in [Stu93], [Kem96], [Der99] and [DK02].

(b) Although it seems to be a well-known fact how to compute the intersection of an ideal with a subring in step (3), we include details about this for lack of an adequate reference. We introduce a new notation, since the following is applicable not only for the case of invariant rings as needed here, but also in a more general context. So let $\mathfrak{a} = (p_1, \ldots, p_r), \mathfrak{b} = (q_1, \ldots, q_t) \trianglelefteq K[x_1, \ldots, x_n]$ be arbitrary ideals and let

$f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. We are interested in generators of the ideal

$$\mathfrak{c} := ((\mathfrak{b} + \mathfrak{a})/\mathfrak{a}) \cap K[f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}] \trianglelefteq K[f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}].$$

For this, take additional indeterminates over K, say $Z_1, \ldots, Z_m$, and consider the ideal

$$\mathfrak{d} := (Z_1 - f_1, \ldots, Z_m - f_m, p_1, \ldots, p_r, q_1, \ldots, q_t) \trianglelefteq K[x_1, \ldots, x_n, Z_1, \ldots, Z_m].$$

Let $F_1, \ldots, F_s \in K[Z_1, \ldots, Z_m]$ be generators of the elimination ideal $\mathfrak{d} \cap K[Z_1, \ldots, Z_m]$ (for the computation of elimination ideals, see Section 1.3). Then generators of $\mathfrak{c}$ are given by

$$F_1(f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}), \ldots, F_s(f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}).$$

To see this, assume first that $g + \mathfrak{a} \in ((\mathfrak{b} + \mathfrak{a})/\mathfrak{a}) \cap K[f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}] \trianglelefteq K[f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}]$. Then $g + \mathfrak{a}$ can be written as $g + \mathfrak{a} = G(f_1, \ldots, f_m) + \mathfrak{a}$, where G is a polynomial in m indeterminates over K. We have

$$\begin{aligned} G(Z_1, \ldots, Z_m) + \mathfrak{d} &= G((Z_1 - f_1) + f_1, \ldots, (Z_m - f_m) + f_m) + \mathfrak{d} \\ &= G(f_1, \ldots, f_m) + \mathfrak{d} = g + \mathfrak{d} = \mathfrak{d}, \end{aligned}$$

and hence $G(Z_1, \ldots, Z_m) \in \mathfrak{d} \cap K[Z_1, \ldots, Z_m]$.
For the reverse conclusion, let $i \in \{1, \ldots, s\}$. Then by definition of F_i, it follows that

$$\begin{aligned} F_i \in &\sum_{j=1}^{m} (Z_j - f_j) K[x_1, \ldots, x_n, Z_1, \ldots, Z_m] + \sum_{j=1}^{r} p_j K[x_1, \ldots, x_n, Z_1, \ldots, Z_m] \\ &+ \sum_{j=1}^{t} q_j K[x_1, \ldots, x_n, Z_1, \ldots, Z_m]. \end{aligned}$$

Specializing x_j to $x_j + \mathfrak{a}$ for $i = 1, \ldots, n$ and Z_j to $f_j + \mathfrak{a}$ for $j = 1, \ldots, m$ gives

$$F_i(f_1 + \mathfrak{a}, \ldots, f_m + \mathfrak{a}) \in \sum_{j=1}^{t} (q_j + \mathfrak{a}) K[x_1 + \mathfrak{a}, \ldots, x_n + \mathfrak{a}] = (\mathfrak{b} + \mathfrak{a})/\mathfrak{a}.$$

Since this is true for every $i = 1, \ldots, s$, the result follows.

(c) In case that it is desired to actually calculate generators of $K[U]^G$, it is advisable not to compute the colon algebra $(S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)}$, but generators of the colon algebra

$$(K[\hat{X}]^G : (((\hat{L} + \hat{I})/\hat{I}) \cap K[\hat{X}]^G)^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)} \tag{4.15}$$

and afterwards applying the homomorphism which sends $\hat{x}_i + \hat{I}$ to ϕ_i for $i = 1, \ldots, \hat{n}$. This is because the algorithm for the computation of colon algebras as given in [DK08] works for subalgebras which are generated by polynomial functions and both

S and $\mathfrak{a}$ might involve rational functions.
To make this rough idea more concrete, steps (2)-(4) could be replaced by

(1) Compute generators $h_1 + \hat{I}, \ldots, h_s + \hat{I}$ of the algebra $K[\hat{X}]^G$.

(2) Let $Z_1, \ldots, Z_s$ be indeterminates over $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$. Compute generators F_1, $\ldots, F_{t'}$ of the elimination ideal

$$\begin{aligned}((Z_1 - h_1, \ldots, Z_s - h_s)_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},Z_1,\ldots,Z_s]} + (\hat{I} + \hat{L})_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},Z_1,\ldots,Z_s]}) \\ \cap K[Z_1, \ldots, Z_s].\end{aligned} \tag{4.16}$$

and choose an element $D \in \{F_1, \ldots, F_{t'}\}$ such that $D(h_1, \ldots, h_s) \notin \hat{I}$.

(3) Let Z_{s+1} be an additional indeterminate over $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, Z_1, \ldots, Z_s]$. Compute generators of the elimination ideal

$$\begin{aligned}\check{I} := \big(((Z_1 - h_1, \ldots, Z_s - h_s, Z_{s+1} \cdot D(h_1, \ldots, h_s) - 1)_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},Z_1,\ldots,Z_{s+1}]} \\ + (\hat{I})_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},Z_1,\ldots,Z_{s+1}]}) : D(h_1, \ldots, h_s)^\infty\big) \cap K[Z_1, \ldots, Z_{s+1}].\end{aligned}$$

(4) Set $\mathcal{A} := \{Z_1, \ldots, Z_s\}$ and $\mathcal{B} := \emptyset$.

(5) While $\mathcal{A} \neq \emptyset$ do

(6) For all $A \in \mathcal{A}$:
Output

$$A(h_1(\phi_1, \ldots, \phi_{\hat{n}}), \ldots, h_s(\phi_1, \ldots, \phi_{\hat{n}}), 1/D(h_1(\phi_1, \ldots, \phi_{\hat{n}}), \ldots, h_s(\phi_1, \ldots, \phi_{\hat{n}})).$$

(7) $\mathcal{B} := \mathcal{B} \cup \mathcal{A}$

(8) Let $\mathcal{A}$ be the output of Algorithm 2.6 of [DK08] for the computation of

$$(K[B + \check{I};\ B \in \mathcal{B}] : (F_1 + \check{I}, \ldots, F_{t'} + \check{I}))_{K[Z_1,\ldots,Z_{s+1}]/\check{I}}$$

(9) End While Loop.

We do not prove the correctness of this variant of Algorithm 4.34. Instead, we give a rough outline of what happens in these steps.
According to Remark (b), generators of the ideal $((\hat{L} + \hat{I})/\hat{I}) \cap K[\hat{X}]^G$ are given by $F_1(h_1 + \hat{I}, \ldots, h_s + \hat{I}), \ldots, F_{t'}(h_1 + \hat{I}, \ldots, h_s + \hat{I})$. Together with the identity $\sqrt{(((\hat{L} + \hat{I})/\hat{I})^G)_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]/\hat{I}}} = \sqrt{(\hat{L} + \hat{I})/\hat{I}} \neq 0$, this implies that in step (2) an element D with the required properties always exists. By (4.15), we first have to calculate

$$(K[\hat{X}]^G : (F_1(h_1 + \hat{I}, \ldots, h_s + \hat{I}), \ldots, F_{t'}(h_1 + \hat{I}, \ldots, h_s + \hat{I}))^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)}$$

Note that

$$(K[\hat{X}]^G : (F_1(h_1+\hat{I},\ldots,h_s+\hat{I}),\ldots,F_{t'}(h_1+\hat{I},\ldots,h_s+\hat{I}))^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)}$$
$$= (K[\hat{X}]^G : (F_1(h_1+\hat{I},\ldots,h_s+\hat{I}),\ldots,F_{t'}(h_1+\hat{I},\ldots,h_s+\hat{I}))^\infty)_{K[\hat{X}]^G_{D(h_1+\hat{I},\ldots,h_s+\hat{I})}}$$

and hence it remains to represent $K[\hat{X}]^G_{D(h_1+\hat{I},\ldots,h_s+\hat{I})}$ as a quotient of a polynomial ring by an ideal (as needed for an application of Algorithm 2.6 of [DK08]). This is done in step (3), yielding the isomorphism

$$K[Z_1,\ldots,Z_{s+1}]/\check{I} \longrightarrow K[\hat{X}]^G_{D(h_1+\hat{I},\ldots,h_s+\hat{I})}$$

which sends $Z_i+\check{I}$ to $h_i+\hat{I}$ for $i=1,\ldots,s$ and $Z_{s+1}+\check{I}$ to $1/D(h_1+\hat{I},\ldots,h_s+\hat{I})$ (see also Remark 4.23(d)). Under this isomorphism, the above colon expression translates to

$$(K[Z_1+\check{I},\ldots,Z_s+\check{I}] : (F_1+\check{I},\ldots,F_{t'}+\check{I})^\infty)_{K[Z_1,\ldots,Z_{s+1}]/\check{I}}.$$

The actual computation of this colon expression takes place in the loop comprising steps (5)-(9). This computation follows the methods of Derksen and Kemper (cf. [DK08], Algorithm 2.7 and Remark 3.18(c)). Note that at the time of the output in step (6), we have to apply both the isomorphisms

$$K[Z_1,\ldots,Z_{s+1}]/\check{I} \longrightarrow K[\hat{X}]^G_{D(h_1+\hat{I},\ldots,h_s+\hat{I})} \quad \text{and} \quad K[\hat{U}] \longrightarrow K[U]$$

to get generators of $K[U]^G = (S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)}$.
By construction, this algorithm terminates if and only if $K[U]^G$ is finitely generated as a K-algebra. ♢

Example 4.36. In Example 4.30, we have already computed the invariant ring of a finite group acting on a quasi-affine variety. In the following we will demonstrate an application of Algorithm 4.34 to this very same situation. As before, all computations have been done with the computer algebra system MAGMA.
By step (1) of the algorithm, we first have to invoke Algorithm 4.22 to embed U as an open subset $\hat{U}$ of an affine G-variety $\hat{X}$. Since we have already calculated an almost identical example for the application of Algorithm 4.22, we just state the result here. It returns $\hat{I} := (\hat{x}_1^2-\hat{x}_2^2+1) \trianglelefteq K[\hat{x}_1,\hat{x}_2,\hat{x}_3]$ and $\hat{L} := ((\hat{x}_1+\hat{x}_2)\cdot(\hat{x}_1+\hat{x}_2-1),(\hat{x}_1+\hat{x}_2)\cdot\hat{x}_3) \trianglelefteq K[\hat{x}_1,\hat{x}_2,\hat{x}_3]$ which means that the varieties $\hat{X}$ resp. $\hat{U}$ are given by $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^3$ and $\hat{U} := \hat{X} \setminus \mathrm{Var}(\hat{L})$. Moreover, it returns an action of G on $\hat{X}$ which is given by

$$G \times \hat{X} \longrightarrow \hat{X},\ (\sigma,(\hat{\xi}_1,\hat{\xi}_2,\hat{\xi}_3)) \longmapsto (-\hat{\xi}_1,\hat{\xi}_2,\hat{\xi}_3)$$

and rational functions $\phi_1 := 1/2\cdot(x_1^2-1)/x_1, \phi_2 := 1/2\cdot(x_1^2+1)/x_1, \phi_3 := x_2$ which define

a G-isomorphism

$$U \longrightarrow \hat{U},\ u \longmapsto (\phi_1(u), \phi_2(u), \phi_3(u)).$$

Next, for the computation of step (2), we have to find generators of $K[\hat{X}]^G$. In the simple case of this example, it can be seen that $K[\hat{X}]^G$ is generated by $\hat{x}_1^2 + \hat{I}, \hat{x}_2 + \hat{I}, \hat{x}_3 + \hat{I}$.
To simplify the verification that the invariant ring computed here is equal to the (same) invariant ring computed in Example 4.30, we do not express the invariant ring as a colon expression $(S : \mathfrak{a}^\infty)_{\mathrm{Quot}(S)}$ as suggested in Algorithm 4.34 but compute a concrete generating set. Therefore, we first have to calculate

$$(K[\hat{X}^G] : (((\hat{L} + \hat{I})/\hat{I})^G)^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)}$$

and then apply the homomorphism $\hat{x}_i + \hat{I} \longmapsto \phi_i$ for $i = 1, 2, 3$. For the computation of the colon expression we can of course use Algorithm 2.7 of [DK08]. In the following, though, we take a more direct approach.

It is not hard to verify that $\hat{X}$ is a normal affine variety (see e. g. Algorithm 4.8). But this means that $K[\hat{X}]^G$ is normal, too. An easy computation with Magma shows that $(\hat{L}+\hat{I})/\hat{I} = (\hat{x}_1+\hat{I}, \hat{x}_2-1+\hat{I}, \hat{x}_3+\hat{I})$. In particular, it follows that the height of $(\hat{L}+\hat{I})/\hat{I}$ is equal to 2. Since $K[\hat{X}]$ is integral over $K[\hat{X}]^G$ and $K[\hat{X}]$ is normal, this implies that the height of $((\hat{L} + \hat{I})/\hat{I}) \cap K[\hat{X}]^G$ is 2, too (cf. [Eis95], Chapter 13, Theorem 13.9).
By the normality of $K[\hat{X}]^G$, this means that

$$K[\hat{U}]^G = (K[\hat{X}^G] : (((\hat{L} + \hat{I})/\hat{I})^G)^\infty)_{\mathrm{Quot}(K[\hat{X}]^G)} = K[\hat{X}]^G$$

(cf. [Eis95], Chapter 11, Corollary 11.4). Finally, applying the homomorphism $\hat{x}_i + \hat{I} \longmapsto \phi_i$ for $i = 1, 2, 3$ yields

$$K[U]^G = K\left[\frac{(x_1^2-1)^2}{4x_1^2}, \frac{x_1^2+1}{2x_1}, x_2\right]. \qquad \lhd$$

Can Algorithm 4.34 be generalized to infinite groups? The key point in the proof of Proposition 4.33 was the applicability of implication (4.13). (Note that (4.13) is true for arbitrary linear algebraic groups.) The precondition of (4.13) can be interpreted geometrically. With the same notation as used in the discussion of (4.13), let G be a reductive group. The invariant ring $K[X]^G$ is finitely generated and the inclusion $K[X]^G \longrightarrow K[X]$ induces a morphism $\pi : X \longrightarrow X/\!\!/G$, the so-called categorical quotient, where $X/\!\!/G$ stands for the affine variety corresponding to the affine algebra $K[X]^G$ (for details about this notion see [DK02]).
In that context, the condition $\sqrt{(L'^G)_{K[X]}} = \sqrt{L'}$ then means that the quasi-affine variety U is the preimage of an open subset of $X/\!\!/G$ under π. For finite groups every G-stable open subset U of X has this property, which is the content of Theorem 4.32 and Proposition 4.33.
For infinite (reductive) groups this is not true any more as the following example shows.

Example 4.37. Let X be the two-dimensional affine space K^2 and let $G := K^\times$ act on X by

$$\lambda(\xi_1, \xi_2) := (\lambda\xi_1, \lambda\xi_2) \qquad \text{for all } \lambda \in G,\ (\xi_1, \xi_2) \in X.$$

Consider the open subset $U := K^2 \setminus \{(0,0)\}$ of X. It is G-stable and therefore a quasi-affine G-variety. If x_1, x_2 denote the coordinate functions on X, then – with the notation of the preceding discussion – the ideal L' is given by $(x_1, x_2) \trianglelefteq K[x_1, x_2]$. But obviously we have $\sqrt{(L'^G)_{K[X]}} = \sqrt{(0)} \neq \sqrt{L'}$. ◁

Nonetheless, for G reductive, it can be checked algorithmically whether the equality $\sqrt{(L'^G)_{K[X]}} = \sqrt{L'}$ holds or not. Therefore, the invariant ring $K[U]^G$ can be computed with ideas as in Algorithm 4.34 at least in some special cases. Unfortunately, we do not have a nice a priori criterion for infinite groups when this method is applicable.

4.3.3 An algorithm for computing invariants of unipotent groups acting on quasi-affine varieties

The computation of "quasi-affine invariants" of finite group actions turned out to be quite straightforward. As we have seen with Example 4.37, in general this approach does not work for infinite groups. In this section, we examine computational methods for the case that a unipotent group G acts regularly on an irreducible quasi-affine variety U.
For the calculation of the invariant ring $K[U]^G$ one could try to mimic the approach which has been chosen for the computation of "affine invariants" of unipotent groups (cf. Chapter 3). More precisely, this would mean to find $h_1, \ldots, h_p, h \in K[U]^G$ with $h \neq 0$ such that

$$K[U]^G_h = K[h_1, \ldots, h_p, 1/h].$$

Then $K[U]^G$ would be given by $(K[h_1, \ldots, h_p, h] : h^\infty)_{K[U]}$. In contrast to the affine case, the algebra $K[U]$ may not be finitely generated, though, and to the best of my knowledge, there is no algorithm to compute a colon algebra within a non-finitely generated algebra. In the following, we will choose another slightly different approach for the computation of $K[U]^G$ which accomplishes to fill this gap. As above, we first calculate $h_1, \ldots, h_p, h \in K[U]^G$ such that $K[U]^G_h = K[h_1, \ldots, h_p, 1/h]$. We embed $h_1, \ldots, h_p, h$ into an auxiliary affine algebra S and perform the calculation of a certain colon algebra within S (which is possible with the existing algorithms, since S is finitely generated). We will eventually show that this yields an algebra which is isomorphic to $K[U]^G$. Moreover, the isomorphism can be given explicitly and therefore – putting all these pieces together – this leads to an algorithm for computing generators of $K[U]^G$. Note that because of the additional "technical layer" consisting of the algebra S, the resulting algorithm for the computation of invariants of unipotent group actions has become quite lengthy.
Some ideas of this construction were motivated by the paper [Nag65] of Nagata and the paper [Win03] of Winkelmann, where – among other things – the relation between certain invariant rings and rings of regular functions of normal quasi-affine varieties have been examined. Especially the arguments of Winkelmann were pretty geometric. In contrast,

the methods used in the following are far more algebraic and work for arbitrary irreducible quasi-affine varieties, not just for normal ones.

We directly start with the algorithm for the computation of $K[U]^G$. Similarly as in previous cases, this algorithm terminates if and only if $K[U]^G$ is finitely generated. Otherwise, it returns an infinite sequence of generators of $K[U]^G$.

Algorithm 4.38. (Computing invariants of unipotent group actions)

Input: A unipotent linear algebraic group G, an irreducible quasi-affine variety U and an action μ of G on U according to Convention 4.16.

Output: A (possibly) infinite sequence of generators of $K[U]^G$.

(1) Use Algorithm 4.22 to compute a G-equivariant embedding of U as an open subset $\hat{U}$ of an irreducible affine G-variety $\hat{X}$. More precisely, compute ideals $\hat{I}, \hat{L} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ such that $\hat{X}$ resp. $\hat{U}$ is given by $\hat{X} := \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ and $\hat{U} := \hat{X} \setminus \mathrm{Var}(\hat{L})$. Moreover, compute a morphism $\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X}$ which describes the action of G on $\hat{X}$, and rational functions $\phi_1, \ldots, \phi_{\hat{n}} \in K[U] \subset \mathrm{Quot}(K[x_1, \ldots, x_n]/I)$ such that $\phi := (\phi_1, \ldots, \phi_{\hat{n}}) : U \longrightarrow \hat{U}$ defines a G-isomorphism of U and $\hat{U}$.
Denote the generators of $\hat{I}$ by $\hat{p}_1, \ldots, \hat{p}_{\hat{r}} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ and the generators of $\hat{L}$ by $\hat{q}_1, \ldots, \hat{q}_{\hat{t}}$. We may assume without loss of generality that $\hat{q}_1, \ldots, \hat{q}_{\hat{t}} \notin \hat{I}$.

(2) Use Algorithm 3.20 to compute $f + \hat{I}, f_1 + \hat{I} \ldots f_s + \hat{I} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ such that

$$K[\hat{X}]^G_{f+\hat{I}} = K[f_1 + \hat{I}, \ldots, f_s + \hat{I}, f + \hat{I}, 1/(f + \hat{I})].$$

(3) Let $T_1, \ldots, T_{\hat{t}}$ be indeterminates over $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ and set

$$S := K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{\hat{t}}]/P,$$

where P is the ideal of $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{\hat{t}}]$ generated by the elements

$$\hat{p}_1, \ldots, \hat{p}_{\hat{r}},\ \hat{q}_1 \cdot T_1 + \hat{q}_2 \cdot T_2 + \ldots + \hat{q}_{\hat{t}} \cdot T_{\hat{t}} - 1.$$

(4) Let $Z_1, \ldots, Z_{\hat{n}}, W_1, \ldots, W_{\hat{t}}$ be indeterminates over $\mathrm{Quot}(S)$. Choose an arbitrary monomial order on $Z_1, \ldots, Z_{\hat{n}}, W_1, \ldots, W_{\hat{t}}$ and let

$$\frac{h_1 + P}{h + P}, \ldots, \frac{h_p + P}{h + P} \in K(f_1 + P, \ldots, f_s + P, f + P)$$

with $h_1, \ldots, h_p, h \in K[f_1, \ldots, f_s, f]$ be the non-zero coefficients of the reduced Gröbner basis $\mathcal{G}$ of the ideal $Q \trianglelefteq \mathrm{Quot}(K[f_1+P, \ldots, f_s+P, f+P])[Z_1, \ldots, Z_{\hat{n}}, W_1, \ldots, W_{\hat{t}}]$,

generated by the elements

$$f_1(Z_1,\ldots,Z_{\hat{n}}) - f_1 + P, \ldots, f_s(Z_1,\ldots,Z_{\hat{n}}) - f_s + P, f(Z_1,\ldots,Z_{\hat{n}}) - f + P,$$
$$\hat{p}_1(Z_1,\ldots,Z_{\hat{n}}),\ldots,\hat{p}_{\hat{r}}(Z_1,\ldots,Z_{\hat{n}}),$$
$$\hat{q}_1(Z_1,\ldots,Z_{\hat{n}})\cdot W_1 + \hat{q}_2(Z_1,\ldots,Z_{\hat{n}})\cdot W_2 + \ldots + \hat{q}_{\hat{t}}(Z_1,\ldots,Z_{\hat{n}})\cdot W_{\hat{t}} - 1.$$

(For details about how to compute this step, see Remark 4.39(a))

(5) Let α be the natural homomorphism

$$\alpha : K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},T_1,\ldots,T_{\hat{t}}] \longrightarrow \mathrm{Quot}(K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]/\hat{I})[T_1,\ldots,T_{\hat{t}}].$$

Set $\mathcal{H} := \{(\hat{q}_1+\hat{I})\cdot T_1 + (\hat{q}_2+\hat{I})\cdot T_2 + \ldots + (\hat{q}_{\hat{t}}+\hat{I})\cdot T_{\hat{t}} - 1\}$ and define the ideal $Q' := (\mathcal{H}) \trianglelefteq \mathrm{Quot}(K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]/\hat{I})[T_1,\ldots,T_{\hat{t}}]$. Note that – Q' being a principal ideal – the set $\mathcal{H}$ is a Gröbner basis of Q' for every monomial order on $T_1,\ldots,T_{\hat{t}}$.

(6) Set $\mathcal{A} := \{h_1,\ldots,h_p,h\}$ and $\mathcal{B} := \emptyset$.

(7) While $\mathcal{A} \neq \emptyset$ do

(8) For all $g \in \mathcal{A}$:
Compute the normal form $\mathrm{NF}_{\mathcal{H}}(\alpha(g))$. We will see in the following proof of correctness that this yields an element of $\mathrm{Quot}(K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}}]/\hat{I})$, i. e. a rational function in the variables $\hat{x}_1+\hat{I},\ldots,\hat{x}_{\hat{n}}+\hat{I}$. Apply the homomorphism which is given by $\hat{x}_i+\hat{I} \longmapsto \phi_i$ for $i = 1,\ldots,\hat{n}$ and output the result.

(9) $\mathcal{B} := \mathcal{B} \cup \mathcal{A}$

(10) Let $\mathcal{A}$ be the output of Algorithm 2.6 of [DK08] for the computation of

$$(K[g+P;\ g \in \mathcal{B}] : (h+P))_S.$$

(11) End While Loop.

Remarks 4.39. (a) A remark is in order about the calculation of $\mathcal{G}$ in step (4), since none of the common computer algebra systems can handle ideals of polynomial rings over subfields of fields of rational functions directly. Usually, it is possible to deal with ideals in polynomial rings over fields of rational functions (cf. also the introductory section to computational algebra in Chapter 1). So one possibility for implementing step (4) is the representation of the subfield $\mathrm{Quot}(K[f_1+P,\ldots,f_s+P,f+P])$ of $\mathrm{Quot}(S)$ as a field of rational functions of its own. This can be achieved for example via $\mathrm{Quot}(K[Y_1,\ldots,Y_{s+1}]/\mathfrak{a})$, where $Y_1,\ldots,Y_{s+1}$ are new indeterminates over K and $\mathfrak{a}$ is the relation ideal of $f_1+P,\ldots,f_s+P,f+P$. Then obviously $Y_1+\mathfrak{a} \longmapsto f_1+P,\ldots,Y_s+\mathfrak{a} \longmapsto f_s+P$ and $Y_{s+1}+\mathfrak{a} \longmapsto f+P$ defines an isomorphism of $\mathrm{Quot}(K[Y_1,\ldots,Y_{s+1}]/\mathfrak{a})$ and $\mathrm{Quot}(K[f_1+P,\ldots,f_s+P,f+P])$.
For algorithmic details about the computation of ideals of relations, see [CLO07],

Chapter 7, Section 4. Note that if this method is chosen, then of course the generators of Q as given in step (4) have to be adapted with respect to this isomorphism.

(b) For the computation of the colon expression in step (10) of the algorithm, we have to ensure that the affine algebra S is a domain. We have

$$\begin{aligned} S &= K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{\hat{t}}] / \left(\hat{p}_1, \ldots, \hat{p}_{\hat{r}}, \sum_{i=1}^{\hat{t}} \hat{q}_i \cdot T_i - 1 \right) \\ &\cong \left(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \right) [T_1, \ldots, T_{\hat{t}}] / \left(\sum_{i=1}^{\hat{t}} (\hat{q}_i + \hat{I}) \cdot T_i - 1 \right), \end{aligned}$$

As $\sum_{i=1}^{\hat{t}} (\hat{q}_i + \hat{I}) \cdot T_i - 1 \in (K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}]$ is a non-zero linear polynomial and therefore obviously prime, the claim follows. ♢

Proof of Correctness. The following proof of correctness for this algorithm is rather long, hence we start with a short outline.
The structure of the algorithm is as follows. In step (1), an affine variety $\hat{X}$ is computed together with an open subset $\hat{U} := \hat{X} \setminus \mathrm{Var}(\hat{L})$ and an action $\hat{\mu} : G \times \hat{X} \longrightarrow \hat{X}$ such that $\hat{U}$ is a quasi-affine G-variety and U and $\hat{U}$ are G-isomorphic via $\phi = (\phi_1, \ldots, \phi_{\hat{n}})$. Then in the following steps (2)-(11), the algorithm computes generators of $K[\hat{U}]^G$. Finally, if this is done, the homomorphism which sends $\hat{x}_i + \hat{I}$ to ϕ_i is applied to the generators of $K[\hat{U}]^G$ to obtain generators of $K[U]^G$ (for details, see Remark 4.23(a)).
The heart of the algorithm is the computation of $K[\hat{U}]^G$. We will prove first that $K[\hat{X}] = K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ can be embedded into the algebra S via $\iota : K[\hat{X}] \longrightarrow S,\ g + \hat{I} \longmapsto g + P$. Then we will show that this embedding extends to an embedding $\iota : K[\hat{U}] \longrightarrow S$. Using this we will see that $K[\hat{U}]^G_{h+\hat{I}} = K[h_1 + \hat{I}, \ldots, h_p + \hat{I}, h + \hat{I}, 1/(h + \hat{I})]$. This will finally imply that the invariant ring $K[\hat{U}]^G$ is isomorphic to $(K[h_1 + P, \ldots, h_p + P, h + P] : (h + P)^\infty)_S$ via ι.
Note that the computation of this colon algebra is performed in steps (7)-(11). Since in general the colon algebra is not finitely generated, we compute generators of this algebra gradually and apply ι^{-1} at the time of the output of these generators.

As outlined above, we start with an examination of the map

$$\iota : K[\hat{X}] \longrightarrow S,\ g + \hat{I} \longmapsto g + P$$

and claim that this defines an embedding of $K[\hat{X}]$ into S. To prove this, it is enough to show that

$$P \cap K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}] = \hat{I}. \tag{4.17}$$

So let $F \in P \cap K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$. By definition of P, there are polynomials $a_1, \ldots, a_{\hat{r}}, b \in$

$K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{\hat{t}}]$ such that

$$F = \sum_{i=1}^{\hat{r}} a_i \cdot \hat{p}_i + b \cdot \left(\sum_{i=1}^{\hat{t}} \hat{q}_i \cdot T_i - 1 \right) \tag{4.18}$$

Since F does not contain any of the $T_1, \ldots, T_{\hat{t}}$-variables we can specialize T_1 in (4.18) to the solution of the equation $\sum_{i=1}^{\hat{t}} \hat{q}_i \cdot T_i - 1 = 0$ without changing F. To be more explicit, we set $T_1 = -(\hat{q}_2 \cdot T_2 + \hat{q}_3 \cdot T_3 + \ldots + \hat{q}_{\hat{t}} \cdot T_{\hat{t}} + 1)/q_1$. Further specializing $T_2 = \ldots = T_{\hat{t}} = 0$ yields

$$F = \sum_{i=1}^{\hat{r}} \widetilde{a}_i \cdot \hat{p}_i + \widetilde{b} \cdot 0$$

where $\widetilde{a}_1, \ldots, \widetilde{a}_{\hat{r}}, \widetilde{b} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]_{\hat{q}_1}$. It follows that $\hat{q}_1^k \cdot F \in \hat{I}$ for some $k \in \mathbb{N}$. Since $q_1 \notin \hat{I}$ and $\hat{I}$ is a prime ideal (cf. step (1)), this implies that $F \in \hat{I}$. Therefore the map $\iota : K[\hat{X}] \longrightarrow S$ defines an embedding of $K[\hat{X}]$ into S, as claimed.

Next we show that this embedding extends to an embedding $\iota : K[\hat{U}] \longrightarrow S$. Let $N, D \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ be polynomials such that $D \notin \hat{I}$ and

$$\frac{N + \hat{I}}{D + \hat{I}} \in K[\hat{U}].$$

By equation (4.1), there exists $k \in \mathbb{N}$ such that

$$\frac{N + \hat{I}}{D + \hat{I}} \cdot ((\hat{L} + \hat{I})/\hat{I})^k \subset K[\hat{X}]$$

or – regarding $K[\hat{X}]$ as a subset of S –

$$\frac{N + P}{D + P} \cdot (\hat{q}_1 + P, \ldots, \hat{q}_{\hat{t}} + P)^k_{K[\hat{x}_1 + P, \ldots, \hat{x}_{\hat{n}} + P]} \subset K[\hat{x}_1 + P, \ldots, \hat{x}_{\hat{n}} + P].$$

Observe that $1 + P = \hat{q}_1 \cdot T_1 + \hat{q}_2 \cdot T_2 + \ldots + \hat{q}_{\hat{t}} \cdot T_{\hat{t}} + P$ which implies that

$$\frac{N + P}{D + P} = \frac{N + P}{D + P} \cdot (1 + P)^k = \frac{N + P}{D + P} \cdot (\hat{q}_1 \cdot T_1 + \hat{q}_2 \cdot T_2 + \ldots + \hat{q}_{\hat{t}} \cdot T_{\hat{t}} + P)^k.$$

But now – regarding $(\hat{q}_1 \cdot T_1 + \hat{q}_2 \cdot T_2 + \ldots + \hat{q}_{\hat{t}} \cdot T_{\hat{t}})^k$ as a polynomial in $T_1, \ldots, T_{\hat{t}}$ – all coefficients lie in $\hat{L}^k$. It follows that

$$\frac{N + P}{D + P} \in S$$

and thus the embedding ι can be extended to $K[\hat{U}]$, indeed.

Next we show that

$$K[\hat{U}]^G_{h+P} = K[h_1 + P, \ldots, h_p + P, h + P, 1/(h + P)]. \tag{4.19}$$

Note that, to be more precise, we should write $\iota(K[\hat{U}]^G_{h+\hat{I}})$ on the left hand side of the above equation. Nonetheless, the implicit identification of $K[\hat{U}]$ with its image under ι should always be clear from the context.
By step (4) of the algorithm, $h_1+P,\dots,h_p+P,h+P$ are elements of $K[f_1+P,\dots,f_s+P,f+P]$, which in turn is a subalgebra of $K[\hat{U}]^G$ by step (2). Therefore, it follows that $K[h_1+P,\dots,h_p+P,h+P,1/(h+P)]\subset K[\hat{U}]^G_{h+P}$.

For the reverse inclusion, let $g+P\in K[\hat{U}]^G$. By Proposition 3.6, $g+P$ is contained in the field of fractions of $K[\hat{X}]^G$, hence it can be written as

$$g+P=\frac{N(f_1,\dots,f_s,f)+P}{D(f_1,\dots,f_s,f)+P}.$$

We will prove in a minute that

$$g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}})-(g+P)\in Q. \tag{4.20}$$

Assume for a moment that the identity (4.20) is true. Then certainly

$$\mathrm{NF}_{\mathcal{G}}(g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}})-(g+P))=0.$$

Since all coefficients of $g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}})$ are contained in K and the elements of $\mathcal{G}$ only have coefficients in $K[h_1+P,\dots,h_p+P,h+P,1/(h+P)]$, it follows by Remark 1.44 that

$$\begin{aligned}&\mathrm{NF}_{\mathcal{G}}(g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}}))\\&\quad\in K[h_1+P,\dots,h_p+P,h+P,1/(h+P)][Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}}].\end{aligned}$$

On the other hand, by the $\mathrm{Quot}(K[f_1+P,\dots,f_s+P,f+P])$-linearity of $\mathrm{NF}_{\mathcal{G}}$, we have

$$\begin{aligned}&\mathrm{NF}_{\mathcal{G}}(g(Z_1,\dots Z_{\hat{n}},W_1,\dots,W_{\hat{t}})-(g+P))=\\&\qquad\mathrm{NF}_{\mathcal{G}}(g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}}))-(g+P)=0.\end{aligned}$$

This implies that $g+P\in K[h_1+P,\dots,h_p+P,h+P,1/(h+P)]$. Hence equation (4.19) follows from the validity of (4.20). For the latter to be true, it is enough to show that

$$(D(f_1,\dots,f_s,f)+P)\cdot g(Z_1,\dots,Z_{\hat{n}},W_1,\dots,W_{\hat{t}})-(N(f_1,\dots,f_s,f)+P)\in Q.$$

In the following we write $\mathbf{Z}$ for $Z_1,\dots,Z_{\hat{n}}$ and $\mathbf{W}$ for $W_1,\dots,W_{\hat{t}}$. Moreover, the equivalence class f_i+P of f_i modulo P will be written as $\overline{f_i}$. We then have

$$\begin{aligned}&D(\overline{f_1}-f_1(\mathbf{Z})+f_1(\mathbf{Z}),\dots,\overline{f}_s-f_s(\mathbf{Z})+f_s(\mathbf{Z}),\overline{f}-f(\mathbf{Z})+f(\mathbf{Z}))\cdot g(\mathbf{Z},\mathbf{W})\\&\quad-N(\overline{f_1}-f_1(\mathbf{Z})+f_1(\mathbf{Z}),\dots,\overline{f_s}-f_s(\mathbf{Z})+f_s(\mathbf{Z}),\overline{f}-f(\mathbf{Z})+f(\mathbf{Z}))=\\&\left(D(f_1(\mathbf{Z}),\dots,f_s(\mathbf{Z}),f(\mathbf{Z}))+\sum_{i=1}^{s}(\overline{f_i}-f_i(\mathbf{Z}))\cdot a_i+(\overline{f}-f(\mathbf{Z}))\cdot a\right)\cdot g(\mathbf{Z},\mathbf{W})\end{aligned}$$

$$
\begin{aligned}
&- N(f_1(\mathbf{Z}),\ldots,f_s(\mathbf{Z}),f(\mathbf{Z})) + \sum_{i=1}^{s}(\overline{f_i} - f_i(\mathbf{Z}))\cdot b_i + (\overline{f} - f(\mathbf{Z}))\cdot b = \\
&(D(f_1(\mathbf{Z}),\ldots,f_s(\mathbf{Z}),f(\mathbf{Z}))\cdot g(\mathbf{Z},\mathbf{W}) - N(f_1(\mathbf{Z}),\ldots,f_s(\mathbf{Z}),f(\mathbf{Z})) \\
&\quad + \left(\sum_{i=1}^{s}(\overline{f_i} - f_i(\mathbf{Z}))\cdot a_i + (\overline{f} - f(\mathbf{Z}))\cdot a\right)\cdot g(\mathbf{Z},\mathbf{W}) \\
&\quad + \sum_{i=1}^{s}(\overline{f_i} - f_i(\mathbf{Z}))\cdot b_i + (\overline{f} - f(\mathbf{Z}))\cdot b,
\end{aligned}
$$

with certain $a_1,\ldots,a_s,a,b_1,\ldots,b_s,b \in K[f_1+P,\ldots,f_s+P,f+P][Z_1,\ldots,Z_{\hat{n}}]$. Obviously, the last parts of the sum, i. e. the summands in the last two lines, are contained in the ideal Q. By definition of g, we have $D(f_1,\ldots,f_s,f)\cdot g - N(f_1,\ldots,f_s,f) + P = 0$ and therefore, it follows that

$$
\begin{aligned}
&D(f_1(\mathbf{Z}),\ldots,f_s(\mathbf{Z}),f(\mathbf{Z}))\cdot g(\mathbf{Z},\mathbf{W}) - N(f_1(\mathbf{Z}),\ldots,f_s(\mathbf{Z}),f(\mathbf{Z})) \\
&\quad \in \big(\hat{p}_1(\mathbf{Z}),\ldots,\hat{p}_{\hat{r}}(\mathbf{Z}),\hat{q}_1(\mathbf{Z})\cdot W_1 + \hat{q}_2(\mathbf{Z})\cdot W_2 + \ldots + \hat{q}_{\hat{t}}(\mathbf{Z})\cdot W_{\hat{t}} - 1\big) \\
&\quad\quad \subset Q.
\end{aligned}
$$

This proves (4.20) and hence equation (4.19).

Next we show that

$$
K[\hat{U}]^G = (K[h_1+P,\ldots,h_p+P,h+P] : (h+P)^\infty)_S. \tag{4.21}
$$

Note that as above, we identify $K[\hat{U}]^G$ with its image under the embedding $K[\hat{U}]^G \longrightarrow S$. Equation (4.19) implies that $K[\hat{U}]^G \subset (K[h_1+P,\ldots,h_p+P,h+P] : (h+P)^\infty)_S$. It remains to show that the right hand of (4.21) side is contained in the left hand side. Let $\widetilde{g} \in K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},T_1,\ldots,T_{\hat{t}}]$, $\widetilde{N}$ be a polynomial over K in $p+1$ variables and let $l \in \mathbb{N}_0$ such that

$$
\widetilde{g} + P = \frac{\widetilde{N}(h_1,\ldots,h_p,h) + P}{(h+P)^l} \in (K[h_1+P,\ldots,h_p+P,h+P] : (h+P)^\infty)_S.
$$

Let $d \in \mathbb{N}_0$ be the total degree of $\widetilde{g}$ regarded as a polynomial in $T_1,\ldots,T_{\hat{t}}$. By construction,

$$
h^l\cdot\widetilde{g} - \widetilde{N}(h_1,\ldots,h_p,h) \in P,
$$

and so in particular,

$$
h^l\cdot\hat{q}_i^d\cdot\widetilde{g} - \hat{q}_i^d\cdot\widetilde{N}(h_1,\ldots,h_p,h) \in P
$$

for all $i \in \{1,\ldots,\hat{t}\}$. Consider the element $(\hat{q}_i+P)^d\cdot(\widetilde{g}+P)$. Since $\hat{q}_1\cdot T_1 + \hat{q}_2\cdot T_2 + \ldots + \hat{q}_{\hat{t}}\cdot T_{\hat{t}} - 1 \in P$, we may "eliminate" one variable out of $T_1,\ldots,T_{\hat{t}}$. To be more precise, for every $i \in \{1,\ldots,\hat{t}\}$, there exists a polynomial $\widetilde{g}_i \in K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},T_1,\ldots,T_{i-1},T_{i+1},\ldots,T_{\hat{t}}]$

such that

$$\widetilde{g}_i + P = (\hat{q}_i + P)^d \cdot (\widetilde{g} + P).$$

We want to show that

$$\widetilde{g}_i + P \in K[\hat{x}_1 + P, \ldots, \hat{x}_{\hat{n}} + P] \quad \text{for all } i \in \{1, \ldots, \hat{t}\}. \tag{4.22}$$

Assume for a moment that this is true. Then equivalently,

$$(\hat{q}_i + P)^d \cdot \frac{\widetilde{N}(h_1, \ldots, h_p, h) + P}{(h + P)^l} \in K[\hat{x}_1 + P, \ldots, \hat{x}_{\hat{n}} + P] \quad \text{for all } i \in \{1, \ldots, \hat{t}\}.$$

Regarding this as an equation in $\mathrm{Quot}(K[\hat{X}])$ via the embedding $\mathrm{Quot}(K[\hat{X}]) \longrightarrow \mathrm{Quot}(S)$ yields

$$(\hat{q}_i + \hat{I})^d \cdot \frac{\widetilde{N}(h_1, \ldots, h_p, h) + \hat{I}}{(h + \hat{I})^l} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} \quad \text{for all } i \in \{1, \ldots, \hat{t}\}$$

and this in turn means by definition of $\hat{L}$ that

$$\frac{\widetilde{N}(h_1, \ldots, h_p, h) + \hat{I}}{(h + \hat{I})^l} \in (K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I} : ((\hat{L} + \hat{I})/\hat{I})^{\hat{t}d})_{\mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})} \subset K[\hat{U}].$$

Finally, since the elements $h_1 + \hat{I}, \ldots, h_p + \hat{I}, h + \hat{I}$ are invariant, it follows that $\widetilde{g} \in K[\hat{U}]^G$ and equation (4.21) is proved.

We still have to prove the validity of equation (4.22). By construction of $\widetilde{g}_i$, it follows for all $i \in \{1, \ldots, \hat{t}\}$ that

$$h^l \cdot \widetilde{g}_i - \hat{q}_i^d \cdot \widetilde{N}(h_1, \ldots, h_p, h) \in P \cap K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}].$$

Let $i \in \{1, \ldots, \hat{t}\}$. Then the ideal $P \cap K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}]$ is equal to the ideal generated by $\hat{I}$ in $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}]$. The proof for this is very similar to the proof of (4.17) above, hence we do not repeat it here.
Regarding $h^l \cdot \widetilde{g}_i - \hat{q}_i^d \cdot \widetilde{N}(h_1, \ldots, h_p, h)$ as a polynomial in $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}$, it follows that all of its coefficients lie in $\hat{I}$. Since $\hat{q}_i^d \cdot \widetilde{N}(h_1, \ldots, h_p, h)$ does not involve any monomials in $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}$, the same holds for all the coefficients of the $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{\hat{t}}$-monomials of positive total degree in $\widetilde{g}_i$. As $\hat{I} \subset P$, this shows (4.22).

As indicated in the outline above, the colon algebra

$$(K[h_1 + P, \ldots, h_p + P, h + P] : (h + P)^\infty)_S \tag{4.23}$$

(and thus the invariant ring $K[\hat{U}]^G$) is computed in the while loop comprising steps (7)-(11). This is done exactly as in the original algorithm of Derksen and Kemper (cf. [DK08], Algorithm 2.7; see also Remark 3.18(c)) – except that there is an additional computation at

the time of the output of the generators (step (8)). We hence only examine this additional step.
By the work of Derksen and Kemper in [DK08], we know that generators of the colon algebra (4.23) are given by $\{g + P;\ g \in \mathcal{B}\}$ (note that if the colon algebra is not finitely generated then the while loop does not terminate finitely and $\mathcal{B}$ will grow infinitely). By construction, these generators are elements of S. Since we are interested in generators of $K[\hat{U}]^G$, it remains to write them as elements of $K[\hat{U}]$ according to the embedding $\iota : K[\hat{U}] \longrightarrow S$. In other words, the generators have to be represented as quotients of polynomials in $\hat{x}_1 + P, \ldots, \hat{x}_{\hat{n}} + P$. This is done as follows. Let $g + P \in (K[h_1 + P, \ldots, h_p + P, h + P] : (h + P)^\infty)_S$. From the discussion above we know that $g + P$ is contained in the image of the embedding $K[\hat{U}] \longrightarrow S$. Hence there exist $N, D \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ with $D \notin P$ such that $g + P = (N + P)/(D + P)$. We claim that the representation of $g + P$ as $(N + P)/(D + P)$ can be found by computing the normal form $\mathrm{NF}_{\mathcal{H}}(\alpha(g))$ (as it is done in step (8)). For the proof of this, recall the definition of α in step (5) and observe that the homomorphism

$$\begin{aligned} K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, \ldots, T_{\hat{t}}] &\xrightarrow{\alpha} \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}] \\ &\longrightarrow \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}]/Q' \end{aligned}$$

induces a homomorphism

$$\tilde{\alpha} : S \longrightarrow \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}]/Q'.$$

The commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\tilde{\alpha}} & \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}]/Q' \\ {\scriptstyle\iota}\uparrow & & \uparrow \\ K[\hat{U}] & \hookrightarrow & \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}) \end{array}$$

shows that $\tilde{\alpha}_{|\iota(K[U])} : \iota(K[U]) \longrightarrow \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})[T_1, \ldots, T_{\hat{t}}]/Q'$ is injective. Note that by the identity $g+P = (N+P)/(D+P)$, we have $0 = \tilde{\alpha}((g+P)\cdot(D+P)-(N+P)) = \tilde{\alpha}(g + P) \cdot \tilde{\alpha}(D + P) - \tilde{\alpha}(N + P) = 0$. Therefore, it follows by the injectivity of $\tilde{\alpha}_{|\iota(K[U])}$ that

$$\tilde{\alpha}(g + P) = \tilde{\alpha}(N + P)/\tilde{\alpha}(D + P) = (N + \hat{I})/(D + \hat{I}) \in \mathrm{Quot}(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}).$$

This implies that the normal form of $\alpha(g)$ with respect to $\mathcal{H}$ is exactly $(N + \hat{I})/(D + \hat{I})$, and hence the calculation of $\mathrm{NF}_{\mathcal{H}}(\alpha(g))$ yields the desired representation, as claimed.

Finally, since we are interested in the invariant ring $K[U]^G$ but have computed generators of the isomorphic invariant ring $K[\hat{U}]^G$, we have to apply the homomorphism which sends $\hat{x}_i + \hat{I}$ to ϕ_i (for $i \in \{1, \ldots \hat{n}\}$) to obtain generators of $K[U]^G$ (cf. Remark 4.23(a)). ∎

Whereas this algorithm together with its proof of correctness is rather long, an application to concrete situations might be quite simple. In the following, we give an example, which is interesting since it is based on a quasi-affine variety whose ring of regular functions is known not to be finitely generated. Up to now, there was no systematic approach to tackle such a problem algorithmically.

Example 4.40. Let K be the algebraic closure of $\mathbb{Q}$. Furthermore, let

$$X := \mathrm{Var}(x_5x_1 - x_2x_4 + x_3, x_6x_1^6 - x_2^3 - x_3^2) \subset K^6$$

be an affine variety and let U be the quasi-affine variety given by

$$U := X \setminus \mathrm{Var}(x_1, x_2, x_3).$$

In [Win03], Winkelmann constructed this quasi-affine variety U from a counterexample to Hilbert's 14th Problem (cf. [DF99]). It follows from his construction that the ring of regular functions of U is not finitely generated.
We claim that the unipotent group $G_a = (K, +)$ acts on U via

$$\mu : G_a \times U \longrightarrow U,\ (\lambda, (\xi_1, \ldots, \xi_6)) \longmapsto (\xi_1, \xi_2, \xi_3, \xi_4 - \lambda\xi_1^2, \xi_5 - \lambda\xi_1\xi_2, \xi_6).$$

Clearly $\mu : G \times U \longrightarrow K^6$ is a morphism. We have to ensure that $\mu(G_a \times U) \subset U$. So take $\lambda \in K$ and $(\xi_1, \ldots, \xi_6) \in U$ and set $(\xi_1', \ldots, \xi_6') := \mu(\lambda, (\xi_1, \ldots, \xi_6))$. Then one calculates

$$\xi_5'\xi_1' - \xi_2'\xi_4' + \xi_3' = \xi_5\xi_1 - \lambda\xi_1^2\xi_2 - \xi_2\xi_4 + \lambda\xi_2\xi_1^2 + \xi_3 = 0$$

and

$$\xi_6'\xi_1'^6 - \xi_2'^3 - \xi_3'^2 = \xi_6\xi_1^6 - \xi_2^3 - \xi_3^2 = 0.$$

Moreover, not all of ξ_1', ξ_2', ξ_3' are zero since this is true for ξ_1, ξ_2, ξ_3 and it follows that $\mu(\lambda, (\xi_1, \ldots, \xi_6)) \in U$.
Together with an easy check of the axioms for an action, this shows that μ defines a regular action of G_a on U, as claimed. In the following, we demonstrate how Algorithm 4.38 may be used to calculate the invariant ring $K[U]^{G_a}$. We do this step-by-step.
The morphism μ can be extended to $G \times X$ in the obvious way, that is

$$\mu : G_a \times X \longrightarrow X,\ (\lambda, (\xi_1, \ldots, \xi_6)) \longmapsto (\xi_1, \xi_2, \xi_3, \xi_4 - \lambda\xi_1^2, \xi_5 - \lambda\xi_1\xi_2, \xi_6),$$

and as this extension actually defines an action of G_a on X, step (1) of the Algorithm is superfluous. So, $\hat{x}_1 := x_1, \ldots, \hat{x}_6 := x_6$, $\hat{I} := (\hat{x}_5\hat{x}_1 - \hat{x}_2\hat{x}_4 + \hat{x}_3, \hat{x}_6\hat{x}_1^6 - \hat{x}_2^3 - \hat{x}_3^2)$, $\hat{L} := (\hat{x}_1, \hat{x}_2, \hat{x}_3)$, $\hat{X} := X$, $\hat{U} := U = \mathrm{Var}(\hat{I}) \setminus \mathrm{Var}(\hat{L})$, $\hat{\mu} := \mu$ and $\phi := \mathrm{id}$.
For simplicity, we use van den Essen's Algorithm for calculating step (2). Choosing $\hat{x}_1^2 + \hat{I}$

for the element to be localized, this yields

$$K[\hat{X}]^{G_a}_{\hat{x}_1^2+\hat{I}} = K[\hat{x}_1+\hat{I}, \hat{x}_2+\hat{I}, \hat{x}_3+\hat{I}, \hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+\hat{I}, \hat{x}_6+\hat{I}, 1/(\hat{x}_1^2+\hat{I})].$$

So we can set

$$f_1 := \hat{x}_1,\ f_2 := \hat{x}_2,\ f_3 := \hat{x}_3,\ f_4 := \hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2,\ f_5 := \hat{x}_6 \text{ and } f := \hat{x}_1^2.$$

According to step (3), we define

$$S := K[\hat{x}_1, \hat{x}_2, \hat{x}_3, \hat{x}_4, \hat{x}_5, \hat{x}_6, T_1, T_2, T_3]/P$$

with

$$P := (\hat{x}_5\hat{x}_1-\hat{x}_2\hat{x}_4+\hat{x}_3, \hat{x}_6\hat{x}_1^6-\hat{x}_2^3-\hat{x}_3^2, \hat{x}_1\cdot T_1+\hat{x}_2\cdot T_2+\hat{x}_3\cdot T_3-1).$$

Next, by step (4), we have to compute a reduced Gröbner basis of the ideal

$$\begin{aligned} Q := (&Z_1-(\hat{x}_1+P), Z_2-(\hat{x}_2+P), Z_3-(\hat{x}_3+P), Z_5Z_1-Z_4Z_2-(\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+P),\\ &Z_6-(\hat{x}_6+P), Z_1^2-(\hat{x}_1^2+P), Z_5Z_1-Z_2Z_4+Z_3, Z_6Z_1^6-Z_2^3-Z_3^2,\\ &Z_1\cdot W_1+Z_2\cdot W_2+Z_3\cdot W_3-1)\\ \trianglelefteq\ &\mathrm{Quot}(K[f_1+P,\ldots,f_5+P,f+P])[Z_1,Z_2,Z_3,Z_4,Z_5,Z_6,W_1,W_2,W_3] \end{aligned}$$

with respect to an arbitrary monomial order on the monomials in $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$, W_1, W_2, W_3. For the lexicographical order $W_3 \leq W_2 \leq W_1 \leq Z_6 \leq Z_5 \leq Z_4 \leq Z_3 \leq Z_2 \leq Z_1$, the computer algebra system Magma (cf. [BCP97]) yields

$$\begin{aligned} \mathcal{G} = \{&Z_1-(\hat{x}_1+P), Z_2-(\hat{x}_2+P), Z_3+(\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+P), Z_6-(\hat{x}_6+P)\\ &Z_4-(\hat{x}_1+P)/(\hat{x}_2+P)\cdot Z_5+(\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+P)/(\hat{x}_2+P),\\ &W_1+(\hat{x}_2+P)/(\hat{x}_1+P)\cdot W_2-(\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+P)/(\hat{x}_1+P)\cdot W_5-1/(\hat{x}_1+P)\}. \end{aligned}$$

Hence we can set

$$\begin{aligned} &h_1 := \hat{x}_1^2\hat{x}_2,\ h_2 := \hat{x}_1\hat{x}_2^2,\ h_3 := (\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2)\hat{x}_1\hat{x}_2,\ h_4 := \hat{x}_6\hat{x}_1\hat{x}_2,\ h_5 := \hat{x}_1^2,\\ &h_6 := (\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2)\hat{x}_1,\ h_7 := \hat{x}_2^2,\ h_8 := (\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2)\hat{x}_2,\ h_9 := \hat{x}_2 \text{ and } h := \hat{x}_1\hat{x}_2. \end{aligned}$$

It now remains to compute

$$(K[h_1+P,\ldots,h_9+P,h+P] : (h+P)^\infty)_S$$

in the loop (7)-(11). A computation with Magma shows that this algebra is given by

$$K[\hat{x}_5\hat{x}_1-\hat{x}_4\hat{x}_2+P, \hat{x}_1+P, \hat{x}_2+P, \hat{x}_6+P].$$

To sum it up, we have found finitely many generators of $K[U]^G$, that is

$$K[U]^G = K[x_5x_1 - x_4x_2 + I, x_1 + I, x_2 + I, x_6 + I]. \qquad \triangleleft$$

Some remarks about a variant of the algorithm for normal quasi-affine varieties

Algorithm 4.38 is rather complex, it requires computations of Gröbner bases several times. As the runtime behaviour of a Gröbner basis computation may be highly influenced by the number of variables of the underlying polynomial ring, it is worth to think about how the number of variables in steps (3) & (4), that is – with the notation of Algorithm 4.38 – $\hat{n} + \hat{t}$, can be reduced. For the special case that U is a normal quasi-affine variety, it will be shown in the following that actually $\hat{t} = 2$ can be achieved.
For this, U will be replaced by another quasi-affine variety U' with $K[U] \cong K[U']$. This isomorphism induces an action of G on $K[U']$ which – as we will see – will allow us to assume $\hat{t} = 2$ by the special choice of U'. Note that this does not imply that G acts regularly on U'. Indeed, there is just an algebraic correspondence between $K[U]$ and $K[U']$. To be more general, unlike to the affine case, an action $K[U] \longrightarrow K[G] \otimes_K K[U]$ of a linear algebraic group G on the ring of regular functions $K[U]$ of a quasi-affine variety U does not necessarily originate from a regular action of G on U (cf. also Proposition 1.29).

Example 4.41. Consider the quasi-affine variety $U := K^2 \setminus \{(1,1)\}$. As we have seen for similar examples before, the ring of regular functions is given by $K[U] = K[x_1, x_2]$, where as usual x_1, x_2 denote the coordinate functions on K^2. Let the multiplicative group $G := K^\times$ act on $K[U]$ via

$$\lambda(x_1) := \lambda x_1,\ \lambda(x_2) := \lambda x_2 \qquad \text{for all } \lambda \in G.$$

Then there is no regular action of G on U which induces this action on $K[U]$. $\triangleleft$

Later, in fact, we will show that if G acts on $K[U]$ via $K[U] \longrightarrow K[G] \otimes_K K[U]$, where U is some quasi-affine variety, then there always exists a quasi-affine G-variety such that its ring of regular functions and $K[U]$ are G-isomorphic.

The next lemma gives an explicit construction of the quasi-affine variety U' which was mentioned a few lines above. Essentially, this lemma is drawn from a proof given by Winkelmann in [Win03]. Nonetheless, we repeat it here for creating a reference, since this result – apart from being useful for an adjustment of Algorithm 4.38 to normal varieties – will also be needed for the proof of a theorem in the next section.

Lemma 4.42. *Let U be a normal quasi-affine variety. Then there exists a normal affine variety $\hat{X}$, say $\hat{X} = \mathrm{Var}(\hat{I})$ for some prime ideal $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$ with $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ new*

indeterminates over K, and regular functions $q_1' + \hat{I}, q_2' + \hat{I} \in K[\hat{X}]$ such that

$$K[U] \cong (K[\hat{X}] : (q_1' + \hat{I}, q_2' + \hat{I})^\infty)_{\mathrm{Quot}(K[\hat{X}])}.$$

In other words, we can always find an open subset $U' := \hat{X} \setminus \mathrm{Var}_{\hat{X}}(q_1' + \hat{I}, q_2' + \hat{I})$ of a normal affine variety $\hat{X}$ such that U' is the complement of a closed subset in $\hat{X}$ given by two regular functions and $K[U']$ is isomorphic to $K[U]$.

Remark. In general, the quasi-affine varieties U and U' are not isomorphic. ♢

Proof. By Proposition 4.7, the normal quasi-affine variety U can be embedded as an open subset $\hat{U}$ in a normal affine variety $\hat{X} \subset K^{\hat{n}}$. Let $\hat{x}_1, \ldots, \hat{x}_{\hat{n}}$ be the coordinate functions on $K^{\hat{n}}$ and set

$$\hat{I} := \mathrm{Id}(\hat{X}) \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}] \quad \text{and} \quad \widetilde{L} := \mathrm{Id}_{K[\hat{X}]}(\hat{X} \setminus \hat{U}) \trianglelefteq K[\hat{X}].$$

By Proposition 4.7, U is isomorphic to $\hat{U}$. We thus have

$$K[U] \cong (K[\hat{X}] : \widetilde{L}^\infty)_{\mathrm{Quot}(K[\hat{X}])}.$$

In case that $\widetilde{L} = K[\hat{X}]$, we can set $q_1' := q_2' := 1$. Then obviously

$$K[U] \cong (K[\hat{X}] : (q_1' + \hat{I}, q_2' + \hat{I})^\infty)_{\mathrm{Quot}(K[\hat{X}])}$$

and the lemma is proved. Otherwise, let M be the finite set of all prime ideals of $K[\hat{X}]$ which are minimal over $\widetilde{L}$. Then $\widetilde{L} = \bigcap_{\mathfrak{p} \in M} \mathfrak{p}$ is the (unique) minimal decomposition of $\widetilde{L}$ into distinct primes (see [Eis95], Chapter 3). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be those primes of M, which are of height one in $K[\hat{X}]$ and set $L' := \bigcap_{i=1}^s \mathfrak{p}_i$. In case that there are no primes of height one in M, set $L' := K[X]$. By Proposition 4.7 and Remark 4.26, we then have

$$\begin{aligned} K[U] &\cong (K[\hat{X}] : \widetilde{L}^\infty)_{\mathrm{Quot}(K[\hat{X}])} \\ &= (K[\hat{X}] : L'^\infty)_{\mathrm{Quot}(K[\hat{X}])}. \end{aligned} \tag{4.24}$$

In case that $L' = K[\hat{X}]$, we can set $q_1' := q_2' := 1$ and the lemma is proved. Otherwise, let $q_1' + \hat{I} \in L' \setminus \{0\}$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_{s'}$ be the distinct prime ideals of height one which are minimal over $(q_1' + \hat{I})_{K[\hat{X}]}$ but do not contain L'. If there do not exist such prime ideals, set $q_2' := q_1'$. Otherwise, there exists $q_2' + \hat{I} \in L'$ such that $q_2' + \hat{I} \notin \mathfrak{q}_1, \ldots, \mathfrak{q}_{s'}$. This can be seen as follows. Choose a nonzero element

$$q_{2,j}' + \hat{I} \in \left(\bigcap_{i=1}^{s} \mathfrak{p}_i \cap \bigcap_{i=1, i \neq j}^{s'} \mathfrak{q}_i \right) \setminus \mathfrak{q}_j$$

for every $j = 1, \ldots, s'$. Note that the right hand side of the above formula is not the empty set since by construction $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{q}_1, \ldots, \mathfrak{q}_{s'}$ are distinct prime ideals of height one. Now

it is not hard to see, that $q_2' := \sum_{i=1}^{s'} q_{2,j}'$ has the desired properties.
By construction, the set of prime ideals of height one minimal over $(q_1' + \hat{I}, q_2' + \hat{I})_{K[\hat{X}]}$ equals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Hence it follows by Remark 4.26 again that

$$(K[\hat{X}] : L'^{\infty})_{\mathrm{Quot}(K[\hat{X}])} = (K[\hat{X}] : (q_1' + \hat{I}, q_2' + \hat{I})^{\infty}_{K[\hat{X}]})_{\mathrm{Quot}(K[\hat{X}])}.$$

Combining this with equation (4.24) proves the lemma. ∎

As indicated above, the previous lemma allows a reduction of the number of variables in steps (3) et seqq. of Algorithm 4.38. We will only sketch the details. Keeping in mind that there are algorithms for the computation of the primary decomposition of an ideal, for testing equality of ideals, as well as for the intersection of ideals (cf. [BW93], Chapter 6 & 8), it is clear that the proof of Lemma 4.42 can be made constructive in the sense that the elements $q_1' + \hat{I}, q_2' + \hat{I}$ can be found algorithmically. We can therefore adjust Algorithm 4.38 in the following way. For step (1), we can use a version of Algorithm 4.22 which respects the normality of U, i. e. a version which embeds U in a normal affine G-variety $\hat{X}$ (cf. Remark 4.23(b)). Furthermore, we insert one additional step between the steps (2) and (3) to replace $\hat{L}$ by an ideal L' which is generated by only two elements. As mentioned above, the resulting G-isomorphism between $K[\hat{U}]$ and $K[\hat{X} \setminus \mathrm{Var}(L')]$ does not imply that G acts regularly on $\hat{X} \setminus \mathrm{Var}(L')$. Nonetheless, one can check that the parts of the proof of correctness of Algorithm 4.38 corresponding to steps (3) et seqq. do not need a regular action of G on the quasi-affine variety $\hat{X} \setminus \mathrm{Var}(L')$. The arguments used there just require an action of G on $K[\hat{X} \setminus \mathrm{Var}(L')]$ which can be described by a homomorphism $K[\hat{X} \setminus \mathrm{Var}(L')] \longrightarrow K[G] \otimes_K K[\hat{X} \setminus \mathrm{Var}(L')]$. By construction, this condition is satisfied for the action of G on $K[\hat{X} \setminus \mathrm{Var}(L')]$.

Note that although the value of $\hat{t}$ is limited to 2 in this variant of Algorithm 4.22, we get additional complexity by the new parts which we have inserted. From a theoretical point of view, though, some facts of this section will turn out to be valuable tools for the proof of Theorem 4.43 below.

Remark. The examination of the case of a normal quasi-affine variety was inspired by the paper [Win03] of Winkelmann. ♢

A generalization of a theorem of Nagata and Winkelmann

As mentioned at the very beginning of this chapter, the invariant ring of an algebraic group acting regularly on a normal affine variety is always isomorphic to the ring of regular functions of some normal quasi-affine variety. In the following, we will generalize this result to the case of an algebraic group acting regularly on a normal quasi-affine variety.
As we will see in the next section, this might by useful for algorithmic purposes. In fact, it might help to compute the invariant ring of an arbitrary algebraic group acting regularly on a factorial variety.

Theorem 4.43. *Let G be a linear algebraic group acting regularly on a normal quasi-affine variety U. Then there exists a quasi-affine variety V such that $K[U]^G \cong K[V]$.*

Proof. By Lemma 4.42, there exists a normal affine variety $\hat{X} = \mathrm{Var}(\hat{I}) \subset K^{\hat{n}}$ (for some prime ideal $\hat{I} \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$) and regular functions $q_1' + \hat{I}, q_2' + \hat{I} \in K[\hat{X}]$ such that the ring of regular functions of $U' := \hat{X} \setminus \mathrm{Var}_{\hat{X}}(q_1' + \hat{I}, q_2' + \hat{I})$ is isomorphic to the ring of regular functions of U, i. e.

$$K[U'] \cong K[U].$$

Set

$$P := (\hat{I})_{K[\hat{x}_1,\ldots,\hat{x}_{\hat{n}},T_1,T_2]} + (q_1' \cdot T_1 + q_2' \cdot T_2 - 1) \trianglelefteq K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, T_2]$$

and

$$S := K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, T_2]/P$$

where T_1, T_2 are indeterminates over K (cf. Algorithm 4.38). Note that the algebra S can be interpreted as the coordinate ring of the affine variety

$$Y := \hat{X} \times_{K^2} \mathrm{SL}_2(K) := \left\{ \left(p, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) \in \hat{X} \times \mathrm{SL}_2(K);\ \phi(p) = \psi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right\},$$

where the fibre product of $\hat{X}$ and $\mathrm{SL}_2(K)$ over K^2 is taken with respect to the morphisms

$$\phi : \hat{X} \longrightarrow K^2,\ p \longmapsto \begin{pmatrix} q_1'(p) \\ -q_2'(p) \end{pmatrix}$$

and

$$\psi : \mathrm{SL}_2(K) \longrightarrow K^2,\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \alpha \\ \gamma \end{pmatrix}.$$

We claim that there exists a regular action of the additive group $G_a = (K, +)$ on Y such that $K[U']$ is isomorphic to S^{G_a}. The same has originally been proven by Winkelmann (see [Win03], Proposition 1), we hence only sketch a proof of this claim here.
Let the additive group G_a act on $\mathrm{SL}_2(K)$ via

$$\lambda \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} := \begin{pmatrix} \alpha & \beta + \lambda\alpha \\ \gamma & \delta + \lambda\gamma \end{pmatrix} \qquad \text{for all } \lambda \in G,\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(K).$$

Note that this action induces a regular action of G_a on Y given by

$$\lambda \left(p, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) := \left(p, \begin{pmatrix} \alpha & \beta + \lambda\alpha \\ \gamma & \delta + \lambda\gamma \end{pmatrix} \right) \qquad \text{for all } \lambda \in G,\ \left(p, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) \in Y.$$

Now the map

$$Y \longrightarrow U',\ \left(p, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) \longmapsto p$$

defines a surjective morphism which is constant on the orbits of G_a on Y. In fact, this map defines a so-called geometric quotient for the action of G_a on Y. This implies that

the corresponding homomorphism

$$\iota : K[U'] \longrightarrow S,\ \hat{x}_i + \hat{I} \longrightarrow \hat{x}_i + P \qquad \text{for } i = 1, \ldots, \hat{n}$$

defines an isomorphism of $K[U']$ and S^{G_a}, i. e.

$$\iota(K[U']) = S^{G_a}, \tag{4.25}$$

as claimed.

By assumption, G acts regularly on U. This induces an action of G on $K[U]$ (via K-algebra automorphisms), hence on $K[U']$ and this in turn induces an action of G on S^{G_a} via (4.25). It follows that

$$K[U]^G \cong K[U']^G \cong (S^{G_a})^G = \mathrm{Quot}(S^{G_a})^G \cap S^{G_a} = \mathrm{Quot}(S^{G_a})^G \cap S. \tag{4.26}$$

Let $\widetilde{S}$ be the normalization of S. We claim that

$$(\mathrm{Quot}(S^{G_a}))^G \cap S = \mathrm{Quot}(S^{G_a})^G \cap \widetilde{S}. \tag{4.27}$$

Assume for a moment that this is true. Then combining (4.26) and (4.27) yields

$$K[U]^G \cong \mathrm{Quot}(S^{G_a})^G \cap \widetilde{S}$$

and since $\widetilde{S}$ is a normal ring, an application of Theorem 2 of [Win03] shows that the intersection $\mathrm{Quot}(S^{G_a})^G \cap \widetilde{S}$ is isomorphic to the ring of regular functions of some quasi-affine variety V, i. e. $K[U]^G \cong K[V]$, which we wanted to prove.

It remains to prove equality (4.27). Clearly the left hand side is contained in the right hand side. For the reverse conclusion, let $(f + P)/(g + P) \in \mathrm{Quot}(S^{G_a})^G \cap \widetilde{S}$. By (4.25) above, we may assume that both f and g are contained in $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]$. Since $(f+P)/(g+P)$ is integral over S, there exist $c_0, \ldots, c_{s-1} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, T_2]$ such that

$$\left(\frac{f+P}{g+P}\right)^s + (c_{s-1} + P) \cdot \left(\frac{f+P}{g+P}\right)^{s-1} + \ldots + (c_1 + P) \cdot \frac{f+P}{g+P} + (c_0 + P) = 0.$$

Multiplying that equation by $(g + P)^s$ yields

$$f^s + c_{s-1} \cdot g \cdot f^{s-1} + \ldots + c_1 \cdot g^{s-1} \cdot f + c_0 \cdot g^s \in P. \tag{4.28}$$

Consider the homormophism

$$\begin{aligned} \phi : K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, T_2] &\longrightarrow (K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})_{q_1' + \hat{I}} \\ F(\hat{x}_1, \ldots, \hat{x}_{\hat{n}}, T_1, T_2) &\longmapsto F(\hat{x}_1 + \hat{I}, \ldots, \hat{x}_{\hat{n}} + \hat{I}, 1/(q_1' + \hat{I}), 0). \end{aligned}$$

Obviously, $P \subset \ker \phi$ and thus, applying ϕ to equation (4.28) yields

$$(f+\hat{I})^s + \phi(c_{s-1}) \cdot (g+\hat{I}) \cdot (f+\hat{I})^{s-1} + \ldots \\ + \phi(c_1) \cdot (g+\hat{I})^{s-1}(f+\hat{I}) + \phi(c_0) \cdot (g+\hat{I})^s = 0.$$

But this implies that

$$\left(\frac{f+\hat{I}}{g+\hat{I}}\right)^s + \phi(c_{s-1}) \cdot \left(\frac{f+\hat{I}}{g+\hat{I}}\right)^{s-1} + \ldots + \phi(c_1) \cdot \frac{f+\hat{I}}{g+\hat{I}} + \phi(c_0) = 0.$$

and it follows that $(f+\hat{I})/(g+\hat{I})$ is integral over $(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})_{q_1'+\hat{I}}$. By construction, $K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ is normal and since localization commutes with normalization (cf. [Eis95], Chapter 4, Proposition 4.13), the algebra $(K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})_{q_1'+\hat{I}}$ is normal, too. Therefore, $(f+\hat{I})/(g+\hat{I}) \in (K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I})_{q_1'+\hat{I}}$. In particular, this means that

$$(f+\hat{I})/(g+\hat{I}) \cdot (q_1'+\hat{I})^k \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$$

for some $k \in \mathbb{N}_0$. Similarly, it follows that

$$(f+\hat{I})/(g+\hat{I}) \cdot (q_2'+\hat{I})^{k'} \in K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$$

for some $k' \in \mathbb{N}_0$. But this implies that $(f+\hat{I})/(g+\hat{I}) \cdot (q_1+\hat{I}, q_2+\hat{I})^{k+k'} \subset K[\hat{x}_1, \ldots, \hat{x}_{\hat{n}}]/\hat{I}$ and therefore $(f+\hat{I})/(g+\hat{I}) \in K[U]$ (cf. equation (4.1)).
Putting this together yields $(f+P)/(g+P) \in \iota(K[U']) \subset S$, which finally proves equation (4.27). ∎

4.3.4 Some remarks about reductive groups and a reduction argument for the computation of invariants of arbitrary linear algebraic groups

In the preceding sections of this chapter, we have developed algorithms for the computation of the invariant ring of a linear algebraic group G acting regularly on an irreducible quasi-affine variety for the case that G is a finite or a unipotent group. Unfortunately, the ideas behind these algorithms cannot be generalized nicely to the reductive case. As we have seen, Algorithm 4.34 works for reductive groups for some special cases. At least it is possible to decide algorithmically whether it is applicable or not for a given input data. The algorithm for unipotent groups (Algorithm 4.38) yields correct results for every linear algebraic group where – with the notation of this algorithm – the identity $\mathrm{Quot}(K[\hat{X}]^G) = K(\hat{X})^G$ holds. Of course it is satisfied for every unipotent group. But again, this identity and thus the applicability of Algorithm 4.38 fails for reductive groups in general. To sum it up, the case that G is reductive still remains unsolved.

As mentioned at the very beginning of this chapter, the case of a reductive group is not only interesting for the sake of its own. It could also be used to construct an algorithm for computing the invariant ring of an arbitrary linear algebraic group G acting regularly

on a normal affine variety X. The rough idea is as follows (cf. [DK08]). First compute the invariant ring $K[X]^N$ of the unipotent radical N of G. Since N is a normal subgroup of G, it follows that the reductive group G/N acts on $K[X]^N$ (via K-algebra homomorphisms). Moreover, it can be shown that this action can be described by a homomorphism of algebras $K[X]^N \longrightarrow K[G/N] \otimes_K K[X]^N$ in the usual sense. Although – as we know – the invariant ring $K[X]^N$ is isomorphic to the ring of regular functions of some quasi-affine variety, this algebraic situation does not necessarily correspond to the geometric situation of the reductive group G/N acting regularly on this quasi-affine variety. Example 4.41 demonstrates this problem. Fortunately, we will prove in the following proposition that there always exists a quasi-affine G/N-variety U such that $K[X]^N$ and $K[U]$ are isomorphic as G/N-algebras (cf. also Proposition 1.29). Therefore, as hinted above, an algorithm for computing invariants of reductive groups acting on quasi-affine varieties would provide a possibility for the computation of $K[X]^G$, indeed.

Proposition 4.44. *Let S be a K-algebra of the form $S = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)}$ where R is an affine domain over K and $\mathfrak{a} \trianglelefteq R$ is a non-zero ideal. Let G be a linear algebraic group and let $\tilde{\mu} : S \longrightarrow K[G] \otimes_K S$ be a homomorphism of K-algebras such that*

$$\sigma(s) := \tilde{\mu}(s)(\sigma) \quad \text{for all } s \in S,\ \sigma \in G$$

defines an action of G on S. Then there exists an irreducible quasi-affine G-variety U such that $K[U]$ and S are G-isomorphic.

Proof. By Proposition 1.31(a), the action of G on S is locally finite. Hence there exists a G-stable affine algebra $\widetilde{R}$ with $R \subset \widetilde{R} \subset S$. Set $\widetilde{\mathfrak{a}} := (G(\mathfrak{a}))_{\widetilde{R}} := (\sigma(a);\ \sigma \in G, a \in \mathfrak{a})_{\widetilde{R}}$. We claim that

$$S = (\widetilde{R} : \widetilde{\mathfrak{a}}^\infty)_{\mathrm{Quot}(\widetilde{R})}.$$

Let $r/r' \in S = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)}$. Since G acts locally finite on S, it follows that there exists a finite dimensional G-stable vector space $V \subset S$ with $r/r' \in V$. By definition of S and the finite dimension of V, we can find $k \in \mathbb{N}_0$ such that

$$\sigma(r/r') \cdot \mathfrak{a}^k \subset R \quad \text{for all } \sigma \in G. \tag{4.29}$$

Note that – as $\widetilde{R}$ is an affine algebra – the ideal $\widetilde{\mathfrak{a}}$ is finitely generated. So let $\mathcal{M} \subset G$ and $\mathcal{N} \subset \mathfrak{a}$ be finite sets such that $\widetilde{\mathfrak{a}}$ is generated by $\{\sigma(a);\ \sigma \in \mathcal{M}, a \in \mathcal{N}\}$. The ideal $\widetilde{\mathfrak{a}}^{|\mathcal{M}|\cdot|\mathcal{N}|\cdot k}$ is generated by products of length $|\mathcal{M}| \cdot |\mathcal{N}| \cdot k$ where the factors are elements of $\{\sigma(a);\ \sigma \in \mathcal{M}, a \in \mathcal{N}\}$. By a standard combinatorial argument, every such generator is divisible by $\sigma(a)^k$ for some $\sigma \in \mathcal{M}, a \in \mathcal{N}$. This shows that for every element $b \in \widetilde{\mathfrak{a}}^{|\mathcal{M}|\cdot|\mathcal{N}|\cdot k}$, there are elements $b_{\sigma,a} \in \widetilde{R}$ for all $\sigma \in \mathcal{M}, a \in \mathcal{N}$ such that b can be written

as $b = \sum_{\sigma\in\mathcal{M},a\in\mathcal{N}} \sigma(a)^k \cdot b_{\sigma,a}$. Together with equation (4.29) it follows that

$$r/r' \cdot b = r/r' \cdot \sum_{\sigma\in\mathcal{M},a\in\mathcal{N}} \sigma(a)^k \cdot b_{\sigma,a} = \sum_{\sigma\in\mathcal{M},a\in\mathcal{N}} \sigma(\sigma^{-1}(r/r') \cdot a^k) \cdot b_{\sigma,a}$$
$$\subset \sum_{\sigma\in\mathcal{M},a\in\mathcal{N}} \sigma(R) \cdot \widetilde{R} \subset \widetilde{R}.$$

But this means that $r/r' \cdot \widetilde{\mathfrak{a}}^{|\mathcal{M}|\cdot|\mathcal{N}|\cdot k} \subset \widetilde{R}$ and therefore $r/r' \in (\widetilde{R} : \widetilde{\mathfrak{a}}^{\infty})_{\mathrm{Quot}(\widetilde{R})}$.
For the reverse inclusion, let $r/r' \in (\widetilde{R} : \widetilde{\mathfrak{a}}^{\infty})_{\mathrm{Quot}(\widetilde{R})}$. By definition, there exists $k \in \mathbb{N}_0$ such that $r/r' \cdot \widetilde{\mathfrak{a}}^k \subset \widetilde{R}$. Let $a_1, \ldots, a_s \in R$ be generators of the ideal $\mathfrak{a}^k$. Then of course, $r/r' \cdot a_i \in \widetilde{R}$ and since $\widetilde{R}$ is contained in S there exists $k' \in \mathbb{N}_0$ such that $r/r' \cdot a_i \cdot \mathfrak{a}^{k'} \subset R$ for all $i = 1, \ldots, s$. But this means $r/r' \cdot \mathfrak{a}^{k+k'} \subset R$ and it follows that $r/r' \in S$, as claimed.

By construction, $\widetilde{R}$ is stable under G and hence Proposition 1.31(b) implies that the action of G on $\widetilde{R}$ can be described by a homomorphism $\widetilde{R} \longrightarrow K[G] \otimes_K \widetilde{R}$. It then follows by Proposition 1.29 that there is an irreducible affine G-variety X such that $K[X]$ and $\widetilde{R}$ are G-isomorphic. By definition, the ideal $\widetilde{\mathfrak{a}}$ is G-stable. Regarding $\widetilde{\mathfrak{a}}$ as an ideal of $K[X]$, it follows that $U := X \setminus \mathrm{Var}_X(\widetilde{\mathfrak{a}})$ is G-stable, too.
Finally, note that by construction the algebras $K[U]$ and S are G-isomorphic, which proves the proposition. ∎

For the computation of invariants of arbitrary linear algebraic groups acting on normal affine varieties as suggested in the outline above, we need an algorithm for the computation of invariants of reductive groups acting on normal quasi-affine varieties. As indicated before, we do not have an algorithm for the reductive case, yet. For the important special case of an arbitrary linear algebraic group acting on a factorial variety, it is in fact enough to solve the problem of finding an algorithm for computing invariants of the one-dimensional torus $T := K^\times$ acting regularly on a quasi-affine variety U. Finding an algorithm for such a special case might be much simpler than the more general case of a reductive group. For the remainder of this section, we want to give a sketch of how invariants of arbitrary linear algebraic groups could be computed if we had an algorithm for the computation of $K[U]^T$. Note that this is only a sketch – we do not prove all the details.
For what follows, let G be an arbitrary linear algebraic group acting regularly on a factorial variety X.

Assumption 4.45. *Let the one-dimensional torus $T := K^\times$ act regularly on an irreducible quasi-affine variety U. We assume that there exists an algorithm for the computation of $K[U]^T$. More precisely, according to Theorem 4.43, we assume that there exists an algorithm for the computation of $K[U]^T$ which returns a finitely generated algebra $R \subset K[U]^T$ and a non-zero ideal $\mathfrak{a} \trianglelefteq R$ such that the invariant ring is given by $K[U]^T = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)}$.*

The rough idea for the computation of $K[X]^G$ is as follows. First compute a normal

series $G = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_s$ such that there is an algorithm for writing $K[X]^{N_s}$ as the ring of regular functions of some quasi-affine variety and such that for $j = 0, \ldots, s-1$ the quotient group N_j/N_{j+1} is either finite or isomorphic to T. Then by Assumption 4.45 and Algorithm 4.34, the invariant ring $K[X]^G$ can be computed successively via

$$\begin{aligned} K[X]^{N_{s-1}} &= (K[X]^{N_s})^{N_{s-1}/N_s} \\ K[X]^{N_{s-2}} &= (K[X]^{N_{s-1}})^{N_{s-2}/N_{s-1}} \\ &\vdots \\ K[X]^G = K[X]^{N_0} &= (K[X]^{N_1})^{N_0/N_1}. \end{aligned}$$

In the following, we make this rough idea a bit more explicit. We first discuss briefly how the computation of a normal series $G = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_s$ with the desired properties can be realized algorithmically. We then give some hints about the computation of $K[X]^G$ along this chain of subgroups.

For the following lemma, we need the definition of the finite generation locus ideal.

Proposition and Definition 4.46 (Derksen and Kemper ([DK08])). *Let S be an affine domain over K and let $R \subset S$ be a subalgebra. The set $\mathfrak{g}$ of elements $f \in R$ such that the localization R_f is finitely generated over K, i. e.*

$$\mathfrak{g} := \{f \in R;\ R_f \text{ is finitely generated as a } K\text{-algebra}\}$$

is a non-zero radical ideal of R. It is called the **finite generation locus ideal of R.** ∎

Lemma 4.47. *Let G be a connected linear algebraic group acting regularly on a factorial affine variety X. Let $\mathfrak{g}$ be the finite generation locus ideal of $K[X]^G$. If $(\mathfrak{g})_{K[X]} \trianglelefteq K[X]$ is of codimension one, then there exists a semi-invariant $f \in K[X]$ which is not invariant.*

Remark. The proof of this lemma is an adaption of an argument originally given by Derksen and Kemper in [DK08]. ♢

Proof. Let $(\mathfrak{g})_{K[X]}$ be of codimension one in $K[X]$. Then by definition, there exists a codimension one prime ideal which is minimal over $(\mathfrak{g})_{K[X]}$. Moreover, since $K[X]$ is factorial, this prime ideal is generated by one element, say $f \in K[X]$. We will show in the following that f is a semi-invariant which is not invariant. Clearly, the ideal $(\mathfrak{g})_{K[X]}$ is stable under G and since G is connected, all the prime ideals which are minimal over $(\mathfrak{g})_{K[X]}$ are G-stable, too. In particular, this is the case for $(f)_{K[X]}$. It follows that f is a semi-invariant.
Assume for a contradiction that f is invariant. The invariant ring is isomorphic to the ring of regular functions of some quasi-affine variety. Hence there exists an affine domain $R \subset K[X]^G$ and an ideal $\mathfrak{a} \trianglelefteq R$ such that $K[X]^G = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)}$. Note that for

all $a \in \mathfrak{a}$ we have $K[X]^G = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)} \subset R_a$ and thus $K[X]^G_a = R_a$ is finitely generated. It follows that $\mathfrak{a} \subset \mathfrak{g} \subset (f)_{K[X]}$. This implies that $f^{-1}\mathfrak{a} \subset K[X]^G$ and $f^{-1} \in (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)} = K[X]^G \subset K[X]$. But obviously $f^{-1} \notin K[X]$, a contradiction. ∎

Remark 4.48. The proof of this lemma can be made constructive in the following sense. Assume that for some connected linear algebraic group G the invariant ring $K[X]^G$ is given in the form $K[X]^G = (R : f^\infty)_{K[X]}$ where $R \subset K[X]^G$ is an affine domain and $f \in R \setminus \{0\}$. For algebras of this type, Derksen and Kemper have developed an algorithm for the computation of the finite generation locus ideal $\mathfrak{g}$ (cf. [DK08], Algorithm 2.13). Their algorithm produces a sequence of algebras $R_1 \subset R_2 \subset \ldots$ and a sequence of ideals $\mathfrak{g}_1 \subset \mathfrak{g}_2 \subset \ldots$ with $\mathfrak{g}_i \trianglelefteq R_i$ for all $i \geq 1$ such that

$$K[X]^G = \bigcup_{i \geq 1} R_i \text{ and } \mathfrak{g} = \bigcup_{i \geq 1} \mathfrak{g}_i.$$

If $(\mathfrak{g})_{K[X]}$ is of codimension one, then $(\mathfrak{g}_i)_{K[X]}$ is of codimension one for all $i \geq 1$. But then, according to the proof of the lemma, there exists a semi-invariant $f \in K[X]$ which is not invariant such that $(\mathfrak{g}_i)_{K[X]} \subset (f)_{K[X]}$ for all $i \geq 1$. A semi-invariant $f \notin K[X]^G$ lying over $(\mathfrak{g}_i)_{K[X]}$ for a given $i \geq 0$ can be found algorithmically by computing the primary decomposition of $(\mathfrak{g}_i)_{K[X]}$ and picking from that an ideal which is generated by a semi-invariant (this works at least in the case where $K[X]$ is a polynomial algebra). Otherwise, if there does not exist such an f, it follows by the lemma that $(\mathfrak{g})_{K[X]}$ has codimension greater or equal to two.
With regard to what follows, note that in this case, Algorithm 2.22 of [DK08] can be applied to obtain an affine domain $\widetilde{R}$ and an ideal $\widetilde{\mathfrak{a}} \trianglelefteq \widetilde{R}$ such that $K[X]^G = (\widetilde{R} : \widetilde{\mathfrak{a}}^\infty)_{\mathrm{Quot}(\widetilde{R})}$. ♢

Computation of a normal series $G = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_s$. We can now give a sketch algorithm for the computation of a normal series $G = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_s$ such that there is an algorithm for writing $K[X]^{N_s}$ as the ring of regular functions of some quasi-affine variety and such that for $j = 0, \ldots, s-1$ the quotient group N_j/N_{j+1} is either finite or isomorphic to T. Moreover, this sketch includes the computation of an affine algebra $R \subset K[X]^{N_s}$ and a non-zero ideal $\mathfrak{a} \trianglelefteq R$ such that $K[X]^{N_s} = (R : \mathfrak{a}^\infty)_{\mathrm{Quot}(R)}$.
Note that the following construction uses an algorithm of Kemper. Details about this can be found in [Kem07].

Sketch Algorithm.

(1) Set $j := 0$ and $N_0 := G$.

(2) Repeat:

(3) If N_j is not connected, set $N_{j+1} := (N_j)^0$, $j := j + 1$ and go back to step (2).

(4) Use Theorem 2.2 of [Kem07] to compute generators of the invariant field $K(X)^{N_j}$. Write them as $f_1/g_1, \ldots, f_{s'}/g_{s'}$ where $f_i, g_i \in K[X]$ are coprime for $i = 1, \ldots, s'$.

(5) If there exists a semi-invariant of weight χ among $f_1, \ldots, f_{s'}, g_1, \ldots, g_{s'}$ with $\chi \neq 1_K$, set $N_{j+1} := \chi^{-1}(1)$, $j := j+1$, and go back to step (2).

(6) By step (5), it follows that $\mathrm{Quot}(K[X]^{N_j}) = K(X)^{N_j}$. Use Algorithm 3.20 to compute an affine algebra $R \subset K[X]^{N_j}$ and an element $f \in R \setminus \{0\}$ such that $K[X]^{N_j} = (R : f^\infty)_{K[X]}$ (cf. Remark 3.21(b)).

(7) According to Remark 4.48, try to write $K[X]^{N_j}$ in the form $K[X]^{N_j} = (\widetilde{R} : \widetilde{\mathfrak{a}}^\infty)_{\mathrm{Quot}(\widetilde{R})}$ for some affine algebra $\widetilde{R} \subset K[X]^{N_j}$ and some non-zero ideal $\widetilde{\mathfrak{a}} \trianglelefteq \widetilde{R}$ (cf. [DK08], Algorithm 2.22). If this is not possible, there exists a non-trivial character $\chi \neq 1_K$. In this case, set $N_{j+1} := \chi^{-1}(1)$, $j := j+1$ and go back to step (2).

The idea behind this algorithm is the following. Let the processing of the algorithm enter step (2) for some $j \in \mathbb{N}$. If N_j is not connected, then N_{j+1} is set to the identity component of N_j in step (3). Note that in this case it is clear that N_j/N_{j+1} is a finite group. After that, the processing goes back to step (2).
The aim of steps (4)-(6) is to write $K[X]^{N_j}$ in the form $K[X]^{N_j} = (R : f^\infty)_{K[X]}$ for some affine algebra $R \subset K[X]^{N_j}$ and some element $f \in R \setminus \{0\}$. Algorithmically, this is no problem as long as (cf. Algorithm 3.20 and Remark 3.21(b))

$$K(X)^{N_j} = \mathrm{Quot}(K[X]^{N_j}). \tag{4.30}$$

The only reason why this equation may fail is the existence of a non-trivial character χ (cf. Proposition 3.11). Consequently, in this case N_{j+1} is set to the normal subgroup $N_{j+1} = \chi^{-1}(1)$, which may be thought of as a subgroup of N_j with the character χ being removed. Note that $N_j/N_{j+1} \cong \chi(N_j) < T$. After that, the processing goes back to step (2).
Otherwise, if equation (4.30) is satisfied, the algorithm proceeds with step (7). The aim of this step is to write $K[X]^{N_j}$ as the ring of regular functions of some quasi-affine variety. By Remark 4.48, the only reason why this cannot be done with the existing algorithms, is the existence of a non-trivial character χ. Similarly to the above, N_{j+1} is then set to $\chi^{-1}(1)$ and the processing goes back to step (2).
Note that this algorithm terminates after a finite number of steps since every time when there is a jump back from step (5) or step (7) to step (2), the dimension of the "active group" N_j decreases strictly.

It remains to show that we have $N_j/N_{j+1} \cong T$ in case that a character χ is found in step (5) or step (7). By step (3) of the algorithm, the group N_j is irreducible and therefore $\chi(N_j)$ cannot be a finite group (cf. [Hum75], Section 7.3, Proposition). Since $\dim(T) = 1$ and $\chi(N_j)$ is a closed subgroup of T (cf. [Hum75], Section 7.4, Proposition B), it follows that $\chi(N_j) = T$. Hence N_j/N_{j+1} is isomorphic to T and this isomorphism can be given explicitly by $N_j/N_{j+1} \longrightarrow T$, $\sigma N_{j+1} \longmapsto \chi(\sigma)$. ◁

Computation of $K[X]^G$ along the normal series $G = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_s$. It now remains to compute $K[X]^G$ from $K[X]^{N_s}$ along the chain of groups N_j/N_{j+1}. Let

$j \in \{1, \ldots, s-1\}$ and assume that by induction, we have found an affine algebra $\widetilde{R} \subset K[X]^{N_{j+1}}$ and a non-zero ideal $\widetilde{\mathfrak{a}} \trianglelefteq \widetilde{R}$ such that $K[X]^{N_{j+1}} = (\widetilde{R} : \widetilde{\mathfrak{a}}^{\infty})_{\mathrm{Quot}(\widetilde{R})}$. In case that N_j/N_{j+1} is finite, we can apply Proposition 4.44 and Algorithm 4.34 to compute an affine algebra $R' \subset K[X]^{N_j}$ and a non-zero ideal $\mathfrak{a}' \trianglelefteq R'$ such that $K[X]^{N_j} = (R' : (\mathfrak{a}')^{\infty})_{\mathrm{Quot}(R')}$. Otherwise, N_j/N_{j+1} is isomorphic to T, as we have seen. We do not go into the details here, but since this isomorphism is given explicitly, it is possible to compute a homomorphism $K[X]^{N_{j+1}} \longrightarrow K[T] \otimes_K K[X]^{N_{j+1}}$ which describes the action of the torus $N_j/N_{j+1} \cong T$ on $K[X]^{N_{j+1}}$. Therefore, Proposition 4.44 and Assumption 4.45 can be used to compute an affine algebra $R' \subset K[X]^{N_j}$ and a non-zero ideal $\mathfrak{a}' \trianglelefteq R'$ such that $K[X]^{N_j} = (R' : (\mathfrak{a}')^{\infty})_{\mathrm{Quot}(R')}$.

By induction, this gives an algorithm for the computation of $K[X]^G$. $\triangleleft$

A Code

We have mentioned at various places in this thesis that the computer algebra system MAGMA (cf. [BCP97]) has been used for several computations. As discussed in Subsection 3.2.1, a preliminary implementation of Algorithm 3.20 has been done with this system, too. In the following, we list the code which has been used for the runtime examination of Algorithm 3.20 in Subsection 3.2.1.
Note that this code is not ready for everyday use, e. g. it contains only a minimal amount of code to check for trivial cases and for errors in the input data. Beyond that, there is possibly also plenty of room for optimizations.

```
/*
  FUNCTION SubalgebraCharIdeal
  Input: I: an ideal of a polynomial ring defining an affine algebra A
            via A := Generic(I)/I.
         genSubalgebra: a sequence of elements of Generic(I).
                        Let B be the subalgebra of A generated by the
                        residue classes defined by the elements of
                        genSubalgebra.

  Output: E: an ideal which is used internally to test membership in B.

  SubalgebraCharIdeal computes a 'characteristic' ideal E of the
  subalgebra B which can be used for testing membership in B.
  This function is called by the membership test function
  SubalgebraMembership. If several membership tests for B shall be done,
  SubalgebraCharIdeal should be called explicitly. Then E should be passed
  as a parameter to the function SubalgebraMembership so avoiding a
  repeated computation of E.
*/


SubalgebraCharIdeal := function(I, genSubalgebra)

KX := Generic(I);
K := CoefficientRing(KX);

n := Rank(KX);

vprint User1, 2: "Computation of characteristic ideal started.";
```

```
KXZ := PolynomialRing(K, n+#genSubalgebra, "lex");
emb := hom<KX -> KXZ | [KXZ.i: i in [1..n]]>;

E := ideal<KXZ | [emb(f): f in Basis(I)] cat [KXZ.(n+i)-emb(genSubalgebra[i])
                                                : i in [1..#genSubalgebra]]>;
Groebner(E);

vprint User1, 2: "Computation of characteristic ideal completed.";

return E;

end function;



/*
  FUNCTION SubalgebraMembership
  Input: I: an ideal of a polynomial ring defining an affine algebra A
            via A := Generic(I)/I.
         f: an element of Generic(I).

  Parameters:
         genSubalgebra: a sequence of elements of Generic(I).
                        Let B be the subalgebra of A generated by the
                        residue classes defined by the elements of
                        genSubalgebra.
         E: characteristic ideal of some subalgebra B
            (cf. SubalgebraCharIdeal).

  Output: true, if the element defined by f lies in B
          false, otherwise.

  SubalgebraMembership tests whether the element defined by f is
  contained in the subalgebra B.
  Either genSubalgebra or E must be defined. If E is not defined, it
  will be calculated via an explicit call of SubalgebraCharIdeal.
*/


SubalgebraMembership := function(I, f: genSubalgebra:=0, E:=0)

vprintf User1, 3: "Computation of subalgebra membership started.";

if E cmpeq 0 then
```

```
  if genSubalgebra cmpeq 0 then
    error "SubalgebraMembership: Either 'genSubalgebra' or 'E' must be defined";
  end if;

  E := SubalgebraCharIdeal(I, genSubalgebra);
end if;

KX := Generic(I);
n := Rank(KX);

KXZ := Generic(E);
emb := hom<KX -> KXZ | [KXZ.i: i in [1..n]]>;

phi := hom<KXZ -> KXZ | [0: i in [1..n]] cat
         [KXZ.(n+i): i in [1..(Rank(KXZ)-n)]]>;
g := NormalForm(emb(f), E);

vprintf User1, 3: "Computation of subalgebra membership completed.";
return (g - phi(g)) eq 0;

end function;



/*
  FUNCTION SubalgebraContainment
  Input: I: an ideal of a polynomial ring defining an affine algebra A
            via A := Generic(I)/I.
         genSubalgebra1: a sequence of elements of Generic(I).
                         Let B1 be the subalgebra of A generated by the
                         residue classes defined by the elements of
                         genSubalgebra.
         genSubalgebra2: a sequence of elements of Generic(I).
                         Let B2 be the subalgebra of A generated by the
                         residue classes defined by the elements of
                         genSubalgebra.

  Output: true, if B1 is contained in B2
          false, otherwise.

  SubalgebraContainment tests whether the subalgebra B1 is contained
  in the subalgebra B2.
*/
```

```
SubalgebraContainment := function(I, genSubalgebra1, genSubalgebra2)

E := SubalgebraCharIdeal(I, genSubalgebra2);
return &and[SubalgebraMembership(I, f: E:=E): f in genSubalgebra1];

end function;


/*
  FUNCTION SubalgebraEquality
  Input: I: an ideal of a polynomial ring defining an affine algebra A
            via A := Generic(I)/I.
         genSubalgebra1: a sequence of elements of Generic(I).
                         Let B1 be the subalgebra of A generated by the
                         residue classes defined by the elements of
                         genSubalgebra.
         genSubalgebra2: a sequence of elements of Generic(I).
                         Let B2 be the subalgebra of A generated by the
                         residue classes defined by the elements of
                         genSubalgebra.

  Output: true, if B1 is equal to B2
          false, otherwise.

  SubalgebraEquality tests whether the subalgebra B1 is equal to
  the subalgebra B2.
*/


SubalgebraEquality := function(I, genSubalgebra1, genSubalgebra2)

return SubalgebraContainment(I, genSubalgebra1, genSubalgebra2) and
    SubalgebraContainment(I, genSubalgebra2, genSubalgebra1);

end function;



/*
  FUNCTION SubalgebraSimplifyGenerators
  Input: I: an ideal of a polynomial ring defining an affine algebra A
            via A := Generic(I)/I.
         genSubalgebra: a sequence of elements of Generic(I).
                        Let B be the subalgebra of A generated by the
                        residue classes defined by the elements of
```

```
                        genSubalgebra.

  Parameters:
         fastMode: a flag which controls the simplification process.

  Output: a subsequence of genSubalgebra such that the residue classes
          defined by the elements of this subsequence generate B.


  SubalgebraSimplifyGenerators tries to simplify the set of generators of B.
  If fastMode is set to true, it will just remove elements contained in
  the field of coefficients of Generic(I). If fastMode is set to false,
  it eliminates redundant elements of genSubalgebra, i.e. elements with
  the property that the sequence genSubalgebra with these elements
  removed still defines a generating set of B. This is done heuristically,
  i.e. genSubalgebra may still contain redundant elements.
*/


SubalgebraSimplifyGenerators := function(I, genSubalgebra: fastMode := true)

vprint User1, 1: "Simplifaction of subalgebra generators started.";

KX := Generic(I);

/*
Remove elements contained in the field of coefficients of KX.
*/

genSubalgebra := [f: f in genSubalgebra | f notin CoefficientRing(KX)];

if fastMode then
  vprint User1, 1: "Simplifaction of subalgebra generators completed.";
  return genSubalgebra;
end if;

/*
Sort the elements of genSubalgebra in ascending order according to their
leading monomials.
*/

Sort(~genSubalgebra, func<f1, f2 |
  (LeadingMonomial(f1) ge LeadingMonomial(f2)) select 1 else
    ((LeadingMonomial(f1) eq LeadingMonomial(f2)) select 0 else -1)>);
```

```
newGenSubalgebra := [];
for i in [1..#genSubalgebra] do
  if not(SubalgebraMembership(I, genSubalgebra[i]
          : genSubalgebra:=newGenSubalgebra)) then
    newGenSubalgebra := newGenSubalgebra cat [genSubalgebra[i]];
  end if;
end for;

vprint User1, 1: "Simplifaction of subalgebra generators completed.";

return newGenSubalgebra;

end function;



/*
  FUNCTION LUSubset
  Input: listPoly: a list of polynomials.

  Output: a sequence of polynomials defining a basis of the vector
          space generated by the elements of listPoly.
*/


LUSubset := function(listPoly)

listPoly := [f: f in listPoly | f ne 0];
if #listPoly le 1 then
  return listPoly;
end if;

K := CoefficientRing(Parent(listPoly[1]));

monsListPoly := SetToSequence(&join[{m: m in Monomials(f)}: f in listPoly]);

V := VectorSpace(K, #listPoly);
W := VectorSpace(K, #monsListPoly);

B := Basis(Image(hom<V -> W | [W![MonomialCoefficient(f, t)
        : t in monsListPoly]: f in listPoly]>));

return [&+[b[i]*monsListPoly[i]: i in [1..#monsListPoly]]: b in B];

end function;
```

```
/*
  FUNCTION GXIdeal
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         J: a radical ideal J defining a linear algebraic group G
            (see Convention 3.19).
         action: a list of polynomials defining a regular action of G on X
                 (see Convention 3.19).

  Output: JI: an ideal which is used internally to test (among other
              things) invariance of elements in K[X].

  GXIdeal computes a the vanishing ideal of G x X. This function is
  called by various functions for the computation of invariant rings
  of unipotent groups (see below).
  If several functions needing this ideal shall be computed, GXIdeal
  should be called explicitly. Then E should be passed as a parameter
  to these functions so avoiding a repeated computation of JI.
*/


GXIdeal := function(I, J, action)

KX := Generic(I);
n := Rank(KX);

KT := Generic(J);
m := Rank(KT);

if #action ne n then
 error "Error in input data";
end if;

KTX := Parent(action[1]);
if Rank(KTX) ne (m+n) then
 error "Error in input data";
end if;


K := CoefficientRing(KTX);

embX := hom<KX -> KTX | [KTX.(m+i): i in [1..n]]>;
```

```
embT := hom<KT -> KTX | [KTX.i: i in [1..m]]>;

JI := ideal<KTX | [embT(g): g in Basis(J)] cat [embX(f): f in Basis(I)]>;
Groebner(JI);

return JI;

end function;


/*
  FUNCTION GClosure (see Algorithm 3.25)
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         J: a radical ideal J defining a linear algebraic group G
            (see Convention 3.19).
         action: a list of polynomials defining a regular action of G on X
                 (see Convention 3.19).
         q: an element of Generic(I).

  Parameters:
         JI:  vanishing ideal of G x X.

  Output: a list b1, ... bs of polynomials such that b1 + I, ... bs + I
          is a basis of a G-module containing q + I.

  If JI is not defined it will be calculated by an explicit call of
  GXIdeal.
*/


GClosure := function(I, J, action, q: JI := 0)

KX := Generic(I);
n := Rank(KX);

if n eq 0 then
  return CoefficientRing(KX);
end if;

m := Rank(Generic(J));

if #action ne n then
 error "Error in input data";
end if;
```

```
if JI cmpeq 0 then
  JI := GXIdeal(I, J, action);
end if;

KTX := Generic(JI);

phi := hom<KX -> KTX | [action[i]: i in [1..n]]>;

KX_T := PolynomialRing(KX, m);
psi := hom<KTX -> KX_T | [KX_T.i : i in [1..m]] cat
            [KX_T!KX.i: i in [1..n]]>;

CoeffList := Coefficients(psi(NormalForm(phi(q), JI)));

return LUSubset(CoeffList);

end function;


/*
  FUNCTION NonzeroInvariant (see Algorithm 3.24)
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         J: a radical ideal J defining a linear algebraic group G
            (see Convention 3.19).
         action: a list of polynomials defining a regular action of G on X
                 (see Convention 3.19).
         f: an element of Generic(I).

  Parameters:
         JI: vanishing ideal of G x X.

  Output: a polynomial h such that h + I is a non-zero invariant and
          h + I is contained in the G-closure of f + I.
*/



NonZeroInvariant := function(I, J, action, f: JI := 0)

KX := Generic(I);
n := Rank(KX);
m := Rank(Generic(J));
```

```
if #action ne n then
 error "Error in input data";
end if;

if JI cmpeq 0 then
  JI := GXIdeal(I, J, action);
end if;

KTX := Generic(JI);
K := CoefficientRing(KTX);

embX := hom<KX -> KTX | [KTX.(m+i): i in [1..n]]>;
phi := hom<KX -> KTX | [action[i]: i in [1..n]]>;

// Check if f + I is already invariant

if NormalForm(phi(f)-embX(f), JI) eq 0 then
  return f;
end if;

genV := GClosure(I, J, action, f: JI := JI);

redDiff := [NormalForm(phi(h)-embX(h), JI): h in genV];
monRedDiff := SetToSequence(&join[{mon: mon in Monomials(g)}
                                    : g in redDiff]);

V := VectorSpace(K, #redDiff);
W := VectorSpace(K, #monRedDiff);

B:=Basis(Kernel(hom<V -> W | [W![MonomialCoefficient(g, mon)
                  : mon in monRedDiff]: g in redDiff]>));
return &+[B[1][i]*genV[i]: i in [1..#redDiff]];

end function;



/*
  FUNCTION UnipotentLocalizedInvariantRing (see Algorithm 3.20)
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         J: a radical ideal J defining a linear algebraic group G
            (see Convention 3.19).
         action: a list of polynomials defining a regular action of G on X
```

```
                (see Convention 3.19).

  Output: curGen: a sequence of elements of Generic(I) and
          f: an element of Generic(I)
          such that the invariant ring localized at the element
          f + I is generated (as a K-algebra) by 1/(f + I) and the
          residue classes of the elements in curGen.
*/


UnipotentLocalizedInvariantRing := function(I, J, action)

vprint User1, 1: "Computation of localized invariant ring started.";

KX := Generic(I);
n := Rank(KX);

if n eq 0 then
  return CoefficientRing(KX);
end if;

KT := Generic(J);
m := Rank(KT);

if #action ne n then
 error "Error in input data";
end if;


KTX := Parent(action[1]);
if Rank(KTX) ne (m+n) then
 error "Error in input data";
end if;

if IsZero(I) then
  Kfx := FieldOfFractions(KX);
else
  Kfx := FieldOfFractions(KX/I);
end if;

KfxTZ := PolynomialRing(Kfx, m+n);

JI := GXIdeal(I, J, action);

phi := hom<KT -> KfxTZ | [KfxTZ.i: i in [1..m]]>;
```

```
alpha := hom<KTX -> KfxTZ | [KfxTZ.i: i in [1..m]] cat
          [KfxTZ!Kfx.i: i in [1..n]]>;

D0 := ideal<KfxTZ | [phi(p): p in Basis(J)] cat
         [KfxTZ.(m+i)-alpha(action[i]): i in [1..n]]>;
D := EliminationIdeal(D0, {KfxTZ.(m+i): i in [1..n]});

CoeffList := &cat[Coefficients(f): f in Basis(D)];
CoeffListNumDenom := [[KX!Numerator(f), KX!Denominator(f)]
                        : f in CoeffList];

if #CoeffListNumDenom eq 0 then
  f := 1;
else
  CoeffListDenomInv := [NonZeroInvariant(I, J, action, nd[2]: JI := JI)
                          : nd in CoeffListNumDenom];
  f := LCM(CoeffListDenomInv);
end if;

curGen := [CoeffListDenomInv[i] eq CoeffListNumDenom[i][2] select
   KX!(CoeffListNumDenom[i][1]*f/CoeffListNumDenom[i][2]) else
     Coordinates(IdealWithFixedBasis([CoeffListNumDenom[i][2]] cat Basis(I)),
       f * CoeffListNumDenom[i][1])[1]
   : i in [1..#CoeffListNumDenom]];

vprint User1, 1: "Computation of localized invariant ring completed.";
return curGen, f;

end function;


/*
  FUNCTION ColonAlgebra (see Remark 3.21(b) and Algorithm 2.7 of [DK08])
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         curGen: a sequence of elements of Generic(I).
                 Let B be the subalgebra of A generated by the
                 residue classes defined by the elements of
                 curGen.

         f: an element contained in Generic(I).

  Output: a sequence of elements of Generic(I) such that their
          residue classes generate the K-algebra which is generated
          by the elements of (the B-module) (B : (f+I))_{K[X]}.
```

```
*/


ColonAlgebra := function(I, curGen, f)

vprint User1, 1: "Computation of saturation started.";

KX := Generic(I);
n := Rank(KX);
K := CoefficientRing(KX);

KXT := PolynomialRing(K, n+#curGen);
emb := hom<KX -> KXT | [KXT.i: i in [1..n]]>;


B := Basis(EliminationIdeal(ideal<KXT | [emb(g): g in Basis(I)] cat
       [emb(f)] cat [KXT.(n+i)-emb(curGen[i]): i in [1..#curGen]]>,
       {KXT.(n+i): i in [1..#curGen]}));

phi := hom<KXT -> KX | [0: i in [1..n]] cat [curGen[i]: i in [1..#curGen]]>;

L := IdealWithFixedBasis([f] cat Basis(I));
newGen := curGen cat [Coordinates(L, phi(b))[1]: b in B];

E := SubalgebraCharIdeal(I, curGen);
newGen := [g: g in newGen | not(SubalgebraMembership(I, g: E := E))];

vprint User1, 1: "Computation of saturation completed.";

return curGen cat newGen, newGen eq [];

end function;



/*
  FUNCTION UnipotentInvariantRing (see Algorithm 3.20 and Remark 3.21(b))
  Input: I: a prime ideal defining an affine variety X
            (see Convention 3.19).
         J: a radical ideal J defining a linear algebraic group G
            (see Convention 3.19).
         action: a list of polynomials defining a regular action of G on X
                 (see Convention 3.19).

  Output: a sequence of elements in Generic(I) such that their residue
```

```
          classes generate the invariant ring K[X]^G (as a K-algebra).

  THIS FUNCTION MAY NOT TERMINATE.
*/


UnipotentInvariantRing := function(I, J, action)

curGen, f := UnipotentLocalizedInvariantRing(I, J, action);

saturated := false;
i := 0;

while not(saturated) do
  i := i + 1;
  vprint User1, 1: "Loop: ", i;

  curGen, saturated := ColonAlgebra(I, curGen, f);
  print curGen;

end while;

vprint User1, 1: "Needed ", i, " iterations.";

return SubalgebraSimplifyGenerators(I, curGen: fastMode := false);

end function;


// Code for the example series in Subsection 3.2.1


SetVerbose("User1", true);

for n in [1..7] do

  ijtoIndex := function(i,j)
    return (i-1)*n+j;
  end function;


  KX := PolynomialRing(Rationals(), n*n);
  AssignNames(~KX, &cat[["x"*IntegerToString(i)*IntegerToString(j)
                         : j in [1..n]]: i in [1..n]]);
  I := ideal<KX | 0>;
```

```
  KT := PolynomialRing(Rationals(), n*n);
  AssignNames(~KT, &cat[["t"*IntegerToString(i)*IntegerToString(j)
                          : j in [1..n]]: i in [1..n]]);
  J := ideal<KT | [KT.(ijtoIndex(i,i))-1: i in [1..n]] cat
           &cat[[KT.(ijtoIndex(i,j)): j in [1..i-1]]: i in [1..n]]>;

  KTX := PolynomialRing(Rationals(), Rank(KT) + Rank(KX));
  AssignNames(~KTX, &cat[["t"*IntegerToString(i)*IntegerToString(j)
                          : j in [1..n]]: i in [1..n]]
                    cat
                    &cat[["x"*IntegerToString(i)*IntegerToString(j)
                          : j in [1..n]]: i in [1..n]]);

  action := &cat[[&+[KTX.(ijtoIndex(i,k))*KTX.(n*n + (ijtoIndex(k,j)))
                       : k in [1..n]]: j in [1..n]]: i in [1..n]];

  time UnipotentLocalizedInvariantRing(I, J, action);

end for;
```

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Buc65] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *Dissertation*, 1965.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[Der99] Harm Derksen. Computation of invariants for reductive groups. *Adv. Math.*, 141(2):366–384, 1999.

[DF99] Daniel Daigle and Gene Freudenburg. A counterexample to Hilbert's fourteenth problem in dimension 5. *J. Algebra*, 221(2):528–535, 1999.

[dJ98] Theo de Jong. An algorithm for computing the integral closure. *J. Symbolic Comput.*, 26(3):273–277, 1998.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[DK08] Harm Derksen and Gregor Kemper. Computing invariants of algebraic groups in arbitrary characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[FM76] Amassa Fauntleroy and Andy R. Magid. Proper G_a-actions. *Duke Math. J.*, 43(4):723–729, 1976.

[FM78] Amassa Fauntleroy and Andy R. Magid. Quasi-affine surfaces with G_a-actions. *Proc. Amer. Math. Soc.*, 68(3):265–270, 1978.

[Hab75] William J. Haboush. Reductive groups are geometrically reductive. *Ann. of Math. (2)*, 102(1):67–83, 1975.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HE71] Melvin Hochster and John A. Eagon. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.*, 93:1020–1058, 1971.

[Hil90] David Hilbert. Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890.

[Hil93] David Hilbert. Ueber die vollen Invariantensysteme. *Math. Ann.*, 42(3):313–373, 1893.

[HR74] Melvin Hochster and Joel L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974.

[Hum75] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[Kem94] Gregor Kemper. Das Noethersche Problem und generische Polynome. *Dissertation*, 1994.

[Kem96] Gregor Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Comput.*, 21(3):351–366, 1996.

[Kem99] Gregor Kemper. An algorithm to calculate optimal homogeneous systems of parameters. *J. Symbolic Comput.*, 27(2):171–184, 1999.

[Kem03] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):159–176, 2003.

[Kem07] Gregor Kemper. The computation of invariant fields and a constructive version of a theorem by Rosenlicht. *Transform. Groups*, 12(4):657–670, 2007.

[Kra84] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[KS99] Gregor Kemper and Allan Steel. Some algorithms in invariant theory of finite groups. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 267–285. Birkhäuser, Basel, 1999.

[Mag79] Andy R. Magid. Separated G_a-actions. *Proc. Amer. Math. Soc.*, 76(1):35–38, 1979.

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[MQB99] Jörn Müller-Quade and Thomas Beth. Calculating generators for invariant fields of linear algebraic groups. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 392–403. Springer, Berlin, 1999.

[Nag59] Masayoshi Nagata. On the 14-th problem of Hilbert. *Amer. J. Math.*, 81:766–772, 1959.

[Nag64] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/1964.

[Nag65] Masayoshi Nagata. *Lectures on the fourteenth problem of Hilbert*. Tata Institute of Fundamental Research, Bombay, 1965.

[New78] Peter E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.

[NM64] Masayoshi Nagata and Takehiko Miyata. Note on semi-reductive groups. *J. Math. Kyoto Univ.*, 3:379–382, 1963/1964.

[Pop79] Vladimir L. Popov. On Hilbert's theorem on invariants. *Dokl. Akad. Nauk SSSR*, 249(3):551–555, 1979.

[Ros56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.

[Ros57] Maxwell Rosenlicht. Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl. (4)*, 43:25–50, 1957.

[Stu93] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.

[vdE93] Arno van den Essen. An algorithm to compute the invariant ring of a $\mathbf{G}_a$-action on an affine variety. *J. Symbolic Comput.*, 16(6):551–555, 1993.

[Win03] Jörg Winkelmann. Invariant rings and quasiaffine quotients. *Math. Z.*, 244(1):163–174, 2003.

Index

Notation

$\emptyset$	the empty set
$\mathbb{N}, \mathbb{N}_0$	the set of natural numbers (excluding resp. including 0)
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{F}_p$	the Galois field with p elements, where p is some prime number
$\lvert M \rvert$	the cardinality of the set M
$\ker \alpha$	the kernel of the linear map α
$R^\times$	the group of units of the ring R
$\mathrm{Quot}(R)$	the field of fractions of the ring R
$(f_1, \ldots, f_m)_R$	the ideal of the ring R generated by $f_1, \ldots, f_m \in R$
$K[f_1, \ldots, f_m]$	the algebra generated by $f_1, \ldots, f_m$ over the field K
$\langle \sigma_1, \ldots, \sigma_m \rangle$	the group generated by $\sigma_1, \ldots, \sigma_m$
$\mathrm{GL}_n(K)$	the general linear group over the field K of degree n, i. e. the set of invertible $n \times n$ matrices with entries in K together with the usual matrix multiplication
$\mathrm{SL}_n(K)$	the special linear group over K of degree n, i. e. the subgroup of $\mathrm{GL}_n(K)$ consisting of matrices with determinant 1