Available online at www.sciencedirect.com
ScienceDirect
Advances in Mathematics 217 (2008) 2089–2129
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

Computing invariants of algebraic groups in arbitrary characteristic

Harm Derksen [a,*,1], Gregor Kemper [b]

[a] *Department of Mathematics, University of Michigan, USA*
[b] *Technische Universität München, Zentrum Mathematik – M11, Germany*

Received 19 April 2007; accepted 30 August 2007

Available online 13 November 2007

Communicated by David J. Benson

Abstract

Let G be an affine algebraic group acting on an affine variety X. We present an algorithm for computing generators of the invariant ring $K[X]^G$ in the case where G is reductive. Furthermore, we address the case where G is connected and unipotent, so the invariant ring need not be finitely generated. For this case, we develop an algorithm which computes $K[X]^G$ in terms of a so-called colon-operation. From this, generators of $K[X]^G$ can be obtained in finite time if it is finitely generated. Under the additional hypothesis that $K[X]$ is factorial, we present an algorithm that finds a quasi-affine variety whose coordinate ring is $K[X]^G$. Along the way, we develop some techniques for dealing with nonfinitely generated algebras. In particular, we introduce the finite generation ideal.

Keywords: Invariant theory; Algorithm; Reductive group; Unipotent group; Algebraic group

Contents

* Corresponding author.
E-mail addresses: hderksen@umich.edu (H. Derksen), kemper@ma.tum.de (G. Kemper).
[1] The research of the first author was supported by NSF grant DMS 0349019.

0001-8708/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.aim.2007.08.016

0. Introduction

Throughout this article, G will be an affine algebraic group over an algebraically closed field K. By a G-variety we understand an affine variety X over K with a G-action given by a morphism $G \times X \to X$. The ring of regular functions on X is denoted by $K[X]$. G acts on $K[X]$ by

$$\sigma(f) = f \circ \sigma^{-1}$$

for $\sigma \in G$ and $f \in K[X]$. The invariant ring is

$$K[X]^G := \left\{ f \in K[X] \,\middle|\, \sigma(f) = f \text{ for all } \sigma \in G \right\}.$$

An algebraic group G is called *geometrically reductive* if for every representation V and every $v \in V^G \setminus \{0\}$ there exists a homogeneous, nonconstant G-invariant polynomial $f \in K[V]^G$ such that $f(v) \neq 0$. Nagata [21] showed that $K[X]^G$ is finitely generated as a K-algebra if G is *geometrically* reductive and X is an affine G-variety. An algebraic group is called *reductive* if every connected unipotent normal subgroup of G is trivial. Haboush [8] proved that reductive groups are geometrically reductive. The converse is also true: geometrically reductive groups are reductive. Popov [23] showed that if G is not reductive, then there exists a G-variety X such that $K[X]^G$ is not finitely generated. Moreover, Nagata [22] showed that if X is normal, then $K[X]^G$ is always isomorphic to the coordinate ring $K[U]$ of a quasi-affine variety U over K, even if $K[X]^G$ is not finitely generated. Several problems arise from these facts:

(1) Find an algorithm that constructs generators of $K[X]^G$ for G reductive.
(2) Find an algorithm that decides whether $K[X]^G$ is finitely generated for G nonreductive.
(3) Find an algorithm that constructs generators of $K[X]^G$ if it is finitely generated.
(4) Find an algorithm that constructs a quasi-affine variety U with $K[X]^G \cong K[U]$ (in the case that X is normal).

In the case that K has characteristic 0, a solution for the first problem was given by the first author [2]. (More precisely, the article [2] deals with the case that G is linearly reductive.) The second author gave a solution of the first problem in the case that $X = \mathbb{A}^n(K)$ is affine n-space and the action of G is linear [15]. The third problem was solved by van den Essen [5]

for $G = \mathbb{G}_a$ being the additive group and K being of characteristic 0 (see Section 3.1.1 of this paper). Van den Essen's algorithm terminates after finitely many steps if and only if $K[X]^{\mathbb{G}_a}$ is finitely generated.

In the first and last section of this paper, we do the following:

- We give a complete solution to the first problem (Algorithm 1.7). An optimized algorithm is given for the case that X is normal and G is connected (Algorithm 1.10).
- We give a new algorithm for computing $K[X]^G$ in the case that $G = \mathbb{G}_a$ is the additive group and X is irreducible (see Section 3.1.2). This algorithm works in arbitrary characteristic. As van den Essen's algorithm, our algorithm first finds an $f \in K[X]^{\mathbb{G}_a} \setminus \{0\}$ and finitely many generators of the localization $K[X]_f^{\mathbb{G}_a}$. This is used for computing generators of $K[X]^{\mathbb{G}_a}$ in a second step. If the invariant ring is not finitely generated, this second step continues to produce generating invariants forever.
- We extend the algorithm for additive group invariants to the case where G is connected and unipotent, and X is irreducible (Algorithm 3.8). The algorithm has the same nature as the one for the additive group. Thus we get a solution of the third problem for this case.
- We find an algorithm for constructing a quasi-affine variety U with $K[X]^G \cong K[U]$ in the case that G is connected and unipotent, and $K[X]$ is factorial (Algorithm 3.9). The isomorphism is given explicitly. This algorithm always terminates after finitely many steps. Thus we solve the fourth problem for this case.
- We develop some ideas how the third problem can be attacked in general (Section 3.3).

We leave it to others to make any progress on the second problem. The middle section of this paper deals with nonfinitely generated algebras. In the context of this paper, this prepares the ground for the last section, but we believe that the following results from the middle section are of more general interest:

- We introduce "colon-operations" $(R : \mathfrak{a})_S$ and $(R : \mathfrak{a}^\infty)_S$ and give algorithms for computing them in the case that $R \subseteq S$ are finitely generated algebras over a field and $\mathfrak{a}$ is an ideal of R (see Section 2.1). The coordinate ring of an irreducible, quasi-affine variety appears as a special case (see Lemma 2.3).
- We prove that for a subalgebra R of a finitely generated domain over a field, there always exists $f \in R \setminus \{0\}$ such that R_f is finitely generated (Proposition 2.7). We also prove that the set of all these f's, together with 0, forms an ideal, the *finite generation ideal*.
- We give a constructive version of Grothendieck's generic freeness lemma (see Theorem 2.13 and Algorithm 2.14).
- We give an algorithm for computing the intersection of a finitely generated domain over a field and the field of fractions of a subalgebra (Algorithm 2.16). This algorithm addresses the original version of Hilbert's fourteenth problem. Our algorithm terminates after finitely many steps if and only if the intersection is finitely generated.

1. Invariants of reductive groups

In this section we give algorithms for computing invariant rings of reductive groups acting on affine varieties. The assumption on reductivity of G is not needed in Section 1.1.

1.1. Embedding into a linear space

If $X = \mathbb{A}^n(K)$ is affine n-space and the action is linear, we say that X is a G-module. We usually use letters like V or W for G-modules. A G-module is given by a morphism $G \to \mathrm{GL}_n(K)$ of algebraic groups.

Our first goal is to embed an arbitrary G-variety X equivariantly into a G-module V. The idea for this is simple and standard. Since the G-action on $K[X]$ is locally finite, there exists a finite-dimensional G-stable vector space $W \subseteq K[X]$ which generates $K[X]$ as a K-algebra. So we obtain a G-equivariant epimorphism from the symmetric algebra $S(W)$ onto $K[X]$. Since $S(W) = K[W^*]$, $V = W^*$ (the dual of W) is the desired G-module. However, for turning this rough idea into an algorithm, we have to work out quite a few details.

Before we can even start to formulate algorithms, we need to specify the form of the input data.

Convention 1.1. We assume that G and X are given by the following data:

(a) generators of a radical ideal $J \subset K[t_1, \ldots, t_m]$ in a polynomial ring such that J defines G as an affine variety in K^m;
(b) generators of a radical ideal $I \subseteq K[x_1, \ldots, x_n]$ in another polynomial ring such that I defines X as an affine variety in K^n;
(c) polynomials $g_1, \ldots, g_n \in K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ such that for a point $(\xi_1, \ldots, \xi_n) \in X$ and a group element $\sigma = (\gamma_1, \ldots, \gamma_m) \in G$ we have

$$\sigma(\xi_1, \ldots, \xi_n) = \big(g_1(\underline{\gamma}, \underline{\xi}), \ldots, g_n(\underline{\gamma}, \underline{\xi})\big),$$

where we write $(\underline{\gamma})$ for $(\gamma_1, \ldots, \gamma_m)$, etc.

We are now ready to formulate our first algorithm.

Algorithm 1.2 *(Embedding X into a G-module V).*

Input: An affine algebraic group G and a G-variety X given according to Convention 1.1.
Output: Polynomials $a_{i,j} \in K[t_1, \ldots, t_n]$ $(i, j \in \{1, \ldots, r\})$ such that

$$G \to \mathrm{GL}_r(K), \qquad (\gamma_1, \ldots, \gamma_m) \mapsto \begin{pmatrix} a_{1,1}(\underline{\gamma}) & \cdots & a_{1,r}(\underline{\gamma}) \\ \vdots & & \vdots \\ a_{r,1}(\underline{\gamma}) & \cdots & a_{r,r}(\underline{\gamma}) \end{pmatrix}$$

defines a G-module $V = K^r$, and a G-equivariant epimorphism $K[V] \to K[X]$. (In particular, the induced morphism $X \to V$ is a G-equivariant closed immersion.)

(1) Compute Gröbner bases $\mathcal{G}_I$ and $\mathcal{G}_J$ of I and J with respect to arbitrary monomial orderings on $K[x_1, \ldots, x_n]$ and $K[t_1, \ldots, t_m]$.
(2) Substitute each g_i by its normal form $\mathrm{NF}_{\mathcal{G}_I \cup \mathcal{G}_J}(g_i)$. (This means that whenever a monomial of g_i is divisible by a leading monomial of an element of $\mathcal{G}_I$ or $\mathcal{G}_J$, the corresponding reduction should be performed.)

(3) Let $C \subseteq K[x_1, \ldots, x_n]$ be the set of all coefficients occurring in the g_i considered as polynomials in $t_1, \ldots, t_m$.
(4) Select a maximal K-linearly independent subset $\{h_1, \ldots, h_r\} \subseteq C$.
(5) For $i = 1, \ldots, r$, form

$$\widetilde{h_i} := \mathrm{NF}_{\mathcal{G}_I \cup \mathcal{G}_J}\big(h_i(g_1, \ldots, g_n)\big) \in K[t_1, \ldots, t_m, x_1, \ldots, x_n].$$

(6) For $i = 1, \ldots, r$, find $a_{i,1}, \ldots, a_{i,r} \in K[t_1, \ldots, t_m]$ such that

$$\widetilde{h_i} = \sum_{j=1}^{r} a_{i,j} h_j. \tag{1.1}$$

This can be done by viewing (1.1) as an equation in $K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$, comparing coefficients in the x-variables, and solving the resulting linear system with coefficients in $K(t_1, \ldots, t_m)$. In fact, there exists a unique solution, which lies in $K[t_1, \ldots, t_m]^r$.
(7) The $a_{i,j}$ give $V := K^r$ the structure of a G-module, and with $K[V] = K[y_1, \ldots, y_r]$, the map $\Phi : K[V] \to K[X]$ is defined by $y_i \mapsto h_i + I$.

Proof of correctness of Algorithm 1.2. We first remark that converting the g_i into normal form (Step 2) does not change their properties given in Convention 1.1(c). We will assume that g_i are in normal form. For $(\xi_1, \ldots, \xi_n) \in X$ and $\sigma \in G$ we have

$$\big(\sigma^{-1}(x_i + I)\big)(\xi_1, \ldots, \xi_n) = (x_i + I)\big(\sigma(\xi_1, \ldots, \xi_n)\big) = g_i(\sigma, \underline{\xi}),$$

so

$$\sigma^{-1}(x_i + I) = g_i(\sigma, \underline{x}) + I. \tag{1.2}$$

We can write

$$g_i = \sum_{j=1}^{l} h_{i,j} f_j$$

with $f_1, \ldots, f_l \in K[t_1, \ldots, t_m]$ pairwise distinct monomials in normal form with respect to $\mathcal{G}_J$, and $h_{i,j} \in K[x_1, \ldots, x_n]$ in normal form with respect to $\mathcal{G}_I$. With this, (1.2) becomes

$$\sigma^{-1}(x_i + I) = \sum_{j=1}^{l} f_j(\sigma)(h_{i,j} + I). \tag{1.3}$$

Let

$$W := \sum_{i=1}^{n} \sum_{j=1}^{l} K \cdot (h_{i,j} + I)$$

be the subspace of $K[X]$ generated by the residue classes of all $h_{i,j}$. With the h_i selected as in Step 4, a K-basis of W is given by $h_1 + I, \ldots, h_r + I$. We claim that

$$W = \langle x_1, \ldots, x_n \rangle_{KG} \tag{1.4}$$

(the module over the group ring generated by the x_i). The inclusion "$\supseteq$" follows directly from (1.3). The f_j are linearly independent as functions on G. So there exist $\sigma_1, \ldots, \sigma_l \in G$ such that the matrix $(f_j(\sigma_i))_{i,j}$ is invertible. From (1.3) we conclude that $h_{i,j} + I \in \langle \sigma_1^{-1}(x_i + I), \ldots, \sigma_l^{-1}(x_i + I) \rangle_K$, so $W \subseteq \langle x_1, \ldots, x_n \rangle_{KG}$. This completes the proof of (1.4).

To see that the $a_{i,j}$ from Step 6 exist, choose a set $B \subseteq K[x_1, \ldots, x_n]$ such that the $h + I$ with $h \in B$ together with all $h_i + I$ form a K-basis of $K[X]$. Then for $i \in \{1, \ldots, n\}$ we can write

$$\widetilde{h_i} + I = \sum_{j=1}^{r} a_{i,j} h_j + \sum_{j=1}^{s} a'_{i,j} h'_j + I$$

with $h'_j \in B$ and $a_{i,j}, a'_{i,j} \in K[t_1, \ldots, t_m]$. As $\widetilde{h_i}$ is in reduced form with respect to $\mathcal{G}_J$, the same holds for all $a_{i,j}$ and $a'_{i,j}$. The definition of $\widetilde{h_i}$, Eq. (1.2) and the G-stability of W imply

$$\widetilde{h_i}(\sigma, x_1, \ldots, x_n) + I = \sigma^{-1}(h_i + I) \in W,$$

so

$$\sum_{j=1}^{r} a_{i,j}(\sigma) h_j + \sum_{j=1}^{s} a'_{i,j}(\sigma) h'_j + I \in W$$

for all $\sigma \in G$. Since W is generated by the $h_j + I$, it follows that all $a'_{i,j}(\sigma)$ are zero, so $a'_{i,j} \in J$. Since they are in normal form, $a'_{i,j} = 0$ for all j, so $\widetilde{h_i} + I = \sum_{j=1}^{r} a_{i,j} h_j + I$. Since all polynomials in this equation are in reduced form with respect to $\mathcal{G}_I$, it follows that this is an equality in $K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. So the $a_{i,j}$ from Step 6 indeed exist. Their uniqueness follows from the fact that $h_1, \ldots, h_r$ are linearly independent over K, thus also over the rational function field $K(t_1, \ldots, t_m)$. We obtain

$$\sigma^{-1}(h_i + I) = \sum_{j=1}^{r} a_{i,j}(\sigma)(h_j + I).$$

It follows that the matrix $(a_{i,j})$ makes $V = K^r$ into a G-module, and we obtain $K[V] = K[y_1, \ldots, y_n]$ with the action given by

$$\sigma^{-1}(y_i) := \sum_{j=1}^{r} a_{i,j}(\sigma) y_j.$$

So the map Φ is G-equivariant. Since $x_i + I \in W = \langle h_1 + I, \ldots, h_r + I \rangle_K$, Φ is also surjective. □

1.2. Inseparable closure

For R an algebra over a field K of characteristic $p > 0$ and $A \subseteq R$ a subalgebra, we write

$$\sqrt[p]{A} := \{g \in R \mid g^p \in A\}$$

and call this the pth root of A in R. Moreover,

$$\widehat{A} := \{g \in R \mid g^q \in A \text{ for some } p\text{-power } q\}$$

is called the *inseparable closure* of A in R. $\sqrt[p]{A}$ and $\widehat{A}$ are clearly A-modules and K-algebras. The following remark sheds some light on the importance of the inseparable closure to invariant theory.

Remark 1.3. Suppose that G is a reductive group over an algebraically closed field K of positive characteristic, and V is a G-module. Let $A \subseteq K[V]^G$ be a *separating* subalgebra. By definition, this means that A has the same capabilities of separating G-orbits as $K[V]^G$ (see Derksen and Kemper [3, Definition 2.3.8]). Since the natural map $V \to \operatorname{Spec}_{\max}(K[V]^G)$ is surjective, this implies that the map $\operatorname{Spec}_{\max}(K[V]^G) \to \operatorname{Spec}_{\max}(A)$ is injective. Assume further that A is generated by homogeneous invariants. Then Theorem 2.3.12 of [3] implies that $K[V]^G$ is integral over A. By van der Kallen [12, Sublemma A.5.1] (for an expanded version of the proof see http://www.math.uu.nl/people/vdkallen/errbmod.pdf), the integrality and the injectiveness of the corresponding morphism imply that $K[V]^G \subseteq \widehat{A}$. Here the inseparable closure can and will be understood to be formed in $K[V]$. Since $\widehat{K[V]^G} = K[V]^G$ is always true, we conclude

$$\widehat{A} = K[V]^G. \tag{1.5}$$

(In fact, the converse is also true: If a subalgebra $A \subseteq K[V]^G$ satisfies (1.5), then it is separating.) The conclusion (1.5) is an improvement of [3, Theorem 2.3.12], which says that $K[V]^G$ is obtained from A by first taking the normalization and then the inseparable closure. This improvement only holds in positive characteristic. Using (1.5), we also get an improvement to the algorithm given by Kemper [15] for computing $K[V]^G$. In fact, Algorithm 1.9 of [15] first calculates the normalization (Step 2) and then the inseparable closure (Step 3). Thus in positive characteristic, Step 2 can in fact be omitted.

In Kemper [15, Algorithm 4.2] an algorithm is given for computing $\sqrt[p]{A}$ in the case that R is a polynomial ring. We need to modify this algorithm substantially to make it suitable for the case that R is any reduced finitely generated K-algebra.

Algorithm 1.4 *(pth root of a subalgebra).*

Input: Polynomials $h_1, \ldots, h_l \in K[x_1, \ldots, x_n]$ over a perfect field K of characteristic $p > 0$ such that $I = (h_1, \ldots, h_l)$ is a radical ideal, and polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ defining a subalgebra $A := K[f_1 + I, \ldots, f_m + I] \subseteq R := K[x_1, \ldots, x_n]/I$.

Output: Polynomials $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ such that

$$\sqrt[p]{A} = \sum_{i=1}^{r} A \cdot (g_i + I).$$

(1) Let F be a free $K[x_1, \ldots, x_n]$-module of rank $(p^m + lp^n + 1)$ with basis vectors $e_{i_1,\ldots,i_m}$ $(i_\nu \in \{0, \ldots, p-1\})$, $e^{(j)}_{i_1,\ldots,i_n}$ $(j \in \{1, \ldots, l\}, i_\nu \in \{0, \ldots, p-1\})$, and $e^{(0)}$.
(2) Form the $K[x_1, \ldots, x_n]$-module $M \subseteq F$ formed by all

$$e_{i_1,\ldots,i_m} + \prod_{\nu=1}^{m} f_\nu^{i_\nu} e^{(0)} \quad \big(i_\nu \in \{0, \ldots, p-1\}\big)$$

and

$$e^{(j)}_{i_1,\ldots,i_n} + \prod_{\nu=1}^{n} x_\nu^{i_\nu} h_j e^{(0)} \quad \big(j \in \{1, \ldots, l\},\ i_\nu \in \{0, \ldots, p-1\}\big).$$

(3) Let $K[y_1, \ldots, y_n]$ be a new polynomial ring and write φ for the map $K[y_1, \ldots, y_n] \to K[x_1, \ldots, x_n]$ sending each y_i to x_i^p. Also use the letter φ for the component-wise application of φ to the free module $K[y_1, \ldots, y_n]^{p^m+lp^m+1}$.
(4) Use Algorithm 1.5 below to compute $C_1, \ldots, C_s \in K[y_1, \ldots, y_n]^{p^m+lp^m+1}$ such that the $\varphi(C_i)$ generate

$$M \cap K\big[x_1^p, \ldots, x_n^p\big]^{p^m+lp^m+1}$$

as a $K[x_1^p, \ldots, x_n^p]$-module.
(5) With $\pi : K[y_1, \ldots, y_n]^{p^m+lp^m+1} \to K[y_1, \ldots, y_n]^{p^m}$ the projection on the first p^m coordinates, form

$$\widetilde{M} := \sum_{i=1}^{s} K[y_1, \ldots, y_n] \cdot \pi(C_i) \subseteq K[y_1, \ldots, y_n]^{p^m}.$$

Moreover, form $\widetilde{f}_1, \ldots, \widetilde{f}_m \in K[y_1, \ldots, y_n]$ from the f_i by raising each coefficient of f_i to its pth power and substituting each x_j by y_j.
(6) Use Algorithm 1.5 to compute generators $s_1, \ldots, s_r$ of $\widetilde{M} \cap K[\widetilde{f}_1, \ldots, \widetilde{f}_m]^{p^m}$ as a module over $K[\widetilde{f}_1, \ldots, \widetilde{f}_m]$ and a matrix $(a_{i,j}) \in K[y_1, \ldots, y_n]^{r \times s}$ such that

$$s_i = \sum_{j=1}^{s} a_{i,j} \pi(C_j).$$

(7) For $i = 1, \ldots, r$, let $g_i \in K[x_1, \ldots, x_n]$ be the (unique) pth root of

$$\sum_{j=1}^{s} \varphi(a_{i,j}) \cdot \varphi\big(C_j^{(0)}\big) \in K\big[x_1^p, \ldots, x_n^p\big],$$

where $C_j^{(0)}$ is the $e^{(0)}$-component of C_j.

Proof of correctness of Algorithm 1.4. Throughout the proof we write $\overline{g} := g + I \in R$ for the residue class of a polynomial $g \in K[x_1, \ldots, x_n]$. Take an element

$$(\underline{u}) = \sum_{i_1,\ldots,i_m=0}^{p-1} u_{i_1,\ldots,i_m} e_{i_1,\ldots,i_m} + \sum_{j=1}^{l} \sum_{i_1,\ldots,i_n=1}^{p-1} u^{(l)}_{i_1,\ldots,i_n} e^{(l)}_{i_1,\ldots,i_n} + u^{(0)} e^{(0)}$$

from F (with all u's from $K[x_1, \ldots, x_n]$). Then $(\underline{u}) \in M$ implies

$$\sum_{i_1,\ldots,i_m=0}^{p-1} u_{i_1,\ldots,i_m} \cdot \prod_{\nu=1}^{m} f_\nu^{i_\nu} + \sum_{j=1}^{l} \sum_{i_1,\ldots,i_n=1}^{p-1} u^{(l)}_{i_1,\ldots,i_n} \cdot \prod_{\nu=1}^{n} x_\nu^{i_\nu} h_j - u^{(0)} = 0,$$

so

$$\overline{u^{(0)}} = \sum_{i_1,\ldots,i_m=0}^{p-1} \overline{u_{i_1,\ldots,i_m}} \cdot \prod_{\nu=1}^{m} \overline{f_\nu}^{i_\nu}. \tag{1.6}$$

First we show that all $\overline{g_i}^p$ lie in A. All $\varphi(C_j)$ lie in M, and therefore also $\sum_{j=1}^{s} \varphi(a_{i,j})\varphi(C_j) \in M$. The $e^{(0)}$-component of $\sum_{j=1}^{s} \varphi(a_{i,j})\varphi(C_j)$ is g_i^p by Step 7 of the algorithm. Moreover, for all $i_1, \ldots, i_m \in \{0, \ldots, p-1\}$, the $e_{i_1,\ldots,i_m}$-component of $\sum_{j=1}^{s} a_{i,j} C_j$ is equal to the corresponding component of s_i by Step 6, and s_i lies in $K[\widetilde{f_1}, \ldots, \widetilde{f_m}]$. Thus the $e_{i_1,\ldots,i_m}$-component of $\sum_{j=1}^{s} \varphi(a_{i,j})\varphi(C_j)$ lies in $K[\varphi(\widetilde{f_1}), \ldots, \varphi(\widetilde{f_m})]$. But $\varphi(\widetilde{f_j}) = f_j^p$ by the definition of the $\widetilde{f_j}$, so from (1.6) we obtain

$$\overline{g_i}^p = \sum_{i_1,\ldots,i_m=0}^{p-1} \overline{u_{i_1,\ldots,i_m}} \cdot \prod_{\nu=1}^{m} \overline{f_\nu}^{i_\nu}$$

with $u_{i_1,\ldots,i_m}$ elements from $K[f_1^p, \ldots, f_m^p]$. Hence indeed $\overline{g_i}^p \in A$.

Now we show that every element from $\sqrt[p]{A}$ is an A-linear combination of $\overline{g_1}, \ldots, \overline{g_r}$. So take $g \in K[x_1, \ldots, x_n]$ such that $\overline{g} \in \sqrt[p]{A}$. This means that $\overline{g}^p \in A \cap K[\overline{x_1}^p, \ldots, \overline{x_m}^p]$. So on the one hand there exists $u^{(0)} \in K[x_1^p, \ldots, x_n^p]$ with $\overline{g}^p = \overline{u^{(0)}}$, and on the other hand we have $u_{i_1,\ldots,i_m} \in K[f_1^p, \ldots, f_m^p]$ (for $i_1, \ldots, i_m \in \{0, \ldots, p-1\}$) such that

$$\overline{u^{(0)}} = \overline{g}^p = \sum_{i_1,\ldots,i_m=0}^{p-1} \overline{u_{i_1,\ldots,i_m}} \cdot \prod_{\nu=1}^{m} \overline{f_\nu}^{i_\nu}. \tag{1.7}$$

Indeed, any element of A can be written like this. But this means that there exist polynomials $u^{(j)}_{i_1,\ldots,i_n} \in K[x_1^p, \ldots, x_n^p]$ (for $j \in \{1, \ldots, l\}$ and $i_1, \ldots, i_m \in \{0, \ldots, p-1\}$) such that

$$u^{(0)} - \sum_{i_1,\ldots,i_m=0}^{p-1} u_{i_1,\ldots,i_m} \cdot \prod_{\nu=1}^{m} f_\nu^{i_\nu} = \sum_{j=1}^{l} \sum_{i_1,\ldots,i_n=1}^{p-1} u^{(j)}_{i_1,\ldots,i_n} \cdot \prod_{\nu=1}^{n} x_\nu^{i_\nu} h_j. \tag{1.8}$$

Indeed, any element from I can be written as an expression as on the right-hand side of (1.8). Equation (1.8) implies that the element

$$(\underline{u}) = \sum_{i_1,\dots,i_m=0}^{p-1} u_{i_1,\dots,i_m} e_{i_1,\dots,i_m} + \sum_{j=1}^{l} \sum_{i_1,\dots,i_n=1}^{p-1} u^{(l)}_{i_1,\dots,i_n} e^{(l)}_{i_1,\dots,i_n} + u^{(0)} e^{(0)}$$

of F lies in M. Observe that all coefficients of $(\underline{u})$ lie in $K[x_1^p, \dots, x_n^p]$. Thus by Step 4 of the algorithm, $(\underline{u})$ lies in the $K[x_1^p, \dots, x_n^p]$-span of the $\varphi(C_i)$. It is convenient to write $u_{i_1,\dots,i_m} = \varphi(U_{i_1,\dots,i_m})$ with $U_{i_1,\dots,i_m} \in K[y_1, \dots, y_n]$. Then

$$\sum_{i_1,\dots,i_m=0}^{p-1} U_{i_1,\dots,i_m} \cdot e_{i_1,\dots,i_m} \in \widetilde{M}$$

with $\widetilde{M}$ as defined in Step 5. But we know that the $u_{i_1,\dots,i_m}$ really lie in $K[f_1^p, \dots, f_m^p]$, which implies $U_{i_1,\dots,i_m} \in K[\widetilde{f_1}, \dots, \widetilde{f_m}]$. So by Step 6 there exist $B_1, \dots, B_r \in K[\widetilde{f_1}, \dots, \widetilde{f_m}]$ such that

$$\sum_{i_1,\dots,i_m=0}^{p-1} U_{i_1,\dots,i_m} \cdot e_{i_1,\dots,i_m} = \sum_{i=1}^{r} B_i s_i = \sum_{i=1}^{r} B_i \cdot \sum_{j=1}^{s} a_{i,j} \pi(C_j).$$

Applying φ to this and setting $b_i := \varphi(B_i) \in K[f_1^p, \dots, f_m^p]$ yields

$$\sum_{i_1,\dots,i_m=0}^{p-1} u_{i_1,\dots,i_m} \cdot e_{i_1,\dots,i_m} = \sum_{i=1}^{r} b_i \sum_{j=1}^{s} \varphi(a_{i,j}) \cdot \sum_{i_1,\dots,i_m=0}^{p-1} \varphi\big(C_j^{(i_1,\dots,i_m)}\big) e_{i_1,\dots,i_m},$$

where $C_j^{(i_1,\dots,i_m)}$ stands for the $e_{i_1,\dots,i_m}$-component of C_j. So for every $i_1, \dots, i_m \in \{0, \dots, p-1\}$ we have

$$u_{i_1,\dots,i_m} = \sum_{i=1}^{r} b_i \sum_{j=1}^{s} \varphi(a_{i,j}) \cdot \varphi\big(C_j^{(i_1,\dots,i_m)}\big).$$

Substituting this into (1.7) yields

$$\overline{g}^p = \sum_{i=1}^{r} \overline{b_i} \sum_{j=1}^{s} \overline{\varphi(a_{i,j})} \cdot \sum_{i_1,\dots,i_m=0}^{p-1} \overline{\varphi\big(C_j^{(i_1,\dots,i_m)}\big)} \cdot \prod_{\nu=1}^{m} \overline{f_\nu}^{i_\nu}.$$

But $\varphi(C_j) \in M$ for all j, so we can apply (1.6) and obtain

$$\overline{g}^p = \sum_{i=1}^{r} \overline{b_i} \sum_{j=1}^{s} \overline{\varphi(a_{i,j})} \cdot \overline{\varphi\big(C_j^{(0)}\big)} = \sum_{i=1}^{r} \overline{b_i}\, \overline{g_i}^p,$$

where the last equality follows from Step 7. Since $b_i \in K[f_1^p, \ldots, f_m^p]$ and since K is perfect, there exist pth roots of the b_i in $K[f_1, \ldots, f_m]$. Hence there exist $\widetilde{b}_i \in A$ with $\widetilde{b}_i^p = \overline{b_i}$. We obtain

$$\overline{g}^p = \sum_{i=1}^{r} \widetilde{b}_i^p \overline{g_i}^p = \left(\sum_{i=1}^{r} \widetilde{b}_i \overline{g_i} \right)^p.$$

Since I is a radical ideal, this implies $\overline{g} = \sum_{i=1}^{r} \widetilde{b}_i \overline{g_i}$ with $\widetilde{b}_i \in A$. This completes the proof. □

The following algorithm is used in Algorithm 1.4. It is a slight extension of Algorithm 7 in Kemper [13] (see also Kreuzer and Robbiano [16, Section 3.6, Exercise 10 c]).

Algorithm 1.5 *(Intersection of a submodule with a subalgebra).*

Input: Generators $b_1, \ldots, b_l$ of a submodule $M \subseteq K[x_1, \ldots, x_n]^r$, and polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ generating a subalgebra $A := K[f_1, \ldots, f_m]$.

Output:
- Generators $c_1, \ldots, c_s$ of $M \cap A^r$ as an A-module;
- if desired, elements $C_1, \ldots, C_s \in K[y_1, \ldots, y_m]^r$ with $K[y_1, \ldots, y_m]$ a polynomial ring such that substituting $y_i \mapsto f_i$ in C_i yields c_i;
- if desired, a matrix $(a_{i,j}) \in K[x_1, \ldots, x_n]^{s \times l}$ such that

$$c_i = \sum_{j=1}^{l} a_{i,j} b_j \tag{1.9}$$

for all $i \in \{1, \ldots, s\}$.

(1) Let $S := K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be a polynomial ring with additional indeterminates $y_1, \ldots, y_m$. Form the submodule $\widetilde{M}$ of S^r generated by b_i $(i = 1, \ldots, l)$ and by $(f_j - y_j) \cdot e_k$ $(j = 1, \ldots, m, k = 1, \ldots, r)$, where the e_k are the free generators of S^r.

(2) Choose a monomial ordering ">" on S^r such that

$$x_i e_j > y_1^{d_1} \cdots y_m^{d_m} e_{j'}$$

for all $i \in \{1, \ldots, n\}$, $j, j' \in \{1, \ldots, r\}$, and $d_k \in \mathbb{N}$.

(3) Compute a Gröbner basis $\mathcal{G}$ of $\widetilde{M}$ with respect to ">". If the matrix $(a_{i,j})$ is desired, keep track of how each element from $\mathcal{G}$ can be represented as an S-linear combination of the b_i and $(f_j - y_j) \cdot e_k$.

(4) Let $C_1, \ldots, C_s$ be those elements from $\mathcal{G}$ which lie in $K[y_1, \ldots, y_m]^r$, and obtain c_i by substituting $y_i \mapsto f_i$ in C_i.

(5) If the matrix $(a_{i,j})$ is desired, use the normal form algorithm to express each c_i as an S-linear combination of the elements of $\mathcal{G}$, and then as a linear combination of the b_j and $(f_j - y_j) \cdot e_k$:

$$c_i = \sum_{j=1}^{l} \widetilde{a}_{i,j} b_j + \sum_{j=1}^{m} \sum_{k=1}^{r} \widetilde{a}_{i,j,k} (f_j - y_j) \cdot e_k \tag{1.10}$$

with $\widetilde{a}_{i,j}, \widetilde{a}_{i,j,k} \in S$. Then $a_{i,j}$ is obtained by substituting $y_k \mapsto f_k$ in $\widetilde{a}_{i,j}$.

Proof of correctness of Algorithm 1.5. We only need to prove the correctness of Step 5, since everything else is already contained in Algorithm 7 from [13]. First, the c_i are contained in M and therefore in $\widetilde{M}$, so the normal form is zero. Hence the $\widetilde{a}_{i,j}$ and $\widetilde{a}_{i,j,k}$ in (1.10) exist. Now substituting $y_v \mapsto f_v$ in (1.10) yields (1.9). □

Remark 1.6. Algorithm 1.5 can be generalized to arbitrary finitely generated commutative K-algebras. Suppose that $A = K[x_1, \ldots, x_l]/J$ is a subalgebra of a K-algebra $B = K[x_1, \ldots, x_n]/I$ with $l \leqslant n$ (so $I \cap K[x_1, \ldots, x_l] = J$), and M is a B-submodule of B^r. Consider the quotient map

$$\varphi : K[x_1, \ldots, x_n]^r \to B^r = K[x_1, \ldots, x_n]^r / I^r$$

and define $\overline{M} = \varphi^{-1}(M)$. To compute $M \cap A^r$, note that

$$\begin{aligned} M \cap A^r &= M \cap \varphi\big(K[x_1, \ldots, x_l]^r\big) \\ &= \varphi\big(\varphi^{-1}(M) \cap K[x_1, \ldots, x_l]^r\big) = \varphi\big(\overline{M} \cap K[x_1, \ldots, x_l]^r\big). \end{aligned}$$

Generators of $\overline{M} \cap K[x_1, \ldots, x_l]^r$ can be computed using Algorithm 1.5.

We are now ready to present an algorithm for computing generating invariants of a reductive groups acting on an affine variety. Recall that every reductive group in characteristic 0 is linearly reductive, so Derksen's algorithm [2] applies for computing its invariant rings. Therefore we may assume that the characteristic is positive.

Algorithm 1.7 *(Invariants of a reductive group acting on an affine variety).*

Input: A reductive algebraic group G over an algebraically closed field K of characteristic p, and a G-variety X given according to Convention 1.1.

Output: Polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ such that the residue classes $f_i + I \in K[X]$ are G-invariant and generate $K[X]^G$.

(1) Use Algorithm 1.2 to calculate an equivariant embedding $X \to V$ into a G-module V. Let $h_1, \ldots, h_r \in K[x_1, \ldots, x_n]$ be the polynomials by which this embedding is given, and write $K[V] = K[y_1, \ldots, y_r]$ with y_i indeterminates.

(2) Use Algorithm 1.9 of [15] to compute generators $F_1, \ldots, F_k \in K[y_1, \ldots, y_r]$ of $K[V]^G$. In fact, it is enough if $F_1, \ldots, F_k$ are homogeneous, separating invariants, as computed by Algorithm 2.9 of [15], in which case $K[V]^G$ will be the inseparable closure of $K[F_1, \ldots, F_k]$ (see Remark 1.3).

(3) For $i = 1, \ldots, k$, set

$$f_i := F_i(h_1, \ldots, h_r) \in K[x_1, \ldots, x_n],$$

and let $A \subseteq K[X]$ be the K-algebra generated by the $\overline{f_i} := f_i + I \in K[X]$.

(4) Use Algorithm 1.4 to compute $\sqrt[p]{A} \subseteq K[X]$. Let S be the set of generators of $\sqrt[p]{A}$ returned by Algorithm 1.4.

(5) For each $\overline{g} \in S$, test whether $\overline{g} \in A$ (see Remark 1.8). If $\overline{g} \notin A$, set

$$f_{k+1} := g, \quad A := K[\overline{f_1}, \ldots, \overline{f_{k+1}}] \quad \text{and} \quad k := k+1.$$

(6) If in Step 5 all $\overline{g} \in S$ were found to already lie in A, then $K[X]^G = A$ and we are done. Otherwise, go back to Step 4.

Remark 1.8. The membership test in Step 5 of Algorithm 1.7 can be done as follows: With additional indeterminates $t, t_1, \ldots, t_k$ choose a monomial ordering on $K[t, t_1, \ldots, t_k, x_1, \ldots, x_n]$ such that every monomial in $t, t_1, \ldots, t_k$ is smaller than any x_i, and every monomial in $t_1, \ldots, t_k$ is smaller than t. Compute a Gröbner basis $\mathcal{G}$ of the ideal in $K[t, t_1, \ldots, t_k, x_1, \ldots, x_n]$ generated by

$$g - t, \quad f_i - t_i \quad (i = 1, \ldots, k), \quad \text{and} \quad I$$

with respect to this monomial ordering. Then $\overline{g} \in A$ if and only if $\mathcal{G}$ contains a polynomial with the lead monomial t. This can be viewed as a (very) special case of Algorithm 1.5.

Proof of correctness of Algorithm 1.7. With $\varphi : X \to V$ the map given in Step 1 of the algorithm, we have a G-equivariant epimorphism

$$\varphi^* : K[V] \to K[X], \qquad F \mapsto F \circ \varphi$$

of K-algebras, and $f_i + I$, as formed in Step 3, is just the φ^*-image of F_i. Thus $A = K[f_1 + I, \ldots, f_k + I]$, also formed in Step 3, is a subalgebra of $K[X]^G$. The algorithm keeps increasing k and enlarging A until reaching the inseparable closure $\widehat{A}$. In this proof, the letter A will always denote the subalgebra formed in Step 3.

Since $K[X]$ is a reduced ring, clearly every $\overline{g} \in \widehat{A}$ is an invariant in $K[X]^G$. Conversely, take $\overline{g} \in K[X]^G$. Since G is reductive, there exists a p-power s such that $\overline{g}^s \in \varphi^*(K[V]^G)$ (see Mumford et al. [19, Lemma A.1.2]), so $\overline{g}^s = \varphi^*(F)$ with $F \in K[V]^G$. Since $K[V]^G$ is the inseparable closure of $K[F_1, \ldots, F_k]$, there exists a p-power q with $F^q \in K[F_1, \ldots, F_k]$, so

$$\overline{g}^{sq} \in \varphi^*\big(K[F_1, \ldots, F_k]\big) = A.$$

This shows that indeed $\widehat{A} = K[X]^G$. Since $K[X]^G$ is finitely generated as a K-algebra (see Nagata [21]) and $K[X]^G = \widehat{A}$ by the above, $K[X]^G$ is finitely generated as an A-module. This proves that Algorithm 1.7 terminates after finitely many steps. □

Problem 1.9. We are still left with the problem of finding an algorithm that computes A^G, where A is a finitely generated K-algebra which need not be reduced and G is a reductive group acting on A such that A is locally finite. By Nagata [21], A^G is finitely generated in this case.

1.3. Connected groups acting on normal varieties

In this section we consider the case of a connected reductive group G acting on a normal, irreducible affine variety X. This case is more special than the one dealt with in Algorithm 1.7. But we will present a simpler and probably faster algorithm for computing $K[X]^G$. The idea for this

algorithm was stimulated by the paper [9] of Hashimoto, which gives an algorithm for computing generating invariants of a simply connected simple linear algebraic group with a linear action.

Recall that for a reductive group G and a G-module V we can always compute a subalgebra $A \subseteq K[V]^G$ such that $K[V]^G$ is integral over A. Indeed, the possibly simplest way of doing this is by computing what Kemper [15] calls the "Derksen ideal" by performing the first two steps of Algorithm 2.9 in [15] (same as the first three steps in Algorithm 4.1.9 from [3]), and then setting one set of variables equal to zero in the generators of the Derksen ideal (Step 4 in [3, Algorithm 4.1.9]). This will yield a set of polynomials $\{g_1, \ldots, g_s\} \subset K[V]$ which define Hilbert's nullcone (see [3, Section 2.4.1 and Remark 4.1.4]). Now use Algorithm 2.7 from [15] to compute homogeneous invariants $f_1, \ldots, f_k \in K[V]^G$ degree by degree until every g_i lies in the radical of the ideal in $K[V]$ generated by the f_j. Then $K[V]^G$ will be integral over $K[f_1, \ldots, f_k]$. An alternative method would be to use Algorithm 2.9 from [15] to compute a graded separating subalgebra of $K[V]^G$. Then $K[V]^G$ will be integral over this subalgebra (see Lemma 1.3 in [15]). Compared with the first method outlined above, computing separating invariants involves one additional major Gröbner basis computation, which is not really necessary for our purposes.

We can now present an algorithm for computing $K[X]^G$ for X normal and G connected and reductive. The algorithm involves the computation of the integral closure of one ring in another, which will be discussed shortly.

Algorithm 1.10 *(Invariants for G connected and reductive, X normal).*

Input: A connected, reductive group G over an algebraically closed field K, and a normal, irreducible G-variety X, given according to Convention 1.1.
Output: Generators of $K[X]^G$ as a K-algebra.

(1) Use Algorithm 1.2 to calculate an equivariant embedding $\varphi : X \to V$ into a G-module V.
(2) Construct invariants $f_1, \ldots, f_k \in K[V]^G$ such that $K[V]^G$ is integral over $K[f_1, \ldots, f_k]$ (see the above discussion).
(3) Form the subalgebra $A \subseteq K[X]^G$ generated by all $f_i \circ \varphi$ (see Step 3 of Algorithm 1.7).
(4) Use Algorithm 1.12 to compute the integral closure B of A in $K[X]$. Then

$$K[X]^G = B.$$

The following lemma will be used in the proof of correctness of Algorithm 1.10. We write G^0 for the connected component of an algebraic group G.

Lemma 1.11. *Let G be an affine algebraic group over an algebraically closed field K, and let X be a G-variety. Let $A \subseteq K[X]^G$ be a subalgebra such that $K[X]^G$ is integral over A. Then $K[X]^{G^0}$ is the integral closure of A in $K[X]$.*

Proof. We write B for the integral closure of A in $K[X]$. First take $b \in B$ arbitrary. There exists a monic polynomial $F \in A[T]$ with $F(b) = 0$. Thus for every $\sigma \in G$ we also have $F(\sigma(b)) = 0$. On the other hand, F has at most finitely many zeros in $K[X]$. Indeed, this follows from the fact that for each irreducible component X_i of X, restricting the coefficients of F yields a nonzero polynomial with only finitely many zeros in $K[X_i]$. It follows that the G-orbit of b is finite. Therefore the stabilizer $G_b \subseteq G$ of b has finite index in G, which implies $G^0 \subseteq G_b$. Hence $b \in K[X]^{G^0}$.

Conversely, take $f \in K[X]^{G^0}$. Then

$$F(T) := \prod_{\sigma \in G/G^0} \big(T - \sigma(f)\big) \in K[X]^G[T],$$

and $F(f) = 0$. So f is integral over $K[X]^G$ and hence also over A. It follows that $f \in B$. □

Proof of correctness of Algorithm 1.10. It follows from the reductivity of G that $K[X]^G$ is integral over A. From this, $K[X]^G = B$ follows by Lemma 1.11. □

The following algorithm for computing the integral closure of one ring in another is mostly drawn from Vasconcelos [24, Chapter 6].

Algorithm 1.12 *(Integral closure).*

Input: A prime ideal $I \subseteq K[x_1, \ldots, x_n]$ defining a normal domain $B := K[x_1, \ldots, x_n]/I$, and polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ defining a subalgebra $A = K[\overline{f_1}, \ldots, \overline{f_k}] \subseteq B$, where we write $\overline{f_i} := f_i + I$.

Output: Polynomials $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ such that $K[\overline{g_1}, \ldots, \overline{g_r}]$ is the integral closure of A in B.

(1) With an additional indeterminate t, form the algebra

$$D := K[\overline{f_1}, \ldots, \overline{f_k}, t, t\overline{x_1}, \ldots, t\overline{x_n}] \subseteq B[t].$$

(2) Compute $h_1, \ldots, h_r \in K[x_1, \ldots, x_n, t]$ such that the $\overline{h_i} \in B[t]$ generate the normalization $\widetilde{D}$ of D. This can be done by using de Jong's algorithm (see de Jong [11] or Derksen and Kemper [3, Section 1.6]).

(3) For $i = 1, \ldots, r$, obtain g_i from by setting $t = 0$ in h_i.

Proof of correctness of Algorithm 1.12. Since B is a normal domain, the same is true for $B[t]$ (see, for example, Eisenbud [4, Exercise 4.18]). Therefore $\widetilde{D}$ is contained in $B[t]$, which shows that its generators $\overline{h_i}$ do lie in $B[t]$ rather than just in $Q(B)[t]$, where $Q(B)$ denotes the field of fractions of B. Consider the map $\varphi : B[t] \to B$ of B-algebras given by $t \mapsto 0$. The definition of D implies $\varphi(D) = A$. For each $h \in \widetilde{D}$ we have an equation

$$h^s + d_1 h^{s-1} + \cdots + d_{r-1} h + d_s = 0$$

with $d_i \in D$. Applying φ to this yields an integral equation for $\varphi(h)$ over A. If follows that the $\overline{g_i} = \varphi(\overline{h_i})$ from Step 3 are integral over A.

Conversely, take $g \in B$ arbitrary such that b is integral over A. Then g, seen as an element of $B[t]$, is integral over D. Moreover, $Q(D) = Q(B[t])$ by the definition of D, so $g \in Q(D)$. It follows that $g \in \widetilde{D}$, so there exists a polynomial F such that $g = F(\overline{h_1}, \ldots, \overline{h_r})$. Applying φ yields

$$g = \varphi(g) = F(\overline{g_1}, \ldots, \overline{g_r}).$$

This completes the proof. □

Remark 1.13. In the previous algorithm, module generators of $\widetilde{A}$ as an A-module can be computed as follows. Using Gröbner elimination one can compute the kernel J of the homomorphism

$$K[y_1, \ldots, y_r, z_1, \ldots, z_k] \to B = K[x_1, \ldots, x_n]/I$$

defined by $y_i \mapsto \overline{g}_i$ and $z_i \mapsto \overline{f}_i$. We now can identify A with the algebra generated by $z_1 + J$, $\ldots, z_k + J$ and its normalization $\widetilde{A}$ with $K[y_1, \ldots, y_r, z_1, \ldots, z_k]/J$. Choose a monomial ordering such that y_i is larger than any monomial in the z-variables for all i and let $\mathcal{G}_J$ be a Gröbner basis of J with respect to this ordering. Since $\widetilde{A}$ is integral over A, $y_i + J$ is integral over A for all i. It follows that a power of y_i appears as a leading monomial in the Gröbner basis. So there are only finitely many monomials in $y_1, \ldots, y_r$ which are not in the leading monomial ideal of J, and these monomials generate $\widetilde{A}$ as an A-module.

Remark 1.14. In Algorithm 1.12 we have assumed that B is normal. We will sketch how to deal with the more general case where B is a domain which need not be normal. Compute the normalization $\widetilde{B}$ of B using de Jong's algorithm (see [11] or [3, Section 1.6]). Let $\widetilde{A}$ be the integral closure of A in $\widetilde{B}$. Generators of $\widetilde{A}$ can be computed using Algorithm 1.12. Find A-module generators $h_1, \ldots, h_s$ of $\widetilde{A}$ as in Remark 1.13. Define

$$M = \left\{ (a_1, \ldots, a_s) \in B^s \;\middle|\; \sum_{i=1}^{s} a_i h_i \in B \right\}.$$

Find $g \in B \setminus \{0\}$ such that $gh_i \in B$ for all i. We may identify M with

$$\left\{ (a_1, \ldots, a_s, b) \in B^{s+1} \;\middle|\; \sum_{i=1}^{s} a_i h_i + b = 0 \right\}$$
$$= \left\{ (a_1, \ldots, a_s, b) \in B^{s+1} \;\middle|\; \sum_{i=1}^{s} a_i g h_i + bg = 0 \right\}.$$

So M can be viewed as a syzygy module, and generators of M can be computed using Vasconcelos [24, §1.3] or Derksen and Kemper [3, §1.3] (computing syzygies between elements $u_1 + I, \ldots, u_t + I$ in $B = K[x_1, \ldots, x_n]/I$ can easily be reduced to computing syzygies between $u_1, \ldots, u_t$ and generators of I in the polynomial ring $K[x_1, \ldots, x_n]$). We have

$$M \cap A^s = \left\{ (a_1, \ldots, a_s) \in A^s \;\middle|\; \sum_{i=1}^{s} a_i h_i \in \widetilde{A} \cap B \right\}.$$

Define $\varphi : M \to B$ by $\varphi(a_1, \ldots, a_r) = \sum_{i=1}^{s} a_i h_i$. Then $\varphi(M \cap A^s) = \widetilde{A} \cap B$ is the integral closure of A in B. Generators of $M \cap A^s$ can be computed, using Remark 1.6.

2. Quasi-affine varieties and Hilbert's fourteenth problem

This section provides some methods for dealing with nonfinitely generated algebras.

2.1. The colon operation

For a subset B of a ring, B^r will denote the set of all products of r elements from B. We generalize the notion of a colon ideal as follows.

Definition 2.1. For a commutative ring S and subsets $A, B \subseteq S$ we define

$$(A : B)_S = \{f \in S \mid fB \subseteq A\}$$

and

$$\left(A : B^\infty\right)_S = \bigcup_{r=1}^{\infty} \left(A : B^r\right)_S = \left\{f \in S \,\middle|\, \exists r \ fB^r \subseteq A\right\}.$$

Example 2.2. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of S, then $(\mathfrak{a} : \mathfrak{b})_S$ and $(\mathfrak{a} : \mathfrak{b}^\infty)_S$ are the usual colon ideals (see for example Vasconcelos [24, Chapter 2]).

If R is a domain with quotient field $Q(R)$, and $f \in R \setminus \{0\}$ then

$$\left(R : \{f\}^\infty\right)_{Q(R)} = R_f,$$

the localization of R with respect to the element f. This generalizes as follows. Suppose that $R = K[X]$ is the coordinate ring of an irreducible affine variety X. Let $Y \subseteq X$ be a zero set of an ideal $\mathfrak{a} \subseteq R$. The ring of regular functions on the quasi-affine variety $U := X \setminus Y$ is denoted by $K[U]$.

Lemma 2.3. *We have*

$$K[U] = \left(R : \mathfrak{a}^\infty\right)_{Q(R)}.$$

Proof. Suppose that $f \in (R : \mathfrak{a}^\infty)_{Q(R)}$ and $p \in U$. There exists $h \in \mathfrak{a}$ with $h(p) \neq 0$. We have $g = h^s f \in R$ for some nonnegative integer s. So $f = h^{-s} g$ is a regular function on an open neighborhood of $p \in U$. Since $p \in U$ was chosen arbitrarily, we conclude that $f \in K[U]$.

Conversely, suppose that $f \in K[U]$. We may write $\mathfrak{a} = (a_1, \ldots, a_r)$. Because $K[U] \subseteq R_{a_i}$ there exists a nonnegative integer l_i such that $a_i^{l_i} f \in R$ for all i. Set $N = l_1 + l_2 + \cdots + l_r - r + 1$. Then

$$\mathfrak{a}^N f \subseteq R,$$

because $\mathfrak{a}^N$ is spanned by monomials $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$ with $k_1 + \cdots + k_r = N$ and the definition of N implies that $k_i \geqslant l_i$ for some i. □

If $f \in \mathfrak{a}$ is nonzero, then we have $K[U] \subseteq R_f$ and

$$K[U] = \left(R : \mathfrak{a}^\infty\right)_{Q(R)} = \left(R : \mathfrak{a}^\infty\right)_{R_f}. \tag{2.1}$$

Note that such a ring of regular functions on a quasi-affine variety is not always finitely generated over K (see Nagata [22, Chapter V.5] or Winkelmann [25]). Rings of the form $(R : \mathfrak{a}^\infty)_{Q(R)}$ are *ideal transforms* in the sense of Nagata [22]. Suppose that G is an algebraic group and X is an affine G-variety. Nagata showed that the invariant ring $K[X]^G$ may not be finitely generated [20]. However, he also showed that if X is normal, then the invariant ring $K[X]^G$ is isomorphic to some *ideal transform* of a finitely generated domain over K [22, Chapter V, Proposition 4]. In other words, $K[X]^G$ can be viewed as $K[U]$ for some quasi-affine variety U. Later, we will study this in more detail.

The following lemma is easy to prove:

Lemma 2.4.

(a) *If $\mathfrak{a}$ is an ideal of the ring S, and $B \subseteq S$ then $(\mathfrak{a} : B)_S$ and $(\mathfrak{a} : B^\infty)_S$ are ideals of S.*
(b) *If S is an algebra over some field, $A \subseteq S$ is a subalgebra and $B \subseteq A$, then $(A : B^\infty)_S$ is a subalgebra of S.*

Suppose that the additive group $\mathbb{G}_a$ acts regularly on an irreducible affine variety X. Then $\mathbb{G}_a$ also acts on the coordinate ring $S := K[X]$. An algorithm for computing the generators of the invariant ring $S^{\mathbb{G}_a}$ was given by van den Essen [5]. Van den Essen first constructs a subalgebra R of the invariant ring, and an element $f \in R$ such that $S^{\mathbb{G}_a} = R_f \cap S = (R : f^\infty)_S$ (for details, see Section 3.1.1). He then gives an algorithm for computing a set of generators of the ring $S^{\mathbb{G}_a} = (R : f^\infty)_S$ over K. The algorithm terminates if this ring is finitely generated.

In this section we will give a generalization of van den Essen's algorithm for computing generators of $(R : f^\infty)_S$. We will give an algorithm for computing generators of the ring $(R : \mathfrak{a}^\infty)_S$ for a finitely generated domain S over K, a finitely generated subalgebra R and any ideal $\mathfrak{a}$ of R. Our algorithm will terminate if and only if $(R : \mathfrak{a}^\infty)_S$ is finitely generated. This extension is quite useful, as it allows us to compute rings of regular functions on irreducible quasi-affine varieties by using (2.1).

Suppose that S is a domain over a field K, R is a finitely generated subalgebra and $\mathfrak{a} \subseteq R$ is an ideal. Then $(R : \mathfrak{a})_S$ is an R-module. Suppose that $\mathfrak{a}$ is nonzero. Then we can choose a nonzero element $f \in \mathfrak{a}$. >From the definition it follows that $f(R : \mathfrak{a})_S \subseteq R$. This way, we may identify $(R : \mathfrak{a})_S$ as a submodule of R. In particular, $(R : \mathfrak{a})_S$ is finitely generated as an R-module. We will first give an algorithm for finding R-module generators of $(R : \mathfrak{a})_S$.

Algorithm 2.5 *(Computation of $(R : \mathfrak{a})_S$).*

Input: A finite set $\mathcal{G}_I$ of generators of a prime ideal I such that $S = K[x_1, \ldots, x_n]/I$, polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ such that R is generated by $f_1 + I, \ldots, f_r + I$, and a finite set $\mathcal{A} \subset K[y_1, y_2, \ldots, y_r]$ such that the (nonzero) ideal $\mathfrak{a} \subseteq R$ is generated by $g(f_1, \ldots, f_r) + I$, $g \in \mathcal{A}$.
Output: A finite set $\mathcal{H} \subseteq K[x_1, \ldots, x_n]$ such that $(R : \mathfrak{a})_S$ is generated by $1 + I$ and all $h + I$, $h \in \mathcal{H}$ as an R-module. Moreover, if $(R : \mathfrak{a})_S = R$ then $\mathcal{H} = \emptyset$.

(1) Let $\mathfrak{b}$ be the ideal in $K[x_1, \ldots, x_n, y_1, \ldots, y_r]$ generated by I and all $y_i - f_i$, $i = 1, \ldots, r$. Compute a Gröbner basis $\mathcal{G}_J$ of $J := \mathfrak{b} \cap K[y_1, \ldots, y_r]$. (Choose an elimination ordering on the monomials of $K[x_1, \ldots, x_n, y_1, \ldots, y_r]$ and compute a Gröbner basis $\mathcal{G}_\mathfrak{b}$ of $\mathfrak{b}$. Then we have $\mathcal{G}_J = \mathcal{G}_\mathfrak{b} \cap K[y_1, \ldots, y_r]$.)

(2) Choose $u \in \mathcal{A}$ such that $u \notin J$. (Reduce all elements $u \in \mathcal{A}$ with respect to the Gröbner basis $\mathcal{G}_J$ until we have found an element u that does not reduce to 0.)
(3) Let $\mathfrak{d} \subseteq K[y_1, \ldots, y_r]$ be the ideal generated by J and $\mathcal{A}$. Compute a Gröbner basis $\mathcal{G}_\mathfrak{c}$ of the colon ideal $\mathfrak{c} := (J + (u)) : \mathfrak{d}$.
(4) Let $\mathfrak{v} \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_r]$ be the ideal generated by I, u and all $y_i - f_i$, $i = 1, 2, \ldots, r$. Compute a Gröbner basis $\mathcal{G}_\mathfrak{u}$ of $\mathfrak{u} := \mathfrak{v} \cap K[y_1, \ldots, y_r]$.
(5) Compute a Gröbner basis $\mathcal{G}_\mathfrak{q}$ of the intersection $\mathfrak{q} := \mathfrak{u} \cap \mathfrak{c}$.
(6) Compute a Gröbner basis $\mathcal{G}_\mathfrak{p}$ of the ideal $\mathfrak{p} := J + (u)$ in $K[y_1, \ldots, y_r]$.
(7) Replace $\mathcal{G}_\mathfrak{q}$ by the subset of all elements that do not reduce to 0 with respect to the Gröbner basis $\mathcal{G}_\mathfrak{p}$.
(8) If $\mathcal{G}_\mathfrak{q} = \{v_1, \ldots, v_s\}$, compute $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ such that

$$v_i(f_1, \ldots, f_r) + I = u(f_1, \ldots, f_r)h_i + I$$

for all i. To find $h_1, \ldots, h_s$, proceed as follows. Each v_i can be expressed in the form

$$v_i = \sum_{g \in \mathcal{G}_I} a_{i,g} g + b_i u + \sum_j c_{i,j}(y_j - f_j),$$

with $a_{i,g}, b_i, c_{i,j} \in K[x_1, \ldots, x_n, y_1, \ldots, y_r]$ for all g, i, j (this can be done using the extended Gröbner basis algorithm in step (4)). Then plug in $y_i = f_i$ for all i. We take

$$h_i = b_i(x_1, \ldots, x_n, f_1, \ldots, f_r)$$

for all i. Set $\mathcal{H} = \{h_1, \ldots, h_s\}$.

Proof of correctness of Algorithm 2.5. Consider the ring homomorphism

$$\varphi : K[y_1, \ldots, y_r] \to K[x_1, \ldots, x_n]/I \cong S$$

defined by $y_i \mapsto f_i + I$. The image of φ is isomorphic to R, and the kernel of φ is J. So we have

$$K[y_1, \ldots, y_r]/J \cong R.$$

The ideal $\mathfrak{a} \subseteq R$ is generated by all $\varphi(g)$, $g \in \mathcal{A}$. Since $\mathfrak{a} \subseteq R$ is a nonzero ideal, there must exist a $u \in \mathcal{A}$ such that $\varphi(u) \neq 0$. Hence there exists a $u \in \mathcal{A}$ that does not reduce to 0 modulo $\mathcal{G}_J$. The colon ideal $(\varphi(u)R : \mathfrak{a})_R \subseteq R$ is equal to $\varphi(\mathfrak{c})$, and $\varphi^{-1}((\varphi(u)R : \mathfrak{a})_R) = \mathfrak{c}$. The ideal $\mathfrak{u}$ is equal to $\varphi^{-1}(\varphi(u)S)$. We have

$$\mathfrak{q} = \varphi^{-1}\big(\varphi(u)R : \mathfrak{a}\big)_R \cap \varphi^{-1}\big(\varphi(u)S\big) = \varphi^{-1}\big(\big(\varphi(u)R : \mathfrak{a}\big)_R \cap \varphi(u)S\big).$$

Also, we get

$$\mathfrak{p} = \varphi^{-1}\big(\varphi(u)R\big) = (u) + J.$$

After step (7), $\mathfrak{q}$ is generated as an ideal in R by $\mathcal{G}_\mathfrak{q}$, u and J. It follows that $(\varphi(u)R : \mathfrak{a})_R \cap \varphi(u)S$ is generated by $\varphi(h)$, $h \in \mathcal{G}_q$ and $\varphi(u)$.

Since

$$\varphi(u)(R:\mathfrak{a})_S = \big(\varphi(u)R:\mathfrak{a}\big)_R \cap \varphi(u)S,$$

we have that $(R:\mathfrak{a})_S$ is generated as an R-module by $1=\varphi(u)/\varphi(u)$ and all $\varphi(v)/\varphi(u)$, $v\in\mathcal{G}_q$. If $\mathcal{G}_q=\{v_1,\ldots,v_s\}$ then

$$\varphi(v_i)=\varphi(u)(h_i+I)$$

for all i. Since $\mathcal{H}=\{h_1,\ldots,h_s\}$ we have that $(R:\mathfrak{a})_S$ is generated by all $1+I$ and all $h+I$, $h\in\mathcal{H}$.

By steps (6) and (7) we have that $\varphi(v_i)\notin\varphi(u)R$, and $h_i+I\notin R$. Hence, if $(R:\mathfrak{a})_S=R$ then $\mathcal{H}=\emptyset$. □

Algorithm 2.6 *(Computation of $(R:\mathfrak{a}^\infty)_S$).*

Input: Polynomials $f_1,\ldots,f_r\in K[x_1,\ldots,x_n]$ such that R is generated by $f_1+I,\ldots,f_r+I$, and a finite set $\mathcal{A}\subset K[y_1,y_2,\ldots,y_r]$ such that the (nonzero) ideal $\mathfrak{a}\subseteq R$ is generated by $g(f_1,\ldots,f_r)+I$, $g\in\mathcal{A}$.

Output: A (possibly infinite) sequence $h_1,h_2,h_3,\ldots$ of elements in $K[x_1,\ldots,x_n]$ such that $h_1+I,h_2+I,\ldots$ generate $(R:\mathfrak{a}^\infty)_S$ as a K-algebra. If $(R:\mathfrak{a}^\infty)$ is finitely generated, then the algorithm will terminate after finite time and the output will be a finite sequence.

(1) $F=\emptyset$
(2) $\mathcal{H}=\{f_1,\ldots,f_r\}$
(3) `while` $\mathcal{H}\neq\emptyset$ `do`
(4) `output`($\mathcal{H}$)
(5) $F:=F\cup\mathcal{H}$.
(6) Let $\mathcal{H}$ be the output of Algorithm 2.5 for the computation of $(\widetilde{R}:\mathfrak{a})_S$, where $\widetilde{R}$ is the algebra generated by all $f+I$, $f\in F$ and $\mathfrak{a}$ is the ideal in $\widetilde{R}$ generated by all $g(f_1,\ldots,f_r)+I$, $g\in\mathcal{A}$.
(7) `enddo`

Proof of correctness of Algorithm 2.6. Let $\widetilde{R}_i$ be the algebra $\widetilde{R}$ in step (6) in the ith iteration of the `while` loop in lines (3)–(7). We have $\widetilde{R}_1=R$ and

$$\widetilde{R}_{i+1}\supseteq(\widetilde{R}_i:\mathfrak{a}\widetilde{R}_i)_S=(\widetilde{R}_i:\mathfrak{a})_S,$$

where $\mathfrak{a}$ is the ideal in R generated by all $g(f_1,\ldots,f_r)+I$, $g\in\mathcal{A}$. It easily follows by induction that $\widetilde{R}_{i+1}\supseteq(R:\mathfrak{a}^i)_S$ for all i. Note that in step (6), the algebra $\widetilde{R}_i$ is generated by all $h+I$ with $h\in F$. Moreover, F is exactly the set of all polynomials that have been sent to the output.

If the algorithm does not terminate, then we have

$$\widetilde{R}_1\subseteq\widetilde{R}_2\subseteq\cdots$$

and

$$\bigl(R:\mathfrak{a}^{\infty}\bigr)_S=\bigcup_{i=1}^{\infty}\bigl(R:\mathfrak{a}^i\bigr)_S\subseteq\bigcup_{i=1}^{\infty}\widetilde{R}_i.$$

On the other hand it is easy to see (by induction) that $\widetilde{R}_i\subseteq(R:\mathfrak{a}^{\infty})_S$ for all i. It follows that

$$\bigl(R:\mathfrak{a}^{\infty}\bigr)_S=\bigcup_{i}\widetilde{R}_i. \tag{2.2}$$

If the output is $h_1,h_2,\ldots$ then the algebra generated by $h_1+I,h_2+I,\ldots$ contains $\widetilde{R}_i$ for all i. Therefore, the algebra generated by $h_1+I,h_2+I,\ldots$ is $(R:\mathfrak{a}^{\infty})_S$.

Suppose that $(R:\mathfrak{a}^{\infty})_S$ is finitely generated. By (2.2), $\widetilde{R}_i$ contains all generators of $(R:\mathfrak{a}^{\infty})_S$ for some i, and $\widetilde{R}_i=(R:\mathfrak{a}^{\infty})_S$. But then $\mathcal{H}=\emptyset$ after the ith iteration of the while loop and the algorithm terminates. The output is exactly F and $\widetilde{R}_i=(R:\mathfrak{a}^{\infty})_S$ is generated by all $h+I$, $h\in F$. □

2.2. Finite generation

In this section we study domains which are not finitely generated over K. We introduce the *finite generation ideal* of such an algebra.

Proposition 2.7. *Suppose that S is a domain which is finitely generated over a field K and that R is a subalgebra of S. Then there exists an nonzero element $f\in R$ such that R_f is finitely generated as a K-algebra.*

Proof. The quotient field of S is finitely generated over K. The quotient field of R lies between K and S, hence it is also finitely generated by Bourbaki [1, Chapter IV, §15, Corollary 3]. Choose a finitely generated subalgebra $T\subseteq R$ such that T and R have the same quotient field. By the theorem of generic freeness (see Eisenbud [4, Theorem 14.4] or Remark 2.15 below), there exists a nonzero element $f\in T$ such that S_f is a free T_f-module. Let B be a basis of S_f over T_f. We can write

$$1=\sum_{i=1}^{r}u_ie_i$$

with $e_1,e_2,\ldots,e_r\in B$ and $u_1,u_2,\ldots,u_r\in T_f$. Since R_f and T_f have the same quotient field, it follows that the submodule $R_f\subseteq S_f$ is contained in

$$T_fe_1\oplus T_fe_2\oplus\cdots\oplus T_fe_r\cong T_f^r.$$

This shows that R_f is contained in a finitely generated T_f-module. Since T_f is a finitely generated algebra, R_f is finitely generated as a T_f-module. It follows that R_f is a finitely generated algebra. □

The following result is well known. We give a proof for the reader's convenience. It is useful (and makes sense) to consider the zero-ring as a finitely generated algebra over K.

Proposition 2.8. *Suppose that R is a commutative algebra over a commutative ring K and $f, g \in R$ such that $(f, g) = R$. If R_f and R_g are finitely generated as K-algebras, then so is R.*

Proof. We may write

$$R_f = K\left[\frac{a_1}{1}, \ldots, \frac{a_r}{1}, \frac{1}{f}\right] \quad \text{and} \quad R_g = K\left[\frac{b_1}{1}, \ldots, \frac{b_l}{1}, \frac{1}{g}\right]$$

with $a_i, b_j \in R$. We have $1 = xf + yg$ with $x, y \in R$. Take $z \in R$. As an element of R_f, we can write $z/1$ as $z/1 = a/f^m$ with $a \in K[a_1, \ldots, a_r, f]$, so there exists a nonnegative integer m' with $f^{m'}(f^m z - a) = 0$. So we may assume $f^m z = a$. Likewise, $g^n z = b$ with $b \in K[b_1, \ldots, b_l, g]$. We obtain

$$\begin{aligned} z &= z(xf + yg)^{m+n} \\ &= \sum_{i=1}^{m} \binom{m+n}{i} (xf)^i y^{m+n-i} g^{m-i} b + \sum_{i=m+1}^{m+n} \binom{m+n}{i} x^i f^{i-m} (yg)^{m+n-i} a. \end{aligned}$$

This shows that

$$R = K[a_1, \ldots, a_r, b_1, \ldots, b_l, f, g, x, y]. \qquad \square$$

Proposition 2.9. *For a commutative algebra R over a commutative ring K, define*

$$\mathfrak{g} := \{f \in R \mid R_f \text{ is a finitely generated } K\text{-algebra}\}.$$

Then $\mathfrak{g}$ is a radical ideal of R.

Proof. If $f \in \mathfrak{g}$ and $g \in R$, then

$$R_{fg} = (R_f)_g$$

is finitely generated, because R_f is finitely generated. This implies $fg \in \mathfrak{g}$.

Suppose $f, g \in \mathfrak{g}$. We have $(f, g)R_{f+g} = R_{f+g}$, and the algebras $(R_{f+g})_f = (R_f)_{f+g}$ and $(R_{f+g})_g = (R_g)_{f+g}$ are finitely generated. By Proposition 2.8, R_{f+g} is finitely generated, so $f + g \in \mathfrak{g}$. It follows that $\mathfrak{g}$ is an ideal.

The ideal $\mathfrak{g}$ is clearly a radical ideal since $R_{f^r} = R_f$ for every $f \in R$ and any positive integer r. $\square$

We will call $\mathfrak{g}$ the *finite generation ideal* of R. Note that $\mathfrak{g} = R$ if and only if R is finitely generated. If R is a subalgebra of a finitely generated domain over a field, then the finite generation ideal is nonzero by Proposition 2.7.

Lemma 2.10. *Suppose that S is a domain over a field K, R is a subalgebra, and $\mathfrak{a} \subseteq R$ is an ideal. Set $\mathfrak{b} = (R : (R : \mathfrak{a})_S)_S$. Then $\mathfrak{b}$ is an ideal of R, and $\mathfrak{a} \subseteq \mathfrak{b}$. Moreover,*

$$\left(R : \mathfrak{a}^i\right)_S = \left(R : \mathfrak{b}^i\right)_S$$

for $i \in \mathbb{N} \cup \{\infty\}$.

Proof. Since $\mathfrak{a}(R:\mathfrak{a})_S \subseteq R$ by definition of $(R:\mathfrak{a})_S$ we get $\mathfrak{a} \subseteq \mathfrak{b} := (R:(R:\mathfrak{a})_S)_S$. Since $1 \in (R:\mathfrak{a})_S$ we get $\mathfrak{b} = (R:(R:\mathfrak{a})_S)_S \subseteq (R:\{1\})_S = R$. Also, $\mathfrak{b}$ is clearly an R-module, so it is an ideal of R. Since $\mathfrak{a} \subseteq \mathfrak{b}$ we have

$$(R:\mathfrak{a})_S \supseteq (R:\mathfrak{b})_S.$$

Because $\mathfrak{b} = (R:(R:\mathfrak{a})_S)_S$, we get $\mathfrak{b}(R:\mathfrak{a})_S \subseteq R$. From this it follows that

$$(R:\mathfrak{a})_S \subseteq (R:\mathfrak{b})_S.$$

We conclude that

$$(R:\mathfrak{a})_S = (R:\mathfrak{b})_S.$$

By induction on i we prove that

$$\left(R:\mathfrak{a}^i\right)_S = \left(R:\mathfrak{b}^i\right)_S.$$

The case $i = 1$ has already been done. Suppose that $i > 1$. Then we have

$$\begin{aligned}\left(R:\mathfrak{a}^i\right)_S &= \left((R:\mathfrak{a})_S:\mathfrak{a}^{i-1}\right)_S = \left((R:\mathfrak{b})_S:\mathfrak{a}^{i-1}\right)_S \\ &= \left(R:\mathfrak{b}\mathfrak{a}^{i-1}\right)_S = \left(\left(R:\mathfrak{a}^{i-1}\right)_S:\mathfrak{b}\right)_S.\end{aligned}$$

By induction we may assume that $(R:\mathfrak{a}^{i-1})_S = (R:\mathfrak{b}^{i-1})_S$. So we get

$$\left(R:\mathfrak{a}^i\right)_S = \left(\left(R:\mathfrak{a}^{i-1}\right)_S:\mathfrak{b}\right)_S = \left(\left(R:\mathfrak{b}^{i-1}\right)_S:\mathfrak{b}\right)_S = \left(R:\mathfrak{b}^i\right)_S.$$

We also have

$$\left(R:\mathfrak{a}^\infty\right)_S = \bigcup_i \left(R:\mathfrak{a}^i\right)_S = \bigcup_i \left(R:\mathfrak{b}^i\right)_S = \left(R:\mathfrak{b}^\infty\right)_S. \qquad \square$$

Lemma 2.11. *Suppose that R is a finitely generated subalgebra of a domain S over a field K, $\mathfrak{a}$ is an ideal of R and suppose that $\widetilde{R} = (R:\mathfrak{a}^\infty)_S = \bigcup_i \widetilde{R}_i$, where*

$$R \subseteq \widetilde{R}_1 \subseteq \widetilde{R}_2 \subseteq \cdots$$

is a sequence of finitely generated K-algebras. Define the ideal $\mathfrak{g}_i$ of $\widetilde{R}_i$ by

$$\mathfrak{g}_i = \sqrt{\left(\widetilde{R}_i:(\widetilde{R}_i:\mathfrak{a})_S\right)_S},$$

where the radical ideal is taken in $\widetilde{R}_i$. Then we have

$$\mathfrak{g}_1 \subseteq \mathfrak{g}_2 \subseteq \cdots$$

and

$$\mathfrak{g} := \bigcup_i \mathfrak{g}_i$$

is the finite generation ideal of $\widetilde{R}$.

Proof. Let us define $\mathfrak{h}_i = (\widetilde{R}_i : (\widetilde{R}_i : \mathfrak{a})_S)_S$ so that $\mathfrak{g}_i = \sqrt{\mathfrak{h}_i}$. Note that

$$\widetilde{R} = \big(R : \mathfrak{a}^\infty\big)_S = \big(\widetilde{R}_i : \mathfrak{a}^\infty\big)_S = \big(\widetilde{R}_i : \mathfrak{h}_i^\infty\big)_S = \big(\widetilde{R}_i : \mathfrak{g}_i^\infty\big)_S \tag{2.3}$$

by Lemma 2.10. Let $u_1, u_2, \ldots, u_t$ be generators of the $\widetilde{R}_{i+1}$-module $(\widetilde{R}_{i+1} : \mathfrak{a})_S$. This module is contained in $\widetilde{R} = (\widetilde{R}_i : \mathfrak{g}_i^\infty)_S$. Therefore, there exists a positive integer l such that

$$\mathfrak{g}_i^l u_j \subseteq \widetilde{R}_i$$

for all j. It follows that

$$\mathfrak{g}_i^l (\widetilde{R}_{i+1} : \mathfrak{a})_S \subseteq \widetilde{R}_{i+1}$$

and

$$\mathfrak{g}_i^l \subseteq \big(\widetilde{R}_{i+1} : (\widetilde{R}_{i+1} : \mathfrak{a})_S\big)_S = \mathfrak{h}_{i+1}.$$

Taking radicals on both sides gives us

$$\mathfrak{g}_i \subseteq \sqrt{\mathfrak{h}_{i+1}} = \mathfrak{g}_{i+1}.$$

We now show that $\mathfrak{g} = \bigcup_i \mathfrak{g}_i$ is the finite generation ideal of $\widetilde{R}$. If $f \in \mathfrak{g} \setminus \{0\}$, then $f \in \mathfrak{g}_i$ for some i. We have

$$\widetilde{R} = \big(\widetilde{R}_i : \mathfrak{g}_i^\infty\big)_S \subseteq (\widetilde{R}_i)_f,$$

because $f \in \mathfrak{g}_i$. It follows that

$$\widetilde{R}_f = (\widetilde{R}_i)_f$$

is finitely generated.

Conversely, suppose that $\widetilde{R}_f$ is finitely generated for some $f \in \widetilde{R} \setminus \{0\}$. Say, $\widetilde{R}_f$ is generated over K by $h_1, h_2, \ldots, h_r \in \widetilde{R}$ and $1/f$. For some i, we have $f, h_1, h_2, \ldots, h_r \in \widetilde{R}_i$. Therefore, we get

$$\widetilde{R} \subseteq \big(K[f, h_1, \ldots, h_r] : f^\infty\big)_S \subseteq (\widetilde{R}_i)_f.$$

Since $(\widetilde{R}_i : \mathfrak{a})_S$ is a finitely generated $\widetilde{R}_i$-module, there exists a positive integer l such that

$$f^l (\widetilde{R}_i : \mathfrak{a})_S \subseteq \widetilde{R}_i.$$

We see that

$$f^l \in \left(\widetilde{R}_i : (\widetilde{R}_i : \mathfrak{a})_S\right)_S = \mathfrak{h}_i$$

and $f \in \mathfrak{g}_i$. □

Using Lemma 2.11, it is now possible to find generators of the finite generation ideal of the ring $(R : \mathfrak{a}^\infty)_S$. To do this, we modify Algorithm 2.6 as follows.

Algorithm 2.12. An algorithm for finding generators of the finite generation ideal of an algebra of the form $(R : \mathfrak{a}^\infty)_S$ where $S = K[x_1, \ldots, x_n]/I$ is a finitely generated domain over a field K, R is a finitely generated subalgebra of S and $\mathfrak{a}$ is an ideal of R.

Input: Polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ such that R is generated by $f_1 + I, \ldots, f_r + I$, and a finite set $\mathcal{A} \subset K[y_1, y_2, \ldots, y_r]$ such that the (nonzero) ideal $\mathfrak{a} \subseteq R$ is generated by $g(f_1, \ldots, f_r) + I$, $g \in \mathcal{A}$.

Output: A (possible infinite) sequence $h_1, h_2, h_3, \ldots$ of elements in $K[x_1, \ldots, x_n]$ such that $h_1 + I, h_2 + I, \ldots$ generate the finite generation ideal $\mathfrak{g}$ of $(R : \mathfrak{a}^\infty)_S$.

(1) $F := \emptyset$
(2) $\mathcal{H} := \{f_1, \ldots, f_r\}$
(3) `while` $\mathcal{H} \neq \emptyset$ `do`
(4) $F := F \cup \mathcal{H}$.
(5) `output` generators of $\widetilde{\mathfrak{g}} := \sqrt{(\widetilde{R} : (\widetilde{R} : \mathfrak{a})_S)_S}$ where $\widetilde{R}$ is the K-algebra generated by all $f + I$, $f \in F$, and $\mathfrak{a}$ is the ideal in $\widetilde{R}$ generated by all $g(f_1, \ldots, f_r) + I$, $g \in \mathcal{A}$.
(6) Let $\mathcal{H}$ be the output of Algorithm 2.5 for the computation of $(\widetilde{R} : \mathfrak{a})_S$.
(7) `enddo`

The algorithm terminates if and only if $(R : \mathfrak{a}^\infty)_S$ is finitely generated. In that case $\mathfrak{g}$ is the whole ring $(R : \mathfrak{a}^\infty)_S$. So the interesting case is when the algorithm does not terminate. One should add a termination criterion in step (3), i.e., replace step (3) by `while` $\mathcal{H} \neq \emptyset$ `and not` [TERMINATION CRITERION] `do`, where [TERMINATION CRITERION] is some criterion. For example, one could allow at most k iterations of the loop (3)–(7) where k is a parameter given in the input. Another example of a possible termination criterion will be given in Algorithm 2.21.

To compute generators of $\widetilde{\mathfrak{g}}$ in step (5), one proceeds as follows. We compute generators of $(\widetilde{R} : \mathfrak{a})_S$ using Algorithm 2.5. Let

$$\mathfrak{h} := \left(\widetilde{R} : (\widetilde{R} : \mathfrak{a})_S\right)_S.$$

Choose a nonzero element $f \in \mathfrak{a}$. Since $1 \in (\widetilde{R} : \mathfrak{a})_S$ we have

$$\mathfrak{h} = \left(\widetilde{R} : (\widetilde{R} : \mathfrak{a})_S\right)_{\widetilde{R}} = \left(f\widetilde{R} : f(\widetilde{R} : \mathfrak{a})_S\right)_{\widetilde{R}},$$

so generators of $\mathfrak{h}$ can be computed because it is again a colon ideal. Finally, generators of $\widetilde{\mathfrak{g}}$ can be computed using an algorithm to compute the radical ideal of $\mathfrak{h}$ (see for example Derksen and Kemper [3, Section 1.5], Matsumoto [18], or Kemper [14]). The correctness of the algorithm follows from Lemma 2.11.

2.3. Hilbert's fourteenth problem

Suppose that K is a field, L is a subfield of the rational function field $K(x_1, x_2, \ldots, x_n)$ containing K. Hilbert's 14th problem asks whether $L \cap K[x_1, \ldots, x_n]$ is finitely generated. Nagata gave a counterexample to this conjecture [20]. In fact, Nagata constructed an algebraic (nonreductive) group G and a linear action of G on the polynomial ring such that $K[x_1, \ldots, x_n]^G$ is not finitely generated. If we take $L = K(x_1, \ldots, x_n)^G$ as the invariant field, then $L \cap K[x_1, \ldots, x_n] = K[x_1, \ldots, x_n]^G$ is not finitely generated, so this gives indeed a counterexample to Hilbert's fourteenth problem. It is not clear whether it is decidable whether $L \cap K[x_1, \ldots, x_n]$ is finitely generated, or even whether $L \cap K[x_1, \ldots, x_n] = K$.

We will replace $K[x_1, \ldots, x_n]$ by an arbitrary finitely generated domain S over K. Let L be a subfield of the quotient field $Q(S)$ of S. We assume that L is generated as a field by elements of the ring S. In other words, L is the quotient field of some subalgebra $R \subseteq S$. We will present an algorithm to compute generators of the algebra $L \cap S = Q(R) \cap S$. This algorithm will terminate if this algebra is finitely generated. First we need the following constructive version of "generic freeness":

Theorem 2.13. *Suppose that S is a finitely generated domain over K, and R is a finitely generated subalgebra, then there exists an algorithm that finds a nonzero element $f \in R$ such that S_f is a free R_f-module, and R_f is a direct summand of S_f with a complement that is free as well.*

See Eisenbud [4, Theorem 14.4] for a proof of a more general version of Grothendieck's generic freeness lemma. Note that this lemma is often called "generic flatness," but that almost all proofs found in the literature prove the stronger "generic freeness" property. We will give here an algorithm to find the f in question. For a slightly different algorithm, see Vasconcelos [24, Theorem 2.6.1]. We assume that K is a field for which we have algorithms for a zero test and all arithmetic operations. Assume that $S = R[x_1, \ldots, x_r]/I$ where $x_1, \ldots, x_r$ are indeterminates.

Algorithm 2.14 *(Generic Freeness).*

Input: R, S, generators of I.
Output: An element $f \in R \setminus \{0\}$ such that S_f is a free R_f-module, and R_f is a direct summand in S_f which has a complement that is free as well.

(1) Let J be the ideal in $Q(R)[x_1, \ldots, x_r]$ generated by I (so it has the same set of generators as I).
(2) Compute a Gröbner basis $\mathcal{G}$ of J with respect to some monomial ordering. If necessary, multiply the polynomials from $\mathcal{G}$ by constants from $Q(R)$ to make their leading coefficients equal to 1.
(3) Compute $f \in R \setminus \{0\}$ such that $fh(x_1, \ldots, x_r) \in R[x_1, \ldots, x_r]$ for every $h(x_1, \ldots, x_r) \in \mathcal{G}$.

Proof of correctness of Algorithm 2.14. Let

$$\varphi : R[x_1, \ldots, x_r] \to S$$

be the homomorphism with kernel I that induces an isomorphism $R[x_1,\dots,x_r]/I \cong S$. Let M be the set of all monomials m such that m is not divisible by any leading monomial $\operatorname{lm}(h)$ with $h \in \mathcal{G}$. We claim that S_f is a free R_f-module with basis $\varphi(M)$.

Suppose that $h \in S_f$. There exists a positive integer l such that $f^l h \in S$. We can write $f^l h = u(x_1,\dots,x_r) + I$ where $u(x_1,\dots,x_r) \in R[x_1,\dots,x_r] \subseteq Q(R)[x_1,\dots,x_r]$. Let $v(x_1,\dots,x_r)$ be the normal form of $u(x_1,\dots,x_r)$ with respect to the Gröbner basis $\mathcal{G}$. Thus if

$$\mathcal{G} = \big\{h_1(x_1,\dots,x_r),\dots,h_s(x_1,\dots,x_r)\big\},$$

then there exist $a_1(x_1,\dots,x_r),\dots,a_s(x_1,\dots,x_r) \in Q(R)[x_1,\dots,x_r]$ such that

$$u(x_1,\dots,x_r) - v(x_1,\dots,x_r) = \sum_{i=1}^{s} a_i(x_1,\dots,x_r)h_i(x_1,\dots,x_r).$$

Note that $h_1(x_1,\dots,x_r),\dots,h_s(x_1,\dots,x_s) \in R_f[x_1,\dots,x_r]$. If $p(x_1,\dots,x_r) \in R_f[x_1,\dots,x_r]$ and $q(x_1,\dots,x_r)$ is obtained from $p(x_1,\dots,x_r)$ by a single reduction step modulo the Gröbner basis $\mathcal{G}$, then $q(x_1,\dots,x_r) \in R_f[x_1,\dots,x_r]$ as well. From this observation one can show using induction that

$$a_1(x_1,\dots,x_r),\dots,a_s(x_1,\dots,x_r), v(x_1,\dots,x_r) \in R_f[x_1,\dots,x_r].$$

Now we get $v(x_1,\dots,x_r) \in R_f M$, $\varphi(v(x_1,\dots,x_r)) = f^l h \in R_f\varphi(M)$ and $h \in R_f\varphi(M)$. This shows that $S_f = R_f\varphi(M)$, i.e., $\varphi(M)$ generates S_f as an R_f module. It is clear from Gröbner basis theory that $\varphi(M)$ is a linearly independent set over $Q(R)$. We conclude that S_f is a free R_f module with basis $\varphi(M)$. We can identify R_f with $R_f\varphi(1) = R_f \cdot 1 \subseteq S_f$, which is a direct summand because

$$S_f = R_f \cdot 1 \oplus R_f \cdot \varphi\big(M \setminus \{1\}\big). \qquad \square$$

Remark 2.15. Algorithm 2.14 is also correct in the case where R is not finitely generated. The only problem is that we cannot provide a way of computing the ideals I and J in this case. In fact, it is not even clear how to compute with elements from $Q(R)$ if R is not finitely generated. Nevertheless, the above proof of correctness of the algorithm does provide a proof of the generic freeness theorem even for R not finitely generated.

Algorithm 2.16 *(Intersection of a field and a finitely generated domain).*

Input: Generators and relations for a finitely generated domain S over K and generators of a finitely generated subalgebra R.

Output: Generators of the algebra $Q(R) \cap S$. The algorithm will terminate if $Q(R) \cap S$ is finitely generated. If $Q(R) \cap S$ is not finitely generated, then the algorithm will not terminate but the (infinite) output will still generate the algebra $Q(R) \cap S$.

(1) Use Algorithm 2.14 to compute $f \in R \setminus \{0\}$ such that R_f is a summand in the R_f-module S_f.
(2) Compute generators of $(R : f^\infty)_S$ using Algorithm 2.6.

Proof of correctness of Algorithm 2.16. We can write

$$S_f = R_f \oplus C$$

where C is an R_f-module. Let $\pi : S_f \to R_f$ be the projection onto R_f. So π is an R_f-module homomorphism such that $\pi(a) = a$ if and only if $a \in R_f$. Suppose that $s = a/b \in S_f$ with $a, b \in R_f$. Then we have $bs = a$ and $b\pi(s) = \pi(bs) = \pi(a) = a$. So we obtain $s = a/b = \pi(s) \in R_f$. This shows that $Q(R) \cap S_f = R_f$. It follows that

$$Q(R) \cap S \subseteq R_f \cap S = \left(R : f^\infty\right)_S,$$

so $Q(R) \cap S = (R : f^\infty)_S$ because the other inclusion is trivial. □

The following theorem is Proposition 4 in Chapter V of Nagata [22].

Theorem 2.17. *Suppose that R is a finitely generated normal domain over a field K, and L is a subfield of $Q(R)$ containing K. Then $R \cap L$ is isomorphic to the ring of regular functions on some quasi-affine variety U defined over K. In other words, there exists a finitely generated domain T over K and an ideal $\mathfrak{a}$ of T such that*

$$R \cap L = \left(T : \mathfrak{a}^\infty\right)_{Q(T)}.$$

Some extensions of this result can be found in Winkelmann [25]. Theorem 2.17 inspires us to ask the following questions.

Problem 2.18. Let R and L be as in Theorem 2.17. Find an algorithm to construct generators of T and $\mathfrak{a}$ where T and $\mathfrak{a}$ are as in Theorem 2.17.

Problem 2.19. Suppose that S is a finitely generated normal domain over K, R is a finitely generated normal subalgebra and $\mathfrak{a}$ is an ideal of R. Is the ring $(R : \mathfrak{a}^\infty)_S$ isomorphic to the ring of regular functions on some quasi-affine variety over K?

The following proposition gives a positive answer to Problem 2.19 under an additional hypothesis. We will later see that this hypothesis is satisfied in a situation which is of interest in invariant theory (see Algorithm 3.9).

Proposition 2.20. *Suppose that S, R, $\mathfrak{a}$ are as in Problem* 2.19. *Let $\mathfrak{g}$ be the finite generation ideal of $(R : \mathfrak{a}^\infty)_S$. Suppose that the affine variety corresponding to the ideal $\mathfrak{g}S$ has codimension $\geqslant 2$, in other words, all prime ideals containing $\mathfrak{g}S$ have height $\geqslant 2$. Then $(R : \mathfrak{a}^\infty)_S$ is isomorphic to the coordinate ring of an quasi-affine variety.*

Proof. The proposition follows from the correctness of the algorithm below. □

The following algorithm is a modification of Algorithm 2.12.

Algorithm 2.21. An algorithm for finding a finitely generated subalgebra $\widetilde{R} \subseteq S$ and an ideal $\widetilde{\mathfrak{g}}$ of $\widetilde{R}$ such that

$$\left(R : \mathfrak{a}^{\infty}\right)_S = \left(\widetilde{R} : \widetilde{\mathfrak{g}}^{\infty}\right)_{Q(\widetilde{R})},$$

where S is a finitely generated normal domain over K, R is a finitely generated subalgebra, and $\mathfrak{a}$ is an ideal of R, such that the affine variety corresponding to $\mathfrak{g}S$ has codimension at least 2, where $\mathfrak{g}$ is the finite generation ideal of $(R : \mathfrak{a}^{\infty})_S$.

Input: Polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ such that R is generated by $f_1 + I, \ldots, f_r + I \in K[x_1, \ldots, x_n]/I =: S$, and a finite set $\mathcal{A} \subset K[y_1, y_2, \ldots, y_r]$ such that the (nonzero) ideal $\mathfrak{a} \subseteq R$ is generated by $g(f_1, \ldots, f_r) + I$, $g \in \mathcal{A}$.

Output: Generators of a subalgebra $\widetilde{R}$ of S and generators of an ideal $\widetilde{\mathfrak{g}}$ of $\widetilde{R}$ such that

$$\left(R : \mathfrak{a}^{\infty}\right)_S = \left(\widetilde{R} : \widetilde{\mathfrak{g}}^{\infty}\right)_{Q(\widetilde{R})}$$

(1) Set $F := \emptyset$ and $\widetilde{\mathfrak{g}} := \{0\}$.
(2) $\mathcal{H} := \{f_1, \ldots, f_r\}$.
(3) `while` $\mathcal{H} \neq \emptyset$ `and [`$\widetilde{\mathfrak{g}}S$ has codimension < 2`] and` $\widetilde{\mathfrak{g}}S \neq S$ `do`
(4) $F := F \cup \mathcal{H}$.
(5) Compute generators of $\widetilde{\mathfrak{g}} := \sqrt{(\widetilde{R} : (\widetilde{R} : \mathfrak{a})_S)_S}$ where $\widetilde{R}$ is the K-algebra generated by all $f + I$, $f \in F$, and $\mathfrak{a}$ is the ideal in $\widetilde{R}$ generated by all $g(f_1, \ldots, f_r) + I$, $g \in \mathcal{A}$. The radical ideal is meant to be formed in $\widetilde{R}$.
(6) Let $\mathcal{H}$ be the output of Algorithm 2.5 for the computation of $(\widetilde{R} : \mathfrak{a})_S$.
(7) `enddo`
(8) Output generators of $\widetilde{R}$ and $\widetilde{\mathfrak{g}}$.

Remark. In step (3) of the algorithm, it is easy to determine the codimension of $\widetilde{\mathfrak{g}}S$, since by [4, Corollary 13.4], the codimension equals $\dim(S) - \dim(S/\widetilde{\mathfrak{g}}S)$. The dimension can be read off a Gröbner basis, see Gruel and Pfister [6, Corollary 7.5.5] or Derksen and Kemper [3, Section 1.2.5].

We also remark that the ideal $\widetilde{\mathfrak{g}}$ found by the algorithm is not necessarily the finite generation ideal.

Proof of correctness of Algorithm 2.21. Let $\widetilde{R}_i$ and $\mathfrak{g}_i$ be the algebra $\widetilde{R}$ and the ideal $\widetilde{\mathfrak{g}}$ in the ith iteration of loop (3)–(7). We have

$$\widetilde{R}_1 \subseteq \widetilde{R}_2 \subseteq \cdots$$

and

$$\mathfrak{g}_1 \subseteq \mathfrak{g}_2 \subseteq \cdots$$

such that $\mathfrak{g}_i$ is an ideal of $\widetilde{R}_i$ for all i.

Assume that the algorithm does not terminate and the loop (3)–(7) is repeated infinitely many times. Then $\bigcup_i \widetilde{R}_i = (R : \mathfrak{a}^{\infty})_S$ and $\mathfrak{g} = \bigcup_i \mathfrak{g}_i$ is the finite generation ideal of $(R : \mathfrak{a}^{\infty})_S$, because of the correctness of Algorithm 2.12. So we have

$$\mathfrak{g}_1 S \subseteq \mathfrak{g}_2 S \subseteq \mathfrak{g}_3 S \subseteq \cdots.$$

Since S is finitely generated over K, it is Noetherian. There exists an index k such that

$$\mathfrak{g}_k S = \mathfrak{g}_{k+1} S = \cdots = \bigcup_i \mathfrak{g}_i S = \mathfrak{g} S.$$

In particular, there exists an index k such that the affine variety corresponding to the ideal $\mathfrak{g}_k S$ has codimension $\geqslant 2$. Let k be minimal with this property. This implies that the algorithm terminates after the kth iteration of the loop (3)–(7), and the output is $\widetilde{R}_k$ and $\mathfrak{g}_k$.

Let X be the affine variety such that $S = K[X]$. If $f \in (S : \mathfrak{g}_k^\infty)_{Q(S)}$, then f is a rational function on X which is regular on all of X except for a closed subset of codimension $\geqslant 2$. Since X is normal, f is regular on X (see Eisenbud [4, below Corollary 11.4]), i.e., $f \in S$. This shows that

$$\left(S : \mathfrak{g}_k^\infty\right)_{Q(S)} = S.$$

So we have

$$\left(\widetilde{R}_k : \mathfrak{g}_k^\infty\right)_{Q(\widetilde{R}_k)} \subseteq \left(S : \mathfrak{g}_k^\infty\right)_{Q(S)} = S.$$

It follows that

$$\left(\widetilde{R}_k : \mathfrak{g}_k^\infty\right)_{Q(\widetilde{R}_k)} = \left(\widetilde{R}_k : \mathfrak{g}_k^\infty\right)_S = \left(R : \mathfrak{a}^\infty\right)_S,$$

where the last equality follows from (2.3) on page 2112. □

3. Invariant rings of algebraic groups

Suppose that K is an algebraically closed field (of arbitrary characteristic) and G is an algebraic group over K which acts regularly on an affine variety X. If G is not reductive, then $K[X]^G$ may not be finitely generated.

Problem 3.1. Find an algorithm which determines whether $K[X]^G$ is finitely generated.

Problem 3.2. Given that $K[X]^G$ is finitely generated, find an algorithm that computes a set of generators for $K[X]^G$.

If G is reductive, then $K[X]^G$ is known to be finitely generated and an algorithm was given in Section 1. If G is the additive group and the characteristic of the ground field is 0, then an algorithm was given by van den Essen [5]. Here we will give such an algorithm in arbitrary characteristic and where G can be any connected unipotent group.

Even if $K[X]^G$ is not finitely generated, there are still interesting questions to ask. Let $K(X)^G$ be the field of invariant rational functions on X. Then we have

$$K[X]^G = K[X] \cap K(X)^G.$$

If X is normal, then there exists a *quasi-affine* variety U over K such that

$$K[X]^G = K[U]$$

by Theorem 2.17.

Problem 3.3. Find an algorithm which constructs a quasi-affine variety U such that $K[X]^G = K[U]$.

We will give such an algorithm where G is a connected unipotent group and $K[X]$ is a unique factorization domain.

3.1. Invariants of the additive group

Suppose that $G = \mathbb{G}_a$ is the additive group acting regularly on an irreducible affine variety X over an algebraically closed field K. The coordinate ring $K[\mathbb{G}_a]$ can be identified with the polynomial ring $K[t]$. The group addition $\mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ corresponds to a ring homomorphism $K[t] \to K[t] \otimes K[t]$ defined by $t \mapsto t \otimes 1 + 1 \otimes t$. The action $\mathbb{G}_a \times X \to X$ corresponds to a ring homomorphism

$$\mu : K[X] \to K[\mathbb{G}_a \times X] \cong K[\mathbb{G}_a] \otimes K[X] \cong K[X][t].$$

Suppose that $f \in K[X]$. We can write

$$\mu(f) = f_0 + f_1 t + f_2 t^2 + \cdots + f_r t^r$$

with $f_0, \ldots, f_r \in K[X]$. If $\sigma \in \mathbb{G}_a$, then we have

$$\big((-\sigma) \cdot f\big)(x) = f(\sigma \cdot x) = \mu(f)(\sigma, x) = f_0(x) + f_1(x)\sigma + \cdots + f_r(x)\sigma^r,$$

so

$$\big((-\sigma) \cdot f\big) = f_0 + f_1\sigma + \cdots + f_r\sigma^r.$$

In particular we have

$$f = 0 \cdot f = f_0. \tag{3.1}$$

We have

$$\begin{aligned}(\tau - \sigma) \cdot f &= f_0 + f_1(\sigma - \tau) + \cdots + f_r(\sigma - \tau)^r \\ &= (\tau) \cdot \big((-\sigma) \cdot f\big) = (\tau \cdot f_0) + (\tau \cdot f_1)\sigma + \cdots + (\tau \cdot f_r)\sigma^r \end{aligned} \tag{3.2}$$

for all $\sigma, \tau \in \mathbb{G}_a \cong K$. Comparing the coefficients of σ^r shows that $\tau \cdot f_r = f_r$ for all $\tau \in \mathbb{G}_a$. This implies that $f_r \in K[X]^{\mathbb{G}_a}$. We may extend μ to be defined for all $f = g/h$ with $g \in K[X]$ and $h \in K[X]^{\mathbb{G}_a}$ by setting $\mu(f) = \mu(g)/h$. Then (3.2) still holds.

If the action of $\mathbb{G}_a$ is trivial, then of course $K[X]^{\mathbb{G}_a} = K[X]$. So let us assume that $\mathbb{G}_a$ acts nontrivially. Then there exists an $f \in K[X]$ such that $\mu(f) \neq f$. This element f will be chosen once and fixed for the rest of Section 3.1. We can write

$$F(t) := \mu(f) = f_0 + f_1 t + \cdots + f_{r-1} t^{r-1} + f_r t^r, \quad t \in \mathbb{G}_a,$$

with $r > 0$ and $f_r \neq 0$.

3.1.1. Characteristic 0 case

If K has characteristic 0, then an algorithm was given by van den Essen for computing generators of $K[X]^{\mathbb{G}_a}$. This algorithm terminates if $K[X]^{\mathbb{G}_a}$ is finitely generated. We will sketch the idea behind this algorithm. We set $s = f_{r-1}/(rf_r)$. From the coefficient of σ^{r-1} in (3.2), it follows that $\tau \cdot f_{r-1} = f_{r-1} - rf_r\tau$ and $\tau \cdot s = s - \tau$ for all $\tau \in \mathbb{G}_a$.

Lemma 3.4. *If $h \in K[X]_{f_r}$, then $\mu(h)\,|_{t=-s} \in K[X]_{f_r}^{\mathbb{G}_a}$.*

Proof. Set

$$H(t) := \mu(h) = h_0 + h_1 t + \cdots + h_l t^l$$

with $h_i \in K[X]_{f_r}$. From (3.2) it follows that

$$H(t-\tau) = h_0 + h_1(t-\tau) + \cdots + h_l(t-\tau)^l = (\tau \cdot h_0) + (\tau \cdot h_1)t + \cdots + (\tau \cdot h_l)t^l.$$

Using this for $t = -s + \tau$ gives us

$$\begin{aligned}\tau \cdot H(-s) &= (\tau \cdot h_0) + (\tau \cdot h_1)(-\tau \cdot s) + \cdots + (\tau \cdot h_l)(-\tau \cdot s)^l \\ &= (\tau \cdot h_0) + (\tau \cdot h_1)(-s+\tau) + \cdots + (\tau \cdot h_l)(-s+\tau)^l \\ &= H\big((-s+\tau) - \tau\big) = H(-s). \qquad \square\end{aligned}$$

Suppose that $K[X] = K[h_1, \ldots, h_m]$. Define

$$g_i = \mu(h_i)|_{t=-s} \in K[X]_{f_r}^{\mathbb{G}_a}$$

for $i = 1, 2, \ldots, m$. For every i, choose a natural number k_i such that $u_i := f_r^{k_i} g_i \in K[X]$.

Lemma 3.5. *We have*

$$K[X]_{f_r}^{\mathbb{G}_a} = K[g_1, \ldots, g_m, 1/f_r] = K[u_1, \ldots, u_m, 1/f_r].$$

Proof. Define the ring homomorphism $\gamma : K[X]_{f_r} \to K[X]_{f_r}^{\mathbb{G}_a}$ by $\gamma(g) = \mu(g)|_{t=-s}$. The homomorphism γ is surjective, because $\gamma(g) = \mu(g)|_{t=-s} = g$ for all $g \in K[X]_{f_r}^{\mathbb{G}_a}$. Since $K[X]_{f_r}$ is generated by $h_1, \ldots, h_m, 1/f_r$, $K[X]_{f_r}^{\mathbb{G}_a}$ is generated by $\gamma(h_1) = g_1, \ldots, \gamma(h_m) = g_m$, $\gamma(1/f_r) = 1/f_r$. $\square$

From Lemma 3.5 it follows that

$$K[X]^{\mathbb{G}_a} = \big(K[u_1, \ldots, u_m, f_r] : (f_r)^\infty\big)_{K[X]}.$$

Now generators of $K[X]^{\mathbb{G}_a}$ can be computed using Algorithm 2.6.

3.1.2. Arbitrary characteristic

Let us now no longer assume that K has characteristic 0. Van den Essen's algorithm may not work because r may be divisible by the characteristic of K for every possible choice of f, as the following example shows.

Example 3.6. Suppose that K is a field of characteristic 2 and define an action of the additive group on $K[x, y]$ by

$$\mu(x) = x + ty + t^2, \qquad \mu(y) = y.$$

For every element $f \in K[x, y]$, $\mu(f)$ is a polynomial of even degree in t.

Let X be an irreducible affine variety on which $\mathbb{G}_a$ acts regularly and nontrivially. Choose again $f \in K[X]$ such that $\mu(f) \neq f$. Again we can write

$$F(t) := \mu(f) = f_0 + f_1 t + \cdots + f_r t^r$$

with $r > 0$ and $f_r \neq 0$.

Lemma 3.7. *If $f_r = 1$, then $K[X]^{\mathbb{G}_a}$ is finitely generated.*

Proof. Suppose an invariant $g \in K[X]^{\mathbb{G}_a}$ is mapped to zero by the canonical map $\pi_f : K[X]^{\mathbb{G}_a} \to K[X]/(f)$. Then $g = hf$ with $h \in K[X]$, so

$$g = \mu(g) = \mu(h)F(t).$$

This implies $g = 0$, since otherwise the degrees of both sides of the above equation would differ. It follows that π_f induces an inclusion $K[X]^{\mathbb{G}_a} \to K[X]/(f)$.

We claim that $K[X]/(f)$ is integral over $K[X]^{\mathbb{G}_a}$. Suppose that $u \in K[X]$ and let $U(t) = \mu(u) \in K[X][t]$. Define $P(s) \in K[X][s]$ as the resultant

$$P(s) = \operatorname{Res}_t\big(U(t) - s, F(t)\big).$$

Since $F(t)$ is monic, it is clear from the definition of the resultant as the determinant of the Sylvester matrix (see Lang [17, IV, §8]) that either $P(s)$ or $-P(s)$ is monic as well.

Consider the action of $\mathbb{G}_a$ on $K[X][t, s]$, where $\mathbb{G}_a$ acts trivially on the variables t, s. If $\sigma \in \mathbb{G}_a$, then $\sigma \cdot U(t) = U(t - \sigma)$ by (3.2), and similarly $\sigma \cdot F(t) = F(t - \sigma)$. Therefore

$$\sigma \cdot P(s) = \operatorname{Res}_t\big(U(t - \sigma) - s, F(t - \sigma)\big) = \operatorname{Res}_t\big(U(t) - s, F(t)\big) = P(s)$$

using [17, Proposition 8.3]. It follows that all coefficients of $P(s)$ lie in $K[X]^{\mathbb{G}_a}$.

There exist polynomials $A(t, s), B(t, s) \in K[X][t, s]$ such that

$$P(s) = A(t, s)\big(U(t) - s\big) + B(t, s)F(t)$$

(see Lang [17, discussion before IV, Proposition 8.1]). If we substitute $t = 0$ and $s = u$, we get

$$P(u) = A(0, u)\big(U(0) - u\big) + B(0, u)F(0) = B(0, u)f,$$

where the last equality follows from (3.1). Therefore $P(u+(f))=0$ in $K[X]/(f)$, so $u+(f)$ is integral over $K[X]^{\mathbb{G}_a}$. The monic polynomial among $P(x), -P(x)$ is the *characteristic polynomial* of $u+(f)$ over $K[X]^{\mathbb{G}_a}$. Since u was arbitrary, $K[X]/(f)$ is integral over $K[X]^{\mathbb{G}_a}$.

Suppose that $h_1,\ldots,h_m$ are generators of $K[X]$. Let $R\subseteq K[X]^{\mathbb{G}_a}$ be the subalgebra generated by the coefficients of the characteristic polynomials of $h_i+(f)\in K[X]/(f)$ over $K[X]^{\mathbb{G}_a}$ for $i=1,2,\ldots,m$. We have $R\subseteq K[X]^{\mathbb{G}_a}\subseteq K[X]/(f)$ and R is clearly finitely generated. Since $K[X]/(f)$ is finitely generated and integral over R, we have that $K[X]/(f)$ is a finite R module. Since $K[X]^{\mathbb{G}_a}$ is a sub-R-module of $K[X]/(f)$, it is finitely generated as an R-module as well. But then $K[X]^{\mathbb{G}_a}$ is also finitely generated as an algebra. □

If $f_r=1$ and X is normal, then generators of $K[X]^{\mathbb{G}_a}$ can be computed as follows. By Lemma 1.11, $K[X]^{\mathbb{G}_a}$ is the integral closure of R in $K[X]$, where R is as in the proof of Lemma 3.7. This integral closure can be computed as described in Algorithm 1.12. If $f_r=1$ but X is not normal, Remark 1.14 may be applied to compute the integral closure.

Let us now consider the general case where f_r need not be 1 and X need not be normal (but is still assumed to be irreducible). Let $\mathfrak{s}\subseteq K[X]$ be the vanishing ideal of the singular locus. This ideal is nonzero and stable under the action of $\mathbb{G}_a$. Without loss of generality, we could have chosen $f\in\mathfrak{s}$ such that $\mu(f)\neq f$. We write

$$F(t)=\mu(f)=f_0+f_1t+\cdots+f_rt^r$$

with $f_r\neq 0$. Choose distinct $\lambda_0,\lambda_1,\ldots,\lambda_r\in K$. Using that the Vandermonde matrix is invertible, we see that $f_0,f_1,\ldots,f_r$ lie in the K-linear span of $F(\lambda_0),F(\lambda_1),\ldots,F(\lambda_r)$. We have $F(\lambda_0),\ldots,F(\lambda_r)\in\mathfrak{s}$ because $\mathfrak{s}$ is $\mathbb{G}_a$-stable. This implies that $f_r\in\mathfrak{s}$. So f_r vanishes on the set of singularities, and $K[X]_{f_r}$ is smooth. We have

$$\mu(f/f_r)=(f_0/f_r)+(f_1/f_r)t+\cdots+(f_{r-1}/f_r)t^{r-1}+t^r.$$

Using the previous discussion we can compute generators of $K[X]_{f_r}^{\mathbb{G}_a}$. Of course there is no need to choose f to lie in $\mathfrak{s}$ if we apply Remark 1.14 to compute the integral closure. Suppose that

$$K[X]_{f_r}^{\mathbb{G}_a}=K[g_1,\ldots,g_l].$$

For every i we can compute a nonnegative integer k_i such that $u_i:=f_r^{k_i}g_i\in K[X]$. We then have

$$K[X]^{\mathbb{G}_a}=\bigl(K[u_1,\ldots,u_l,f_r]:(f_r)^\infty\bigr)_{K[X]}.$$

Now generators of $K[X]^{\mathbb{G}_a}$ can be computed using Algorithm 2.6.

3.2. Invariants of connected unipotent groups

Suppose that X is an irreducible affine variety on which the additive group $\mathbb{G}_a$ acts regularly. We have already seen that there exists an algorithm that computes generators for a subalgebra $R\subseteq S:=K[X]$ and generators of an ideal $\mathfrak{a}$ such that $S^{\mathbb{G}_a}=(R:\mathfrak{a}^\infty)_S$. We now will deal with the more general case where a connected unipotent group N acts regularly on X. A unipotent

group N is nilpotent (see Humphreys [10, Corollary 17.5]) and therefore solvable. If moreover N is connected, then by [10, Theorem 19.3] there exists a descending chain of normal subgroups

$$N = N_k \supset N_{k-1} \supset N_{k-2} \supset \cdots \supset N_0 = (0)$$

such that each quotient N_i/N_{i-1} has dimension one. By [10, Theorem 15.3(c)], each quotient is again unipotent, and therefore it is isomorphic to the additive group $\mathbb{G}_a$ by [10, Theorem 20.5]. This allows us to give a recursive approach to the computation of generators of $K[X]^N$. The tricky part here is that $K[X]^{N_i}$ may not be finitely generated for some i, even if $K[X]^N$ is finitely generated.

Algorithm 3.8.

Input: The irreducible, affine variety X (given by its coordinate ring $S := K[X]$), the connected unipotent group N with its group structure (multiplication $N \times N \to N$ and inverse $N \to N$ and the identity element $e \in N$), the action $N \times X \to X$, and a descending chain of normal subgroups

$$N = N_k \supset N_{k-1} \supset \cdots \supset N_1 \supset N_0 = (0)$$

with explicit isomorphisms $N_i/N_{i-1} \cong \mathbb{G}_a$ for $i = 1, 2, \ldots, k$.

Output: A subalgebra $T \subseteq K[X]$ and an ideal $\mathfrak{d} \subseteq T$ such that $K[X]^N = (T : \mathfrak{d}^\infty)_{K[X]}$.

(1) If $N = (0)$ (and $k = 0$), then terminate with as output the algebra S and its ideal S.
(2) Find a finitely generated subalgebra $R \subseteq S := K[X]$ and a nonzero ideal $\mathfrak{a}$ such that $S^{N_1} = (R : \mathfrak{a}^\infty)_S$ as in Section 3.1. Say $R = K[f_1, \ldots, f_r]$ and $\mathfrak{a} = (h_1, \ldots, h_s)$.
(3) Let R' be the algebra generated by all $u \cdot f_i$ where $u \in N$ and $i = 1, 2, \ldots, r$.
(4) Let $\mathfrak{a}'$ be the ideal of R' generated by all $u \cdot h_j$ where $u \in N$ and $j = 1, 2, \ldots, s$.
(5) Invoke this algorithm with input R' and $N' := N/N_1$ to find a subalgebra $T \subseteq (R')^{N'}$ and an ideal $\mathfrak{c}$ of T such that $(T : \mathfrak{c}^\infty)_{R'} = (R')^{N'}$.
(6) Find a nonzero element a in $(\mathfrak{a}')^{N'} = \mathfrak{a}' \cap (R')^{N'}$. Replace T by $T[a]$ to ensure that $\mathfrak{a}' \cap T$ is not the zero ideal.
(7) Output the algebra T and the ideal $\mathfrak{d} := \mathfrak{c}(\mathfrak{a}' \cap T)$.

Before we prove the correctness of this algorithm, we explain some of the steps in more detail. In step (3), since N_1 is normal in N, S^{N_1} is stable under N and $R' \subseteq S^{N_1}$.

In step (6): Note that N' is unipotent and $\mathfrak{a}'$ is nonzero. We can find a nonzero finite dimensional subrepresentation $W \subseteq \mathfrak{a}'$ because N' acts regularly on the infinite dimensional vector space $\mathfrak{a}'$. But then $W^{N'}$ is nonzero. This shows that $(\mathfrak{a}')^{N'}$ is nonzero. A nonzero element in $(\mathfrak{a}')^{N'}$ can be found using linear algebra.

Proof of correctness of Algorithm 3.8. We need to show that

$$S^N = \left(T : \mathfrak{d}^\infty\right)_S.$$

We have

$$S^{N_1} = \left(R : \mathfrak{a}^\infty\right)_S.$$

We claim that we also have

$$S^{N_1} = \left(R' : (\mathfrak{a}')^\infty\right)_S.$$

Suppose that $f \in S^{N_1}$. Since N_1 is a normal subgroup, S^{N_1} is N-stable. Let W be the vector space spanned by all $u \cdot f$, $u \in N$. Then W is finite dimensional and contained in $S^{N_1} = (R : \mathfrak{a}^\infty)_S$. Then there exists a positive integer l such that

$$\mathfrak{a}^l W \subseteq R.$$

So in particular,

$$\mathfrak{a}^l \left(u^{-1} \cdot f\right) \subseteq R$$

for all $u \in N$. Applying u gives

$$(u \cdot \mathfrak{a})^l f \subseteq u \cdot R \subseteq R'.$$

Since $\mathfrak{a}'$ is finitely generated, there exist finitely many elements $u_1, \ldots, u_m$ such that $\mathfrak{a}'$ is generated by $u_i \cdot \mathfrak{a}$, $i = 1, 2, \ldots, m$.

Since

$$(\mathfrak{a}')^{lm} = (u_1 \cdot \mathfrak{a} + u_2 \cdot \mathfrak{a} + \cdots + u_m \cdot \mathfrak{a})^{lm} \subseteq u_1 \cdot \mathfrak{a}^l + \cdots + u_m \cdot \mathfrak{a}^l$$

we get

$$(\mathfrak{a}')^{lm} f \subseteq R'$$

and

$$f \in \left(R' : (\mathfrak{a}')^\infty\right)_S.$$

Conversely, if $f \in (R' : (\mathfrak{a}')^\infty)_S$, then f is invariant under N_1 because $R' \subseteq S^{N_1}$ and $\mathfrak{a}' \subseteq S^{N_1}$ is not equal to (0).

Next we will show that

$$S^N = \left(T : \mathfrak{d}^\infty\right)_S$$

where

$$\mathfrak{d} = \mathfrak{c}(\mathfrak{a}' \cap T).$$

Suppose that $f \in S^N$. Then $f \in S^{N_1} = (R' : (\mathfrak{a}')^\infty)_S$, so there exists a positive integer l such that

$$(\mathfrak{a}')^l f \subseteq R'.$$

It follows that

$$(\mathfrak{a}' \cap T)^l f \subseteq (R')^N = (R')^{N'}.$$

Since $\mathfrak{a}' \cap T$ is finitely generated, there exists a positive integer m such that

$$\mathfrak{c}^m (\mathfrak{a}' \cap T)^l f \subseteq T.$$

This shows that $\mathfrak{d}^n f \subseteq T$ for $n \geqslant \max\{l, m\}$ and therefore $f \in (T : \mathfrak{d}^\infty)_S$. It follows that

$$S^N \subseteq \big(T : \mathfrak{d}^\infty\big)_S.$$

The reverse inclusion

$$S^N \supseteq \big(T : \mathfrak{d}^\infty\big)_S$$

follows because $T, \mathfrak{d} \subseteq S^N$ and $\mathfrak{d} \neq (0)$. □

Finally we consider the case where N is a connected unipotent group acting regularly on an irreducible *factorial* variety X. In this case we can effectively find a quasi-affine variety U such that $K[X]^G = K[U]$.

Algorithm 3.9.

Input: The irreducible affine factorial variety X, a connected unipotent group N and a regular action $N \times X \to X$.

Output: A finitely generated subalgebra $\widetilde{R} \subseteq K[X]$ and an ideal $\mathfrak{g} \subseteq \widetilde{R}$ such that

$$K[X]^N = \big(\widetilde{R} : \mathfrak{g}^\infty\big)_{Q(\widetilde{R})}.$$

(1) Find a finitely generated subalgebra $R \subseteq K[X]$ and an ideal $\mathfrak{a}$ of R such that

$$K[X]^N = \big(R : \mathfrak{a}^\infty\big)_{K[X]}$$

using Algorithm 3.8.

(2) Apply Algorithm 2.21 to find $\widetilde{R}$ and $\widetilde{g}$ such that $(\widetilde{R} : \widetilde{\mathfrak{g}}^\infty)_{Q(\widetilde{R})} = K[X]^N$.

Proof of correctness of Algorithm 3.9. We need to show that Algorithm 2.21 applies here, i.e., we have to prove that the variety corresponding to $\mathfrak{g}K[X]$ is equal to $K[X]$ or has codimension $\geqslant 2$. Suppose not. We can write $\sqrt{\mathfrak{g}K[X]}$ as the intersection of finitely many distinct prime ideals. One of these prime ideals has height 1, say $\mathfrak{p}$ is such a prime ideal. Since N is connected, $\mathfrak{p}$ must be stable under N. Since $K[X]$ is factorial, $\mathfrak{p}$ is a principal ideal, say $\mathfrak{p} = (h)$. View $h(g \cdot x)$ as a regular function of $(g, x) \in N \times X$. Then $h(g \cdot x)$ is divisible by $h \in K[X]$, so we can write

$$h(g \cdot x) = u(g, x)h(x)$$

for some $u \in K[N \times X]$. It follows that

$$h(x) = h\big(g^{-1} g \cdot x\big) = u\big(g^{-1}, g \cdot x\big) h(g \cdot x) = u\big(g^{-1}, gx\big) u(g, x) h(x),$$

so $u(g^{-1}, gx)u(g, x) = 1$ and $u(g, x) \in K[N \times X]^\star$ is invertible. For fixed x, $u(g, x) \in K[N]^\star = K^\star$. If $h(x) \neq 0$, then we get $u(g, x) = u(e, x) = 1$. We conclude that $u = 1$ and h is invariant under N.

We have already seen that $K[X]^N$ is isomorphic to the ring of regular functions on some quasi-affine variety U. There exists a finitely generated subalgebra S of $K[X]^N$ and an ideal $\mathfrak{b}$ of S such that

$$K[X]^N = \big(S : \mathfrak{b}^\infty\big)_{Q(S)}.$$

Clearly $\mathfrak{b} \subset \mathfrak{g}$ since $K[X]^N_f$ is finitely generated for all $f \in \mathfrak{b}$. Therefore $\mathfrak{b} \subseteq \mathfrak{g}K[X] \subseteq hK[X]$. It follows that $h^{-1}\mathfrak{b} \subseteq K[X]$ and $h^{-1}\mathfrak{b} \subseteq K[X]^N$. This shows that $h^{-1} \in (S : \mathfrak{b}^\infty)_{Q(S)} = K[X]^N$. But $h^{-1} \notin K[X]$, so $h^{-1} \notin K[X]^N$. Contradiction.

We have shown that the variety corresponding to $\mathfrak{g}K[X]$ has codimension $\geqslant 2$. □

3.3. Invariants of arbitrary algebraic groups

If G is an arbitrary algebraic group, then there exists a connected unipotent normal subgroup N such that G/N is reductive. Suppose that G acts on an irreducible affine variety X. One approach to compute generators of $K[X]^G$ is by computing generators of $K[X]^N$ first. The problem of this is that $K[X]^N$ may not be finitely generated, even if $K[X]^G$ is finitely generated. If $K[X]^N$ is finitely generated, then Algorithm 3.8 can be used to compute a finitely generated subalgebra R of $K[X]^N$ and an ideal $\mathfrak{a}$ of R such that $K[X]^N = (R : \mathfrak{a}^\infty)_{K[X]}$. Then Algorithm 2.6 can be used to find generators of $K[X]^N$. Finally Algorithm 1.7 can be used to compute generators of $K[X]^G = (K[X]^N)^{G/N}$ because G/N is reductive.

Even if $K[X]^N$ is not finitely generated, we might be able to compute generators of $K[X]^G$. Suppose that we have found R and $\mathfrak{a}$ such that $K[X]^N = (R : \mathfrak{a}^\infty)_{K[X]}$ using Algorithm 3.8. Assume that $R = K[f_1, \ldots, f_r]$ and $\mathfrak{a} = (h_1, \ldots, h_s)$. We could try to copy the approach in Section 3.2. So let R' be the algebra generated by $\sigma \cdot f_i$ with $\sigma \in G$ and $i = 1, 2, \ldots, r$, and let $\mathfrak{a}'$ be the ideal generated by all $\sigma \cdot h_j$ with $\sigma \in G$ and $j = 1, 2, \ldots, s$. Similarly as in the proof of Algorithm 3.8 we can show that

$$K[X]^G = \big(R' : (\mathfrak{a}')^\infty\big)_{K[X]}.$$

If $(\mathfrak{a}')^{G/N}$ is not equal to the zero ideal, then one can show that

$$K[X]^G = \big((R')^{G/N} : \big((\mathfrak{a}')^{G/N}\big)^\infty\big)_{K[X]}. \tag{3.3}$$

Generators of $(R')^{G/N}$ can be computed using Algorithm 1.7. Generators of $(\mathfrak{a}')^{G/N} = \mathfrak{a}' \cap (R')^{G/N}$ can be computed by using the usual Gröbner basis techniques. Finally generators of $K[X]^G$ can be found using (3.3) and Algorithm 2.6. Of course this algorithm will not terminate, unless $K[X]^G$ is finitely generated.

So what can we do if $(\mathfrak{a}')^{G/N}$ is zero? Perhaps the choice of R' and $\mathfrak{a}'$ were unfortunate. Suppose that there exists an element $f \in K[X]^G$ such that $(K[X]^N)_f$ is finitely generated. Then

$f \in \mathfrak{g}$ where $\mathfrak{g}$ is the finite generation ideal of $K[X]^N$. Using Algorithm 2.12 we can construct subalgebras

$$\widetilde{R}_1 \subseteq \widetilde{R}_2 \subseteq \cdots$$

and ideals

$$\mathfrak{g}_1 \subseteq \mathfrak{g}_2 \subseteq \cdots$$

such that $\bigcup \widetilde{R}_i = K[X]^N$ and $\mathfrak{g} = \bigcup_i \mathfrak{g}_i$. So we have $f \in \mathfrak{g}_i$ for some i. We terminate Algorithm 2.12 at step i when $f \in \mathfrak{g}_i$. We have

$$K[X]^N = \left(R : \mathfrak{a}^\infty\right)_{K[X]} = \left(\widetilde{R}_i : \mathfrak{g}_i^\infty\right)_{K[X]}.$$

So we might as well replace R by $R = \widetilde{R}_i$ and $\mathfrak{a}$ by $\mathfrak{a} = \mathfrak{g}_i$. We then still have

$$K[X]^N = \left(R : \mathfrak{a}^\infty\right)_{K[X]}$$

but we also have $f \in \mathfrak{a}^{G/N}$, so $\mathfrak{a}^{G/N}$ is not the zero ideal. We can proceed to compute generators of the invariant ring $K[X]^G$ as discussed before.

We just saw that there exists an algorithm to compute generators of $K[X]^G$ if there exists a nonzero element $f \in K[X]^G$ such that $K[X]_f^N$ is finitely generated. This may not always be the case as the following example shows.

Example 3.10. Let H be the group and X be the representation in Nagata's counterexample to Hilbert's fourteenth problem (see Nagata [20]). Here V is a 32-dimensional representation and H is an algebraic group over the base field $K = \mathbb{C}$ and $K[X]^H$ is not finitely generated. Let N be the unipotent radical of H. Then N is a connected unipotent group, H/N is reductive, and $K[X]^N$ is not finitely generated, because otherwise $K[X]^H = (K[X]^N)^{H/N}$ would be finitely generated. Let $\mathcal{G}_m = \mathbb{C}^\star$ be the multiplicative group acting by scalar multiplication, and let $G = \mathcal{G}_m N$. Then N is the unipotent radical of G. Since $K[X]^G = K$, for every nonzero $f \in K[V]^G$ we have $K[X]_f^N = K[X]^N$ is not finitely generated.

Suppose that G is an algebraic group and X is an irreducible normal G-variety. Suppose that the quotient field $Q(K[X]^G)$ of the invariant ring $K[X]^G$ is equal to the field of invariant rational functions on X, denoted by $K(X)^G$. First we can find the transcendence degree of $K(X)^G : K$ as follows. Let $n = \dim X$ and let m be the dimension of a generic G-orbit in X. Then the transcendence degree of $K(X) : K(X)^G$ is m, and the transcendence degree of $K(X)^G : K$ is $n - m$. If we consider the morphism

$$\psi : G \times X \to X \times X$$

defined by

$$\psi(\sigma, x) = (x, \sigma \cdot x)$$

then the dimension of the closure of the image is $n + m$. Using Gröbner basis techniques one can compute the dimension of the Zariski closure of the image of ψ, and hence determine m.

Using linear algebra, one can compute a linear basis of invariants $f_1, f_2, \ldots \in K[X]^G$. Terminate this search for invariants if one finds among these invariants $n - m$ algebraically independent functions. Let us call them $h_1, \ldots, h_{n-m}$. Let L be the field generated by $h_1, \ldots, h_{n-m}$. Then $K(X)^G : L$ is an algebraic extension. Let R be the integral closure of $K[h_1, \ldots, h_{n-m}]$ in $K[X]$. Generators of R can be computed using Algorithm 1.12. We have $Q(R) = Q(K[X]^G)$. It follows that

$$K[X]^G = K(X)^G \cap K[X] = Q(R) \cap K[X].$$

So we can use Algorithm 2.16 to find generators of $K[X]^G$.

Acknowledgments

This work was initiated during a visit of the second author to the University of Michigan. The second author thanks the first one for his hospitality. Both authors thank Tobias Kamke for carefully reading the manuscript and pointing out some errors to us. We also thank Frank Grosshans for sending us his nice paper [7] and thereby bringing a result of [12] to our attention. Finally, we thank the anonymous referee for some very helpful comments.

References

[1] Nicolas Bourbaki, Algebra II, Elem. Math., Springer, 1989, Chapters 4–7.
[2] Harm Derksen, Computation of invariants for reductive groups, Adv. Math. 141 (1999) 366–384.
[3] Harm Derksen, Gregor Kemper, Computational Invariant Theory, Encyclopaedia Math. Sci., vol. 130, Springer-Verlag, Berlin, 2002.
[4] David Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995.
[5] Arno van den Essen, An algorithm to compute the invariant ring of a G_a-action on an affine variety, J. Symbolic Comput. 16 (1993) 551–555.
[6] Gert-Martin Greuel, Gerhard Pfister, A Singular Introduction to Commutative Algebra, Springer-Verlag, Berlin, 2002.
[7] Frank D. Grosshans, Vector invariants in arbitrary characteristic, Transform. Groups (2007), doi:10.1007/s00031-006-0046-z, in press.
[8] William J. Haboush, Reductive groups are geometrically reductive, Ann. of Math. 102 (1975) 67–83.
[9] Mitsuyasu Hashimoto, Computation of invariants for reductive groups, preprint, Nagoya University, 2002.
[10] James E. Humphreys, Linear Algebraic Groups, second ed., Springer-Verlag, Berlin, 1981.
[11] Theo de Jong, An algorithm for computing the integral closure, J. Symbolic Comput. 26 (1998) 273–277.
[12] Wilberd van der Kallen, Lectures on Frobenius Splittings and B-Modules, Published for the Tata Institute of Fundamental Research, Bombay, 1993, notes by S.P. Inamdar.
[13] Gregor Kemper, Calculating invariant rings of finite groups over arbitrary fields, J. Symbolic Comput. 21 (1996) 351–366.
[14] Gregor Kemper, The calculation of radical ideals in positive characteristic, J. Symbolic Comput. 34 (2002) 229–238.
[15] Gregor Kemper, Computing invariants of reductive groups in positive characteristic, Transform. Groups 8 (2003) 159–176.
[16] Martin Kreuzer, Lorenzo Robbiano, Computational Commutative Algebra 1, Springer-Verlag, Berlin, 2000.
[17] Serge Lang, Algebra, revised third ed., Grad. Texts in Math., vol. 211, Springer-Verlag, New York, 2002.
[18] Ryutaroh Matsumoto, Computing the radical of an ideal in positive characteristic, J. Symbolic Comput. 32 (2001) 263–271.
[19] David Mumford, John Fogarty, Frances Kirwan, Geometric Invariant Theory, third ed., Ergeb. Math. Grenzgeb., vol. 34, Springer-Verlag, Berlin, 1994.
[20] Masayoshi Nagata, On the 14th problem of Hilbert, Amer. J. Math. 81 (1959) 766–772.
[21] Masayoshi Nagata, Invariants of a group in an affine ring, J. Math. Kyoto Univ. 3 (1963) 369–377.
[22] Masayoshi Nagata, Lectures on the Fourteenth Problem of Hilbert, Tata Institute of Fundamental Research, Bombay, 1965.

[23] Vladimir L. Popov, On Hilbert's theorem on invariants, Dokl. Akad. Nauk SSSR 249 (1979), English translation: Soviet Math. Dokl. 20 (1979) 1318–1322.
[24] Wolmer V. Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Algorithms Comput. Math., vol. 2, Springer-Verlag, Berlin, 1998.
[25] Jörg Winkelmann, Invariant Rings and Quasiaffine Quotients, Math. Z. 244 (2003) 163–174.