AN ALGORITHM TO COMPUTE THE INVARIANT RING OF A $G_a$-ACTION ON AN AFFINE VARIETY

by

Arno van den Essen

Report 9202
January 1992
DEPARTMENT OF MATHEMATICS
CATHOLIC UNIVERSITY
Toernooiveld
6525 ED Nijmegen
The Netherlands
AN ALGORITHM TO COMPUTE THE INVARIANT RING OF
A $\mathbb{G}_a$-ACTION ON AN AFFINE VARIETY

Arno van den Essen
Department of Mathematics, Catholic University Nijmegen,
Nijmegen, The Netherlands

To my mother on her 75th birthday

ABSTRACT
We describe an algorithm which computes the invariants of all $\mathbb{G}_a$-actions on affine varieties, in case the invariant ring is finitely generated.
The algorithm is based on a study of the kernel of a locally nilpotent derivation and some algorithms from the theory of Gröbner bases.

§0. INTRODUCTION
Let $k$ be a field of characteristic zero and $A$ a commutative $k$-algebra of finite type. Then every action of the additive group $\mathbb{G}_a$ on $\text{Spec} A$ is given by a locally nilpotent derivation $D$ on $A$. The element $t \in \mathbb{G}_a$ operates on $A$ by the automorphism $\exp(tD)$ ($= \sum_{k=0}^{\infty} \frac{1}{k!} D^k$) and the invariant ring of this $\mathbb{G}_a$-action i.e. the set of all $a$ in $A$ such that $\exp(tD)(a) = a$ for all $t \in k$, is equal to $\ker(D, A) = \{ a \in A \mid D(a) = 0 \}$ (cf. [5]).
In general it is not known if this invariant ring, which is a $k$-algebra, is finitely generated over $k$ (if $A$ is a polynomial ring a counterexample in this case would give a new counterexample to Hilbert 14, cf. [4]). However in several special cases the finiteness of the invariant ring is known, for example every linear action of $\mathbb{G}_a$ on $\mathbb{A}^n$ has a finitely
generated ring of invariants (this is a result of Weitzenböck, [8]) and also all $G_a$-actions on normal affine varieties of dimension $\leq 3$ have a finitely generated invariant ring (this result is due to Zariski, [9]).

In 1989 Lin Tan in [7] gave an algorithm to compute the invariant ring of the so-called basic $G_a$-actions on $\mathbb{A}^n$ (in which case the finiteness of the invariant ring is known).

In this paper we give an algorithm, inspired by Lin Tan’s algorithm, which computes the invariant ring of a $G_a$-action on an affine variety, in case the invariant ring is finitely generated. We will use the fact that this invariant ring is equal to the kernel of the corresponding locally nilpotent derivation on $A$. Therefore this paper is completely devoted to give an algorithm which describes the generators of the kernel of a locally nilpotent derivation $D$ on an affine $k$-algebra $A$ without zero-divisors, in case the kernel is finitely generated over $k$. It is worthy to note that in a recent preprint [2], H. Derksen has given an example of a (non-locally nilpotent) derivation on a polynomial ring in 32 variables, which kernel is not finitely generated over $k$. The contents of the paper are arranged as follows: in §1 we give explicit generators for the kernel of $D$ in case there exists an element $a$ in $A$ satisfying $D(a) = 1$. In §2 we define an ascending chain of finitely generated $k$-subalgebras $R_0 \subseteq R_1 \subseteq \ldots$ of $R := \ker D$, with the property that $R = R_r$ for some $r \in \mathbb{N}$. In §3 we show how to compute the $k$-subalgebras $R_j$ and how to decide for which $j$ we have $R = R_j$. Main ingredients in these computations are two algorithms, described in §4. They are based on methods from the theory of Gröbner bases. One of the algorithms, the membership algorithm, is a straightforward generalization to finitely generated $k$-algebras of the membership algorithm due to Shannon and Sweedler ([6]) for polynomial rings.

§1. GENERATORS FOR THE KERNEL OF A LOCALLY NILPOTENT DERIVATION; A SPECIAL CASE

Let $A$ be a commutative $\mathbb{Q}$-algebra and $D$ a derivation on $A$.

Then the map $\varphi: A \to A[[t]]$ defined by

$$
\varphi(a) = \sum_{k=0}^{\infty} \frac{1}{k!} D^k(a) t^k
$$

is a ringhomomorphism which satisfies

$$
\frac{d}{dt} \circ \varphi = \varphi \circ D
$$

(1.1)
Since the constant term of $\varphi(a)$ equals $a$, $\varphi$ is injective. So $\varphi : A \to \varphi(A)$ is a ring isomorphism. Also observe that if $a \in A$ belongs to $\varphi(A)$ (we have identified $A$ with $\varphi(A)$ in $A[[t]]$), say $a = \varphi(a')$, then $a = a'$ (looking at constant terms), hence $a = a + D(a)t + \cdots$, so $D(a) = 0$. Conversely, if $D(a) = 0$, then $a = \varphi(a)$. So we get

$$A \cap \varphi(A) = \ker D.$$  

The derivation $D$ is called locally nilpotent if for every $a \in A$ there exists a positive integer $n$ such that $D^n(a) = 0$. In terms of $\varphi$ this is equivalent to $\varphi(A) \subset A[t]$.

**Lemma 1.3.** Suppose $D$ is locally nilpotent on $A$ and that there exists an element $a_0 \in A$ such that $D(a_0) = 1$. Then every $f \in \varphi(A)$ can be written uniquely on the form

$$f = \sum_{i=0}^{m} f_i (t+a_0)^i,$$

with $m \in \mathbb{N}$ and every $f_i$ in $\ker D$.

**Proof.** Since $\varphi(A) \subset A[t]$, $f$ belongs to $A[t]$ and hence can be written uniquely on the form $f = \sum_{i=0}^{m} f_i (t+a_0)^i$, with $m \in \mathbb{N}$ and every $f_i$ in $A$. So it remains to prove that all $f_i$ belong to $\ker D$. We use induction on $m = \deg f$. If $m = 0$ $f = f_0 \in A \cap \varphi(A) = \ker D$ by (1.2)) and we are done. So let $m \geq 1$. From (1.1) it follows that $\frac{d}{dt} \varphi(A) \subset \varphi(D(A)) \subset \varphi(A)$ i.e. $\varphi(A)$ is stable under the derivation $\frac{d}{dt}$. Applying $\frac{d}{dt}$ $m$ times to $f$, we conclude that $m! f_m \in \varphi(A)$, whence $f_m \in \varphi(A) \cap A = \ker D$ (by (1.2)). Furthermore observe that $t+a_0 \in \varphi(A)$ (since $D(a_0) = 1$) and $f_m \in \varphi(f_m)$ (since $D(f_m) = 0$). So $f_m (t+a_0)^m = \varphi(f_m a_0^m) \in \varphi(A)$. Consequently $f_m (t+a_0)^m + \cdots + f_1 (t+a_0) + f_0 = f - f_m (t+a_0)^m \in \varphi(A)$. Then by the induction hypothesis we get that $f_0, f_1, \ldots, f_{m-1}$ belong to $\ker D$.

Let $k$ be a field of characteristic zero. Assume that $A$ is a finitely generated $k$-algebra, say $A = k[a_0, a_1, \ldots, a_n]$, and that $D$ is a locally nilpotent derivation on $A$ satisfying $D(a_0) = 1$. Then $\varphi(A) = k[\varphi(a_0), \ldots, \varphi(a_n)]$. Write $a_i(t)$ instead of $\varphi(a_i)$. So $a_i(t) = \exp(tD)(a_i)$ which belongs to $A[t]$. Developpe $a_i(t)$ as a polynomial in $t+a_0$ with coefficients in $A$ i.e. $a_i(t) = \sum a_{ij}(t+a_0)^j$, with $a_{ij} \in A$. Then by Lemma 1.3 each $a_{ij}$ belongs to $\ker D$. In fact they generate all of $\ker D$. To see this just observe that

$$\varphi(A) = k[a_0(t), a_1(t), \ldots, a_n(t)] = k[t+a_0, \sum a_{ij}(t+a_0)^j, \ldots, \sum a_{nj}(t+a_0)^j]$$

$$= k[a_{ij}; i \geq 1, j \geq 0][t+a_0] = k[\varphi(a_{ij}); i \geq 1, j \geq 0][\varphi(a_0)]$$

$$= \varphi(k[a_{ij}; i \geq 1, j \geq 0][a_0])$$

So $A = k[a_{ij}; i \geq 1, j \geq 0][a_0]$. Since $D(a_0) = 1$ and $D(a_{ij}) = 0$ for all $i, j$ it readily follows that $\ker D = k[a_{ij}; i \geq 1, j \geq 0]$. Finally, since $a_i(t-a_0) = \sum a_{ij}t^j$ we have proved.
\textbf{Proposition 1.4.} Let \( A = k[a_0, a_1, \ldots, a_n] \) and \( D \) a derivation on \( A \) satisfying \( D(a_0) = 1 \). Then \( \ker D = k[a_{ij}; i \geq 1, j \geq 0] \), where \( a_{ij} \) is the coefficient of \( t^j \) in

\[ \sum_{p \geq 0} \frac{1}{p!} (t-a_0)^p D^p(a_i) \]

\section{THE KERNEL OF A LOCALLY NILPOTENT DERIVATION}

Let \( A \) be a commutative ring without zero divisors and \( D \) a non-zero locally nilpotent derivation on \( A \) (So we do not assume that there exists an element \( a \) in \( A \) with \( D(a) = 1 \)). It follows easily that there exists an element \( a \in A \) such that \( d := D(a) \neq 0 \) and \( D^2(a) = 0 \) i.e. \( d \in \ker D \) (in other words \( \text{Im} D \cap \ker D \neq (0) \)). Define \( A' := A[d^{-1}] \).

\( A \subset A' \). The extension of \( D \) to \( A' \) (which we also denote by \( D \)) is again locally nilpotent and the element \( a_0 := d^{-1}a \in A' \) satisfies \( D(a_0) = 1 \). Observe that if \( d^{-m}b \in A'(m \in \mathbb{N}, b \in A) \), then \( d^{-m}b \in \ker(D, A') \) if and only if \( b \in \ker(D, A) \) (since \( d \in \ker D \)).

So

\[ \ker(D, A') = \ker(D, A)[d^{-1}] \]

Now suppose furthermore that \( A \) is a finitely generated \( k \)-algebra (i.e. \( A \) is an affine \( k \)-algebra), say \( A = k[a_1, \ldots, a_m] \), where \( k \) is a field of characteristic zero. So \( A' = k[a_1, \ldots, a_m, d^{-1}] = k[a_0, a_1, \ldots, a_m, d^{-1}] \), where \( a_0 \) is defined above. Then Proposition 1.4 implies that \( \ker(D, A') = k[a_{ij}; i \geq 1, j \geq 0][d^{-1}] \) where the \( a_{ij} \in A' \) are as described in Proposition 1.4. By (2.1) \( a_{ij} = d^{-i+j}r_{ij} \) for some \( e_{ij} \in \mathbb{N} \) and \( r_{ij} \in \ker(D) \). Hence, again by (2.1), \( (ker D)[d^{-1}] = \ker(D, A') = k[r_{ij}; i \geq 1, j \geq 0][d^{-1}] \).

Summarizing we showed

\textbf{Proposition 2.2.} Let \( A = k[a_1, \ldots, a_m] \) be a finitely generated \( k \)-algebra without zero-divisors and \( D \) a non-zero locally nilpotent derivation on \( A \). Then there exists a finite number of elements \( r_{ij} \in \ker D \) such that

\[ k[\cdots, r_{ij}, \cdots] \subset \ker(D) \subset k[\cdots, r_{ij}, \cdots][d^{-1}] \]

Furthermore, the \( r_{ij} \) can be computed as follows: for each \( 1 \leq i \leq m \) let \( a_{ij} \) be the coefficient of \( t^j \) in \( \sum_{p \geq 0} \frac{1}{p!} (t-a_0)^p D^p(a_i) \). Choose \( e_{ij} \in \mathbb{N} \) such that \( d^{-i+j}a_{ij} \) belongs to \( A \). Then take \( r_{ij} := d^{-i+j}a_{ij} \).

\textbf{Remark 2.3.} Since \( a_0 = d^{-1}a \), with \( a \in A \), it follows from formula (1.5) that \( d^N a_{ij} \in A \) for all \( j \), if \( D^{N+1}(a_i) = 0 \). i.e. we can take \( e_{ij} = N \) for all \( j \) in Proposition 2.2 if we want.
Put \( R := \ker(D, A) \). So the first part of Proposition 2.2 can be written as: there exists a finitely generated \( k \)-subalgebra \( R_0 \) of \( R \) and an element \( d \in R_0 \) such that

\[
R_0 \subset R \subset R_0[d^{-1}].
\]

For every integer \( m \geq 1 \) we define \( R_m \) inductively as the \( k \)-subalgebra of \( A \) generated by the elements \( g \in A \) satisfying \( dg \in R_{m-1} \). Since \( d \in R_0 \) it follows (by induction on \( m \)) that \( R_0 \subset R_m \) for all \( m \geq 1 \) and hence that \( R_{m-1} \subset R_m \) for all \( m \geq 1 \). By induction on \( m \) we also see that \( R_m \subset R \) for all \( m \geq 0 \): the case \( m = 0 \) is given, so let \( m \geq 1 \) and assume that \( R_{m-1} \subset R \). If \( g \in R_{m-1} \) then \( dg \in R_{m-1} \subset R \), so \( D(dg) = 0 \). Hence \( D(g) = 0 \), i.e. \( g \in R \).

**Lemma 2.5.** 1) For every \( m \geq 1 \) \( R_m \) is a finitely generated \( k \)-subalgebra of \( R \).  
2) If \( R \) is finitely generated over \( k \), then \( R = R_r \) for some \( r \in \mathbb{N} \).

**Proof.** 1) We use induction on \( m \). So let \( m \geq 1 \) and assume that \( R_{m-1} = k[F_1, \ldots, F_t] \). Let \( J \) be the set of \( P \in k[Y] := k[Y_1, \ldots, Y_n] \) such that \( P(F) := P(F_1, \ldots, F_t) \in \text{Ad} \). This is an ideal of \( k[Y] \) and hence of finite type. Let \( P_1, \ldots, P_s \) be its generators. So \( P_i(F) = f_i d \) for some \( f_i \in A \), which by definition belongs to \( R_m \) (since obviously \( P_i(F) \in R_{m-1} \)). Now we claim that \( R_m = k[F_1, \ldots, F_t, f_1, \ldots, f_s] \) (which implies 1)).

It remains to show "\( C \)." Therefore let \( g \in R_m \) i.e. \( dg \in R_{m-1} \). Then \( dg = P(F) \) for some \( P \in k[Y] \). In other words \( P(F) \in \text{Ad} \) i.e. \( P \in J \). So \( P = \sum a_i(Y)P_i \) for some \( a_i(Y) \in k[Y] \). Consequently \( P(F) = \sum a_i(F)P_i(F) \). Since \( P_i(F) = f_i d \) and \( P(F) = dg \) we conclude that \( dg = d \sum a_i(F)f_i \) whence \( g \in \sum k[F]f_i \subset k[F_1, \ldots, F_t, f_1, \ldots, f_s] \), which proves the claim.

2) By hypothesis \( R \) is a finitely generated \( k \)-algebra i.e. \( R = k[I_1, \ldots, I_n] \) for some \( I_j \in R \). Since \( R \subset R_0[d^{-1}] \) there exists \( r \in \mathbb{N} \) with \( d^r I_j \subset R_0 \) for all \( j \). So \( d^{r-1} I_j \subset R_1 \) whence \( d^{r-2} I_j \subset R_2 \) etc. Continuing in this way we find that \( I_j \in R_r \) for all \( j \). Hence \( R \subset R_r \subset R \) i.e. \( R = R_r \) as desired. \( \square \)

§3. THE ALGORITHM

We use the same notations as in §2. So \( A \) is a finitely generated \( k \)-algebra and \( R = \ker D \). Furthermore we assume: \( R \) is a finitely generated \( k \)-algebra.

Now we are able to describe the algorithm announced in the introduction. First by Proposition 2.2 we can compute a finitely generated \( k \)-subalgebra \( R_0 \) of \( R \) satisfying (2.4). In Lemma 2.5 we saw that \( R = R_r \) for some \( r \in \mathbb{N} \) i.e. the ascending chain of
finitely generated $k$-subalgebras $R_0 \subset R_1 \subset \ldots$ of $R$ becomes stationary after a finite number of steps where they all are equal to $R$. So to compute $R$ we need to solve the following two questions:

**Question 1.** How can we compute $R_m$ from $R_{m-1}$ (for all $m \geq 1$)?

**Question 2.** How can we decide if $R_{m-1} = R_m$? (if $R_{m-1} = R_m$, then obviously $R = R_{m-1}$).

To answer the first question we look at the proof of Lemma 2.5. So knowing that $R_{m-1} = k[F_1, \ldots, F_t]$ we must be able to compute the elements $f_1, \ldots, f_t$. Therefore we first compute generators $P_1, \ldots, P_s$ for the ideal $J$ in $A$. This can be done as follows: put $\overline{A} := A/Ad$. Let $P \in k[Y]$. Then $P(F_1, \ldots, F_t) \in Ad$ if and only if $P(\overline{F_1}, \ldots, \overline{F_t}) = 0$ in $\overline{A}$. So by applying the relation algorithm of §4 to the finitely generated $k$-algebra $\overline{A}$ and the elements $\overline{F_i}$ we find generators $P_1, \ldots, P_s$ for the ideal $J$. So we know that $P_i(F) = df_i$ for some $f_i$ in $A$. It remains to show how we can compute $f_i$ from the element $P_i$.

Let $A$ be given as $k[X_1, \ldots, X_n]/I$ where $I$ is the ideal in the polynomial ring $k[X] := k[X_1, \ldots, X_n]$ generated by the elements $h_1, \ldots, h_t$ say. Let $F_i = \overline{F_i} = F_i^* + I$ for some $F_i^*$ in $k[X]$ and $d = d^* + I$ for some $d^*$ in $k[X]$. Then $P(F) \in dA$ means that $P(F^*) = f_i^* d^* + \sum g_i h_i$ for some $f_i^*$ in $k[X]$ and $g_1, \ldots, g_t$ in $k[X]$. To find the coefficient $f_i^*$ of $d^*$ one can use well-known methods from Gröbner basis theory; more precisely, compute a reduced Gröbner basis $(G_1, \ldots, G_p)$ of the ideal $(d^*, h_1, \ldots, h_t)$ in $k[X]$. Write $P_i(F^*) = \sum c_i G_i$ (the coefficients $c_i$ can be computed). Express each $G_i$ as a linear combination of the basis elements $d^*, h_1, \ldots, h_t$ and substitute these expressions in $(*).$ Then one can find $f_i^*$ as the coefficient of $d^*$.

Finally, the second question is solved in §4 by the membership algorithm.

§4. A MEMBERSHIP AND A RELATION ALGORITHM FOR FINITELY GENERATED $k$-ALGEBRAS

In this section $k$ is an arbitrary field and $A$ a finitely generated $k$-algebra. So we may assume that $A = k[X]/I$, where $k[X] := k[X_1, \ldots, X_n]$ is the polynomial ring in $n$ variables over $k$ and $I$ an ideal in $k[X]$ generated by $h_1, \ldots, h_m$.

Let $\overline{F_1}, \ldots, \overline{F_t}$ be a finite number of elements of $A$ (i.e. $F_i$ belongs to $k[X]$ and $\overline{F_i}$ denotes the residue class of $F_i$ in $A$). Let $J$ be the ideal in $k[X,Y]$ generated by $Y_1 - F_1(X), \ldots, Y_t - F_t(X), h_1(X), \ldots, h_m(X)$. (here $k[X,Y] := k[X_1, \ldots, X_n, Y_1, \ldots, Y_t]$). On $k[X,Y]$ we choose an admissible ordering such that $X_i > k[Y]$ for all $i$ (cf. [6]). Let $G$ be the reduced Gröbner basis of $J$ with respect
to this ordering.

**Question 1.** Find generators for the ideal

\[ R := \{ P \in k[Y] \mid P(\bar{F}_1, \ldots, \bar{F}_t) = 0 \text{ in } A \} \].

**Solution (Relation algorithm).** \( G \cap k[Y] \) is a generating set for the ideal \( R \).

**Proof.** Let \( P \in k[Y] \). Then \( P \in R \iff P(\bar{F}) = 0 \text{ in } A \iff P(F) \in (h_1, \ldots, h_m) \text{ in } k[X] \iff P(P(Y)) \in J \text{ in } k[X, Y] \iff P \in k[Y] \cap J \). So \( R = k[Y] \cap J \). Then by [1] \( G \cap J \) is a Gröbner basis of \( k[Y] \cap J = R \).

**Remark 4.1.** Reformulating question 1 more geometrically, its solution was given by M. Kwieciński in [3]. To see this consider the polynomial map \( F = (F_1, \ldots, F_t) : k^n \rightarrow k^t \) and let \( V \subset k^n \) be the algebraic set defined by the polynomials \( h_1, \ldots, h_m \). Then one easily verifies that \( R \) is equal to the ideal of \( F(V) \) (= the Zariski closure of \( F(V) \)). Hence the solution to question 1 given above is just Theorem 4.1 of [3].

**Question 2.** Let \( \bar{f}(= f+1) \in A \). How can we decide if \( \bar{f} \in k[\bar{F}_1, \ldots, \bar{F}_t] \)?

**Solution (Membership algorithm).** Reduce \( f \) over \( G \) until reduction terminates with, say \( h \in k[X, Y] \). Then: \( \bar{f} \in k[\bar{F}_1, \ldots, \bar{F}_t] \iff h \in k[Y] \).

In this case \( \bar{f} = h(\bar{F}_1, \ldots, \bar{F}_t) \).

**Proof.** Just copy the proof of the membership algorithm given in [6].

**ACKNOWLEDGEMENT**

I like to thank Harm Derksen for several stimulating discussions.

**REFERENCES**


