J. Math. Kyoto Univ.
3-3 (1964) 275~286.

On Mumford conjecture concerning reducible rational representations of algebraic linear groups

By

Tadao ODA

(Communicated by Prof. Nagata, May 27, 1964)

I. Let K be an algebraically closed field of an arbitrary characteristic and let G be an algebraic linear group. We consider only K-rational points of G. Let V be a vector space over K on which G acts as a group of K-automorphisms. We call V a rational G-module or G acts rationally on V, if for any element v in V the translates gv for all g in G generates only a finite dimensional subspace on which the induced action of G is a rational representation.

Definition 1. G is called semi-reductive if it has the following equivalent properties:

(1) For any exact sequence of finite dimensional rational G-modules

$$O \to W \to V \to K \to O$$

where K is considered to be a trivial rational G-module, there exists a positive integer m such that if we take the m-th symmetric products, the surjective G-homomorphism

$$V^m \to K^m \cong K$$

splits.

(2) Let $X_1, X_2, \cdots, X_n$ be indeterminates and suppose G acts rationally on the polynomial ring $K[X_1, X_2, \cdots, X_n]$ as a group of automorphisms of K-algebra in such a way that the K-subspaces $KX_1+KX_2+\cdots+KX_n$ and $KX_2+KX_3+\cdots+KX_n$ are G-stable and that X_1 is G-invariant modulo $KX_2+KX_3+\cdots+KX_n$. Then there exists a G-invariant homogeneous polynomial in $K[X_1, X_2, \cdots, X_n]$ which is monic in X_1.

(3) Let S be a finite dimensional projective space over K on which G acts rationally as a group of projective transformations. Suppose there exists a G-invariant point P in S. Then there exists a G-stable hypersurface in S which does not pass through P.

(4) Same assumptions as in (2) except that X_1 is G-semi-invariant modulo $KX_2+KX_3+\cdots+KX_n$. Then there exists a G-semi-invariant homogeneous polynomial in $K[X_1, X_2, \cdots, X_n]$ which is monic in X_1.

The equivalence of these properties can be proved easily. (See [1].) It is evident that reductive algebraic linear groups (i.e. every rational representation is completely reducible) are semi-reductive. Torus groups are reductive, hence semi-reductive. Finite algebraic linear groups are semi-reductive, but may not be reductive in general (i.e. if the order of the group is divisible by the characteristic of the field.).

The following facts are proved in [1].

Proposition 1. Let N be a normal algebraic subgroup of an algebraic linear group G. If N and G/N are semi-reductive, then G is itself semi-reductive. If G is semi-reductive, then G/N is semi-reductive.

Theorem 1. Let R be a commutative K-algebra of finite type. Suppose a semi-reductive algebraic linear group G acts rationally on R as a group of automorphisms of K-algebra. Then the K-subalgebra $I_G(R)$ of G-invariant elements of R is a K-algebra of finite type.

The following equivalent conjectures were given by D. Mumford:

Mumford conjecture. (1) If the radical of the connected component G_0 of the identity of an algebraic linear group G is a torus group, then G is semi-reductive.

(2) If G is a connected semi-simple algebraic linear group, then G is semi-reductive.

(3) If G is an almost simple algebraic linear group (in the sense of [3] i.e. any normal algebraic subgroup is either G itself or a finite subgroup), then G is semi-reductive.

The equivalence of these three properties can be proved easily

using Proposition 1. (cf. [1].)

It is known that if the field K is of characteristic 0 and if the radical of the connected component of the identity of an algebraic linear group G is a torus group, then G is reductive (hence semi-reductive). Thanks to this fact we have a good invariant theory in the case of characteristic 0. The importance of Mumford conjecture is due to the fact that if the conjecture is true, then we get a good invariant theory even in the case of positive characteristic thanks to Theroem 1.

Our purpose here is to prove Mumford conjecture in a very special case, i.e.

Theorem 2. If the field K is of characteristic 2, then the almost simple algebraic linear groups $G=SL(2, K)$ is semi-reductive.

Our method seems to be peculiar to this special case and some device will be indispensable to prove the conjecture in more general cases.

II. According to the "rational cohomology theory" of algebraic linear groups in [2], the extensions of left rational G-modules $O\to W\to V\to K\to O$ are classified up to equivalence by $\mathrm{Ext}^1_G(K, W)=H^1(G, W)=Z^1(G, W)/B^1(G, W)$ for a given left rational G-module W, where $Z^1(G, W)$ is the vector space of "rational crossed homomorphisms" form G to W i.e. morphisms of affine schemes f from G to W such that $f(gh)=gf(h)+f(g)$ for all g and h in G, and $B^1(G, W)$ is the subspace of "principal rational crossed homomorphisms" from G to W i.e. rational crossed homomorphisms dw for all w in W, where $dw(g)=gw-w$ for all g in G. To f in $Z^1(G, W)$ corresponds a rational G-module $V=K\oplus W$ with a decomposition as a vector space over K, where G acts on V on the left according to the rule $g(k+w)=k+kf(g)+gw$ for all g in G, k in K and w in W. A change of f to another rational crossed homomorphism f' in the same cohomology class modulo $B^1(G, W)$ corresponds to a change of the 1-dimensional K-subspace of V which is complementary to W (only as a vector space over K). Let H be an algebraic subgroup of G. The complementary

subspace K in $V=K\oplus W$ is H-stable if and only if the corresponding rational crossed homomorphism f vanishes on H. This is also equivalent to the following: $f(gh)=f(g)$ for all g in G and h in H.

We denote by $K[G]$ the affine ring of G and by $\mathfrak{M}$ the maximal ideal in $K[G]$ of functions which vanishes at the identity element e of G. Then $K[G]$ is a right rational G-module under the right translations $F\to F^g$, where $F^g(h)=F(gh)$ for F in $K[G]$ and g, h in G. We have another action of G, namely the left translations $F\to L_gF$, where $(L_gF)(h)=F(hg)$ for F in $K[G]$ and g, h in G.

Let W be a finite dimensional rational G-module and let $\mathrm{Hom}_K(W, K)$ be the dual space of W. We make it into a right rational G-module via the dual action of G: $u^g(w)=u(gw)$ for all g in G, w in W and u in $\mathrm{Hom}_K(W, K)$. For an element f in $Z^1(G, W)$ we have a K-homomorphism f^* from the vector space $\mathrm{Hom}_K(W, K)$ into the subspace $\mathfrak{M}$ of $K[G]$ defined by $f^*(u)(g)=u(f(g))$ for g in G and u in $\mathrm{Hom}_K(W, K)$. Note that $f(e)=0$. It is easy to check that $[f^*(u)]^g=f^*(u^g)+[f^*(u)](g)$ for u in $\mathrm{Hom}_K(W, K)$ and g in G. Hence $K+$(the image of f^*) is a finite dimensional G-stable subspace of $K[G]$. If the set theoretic image $f(G)$ generates W as a vector space over K, then f^* is injective. In this case we can consider the right rational G-module $K+$(the image of f^*) to be the dual rational G-module of the left rational G-module $V=K\oplus W$ determined by f through the pairing $\langle c+f^*(u), k+w\rangle=ck+u(w)$ for c, k in K, u in $\mathrm{Hom}_K(W, K)$ and w in W i.e. this pairing is non-degenerate and $\langle[c+f^*(u)]^g, k+w\rangle=\langle c+f^*(u), g(k+w)\rangle$. Conversely for a given finite dimensional subspace M of $\mathfrak{M}$ such that $K+M$ in $K[G]$ is G-stable under the right translation, we consider the dual vector space $\mathrm{Hom}_K(K+M, K)$ with the dual action of G on the left. It is finite dimensional and it has a canonical decomposition as a vector space $\mathrm{Hom}_K(K+M, K)=K\pi\oplus\mathrm{Hom}_K((K+M)/K, K)$ where π is the projection $K+M\ni F\to F(e)\in K$. It is easy to check that the set-theoretic image of the crossed homomorphism f in $Z^1(G, \mathrm{Hom}_K((K+M)/K, K))$ defined by $f(g)=g\pi-\pi$ generates the whole $\mathrm{Hom}_K((K+M)/K, K))$.

Lemma 1. A finite dimensional left rational G-module $V=K\oplus W$ corresponds to such a f in $Z^1(G, W)$ that the set-theoretic image $f(G)$ generates the whole W as a vector space over K, if and only if it is dual to such a finite dimensional G-submodule of the right rational G-module $K[G]$ that contains the constant field K. For an algebraic subgroup H of G the decomposition $V=K\oplus W$ is H-stable if and only if the corresponding finite dimensional G-submodule of the right rational G-module $K[G]$ is contained in the K-subalgebra $I_H(K[G])$ of H-invariant elements under the left translations.

Proof. The former part has already been proved. As for the latter we know from the remark before that $f(gh)=f(g)$ for all g in G and h in H, hence we have $L_h(f^*(u))=f^*(u)$ for all h in H and u in $\mathrm{Hom}_K(W, K)$.

Now we reduce our problem.

Lemma 2. (1) Let $O\to W\to V\to K\to O$ be an exact sequence of rational G-modules, and take its m-th symmetric product $O\to\sum_{i=1}^{m} W^i\to V^m\to K\to O$. If the n-th symmetric product of $V^m\to K\to O$ splits, then the mn-th symmetric product of $V\to K\to O$ splits.

(2) Let u: $W\to W'$ be a homomorphism of rational G-modules and let f be an element of $Z^1(G, W)$ and f' be the image of f under the homomorphism u_*: $Z^1(G, W)\to Z^1(G, W)$. If the m-th symmetric product of the exact sequence of rational G-modules $O\to W\to V\to K\to O$ corresponding to f splits, then the m-th symmetric product of the exact sequence of rational G-modules $O\to W'\to V'\to K\to O$ corresponding to f' splits.

The proofs are both trivial.

To prove that an algebraic linear group is semi-reductive we may restrict our attention to such finite dimensional left rational G-modules $V=K\oplus W$ that is determined by an f in $Z^1(G, W)$ whose set-theoretic image $f(G)$ generates the whole W as a vector space over K. In fact the subspace W' of W generated by $f(G)$ is G-stable because $gf(h)=f(gh)-f(g)$ for all g, h in G. Consider f to be an element of $Z^1(G, W')$ and apply Lemma 1 (2) to the injection $W'\to W$.

When an algebraic linear group G is connected, we denote by T, $N(T)$ and $W(T)=N(T)/T$ a maximal torus of G, the normalizer of T in G and the Weyl group of G respectively. It is well known that the torus group T is reductive. Hence for an exact sequence of rational G-modules $O\to W\to V\to K\to O$, we have a T-stable 1-dimensional subspace of V which is complementary to W. The element f in $Z^1(G, W)$ corresponding to this decomposition vanishes on T, or equivalently $f(gt)=f(g)$ for all g in G and t in T. If the order r of the Weyl group $W(T)$ is not divisible by the characteristic p of the field K, then $N(T)$ is reductive and the same argument can be applied. However to prove that a connected algebraic linear group G is semi-reductive we may suppose that f vanishes on $N(T)$ even if r is divisible by p. In fact we first take such a f in $Z^1(G, W)$ that vanishes on T as above. Then we take the r-th symmetric product $O\to\sum_{i=1}^{r} W^i\to V^r\to K\to O$. The subspace $K\prod_{i=1}^{r}(1+f(\sigma_i))$ which is complementary to $\sum_{i=1}^{r} W^i$ is evidently $N(T)$-stable, where $\sigma_1, \sigma_2, \cdots, \sigma_r$ are the representatives of $N(T)$ modulo T. Then apply Lemma 2 (1).

Combining Lemma 1 and Lemma 2 we get:

Proposition 2. (1) An algebraic linear group G is semi-reductive if and only if for any finite dimensional subspace M of $K[G]$ which contains the constant field K and which is G-stable under the right translations, there exists a positive integer m such that the surjective G-homomorphism of the m-th symmetric products $[\mathrm{Hom}_K(M, K)]^m\to[\mathrm{Hom}_K(K, K)]^m\cong K$ splits. An algebraic linear group G is semi-reductive if and only if the connected component G_0 of the identity is semi-reductive. As for a connected algebraic linear group G, G is semi-reductive if and only if there exists a positive integer m such that the surjective G-homomorphism $[\mathrm{Hom}_K(M, K)]^m\to[\mathrm{Hom}_K(K, K)]^m\cong K$ splits for any finite dimensional right G-stable subspace M of $K[G]$ which contains K and is contained in the K-subalgebra $I_T(K[G])$ (or in $I_{N(T)}(K[G])$) of T-invariant elements (resp. $N(T)$-invariant elements) of $K[G]$ under the left translations.

(2) Let $M'\subseteq M$ be a finite dimensional G-stable subspace of $K[G]$ con-

taining the constant field K. If the surjective G-homomorphism of the m-th symmetric products $[\mathrm{Hom}_K(M, K)]^m \to [\mathrm{Hom}_K(K, K)]^m \cong K$ splits, the same is true for $[\mathrm{Hom}_K(M', K)]^m \to [\mathrm{Hom}_K(K, K)]^m \cong K$.

(2) is nothing but (2) of Lemma 2.

III. In this section we denote by p the characteristic of the field K. We put $G=SL(2, K)$, $T=\left\{(t)=\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix};\ t\in K^*\right\}$ and $\sigma=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\in N(T)$. Then the affine ring of G is of the form $K[G]=K[A, B, C, D]$ where $AD-BC=1$ and $A(g)=a$, $B(g)=b$, $C(g)=c$, $D(g)=d$ for an element $g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ in G. We have $A^g=aA+cB$, $B^g=bA+dB$, $C^g=aC+cD$, $D^g=bC+dD$ for $g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ in G. Taking into account that $L_{(t)}A=tA$, $L_{(t)}B=tB$, $L_{(t)}C=t^{-1}C$, $L_{(t)}D=t^{-1}D$ and $L_\sigma A=C$, $L_\sigma B=D$, $L_\sigma C=-A$, $L_\sigma D=-B$ we have $L_{(t)}(AC)=AC$, $L_{(t)}(BD)=BD$, $L_{(t)}(AD+BC)=AD+BC$, $L_{(t)}(AD)=AD$, $L_{(t)}(BC)=BC$; $L_\sigma(AC)=-AC$, $L_\sigma(BD)=-BD$, $L_\sigma(AD+BC)=-(AD+BC)$, $L_\sigma(AD)=-BC$, $L_\sigma(BC)=-AD$. For $g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ in G we get

$$\begin{aligned}(AD+BC)^g &= (ad+bc)(AD+BC)+2abAC+2cdBD\\ (AC)^g &= ac(AD+BC)+a^2AC+c^2BD\\ (BD)^g &= bd(AD+BC)+b^2AC+d^2BD\end{aligned}$$

From these and $AD-BC=1$ we get:
if $p=2$, $I_{N(T)}(K[G])=K[AC, BD]$ with AC and BD algebraically independent over K and

$$\begin{aligned}(AC)^g &= ac+a^2AC+c^2BD\\ (BD)^g &= bd+b^2AC+d^2BD\end{aligned} \qquad \text{for} \quad g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

if $p\neq 2$, $I_T(K[G])=K[(AD+BC), AC, BD]$ with algebraic relation $(AD+BC)^2=1+4(AC)(BD)$. Monomials $\{F_{\varepsilon,i,j}=(AD+BC)^\varepsilon(AC)^i \times(BD)^j;\ \varepsilon=0 \text{ or } 1;\ i, j \text{ non-negative integers}\}$ are linearly independent over K and $F_{\varepsilon,i,j}$ is in $I_{N(T)}(K[G])$ if and only if $\varepsilon+i+j$ is even.

Proof of Theorem 2. For brevity we put $X=AC$, $Y=BD$, then $X(g)=ac$, $Y(g)=bd$ for $g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $I_{N(T)}(K[G])=K[X, Y]$ and

$$\begin{aligned} X^g &= ac + a^2X + c^2Y \\ Y^g &= bd + b^2X + d^2Y \end{aligned} \qquad \text{for} \quad g = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

We denote by $M[m]$ for non-negative integer m the finite dimensional subspace of $K[X, Y]$ consisting of the polynomials in X and Y of total degree at most m. From the action of G under the right translations given above we see that $M[m]$ are G-stable, hence we have a increasing chain of finite dimensional G-stable subspaces whose union equals the whole $I_{N(T)}(K[G])$

$$K = M[0] \subset M[1] \subset M[2] \subset \cdots \subset M[m] \subset \cdots .$$

Every finite dimensional subspace is contained in $M[m]$ for some m. This and proposition 2 permit us to restrict our attention to the dual left rational G-modules $V[m] = \mathrm{Hom}_K(M[m], K)$ for all m. We denote by $\{[m; i, j]; i, j \geqq 0 \text{ and } i+j \leqq m\}$ the dual base of $V[m]$ corresponding to the base $\{X^iY^j; i, j \geqq 0 \text{ and } i+j \leqq m \text{ of } M[m]\}$. From $X^g = ac + a^2X + c^2Y$, $Y^g = bd + b^2X + d^2Y$ we have

$$\begin{aligned} (X^iY^j)^g &= (ac + a^2X + c^2Y)^i (bd + b^2X + d^2Y)^j \\ &= \sum_{\substack{0 \leqq u, v \\ u+v \leqq i+j}} X^u Y^v E(u, v; i, j)(g) \end{aligned}$$

for $g = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, where $E(u, v; i, j)$, defined only for 4-ples of non-negative integers $(u, v; i, j)$ satisfying $u+v \leqq i+j$, are in the affine ring $K[G]$ and easily computed from the formula above. In the following we only need the following explicit forms:

$$\begin{aligned} &E(0, 0; i, j)(g) = (ac)^i (bd)^j = (X^iY^j)(g) \\ &\qquad\qquad \text{for } i, j \ m, \text{ such that } i+j \leqq m \\ &E(m, 0; i, j)(g) = a^{2i}b^{2j} \\ &E(0, m; i, j)(g) = c^{2i}d^{2j} \quad \text{for } i, j, m \text{ such that } i+j = m. \end{aligned}$$

The action of G on $V[m]$ dual to that on $M[m]$ is

$$g[m; u, v] = \sum_{\substack{0 \leqq i, j \\ u+v \leqq i+j \leqq m}} E(u, v; i, j)(g)\,[m; i, j]$$

In particular

$$g[m;\,0,0]=\sum_{\substack{0\le i,j\\ i+j\le m}}(ac)^i(bd)^j[m;\,i,j]=\sum_{\substack{0\le i,j\\ i+j\le m}}(X^iY^j)(g)[m;\,i,j]$$

$$=[m;\,0,0]+f_m(g)\quad\text{for}\quad g=\begin{pmatrix}a & c\\ b & d\end{pmatrix},\quad\text{where}$$

$$f_m(g)=\sum_{\substack{0\le i,j\\ 0<i+j\le m}}(X^iY^j)(g)[m;\,i,j]$$

is the crossed homomorphism with values in the G-stable subspace $W[m]=\sum_{\substack{0\le i,j\\ 0<i+j\le m}}K[m;\,i,j]$ of codimension 1. As X^iY^j are linearly independent over K, the image of f_m generates $W[m]$ over K. $[m;\,0,0]$ is G-invariant modulo $W[m]$. We also know that

$$g[m;\,m,0]=\sum_{\substack{0\le i,j\\ i+j=m}}a^{2i}b^{2j}[m;\,i,j]$$

$$g[m;\,0,\mathrm{m}]=\sum_{\substack{0\le i,j\\ i+j=m}}c^{2i}d^{2j}[m;\,i,j]\qquad\text{for}\quad g=\begin{pmatrix}a & c\\ b & d\end{pmatrix}$$

In the following we prove by induction on m that the 2^m-th symmetric product of the surjective G-homomorphism

$$V[m]=\mathrm{Hom}_K(M[m],K)\to\mathrm{Hom}_K(K,K)\cong K$$

splits. In fact we get a stronger result, that is, there exists a G-invariant element in $V[m]^n$ of the form $[m;\,0,0]^n+R[m]$ where $n=2^m$ and $R[m]$ is a homogeneous polynomial of degree n in the base $\{[m;\,i,j);\ (i,j)\neq(0,0)\}$ of $W[m]$.

First we take the element $[m;\,0,0]^2+[m;\,m,0][m;\,0,m]$ in $V[m]^2$. We have

$$g([m;\,0,0]^2+[m;\,m,0][m;\,0,m])$$

$$=\left\{\sum_{\substack{0\le i,j\\ i+j\le m}}(ac)^i(bd)^j[m;\,i,j]\right\}^2+\left\{\sum_{\substack{0\le i,j\\ i+j=m}}a^{2i}b^{2j}[m;\,i,j]\right\}$$

$$\times\left\{\sum_{\substack{0\le i,j\\ i+j=m}}c^{2i}d^{2j}[m;\,i,j]\right\}$$

$$=\sum_{\substack{0\le i,j\\ i+j\le m-1}}(ac)^{2i}(bd)^{2j}[m;\,i,j]^2+\sum_{\substack{0\le i,j\\ i+j\le m-1}}(ac)^{2i}(bd)^{2j}$$

$$\times\{(ad)^{2(m-i-j)}+(bc)^{2(m-i-j)}\}[m;\,i,m-i][m;\,m-j,j]$$

Note that the characteristic $p=2$.

Lemma 3. Let $\bar{x}$ and $\bar{y}$ be elements in a field K of characteristic 2 which satisfy $\bar{x}+\bar{y}=1$. Let N be a positive integer. Then $\bar{x}^N+\bar{y}^N=P_N(\bar{x}\bar{y})$, where P_N is a polynomial of one variable with coefficients in $Z/(2)$ whose degree is less than $N/2$ and whose constant term $P_N(0)=1$.

Proof. Let Z be the ring of integers and let x and y be two indeterminates. In the ring $Z[x, y]$

$$x^N+y^N=(1/2^{N-1})\sum_{0\leq 2k\leq N}\binom{N}{2k}(x+y)^{N-2k}\{(x+y)^2-4xy\}^k$$

Hence in the ring $Z[\tilde{x}, \tilde{y}]=Z[x, y]/(x+y-1)$

$$\tilde{x}^N+\tilde{y}^N=(1/2^{N-1})\sum_{0\leq 2k\leq N}\binom{N}{2k}(1-4\tilde{x}\tilde{y})^k$$

This is a polynomial in $(\tilde{x}\tilde{y})$ with 1 as the constant term, of degree $N/2$ (resp. $(N-1)/2$) if N is even (resp. odd) and with $(-1)^{(N/2)}2$ (resp. $(-1)^{[(N-1)/2]}N$) as the leading coefficient if N is even (resp. odd). Reducing this equation modulo 2, we get the required result.

Proof of Theorem 2 continued. Denoting by π the rational Frobenius endomorphism of $G=SL(2, K)$ which maps an element $g=\begin{pmatrix}a & c\\ b & d\end{pmatrix}$ to $\pi(g)=\begin{pmatrix}a^2 & c^2\\ b^2 & d^2\end{pmatrix}$, the last equality before Lemma 3 becomes:

$$\begin{aligned}
&g([m; 0, 0]^2+[m; m, 0][m; 0, m])\\
&\quad=\sum_{\substack{0\leq i, j\\ i+j\leq m-1}}(a^2c^2)^i(b^2d^2)^j[m; i, j]^2\\
&\quad+\sum_{\substack{0\leq i, j\\ i+j\leq m-1}}(a^2c^2)^i(b^2d^2)^jP_{m-i-j}((a^2c^2)(b^2d^2))[m; i, m-i][m; m-j, j]\\
&\quad=\sum_{\substack{0\leq i, j\\ i+j\leq m-1}}(X^iY^j)(\pi(g))[m; i, j]^2\\
&\quad+\sum_{\substack{0\leq i, j\\ i+j\leq m-1}}(X^iY^jP_{m-i-j}(XY))(\pi(g))[m; i, m-i][m; m-j, j]
\end{aligned}$$

We know that $X^iY^jP_{m-i-j}(XY)$ is a polynomial in X and Y of less total degree than $i+j+2((m-i-j)/2)=m$. Hence we can write

$$g([m; 0, 0]^2+[m; m, 0][m; 0, m])=\sum_{\substack{0\leq i, j\\ i+j\leq m-1}}(X^iY^j)(\pi(g))[i, j]$$

for $g=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$, where $[0,0]=[m;0,0]^2+P_m(0)[m;0,m][m;m,0]=[m;0,0]^2+[m;m,0][m;0,m]$ and for $i,j\geqq 0$ satisfying

$$0<i+j\leqq m-1,\quad [i,j]=[m;i,j]^2+[m;i_1,m-i_1][m;m-j_1,j_1]+\cdots.$$

Note that $[m;0,0]$ does not appear in $[i,j]$ for $(i,j)\neq(0,0)$. It is easy to check that the elements $\{[i,j];\ i,j\geqq 0,\ i+j\leqq m-1\}$ in $V[m]^2$ are linearly independent over K. We can rewrite the above equality as

$$g[0,0]=[0,0]+\sum_{\substack{0\leqq i,j\\ 0<i+j\leqq m-1}}(X^iY^j)(\pi(g))[i,j]$$

Compairing this with

$$\begin{aligned} g[m-1;0,0] &= [m-1;0,0]+\sum_{\substack{0\leqq i,j\\ 0<i+j\leqq m-1}}(X^iY^j)(g)[m-1;i,j] \\ &= [m-1;0,0]+f_{m-1}(g) \end{aligned}$$

and taking Lemma 1 into account, we see that the subspaces

$$V'=\sum_{\substack{0\leqq i,j\\ i+j\leqq m-1}}K[i,j]\quad\text{and}\quad W'=\sum_{\substack{0\leqq i,j\\ 0<i+j\leqq m-1}}K[i,j]\quad\text{of}\quad V[m]^2$$

are G-stable and that the rational representation of G associated with the rational G-module V' is equivalent to the composition $\rho_{m-1}\circ\pi$ of the representation π and the representation ρ_{m-1} associated with the rational G-module $V[m-1]$. As π does not affect our induction hypothesis for $m-1$, there exists a G-invariant element of the form $[0,0]^n+R$ where $n=2^{m-1}$ and R is a homogeneous polynomial of degree n in the base $\{[i,j];\ (i,j)\neq(0,0)\}$ of W'. The image of this G-invariant element under the G-homomorphism $(V')^n\to((V[m])^2)^n\to V[m]^{2n}$ is $([m;0,0]^2+[m;m,0][m;0,m])^n+\overline{R}=[m;0,0]^{2n}+([m;m,0]^n[m;0,m]^n+\overline{R})$ where $2n=2^m$ and $\overline{R}$ is the image of R, hence is a homogeneous polynomial of degree $2n=2^m$ in the base $\{[m;i,j];\ (i,j)\neq(0,0)\}$. Thus we get a G-invariant element of the form $[m;0,0]^{2^m}+R[m]$ where $R[m]$ is a homogeneous polynomial of degree 2^m in $\{[m;i,j];\ (i,j)\neq(0,0)\}$. q.e.d.

BIBLIOGRAPHY

[1] M. Nagata, Invariants of a group in an affine ring, to appear in this issue.
[2] G. Hochschild, Cohomology of algebraic linear groups, Ill. J. Math., vol. 5, 1961.
[3] Séminaire C. Chevalley 1956/58.
[4] M. Nagata, Complete reducibility of rational representations of a matric group, J. Math. Kyoto Univ., vol. 1, 1961.