Additive groups associated with points of a projective space

By HEISUKE HIRONAKA*

1. Let k be an arbitrary field (commutative). As will become clear, we are primarily interested in the case of an imperfect field. With a polynomial ring $S = k[X_0, X_1, \cdots, X_r]$, naturally graded, we define a projective space $\mathbf{P} = \operatorname{Proj}(S)$ and a vector space $\mathbf{V} = \operatorname{Spec}(S)$. We then find an additive subgroup scheme of $\mathbf{V}$, denoted by $\mathcal{B}_{\mathbf{P},y}$, naturally associated with each point y of $\mathbf{P}$. The following definition is preliminary as far as the existence is concerned.

Definition. $\mathcal{B}_{\mathbf{P},y}$ is the group subscheme of $\mathbf{V}$ such that the ring of invariants of $\mathcal{B}_{\mathbf{P},y}$ in S is the graded k-subalgebra $\mathfrak{U}$ generated by those homogeneous polynomials h in S having the following property:

(1.1) $\deg h$ is equal to the multiplicity of the hypersurface $\operatorname{Proj}(S/hS)$ of $\mathbf{P}$ at the point y.

This definition will be justified in the next section by showing that the k-subalgebra $\mathfrak{U}$ so defined is such that the fibre of the morphism $\operatorname{Spec}(S) \to \operatorname{Spec}(\mathfrak{U})$, through the origin, is a group subscheme of $\mathbf{V}$. In fact, for this purpose, we shall prove that after a suitable automorphism of the graded k-algebra S,

(1.2) $\mathfrak{U} = k[\sigma_1, \sigma_2, \cdots, \sigma_e]$ with $\sigma_i = X_i^{q_i} + \sum_{j=i+1}^{r+1} c_{ij} X_j^{q_i}$, where $c_{ij} \in k$, $X_{r+1} = X_0$, $1 \leqq q_1 \leqq \cdots \leqq q_e$ and each q_i is a power of the characteristic p of k. (In the case of characteristic zero, $q_i = 1$ for all i.)

As is seen from this, $\mathcal{B}_{\mathbf{P},y}$ is *homogeneous* in the sense that it is invariant under the scalar multiplication in $\mathbf{V}$. Quite generally, if $\mathbf{W}$ is a homogeneous subscheme of $\mathbf{V}$, then we have a corresponding subscheme $\mathcal{P}(\mathbf{W})$ of $\mathbf{P}$, i.e., $\mathcal{P}(\mathbf{W}) = \operatorname{Proj}(G)$ for $\mathbf{W} = \operatorname{Spec}(G)$. We will see in the third section that $\mathcal{B}_{\mathbf{P},y}$ need not be a vector subspace of $\mathbf{V}$, i.e., the degrees q_i of (1.2) need not be all 1. If it is, however, $\mathcal{B}_{\mathbf{P},y}$ is obviously the smallest vector subspace of $\mathbf{V}$ such that $\mathcal{P}(\mathcal{B}_{\mathbf{P},y})$ contains the point y. It is also obvious from the definition that if y is k-rational, i.e., $k(y) = k$, then $\mathcal{B}_{\mathbf{P},y}$ is nothing but the line corresponding to the point y. We can always have the *smallest homogeneous group subscheme* $\mathcal{B}^*_{\mathbf{P},y}$ *of* $\mathbf{V}$ *such that* $\mathcal{P}(\mathcal{B}^*_{\mathbf{P},y})$ *contains* y. It is then clear that $\mathcal{B}_{\mathbf{P},y}$ contains $\mathcal{B}^*_{\mathbf{P},y}$. We will see below that these two groups do not coincide in

* The work was partly supported by NSF-GP-9152.

general.

It turns out that this group scheme $\mathcal{B}_{\mathrm{P},y}$ plays a very important role in the study of singularities, especially from the point of view of desingularization problems for general schemes. Namely, if $\pi\colon Z' \to Z$ is a blowing-up over a regular scheme Z with a regular center, then $\pi^{-1}(x)$ with a point x of the center E is a projective space. In fact, $\pi^{-1}(x) = \mathcal{P}(N_{Z,E,x})$ where $N_{Z,E,x}$ is the fibre at x of the normal bundle of E in Z. Hence we associate with each point x' of $\pi^{-1}(x)$ the group subscheme $\mathcal{B}_{\pi,x'}$ of the tangent vector space $T_{Z,x}$ such that $\mathcal{B}_{\pi,x'}$ contains $T_{E,x}$ and $\mathcal{B}_{\pi^{-1}(x),x'}$ is equal to $\mathcal{B}_{\pi,x'}/T_{E,x}$. Consider a subscheme X of Z such that X contains E and is normally flat along E, and let X' be the strict transform of X by π. It can be proven that[1] *if the Hilbert-Samuel function of X' at x' is equal to that of X at x, then the tangential cone of X at x is invariant under the action of $\mathcal{B}_{\pi,x'}$.* We shall prove in the third section that $\mathcal{B}_{\mathrm{P},y}$ is a vector subspace if its dimension is at most equal to the characteristic p of k. This is one of the many reasons that the resolution of singularities of surfaces is substantially easier than the higher dimensional cases. (No characteristic is less than two, for characteristic zero should be better thought of characteristic infinity from that point of view!)

2. Let A be a commutative ring with unity, and J the kernel of the natural map $A \otimes A \to A$ by multiplication. We denote by $j\colon A \to A \otimes A$ the monomorphism defined by $j(s) = 1 \otimes s$. Let us view $A \otimes A$ as A-module from the left, i.e., $s(s' \otimes s'') = (ss') \otimes s''$. *A differential operator of order* $\leqq n$ in A will then mean a composition αj where α is an A-homomorphism $A \otimes A \to A$ whose kernel contains J^{n+1}. The differential operators of order $\leqq n$ in A form an A-module in a natural manner, which we shall denote by $\mathrm{Diff}_n(A)$. If A is a graded algebra, then we define: $D \in \mathrm{Diff}_n(A)$ *is homogeneous of degree* d if and only if $D(A_m) \subset A_{m+d}$ for all m, where A_i denotes the homogeneous part of degree i of A. We shall denote by $\mathrm{Diff}_{n,d}(A)$ the A_0-module of all differential operators of order $\leqq n$ in A which are homogeneous of degree d. For the polynomial ring S as before, we have an obvious differential operator D_B in S associated with each multi-index $B = (b_0, b_1, \cdots, b_r)$ with non-negative integers b_j. Namely, if $t = (t_0, t_1, \cdots, t_r)$ is a system of indeterminates over S, then $f(X + t) = \sum_B (D_B f) t^B$ for $f = f(X) \in S$. Moreover each element of $\mathrm{Diff}_a(k)$ extends to a differential operator in S by acting trivially on the chosen variables X_j. In this sense, $\mathrm{Diff}_{n,d}(S)$ is generated additively by those $S_m D_B \mathrm{Diff}_a(k)$ for $m - |B| = d$ and $a + |B| = n$, where $|B| = b_0 + b_1 + \cdots + b_r$.

[1] This fact among others (including the contents of this paper) was presented in Mathematics 252 "*Theory of singularities*", 1969 Spring, at Harvard University. See [1, Th. IV].

Let $y \in \mathbf{P} = \operatorname{Proj}(S)$ as before. If D is in $\operatorname{Diff}_{n,d}(S)$ and h is in S_d, different from zero, then we can associate with them a differential operator in the local ring $0_{\mathbf{P},y}$, denoted by $(h^{-1}D)^{(y)}$, as follows. Assuming $X_0 \notin \mathfrak{U}$ without any loss of generality, first D extends uniquely to a differential operator D' in the localization $S[X_0^{-1}]$, secondly $h^{-1}D'$ is homogeneous of degree zero and induces an operator D'' in the homogeneous part of degree zero $A_0 = (S[X_0^{-1}])_0$, and finally D'' extends uniquely to $(h^{-1}D)^{(y)}$ in the localization $0_{\mathbf{P},y}$ of A_0.

THEOREM 1. *Let $\mathfrak{U}$ be the graded k-subalgebra of S generated by those homogeneous polynomials h having the property* (1.1) *of* § 1. *Then we have*

$$\mathfrak{U}_m = \bigcup_{a \geqq 1} \lambda_a^{-1}\left(\sum_b \operatorname{Diff}_{a+b-1,-b}(S)\mathfrak{U}_{am+b}\right), \tag{2.1}$$

where $\mathfrak{U}_i$ denotes the homogeneous part of degree i of $\mathfrak{U}$ (in the sense of the grading inherited from S) and λ_a is the a^{th}-power map of S into itself, i.e., $\lambda_a(s) = s^a$.

PROOF. Clearly $\mathfrak{U}_m$ is contained in the right side of (2.1). In fact, take $a = 1$ and $b = 0$. Now to prove the reversed inclusion, pick $f \in S_m$ and suppose $f^a = \sum_i D_i g_i$, a finite sum with $D_i \in \operatorname{Diff}_{a+i-1,-i}(S)$ and $g_i \in \mathfrak{U}_{am+i}$. Let us assume that X_0 is not in $\mathfrak{U}$. Then the multiplicity of $\operatorname{Proj}(S/fS)$ at y is the order of f/X_0^m in the local ring $0_{\mathbf{P},y}$, which we denote by $\operatorname{ord}_y(f/X_0^m)$. $D_i X_0^{am+i}$ (the differential operator which is the multiplication by X_0^{am+i} followed by D_i) is homogeneous of degree am. Let $E_i = (X_0^{-am}D_iX_0^{am+i})^{(y)}$ in the sense defined above. Then we have the equality in the local ring $0_{\mathbf{P},y}$: $(f/X_0^m)^a = \sum_i E_i(g_i/X_0^{am+i})$. Since $g_i \in \mathfrak{U}$, we have $g_i/X_0^{am+i} \in M_{\mathbf{P},y}^{am+i}$ where $M_{\mathbf{P},y}$ denotes the maximal ideal of $0_{\mathbf{P},y}$. Since $E_i \in \operatorname{Diff}_{a+i-1}(0_{\mathbf{P},y})$, we have $E_i(M_{\mathbf{P},y}^{am+i}) \subset M_{\mathbf{P},y}^{a(m-1)+1}$. Thus $(f/X_0^m)^a \in M_{\mathbf{P},y}^{a(m-1)+1}$, which implies $\operatorname{ord}_y(f/X_0^m) \geqq m$. This means $f \in \mathfrak{U}_m$.

Supplement (2.2). In the above proof, we used the general fact that *if D is a differential operator of order $\leqq n$ in A, then $D(H^m) \subset H^{m-n}$ for every ideal H in A and for all $m \geqq n$.* This is easy to prove. In fact, let $z_i \in H$ for $1 \leqq i \leqq m$. Then, J being the kernel of the canonical map $A \otimes A \rightarrow A$, we have

$$j\left(\prod_{i=1}^m z_i\right) = 1 \otimes \left(\prod_{i=1}^m z_i\right) = \prod_{i=1}^m \left(z_i \otimes 1 - \omega(z_i)\right),$$

where $\omega(z_i) = z_i \otimes 1 - 1 \otimes z_i \in J$. Since $(z_i \otimes 1)\beta = z_i\beta$ for $\beta \in A \otimes A$, we set $j\left(\prod_{i=1}^m z_i\right) \in H^{m-n}A \otimes A + J^{n+1}$. It immediately follows that $D(H^m) \subset H^{m-n}$.

In the sequel, a *purely inseparable form* in S will mean a homogeneous polynomial of the form $\sum_{i=0}^r c_i X_i^q$ with $c_i \in k$ and a power $q \geqq 1$ of the characteristic p of k. It means a linear form in the case of characteristic zero. Remark that the assertion (1.2) of § 1 is now immediate from the following

COROLLARY (2.3). *The k-algebra $\mathfrak{A}$ is generated by purely inseparable forms.*

PROOF. Let T denote the k-subalgebra of $\mathfrak{A}$ generated by all the purely inseparable forms in $\mathfrak{A}$. We write each $f \in S$ as $f = \sum_B f(B)X^B$ with $f(B) \in k$ and multi-indices $B = (b_0, b_1, \cdots, b_r)$. We then denote by $\mathrm{ex}(f)$ the largest B in the lexicographical ordering such that $f(B) \neq 0$. Now, suppose $T \neq \mathfrak{A}$. Then pick a homogeneous polynomial g of the smallest degree in $\mathfrak{A} - T$. Clearly we can choose g in such a way that $g(B) = 0$ for all $B = \mathrm{ex}(f)$ with $f \in T$. Since $g \notin T$, there exists B such that $g(B) \neq 0$ and X^B is not purely inseparable. Pick the largest B with these properties. Then we can write $B = B' + B''$ so that $B' \neq (0)$, $B'' \neq (0)$ and $D_{B'}(X^B) \neq 0$ (which implies $D_{B''}(X^B) \neq 0$). By the maximality of B, we then have $\mathrm{ex}\,(D_{B'}(g)) = B''$ and $\mathrm{ex}\,(D_{B''}(g)) = B'$, so that $\mathrm{ex}\,(D_{B'}(g)D_{B''}(g)) = B$. On the other hand, (2.1) of the theorem for $a = 1$ and $b = |B'|$ implies $D_{B'}(g) \in \mathfrak{A}$. By the minimality of $\deg g$, we get $D_{B'}(g) \in T$. Similarly, $D_{B''}(g) \in T$. Thus $g(B) \neq 0$ contradicts the above selection of g. We obtain $T = \mathfrak{A}$.

Remark. (2.4). In the proof of (2.3), we used only a small part of the property (2.1) of $\mathfrak{A}$, i.e., only for the case of differential operators of S which are trivial in the base field k. We need the full strength of (2.1), however, in more delicate problems about the group $\mathcal{B}_{\mathbf{P},y}$.

3. It is very desirable from the point of view of desingularization problems, to have any reasonable classification theorem of those groups $\mathcal{B}_{\mathbf{P},y}$. We have, and present below, a complete classification only in small dimensions.

THEOREM 2. *If* $\dim \mathcal{B}_{\mathbf{P},y} \leqq p = \mathrm{char}\,(k)$, *then* $\mathcal{B}_{\mathbf{P},y}$ *is a vector subspace of* $\mathbf{V}$.

To prove this theorem, we choose the X_j so that the ring of invariants $\mathfrak{A}$ of $\mathcal{B}_{\mathbf{P},y}$ has the property (1.2) of § 1. Then $\dim \mathcal{B}_{\mathbf{P},y} = r + 1 - e$, say $= d$. Write $(Y_0, Y_1, \cdots, Y_d)$ for $(X_e, X_{e+1}, \cdots, X_{r+1})$. Note $\sigma_e \in k[Y]$. It suffices to show that if $d \leqq p$, then either $\deg \sigma_e = 1$ or $\mathfrak{A}$ contains a non-constant polynomial of degree $< \deg \sigma_e$ in $k[Y]$ (where the latter is clearly impossible by (1.2)). Thanks to the property (2.1) of $\mathfrak{A}$ (for $a = p$, $b = 0$ and $m = p^{a-1}$), Theorem 2 will thus follow from the following

LEMMA (3.1). *Let us assume $p > 0$. Let $\sigma = \sum_{i=0}^{d} c_i Y_i^q$ where $c_i \in k$, $c_0 = 1$ and $q = p^a$ with $a > 0$. Each element of* $\mathrm{Diff}_n(k)$ *will be viewed as a differential operator in $k[Y]$ by their trivial action on the variables Y_i. Then*

(i) *if $d < p$, then there exists $D \in \mathrm{Diff}_d(k)$ such that $D(\sigma) \neq 0$ and $D(\sigma) \in (k[Y])^p$.*

(ii) *if* $d = p$, *then there exists* $D \in \mathrm{Diff}_{p-1}(k)$ *such that* $D(\sigma) \neq 0$ *and* $D(\sigma) \in (k[Y])^p$.

PROOF. (i) is proven by induction on $d \geqq 0$. If $d = 0$, then $D = 1$ will do. Say $d > 0$. If all $c_i \in k^p$, then again $D = 1$ will do. We may hence assume $c_1 \notin k^p$. Then there exists a derivation D' in k with $D'(c_1) = 1$. Then $D'(\sigma) \neq 0$ and $D'(\sigma) \in k[Y_1, \cdots, Y_d]$. By induction assumption, there exists $D'' \in \mathrm{Diff}_{d-1}(k)$ such that $D''(D'(\sigma)) \neq 0$ and $D''(D'(\sigma)) \in (k[Y])^p$. $D = D''D'$ thus have the required property. To prove (ii), there are two cases. First take the case of $[k^p(c): k^p] \leqq p$, where $c = (c_1, \cdots, c_r)$. If this is $<p$, then $\sigma \in (k[Y])^p$ and $D = 1$ will do. Assume it is $=p$ and say $c_1 \notin k^p$. Then each c_j is written uniquely as a polynomial in c_1 of degree $<p$ with coefficients in k^p. Let s be the maximum of these degrees. If T is the derivation in k with $T(c_1) = 1$, then $D = T^s$ has the required property. Next consider the case of $[k^p(c): k^p] \geqq p^2$. We may assume that $[k^p(c_1, c_2): k^p] = p^2$. Then there exists a derivation D' of k such that $D'(c_1) = 1$ and $D'(c_2) = 0$. Then $D'(\sigma) \in k[Y_1, Y_2, \cdots, Y_d]$. Hence, by (i), there exists $D'' \in \mathrm{Diff}_{d-2}(k)$ such that $D = D''D'$ has the required property.

COROLLARY (3.2). *If* $\dim \mathcal{B}_{\mathbf{P},y} \leqq 2$, *then* $\mathcal{B}_{\mathbf{P},y}$ *is a vector subspace of* $\mathbf{V}$.

THEOREM 3. *If* $\dim \mathcal{B}_{\mathbf{P},y} = 3$, *then one and only one of the following two is true.*

(i) $\mathcal{B}_{\mathbf{P},y}$ *is a vector subspace of* $\mathbf{V}$.

(ii) $\mathrm{char}\,(k) = 2$, *and the ring of invariants* $\mathfrak{A}$ *of* $\mathcal{B}_{\mathbf{P},y}$ *takes the following form after a suitable automorphism of the graded* k*-algebra* S:

$\mathfrak{A} = k[\sigma, X_4, \cdots, X_r]$ *with* $\sigma = X_0^2 + uX_1^2 + vX_2^2 + uvX_3^2$ *where* u *and* v *are elements of* k *such that* $[k^2(u, v): k^2] = 4$.

Theorem 3 will be proven after the following few lemmas.

LEMMA (3.3). *Assume* $p > 0$ *and let* $\sigma = Y_0^q + c_1Y_1^q + \cdots + c_sY_s^q$ *where* $c_i \in k$ *for all* i *and* $q = p^a$ *with* $a \geqq 1$. *Let* $[k^p(c): k^p] = p^e$ *with* $c = (c_1, \cdots, c_s)$. *Then*

(i) *there exists* $D_1 \in \mathrm{Diff}_\alpha(k)$ *with* $\alpha = (p-1)^e$ *such that* $D_1(\sigma) \neq 0$ *and* $D_1(\sigma) \in (k[Y])^p$,

(ii) *for every* $q' = p^{a'}$ *with* $1 \leqq a' \leqq a$, *there exists* $D_2 \in \mathrm{Diff}_\beta(k)$ *with* $\beta = 1 + (q'/p)(s - e)$ *such that* $D_2(\sigma) \neq 0$ *and* $D_2(\sigma) \in (k[Y])^{q'}$.

PROOF. We may assume that $c_1, \cdots, c_e$ are p-independent over k^p. The existence of D_1 is clear because each c_j can be written uniquely as a polynomial in $c_1, \cdots, c_e$ with all respective degrees $<p$ and with coefficients in k^p. To prove (ii), we give here a general recipe to find such D_2 and show that its

order is at most β. The recipe is by induction on the number of variables Y_j. Let q^* be the largest power of p such that $q^* \leqq q'$ and $\sigma = (\sigma^*)^{q^*}$ with some $\sigma^* \in k[Y]$. If $q^* = q'$, then we take $D_2 = 1$. If $q^* < q'$, then write $\sigma^* = Y_0^{q''} + c_1^* Y_1^{q''} + \cdots + c_s^* Y_s^{q''}$ with $c_j^* \in k$ and $q'' = q/q^*$. Let $p^f = [k^p(c^*): k^p]$. After a suitable permutation among the Y_i, let $p^f = [k^p(c_1^*, \cdots, c_f^*): k^p]$. Let E be a derivation of k such that $E(c_i^*) = 0$ for $i < f$ and $E(c_f^*) = 1$. Pick one differential operator D' of the smallest order in k which has the property that $D'(\sigma^{**}) \neq 0$ and $D'(\sigma^{**}) \in (k[Y])^{q'}$, where $\sigma^{**} = E(\sigma^*)^{q^*} = (Y_f^{q''} + \cdots)^{q^*}$ which involves only $(s - f) + 1$ variables or less. Let D be a differential operator of order $\leqq q^*$ in k such that $D(\tau^{q^*}) = E(\tau)^{q^*}$ for all $\tau \in k$. (Such D exists but is not unique. See (3.4) below.) Then we take $D_2 = D'D$ and complete the recipe. The above process does not repeat more than s times for σ of (3.3) and each time we add a differential operator D of order at most $q^* \leqq q'/p$. Hence D_2 should have order $\leqq (q'/p)s$. This proves (ii) for the case of $e = 0$. If $e > 0$, then $q^* = 1$ and the above $D = E$ is a derivation. Since $E(\sigma^*)$ involves at most $1 + s - e$ variables, the order of D' is at most $(q'/p)(s - e)$. Thus the order of D_2 in this case is at most $1 + (q'/p)(s - e)$.

Supplement (3.4). The existence of D for the given E, used in the above proof, can be proven as follows. Let us pick and fix a p-base $\{u_a\}_{a \in A}$ for k over k^p. Let $\hat{A}$ be the semigroup of all those maps $f: A \rightarrow \mathbf{Z}_0$ (=the semigroup of non-negative integers) such that $f(a) = 0$ except for a finite number of a. For each $f \in \hat{A}$, we write u^f for the monomial $\prod_{a \in A} u_a^{f(a)}$. We have a differential operator D_f in k associated with each $f \in \hat{A}$, which is defined by $D_f(u^g) = (g: f)u^h$ with the binomial coefficients $(g: f) = \prod_{a \in A} g(a)!/f(a)!h(a)!$ if $h \in \hat{A}$ with $f + h = g$ exists, and $D_f(u^g) = 0$ if such h does not exist. This property determines D_f because every differential operator in k, say of order $\leqq n$, is trivial (i.e., a k-multiple of the identity) in k^N with $N = p^e > n$. For this same reason, moreover, every differential operator in k is uniquely written as a finite k-linear combination of those D_f. Say $E = \sum b_f D_f$ with $b_f \in k$. Then we can choose D to be $\sum b_f^{q^*} D_{q^*f}$, where q^*f means the element of $\hat{A}$ with $(q^*f)(a) = q^*(f(a))$. See that this D has the required property in the proof of (3.3). Note that D so defined does depend not only upon E but also upon the choice of the p-base of k over k^p.

COROLLARY (3.5). *In Lemma* (3.3), *take the case of* $s = 3$. *If* $\mathrm{Diff}_{N-1}(k)\sigma \cap (k[Y])^N = (0)$ *for every* $N = p^b$ *with* $b \geqq 1$, *then we must have* $p = q = 2$ *and* $e = 2$.

PROOF. The notation being the same as in (3.3), if $e = 0$ then the assumption of (3.5) fails with $N = p$. It does the same if $e = 1$ by (i) of (3.3).

Say $e \geqq 2$. By taking $q' = p$ in (ii) of (3.3), we see that $p < s = 3$. Hence $p = 2$. Then again by (ii) of (3.3), but taking $q' = q$, we get $q = 2$ and $e = 2$.

COROLLARY (3.6). *Under the assumption of* (3.5), *σ can be put into the form given in* (ii) *of Theorem* 3 *by means of a suitable k-linear transformation of variables.*

PROOF. By (3.5), we have $p = 2$ and $\sigma = Y_0^2 + c_1 Y_1^2 + c_2 Y_2^2 + c_3 Y_3^2$ where (we may assume) $[k^2(c_1, c_2): k^2] = 4$ and $c_3 \in k^2(c_1, c_2)$. Let E_i be the derivation in k such that $E_i(c_i) = 1$ and $E_i(c_j) = 0$ for $1 \leqq i, j \leqq 2$ and $i \neq j$. Let $c_1 = u$ and $c_2 = v$. The assumption of (3.5) for $N = 2$, implies that $E_i(c_3) \notin k^2$ for $i = 1, 2$. Hence $c_3 = a_0^2 + a_1^2 u + a_2^2 v + a_3^2 uv$ with $a_i \in k$ and $a_3 \neq 0$. Now let $X_0 = Y_0 + a_0 Y_3$, $X_1 = Y_1 + a_1 Y_3$, $X_2 = Y_2 + a_2 Y_3$, and $X_3 = a_3 Y_3$.

LEMMA (3.7). *Let σ be the same as the one in* (ii) *of Theorem* 3. *Let*

$$\sigma' = b_0 X_0^2 + b_1 X_1^2 + b_2 X_2^2 + b_3 X_3^2 + X_4^2$$

with $b_j \in k$. Then there exists a pair of differential operators of degrees $\leqq 1$ in k, say D and D', such that $D(\sigma) - D'(\sigma') \neq 0$ and $\in (k[X])^2$.

PROOF. We may replace σ' by $\sigma' - b_0\sigma$ so that $b_0 = 0$. Moreover, it is enough to consider the case in which there is no differential operator D' of degree $\leqq 1$ in k such that $D'(\sigma') \neq 0$ and $\in (k[X])^2$. Then by (3.5) and (3.6), every pair but not all of the three b_j are 2-independent over k^2. In particular, $b_3 \in k^2(b_1, b_2)$. Therefore, if D (resp. D') is the derivation of k such that $D(u) = 1$ (resp. $D'(b_1) = 1$) and $D(v) = 0$ (resp. $D'(b_2) = 0$), then $D(\sigma) - D'(\sigma') = (v - D'(b_3))X_3^2$ and $D'(b_3) = f^2 b_2 + g^2$ with $f, g \in k$. If $v - D'(b_3) \neq 0$, then D and D' divided by this constant have the property of (3.7). If $v = D'(b_3) = f^2 b_2 + g^2$, then $\sigma - f^2\sigma' = Y^2 + \alpha X_1^2 + \beta X_3^2$ where $Y = X_0 + gX_2 - fX_4$ and certain α and β in k. It is then easy to find a differential operator of order $\leqq 1$ in k, say D, such that $D(\sigma - f^2\sigma') \neq 0$ and $\in (k[X])^2$.

LEMMA (3.8). *Let $\mathbf{P} = \mathrm{Proj}\,(S)$ with $S = k[X_0, X_1, \cdots, X_r]$ as before. Let us assume that we have two elements u and v having the property given in* (ii) *of Theorem* 3. *Let y be the point of $\mathbf{P}$ whose maximal ideal in the affine ring $k[t]$ with $t_i = X_i/X_3$, $0 \leqq i \leqq r$ and $i \neq 3$, is generated by the following*

$$(t_0 + t_1 t_2,\ t_1^2 + v,\ t_2^2 + u,\ t_4,\ \cdots,\ t_r)\ .$$

Then the ring of invariants $\mathfrak{U}$ of $\mathcal{B}_{\mathbf{P},y}$ is the one given in (ii) *of Theorem* 3.

PROOF. It is easy to check that $\mathfrak{U}$ of (ii) of Theorem 3 is contained in the ring of invariants $\mathcal{B}_{\mathbf{P},y}$. (See $\sigma/X_3^2 = (t_0 + t_1 t_2)^2 + (t_1^2 + v)(t_2^2 + u) \in M_{\mathbf{P},y}^2$.) Call the latter $\mathfrak{U}'$. By the assumption on u and v, it is easy to see that the group subscheme $\mathbf{W}$ of $\mathbf{V}$ associated with $\mathfrak{U}$ is reduced and irreducible. (This subscheme is by definition the fibre through the origin of the canonical morphism $\mathrm{Spec}(S) \to \mathrm{Spec}(\mathfrak{U})$.) Therefore if $\mathfrak{U} \neq \mathfrak{U}'$, then $\dim \mathcal{B}_{\mathbf{P},y} < \dim \mathbf{W} = 3$. Then by (3.2), $\mathcal{B}_{\mathbf{P},y}$ should be a vector subspace of $\mathbf{V}$ and there should be a linear polynomial in t_0, t_1, and t_2 which is $\neq 0$ and belongs to the maximal ideal of y. This is impossible because the square roots of u and v are 2-independent over k.

Now Theorem 3 can easily be deduced from these lemmas and their corollaries starting with the general fact (1.2) of § 1 (or Corollary (2.3) of Theorem 1).

Remark (3.9). In the case of (ii) of Theorem 3 (or the case of Lemma (3.8)), the group scheme $\mathcal{B}^*_{\mathbf{P},y}$ mentioned in § 1 is strictly smaller than $\mathcal{B}_{\mathbf{P},y}$. In fact, the ring of invariants of $\mathcal{B}^*_{\mathbf{P},y}$ in S is $k[X_1^2 + vX_3^2, X_2^2 + uX_3^2, \sigma, X_4, \cdots, X_r]$.

HARVARD UNIVERSITY

REFERENCE

[1] HEISUKE HIRONAKA, *Certain numerical characters of singularities*, to appear in Kyoto Journal of Mathematics, 1970.

(Received July 24, 1969)