The Computation of Invariant Fields and a Constructive Version of a Theorem by Rosenlicht

Gregor Kemper
Technische Universität München, Zentrum Mathematik - M11
Boltzmannstr. 3, 85 748 Garching, Germany
kemper@ma.tum.de

July 18, 2007

Abstract

Let G be an algebraic group acting on an irreducible variety X. We present an algorithm for computing the invariant field $k(X)^G$. Moreover, we give a constructive version of a theorem of Rosenlicht, which says that almost all orbits can be separated by rational invariants. More precisely, we give an algorithm for computing a non-empty open subset of X with a geometric quotient.

Introduction

One of the classical problems of invariant theory is the construction of generating sets for invariant rings. It is well-known that for a reductive group all invariant rings are finitely generated. It has taken a number of steps to convert the existence theorems of finite generating sets into actual algorithms. We refer to the book [5] and to the more recent papers [10] and [6] for details. A variant of this problem is the problem of constructing a generating set for the invariant field, i.e., the field of all rational invariants. It should come as no surprise that this problem turns out to be easier. Indeed, the paper [12] by Müller-Quade and Beth provides an algorithm for constructing a generating set of the invariant field of a linear algebraic group acting linearly on a finite-dimensional vector space V. The restriction to reductive groups no longer applies. The paper [9] by Hubert and Kogan contains, among other results, a variant of the algorithm that applies to the slightly more general situation where the action on V need not be linear and may, in fact, be rational. By considering so-called cross sections, the authors obtain an optimization of the algorithm. For finite groups, we have an algorithm, contained in the paper by Fleischmann et al. [7], which does not require any Gröbner basis techniques.

In this paper, the algorithm of Müller-Quade and Beth is generalized to the situation where G is an algebraic group acting on an irreducible variety X by a rational map. Neither G nor X are assumed to be affine. The proof of correctness of the algorithm is a simplification of the proof given in [12]. Being simpler, it applies to a more general situation. The algorithm allows iteration along a chain of subgroups of G. The second result of the paper is an algorithm which makes Rosenlicht's theorem constructive. For an action on an irreducible, affine variety, this algorithm finds a non-empty, open subset where all orbits are separated by rational invariants. If G is connected, we can iterate this algorithm and thus obtain a parametrization of all G-orbits by invariants with case distinctions.

The paper is organized as follows. In the first section, we consider the *Derksen ideal*, named after Derksen's algorithm [4], in a very general situation: We only assume that G is a group acting on a field K, fixing a subfield k over which K is finitely generated. We show that if $\mathcal{G}$ is a monic, reduced Gröbner basis of the Derksen ideal, then the coefficients of all polynomials in $\mathcal{G}$ generate the invariant field K^G. We also present an algorithm which tests a rational function for

invariance, and represents it in terms of the generators of K^G. This leaves the question of how the Derksen ideal can be computed. This question is addressed in Section 2. In that section, we consider the situation where G is an algebraic group acting on an irreducible variety X by a rational map. We present an algorithm for computing the Derksen ideal. The computational core of the algorithm is the calculation of an elimination ideal. In the final section, we consider an action of a linear algebraic group on an affine variety X. We give an algorithm that computes a non-empty, open subset $\widehat{X}$ of X such that all G-orbits in $\widehat{X}$ are separated by rational invariants defined on $\widehat{X}$. Optionally, the algorithm computes a geometric quotient. The proof of correctness is a modification of proofs of Rosenlicht's theorem known from the literature.

Acknowledgments. I thank Harm Derksen for fruitful conversations. Further thanks go to the anonymous referees and to Vladimir Popov for very valuable comments, which led to a major revision of the paper.

1 Invariant fields

Let K be a commutative ring with unity, and let $G \subseteq \mathrm{Aut}(K)$ be a group of automorphisms of K. We write K^G for the invariant ring. Fix elements $x_1, \ldots, x_n \in K$, and let $K[y_1, \ldots, y_n]$ the polynomial ring in n indeterminates. Then the *Derksen ideal* is defined as

$$D := \bigcap_{\sigma \in G} \langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n) \rangle_{K[y_1,\ldots,y_n]}, \tag{1.1}$$

in which the pointed brackets indicate generation as an ideal. We have a homomorphism

$$\varphi\colon K^G[y_1, \ldots, y_n] \to K,\ y_i \mapsto x_i$$

of K^G-algebras.

For the rest of Section 1, we assume that K is a field. Choose a monomial ordering ">" on $K[y_1, \ldots, y_n]$, and let $\mathcal{G}$ be a monic, reduced Gröbner basis of D w.r.t. ">". (Here *monic* means that all leading coefficients are 1.) By the following proposition, the relations of the x_i over K^G are given by $\mathcal{G}$.

Proposition 1.1. *In the above situation, $\mathcal{G}$ is a Gröbner basis of* $\ker(\varphi) \subseteq K^G[y_1, \ldots, y_n]$ *w.r.t. the monomial ordering ">".*

Proof. We apply the elements of G to polynomials in $K[y_1, \ldots, y_n]$ coefficient-wise. By definition, D is G-stable. Take $\sigma \in G$. Then $\sigma(\mathcal{G})$ is a reduced, monic Gröbner basis of $\sigma(D) = D$. By the uniqueness of reduced, monic Gröbner bases (see Becker and Weispfenning [1, Theorem 5.43]), it follows that $\sigma(\mathcal{G}) = \mathcal{G}$. Since applying σ preserves monomials and since all leading monomials of polynomials from $\mathcal{G}$ are distinct, G fixes $\mathcal{G}$ element-wise, so $\mathcal{G} \subseteq K^G[y_1, \ldots, y_n]$. Moreover, every $f \in \mathcal{G}$ lies in D, therefore also in $\langle y_1 - x_1, \ldots, y_n - x_n \rangle_{K[y_1,\ldots,y_n]}$. Thus substituting $y_i = x_i$ in f yields 0, so $\varphi(f) = 0$. So $\mathcal{G} \subseteq \ker(\varphi)$.

To complete the proof, take $g \in \ker(\varphi) \setminus \{0\}$. We need to show that the leading monomial $\mathrm{LM}(g)$ is divisible by the leading monomial of a polynomial from $\mathcal{G}$. From $\varphi(g) = 0$, it follows that $g \in \langle y_1 - x_1, \ldots, y_n - x_n \rangle_{K[y_1,\ldots,y_n]}$. Let $\sigma \in G$. Then

$$g = \sigma(g) \in \sigma\left(\langle y_1 - x_1, \ldots, y_n - x_n \rangle\right) = \langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n) \rangle,$$

so $g \in D$. Since $\mathcal{G}$ is a Gröbner basis of D, the leading monomial of g is divisible by some $\mathrm{LM}(f)$ with $f \in \mathcal{G}$. □

The next theorem contains an invariance test. For the definition of a normal form with respect to a Gröbner basis (or any set of polynomials) we refer the reader to Becker and Weispfenning [1, p. 196].

Theorem 1.2. *In the situation of Proposition 1.1, let* $f, g \in K^G[y_1, \ldots, y_n]$ *be polynomials with* $g(x_1, \ldots, x_n) \neq 0$*, and set* $a := \frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$*. Then*

$$a \in K^G \quad \Longleftrightarrow \quad \mathrm{NF}_{\mathcal{G}}(f) = a \cdot \mathrm{NF}_{\mathcal{G}}(g),$$

where $\mathrm{NF}_{\mathcal{G}}$ *denotes the normal form w.r.t.* $\mathcal{G}$*.*

Proof. Assume that $a \in K^G$. Then $f - ag$ lies in the domain of definition of φ, and $\varphi(f - ag) = 0$. By the K-linearity of the normal form map and by Proposition 1.1, we obtain

$$\mathrm{NF}_{\mathcal{G}}(f) - a \cdot \mathrm{NF}_{\mathcal{G}}(g) = \mathrm{NF}_{\mathcal{G}}(f - ag) = 0.$$

Conversely, assume $\mathrm{NF}_{\mathcal{G}}(f) - a \cdot \mathrm{NF}_{\mathcal{G}}(g) = 0$. Then, since $\mathcal{G}$ is a Gröbner basis of D, it follows that $f - ag \in D$. So for every $\sigma \in G$, we have $f - ag \in \langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n)\rangle_{K[y_1,\ldots,y_n]}$, so $f(\sigma(x_1), \ldots, \sigma(x_n)) - a \cdot g(\sigma(x_1), \ldots, \sigma(x_n)) = 0$. This equation, together with the fact that σ is an automorphism of K^G-algebras, implies $\sigma(f(x_1, \ldots, x_n)) - a \cdot \sigma(g(x_1, \ldots, x_n)) = 0$, so

$$a = \frac{\sigma(f(x_1, \ldots, x_n))}{\sigma(g(x_1, \ldots, x_n))} = \sigma(a).$$

Thus $a \in K^G$. □

Let K, G, $x_1, \ldots, x_n$ and $\mathcal{G}$ be as above. Moreover, let $k \subseteq K^G$ be a subfield of the invariant field. We write $k(x_1, \ldots, x_n) \subseteq K$ for the field extension of k generated by the x_i, which need not be G-stable. For example, $k(x_1, \ldots, x_n)$ may be the invariant field of a subgroup $H \subseteq G$. Let $L \subseteq K$ be the field extension of k generated by all coefficients of polynomials from $\mathcal{G}$.

Corollary 1.3. *In the above situation, assume that* $K^G \subseteq k(x_1, \ldots, x_n)$*. Then*

$$K^G = L.$$

Proof. Proposition 1.1 implies that $\mathcal{G}$ is a subset of $K^G[y_1, \ldots, y_n]$, so $L \subseteq K^G$.

For the reverse inclusion, take $a \in K^G$. Since $K^G \subseteq k(x_1, \ldots, x_n)$, we can write $a = \frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ with $f, g \in k[y_1, \ldots, y_n]$. By Theorem 1.2, we obtain

$$\mathrm{NF}_{\mathcal{G}}(f) = a \cdot \mathrm{NF}_{\mathcal{G}}(g).$$

Observe that both $\mathrm{NF}_{\mathcal{G}}(f)$ and $\mathrm{NF}_{\mathcal{G}}(g)$ lie in $L[y_1, \ldots, y_n]$, since f, g, and all elements of $\mathcal{G}$ lie in $L[y_1, \ldots, y_n]$. We have $\mathrm{NF}_{\mathcal{G}}(g) \neq 0$, since otherwise $g(x_1, \ldots, x_n)$ would be 0 by Proposition 1.1. Hence

$$a = \frac{\mathrm{NF}_{\mathcal{G}}(f)}{\mathrm{NF}_{\mathcal{G}}(g)} \in L(y_1, \ldots, y_n) \cap K = L.$$

□

We conclude this section by giving an algorithm for representing an invariant $a \in K^G$ as a rational function (with coefficients in the field k) in the generators of L. Assume that we have the monic, reduced Gröbner basis $\mathcal{G}$ of the Derksen ideal. We can choose $a_1, \ldots, a_r \in K^G$ such that all coefficients of polynomials in $\mathcal{G}$ can be written as polynomials in $a_1, \ldots, a_r$ with coefficients in k. For example, every coefficient a of a polynomial in $\mathcal{G}$ with $a \notin k$ may be taken as one of the a_i. More formally, with indeterminates $A_1, \ldots, A_r$ and ψ: $k[A_1, \ldots, A_r, y_1, \ldots, y_n] \to K^G[y_1, \ldots, y_n]$ being the homomorphism of $k[y_1, \ldots, y_n]$-algebras sending A_i to a_i, we have a set $\mathcal{G}_0 \subseteq k[A_1, \ldots, A_r, y_1, \ldots, y_n]$ consisting of preimages of the polynomials in $\mathcal{G}$ under ψ.

Algorithm 1.4 (Invariance test and expression by generating invariants)**.**

Input: Invariants $a_1, \ldots, a_r \in K^G$ and a preimage $\mathcal{G}_0$ of $\mathcal{G}$ as above; moreover, polynomials $f, g \in k[y_1, \ldots, y_n]$.

Output: "False" if $g(x_1,\dots,x_n)=0$ or $a:=\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}\notin K^G$; but if $a\in K^G$, a rational function $h\in k(A_1,\dots,A_r)$ with $a=h(a_1,\dots,a_r)$.

(1) Regarding f, g, and the polynomials from $\mathcal{G}_0$ as elements of $k(A_1,\dots,A_r)[y_1,\dots,y_n]$, compute normal forms f_0 and g_0 of f and g w.r.t. $\mathcal{G}_0$ and the monomial ordering ">". (Both f_0 and g_0 will lie in $k[A_1,\dots,A_r,y_1,\dots,y_n]$ since the leading coefficients of all polynomials in $\mathcal{G}_0$ are 1.)

(2) Set $\widetilde{f}:=\psi(f_0)$ and $\widetilde{g}:=\psi(g_0)$.

(3) If $\widetilde{g}=0$ or $\widetilde{f}-a\widetilde{g}\neq 0$, return "False".

(4) Choose a monomial m in the y-variables such that m appears with non-zero coefficient in $\widetilde{g}$.

(5) Let f_m and g_m be the coefficients of the monomial m in f_0 and g_0, respectively, and set $h:=\frac{f_m}{g_m}$.

Proof of correctness of Algorithm 1.4. It is clear that $\widetilde{f}$ and $\widetilde{g}$ are the (uniquely defined) normal forms of f and g w.r.t. $\mathcal{G}$. By Theorem 1.2, a is invariant if and only if $\widetilde{f}-a\widetilde{g}=0$, in which case $a=\widetilde{f}/\widetilde{g}$. Thus for the monomial m chosen in step 4, we have

$$a=\frac{\operatorname{coeff}_m(\widetilde{f})}{\operatorname{coeff}_m(\widetilde{g})}=\frac{\psi\left(\operatorname{coeff}_m(f_0)\right)}{\psi\left(\operatorname{coeff}_m(g_0)\right)}.$$

This concludes the proof. □

2 Algebraic actions

If G is a finite group acting on a field K, it is clear how the Derksen ideal D, as given by (1.1), can be calculated. For infinite groups, this is far less clear, and will depend on the specific situation. In this section we will look at the algebraic situation. We will give an algorithm for calculating a Gröbner basis of D. Together with Corollary 1.3, this will yield an algorithm for computing the invariant field.

Let us consider the following situation. Assume k to be an algebraically closed field. (Without this assumption, everything should also work in the scheme-theoretic sense.) Let X be an irreducible variety and G an algebraic group, both over k (neither X nor G need be affine). Moreover, let $U\subseteq G\times X$ be an open subset and $\rho\colon U\to X$ a morphism such that

(i) for all $\sigma\in G$, the set $U_\sigma:=\{x\in X\mid(\sigma,x)\in U\}$ is non-empty.

So $\rho_\sigma\colon U_\sigma\to X,\ x\mapsto\rho(\sigma,x)$ defines a rational map from X to itself. We also assume that

(ii) all ρ_σ are birational maps, and assigning ρ_σ to σ yields a homomorphism from G into the group of birational maps from X to itself.

Thus G acts on the function field $K:=k(X)$ by $\sigma(f):=f\circ\rho_\sigma^{-1}$. This situation coincides with the definition of a rational action by Popov and Vinberg [13, Section 1.1]. Clearly the "standard" situation, in which G is a linear algebraic group and X is an (affine) G-variety, is included in our situation. G is a finite union of open, affine subsets. These subsets can be dealt with computationally. So let $G'\subseteq G$ be an open, affine subset (which need not be a subgroup). We thus have an embedding $G'\subseteq k^m$ into some affine m-space. Let $I:=\operatorname{Id}(G')\subseteq k[t_1,\dots,t_m]$ be the vanishing ideal. The following lemma describes the action on $K=k(X)$.

Lemma 2.1. *In the above situation, let $f\in K$ be a rational function on X. Then there exists a rational function $F\in K(t_1,\dots,t_m)$ in m indeterminates that is defined at all $\sigma=(\xi_1,\dots,\xi_m)\in G'\subseteq k^m$, such that*

$$\sigma^{-1}(f)=F(\xi_1,\dots,\xi_m).$$

The lemma seems almost obvious, but the proof is nevertheless somewhat tedious.

Proof. There exists a non-empty, open subset $V \subseteq X$ such that $f\colon V \to k$ is a regular function. It is convenient to consider a non-empty, open, affine subset X' of X. The set $\rho^{-1}(V) \cap (G' \times X') \subseteq G \times X$ is open, and $f \circ \rho$ is a regular function on this set. X' is embedded in some affine space k^n, so there exists a rational function $F_0 \in k(t_1, \ldots, t_m, x_1, \ldots, x_n)$ which is defined on $\rho^{-1}(V) \cap (G' \times X') \subseteq k^m \times k^n$, and

$$f(\rho(\sigma, x)) = F_0(\sigma, x) \tag{2.1}$$

for all $(\sigma, x) \in \rho^{-1}(V) \cap (G' \times X')$. With $J := \mathrm{Id}(X') \subseteq k[x_1, \ldots, x_n]$ we have $K = k(X') = \mathrm{Quot}\,(k[x_1, \ldots, x_n]/J)$. The denominator of F_0 does not lie in $\langle J \rangle_{k[t_1,\ldots,t_m,x_1,\ldots,x_n]}$, so we can form the reduction

$$F := F_0(t_1, \ldots, t_m, x_1 + J, \ldots, x_n + J) \in K(t_1, \ldots, t_m)$$

modulo J. Let $\sigma = (\xi_1, \ldots, \xi_m) \in G'$. To prove the lemma, it suffices to show that F is defined at $(\xi_1, \ldots, \xi_m)$ and that there exists a non-empty, open subset $W \subseteq X$ on which $f \circ \rho_\sigma$ and $F(\xi_1, \ldots, \xi_m)$ coincide. Since ρ_σ is birational, its image $\rho_\sigma(U_\sigma)$ contains a non-empty, open subset of X. Therefore $\rho_\sigma(U_\sigma) \cap V$ is also non-empty, and thus the same is true for $\rho_\sigma^{-1}(V)$ and for $W := \rho_\sigma^{-1}(V) \cap X'$. Take $x \in W$. Equation (2.1) implies that F is defined at (σ, x) and

$$F(\xi_1, \ldots, \xi_m, x) = f(\rho(\sigma, x)) = (f \circ \rho_\sigma)(x).$$

This completes the proof. □

We will now assume that the affine subset $G' \subseteq G$ is dense. Being a disjoint union of its irreducible components, every algebraic group has a dense, affine subset. The following theorem gives a way to compute the Derksen ideal. Combining the theorem with Corollary 1.3 provides an algorithm for computing K^G. I thank one of the referees for bringing up the idea of using a dense affine subset of G.

Theorem 2.2. *Let G be an algebraic group acting rationally on an affine variety X, as described above. Let $G' \subseteq G$ be a dense, affine subset defined as an affine variety by an ideal $I \subseteq k[t_1, \ldots, t_m]$. Let $x_1, \ldots, x_n \in K := k(X)$, so*

$$\sigma^{-1}(x_i) = F_i(\underline{\xi})/H(\underline{\xi}) \quad \text{for} \quad \sigma = (\xi_1, \ldots, \xi_m) = (\underline{\xi}) \in G'$$

with $F_1, \ldots, F_n, H \in K[t_1, \ldots, t_m]$ as in Lemma 2.1. Take additional indeterminates $y_1, \ldots, y_n$ and z, and form the ideal

$$J := \Big\langle I \cup \{Hy_1 - F_1, \ldots, Hy_n - F_n\} \cup \{zH - 1\} \Big\rangle_{K[t_1,\ldots,t_{m_i},z,y_1,\ldots,y_n]}.$$

Then the Derksen ideal is given by

$$D := \bigcap_{\sigma \in G} \langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n) \rangle_{K[y_1,\ldots,y_n]} = J \cap K[y_1, \ldots, y_n].$$

Proof. Set

$$D' := \bigcap_{\sigma \in G'} \langle y_1 - \sigma(x_1), \ldots, y_n - \sigma(x_n) \rangle_{K[y_1,\ldots,y_n]}.$$

We first show that

$$J \cap K[y_1, \ldots, y_n] = D' \tag{2.2}$$

To show that $J \cap K[y_1, \ldots, y_n] \subseteq D'$, let $f \in J \cap K[y_1, \ldots, y_n]$. We can write

$$f = \sum_{j=1}^{r} g_j h_j + \sum_{j=1}^{n} f_j \cdot (Hy_j - F_j) + f_0 \cdot (zH - 1) \tag{2.3}$$

with $g_j, f_j \in K[t_1,\dots,t_m,z,y_1,\dots,y_n]$ and $h_j \in I$. Take $\sigma = (\xi_1,\dots,\xi_m) \in G'$. Since f only depends on $y_1,\dots,y_n$, we can substitute arbitrary values for z and the t_j in f. We will substitute $t_j = \xi_j$ and $z = H(\sigma)^{-1}$. Furthermore, we substitute $y_j = F_j(\sigma)/H(\sigma)$ and, using (2.3), obtain

$$f\left(F_1(\sigma)/H(\sigma),\dots,F_n(\sigma)/H(\sigma)\right) = 0.$$

Moreover, we have

$$f - f\left(F_1(\sigma)/H(\sigma),\dots,F_n(\sigma)/H(\sigma)\right) \in \left\langle y_1 - F_1(\sigma)/H(\sigma),\dots,y_n - F_n(\sigma)/H(\sigma)\right\rangle.$$

(This holds for any $f \in K[y_1,\dots,y_n]$.) Therefore $f \in \langle y_1 - F_{i,1}(\sigma)/H_i(\sigma),\dots, y_n - F_{i,n}(\sigma)/H_i(\sigma)\rangle_{K[y_1,\dots,y_n]}$. Since this holds for all $\sigma \in G'$, $f \in D'$ follows.

Conversely, let $f \in D'$. Let d be the maximal total degree of a monomial (in the y_j) occurring in f. By Lemma 2.3 below, we have

$$H^d \cdot f\,(F_1/H,\dots,F_n/H) - H^d \cdot f \in J. \tag{2.4}$$

Set $g := H^d \cdot f\,(F_1/H,\dots,F_n/H) \in K[t_1,\dots,t_m]$. For all $\sigma \in G'$ we have

$$g(\sigma) = H(\sigma)^d \cdot f\left(F_1(\sigma)/H(\sigma),\dots,F_i(\sigma)/H(\sigma)\right) = 0$$

since $f \in D'$. There exist $a_1,\dots,a_s \in K$ which are linearly independent over k such that g can be written as $g = \sum_{j=1}^{s} a_j g_j$ with $g_j \in k[t_1,\dots,t_m]$. For all $\sigma \in G'$ we have

$$0 = g(\sigma) = \sum_{j=1}^{s} g_j(\sigma)\cdot a_j,$$

which implies $g_j(\sigma) = 0$ for all j. Thus $g_j \in I$, so $g \in J$. With (2.4) we obtain $H^d \cdot f \in J$. Moreover,

$$z^d H^d - 1 = (zH-1)\cdot\sum_{j=0}^{d-1}(zH)^j \in J,$$

so $f \in J$. It follows that $f \in J \cap K[y_1,\dots,y_n]$. Thus (2.2) is proved.

Next we show that $D' = D$. Clearly $D \subseteq D'$. Conversely, take $f \in D'$ and consider the set

$$G_f := \left\{\sigma \in G \mid f \in \langle y_1 - \sigma(x_1),\dots,y_n - \sigma(x_n)\rangle_{K[y_1,\dots,y_n]}\right\} = \{\sigma \in G \mid f\,(\sigma(x_1),\dots,\sigma(x_n)) = 0\}.$$

Then $G' \subseteq G_f$, and it follows from Lemma 2.1 that the intersection of G_f with an affine subset of G is closed in that subset. By the denseness of G', every open, affine subset of G is contained in G_f, so $G_f = G$. This implies $f \in D$. □

The following lemma was used in the proof of Theorem 2.2.

Lemma 2.3. *Let R be an integral domain, $f \in R[y_1,\dots,y_n]$ a polynomial, and take d to be a non-negative integer that is bigger than or equal to the total degree of every monomial occurring in f. Moreover, let $H, F_1,\dots,F_n \in R$. Then*

$$H^d \cdot f\,(F_1/H,\dots,F_n/H) - H^d \cdot f \in \langle Hy_1 - F_1,\dots,Hy_n - F_n\rangle_{R[y_1,\dots,y_n]}.$$

Proof. By R-linearity, it suffices to prove the lemma for the case that f is a monomial. We may also assume $d = \deg(f)$. We proceed by induction on d. For $d = 0$, there is nothing to show. If $d > 0$ we can write $f = y_i \cdot \widetilde{f}$ with $\deg(\widetilde{f}) = d-1$. Then

$$H^d \cdot f\,(F_1/H,\dots,F_n/H) - H^d \cdot f = F_i \cdot \left(H^{d-1}\widetilde{f}\,(F_1/H,\dots,F_n/H) - H^{d-1}\cdot\widetilde{f}\right) + (F_i - Hy_i)\cdot H^{d-1}\widetilde{f}.$$

Both summands lie in $\langle Hy_1 - F_1,\dots,Hy_n - F_n\rangle$, the first by induction and the second by definition. □

Remark 2.4. (a) Theorem 2.2 carries over to the case that K is an arbitrary commutative ring containing the field k as a subring. We only need to assume that $H(\xi_1, \ldots, \xi_m)$ is invertible in K for each $(\xi_1, \ldots, \xi_m) \in G'$. The proof of Theorem 2.2 carries over word by word to the more general case. For example, K can be the ring of regular functions on an affine variety on which G acts by a morphism.

(b) The ideal D appearing in Theorem 2.2, with K being a polynomial ring, is precisely the ideal that plays a central role in Derksen's algorithm [4]. This is why we chose to call it the *Derksen ideal*.

(c) It is also possible to formulate Theorem 2.2 without assuming that we have a dense, affine subset $G' \subseteq G$. Instead, one covers G with affine subsets and forms the union of the Derksen ideals of these subsets. ◁

Since the computation of $K \cap k[y_1, \ldots, y_n]$ can be done algorithmically (this is an elimination ideal), we obtain an algorithm for computing invariant fields. This generalizes the algorithm first given by Müller-Quade and Beth [12].

Example 2.5. The purpose of this example is to illustrate our algorithm. In particular, we will illustrate the use of a subgroup which is not normal. We consider the diagonal action of $G := \mathrm{PGL}_2(k)$ on $X := \left(\mathbb{P}^1(k)\right)^4$ with k a field of characteristic 0. We first compute the invariants of the Borel subgroup

$$H := \{\sigma_{a,b} = K^* \cdot \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in k, a \neq 0\} \subset G.$$

The function field $K := k(X)$ is generated by four algebraically independent elements x_i, defined by

$$x_i(P_1, \ldots, P_4) = \frac{\text{first homogeneous coordinate of } P_i}{\text{second homogeneous coordinate of } P_i} \quad \text{for} \quad (P_1, \ldots, P_4) \in \left(\mathbb{P}_1(k)\right)^4,$$

for $\sigma_{a,b} \in H$ we have $\sigma_{a,b}^{-1}(x_i) = ax_i + b$, so the action is given by the polynomials $F_i = t_1 x_i + t_2$. The ideal J from Theorem 2.2 is

$$J = \langle \{t_1 t_3 - 1\} \cup \{y_i - t_1 x_i - t_2 \mid i = 1, \ldots, 4\} \rangle_{K[t_1, t_2, t_3, y_1, y_2, y_3, y_4]}.$$

Using Magma (Bosma et al. [2]), we compute a monic, reduced Gröbner basis $\mathcal{G}$ of the elimination ideal $J \cap K[y_1, \ldots, y_4]$, which is

$$\mathcal{G} = \left\{ y_1 - \frac{x_1 - x_4}{x_3 - x_4} y_3 + \frac{x_1 - x_3}{x_3 - x_4} y_4, y_2 - \frac{x_2 - x_4}{x_3 - x_4} y_3 + \frac{x_2 - x_3}{x_3 - x_4} y_4 \right\}$$

This yields

$$K^H = k\left(f_1 := \frac{x_1 - x_4}{x_3 - x_4}, f_2 := \frac{x_2 - x_4}{x_3 - x_4} \right),$$

since the other coefficients appearing in polynomials of $\mathcal{G}$ can be expressed as rational functions in f_1 and f_2.

In the next step we use Theorem 2.2 and Corollary 1.3 again to calculate K^G from K^H. Notice that K^H is not G-stable, but $K^G \subseteq K^H$. A dense, affine subset of G is given by

$$G' := \{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \cdot \sigma_{a,b} \mid a, b, c \in k, a \neq 0 \}.$$

For $\tau \in G'$ with parameters a, b, c, we obtain

$$\tau^{-1}(f_1) = \frac{(x_1 - x_4)(cx_3 + 1)}{(x_3 - x_4)(cx_1 + 1)} \quad \text{and} \quad \tau^{-1}(f_2) = \frac{(x_2 - x_4)(cx_3 + 1)}{(x_3 - x_4)(cx_2 + 1)}.$$

Thus the "new" ideal J is

$$J := \langle (x_3-x_4)(tx_1+1)y_1 - (x_1-x_4)(tx_3+1), \\ (x_3-x_4)(tx_2+1)y_2 - (x_2-x_4)(tx_3+1), z(tx_1+1)(tx_3+1)-1 \rangle_{K[t,z,y_1,y_2]}.$$

The elimination ideal $J \cap k[y_1,y_2]$ is calculated by using Magma and has the reduced Gröbner basis

$$\mathcal{G}' = \left\{ y_1y_2 - \frac{(x_1-x_3)(x_2-x_4)}{(x_1-x_2)(x_3-x_4)}y_1 + \frac{(x_1-x_4)(x_2-x_3)}{(x_1-x_2)(x_3-x_4)}y_2 \right\}.$$

We pick out two coefficients, and notice that their difference is 1, hence K^G is generated by

$$g = \frac{(x_1-x_2)(x_3-x_4)}{(x_1-x_3)(x_2-x_4)}$$

This is the function which assigns to a tuple $(P_1,\dots,P_4) \in \big(\mathbb{P}^1(k)\big)^4$ the cross-ratio of the P_i. Thus we get the well-known and classical result that the projective invariants of four points on a projective line are generated by the cross-ratio.

The total computing time for this example was about 0.1 seconds.

Example 2.6. We run the algorithm on the example given by Daigle and Freudenburg [3]. This is the smallest example known to date of an action with a non-finitely generated invariant ring. The additive group acts on five variables x_i by

$$x_1 \mapsto x_1, \quad x_2 \mapsto x_2 + tx_1^3, \quad x_3 \mapsto x_3 + tx_2 + \frac{t^2}{2}x_1^3,$$
$$x_4 \mapsto x_4 + tx_3 + \frac{t^2}{2}x_2 + \frac{t^3}{6}x_1^3, \quad \text{and} \quad x_5 \mapsto x_5 + tx_1^2.$$

It is straightforward to set up the ideal $J \subseteq k(x_1,\dots,x_5)[t,y_1,\dots,y_5]$ from Theorem 2.2 and to compute the elimination ideal $D = J \cap k(x_1,\dots,x_5)[y_1,\dots,y_5]$. In fact, a Gröbner basis of J with respect to the lexicographical monomial ordering with $t > y_1 > \cdots > y_5$ can even be computed by hand, and a Gröbner basis of D can be extracted. Gathering coefficients, we obtain

$$k(x_1,\dots,x_5)^{G_a} = k(x_1, x_1x_5 - x_2, 2x_2x_5 - 2x_1^2x_3 - x_1x_5^2, 6x_3x_5x_1^2 + x_1x_5^3 - 3x_2x_5^2 - 6x_1^4x_4).$$

In particular, the invariant field has the simplest possible structure: it is purely transcendental.

3 The theorem of Rosenlicht

In this section we consider an action of a linear algebraic group G on an irreducible, affine variety X. As above, all varieties will be over an algebraically closed field k. We will use the term *geometric quotient* in the sense of Definition 4.1 in Popov and Vinberg [13]. In particular, if $f_1,\dots,f_r \in k[X]^G$ define a geometric quotient $X \to Y$, then $k[X]^G = k[f_1,\dots,f_r]$.

It will be convenient to use the following abbreviation. If $S \subseteq X$ is a subset of an affine variety, then a non-empty subset $U \subseteq S$ will be called a p.o.s. of S if it has the form $U = \{x \in \overline{S} \mid g(x) \neq 0\}$ with $g \in k[X]$ and $\overline{S}$ being the Zariski closure. (Of course the letters come from "principal open subset", since a p.o.s. is a principal open subset of $\overline{S}$.) Every p.o.s. is an affine variety. In the following we will make use of Algorithm 1.1 in [11]. This algorithm computes a p.o.s. U of the image $f(X)$ of a morphism $f\colon X \to Y$ of non-empty affine varieties, with the additional property that all $y \in U$ have the same fibre dimension $\dim\big(f^{-1}(y)\big)$. Let Y be embedded in k^n. Then the algorithm also yields a reduced Gröbner basis of the vanishing ideal $J \subseteq k[y_1,\dots,y_n]$ of $f(X)$ with respect to an arbitrarily chosen monomial ordering.

The following algorithm makes the theorem of Rosenlicht constructive.

Algorithm 3.1 (Computation of an open subset with a geometric quotient)**.**

Input: A linear algebraic group G and an irreducible, affine variety X, embedded in some k^n, with an action given by a morphism $G \times X \to X$.

Output: A non-empty, G-stable, open subset $\widehat{X} \subseteq X$, and invariants $f_1, \ldots, f_r \in k[\widehat{X}]^G$ which separate all G-orbits in $\widehat{X}$. With $Y \subseteq k^r$ the variety defined by the relation ideal of the f_i, the algorithm can also achieve that the map $\widehat{X} \to Y$ given by the f_i is a geometric quotient.

(1) Consider the map

$$\varphi\colon G \times X \to X \times X,\ (\sigma, x) \mapsto (x, \sigma(x))\,.$$

Use Algorithm 1.1 in [11] to compute a p.o.s. U of the image $\mathcal{D} := \mathrm{im}(\varphi) \subseteq X \times X$. Let $\mathcal{B} \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ be the Gröbner basis of the vanishing ideal of $\mathcal{D}$ returned by the algorithm, where a lexicographical monomial ordering with $y_i > x_j$ for all i, j was chosen (or any monomial ordering for which every y_i is bigger than every power of an x_j).

(2) Let $\mathrm{pr}_1 : X \times X \to X$ be the first projection. Use Algorithm 1.1 in [11] again to compute a p.o.s. X' of $\mathrm{pr}_1(U) \subseteq X$.

(3) With G acting on the second factor of $X \times X$, set

$$B := \Big(\overline{\mathcal{D}} \setminus \bigcup_{\sigma \in G} \sigma(U)\Big) \cap (X' \times X')$$

and compute a p.o.s. X'' of $X' \setminus \mathrm{pr}_1(B) \subseteq X$. See Remark 3.2 for details.

(4) Set $\mathcal{G}_0 := \mathcal{B} \setminus k[x_1, \ldots, x_n]$. View elements f from $\mathcal{G}_0$ as polynomials in $y_1, \ldots, y_n$ with coefficients in $k[x_1, \ldots, x_n]$ and let $\mathrm{LC}_y(f) \in k[x_1, \ldots, x_n]$ be the leading coefficient. Compute a non-zero common multiple p of all $\mathrm{LC}_y(f)$, $f \in \mathcal{G}_0$. Let $X^{(3)} \subseteq X''$ be the subset of points where p does not vanish.

(5) Now view the elements of $\mathcal{G}_0$ as polynomials with coefficients in the rational function field $k(x_1, \ldots, x_n)$. Then $\mathcal{G}_0$ is a Gröbner basis. Convert this into a monic, reduced Gröbner basis $\mathcal{G}$. (This only involves divisions by divisors of p.) Let $f_1, \ldots, f_r \in k(x_1, \ldots, x_n)$ be the coefficients appearing in the polynomials from $\mathcal{G}$. The f_i are defined on $X^{(3)}$, and are elements of the invariant field $k(X)^G$.

(6) This step is optional and can be omitted if only orbit-separation but no geometric quotient is desired. Use Algorithm 1.1 in [11] to compute a p.o.s. Y of $\pi(X^{(3)})$ with $\pi\colon X^{(3)} \to k^r$ the morphism given by the f_i. Make Y smaller by excluding the non-normal locus (or, perhaps more practically, the singular locus) of $\overline{Y}$. If $Y = \{y \in \overline{Y} \mid q(y) \neq 0\}$, include $f_{r+1} := q(f_1, \ldots, f_r)^{-1}$ into the list of f_i's. Let $X^{(4)} \subseteq X^{(3)}$ be the subset of points where $q(f_1, \ldots, f_r)$ does not vanish.

(7) With $i = 4$ or $i = 3$ depending on whether step 6 was taken or not, compute

$$\widehat{X} := \bigcup_{\sigma \in G} \sigma(X^{(i)}).$$

See Remark 3.2 how this union can be computed.

Remark 3.2. In steps 3 and 7 of the algorithm, it is required that the union of all $\sigma(V)$ of a p.o.s. V of some G-variety Z is computed. In both cases, V is a p.o.s. of a closed G-stable subset of Z (namely, $\overline{\mathcal{D}}$ or X). So the computation of the union amounts to computing the ideal generated by all $\sigma(f)$, $\sigma \in G$, for an $f \in k[Z]$. If G is given by an ideal $I_G \subseteq k[t_1, \ldots, t_m]$, then we have $F \in k[Z][t_1, \ldots, t_m]$ such that the G-images of f are given as in Lemma 2.1. Let $\mathcal{G}_G \subseteq k[t_1, \ldots, t_m]$ be a Gröbner basis of I_G w.r.t. some monomial ordering. Write the normal form of F as

$$\mathrm{NF}_{\mathcal{G}_G}(F) = \sum_{i=1}^{l} g_i \cdot m_i$$

with $g_i \in k[Z]$ and $m_i \in k[t_1, \ldots, t_m]$ monomials. Then it is not hard to show that $g_1, \ldots, g_l$ span the same k-space as all $\sigma(f)$. So the same is true for the ideals spanned by both sets. This is how the unions in steps 3 and 7 can be computed.

In step 3, the set B (which may be empty) is then explicitly obtained as a principal open subset of the closed set $\overline{\mathcal{D}} \setminus \bigcup \sigma(U)$, and $\overline{\mathrm{pr}_1(B)} \subset X$ is given by an elimination ideal. Computing X'' amounts to finding an element in this elimination ideal which does not lie in the vanishing ideal of X. It is shown in the proof of correctness of Algorithm 3.1 that $\overline{\mathrm{pr}_1(B)}$ is properly contained in X. ◁

We now prove the correctness of Algorithm 3.1. The main ideas of the proof are drawn from the proofs of Theorem 2.3 in Popov and Vinberg [13] and Satz 2.2 in Springer [14]. The new elements are the usage of Gröbner bases and the circumstance that the various subsets $X^{(i)}$ need not be G-stable. (This is essential for the effectiveness of the computations, since the $X^{(i)}$ can be chosen to be p.o.s. and therefore affine varieties.)

Proof of correctness of Algorithm 3.1. We use the notation from the algorithm. For $(x, y) \in \mathcal{D}$, we have $\varphi^{-1}(x, y) \cong G_x$ (the point-stabilizer). Since Algorithm 1.1 from [11] yields a p.o.s. with constant fibre dimension, G_x has constant dimension on X', so the orbit dimension is also constant:

$$\dim\left(G(x)\right) = d \quad \text{for all} \quad x \in X'. \tag{3.1}$$

The irreducible components of $G \times X'$ have the form $\left(\sigma G^0\right) \times X'$ with $\sigma \in G$ and G^0 the unit component. By (3.1), all fibres of φ restricted to such a component have dimension $\dim(G) - d$, so by a theorem of Chevalley (see Hartshorne [8, Exercise 3.22(c)]), we obtain

$$\dim\left(\overline{\varphi\left(\left(\sigma G^0\right) \times X'\right)}\right) = \dim\left(\left(\sigma G^0\right) \times X'\right) - (\dim(G) - d) = \dim(X) + d.$$

Therefore

$$\dim\left(\overline{\mathcal{D}}\right) = \dim(X) + d. \tag{3.2}$$

Consider the set

$$G(B) := \left(\overline{\mathcal{D}} \setminus \bigcup_{\sigma \in G} \sigma(U)\right) \cap \left(X' \times \bigcup_{\sigma \in G} \sigma\left(X'\right)\right),$$

which contains B. U has non-empty intersection with at least one irreducible component of $\overline{\mathcal{D}}$. Since the irreducible components have the form $\overline{\varphi\left(\left(\sigma G^0\right) \times X\right)}$, the union $\bigcup_{\sigma \in G} \sigma(U)$ intersects all of them and is therefore dense in $\overline{\mathcal{D}}$. With (3.2), it follows that

$$\dim\left(\overline{G(B)}\right) < \dim\left(\overline{\mathcal{D}}\right) = \dim(X) + d. \tag{3.3}$$

Every irreducible component C of $G(B)$ is G^0-stable, so for $(x, y) \in C$, the orbit $G^0(y)$ is included in the fibre $C \cap \mathrm{pr}_1^{-1}(x)$. Since $y \in \sigma(X')$ for some $\sigma \in G$, it follows by (3.1) that the fibre dimension is at least d. So invoking Chevalley's theorem again and using (3.3) yields

$$\dim\left(\overline{\mathrm{pr}_1(C)}\right) \leqslant \dim(C) - d < \dim(X).$$

Therefore $\overline{\mathrm{pr}_1\left(G(B)\right)}$ and also $\overline{\mathrm{pr}_1(B)}$ are proper subsets of X. So X'' as in step 3 of the algorithm can be constructed. By construction, we have

$$\left(X'' \times X''\right) \cap \overline{\mathcal{D}} \subseteq \mathcal{D}. \tag{3.4}$$

By construction, $\mathcal{G}$ and $\mathcal{G}_0$ generate the same ideals in $k[x_1, \ldots, x_n, y_1, \ldots, y_n, 1/p]$. Viewed as subsets of $k[X^{(3)}][y_1, \ldots, y_n]$ (or of the larger ring $k(X)[y_1, \ldots, y_n]$), $\mathcal{G}$ and $\mathcal{B}$ then generate the same ideal. Since $\mathcal{B}$ is the vanishing ideal of $\overline{\mathcal{D}}$, which is stable under the action of G on the first component, the invariance of the f_i follows from the uniqueness of monic, reduced Gröbner bases. We also obtain

$$\mathrm{Var}_{X^{(3)} \times X}(\mathcal{G}) = \mathrm{Var}_{X^{(3)} \times X}(\mathcal{B}) = \left(X^{(3)} \times X\right) \cap \overline{\mathcal{D}}.$$

This also holds with $X^{(3)}$ replaced by the smaller set $X^{(4)}$ from step 6. In the following equation, applying $(\sigma,\tau)\in G\times G$ means that σ acts on the first component and τ on the second. So with $i=3$ or $i=4$, depending on whether step 6 is performed, we obtain

$$\begin{aligned}\mathrm{Var}_{\widehat{X}\times\widehat{X}}(\mathcal{G}) &= \bigcup_{\sigma\in G}\mathrm{Var}_{\sigma(X^{(i)})\times\widehat{X}}(\mathcal{G}) = \bigcup_{\sigma\in G}(\sigma,\mathrm{id})\left(\mathrm{Var}_{X^{(i)}\times\widehat{X}}(\mathcal{G})\right) = \\ &= \bigcup_{\sigma\in G}(\sigma,\mathrm{id})\left(\left(X^{(i)}\times\widehat{X}\right)\cap\overline{\mathcal{D}}\right) = \bigcup_{\sigma,\tau\in G}(\sigma,\tau)\left(\left(X^{(i)}\times X^{(i)}\right)\cap\overline{\mathcal{D}}\right) = \\ &= \bigcup_{\sigma,\tau\in G}(\sigma,\tau)\left(\left(X^{(i)}\times X^{(i)}\right)\cap\mathcal{D}\right) = \left(\widehat{X}\times\widehat{X}\right)\cap\mathcal{D},\end{aligned}$$

where (3.4) was used in the second last equality. Therefore two points $x,y\in\widehat{X}$ lie in the same G-orbit if and only of $F(x,y)=0$ for all $F\in\mathcal{G}$. This implies that the f_i separate all G-orbits in $\widehat{X}$.

Finally, let us turn our attention to step (6). Since $k[f_1,\ldots,f_r]$ is a subring of $k[X^{(3)}]$, the image closure of π, which is $\overline{Y}$, is the variety defined by the relation ideal of $f_1,\ldots,f_r$. Adding f_{r+1} changes the relation ideal in such a way that the corresponding variety is isomorphic to Y, and substituting $X^{(3)}$ by $X^{(4)}$ assures that $\pi(X^{(4)})=Y$. The invariance of the f_i implies that $\pi(\widehat{X})=Y$. So we have a surjective morphism onto a normal variety with G-orbits as fibres. By Theorem 4.2 from Popov and Vinberg [13], $\widehat{X}\to Y$ is a geometric quotient. □

If G is connected, then G acts on all irreducible components of $X\setminus\widehat{X}$. So we can apply Algorithm 3.1 iteratively, and will end up with a description of all G-orbits on X by means of invariants, with case distinctions given by polynomials.

References

[1] Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Springer-Verlag, Berlin, Heidelberg, New York 1993.

[2] Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comput. **24** (1997), 235–265.

[3] Daniel Daigle, Gene Freudenburg, *A Counterexample to Hilbert's Fourteenth Problem in Dimension* 5, J. Algebra **221** (1999), 528–535.

[4] Harm Derksen, *Computation of Invariants for Reductive Groups*, Adv. Math. **141** (1999), 366–384.

[5] Harm Derksen, Gregor Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, Heidelberg, New York 2002.

[6] Harm Derksen, Gregor Kemper, *Computing Invariants of Algebraic Group Actions in Arbitrary Characteristic*, preprint, University of Michigan and Technische Universität München, 2007, `http://arxiv.org/abs/0704.2594`.

[7] Peter Fleischmann, Gregor Kemper, Chris Woodcock, *Homomorphisms, localizations and a new algorithm to construct onvariant rings of finite groups*, J. Algebra **309** (2007), 497–517.

[8] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, Heidelberg, Berlin 1977.

[9] Evelyne Hubert, Irina A. Kogan, *Rational Invariants of an Algebraic Groups Action*, J. Symb. Comput. **42** (2007), 203–217.

[10] Gregor Kemper, *Computing Invariants of Reductive Groups in Positive Characteristic*, Transformation Groups **8** (2003), 159–176.

[11] Gregor Kemper, *Morphisms and Constructible Sets: Making Two Theorems of Chevalley Constructive*, preprint, Technische Universität München, 2007, `http://www-m11.ma.tum.de/~kemper/publications.html`.

[12] Jörn Müller-Quade, Thomas Beth, *Calculating Generators for Invariant Fields of Linear Algebraic Groups*, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Honolulu, HI, 1999)*, Lecture Notes in Comput. Sci. **1719**, pp. 392–403, Springer, Berlin 1999.

[13] Vladimir L. Popov, Ernest B. Vinberg, *Invariant Theory*, in: N. N. Parshin, I. R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer-Verlag, Berlin, Heidelberg 1994.

[14] Tonny A. Springer, *Aktionen reduktiver Gruppen auf Varietäten*, in: Hanspeter Kraft, Peter Slodowy, Tonny A. Springer, eds., *Algebraische Transformationsgruppen und Invariantentheorie, DMV Seminar* **13**, Birkhäuser, Basel 1987.