J. Math. Kyoto Univ.
3-3 (1964) 369~377.

Invariants of a group in an affine ring

By

Masayoshi NAGATA

With an Appendix
by Masayoshi MIYANISHI

(Received May 6, 1964)

---

1. When a group G acts on a ring R inducing a group of automophisms, then we can speak of G-invariants in R. Let us denote the set of G-invariants in R by $I_G(R)$. Our particular interest lies in the case where R is a finitely generated (commutative) ring over a field K and the action of G on R is such that 1) the automorphisms are K-isomorphisms and 2) $\Sigma_{g\in G} f^g K$ is a finite K-module for every $f\in R$. In this case, let $f_1, \cdots, f'_{n'}$ be a set of generators of R over K and choose a linearly independent base $f_1, \cdots, f_n$ of $\Sigma_i(\Sigma_{g\in G}(f_i)^g K)$. Then $R=K[f_1, \cdots, f_n]$ and the action of F on R is characterized by the representation of G defined by the module $\Sigma_{i,g} f_i^g K$. Thus, in order to observe $I_G(R)$, we may assume that

(1) G is a matric group contained in $GL(n, K)$, and

(2) $R=K[f_1, \cdots, f_n]$ and, for every $g\in G$, the automorphis of R defined by g is induced by the linear transformation

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \to g \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}.$$

Under the circumstance, the following results are known:

Lemma 1. *$I_G(R)$ is finitely generated if every rational representation of G is completely reducible or if G is a finite group, hence if G has a normal subgroup N of finite index such that every rational representation of N is completely reducible.*

In the general case, there are some examples of a pair of G and R such that $I_G(R)$ is not finitely generated.

Lemma 1.2. *If $\overline{G}$ is the smallest algebraic set in $GL(n, K)$ among those containing G, then $\overline{G}$ is a group which acts on R naturally and $I_G(R)=I_{\overline{G}}(R)$.*

Lemma 1.3. *If K' is a ring containing K, then, under a natural extension of the action of G on $R\otimes_K K'$ such that every element of K' is G-invariant, we have $I_G(R\otimes_K K')=I(R)\otimes_K K'$.*

By virtue of Lemmas 1.2, 1.3, above, we see that, in asking finite generation of $I_G(R)$, fundamental is the case where G is an algebraic group with universal domain K. But, such an assumption does not bring us any simplicity in our treatment. Therefore we shall not assume that G is an algebraic group, but assume the assumptions (1) and (2) above.

Furthermore, rational representations of G which we meet in our treatment are rather special, and therefore it is good enough to understand by a rational representation of G a representation obtained in the following manner;

Let R^* be the polynomial ring over K in indeterminates $X_1, \cdots, X_n$. Then G acts on R^* as defined by

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \to g \begin{pmatrix} X_1 \\ \cdots \\ X_n \end{pmatrix} \quad \text{for each } g\in G.$$

Let M and N be G-stable finite K-modules contained in R^* such that $N\subseteq M$. M/N defines a rational representation of G. Rational representations we shall meet with in this paper are those of this type.

2. We call G a *reductive group* if every rational representation of G is completely reducible. It is known that

Lemma 2.1. *If G is an algebraic group, then* (i) *in the characteristic zero case, the reductivity is equivalent to the condition that the radical is a torus and* (ii) *in the case of characteristic $p\neq 0$, the reductivity is equivalent to the condition that the connected* *component* G_0 *of the identity of* G *is a torus and furthermore the index* $[G:G_0]$ *is prime to* p.

Thus the class of reductive groups is not very small in the characteristic zero case, but is very small in the positive characteristic case. Thus, in view of the known counter-example to the 14-th problem of Hilbert, the following consequence of Lemma 1.1 is rather satisfactory in the characteristic zero case and is very unsatisfactory in the positive characteristic case:

Lemma 2.2. *In the characteristic zero case,* $I_G(R)$ *is finitely generated if the radical of the smallest algebraic group* $\overline{G}$, *in* $GL(n, K)$ *among those containing* G, *is a torus: in the positive characteristic case,* $I_G(R)$ *is finitely generated if the connected component of the identity of* $\overline{G}$ *is a torus.*

3. Let us denote by P_m from now on the polynomial ring over K in m indeterminates $X_1, \cdots, X_m$.

Let ρ be a rational representation of G. If $\rho(G) \subseteq GL(m, K)$, then we define an action of G on P_m by

$$\begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} \to \rho(g) \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} \quad \text{for every } g \in G.$$

This is called the action of G on P_m defined by ρ.

We call G a *semi-reductive group* if the following is true: If ρ is a rational representation of G which defines an action on P_m (m being such that $\rho(G) \subseteq GL(m, K)$) such that (i) $\Sigma_{i \geq 2} X_i K$ is G-stable and (ii) X_1 modulo $\Sigma_{i \geq 2} X_i K$ is G-invariant, then there is a polynimial $F \in P_m$ which is G-invariant, monic in X_1 and of positive degree in X_1.

Since the action of G preserves the degree of every homogeneous form, the condition on F above may be replaced by the condition to be a G-invariant homogeneous form of positive degree which is monic in X_1.

For algebraic linear groups, it was conjectured by D. Mumford that if the radical is a torus then the group is semi-reductive. As will be shown below, this conjecture is equivalent to the following, which we like to call Mumford Conjecture:

Mumford Conjecture. *If G is a connected semi-simple algebraic linear group, then G is semi-reductive.*

To the writer's knowledge, Mumford Conjecture has been solved only in a very special case where characteristic is 2 and $G=SL(2, K)$; it was done by Mr. Tadao Oda.[1]

The purpose of the present note is to show

Main Theorem. *$I_G(R)$ is finitely generated if G is semi-reductive.*

Let us indicate here how to prove the equivalence of Mumford conjecture with the case of an algebraic group whose radical is a torus. The key lemma is:

Lemma 3. 1. *Let N be a normal subgroup of G. If both N and G/N are semi-reductive, then G is also semi-reductive.*

Proof. Let ρ be a rational representation of G as stated in the definition of semi-reductivity. Then the restriction ρ' of ρ on N is of the same type, whence there is a homogeneous form $F\in P_m$ of positive degree such that F is monic in X_1 and N-invariant under the action of N defined by ρ'. Consider the G-module $M=\Sigma_{g\in G}F^g K$. The action of G on M is really an action of G/N. Let M^* be $M\cap\Sigma_{i\geq 2}X_iP_m$, and let $F_1, \cdots, F_s$ be a base of M^*. Then, since $M=FK+M^*$, since any power of X_1 is G-invariant module $\Sigma_{i\geq 2}X_iP_m$, the semi-reductivity of G/N implies the existence of a homogeneous form F^* in F, F_1, $\cdots, F_s$ of positive degree such that (i) it is monic in F and (ii) it is G-invariant. F^* is a homogeneous form of positive degree in $X_1, \cdots$, X_m. Since $F_i\in\Sigma_{j\geq 2}X_jP_m$ and since F is monic in X_1, we see that F^* is monic in X_1. Thus G is semi-reductive.

Now the equivalence said above is proved easily by the fact that finite groups and tori are all semi-reductive.

1) To be published in this issue.

4. Before proving our main theorem, we like to give a remark on our formulation of Mumford Conjecture. Momford's formulation was stated in projective space. Namely, if ρ is a rational representation of G and if $\rho(G)\subseteq GL(m, K)$, then an action of G on P_m is defined, which defines an action of G on the projective space S^{m-1} of dimension $m-1$. The condition proposed by Mumford is that if a point $P\in S^{m-1}$ is G-invarinat, then there is a G-stable hypersurface in S^{m-1} which does not go through P.

If this condition is stated in P_m, then, choosing coordinates of P to be $(1, 0, \cdots, 0)$, it can be stated as follows:

If $\Sigma_{i\geq 2}X_iK$ is G-stable (hence, X_i modulo $\Sigma_{i\geq 2}X_iK$ is G-semi-invariant), then there is a G-semi-invariant homogeneous form F which is monic in X_1 and of positive degree.

Proposition 4.1. *If the above condition is satisfied by G, then G is semi-reductive.*

Proof. Let ρ be as in the definition of semi-reductivity. Then there is a homogeneous form F as in the above condition. Since X_1 is invariant modulo $\Sigma_{i\geq 2}X_iK$ under the action of G, any power of X_1 is G-invariant modulo the ideal generated by $\Sigma_{i\geq 2}X_iK$. Therefore that F is G-semi-invariant implies that F is G-invariant.

The converse of Proposition 4.1 is also true under the usual definition of rational representations and was proved by Mr. M. Miyanishi. The proof will be given at the end of this article as an appendix.

5. A reductive group is obviously a semi-reductive group, hence our main theorem includes the corresponding result for reductive groups. As for the proof, that special case is much simpler than the semi-reductive case. In order to compair these cases, let us begin with glance at the reductive case.

The following two are key lemmas to prove our main theorem for reductive groups:

Lemma 5.1.A. *Let ϕ be a G-homomorphism from R onto a ring R'. If G is reductive, then $I_G(R')=\phi(I_G(R))$.*

Lemma 5.2.A. *If G is reductive, then for any $h_1, \cdots, h_s$ in $I_G(R)$, we have $(\Sigma_i h_i R) \cap I(R) = \Sigma_i h_i(I_G(R))$.*

Namely, the first lemma enables us to assume that $f_1, \cdots, f_n$ are algebraically independent. Then the second lemma shows that $I_G(R)$ is a graded Noetherian ring, and we see easily that $I_G(R)$ is finitely generated, by virtue of a well known lemma which will be recalled later.

For semi-reductive groups, we have the following adaptions of the above lemmas:[2)]

Lemma 5.1.B. *With the same notations as above, if G is semi-reductive, then, for every element x of $I_G(R')$, there is a power x^t of x such that $x^t \in \phi(I_G(R))$. Consequently, $I_G(R')$ is integral over $\phi(I_G(R))$ in this case.*

Lemma 5.2.B. *Assume that G is semi-reductive. Then for any $h_1, \cdots, h_s \in I_G(R)$, every element of $(\Sigma_i h_i R) \cap I_G(R)$ is nilpotent modulo $\Sigma_i h_i(I_G(R))$.*

Proof of Lemma 5.1.B. Let y be an element of R such that $\phi(y) = x$. Set $M = \Sigma_{g \in G} y^g K$, $\mathfrak{a} = \phi^{-1}(0)$, $N = M \cap \mathfrak{a}$. If $x = 0$, then the assertion is obvious, and we assume that $x \neq 0$. Since x is G-invariant, we have $y^g - y \in N$ for every $g \in G$. Therefore, letting $y_1, \cdots, y_m$ be a linearly independent base of N, we see that, by virtue of the semi-reductivity of G, there is a G-invariant element F of $K[y, y_1, \cdots, y_m]$ which is monic and of positive degree, say t, in y, and homogeneous in $y, y_1, \cdots, y_m$. Then $\phi(F) = x^t \in \phi(I_G(R))$. This completes the proof of Lemma 5.1.B.

Proof of Lemma 5.2.B. We shall make use of induction argument on s without fixing R. Let ϕ be the natural homorphism from R onto R/h_1R. Let x be an arbitrary element of $(\Sigma_i h_i R) \cap I_G(R)$. Then $\phi(x)$ is in $\Sigma_{i \geq 2} \phi(h_i)\phi(R) \cap \phi(I_G(R))$, whence by induction on s, we see that there is a natural number t such that $\phi(x^t)$ is in $\Sigma_{i \geq 2} \phi(h_i) I_G(\phi(R))$. This means that $x^t = \Sigma_i h_i F_i$ with $F_1 \in R$ and $F_2, \cdots, F_s \in \phi^{-1}(I_G(\phi(R)))$. By Lemma 5.1.B, there is a natural number

2) We do not need Lemma 5.2.B in our proof of the main theorem. See §8 below.

u such that $\phi(F''_s)\in\phi(I_G(R))$. Then, considering x'^u instead of x', we may assume that $F_s\in I_G(R)$ (if $s>1$). Then $x'-h_sF_s\in(\Sigma_{i\leq s-1}h_iR)\cap I_G(R)$, and $x'-h_sF_s$ is nilpotent modulo $\Sigma_{i\leq s-1}h_i(I_G(R))$, which implies the assertion. Therefore we have only to prove the case where $s=1$. In this case, $x=h_1x'$ with $x'\in R$ and x' is G-invariant modulo $0:h_1R$. Let σ be the natural homorphism $R\rightarrow R/(0:h_1R)$. Then $\sigma(x')\in I_G(\sigma(R))$, whence there is a natural number t such that $\sigma(x'^t)\in\sigma(I_G(R))$. Let $z\in I_G(R)$ be such that $\sigma(z)=\sigma(x'^t)$. Then $x^t=h_1^tx'^t=h_1^tz\in h_1(I_G(R))$. This completes the proof of Lemma 5.2.B.

We recall here the lemma on graded Noetherian ring refered above:

Lemma 5.3. *Assume that a ring A is such that* (i) *it is the direct sum of submodules $A_0, A_1, \cdots, A_n, \cdots$* and (ii) *$A_iA_j\subseteq A_{i+j}$ for every possible pair (i, j). If the ideal $\Sigma_{i\geq 1}A_i$ has a finite basis, then A is finitely generated over A_0.*

6. Let ϕ be the homomorphism from P_n onto R such that $\phi(X_i)=f_i$ for every i and let $\mathfrak{k}$ be the kernel of ϕ. We shall prove here the main theorem in the case where $\mathfrak{k}$ is a homogeneous ideal. Since P_n is Noetherian, we can use induction argument on the largeness of $\mathfrak{k}$. Thus we assume that if $\mathfrak{k}'$ is a G-stable homogeneous ideal of P_n and contains $\mathfrak{k}$ properly, then $I_G(P_n/\mathfrak{k}')$ is finitely genenated.

Lemma 6.1. *Under the circumstance, if $\mathfrak{h}$ is a graded G-stable ideal $\neq 0$ of R, then $I_G(R)/(\mathfrak{h}\cap I_G(R))$ is finiterly generated.*

Proof. By assumption, $I_G(R/\mathfrak{h})$ is finitely generated. By Lemma 5.1.B. $I_G(R/\mathfrak{h})$ is integral over $I_G(R)/(\mathfrak{h}\cap I_G(R))$. These two facts show the result.

Therefore, by virtue of Lemma 5.3, if there is such an ideal $\mathfrak{h}$ (not containing 1) as above so that $\mathfrak{h}\cap I_G(R)$ has a finite basis, then we see the finite generation of $I_G(R)$.

As a particular case, we have the case of an integral domain. Namely, if h is a homogeneous element of $I_G(R)$ and if R is an integral domain, then $hR\cap I_G(R)=h(I_G(R))$. The same reasoning is applied if there is a homogeneous element h of positive degree which is not a zero-divisor.

Next we consider the case where R is not an integral domain. Let $h\neq 0$ be a homogeneous element of $I_G(R)$ of positive degree. Set $\mathfrak{a}=0:hR$. If $\mathfrak{a}=0$, then we finished already, and we assume that $\mathfrak{a}\neq 0$. Then, by Lemma 6.1, both $I_G(R)/(hR\cap I_G(R))$ and $I_G(R)/(\mathfrak{a}\cap I_G(R))$ are finitely generated. Therefore there is a finitely generated subring A of $I_G(R)$ such that $I_G(R)/(hR\cap I_G(R))=A/(hR\cap A)$ and such that $I_G(R)/(\mathfrak{a}\cap I_G(R))=A/(\mathfrak{a}\cap A)$. Since $I_G(R/\mathfrak{a})$ is a finite module over $A/(\mathfrak{a}\cap A)$, ther are elements $c_1, \cdots, c_t$ of R such that $I_G(R/\mathfrak{a})$ is generated by these c_i modulo $\mathfrak{a}$ as an $A/(\mathfrak{a}\cap A)$-module. We like to show that $I_G(R)$ is then generated by c_ih over A. Since c_i modulo $\mathfrak{a}$ are G-invariant, we see that c_ih are G-invariant. Conversely, let x be any element of $I_G(R)$. Then there is an element a of A such that $x-a\in hR$. Let r be such that $x-a=hr$ $(r\in R)$. Since hr is G-invariant, we see that r modulo $\mathfrak{a}$ is G-invariant, whence there is an element b of ΣAc_i such that $r-b\in\mathfrak{a}$. Then $hr=hb\in A[hc_1, \cdots, hc_t]$, this completes the proof, provided that the kernel $\mathfrak{k}$ of ϕ is homogeneous.

7. Now we consider the general case. We adapt the notation in §6 without assuming that $\mathfrak{k}$ is homogeneous. The induction argument is also adapted, considering all G-stable ideals of P_n. Then we need a different proof only in the case where $I_G(R)$ is an integral domain (for, othewise, take an element h of $I_G(R)$ which is a zero-divisor in $I_G(R)$, and adapt the proof just above). In this case, $I_G(R)$ is integral over $I_G(P_n)/(\mathfrak{k}\cap I_G(P_n))$. Since the result in §6 includes the case where $\mathfrak{k}=0$, we see that $I_G(P_n)$ is finitely generated, hence the integral dependence implies that $I_G(R)$ is finitely generated. Thus the proof of the main theorem is completed.

8. We like to add a remark here. As was remarked in a footnote, we did not use Lemma 5.2.B. What we remark here is that Lemma 5.2.B has the following meaning:

Consider the case where G is a semi-reductive algebraic group acting on an affine variety V with affine ring R. Let W be the affine variety defined by the affine ring $I_G(R)$. Then there is a one to one correspondence between closed orbits on V and points on W in such a way that if the orbit of $P \in V$ is closed and corresponds to $P' \in W$, then the local ring of P' is the set of G-invariants in the local ring of P.

If we define a relation $\sim$ such that $P \sim Q$ $(P, Q \in V)$ if and only if the closures of the orbits of P and Q meet, then we see that $\sim$ is an equivalence relation and each equivalence class contains unique closed orbit. If the class of P contains a closed orbit QG, then the set of G-invariants in the local ring of Q is contained in that of P.

In particular, if G is a linear algebraic group and if H is a semi-reductive algebraic subgroup of G, then G/H is affine.

The proof of the above statement can be given quite simiarly as in our lecture notes on the 14th problem of Hilbert at Tata Institute of Fundamental Research (that was for the case of reductive groups.)

APPENDIX

The converse of Proposition 4. 1.

We shall prove here the converse of Proposition 4. 1 above. Assume that a rational representation ρ of G is of the form

$$\begin{pmatrix} t & \sigma \\ 0 & \rho' \end{pmatrix}$$

where t is of degree 1. Let m be the degree of ρ. Then we consider a representation $\tau = tE$, E being the unit matrix of degree m. Then $\tau(g)$ is in the cener of $GL(m, K)$ for every $g \in G$, and therefore $\rho\tau^{-1}$ gives a rational representation of G (not in the restricted sense above, but in the usual sense). By the semi-reductivity of G, there is a homogeneous form F in P_m of positive degree such that it is monic in X_1 and G-invariant under the action of G defined by $\rho\tau^{-1}$. Then F is semi-invariant under the action of G defined by ρ. This proves the converse of Proposition 4. 1.