J. Sci. Hiroshima Univ. Ser. A-I
34 (1970), 29-58

On the Structure of Bialgebras Attached to Group Varieties

Hiroshi Yanagihara

(Received February 20, 1970)

As compared with separable isogenies of group varieties, inseparable ones have a peculiar aspect. Let G and G' be two group varieties and let α be an isogeny of G onto G'. Then the tangential mapping α_* of the tangent space at the unit point of G to that of G' associated with α is not an isomorphism if α is inseparable, whereas α_* is an isomorphism if α is separable. We may say, in the scheme theoretic languages, that an inseparable isogeny α of G has the kernel of α which is a group subscheme of G with the non-reduced structure sheaf. In particular the kernel of a purely inseparable isogeny of G is a group subscheme of G with one point e such that the stalk of the structure sheaf at e is an artinian local ring.

As to the purely inseparable isogenies of height 1, it is known that the kernels of the tangential mappings determine these isogenies. Precisely, let $\mathfrak{g}$ be the Lie algebra of G consisting of the left invariant derivations of G. Then p-subalgebras of Lie of $\mathfrak{g}$ stable under the adjoint representation of G correspond to purely inseparable isogenies of G of height 1. This was obtained essentially by I. Barsotti in [1], and some authors generalized his results (cf. [3], [5] and [11]). Barsotti considered in [1] also kernels of general purely inseparable isogenies of group varieties and used invariant semi-derivations (or hyperderivations in his terminologies) on G as tools, which were introduced by J. Dieudonné for formal Lie groups of a positive characteristic in [6]. However he did not pursue complete results in general cases, and P. Cartier developed some theories on this subject (cf. [2], [3] and [4]).

The aim of this paper is to give a theory of purely inseparable isogenies of group varieties essentially from Barsotti's point of view originated in the paper [1]. The main results are as follows. Let G be a group variety defined over an algebraically closed field k, and denote by $\mathfrak{g}(G)$ the set of left invariant semi-derivations on G. Then we shall show that $\mathfrak{H}(G) = k \oplus \mathfrak{g}(G)$ is a bialgebra over k using the main results in [3], and that the set of isomorphism classes of purely inseparable isogenies of G corresponds bijectively to the set of subbialgebras of $\mathfrak{H}(G)$ of finite dimensions which are stable under the adjoint representation of G. Moreover if $N(\alpha)$ is the corresponding subbialgebra of a purely inseparable isogeny α of G, it will be shown that the affine algebraic group scheme Spec $(N(\alpha)^D)$ is the kernel of α in the scheme theoretic sense, where $N(\alpha)^D$ is the linear dual of the bialgebra $N(\alpha)$.

The first three sections are devoted to the development of a systematic theory of local semi-derivations of a local ring, global semi-derivations of an algebraic function field and regular semi-derivations at a simple point of an algebraic variety, respectively, which are used later. In §4 we give a theory of invariant semi-derivations on a group variety G following Barsotti's idea in [1]. In particular we shall show that a semi-derivation D on an abelian variety is invariant if and only if D is regular at any point of it. This is a generalization of the result for ordinary invariant derivations on an abelian variety. In §5 we shall show first that G is commutative if and only if $\mathfrak{H}(G)$ is a commutative algebra over k. This was given by Dieudonné for formal Lie groups in [6], but we shall prove it directly without making use of his result. Moreover some functorial properties of $\mathfrak{H}(G)$ will be given in this section. In §6 we shall give the correspondence between the set of purely inseparable isogenies of G and the set of finite dimensional subbialgebras of $\mathfrak{H}(G)$ stable under the adjoint representation of G. In the last section, we shall define the kernel of a purely inseparable isogeny of G as a group subscheme of G and give the relations between this subscheme and the subbialgebra of $\mathfrak{H}(G)$ corresponding to the isogeny. Moreover we shall give a condition for a group subscheme of G to be the kernel of a purely inseparable isogeny of G.

Our terminologies are mainly Weil's in [12] and [13], but we use in part also the languages of the scheme theory in [7] and [10].

In the course of this work, the author had stimulating conversations with Prof. M. Nishi constantly, and obtained many valuable suggestions from him. Here the author wishes to express his thanks to the Professor.

§ 1. Local semi-derivations on a local ring

Let k be a field of a positive characteristic p, and O a local ring containing k such that the residue field $O/\mathfrak{m}$ of O modulo its maximal ideal $\mathfrak{m}$ is canonically isomorphic to k. Then we denote by $f(O)$ the element of k representing the class of an element f in O modulo $\mathfrak{m}$, and by O^{p^r} the subring of O consisting of the elements of the p^r-th power x^{p^r} of x in O.

We understand by *a local semi-derivation D of height r on O* a k-linear mapping of O into k satisfying the equality

$$D(fg)=f(O)D(g)+g(O)D(f) \quad \text{for} \quad f \text{ in } O \text{ and } g \text{ in } O^{p^r}.$$

A local semi-derivation D of height r on O is called *special* if $D(f)=0$ for any f in O^{p^r}. We shall denote by $\mathfrak{D}_r(O)$ the set of the local semi-derivations of height r on O and by $\mathfrak{S}_r(O)$ the subset of $\mathfrak{D}_r(O)$ consisting of the special ones. Let α be an element of k and D an element of $\mathfrak{D}_r(O)$. Then the linear mapping αD defined by $(\alpha D)(f)=\alpha(D(f))$ for f in O is in $\mathfrak{D}_r(O)$ and $\mathfrak{D}_r(O)$ is a vector space over k by this scalar product. It is obvious that $\mathfrak{S}_r(O)$ is

a linear subspace of $\mathfrak{D}_r(O)$. Since the restriction to O^{p^r} of any element D in $\mathfrak{D}_r(O)$ is a local derivation in a usual sense, we can easily see that $D(O^{p^{r+1}})=0$. Therefore we have the following

LEMMA 1. *For any integer $r\geq 0$, we have*

$$\mathfrak{S}_r(O)\subset\mathfrak{D}_r(O)\subset\mathfrak{S}_{r+1}(O).$$

If $\{x_1, \cdots, x_n\}$ is a system of generators for the maximal ideal $\mathfrak{m}$ of O, let $\mathfrak{M}_r$ be the ideal of O generated by the elements $x_1^{p^r}, \cdots, x_n^{p^r}$. Then it is easily seen that $\mathfrak{M}_r$ is determined independently of the choice of the generators $x_1, \cdots, x_n$ of $\mathfrak{M}$ and that O^{p^r} is contained in the set $k+\mathfrak{m}_r$.

LEMMA 2. *If D is in $\mathfrak{S}_r(O)$, then we have $D(k+\mathfrak{m}_r)=0$.*

PROOF. Since O^{p^r} contains 1 and D is k-linear, we have $D(k)=0$. If f is in $\mathfrak{m}_r$, f is a linear combination $\sum\alpha_i x_i^{p^r}(\alpha_i\in O)$, and hence we have $D(f)=\sum\alpha_i(O)D(x_i^{p^r})+\sum(x_i(O))^{p^r}D(\alpha_i)=0$ since $x_i(O)=D(x_i^{p^r})=0$. Therefore $D(k+\mathfrak{m}_r)=0$. q. e. d.

PROPOSITION 1. *Suppose that O is a regular local ring of rank n. Then $\mathfrak{S}_r(O)$ is a vector space of dimension $p^{nr}-1$ over k.*

PROOF. By Lemma 2, D in $\mathfrak{S}_r(O)$ vanishes on $k+\mathfrak{m}_r$ and hence corresponds to an element $\bar{D}$ in the dual space $(O/k+\mathfrak{m}_r)^*$ of $O/k+\mathfrak{m}_r$ over k. The mapping $\phi: D\to\bar{D}$ is an injective k-linear mapping. If $\{t_1, \cdots, t_n\}$ is a regular system of parameters of O, $O/k+\mathfrak{m}_r$ is isomorphic to $\sum_{e_i<p^r} k\prod_{i=1}^{n} t_i^{e_i}$ as vector spaces over k, where the sum $\sum_{e_i<p^r}$ runs over all $(e_1, \cdots, e_n)$ such that $0\leq e_i<p^r$ and $\sum_{i=1}^{n} e_i>0$. Therefore $\dim_k(O/k+\mathfrak{m}_r)$ is equal to $p^{nr}-1$ and hence we have $\dim_k\mathfrak{S}_r(O)\leq p^{nr}-1$. On the other hand f in O has the following expression

$$f\equiv f(O)+\sum_{e_i<p^r}\alpha_{e_1\cdots e_n}t_1^{e_1}\cdots t_n^{e_n}(\text{mod. }\mathfrak{m}_r),$$

where $f(O)$ and $\alpha_{e_1\cdots e_n}$ are in k, and uniquely determined. Let $D_{e_1\cdots e_n}$ be the mapping of O into k which maps f to $\alpha_{e_1\cdots e_n}$. Then it is easily seen that $D_{e_1\cdots e_n}$ is in $\mathfrak{S}_r(O)$. Moreover these $p^{nr}-1$ semi-derivations are linearly independent over k. In fact if $\sum_{e_i<p^r}\beta_{e_1\cdots e_n}D_{e_1\cdots e_n}=0$ $(\beta_{e_1\cdots e_n}\in k)$, we have $(\sum_{e_i<p^r}\beta_{e_1\cdots e_n})t_1^{e_1}\cdots t_n^{e_n})=\beta_{e_1\cdots e_n}=0$. Therefore $\dim_k\mathfrak{S}_r(O)$ is at least $p^{nr}-1$ and hence is equal to $p^{nr}-1$. q. e. d.

COROLLARY. *Suppose that O is a regular local ring and let D be a k-linear mapping of O into k. Then D is in $\mathfrak{S}_r(O)$ if and only if $D(k+\mathfrak{m}_r)=0$, and $\mathfrak{S}_r(O)$ is canonically isomorphic to the dual space of $\mathfrak{m}/\mathfrak{m}_r$ over k.*

PROOF. Since we have $\dim_k\mathfrak{S}_r(O)=\dim_k(O/k+\mathfrak{m}_r)^*=\dim_k(\mathfrak{m}/\mathfrak{m}_r)^*$, the

mapping ϕ in the proof of Proposition 1 is an isomorphism. Then $\mathfrak{S}_r(O)$ is exactly the set of k-linear mapping of O into k vanishing on $k+\mathfrak{m}_r$. q.e.d.

The basis $\{D_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ of $\mathfrak{S}_r(O)$ over k in the proof of Proposition 1 will be called *the canonical basis of* $\mathfrak{S}_r(O)$ *with respect to the regular system* $\{t_1, \cdots, t_n\}$ *of parameters of* O. Moreover we put $E_{1,r}=D_{p^r 0\cdots 0}$, $\cdots$, $E_{i,r}=D_{0\cdots \overset{i}{p^r}\cdots 0}$, $\cdots$, $E_{n,r}=D_{0\cdots 0 p^r}$, where $D_{0\cdots 0 p^r 0\cdots 0}$ is an element of the canonical basis $\{D_{e_1\cdots e_n}\}$ of $\mathfrak{S}_{r+1}(O)$ with respect to $\{t_1, \cdots, t_n\}$. Then we have the following

PROPOSITION 2. *Suppose that* O *is a regular local ring of rank* n. *Then we have* $\mathfrak{D}_r(O)=\mathfrak{S}_r(O)\oplus \sum_{i=1}^{n} kE_{i,r}$. *In particular* $\dim_k \mathfrak{D}_r(O)$ *is* $p^{nr}+n-1$.

PROOF. First we consider the case $r=0$. Then we can easily see that $D(k+\mathfrak{m}^2)=0$, and that $\mathfrak{D}_0(O)$ is isomorphic to $(\mathfrak{m}/\mathfrak{m}^2)^*$, it is well known in this case that $\{E_{1,0}, \cdots, E_{n,0}\}$ is a basis of $\mathfrak{D}_0(O)$ over k. In general cases $r>0$, we put $O_r=kO^{p^r}$. Then the restriction to O_r of D in $\mathfrak{D}_r(O)$ is an element D' in $\mathfrak{D}_0(O_r)$, and $\mathfrak{D}_0(O_r)$ is generated by the restrictions $E_{1,r}|_{O_r}, \cdots, E_{n,r}|_{O_r}$ of $E_{1,r}, \cdots, E_{n,r}$, since the maximal ideal of O_r is generated by $t_1^{p^r}, \cdots, t_n^{p^r}$. Therefore for any D in $\mathfrak{D}_r(O)$ there exist $\beta_1, \cdots, \beta_n$ in k such that the restriction to O_r of $D-\sum_{i=1}^{n} \beta_i E_{i,r}$ is 0. Then $D-\sum_{i=1}^{n} \beta_i E_{i,r}$ is in $\mathfrak{S}_r(O)$ by definition. This shows that $\mathfrak{D}_r(O)$ is the sum $\mathfrak{S}_r(O)+\sum_{i=1}^{n} kE_{i,r}$. Moreover if $E=D+\sum_{i=1}^{n}\alpha_i E_{i,r}=0$ for D in $\mathfrak{S}_r(O)$ and α_i in k, we have $E(t_j^{p^r})=D(t_j^{p^r})+\sum_{i=1}^{n} \alpha_i E_{i,r}(t_j^{p^r})=\alpha_j=0$. This means that the sum is direct. q.e.d.

Remark. Since $\{\mathfrak{m}_r | r=1, 2, \cdots, n, \cdots\}$ is a basis of the neighbourhoods at 0 in 0 with respect to the $\mathfrak{m}$-adic topology, we can see that any element D in the dual space O^* of O is in $\mathfrak{S}_r(O)$ for some r if and only if D is a continuous mapping of O with $\mathfrak{m}$-adic topology into a discrete space k which vanishes on k.

§ 2. Semi-derivations of a function field

Let k be a field of a positive characteristic p and K a finitely generated and separable extension of k. We shall denote by K_r the subfield kK^{p^r} of K for a positive integer r.

We understand by *a semi-derivation* D *of height* r *of* K *over* k a k-linear endomorphism of K satisfying the following conditions: i) if $x \in K_r$, then $D(x)$ is in K_r, and ii) $D(xy)=D(x)y+xD(y)$ for $x \in K$ and $y \in K_r$. Moreover D is called *special* if $D(K_r)=0$. We shall denote by $\mathfrak{D}_r(K/k)$ the set of the semi-derivations of height r of K over k and by $\mathfrak{S}_r(K/k)$ the subset of $\mathfrak{D}_r(K/k)$

consisting of all the special ones. Let x be an element of K_r and D an element of $\mathfrak{D}_r(K/k)$. Then the linear mapping xD defined by $(xD)(y)=x(D(y))$ for $y\in K$ is in $\mathfrak{D}_r(K/k)$ and hence we see that $\mathfrak{D}_r(K/k)$ is a vector space over K_r. Similarly $\mathfrak{S}_r(K/k)$ is a vector space over K.

The following lemma is a direct consequence of definition.

LEMMA 3. (i) *For any integer $r\geq 0$, we have*

$$\mathfrak{S}_r(K/k)\subset\mathfrak{D}_r(K/k)\subset\mathfrak{S}_{r+1}(K/k).$$

(ii) *Let D be a mapping of K into itself. Then D is in $\mathfrak{S}_r(K/k)$ if and only if D is K_r-linear endomorphism of K such that $D(1)=0$.*

Let n be the transcendental degree of K over k and $\{x_1, \cdots, x_n\}$ a separating transcendence basis of K over k. Then we see that $K=K_r(x_1, \cdots, x_n)=K_r[x_1, \cdots, x_n]$ and that $\{\prod_{i=1}^{n} x_i^{e_i} \mid 0\leq e_i<p^r\}$ is a linear basis of K over K_r. Let $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r\}$ be the dual basis in the dual space of K over K_r with respect to the above basis $\{\prod_{i=1}^{n} x_i^{e_i}\}$ of K. Then $D^{(r)}_{e_1\cdots e_n}$ is in $\mathfrak{S}_r(K/k)$ if and only if $e_i\neq 0$ for some i by Lemma 3. It is easy to see that $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r, \sum_{i=1}^{n} e_n>0\}$ is a basis of $\mathfrak{S}_r(K/k)$ over K. Therefore we have the following

PROPOSITION 3. *Let K be a finitely generated and separable extension of the transcendental degree n over k, and $\{x_1, \cdots, x_n\}$ a separating transcendence basis of K over k. For $0\leq e_i<p^r$ and $\sum_{i=1}^{n} e_i>0$ let $D^{(r)}_{e_1\cdots e_n}$ be the K_r-linear endomorphism of K such that $D^{(r)}_{e_1\cdots e_n}(x_1^{e_1}\cdots x_n^{e_n})=1$ and $D_{e_1\cdots e_n}(x_1^{e_1'}\cdots x_n^{e_1'})=0$ for $0\leq e_i'<p^r$ and $(e_1, \cdots, e_n)\neq(e_1', \cdots, e_n')$. Then $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r, \sum_{i=1}^{n} e_i>0\}$ is a basis of $\mathfrak{S}_r(K/k)$ and hence the dimension of $\mathfrak{S}_r(K/k)$ over K is $p^{nr}-1$. Moreover K_r is the set of the elements x is K such that $D(x)=0$ for any D in $\mathfrak{S}_r(K/k)$.*

The set $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r, \sum e_i>0\}$ will be called *the canonical basis of $\mathfrak{S}_r(K/k)$ with respect to the separating transcendence basis $\{x_1, \cdots, x_n\}$ of K over k.* Note that $\{D^{(r)}_{e_1\cdots e_n}\}$ is not a subset of $\{D^{(r+1)}_{e_1\cdots e_n}\}$.

PROPOSITION 4. (*Barsotti*) *Let K be a finitely generated and separable extension of k and H a finite separable extension of K. Then for any D in $\mathfrak{D}_r(K/k)$ there exists unique element D' in $\mathfrak{D}_r(H/k)$ such that the restriction of D' to K is D. Moreover D is in $\mathfrak{S}_r(K/k)$ if and only if D' is in $\mathfrak{S}_r(H/k)$.*

This is Lemma 1. 3 in [1]. But we give an outline of Barsotti's proof for the convenience of the reader. There exists an element x in H such that $H=K(x)=K[x]$, and then for any positive integer r, we have $H=K(x^{p^r})=K[x^{p^r}]$. If y is in H, y is uniquely expressed as a linear combination $\sum_{j=0}^{n-1} a_j x^{jp^r}$,

where $n=[H: K]$ and $a_j \in K$. Therefore D' is defined by $D'(y)=\sum_{j=0}^{n-1} D(a_j)x^{jp^r}$ for any D in $\mathfrak{S}_r(K/k)$, since D' should be an H_r-linear endomorphism of H. Then we can easily see that D' is in $\mathfrak{S}_r(H/k)$. If D is in $\mathfrak{D}_r(K/k)$, D is in $\mathfrak{S}_{r+1}(K/k)$ and hence there exists D' in $\mathfrak{S}_{r+1}(H/k)$ such that the restriction of D' to K is equal to D. It can be seen that D' is in $\mathfrak{D}_r(H/k)$.

LEMMA 4. *Let F be a field of a positive characteristic p and K a purely transcendental extension of one variable x over F. Then there exists a semi-derivation D_r of height r of K over F such that $D_r(x^\alpha)=ax^{\alpha-p^r}$ for any positive integer α, where $\alpha=ap^r+b$ and $0\leq b<p^r$.*

PROOF. Since $\{x^\alpha \mid \alpha=0, 1, 2, \cdots\}$ is a basis of the polynomial ring $F[x]$ over F, there exists an F-linear endomorphism D_r of $F[x]$ satisfying the condition in our lemma. Then we see that $D_r(fg)=D_r(f)g+fD_r(g)$ and $D(g)$ is in $F[x^{p^r}]$ for f in $F[x]$ and g in $F[x^{p^r}]$. In fact, for $\beta=a'p^r$, we have $D_r(x^{\alpha+\beta})=(a+a')x^{\alpha+\beta-p^r}=ax^{\alpha+\beta-p^r}+a'x^{\alpha+\beta-p^r}=D_r(x^\alpha)x^\beta+x^\alpha D_r(x^\beta)$. Now we extend D_r to an F-linear endomorphism of $K=F(x)$ as follows. For any y in K, there exist f in $F[x]$ and g in $F[x^{p^r}]$ such that $y=f/g$. We put $D_r(y)=D_r(f)g-fD_r(g)/g^2$. If $y=f'/g'$ is another expression of y where f' in $F[x]$ and g' in $F[x^{p^r}]$, we have $fg'=f'g$ and hence $D_r(f)g'+D_r(g')f=D_r(f')g+D_r(g)f'$ as shown in the above. From this relation we can easily obtain the equality $D_r(f)g-D_r(g)f/g^2=D_r(f')g'-D_r(g')f'/g'^2$. This means that $D_r(y)$ is independent of the choice of f and g. A similar routine calculation shows that we have $D_r(yz)=D_r(y)z+yD_r(z)$ for y in K and z in $F(x^{p^r})=K_r$. This completes the proof. q. e. d.

Let K be a finitely generated extension of k with a separating transcendence basis $\{x_1, \cdots, x_n\}$ as before. We define $E_{i,r}$ in $\mathfrak{S}_{r+1}(K/k)$ as follows:

$$(*) \qquad E_{i,r}(\prod_{j=1}^{n} x_j^{e_j})=a_i x_i^{e_i-p^r}\prod_{j\neq i} x_j^{e_j},$$

where $0\leq e_j<p^{r+1}$, $\sum_{j=1}^{n} e_j>0$, $e_i=a_ip^r+b_i$, and $0\leq b_i<p^r$. Since $\{\prod_{j=1}^{n} x^{e_j} \mid 0\leq e_j<p^{r+1}\}$ is a linear basis of K over K_{r+1}, we easily see that there exists the exact one $E_{i,r}$ in $\mathfrak{S}_{r+1}(K/k)$ satisfying the above condition by Lemma 3.

PROPOSITION 5. *Let $E_{i,r}$ be as above. Then $E_{i,r}$ is in $\mathfrak{D}_r(K/k)$ for $i=1, 2, \cdots, n$.*

PROOF. Let K_0 be the subfield $k(x_1, \cdots, x_n)$ generated by the separating transcendence basis $x_1, \cdots, x_n$ over k and F the subfield $k(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n)$ of K_0 generated by $n-1$ elements $x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n$ over k. Then K_0 is a purely transcendental extension of one variable x_i over F. If D_r is the semi-derivation of height r of K_0 over F defined as in Lemma 4, it is clear that D_r is in $\mathfrak{D}_r(K_0/k)$ and is the restriction of $E_{i,r}$ to K_0. By Proposition 4

$E_{i,r}$ is the unique extension of D_r to K and is in $\mathfrak{D}_r(K/k)$, since K is a finite separable extension of K_0. q. e. d.

PROPOSITION 6. *Let K be a finitely generated and separable extension of transcendental degree n over k with a separating transcendence basis $\{x_1, \cdots, x_n\}$. If $E_{i,r}$ $(i=1, 2, \cdots, n)$ is the element of $\mathfrak{D}_r(K/k)$ defined by the formula (*), $E_{1,r}, \cdots, E_{n,r}$ are linearly independent over K_r, and $\mathfrak{D}_r(K/k)$ is equal to the direct sum $\mathfrak{S}_r(K/k) \oplus \sum_{i=1}^{n} K_r E_{i,r}$.*

PROOF. Since $\{x_1, \cdots, x_n\}$ is a separating transcendence basis of K over k, $\{x_1^{p^r}, \cdots, x_b^{p^r}\}$ is that of K_r over k and it is well known that there exists an ordinary derivation C_i of K_r over k such that $C_i(x_j^{p^r})=\delta_{ij}$ for each $i=1, 2, \cdots, n$ (cf. [8]). They are a basis of $\mathfrak{D}_0(K_r/k)$ over K_r and the restriction of $E_{i,r}$ to K_r is C_i. If D is any element of $\mathfrak{D}_r(K/k)$, the restriction of D to K_r is in $\mathfrak{D}_0(K_r/k)$, and hence the restriction of $E=D-\sum_{j=1}^{n} \alpha_j E_{j,r}$ to K_r is 0, where $\alpha_j=D(x_j^{p^r}) \in K_r$. Therefore E is in $\mathfrak{S}_r(K/k)$. This shows that $\mathfrak{D}_r(K/k)$ is the sum $\mathfrak{S}_r(K/k)$ and $\sum_{i=1}^{n} K_r E_{i,r}$. On the other hand if $E+\sum_{i=1}^{n} \alpha_i E_{i,r}$ is 0 for $\alpha_i \in K_r$ and $E \in \mathfrak{S}_r(K/k)$, we have $E(x_j^{p^r})+\sum_{i=1}^{n} \alpha_i E_{i,r}(x_j^{p^r})=\alpha_j=0$ for each j, and hence $E=0$. This means that $E_{1,r}, \cdots, E_{n,r}$ are linearly independent over K_r, and that the sum $\mathfrak{D}_r(K/k)=\mathfrak{S}_r(K/k)+\sum_{i=1}^{n} K_r E_{i,r}$ is a direct one. q. e. d.

LEMMA 5. *Let K, k, $\{x_1, \cdots, x_n\}$ and $E_{i,r}$ be as above. Then we have $E_{i,h}E_{j,k}=E_{j,k}E_{i,h}$ for $1 \leq i, j \leq n$ and $h, k \geq 0$.*

PROOF. Since $E_{i,h}$ and $E_{j,k}$ are in $\mathfrak{S}_r(K/k)$ for $r=\max\{h, k\}+1$, $E_{i,h}E_{j,k}$ and $E_{j,k}E_{i,h}$ are also in $\mathfrak{S}_r(K/k)$ by Lemma 3. (ii). Therefore we may assume that $K=k(x_1, \cdots, x_n)$ by Proposition 4. Then if $i \neq j$, it is clear from definition that $E_{i,h}E_{j,k}$ is equal to $E_{j,k}E_{i,h}$. Suppose that $i=j$ and $h>k$. If we expand a positive integer α as a p-adic series $\alpha=\sum_s \lambda_s p^s (0 \leq \lambda_s < p)$, we can easily see that $E_{i,t}(x_i^{\alpha})=\lambda_t x_i^{\alpha-p^t}$ and $\alpha-p^t=(\lambda_t-1)p^t+\sum_{s \neq t} \lambda_s p^s$. Therefore if at least one of λ_h and λ_k is zero, we see that $E_{i,h}E_{i,k}(x_i^{\alpha})=E_{i,k}E_{i,h}(x_i^{\alpha})=0$, and if otherwise, we have $E_{i,h}E_{i,k}(x_i^{\alpha})=E_{i,k}E_{i,h}(x_i^{\alpha})=\lambda_h\lambda_k x_i^{\alpha-p^h-p^k}$. This proves our lemma. q. e. d.

Let e_i be an integer such that $0 \leq e_i < p^r$ and expand it as a p-adic series $\sum_{h=1}^{r-1} \lambda_{hi} p^h (0 \leq \lambda_{hi} < p)$. Lemma 5 shows that the product $\prod_{h=0}^{r-1} \prod_{i=1}^{n} E_{i,h}^{\lambda_{h,i}}$ is well defined, and we denote it by $E_{e_1 \cdots e_n}$. Then we have the following

PROPOSITION 7. *Let K be a finitely generated and separable extension of k*

with a separating transcendence basis $\{x_1, \cdots, x_n\}$. *Let* $\{D^{(r)}_{e_1\cdots e_n}\}$ *be the canonical basis of* $\mathfrak{S}_r(K/k)$ *with respect to* $\{x_1, \cdots, x_n\}$, *and* $\{E_{e_1\cdots e_n}\}$ *the elements of* $\mathfrak{S}_r(K/k)$ *defined in the above. Then we have*

$$D^{(r)}_{e_1\cdots e_n}=(\prod_{h=0}^{r-1}\prod_{i=1}^{n}\lambda_{hi}!)^{-1}E_{e_1\cdots e_n}+\sum_{(e')}f_{e'_1\cdots e'_n}(x_1, \cdots, x_n)E_{e'_1\cdots e'_n},$$

where $\sum_{(e')}$ *runs over all* $(e'_1\cdots e'_n)$ *such that* $e_i\leq e'_i$ *for each* i *and* $\sum_{i=1}^{n}e_i<\sum_{i=1}^{n}e'_i$, *and where* $f_{e'_1\cdots e'_n}(X_1, \cdots, X_n)$ *is a polynomial in* $X_1, \cdots, X_n$ *with coefficients in the prime field of characteristic* p.

PROOF. It is easily seen that $E_{e_1\cdots e_n}(x_1^{e_1}\cdots x_n^{e_n})=\prod_{h=0}^{r-1}\prod_{i=1}^{n}\lambda_{hi}!$. If $e_i>e'_i=\sum_{h=1}^{r-1}\lambda'_{hi}p^h(0\leq\lambda'_{hi}<p)$, there exists an integer s such that $\lambda_{ji}=\lambda'_{ji}$ for $j\geq s+1$ and $\lambda_{si}>\lambda'_{si}$, and hence we have

$$\begin{aligned}\prod_{h=0}^{r-1}E_{i,h}^{\lambda_{hi}}(x_i^{e'_i})&=\prod_{h=s+1}^{r-1}\lambda_{hi}!\prod_{h=0}^{s}E_{i,h}^{\lambda_{hi}}(x_i^{e'_i-\sum_{h\geq s}\lambda_{hi}p^h})\\&=\prod_{h=s+1}^{r-1}\lambda_{hi}!\prod_{h=0}^{s}E_{i,h}^{\lambda_{hi}}(x_i^{\sum_{h=0}^{s}\lambda'_{hi}p^h})\\&=0\end{aligned}$$

On the other hand let $g_{e'_1\cdots e'_n}(X_1, \cdots, X_n)$ be the polynomial in $X_1, \cdots, X_n$ with coefficients in the prime field of characteristic p such that

$$(\prod_{h=0}^{r-1}\prod_{i=1}^{n}\lambda_{hi}!)^{-1}E_{e_1\cdots e_n}(x_1^{e'_1}\cdots x_n^{e'_n})=g_{e'_1\cdots e'_n}(x_1, \cdots, x_n).$$

Then the above equality shows that $g_{e'_1\cdots e'_n}(X_1\cdots X_n)=0$ if $e'_i<e_i$ for some i. Therefore we see easily that

$$D^{(r)}_{e_1\cdots e_n}=(\prod_{h=0}^{r-1}\prod_{i=1}^{n}\lambda_{hi}!)^{-1}E_{e_1\cdots e_n}+\sum_{(e')}g_{e'_1\cdots e'_n}(x_1\cdots x_n)D^{(r)}_{e'_1\cdots e'_n}$$

for any $(e_1\cdots e_n)$ satisfying $0\leq e_i<p^r$. Proposition 7 is a direct consequence of these equalities. q. e. d.

COROLLARY. *Let* $\{E_{e_1\cdots e_n}\mid 0\leq e_i<p^r, \sum_{i=1}^{n}e_i>0\}$ *be as in Proposition* 7. *Then* $\{E_{e_1\cdots e_n}\}$ *is a basis of* $\mathfrak{S}_r(K/k)$ *over* K.

§ 3. Regular semi-derivations at points of an algebraic variety

Let X be an algebraic variety over a perfect field k of a positive characteristic p, and let K be the field of the rational functions of X over k. Then X may be identified with an integral algebraic scheme over k. If x is a point

of X, we shall identify the stalk $\mathcal{O}_{x,X}$ of the structure sheaf $\mathcal{O}_X$ of X at x with a subring of K. Then we say that an element D in $\mathfrak{D}_r(K/k)$ is *a regular semi-derivation of X at x* if $D(\mathcal{O}_{x,X})$ is contained in $\mathcal{O}_{x,X}$. We shall denote by $\mathfrak{D}_r(X, x)$ the subset of the semi-derivations in $\mathfrak{D}_r(K/k)$ regular at x, and by $\mathfrak{S}_r(X, x)$ the subset of $\mathfrak{D}_r(X, x)$ consisting of special ones. Then we see that $\mathfrak{S}_r(X, x)$ is an $\mathcal{O}_{x,X}$-module and $\mathfrak{D}_r(X, x)$ is an $\mathcal{O}^{(r)}$-module, where $\mathcal{O}^{(r)}$ is the intersection of $\mathcal{O}_{x,X}$ and K_r.

PROPOSITION 8. *Let x be a point of X rational over k. Assume that x is non-singular, and let $\{t_1, \cdots, t_n\}$ be a regular system of parameters of $\mathcal{O}_{x,X}$. Then $\{t_1, \cdots, t_n\}$ is a separating transcendence basis of K over k and any element of the canonical basis $\{D^{(r)}_{e_1\cdots e_n}\}$ of $\mathfrak{S}_r(K/k)$ with respect to it is regular at x.*

PROOF. It is well known that $\{t_1 \cdots t_n\}$ is a separating transcendence basis of K over k. For example see [8]. Let $R=k[t_1, \cdots, t_n]$ be the subring of $\mathcal{O}_{x,X}$ generated by $t_1, \cdots, t_n$ over k and L the quotient field of R. Then the restriction $D^{(r)}_{e_1\cdots e_n}|_L$ of $D^{(r)}_{e_1\cdots e_n}$ to L is in $\mathfrak{S}_r(L/k)$ by the definition of the canonical basis, and we can see easily that $D^{(r)}_{e_1\cdots e_n}(R)$ is contained in R. Moreover if we denote by $\mathfrak{a}_s$ the ideal of R generated by n elements $t_1^{p^s}, \cdots, t_n^{p^s}$, we see $D^{(r)}_{e_1\cdots e_n}(\mathfrak{a}_s)\subset\mathfrak{a}_s$ for $s\geq r$ because of K_r-linearity of $D^{(r)}_{e_1\cdots e_n}$. Therefore we see that $D^{(r)}_{e_1\cdots e_n}|_R$ is a continuous k-linear endomorphism of R with the $\mathfrak{a}_0$-adic topology and hence it has unique extension $\bar{D}_{e_1\cdots e_n}: \bar{R}\to\bar{R}$, where $\bar{R}$ is the $\mathfrak{a}_0$-adic completion of R. We can easily see that $\bar{D}_{e_1\cdots e_n}$ is a $k\bar{R}^{p^r}$-linear endomorphism of $\bar{R}$, since $D^{(r)}_{e_1\cdots e_n}|_R$ is $k[x_1^{p^r}, \cdots, x_n^{p^r}]$-linear by Lemma 3. By the same way as in the proof of Lemma 4 we extend $\bar{D}_{e_1\cdots e_n}$ to $\bar{K}_r$-endmorphism of K, where $\bar{K}$ is the quotient field of $\bar{R}$. If we also denote this extension to $\bar{K}$ by $\bar{D}_{e_1\cdots e_n}$, $\bar{D}_{e_1\cdots e_n}$ is in $\mathfrak{S}_r(K/k)$ by Lemma 3. On the other hand $\bar{R}$ is also the $\mathfrak{m}_{x,X}$-adic completion of $\mathcal{O}_{x,X}$, and hence we can consider $\mathcal{O}_{x,X}$ (resp. K) as a subring of $\bar{R}$ (resp. as a subfield of K). If K is generated by an element x of K ove L, we have $K=L(x^{p^r})=L[x^{p^r}]$. Since $\bar{D}_{e_1\cdots e_n}$ is $\bar{K}_r$-linear and $\bar{D}_{e_1\cdots e_n}(L)$ is in L, we have $\bar{D}_{e_1\cdots e_n}(K)\subset K$. This means that the restriction $\bar{D}_{e_1\cdots e_n}|_K$ of $\bar{D}_{e_1\cdots e_n}$ to K is in $\mathfrak{S}_r(K/k)$ and hence is equal to $D^{(r)}_{e_1\cdots e_n}$ by Lemma 3. It is well known that $\mathcal{O}_{x,X}$ is the intersection of K and the $\mathfrak{m}_{x,X}$-adic completion $\bar{R}$ of $\mathcal{O}_{x,X}$. Therefore if y is any element of $\mathcal{O}_{x,X}$, $D^{(r)}_{e_1\cdots e_n}(y)=\bar{D}_{e_1\cdots e_n}(y)$ is contained in $\mathcal{O}_{x,X}=K\cap\bar{R}$. This means that $D^{(r)}_{e_1\cdots e_n}$ is regular at x. q. e. d.

COROLLARY. *Let X, x, $\mathcal{O}_{x,X}$ and $\{t_1, \cdots, t_n\}$ be as in Proposition 8. Then D in $\mathfrak{D}_r(K/k)$ (resp. in $\mathfrak{S}_r(K/k)$) is regular at x if and only if $D(t_1^{e_1}\cdots t_n^{e_n})$ and $D(t_j^{p^r})$ (resp. $D(t_1^{e_1}\cdots t_n^{e_n})$) are contained in $\mathcal{O}_{x,X}$ for $0\leq e_i<p^r$ and $j=1, 2, \cdots, n$.*

PROOF. There exists $\alpha_{e_1\cdots e_n}$ and β_j in K for $0\leq e_i<p^r$ and $j=1, 2, \cdots, n$ such that $D=\sum\alpha_{e_1\cdots e_n}D^{(r)}_{e_1\cdots e_n}+\sum\beta_jE_{j,r}$ by Proposition 6, where $\{D^{(r)}_{e_1\cdots e_n}\}$ is the canonical basis of $\mathfrak{S}_r(K/k)$ over K with respect to $\{t_1, \cdots, t_n\}$ and $\{E_{j,r}\}$ is the same as in Proposition 6. Then we have $D(t_1^{e_1}\cdots t_n^{e_n})=\alpha_{e_1\cdots e_n}$ and $D(t_j^{p^r})=\beta_j$. On the other hand $E_{j,r}$ is a linear combination of the canonical basis $\{D^{(r+1)}_{e_1\cdots e_n}\}$

of $\mathfrak{S}_{r+1}(K/k)$ with respect to $\{t_1, \cdots, t_n\}$ with coefficient in the polynomial ring in $t_1, \cdots, t_n$ over the prime field of the characteristic p. Therefore $E_{j,r}$ is regular at x for each $j=1, 2, \cdots, n$. This means by Proposition 8 that D is regular at x if and only if $\alpha_{e_1\cdots e_n}$ and β_j are contained in $\mathcal{O}_{x,X}$ for $0 \leq e_i \leq p^r$ and $j=1, 2, \cdots, n$. This proves our assertion for the case D in $\mathfrak{D}_r(K/k)$. The other case also can be obtained in the similar way. q. e. d.

PROPOSITION 9. *Let X, x, $\mathcal{O}_{x,X}$ and $\{t_1, \cdots, t_n\}$ be as in Proposition* 8. *Let $\{D^{(r)}_{e_1\cdots e_n} \mid 0 \leq e_i < r, \sum_{i=1}^{n} e_i > 0\}$ and $\{E_{i,r} \mid i=1, 2, \cdots, n\}$ be as in Propositions* 3 *and* 5 *for the separating transcendence basis $\{t_1, \cdots, t_n\}$ of K over k. Then $\mathfrak{S}_r(X, x)$ is a free $\mathcal{O}_{x,X}$-module of rank $p^{nr}-1$ with a free basis $\{D^{(r)}_{e_1\cdots e_n}\}$ and $\mathfrak{D}_r(X, x)$ is equal to $\mathfrak{S}_r(X, x) \oplus \sum_{i=1}^{n} \mathcal{O}^{(r)} E_{i,r}$.*

PROOF. By Corollary of Proposition 8 we see easily that $\{D^{(r)}_{e_1\cdots e_n} \mid 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a free basis of $\mathfrak{S}_r(X, x)$ over $\mathcal{O}_{x,X}$. On the other hand each $E_{i,r}$ is regular at x by the definition and Corollary of Proposition 8, and any element E contained in $\mathfrak{D}_r(X, x)$ is writen as a sum $D + \sum_{i=1}^{n} \alpha_i E_{i,r}$, where D is in $\mathfrak{S}_r(K/k)$ and each α_i is in K. Then $E(t_j^{p^r})$ is equal to α_i and hence α_i must be contained in $K_r \cap \mathcal{O}_{x,X} = \mathcal{O}^{(r)}$. From this D is regular at x. Therefore we see easily see that $\mathfrak{D}_r(X, x)$ is the direct sum of $\mathfrak{S}_r(X, x)$ and $\sum_{i=1}^{n} \mathcal{O}^{(r)} E_{i,r}$.

q. e. d.

For the later use we give an application of Proposition 9.

LEMMA 6. *Let X and K be as above. Assume that k is algebraically closed, and let D be a semi-derivation of K over k. Then there exists a dense open subset U of X such that D is regular at any closed point of U.*

PROOF. Let $\{t_1, \cdots, t_n\}$ be a separating transcendence basis of K over k. Then there exists an open subset V of X such that each t_i is in $\mathcal{O}_{x,X}$ at any point x in V for $i=1, 2, \cdots, n$ and that $\{t_1 - t_1(x), \cdots, t_n - t_n(x)\}$ is a regular system of parameters of the local ring $\mathcal{O}_{x,X}$ for any non-singular closed point x in V. (cf. Chap. VIII. in [8]). On the other hand there exist $p^{nr}-1$ elements $\alpha_{e_1\cdots e_n} (0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0)$ such that $D = \sum \alpha_{e_1\cdots e_n} D^{(r)}_{e_1\cdots e_n}$, where $\{D^{(r)}_{e_1\cdots e_n}\}$ is the canonical basis of $\mathfrak{S}_r(K/k)$ with respect to $\{t_1 \cdots t_n\}$. Let W be the open subset of X such that each $\alpha_{e_1\cdots e_n}$ is in $\mathcal{O}_{x,X}$ at any point x in w for $0 \leq e_i < p^r$ and $\sum_{i=1}^{n} e_i > 0$, and such that any point in W is non-singular. Then $U = V \cap W$ is a dense open subset of X, and, by Proposition 9, it is easy to see that U satisfies our assertion, because the canonical basis of $\mathfrak{S}_r(K/k)$ with respect to $\{t_1 - t_1(x), \cdots, t_n - t_n(x)\}$ for x in U is nothing else than $\{D^{(r)}_{e_1\cdots e_n}\}$. q. e. d.

Let Y be another algebraic variety over k with the field L of the rational functions over k. If there exists a dominant k-morphism f of X into Y, we may identify L with the subfield $f^*(L)$ of K. Then a semi-derivation D of K over k does not generally induce that of L over k, because the image of L by D may not be contained in L. However we have the following

LEMMA 7. *Let K and L be as above, and let $\{t_1, \cdots, t_n\}$ be a separating transcendence basis of L over k. Then the restriction $D|_L$ of a semi-derivation D in $\mathfrak{S}_r(K/k)$ to L is contained in $\mathfrak{S}_r(L/k)$, if each element $D(t_1^{e_1}\cdots t_n^{e_n})$ is in L for $0 \leq e_i < p^r$.*

PROOF. If we denote by L_r the subfield kL^{p^r} of L generated by the p^r-th powers of L over k, we have $L=L_r(t_1, \cdots, t_n)=L_r[t_1, \cdots, t_n]$ and $\{\prod_{i=1}^{n} t_i^{e_i} \mid 0 \leq e_i < p^r\}$ is a linear basis of L over L_r. On the other hand the restriction $D|_L$ of D to L is L_r-linear, since D is K_r-linear by Lemma 3. Therefore $D(L)$ is contained in L by the assumption and $D|_L$ is in $\mathfrak{S}_r(L/k)$. q. e. d.

LEMMA 8. *Let K, L and $\{t_1, \cdots, t_n\}$ be as in Lemma 7, and let D be an element of $\mathfrak{D}_r(K/k)$. Then if each $D(t_1^{e_1}\cdots t_n^{e_n})$ is in L for $0 \leq e_i < p^r$ and if each $D(t_i^{p^r})$ is in L_r for $i=1, 2, \cdots, n$, the restriction $D|_L$ of D to L is contained in $\mathfrak{D}_r(L/k)$.*

PROOF. If e_i is an integer such that $0 \leq e_i < p^{r+1}$, we put $e_i = \alpha_i p^r + \beta_i (0 \leq \alpha_i < p,\ 0 \leq \beta_i < p^r)$. Then we have

$$D(\prod_{i=1}^{n} t_i^{e_i}) = D(\prod_{i=1}^{n} t_i^{\alpha_i p^r}) \prod_{i=1}^{n} t_i^{\beta_i} + \prod_{i=1}^{n} t_i^{\alpha_i p^r} D(\prod_{i=1}^{n} t_i^{\beta_i}),$$

since $t_i^{p^r}$ is in K_r for each $i=1, 2, \cdots, n$. By definition $D|_{K_r}$ is an ordinary derivation of K_r over k and hence we have

$$D(\prod_{i=1}^{n} t_i^{\alpha_i p^r}) = \sum_{i=1}^{n} \alpha_i t_i^{(\alpha_i - 1)p^r} \prod_{i \neq j} t_j^{\alpha_j p^r} D(t_i^{p^r}).$$

This means by the assumption that each $D(t_1^{e_1}\cdots t_n^{e_n})$ is contained in L for $0 \leq e_i < p^{r+1}$. On the other hand D is an element of $\mathfrak{S}_{r+1}(K/k)$ and hence $D|_L$ is contained in $\mathfrak{S}_{r+1}(L/k)$ by Lemma 7. Therefore the proof of Lemma 8 will be complete, if we show that $D(L_r)$ is contained in L_r. Let F be the subfield $k(t_1, \cdots, t_n)$ of L generated by $t_1, \cdots, t_n$ over k, and assume that L is generated by an element t over F. Then any element u in L can be written uniquely as a polynomial $\sum_{j=0}^{m-1} a_j t^{jp^{r+1}}$ of $t^{p^{r+1}}$ with coefficients a_j in F, where $m=[L: F]$, and u is in L^{p^r} if and only if each a_j is in F^{p^r} for $j=0, 1, \cdots, m-1$. Since D is in $\mathfrak{D}_r(K/k)$, we have $D(u)=\sum_{j=0}^{m-1} D(a_j) t^{jp^{r+1}}$. Therefore it is sufficient to show that $D(a_j)$ is in L_r for a_j in F^{p^r}. But this follows form the fact that the restriction $D|_{F^{p^r}}$ of D to F^{p^r} is an ordinary derivation of F^{p^r} to L and

from the assumption that $D(t_i^{p^r})$ is in L_r. q. e. d.

Let D be a semi-derivation of X regular at a rational point x in X over k. Then we can attach to it a local semi-derivation D_x on the local ring $\mathcal{O}_{x,X}$ as follows. If π_x is the natural homomorphism of $\mathcal{O}_{x,X}$ onto the residue field $k=\mathcal{O}_{x,X}/\mathfrak{m}_{x,X}$, we define D_x by the formula $D_x(f)=\pi_x(D(f))$ for any element f of $\mathcal{O}_{x,X}$. In the following we write often $D(f)(x)$ instead of $\pi_x(D(f))$. We can easily see that D_x is of height r (resp. of height r and special) if D is of height r (resp. of height r and special). This local semi-derivation D_x will be called *the local component of D at x*. We denote also by π_x the mapping of D to its local component D_x at x. The following proposition is a direct consequence of definitions, and Propositions 1, 2 and 9.

PROPOSITION 10. *Let the nototions be as in Proposition* 9. *Then the image of a free basis* $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r, \sum_{i=1}^{n} e_i>0\}$ *of* $\mathfrak{S}_r(X, x)$ *over* $\mathcal{O}_{x,X}$ *by the mapping* π_x *is a basis of* $\mathfrak{S}_r(\mathcal{O}_{x,X})$ *over* k *and the images of* $\{D^{(r)}_{e_1\cdots e_n} \mid 0\leq e_i<p^r, \sum_{i=1}^{n} e_i>0\}$ *and* $E_{i,r}(i=1, 2, \cdots, n)$ *are a basis of* $\mathfrak{D}_r(\mathcal{O}_{x,X})$ *over* k. *Moreover the kernel of the restriction of* π_x *to* $\mathfrak{S}_r(X, x)$ *is* $\mathfrak{m}_{x,X}\mathfrak{S}_r(X, x)$, *where* $\mathfrak{m}_{x,X}$ *is the maximal ideal of* $\mathcal{O}_{x,X}$.

Next we give a generalization of a tangential mapping for usual local derivations associated with a morphism of an algebraic variety to another one. Let X, Y be algebraic varieties over k and f a k-morphism of X to Y. Let x be a non-singular closed point of X rational over k and y the image $f(x)$ of x by f. We assume that y is also non-singular, and denote by f^* the canonical homomorphism of $\mathcal{O}_{y,Y}$ to $\mathcal{O}_{x,X}$ associated with f. If D is a local semi-derivation on $\mathcal{O}_{x,X}$, we denote by $f_*(D)$ the composite mapping $D\circ f^*$. Then $f_*(D)$ is a k-linear mapping of $\mathcal{O}_{y,Y}$ to k, and $f_*(D)$ is in $\mathfrak{D}_r(\mathcal{O}_{y,Y})$ (resp. in $\mathfrak{S}_r(\mathcal{O}_{y,Y})$) if D is in $\mathfrak{D}_r(\mathcal{O}_{x,X})$ (resp. in $\mathfrak{S}_r(\mathcal{O}_{x,X})$). f_* will be called *the tangential mapping at x associated with the morphism f of X to Y.*

PROPOSITION 11. *Let X, Y, f, x and $y=f(x)$ be as above. Suppose that f is dominant and that if K (resp. L) is the field of the rational functions of X (resp. of Y), L, $\mathcal{O}_{x,X}$ and $\mathcal{O}_{y,Y}$ are identified with subsets of K. Let $\{t_1, \cdots, t_n\}$ be a regular system of parameters of $\mathcal{O}_{y,Y}$. Then if D is in $\mathfrak{S}_r(K/k)$ (resp. in $\mathfrak{D}_r(K/k)$) and if $D(t_1^{e_1}\cdots t_n^{e_n})$ (resp. $D(t_1^{e_1}\cdots t_n^{e_n})$ and $D(t_j^{p^r})$) are in $\mathcal{O}_{y,Y}$ for $0\leq e_i<p^r$ (resp. $0\leq e_i<p^r$ and $j=1, 2, \cdots, n$), the restriction $D'=D\mid_L$ of D to L is regular at y, and we have $D'_y=f_*(D_x)$ if D is regular at x.*

PROOF. By Lemma 7 (resp. Lemma 8) we see that $D'=D\mid_L$ is in $\mathfrak{S}_r(L/k)$ (resp. in $\mathfrak{D}_r(L/k)$), and hence by Corollary of Proposition 8 D' is regular at y. The last assertion is clear from the definition of local components. q. e. d.

§ 4. Invariant semi-derivations of a group variety

In the sequel we assume that k is an algebraically closed field of a positive characteristic p. It is well known that there exists a natural correspondence between integral algebraic group schemes over k and group varieties defined over k in the sense of Weil [13]. Hereafter we shall identify an integral algebraic group scheme over k with the corresponding group variety defined over k. Then the set of all the closed points of a group scheme over k is nothing else than that of all the rational points of the corresponding group variety over k, since k is algebraically closed. This set of the closed points is an abstract group. We shall use rather the Weil's languages than those of schemes in this section for convenience' sake. We denote by e the unit element of G and, for a closed point a in G, by L_a the k-morphism of G onto itself defined by the left translation $x \to ax$ for any point x in G. Then the associated homomorphism L_a^* of $\mathcal{O}_{ax,G}$ to $\mathcal{O}_{x,G}$ is an onto isomorphism. In particular L_a^* gives an automorphism of the field $k(G)$ of the rational functions of G over k.

A semi-derivation D of $k(G)$ over k will be called *left invariant* or, simply, *invariant* if $L_a^* D = D L_a^*$ for any closed point a in G. First we give a characterization of an invariant semi-derivation by its local components.

PROPOSITION 12. *Let G be a group variety defined over k and D a semi-derivation of $k(G)$ over k. Then if D is left invariant, D is regular at any closed point of G and satisfies the realation $D_{ab} = (L_a)_*(D_b)$ for any closed points a and b in G, where $(L_a)_*$ is the tangential mapping associated with the morphism L_a. Conversely if these conditions are satisfied, D is left invariant.*

PROOF. First we assume that D is left invariant. Then there exists a dense open subset U of G such that D is regular at any closed point b in U by Lemma 6. Let c be any closed point in G and put $a = cb^{-1}$. a is also a closed point in G. Since D is left invariant, we have $D = L_{a^{-1}}^* D L_a^*$ and $L_a^*(\mathcal{O}_{c,G}) = \mathcal{O}_{b,G}$. This means that $D(\mathcal{O}_{c,G}) = L_{a^{-1}}^* D L_a^*(\mathcal{O}_{c,G}) = L_{a^{-1}}^* D(\mathcal{O}_{b,G}) \subset L_{a^{-1}}^*(\mathcal{O}_{b,G}) = \mathcal{O}_{c,G}$, and hence that D is regular at c. Next let a and b be any two closed points in G and f an element of $\mathcal{O}_{ab,G}$. Then we have $(L_a)_*(D_b)(f) = D_b(L_a^*(f)) = D(L_a^*(f))(b) = (L_a^* D)(f)(b) = D(f)(ab) = D_{ab}(f)$. This means that $(L_a)_*(D_b) = D_{ab}$. Conversely assume that D is regular at any closed point in G and that $D_{ab} = (L_a)_*(D_b)$ for any closed point a and b in G. Let f be an element of $k(G)$. Then there exists an affine open subset U of G such that f is contained in the coordinates ring of U. We put $V = L_{a^{-1}}(U)$ for any closed point a in G. Then if b is a closed point in V, we have $(L_a)_*(D_b)(f) = D_{ab}(f)$ by assumptions. This shows that $D(L_a^*(f))(b) = L_a^*(D(f))(b)$ for any point b in U. Since G is reduced, we see that $D L_a^*(f) = L_a^* D(f)$. This completes the proof. q. e. d.

Remark. Let A be an abelian variety defined over k. Then it will be shown later that a semi-derivation D is invariant, if D is regular at any closed point in A.

COROLLARY. *Let G be as above and let D and D' be two left invariant semi-derivations of G over k such that their local components D_a and D'_a are equal to each other at a closed point a in G. Then D is equal to D'.*

PROOF. Let b be any closed point in G. Then we have $D_{ba}=(L_b)_*D_a=(L_a)_*D'_a=D'_{ba}$ by the assumption and Proposition 12. Therefore if f is an element of $k(G)$, $D(f)(x)=D'(f)(x)$ for any closed point x of a dense open subset of G. This shows that $D(f)=D'(f)$, since G is reduced. q. e. d.

Now we denote by $\mathfrak{g}(G)$ the set of all left invariant semi-derivations of G over k and put $\mathfrak{g}_r(G)=\mathfrak{g}(G)\cap\mathfrak{D}_r(k(G)/k)$ and $\mathfrak{s}_r=\mathfrak{g}(G)\cap\mathfrak{S}_r(k(G)/k)$. It is easy to see that $\mathfrak{g}(G)$, $\mathfrak{g}_r(G)$ and $\mathfrak{s}_r(G)$ are vector spaces over k and that $\mathfrak{g}(G)$ and $\mathfrak{s}_r(G)$ are associative algebras. $\mathfrak{g}_r(G)$ is a Lie algebra over k with the multiplication $[D, D']=DD'-D'D$. In the rest of this section we shall determine basis of $\mathfrak{s}_r(G)$ and $\mathfrak{g}_r(G)$ using Barsotti's original idea (cf. [1]).

Let x and y be two independent generic points of G over k. Then $k(x)$ (resp. $k(x, y)$) is isomorphic to the field $k(G)$ (resp. $k(G\times G)$) of the rational functions of G (resp. the product variety $G\times G$) over k. For simplicity put $\mathcal{O}=\mathcal{O}_{e,G}$ and $\mathcal{O}'=\mathcal{O}_{e\times e,G\times G}$. If $\{t_1, \cdots, t_n\}$ is a regular system of parameters of $\mathcal{O}$, there exists a regular system $\{t'_1, \cdots, t'_{2n}\}$ of parameters of $\mathcal{O}'$ such that $t'_i(x, y)=t_i(x)$ and $t'_{i+n}(x, y)=t_i(y)$ for $i=1, 2, \cdots, n$. We shall put $\xi_i=t_i(x)$ and $\eta_i=t_i(y)$ for $i=1, 2, \cdots, n$. Let f be a rational function of G defined over k which is contained in $\mathcal{O}$. Then it is easy to see that there exist a rational function $\hat{f}$ in $\mathcal{O}'$ such that $\hat{f}(x, y)=f(xy)-f(x)$. If $\mathfrak{p}$ is the prime ideal in $\mathcal{O}'$ generated by n elements $t'_{n+1}, \cdots, t'_{2n}$, $\mathcal{O}$ is canonically isomorphic to the residue ring $\mathcal{O}'/\mathfrak{p}$ and $\hat{f}$ is contained in $\mathfrak{p}$, since $\hat{f}(x, e)=0$. Therefore $\hat{f}(x, y)$ is equal to $\sum_{j=1}^{n} a'_j(x, y)\eta_j$, where a'_j is in $\mathcal{O}'$ for each $j=1, 2, \cdots, n$. From the fact that $\mathcal{O}$ is canonically isomorphic to $\mathcal{O}'/\mathfrak{p}$, there exists unique element a_j in $\mathcal{O}$ for $j=1, 2, \cdots, n$ such that $a_j(x)\equiv a'_j(x, y)$ mod. $\mathfrak{p}$. This means that

$$\hat{f}(x, y)=\sum_{j=1}^{n} a_j(x)\eta_j+\sum_{i,j=1}^{n} a'_{ij}(x, y)\eta_i\eta_j,$$

where a'_{ij} is in $\mathcal{O}'$ for each $i, j=1, 2, \cdots, n$. Reperating this procedure we obtain the following equality

$$\hat{f}(x, y)=\sum_{i=1}^{n} a_i(x)\eta_i+\sum_{i,j=1}^{n} a_{ij}(x)\eta_i\eta_j+\cdots+\sum_{(i)} a_{i_1\cdots i_k}(x)\eta_{i_1}\cdots\eta_{i_k}$$
$$+\sum_{(i)} a'_{i_1\cdots i_{k+1}}(x, y)\eta_{i_1}\cdots\eta_{i_1\cdots}\eta_{i_{k+1}},$$

where $a_{i_1\cdots i_k}\in\mathcal{O}$ and $a'_{i_1\cdots i_{k+1}}\in\mathcal{O}'$. We denote by $I_{e_1\cdots e_n}(f)$ the coefficient $a_{i_1\cdots i_s}$

of $\eta_{i_1}\cdots\eta_{i_s}=\eta_1^{e_1}\cdots\eta_n^{e_n}$ in this expansion, which is uniquely determined, since O' is a regular local ring. Then the mapping $I_{e_1\cdots e_n}$ of O into itself is a k-linear mapping.

LEMMA 9. *For* $0\leq e_i<p^r$ $(i=1, 2, \cdots, n)$, $I_{e_1\cdots e_n}$ *is* O^{p^r}*-linear and* $I_{0\cdots 0p^r 0\cdots 0}(fg)$ *is equal to* $fI_{0\cdots 0p^r 0\cdots 0}(g)+gI_{0\cdots 0p^r 0\cdots 0}(f)$ *for* f *in* 0 *and* g *in* O^{p^r}

PROOF. If f and h are in O, we have

$$\begin{aligned}(\widehat{fh^{p^r}})(x, y)&=f(xy)h^{p^r}(xy)-f(x)h^{p^r}(x)\\&=(h^{p^r}(xy)-h^{p^r}(x))f(xy)+h^{p^r}(x)(f(xy)-f(x)).\end{aligned}$$

$I_{e_1\cdots e_n}(fh^{p^r})$ is the coefficient of $\eta_1^{e_1}\cdots\eta_n^{e_n}$ in the left-hand side of this equality and the coefficient of $\eta_1^{e_1}\cdots\eta_n^{e_n}$ in the right-hand side is $h^{p^r}(x)I_{e_1\cdots e_n}(f)(x)$, because $(h^{p^r}(xy)-h^{p^r}(x))f(xy)$ has no terms of total degrees in $\eta_1, \cdots, \eta_n$ less than p^r. This shows that $I_{e_1\cdots e_n}$ in O^{p^r}-linear. Similarly the second assertion can be shown. q. e. d.

Now we can extend $I_{e_1\cdots e_n}(0\leq e_i<p^r, \sum e_i>0)$ to a semi-derivation of $K=k(G)$ over k naturally as in the proof of Lemma 4, which will be also denoted by $I_{e_1\cdots e_n}$. Then $I_{e_1\cdots e_n}$ is in $\mathfrak{S}_r(k(G)/k)$ if $0\leq e_i<p^r$ and $\sum_{i=1}^n e_i>0$, and $I_{0\cdots 0p^r 0\cdots 0}$ is in $\mathfrak{D}_r(k(G)/k)$.

LEMMA 10. $I_{e_1\cdots e_n}$ *is left invariant.*

PROOF. Let a be a closed point of G and let f be an element of the intersection of $O=O_{e,G}$ and $O_{a,G}$. Assume that $0\leq e_i<p^r$ for each $i=1, 2, \cdots, n$. Then we have

$$\hat{f}(x, y)=\sum_{e_i<p^r} I_{e_1\cdots e_n}(f)(x)\eta_1^{e_1}\cdots\eta_n^{e_n}+\sum_{j=1}^n b_j(x, y)\eta_j^{p^r},$$

where $b_j(x, y)$ is in O for each j. By replacing f by L_a^*f, we have

$$(\widehat{L_a^*f})(x, y)=\sum_{e_i<p^r} I_{e_1\cdots e_n}(L_a^*f)(x)\eta_1^{e_1}\cdots\eta_n^{e_n}+\sum_{j=1}^n b_j(ax, y)\eta_j^{p^r},$$

and by replacing x by ax, we have

$$\begin{aligned}\hat{f}(ax, y)&=\sum_{e_i<p^r} I_{e_1\cdots e_n}(f)(ax)\eta_1^{e_1}\cdots\eta_n^{e_n}+\sum_{j=1}^n b_j(ax, y)\eta_j^{p^r}\\&=\sum_{e_i<p^r}(L_a^*I_{e_1\cdots e_n})(f)(x)\eta_1^{e_1}\cdots\eta_n^{e_n}+\sum_{j=1}^n b_j(ax, y)\eta_j^{p^r}.\end{aligned}$$

This means that $L_a^*I_{e_1\cdots e_n}=I_{e_1\cdots e_n}L_a^*$. q. e. d.

THEOREM 1. *Let* G *be a group variety of dimension* n *defined over an*

algebraically closed field k. Let $\{t_1, \cdots, t_n\}$ be a regular system of parameters of the local ring $\mathcal{O}=\mathcal{O}_{e,G}$ of G at the unit point e and let $\{I_{e_1\cdots e_n}\}$ be as above. Then $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{s}_r(G)$ over k and $\mathfrak{g}_r(G)$ is the direct sum $\mathfrak{s}_r(G) \oplus \sum_{i=1}^{n} k I_{0\cdots 0 \overset{i}{p} 0\cdots 0}$.

PROOF. Putting $f=t_1^{e'_1}\cdots t_n^{e'_n}$ for $0 \leq e'_i < p^r$, we have

$$\widehat{(t_1^{e'_1}\cdots t_n^{e'_n})}(x, y) = \sum_{e_i<p^r} I_{e_1\cdots e_n}(t_1^{e'_1}\cdots t_n^{e'_n})(x)\eta_1^{e_1}\cdots\eta_n^{e_n} + \sum_{j=1}^{n} b_j(x, y)\eta_j^{p^r}.$$

Since $(t_1^{e'_1}\cdots t_n^{e'_n})(x, y)$ is regular at (e, y) of $G\times G$, we may specialize x to e in the above equation. Then we have

$$\eta_1^{e'_1}\cdots\eta_n^{e'_n} = \sum_{e_i<p^r} (I_{e_1\cdots e_n})_e(t_1^{e'_1}\cdots t_n^{e'_n})\eta_1^{e_1}\cdots\eta_n^{e_n} + \sum_{j=1}^{n} b_j(e, y)\eta_j^{p^r},$$

where $(I_{e_1\cdots e_n})_e$ is the local component of $I_{e_1\cdots e_n}$ at e, and hence we see that $(I_{e_1\cdots e_n})_e(t_1^{e'_1}\cdots t_n^{e'_n}) = 0$ if $(e_1\cdots e_n) \neq (e'_1\cdots e'_n)$ and $(I_{e'_1\cdots e'_n})_e(t_1^{e'_1}\cdots t_n^{e'_n}) = 1$. This means that $I_{e_1\cdots e_n}(t_1^{e_1}\cdots t_n^{e_n}) - 1$ is in the maximal ideal $\mathfrak{m}$ of $\mathcal{O}=\mathcal{O}_{e,G}$ for $0 \leq e_i < p^r$ and $\sum_{i=1}^{n} e_i > 0$, and $I_{e_1\cdots e_n}(t_1^{e'_1}\cdots t_n^{e'_n})$ is in $\mathfrak{m}$ for $(e_1, \cdots, e_n) \neq (e'_1, \cdots, e'_n)$. In other words the local components of $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum e_i > 0\}$ is the canonical basis $\mathfrak{S}_r(\mathcal{O})$ over k with respect to $\{t_1, \cdots, t_n\}$. By Corollary of Proposition 12, $\mathfrak{s}_r(G)$ is isomorphic to a subspace of $\mathfrak{S}_r(\mathcal{O})$ over k. But from the above, we see that $\mathfrak{s}_r(G)$ is isomorphic to $\mathfrak{S}_r(\mathcal{O})$ and hence $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{s}_r(G)$ over k. Similarly we easily see that $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ and $\{I_{0\cdots 0 p^r 0\cdots 0} | i=1, 2, \cdots, n\}$ is a basis of $\mathfrak{g}_r(G)$ over k.

q. e. d.

COROLLARY 1. *Let G and $\{I_{e_1\cdots e_n}\}$ be as in Theorem 1 and let a be a closed point in G. Then $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{S}_r(G, a)$ over $\mathcal{O}_{a,G}$ and the local components of this basis at a is a basis of $\mathfrak{S}_r(\mathcal{O}_{a,G})$ over k.*

PROOF. If $a=e$, we see in the proof of Theorem 1 that the local components of $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{S}_r(\mathcal{O}_{e,G})$ over k. Therefore $\mathfrak{S}_r(G, e)$ is equal to $\sum_{e_i<p^r} \mathcal{O}_{e,G} I_{e_1\cdots e_n} + \mathfrak{m}_e \mathfrak{S}_r(G, e)$ and hence to $\sum_{e_i<p^r} \mathcal{O}_{e,G} I_{e_1\cdots e_n}$ by Nakayama's lemma. In the general cases, $\{(I_{e_1\cdots e_n})_a | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is also a basis of $\mathfrak{S}_r(\mathcal{O}_{a,G})$, since $D_a = (L_a)_* D_e$ for D in $\mathfrak{g}(G)$. Therefore we

see that $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{S}_r(G, a)$ over $\mathcal{O}_{a,G}$ by the same reason as the case $a=e$. q. e. d.

COROLLARY 2. *Let G be an abelian variety defined over k and D a semi-derivation of G over k. Then D is invariant if and only if D is regular at any closed point in G.*

PROOF. Assume that D is regular at any closed point in G and that D is in $\mathfrak{S}_r(k(G)/k)$. Since $\{I_{e_1\cdots e_n} | 0 \leq e_i < p^r, \sum_{i=1}^{n} e_i > 0\}$ is a basis of $\mathfrak{S}_r(k(G)/k)$ over $k(G)$, we have $D = \sum_{e_i<p^r} a_{e_1\cdots e_n} I_{e_1\cdots e_n}$. By Corollary 1 of Theorem 1 $\{I_{e_1\cdots e_n}\}$ is also a basis of $\mathfrak{S}_r(G, a)$ over $\mathcal{O}_{a,G}$ for any closed point a in G, these $a_{e_1\cdots e_n}$ must be in $\mathcal{O}_{a,G}$. This means that each $a_{e_1\cdots e_n}$ is a constant, i.e., an element of k, because G is a complete variety defined over k. This completes the proof. q. e. d.

§ 5. Functorial properties of $\mathfrak{H}(G) = k \oplus \mathfrak{g}(G)$ as an algebra

First we recall some definitions concerning Hopf algebras over a field k for convenience' sake. Let A be a vector space over a field k. Then A is called a *unitary algebra over k* if there exist a k-linear mapping m of $A \otimes_k A$ into A and a k-linear mapping η of k into A such that $m(id_A \otimes m) = m(m \otimes id_A)$, and that $m(\eta \otimes id_A)$ and $m(id_A \otimes \eta)$ give the canonical isomorphisms of $k \otimes_k A$ and $A \otimes_k k$ onto A respectively. m is called the multiplication of A. Let τ be the automorphism of $A \otimes_k A$ defined by $\tau(a \otimes b) = b \otimes a$. Then the unitary algebra A is called *commutative* if $m\tau = m$. Let (A', m', η') be another unitary algebra over k and f a k-linear mapping of A into A'. Then we say that f is *an algebra homomorphism* of A into A' if $m'(f \otimes f) = fm$ and $\eta' = f\eta$. Similarly we can define an augmented coalgebra over k, which is the dual notion of a unitary algebra over k. A vector space A over k is called *an augmented coalgebra over k* if there exist a k-linear mapping Δ of A into $A \otimes_k A$ and a k-linear mapping ε of A into k such that $(id_A \otimes \Delta)\Delta = (\Delta \otimes id_A)\Delta$ and that $(\varepsilon \otimes id_A)\Delta$ and $(id_A \otimes \varepsilon)\Delta$ give the canonical isomorphisms of A onto $k \otimes_k A$ and $A \otimes_k k$ respectively. Δ and ε are called the diagonal and the augmentation of A respectively. The cocommutativity and coalgebra homomorphisms of augmented coalgebras over k can be defined in the same way as the commutativity and algebra homomorphisms of unitary algebras over k. Moreover notice that if (A, m, η) is a unitary algebra over k, $A \otimes_k A$ has a structure of a unitary algebra over k. In fact if we put $\bar{m} = (m \otimes m)(id_A \otimes \tau \otimes id_A)$ and $\bar{\eta} = \eta \otimes \eta$, $(A \otimes_k A, \bar{m}, \bar{\eta})$ is a unitary algebra over k. Similary, if (A, Δ, ε) is an augmented coalgebra over k, we see that $A \otimes_k A$ has a structure of an augmented coalgebra over k defined naturally by that of A. It is easy to see that k itself

is a unitary algebra and an augmented coalgebra over k.

A vector space A over k is called *a bialgebra over* k or *a hyperalgebra over* k if A has both structures of a unitary algebra (A, m, η) and an augmented coalgebra (A, Δ, ε) such that Δ and ε are algebra homomorphisms of A into $A \otimes_k A$ and k respectively. It can be seen easily that the last condition is satisfied if and only if m and η are coalgebra homomorphisms of $A \otimes_k A$ and k into A respectively. A k-linear mapping f of $(A, m, \eta, \Delta, \varepsilon)$ into another bialgebra $(A', m', \eta', \Delta', \varepsilon')$ is called *a bialgebra homomorphism* if f is both an algebra homomorphism and a coalgebra homomorphism of A into A' over k. If a k-linear endomorphism of a bialgebra $(A, m, \eta, \Delta, \varepsilon)$ over k is called *an antipode of* A if $\eta \circ \varepsilon = m(c \otimes id_A)\Delta = m(id_A \otimes c)\Delta$, and then $(A, m, \eta, \Delta, \varepsilon, c)$ is called a *Hopf algebra with the antipode* c.

If A is a vector space of a finite dimension over k, we denote by A^* the dual space $\mathrm{Hom}_k(A, k)$. For a k-linear mapping of A into a finite dimensional vector space B over k, f^* will be the dual mapping of B^* into A^* defined by $f^*(\phi) = \phi \circ f$ for ϕ in B^*. Then if $(A, m, \eta, \Delta, \varepsilon)$ is a bialgebra over k such that $\dim_k A$ is finite, we can easily see that $(A^*, \Delta^*, \varepsilon^*, m^*, \eta^*)$ is also a bialgebra over k, where $(A^*, \Delta^*, \varepsilon^*)$ (resp. (A^*, m^*, η^*)) is the underlying unitary algebra (resp. the underlying augmented coalgebra). $(A^*, \Delta^*, \varepsilon^*, m^*, \eta^*)$ is called *the linear dual* of $(A, m, \eta, \Delta, \varepsilon)$ and denoted by A^D. Moreover if a Hopf algebra A has the antipode c, c^* is the antipode of A^D, and hence A^D is also a Hopf algebra over k.

Now we return to an integral algebraic group scheme G over an algebraically closed field k. Since the set $\mathfrak{g}(G)$ of left invariant semi-derivations of G over k is a subalgebra of $\mathrm{Aut}_k(k(G))$, $\mathfrak{H}(G) = k \oplus \mathfrak{g}(G)$ can be also considered a subalgebra of $\mathrm{Aut}_k(k(G))$. Then $\mathfrak{H}(G)$ is a unitary algebra over k in the above sense. We shall denote by m_G the multiplication of $\mathfrak{H}(G)$ and by η_G the mapping of k into $\mathfrak{H}(G)$ defined by $\eta(\alpha) = \alpha \oplus 0$ in $\mathfrak{H}(G)$ for α in k. The coalgebra structure of $\mathfrak{H}(G)$ is defined as follows. For simplicity we denote by $I_{0\cdots0}$ the identity mapping of $k(G)$ onto itself. Then $\mathfrak{H}(G)$ is a vector space over k such that $\{I_{e_1 \cdots e_n} \mid e_i$: non-negative integer for $i = 1, 2, \cdots, n\}$ is a basis of $\mathfrak{H}(G)$ over k. The augmentation ε_G of $\mathfrak{H}(G)$ is given by the value $D(1)$ of D in $\mathfrak{H}(G)$, i.e., the projection of the direct sum $\mathfrak{H}(G) = k \oplus \mathfrak{g}(G)$ to the first factor k. The diagonal Δ_G of $\mathfrak{H}(G)$ can be determined by the values of a basis of $\mathfrak{H}(G)$ over k. Therefore we put $\Delta_G(I_{e_1 \cdots e_n}) = \sum_{(e') + (e'') = (e)} I_{e'_1 \cdots e'_n} \otimes_k I_{e''_1 \cdots e''_n}$, where the sum runs over all $(e'_1, \cdots, e'_n)$ and $(e''_1, \cdots, e''_n)$ such that $e'_i + e''_i = e_i$ for any $i = 1, 2, \cdots, n$. It is easy to see that Δ_G is cocommutative and that $(\mathfrak{H}(G), \Delta_G, \varepsilon_G)$ is an augmented coalgebra over k, since $\varepsilon_G(I_{e_1 \cdots e_n}) = 0$ if $(e_1, \cdots, e_n) \neq (0, \cdots, 0)$. We must see that $(\mathfrak{H}(G), m_G, \eta_G, \Delta_G, \varepsilon_G)$ is a bialgebra over k. If it is done, we see that the subalgebras $\mathfrak{H}_r(G) = k \oplus \mathfrak{g}_r(G)$ are subbialgebras of $\mathfrak{H}(G)$ and that $\mathfrak{H}(G) = \bigcup_{r=1}^{\infty} \mathfrak{H}_r(G)$. Conversely if we see that each $\mathfrak{H}_r(G)$ is a bialgebra over k, $\mathfrak{H}(G)$ is necessarily a bialgebra over k. We shall see later that $\mathfrak{H}_r(G)$ is

a Hopf algebra over k for each i and postpone there the verification for $\mathfrak{H}(G)$ to be a bialgebra over k. But we show here that the multiplication m_G of $\mathfrak{H}(G)$ is related closely to that of G. For this purpose we show the following.

THEOREM 2. *Let G be a group variety over an algebraically closed field k, and let $\{t_1, \cdots, t_n\}$ be a regular system of parameters of $O=O_{e,G}$. Let x and y be two independent generic points of G over k and put $\xi_i=t_i(x)$ and $\eta_i=t_i(y)$ for $i=1, 2, \cdots, n$. Then, for any element f of O and for any r, we have*

$$f(xy)=\sum_{0\leq e_i, e'_j<p^r}(I_{e_1\cdots e_n}I_{e'_1\cdots e'_n})_e(f)\xi_1^{e_1}\cdots\xi_n^{e_n}\eta_1^{e'_1}\cdots\eta_n^{e'_n}$$

$$+\sum_{i=1}^{n}a_i(x, y)\xi_i^{p^r}+\sum_{i=1}^{n}b_i(x, y)\eta_i^{p^r},$$

where a_i and b_i are rational functions of $G\times G$ regular at $e\times e$ and $(I_{e_1\cdots e_n}I_{e'_1\cdots e'_n})_e$ is the local component of $I_{e_1\cdots e_n}I_{e'_1\cdots e'_n}$ at e.

PROOF. Let x, y and z be three independent generic points of G over k and denote by O'' the local ring of $G\times G\times G$ at $e\times e\times e$. Then there exists a regular system $\{t''_1, \cdots, t''_{3n}\}$ of parmeters of O'' such that $\xi_i=t_i(x)=t''_i(x, y, z)$, $\eta_i=t_i(y)=t''_{n+j}(x, y, z)$ and $\zeta_i=t_i(z)=t''_{2n+i}(x, y, z)$ for $i=1, 2, \cdots, n$. Then we can easily see that $O''/(t''_{2n+1}, \cdots, t''_{3n})$ is canonically isomorphic to $O'=O_{e\times e, G\times G}$. Therefore if g is a rational function of $G\times G$ defined over k and if g is regular at $e\times e$, we can expand $g(xz, y)$ to a series in the veriables $\zeta_1, \cdots, \zeta_n$ as follows:

$$g(xz, y)=g(x, y)+\sum_{e_i<p^r}I'_{e_1\cdots e_n}(g)(x, y)\zeta_1^{e_1}\cdots\zeta_n^{e_n}$$

$$+\sum_{j=1}^{n}a'_j(x, y, z)\zeta_j^{p^r},$$

where $I'_{e_1\cdots e_n}(g)$ and a'_j are contained in O' and O'' respectively. It is easy to see that $I'_{e_1\cdots e_n}$ is a k-linear mapping of O' to itself and that the restriction of $I'_{e_1\cdots e_n}$ to the field $k(G)=k(G\times e)$ is $I_{e_1\cdots e_n}$ defined in §4. Putting in particular $g(x, y)=f(xy)$, we have

$$g(xz, y)=f(xzy)=f(xy)+\sum_{e_i<p^r}I'_{e_1\cdots e_n}(g)(x, y)\zeta_1^{e_1}\cdots\zeta_n^{e_n}$$

$$+\sum_{j=1}^{n}a'_j(x, y, z)\zeta_j^{p^r}.$$

Since $f(xy)=f(x)+\sum_{e'_i<p^r}I_{e'_1\cdots e'_n}(f)(x)\eta_1^{e'_1}\cdots\eta_n^{e'_n}+\sum_{j=1}^{n}b'_j(x, y)\eta_j^{p^r}$,
we see easily that

$$I'_{e_1\cdots e_n}(g)(x, y)=I_{e_1\cdots e_n}(f)(x)$$

$$+\sum_{e_i'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})(f)(x)\eta_1^{e_1'}\cdots\eta_n^{e_n'}+\sum_{j=1}^{n}I'_{e_1\cdots e_n}(b_i')(x,\ y)\eta_i^{p^r}$$

and hence that

$$f(xzy)=\sum_{0\leq e_i,e_j'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})(f)(x)\eta_1^{e_1'}\cdots\eta_n^{e_n'}\zeta_1^{e_1}\cdots\zeta_n^{e_n}$$

$$+\sum_{j=1}^{n}a_j(x,\ y,\ z)\zeta_j^{p^r}+\sum_{j=1}^{n}b_j(x,\ y,\ z)\eta_j^{p^r},$$

where a_j and b_j are in $\mathcal{O}''$. Specializing x to e and replacing z by x, we obtain the following

$$f(xy)=\sum_{0\leq e_i,e_j'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})_e(f)\xi_1^{e_1}\cdots\xi_n^{e_n}\eta_1^{e_1'}\cdots\eta_n^{e_n'}$$

$$+\sum_{j=1}^{n}a_j(x,\ y)\xi_j^{p^r}+\sum_{j=1}^{n}b_j(x,\ y)\eta_j^{p^r},$$

where a_j and b_j are in $\mathcal{O}'$. q. e. d.

COROLLARY. *Let G be as in Theorem 2. Then G is commutative if and only if the algebra $\mathfrak{g}(G)$ is commutative.*

PROOF. G is commutative if and only if $xy=yx$ for any independent generic points x and y of G over k. If $xy=yx$, then $I_{e_1\cdots e_n}I_{e_1'\cdots e_n'}=I_{e_1'\cdots e_n'}I_{e_1\cdots e_n}$ by Theorem 2 and Corollary of Proposition 12. This shows that $\mathfrak{g}(G)$ is a commutative algebra over k, since $\{I_{e_1\cdots e_n}\}$ is a basis of $\mathfrak{g}(G)$ over k. Conversely if $\mathfrak{g}(G)$ is commutative, we see that $f(xy)=f(yx)$ for any function f in $\mathcal{O}_{e,G}$. But this means that $xy=yx$, since G is reduced. q. e. d.

Next we give some functorial properties of $\mathfrak{H}(G)$ as an algebra over k. Let G and G' be two group varieties defined over k and let α be a homomorphism of G into G' defined over k. If D is an element of $\mathfrak{g}(G)$, $\alpha_*(D_e)$ is a local semi-derivation of the local ring $\mathcal{O}_{e',G'}$ of G' at the unit point e', where α_* is the tangential mapping at the unit point e of G attached to the k-morphism α. Then there is the unique left invariant semi-derivation D' such that the local component $D'e'$ of D' is $\alpha_*(D_e)$ by Corollary 1 of Theorem 1 and Corollary of Proposition 12. Putting $\alpha_*(D)=D'$, we obtain a k-linear mapping α_* of $\mathfrak{g}(G)$ into $\mathfrak{g}(G')$, and extend it to a k-linear mapping of $\mathfrak{H}(G)$ into $\mathfrak{H}(G')$ such that the restriction of the mapping to k is the identity mapping of k. We shall also denote by α_* the extended mapping and this α_* will be called *the tangential mapping of $\mathfrak{H}(G)$ to $\mathfrak{H}(G')$ attached to α.*

LEMMA 11. *Let G, G' and α be as above and D a left invariant semi-derivation of G. Then we have*

(i) $(\alpha_*D)_{\alpha(a)}=\alpha_*(D_a)$ *for any closed point a in G, and*

(ii) $\alpha^*(\alpha_*D)(f)=D\alpha^*(f)$ *for any f in $k(G')$ regular along $\alpha(G)$.*

PROOF. By the definition of α_* and Proposition 12 we have $(\alpha_*D)_{\alpha(a)}=(L_{\alpha(a)})_*(\alpha_*D)_{e'}=(L_{\alpha(a)})_*\alpha_*(D_e)=(L_{\alpha(a)}\alpha)_*(D_e)=(\alpha L_a)(D_e)=\alpha_*D_a$. This proves (i). Take a closed point a in G such that f is regular at $\alpha(a)$. Then we have, using (i), $(\alpha^*(\alpha_*D)f)(a)=(\alpha_*D)(f)(\alpha(a))=(\alpha_*D)_{\alpha(a)}(f)=(\alpha_*D_a)(f)=D_a(\alpha^*f)=D(\alpha^*f)(a)$. Since G is reduced, we can easily see that $\alpha^*(\alpha_*D)(f)=D(\alpha^*f)$. q. e. d.

LEMMA 12. *Let G, G' and α be as in Lemma 11. Then the k-linear mapping α_* of $\mathfrak{D}(G)$ into $\mathfrak{D}(G')$ is an algebra homomorphism and hence the restriction of α_* to $\mathfrak{g}(G)$ is a Lie algebra homomorphism of $\mathfrak{g}(G)$ into $\mathfrak{g}(G')$.*

PROOF. It is sufficient to see that $\alpha_*(D_1D_2)_{e'}(f)=(\alpha_*(D_1)\alpha_*(D_2))_{e'}(f)$ for f in $\mathcal{O}_{e',G'}$ and D_i in $\mathfrak{g}(G)$ $(i=1,2)$. By Lemma 11 and the definition of α_* we have $(\alpha_*(D_1)\alpha_*(D_2))_{e'}(f)=(\alpha_*(D_1)\alpha_*(D_2)(f))(e')=(\alpha_*D_1)_{e'}((\alpha_*D_2)(f))=\alpha_*(D_{1e})((\alpha_*D_e)(f))=D_{1e}(\alpha^*\alpha_*(D_2)(f))=D_{1e}(D_2(\alpha^*f))=(D_1D_2(\alpha^*f))(e)=\alpha_*(D_1D_2)_{e'}(f)$. q. e. d.

PROPOSITION 13. *Let G be a group variety defined over k and let G' be a group subvariety of G defined over k. Then j_* attached to the injection j of G' into G is an injective mapping.*

PROOF. Put $\mathcal{O}=\mathcal{O}_{e,G}$ and $\mathcal{O}'=\mathcal{O}_{e,G'}$ and let $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ corresponding to the subvariety G' of G. Then $\mathcal{O}/\mathfrak{p}$ is canonically isomorphic to $\mathcal{O}'$ and j^* is nothing else but the natural homomorphism of $\mathcal{O}$ onto $\mathcal{O}'$, if we identify $\mathcal{O}'$ with $\mathcal{O}/\mathfrak{p}$. Therefore the tangential mapping j_* in the sense of §3 is injective. But this means that the mapping j_* of $\mathfrak{D}(G)$ to $\mathfrak{D}(G')$ is also injective by Corollary of Proposition 12. q. e. d.

PROPOSITION 14. *Let G and G' be two group varieties defined over k, and α a separable homomorphism of G onto G' defined over k. Then the tangential mapping α_* attached to α is surjective.*

PROOF. We may identify $k(G')$ with the subfield $\alpha^*(k(G'))$ of $k(G)$. By assumptions, there exists a separating transcendence basis $\{s_1, \cdots, s_m\}$ of $k(G)$ over $k(G')$. If $\{t_1, \cdots, t_r\}$ is a separating transcendence basis of $k(G')$ over k, $\{t_1, \cdots, t_r, s_1, \cdots, s_m\}$ is that of $k(G)$ over k. Then there exist non-empty open subsets U and V of G and G' respectively such that $\{t_1-t_1(a), \cdots, t_r-t_r(a), s_1-s_1(a), \cdots, s_m-s_m(a)\}$ is a regular system of parameters of the local ring $\mathcal{O}_{a,G}$ at any closed point a of U and that $\{t_1-t_1(b), \cdots, t_r-t_r(b)\}$ is that of the local ring $\mathcal{O}_{b,G'}$ at any closed point b of V. Let a be a closed point of the non-empty set $U\cap\alpha^{-1}(V)$ and put $b=\alpha(a)$. Then we see that $\{L_a^{*-1}(t_1-t_1(a), \cdots, L_a^{*-1}(t_r-t_r(a))\}$ is a regular system of parameters of the localing $\mathcal{O}_{e',G'}$ and that $\{L_a^{*-1}(t_1-t_1(a)), \cdots, L_a^{*-1}(t_r-t_r(a)), L_a^{*-1}(s_1-s_1(a)), \cdots, L_a^{*-1}(s_m-s_m(a))\}$ is that of the local ring $\mathcal{O}_{e,G}$. Therefore we may assume that $\{t_1, \cdots, t_r\}$ is a regular system of parameters of $\mathcal{O}_{e',G'}$ and that $\{t_1, \cdots, t_r, s_1, \cdots, s_m\}$ is that

of $\mathcal{O}_{e,G}$. If $\{I_{e_1\cdots e_{m+r}}\}$ is the canonical basis of $\mathfrak{g}(G)$ with respect to $\{t_1, \cdots, t_r, s_1, \cdots, s_m\}$, then we see easily that $\{\alpha_*(I_{e_1\cdots e_r 0\cdots 0})\}$ is that of $\mathfrak{g}(G')$ with respect to $\{t_1, \cdots, t_r\}$. This shows that α_* is surjective. q. e. d.

We terminate this section by giving an interpretation of α_* attached to a surjective homomorphism α.

PROPOSITION 15. *Let G and G' be group varieties defined over k and α a homomorphism of G onto G' defined over k. Let $k(G')$ be identified with the subfield $\alpha^*(k(G'))$ of $k(G)$. Then if D is in $\mathfrak{D}(G)$, the restriction $D|_{k(G')}$ of D to $k(G')$ is in $\mathfrak{D}(G')$ and we have $\alpha_*(D)=D|_{k(G')}$ and $\alpha_*(D_a)=\alpha_*(D)_{\alpha(a)}$ for any closed point a in G.*

PROOF. By (ii) of Lemma 11, we have $\alpha^*(\alpha_*(D))(f)=D(\alpha^*(f))$ for any f in $\mathcal{O}_{e',G'}$, since α is surjective. By the definition of α_* and Proposition 12 $\alpha_*(D)$ is regular at e', and hence $\alpha_*(D)(f)$ is in $\mathcal{O}_{e',G'}$. This means that $D(\alpha^*(\mathcal{O}_{e',G'}))$ is in $\alpha^*(\mathcal{O}_{e',G'})$ and hence $D(k(G'))$ is in $k(G')$. Moreover the above equality shows that $D|_{k(G')}$ is $\alpha_*(D)$. The last assertion is easily seen. q. e. d.

§ 6. Bialgebra structure of $\mathfrak{H}(G)$ and purely inseparable isogenies of G

First we summarize the Cartier's results on isogenies of group varieties given in [3], which are necessary for determining the structure of $\mathfrak{H}(G)$ of a group variety G. For convenience we state them in our terminologies.

Let G be a group variety defined over an algebraically closed field k and let L be a subfield of $k(G)$ containing k such that $[k(G):L]=r<\infty$. Assume that L is stable under the automorphism L_a^* of $k(G)$ attached to the left translation L_a of G for any closed point a of G. Let A_L be the set of L-linear endomorphisms of $k(G)$ and N_L the subset of the elements u in A_L such that $uL_a^*=L_a^*u$ for any closed point a of G. Moreover denote by $N_L^{(s)}$ the set of L-multilinear mappings u of the product space $k(G)\times\cdots\times k(G)$ with s factors into $k(G)$ such that $L_a^*u(f_1, \cdots, f_s)=u(L_a^*(f_1), \cdots, L_a^*(f_s))$ for any closed point a of G and for any f_i in $k(G)$ $(i=1, 2, \cdots, s)$. Then Cartier obtained the followings.

(A) A_L is a ring containing $k(G)$ (as translations) and a vector space over $k(G)$. N_L is a subring of A_L containing k and a vector space over k. Therefore N_L is a unitary algebra over k. Moreover any basis of N_L over k is that of A over $k(G)$. In particular $r=\dim_k N_L=\dim_{k(G)}A_L$.

(B) The tensor product $N_L\otimes_k\cdots\otimes_k N_L$ of copies of N_L is isomorphic to $N_L^{(s)}$ by a k-linear mapping π_s such that $\pi_s(u_1\otimes\cdots\otimes u_s)(f_1, \cdots, f_s)=u_1(f_1)\cdots u_s(f_s)$ for u_i in N_1 and f_i in $k(G)$ $(i=1, 2, \cdots, s)$. We shall identify $N_L\otimes_k\cdots\otimes_k N_L$ with $N^{(s)}$.

(C) N_L is a bialgebra over k, where the diagonal Δ_L and the augmentation ε_L are defined as follows. For any f_1 and f_2 in $k(G)$ we put $\Delta_L(u)(f_1, f_2) = u(f_1 f_2)$. Then Δ_L is a k-linear mapping of N_L into $N_L \otimes_k N_L = N^{(2)}$. The augmentation ε_L is given by $\varepsilon_L(u) = u(1)$.

(D) Let M be an algebra eith identity of k-linear endomorphisms of $k(G)$ satisfying the following conditions: (i) M is of finite dimension over k. (ii) $uL_a^* = L_a^* u$ for any u in M and any closed point a in G, and (iii) for any u in M, there exist u_i and $u_i'(i = 1, 2, \cdots, t)$ such that $u(f_1 f_2) = \sum_{i=1}^{t} u_i(f_1) u_i'(f_2)$ for any f_i in $k(G)$ $(i = 1, 2)$. Let M^+ be the set of u of M such that $u(1) = 0$ and let L be the subfield consisting of the elements f in $k(G)$ such that $u(f) = 0$ for any u in M^+. Then L is stable under the automorphisms L_a^* of $k(G)$ for any closed point a in G and $M = N_L$. In particular we have $[k(G) : L] = \dim_k M$.

Let G' be another group variety defined over k and α an isogeny of G onto G' defined over k. Then we may identify $k(G')$ with the subfield $\alpha^*(k(G'))$ of $k(G)$ and $k(G')$ is stable under the automorphisms L_a^* and R_a^* of $k(G)$ for any closed point a in G, where R_a is the morphism of G onto G such that $R_a(x) = xa$ for any point x in G (cf. Proposition 7 in [3]). We denote by $N(\alpha)$ the bialgebra $N_{k(G')}$ attached to the subfield $k(G')$ of $k(G)$. We put $ad_a(u) = R_a^{*-1} u R_a^*$ for any closed point a in G and a k-linear endomorphism u of $k(G)$. Then the operator ad is called *the adjoint representation of* G.

(E) Let G, G' and α be as above. Let M be a subalgebra of $N(\alpha)$. Then M is the corresponding subalgebra $N(\beta)$ to an isogeny β of G onto G'' if and only if M is a subbialgebra of $N(\alpha)$ over k which is stable under the adjoint representation of G. Then if so, β is determined uniquely up to isomorphisms, and there exists an isogeny γ of G'' onto G' such that $\alpha = \gamma \circ \beta$. Conversely if $\alpha = \gamma \circ \beta$, $N(\beta)$ is a subbialgebra of $N(\alpha)$ stable under the adjoint representation of G.

Now we apply these results to purely inseparable isogenies of group varieties. Let G be a group variety defined over k. Then it is well known that there exists a purely inseparable isogeny π_r of G onto a group variety G_r defined over k, isomorphic to G over k, such that $\pi_r^*(k(G_r))$ is the subfield $k(G)^{p^r}$ of $k(G)$ and that such π_r is uniquely determined up to isomorphisms. We call π_r the *Frobenius morphism of height* r *of* G. Moreover we easily see that a purely inseparable isogeny α of G onto a group variety G' decompose a π_r, i.e., $\pi_r = \beta \circ \alpha$ for some isogeny β of G' onto G_r, if and only if $\pi_r^*(k(G_r)) = k(G)^{p^r}$ is contained in $\alpha^*(k(G'))$. Such an isogeny α will be called *of height* $\leqslant r$.

LEMMA 13. *Let G be a group variety defined over k. Then $k(G) \oplus \mathfrak{S}_r(k(G)/k)$ is the set A_r of all the $k(G)^{p^r}$-linear endomorphisms of $k(G)$.*

PROOF. Since an element f of $k(G)$ operates on $k(G)$ as a left translation,

$k(G)$ is contained in A_r. On the other hand $\mathfrak{S}_r(k(G)/k)$ is contained in A_r by Lemma 3, Moreover we have $\dim_{k(G)}\mathfrak{S}_r(k(G)/k)=p^{nr}-1$ if $\dim G=n$ by Proposition 3, and hence $\dim_{k(G)}(k(G)\oplus\mathfrak{S}_r(k(G)/k)=p^{nr}$, which is equal to $\dim_{k(G)}A_r$, since it is easy to see that $[k(G):k(G)^{p^r}]=p^{nr}$ q. e. d.

PROPOSITION 16. *If π_r is the Frobenius morphism of height r of a group variety G defined over k, then $N(\pi_r)$ is equal to $\mathfrak{H}_r(G)=k\oplus\mathfrak{s}_r(G)$.*

PROOF. By Lemma 13 and the definitions of $\mathfrak{s}_r(G)$ and $N(\pi_r)$, $N(\pi_r)$ contains $k\oplus\mathfrak{s}_r(G)$, whose dimention over k is p^{nr} by Theorem 1. On the other hand $\dim_k N(\pi_r)$ is equal to $\dim_{k(G)}A_r=p^{nr}$ by (A). This shows that $N(\pi_r)=k\oplus\mathfrak{s}_r(G)=\mathfrak{H}_r(G)$. q. e. d.

PROPOSITION 17. *Let G be a group variety defined over k. Then $(\mathfrak{H}(G), m_G, \eta_G, \Delta_G, \varepsilon_G)$ defined in* §5 *is a bialgebra over k, and $N(\pi_r)$ with the structure defined in* (C) *is a subbialgebra of $\mathfrak{H}(G)$.*

PROOF. As noticed in §5, it suffices to show that $\mathfrak{H}_r(G)=k\oplus\mathfrak{s}_r(G)$ is a bialgebra over k. Since $N(\pi_r)=\mathfrak{H}_r(G)$ by Proposition 16, we show that $\Delta_G|_{\mathfrak{H}_r(G)}$ and $\varepsilon_G|_{\mathfrak{H}_r(G)}$ are nothing else than the diagonal Δ_r and the augmentation ε_r of $N(\pi_r)$ in (C) of this section. By the definitions $\varepsilon_G|_{\mathfrak{H}_r(G)}$ is equal to ε_r. On the other hand let f and g be two elements of $k(G)$ regular at the unit point e of G, and let x and y be two independent generict points of G over k. Then we easily see that

$$f(xy)g(xy)=f(x)g(x)+\sum_{e_i<p^r}\Big(\sum_{(e')+(e'')=(e)}I_{e'_1\cdots e'_n}(f)I_{e''_1\cdots e''_n}(g)\Big)\eta_1^{e_1}\cdots\eta_n^{e_n}$$

$$+\sum_{j=1}^{n}a_j(x,\ y)\eta_j^{p^r},$$

where a_j is in $\mathcal{O}_{e\times e,G\times G}$ for any $j=1, 2, \cdots, n$. This means, putting $I_{0\cdots 0}=$ the identity map of $k(G)$, that $I_{e_1\cdots e_n}(fg)=\sum_{(e')+(e'')=(e)}I_{e'_1\cdots e'_n}(f)I_{e''_1\cdots e''_n}(g)$, where the sum $\sum_{(e')+(e'')=(e)}$ runs over all $(e'_1, \cdots, e'_n)$ and $(e''_1, \cdots, e''_n)$ such that $e'_i+e''_i=e_i$ for each $i=1, 2, \cdots, n$. From this we have $\Delta_r(I_{e_1\cdots e_n})(f, g)=I_{e_1\cdots e_n}(fg)=\sum_{(e')+(e'')=(e)}I_{e'_1\cdots e'_n}(f)I_{e''_1\cdots e''_n}(g)=\sum_{(e')+(e'')=(e)}(I_{e'_1\cdots e'_n}\otimes I_{e''_1\cdots e''_n})(f, g)=\Delta_G(I_{e_1\cdots e_n})(f, g)$. q. e. d.

THEOREM 3. *Let G be a group variety defined over k and $\mathfrak{H}(G)$ its bialgebra generated by left invariant semi-derivations on G. Then there exists one to one correspondence between isomorphism classes of purely inseparable isogenies of G and finite dimensional subbialgebras of $\mathfrak{H}(G)$ which is stable under the adjoint representation of G. Moreover a purely inseparable isogeny α of G is of height $\leqq r$ if and only if the corresponding bialgebra $N(\alpha)$ is contained in $\mathfrak{H}_r(G)=k\oplus\mathfrak{s}_r(G)$.*

PROOF. Let α be a purely inseparable isogeny of G onto a group variety G' defined over k. Then there exists an isogeny β of G' to G_r defined over k such that $\pi_r=\beta\alpha$. Then the bialgebra $N(\alpha)$ of α is a subbialgebra of $\mathfrak{H}_r(G)=N(\pi_r)$ by (E), and hence a subbialgebra of $\mathfrak{H}(G)$, which is of a finite dimension. Conversely if M is a subbialgebra of $\mathfrak{H}(G)$ of a finite dimension, there exist an subbialgebra $\mathfrak{H}_r(G)$ containing M, since $\mathfrak{H}(G)$ is the union of $\mathfrak{H}_n(G)$ $(n=1, 2, \cdots)$. Then if M is stable under the adjoint representation of G, M is equal to $N(\alpha)$ for an isogeny α of G onto G' such that $\pi_r=\beta\alpha$, where β is an isogeny of G' onto G_r. Then correspondence of α and $N(\alpha)$ is evidently a bijection between isomorphism classes of isogenies of G defined over k and invariant subbialgebras of finite dimensions of $\mathfrak{H}(G)$ under the adjoint representation of G. The last assertion follows from the above. q. e. d.

§ 7. Kernels of purely inseparable isogenies

The aim of this section is to determine the kernel of a purely inseparable isogeny α of a group variety G as a closed group subscheme of G whose underlying space consists of the unique point e of G, and to show that the kernel of α is isomorphic to Spec $(N(\alpha)^D)$ of the linear dual $N(\alpha)^D$ of the bialgebra $N(\alpha)$ defined in §6.

Let G be a group variety defined over k and α a purely inseparable isogeny of G onto a group variety G' defined over k. If we denote by $\mathcal{O}$ and $\mathfrak{m}$ (resp. $\mathcal{O}'$ and $\mathfrak{m}'$) the local ring of G (resp. G') at the unit point e (resp. e') and its maximal ideal, there exists a local homomorphism α^* of $\mathcal{O}'$ into $\mathcal{O}$ attached to the morphism α. Since G and G' are group schemes over k, there exist k-morphisms μ and μ' of $G\times G$ and $G'\times G'$ to G and G' respectively which define the multiplications of G and G'. Therefore there exist local homomorphisms δ and δ' of $\mathcal{O}$ and $\mathcal{O}'$ to the local rings $\mathcal{O}_1=\mathcal{O}_{e\times e, G\times G}$ and $\mathcal{O}'_1=\mathcal{O}_{e'\times e', G'\times G'}$ of $G\times G$ and $G'\times G'$ respectively such that $\delta\alpha^*=(\alpha\times\alpha)^*\delta'$.

Now we put $R=\mathcal{O}/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal of $\mathcal{O}$ generated by the image $\alpha^*(\mathfrak{m}')$ of the maximal ideal $\mathfrak{m}'$ of $\mathcal{O}'$ by α^*, and let ϕ be the canonical homomorphism of $\mathcal{O}$ onto $R=\mathcal{O}/\mathfrak{a}$. On the other hand it is easy to see that $\mathcal{O}_1$ (resp. $\mathcal{O}'_1$) is isomorphic to the quotient ring $(\mathcal{O}\otimes_k\mathcal{O})_{\mathfrak{n}}$ (resp. $(\mathcal{O}'\otimes_k\mathcal{O}')_{\mathfrak{n}'}$) with respect to the prime ideal $\mathfrak{N}$ (resp. $\mathfrak{N}'$), where $\mathfrak{n}$ (resp. $\mathfrak{n}'$) is the ideal $\mathfrak{m}\otimes_k\mathcal{O}+\mathcal{O}\otimes_k\mathfrak{m}$ of $\mathcal{O}\otimes_k\mathcal{O}$ (resp. $\mathfrak{m}'\otimes_k\mathcal{O}'+\mathcal{O}'\otimes_k\mathfrak{m}'$ of $\mathcal{O}'\otimes_k\mathcal{O}'$), and hence if we identify $\mathcal{O}'_1$ with the subring $(\alpha\times\alpha)^*(\mathcal{O}'_1)$ of $\mathcal{O}_1$, $\mathcal{O}'\otimes_k\mathcal{O}'$ is a subring of $\mathcal{O}\otimes_k\mathcal{O}$ and $\mathfrak{n}'$ is equal to $\mathfrak{n}\cap(\mathcal{O}'\otimes_k\mathcal{O}')$. Therefore $\mathcal{O}_1/\mathfrak{n}'\mathcal{O}_1$ is isomorphic to $(\mathcal{O}\otimes_k\mathcal{O}/\mathfrak{n}'(\mathcal{O}\otimes_k\mathcal{O}))_{\mathfrak{n}/\mathfrak{n}'(\mathcal{O}\otimes_k\mathcal{O})}=\mathcal{O}\otimes_k\mathcal{O}/\mathfrak{n}'(\mathcal{O}\otimes_k\mathcal{O})$, since $\mathcal{O}\otimes_k\mathcal{O}/\mathfrak{n}'(\mathcal{O}\otimes_k\mathcal{O})$ is a local ring. Moreover $\mathcal{O}\otimes_k\mathcal{O}/\mathfrak{n}'(\mathcal{O}\otimes_k\mathcal{O})$ is equal to $\mathcal{O}\otimes_k\mathcal{O}/(\mathfrak{a}\otimes_k\mathcal{O}+\mathcal{O}\otimes_k\mathfrak{a})\cong\mathcal{O}/\mathfrak{a}\otimes_k\mathcal{O}/\mathfrak{a}=R\otimes_kR$. This means that there exists a canonical homomorphism ψ of $\mathcal{O}_1=\mathcal{O}_{e\times e, G\times G}$ to $R\otimes_kR$ whose kernel is the ideal $\mathfrak{n}'\mathcal{O}_1$. Then we see that the kernel of the homomorphism $\psi\circ\delta$ of $\mathcal{O}$ to $R\otimes_kR$ contains $\mathfrak{a}$. In fact $\alpha^*(\mathfrak{m}')$ generates $\mathfrak{a}$ and we have $(\psi\delta\alpha^*)(\mathfrak{m}')=\psi(\alpha\times\alpha)^*(\delta'(\mathfrak{m}'))\subset\psi(\alpha\times\alpha)^*(\mathfrak{m}'_1)\subset\psi(\mathfrak{n}'\mathcal{O}_1)=0$,

where $\mathfrak{m}'_1$, is the maximal ideal of $\mathcal{O}'_1$. Hence there exists a homomorphism Δ_R of R into $R\otimes_k R$ such that $\Delta_R\circ\phi=\psi\circ\delta$. Since R is equal to $\mathcal{O}/\mathfrak{a}$, there exists a canonical homomorphism ε_R of R onto $k=R/\mathfrak{m}_R$, where $\mathfrak{m}_R$ is the maximal ideal $\mathfrak{m}/\mathfrak{a}$ of R. Then we can easily see that $(R, \Delta_R, \varepsilon_R)$ is a coalgebra over k, since Δ_R and ε_R are defined by dualizing the multiplication of G and the injection of the unit point e into G. We omit the detail proof. This means that $(R, m_R, \eta_R, \Delta_R, \varepsilon_R)$ is a bialgebra over k, where m_R and η_R are the multiplication of the ring R and the injection of k into R respectively.

Moreover let γ (resp. γ') be the k-morphism of G (resp. G') onto itself such that $\gamma(x)=x^{-1}$ for any point x in G (resp. $\gamma'(x')=x'^{-1}$ for any point x' in G'). Then there exist automorphisms γ^* and γ'^* of O and O' respectively such that $\gamma^*\alpha^*=\alpha^*\gamma'^*$. From this we see that $\mathfrak{a}=\gamma^*(\mathfrak{a})$ and hence there exists an automorphism c_R of R, which is an antipode of the bialgebra $(R, m_R, \eta_R, \Delta_R, \varepsilon_R)$ over k, since c_R is obtained from the morphism γ. Therefore $\mathrm{Spec}(R)$ has a structure of an affine group scheme over k and there exists a closed immersion j_α of $\mathrm{Spec}(R)$ into G such that j_α is a morphism of group schemes over k (cf. Chap. I in [10]). The group scheme $\mathrm{Spec}(R)$ over k is called *the kernel of the purely inseparable isogeny α of G* and denoted by *$\mathrm{Ker}\,\alpha$*. We also say that R is *the bialgebra (or Hopf algebra) of the group subscheme $\mathrm{Ker}\,\alpha$ of G*.

LEMMA 14. *Let G, G' and α be as above. Then the dual space R^* of the bialgebra R of $\mathrm{Ker}\,\alpha$ is canonically isomorphic to the subbialgebra $N(\alpha)$ of $\mathfrak{H}(G)$ corresponding to the isogeny α as vector spaces over k.*

PROOF. If u is an element of $N(\alpha)$, u maps $\mathcal{O}=\mathcal{O}_{e,G}$ into itself, since any left invariant semi-derivation is regular at any closed point of G. Then if π is the natural homomorphism of $\mathcal{O}$ onto $k=\mathcal{O}/\mathfrak{m}_{e,G}$, $\pi\circ(u\,|_e)$ is a k-linear mapping of $\mathcal{O}$ to k. Moreover, since u is $\alpha^*(k(G'))$-linear by the definition of $N(\alpha)$, the image of $\mathfrak{a}=\alpha^*(\mathfrak{m}')\mathcal{O}$ by u is in $\mathfrak{a}$, where $\mathfrak{m}'$ is the maximal ideal of $\mathcal{O}'=\mathcal{O}_{e',G'}$. This means that $\pi\circ(u\,|_e)$ induces a k-linear mapping of $R=\mathcal{O}/\mathfrak{a}$ to k, which will be denoted by $\lambda(u)$. We shall show that the mapping λ of $N(\alpha)$ to R^* is an isomorphism over k. First we see that λ is injective. In fact any element u of $N(\alpha)$ is decomposed to $\xi+u_1$, where ξ is in k and u_1 is in $\mathfrak{g}(G)$, and $\pi\circ(u_1\,|_e)$ is the local component u_{1e} of u_1. Therefore λ is injective by Corollary of Proposition 12 and the surjectivity of π. As to show the surjectivity of λ, it suffices to see that $\dim_k N(\alpha)=\dim_k R=\dim_k R^*$. Identifying $\mathcal{O}'$ with $\alpha^*(\mathcal{O}')$ in $\mathcal{O}$, we easily see that $\mathcal{O}$ is a finite $\mathcal{O}'$-module, since α is a purely inseparable isogeny. Therefore the relative multiplicity $rm(\mathfrak{m}'\mathcal{O}:\mathcal{O}')$ of the primary ideal $\mathfrak{m}'\mathcal{O}$ of $\mathcal{O}$ with respect to $\mathcal{O}'$ is defined and equal to $e(\mathfrak{m}'\mathcal{O})[\mathcal{O}/\mathfrak{m}:\mathcal{O}'/\mathfrak{m}']$ by definitions, where $\mathfrak{m}$ and $\mathfrak{m}'$ are the maximal ideals of $\mathcal{O}$ and $\mathcal{O}'$ respectively (cf. §4 in [9]). Moreover $rm(\mathfrak{m}'\mathcal{O};\mathcal{O}')$ is equal to $[k(G):k(G')]e(\mathfrak{m}')$ by Corollary 2 of Theorem 2 in [9]. Since $\mathcal{O}'$ is a regular local ring, the multiplicity $e(\mathfrak{m}')$ is equal to 1 and hence $[k(G):k(G')]$ is equal to the

multiplicity $e(\mathfrak{m}'O)$ of the primary ideal $\mathfrak{m}'O$ of O. On the other hand any system of parameters of O is a distinct system of parameters of O by Theorem 4 in [9], since O is a regular local ring. $\mathfrak{m}'$ is generated by a regular system of parameters of O' and hence $\mathfrak{m}'O$ is a primary ideal generated by a system of parameters of O. This means by the definition of a distinct system of parameters that $e(\mathfrak{m}'O)=l(O/\mathfrak{m}'O)=l(R)=\dim_k R$. Therefore we have $\dim_k R=[k(G):k(G')]$. On the other hand we see $\dim_k N(\alpha)=[k(G):k(G')]$ by (A) in §6, and hence $\dim_k N(\alpha)=\dim_k R=\dim_k R^*$. q. e. d.

THEOREM 4. *Let G and G' be group varieties defined over k and let α be a purely inseparable isogeny of G onto G' defined over k. Then the bialgebra R of the group subscheme Ker α of G is isomorphic to the linear dual $N(\alpha)^D$ of the subbialgebra $N(\alpha)$ of $\mathfrak{H}(G)$ corresponding to α as bialgebras over k.*

PROOF. Since $R^{DD}=R$, it suffices to show that $R^D=(R^*, \Delta_R^*, \varepsilon_R^*, m_R^*, \eta_R^*)$ is isomorphic to $N(\alpha)=(N(\alpha), m_G, \eta_G, \Delta_G, \varepsilon_G)$. We may identify R^* with $N(\alpha)$ by λ in the proof of Lemma 14. If u is in $N(\alpha)$, $\Delta_G(u)(f_1\otimes f_2)=u(f_1f_2)$ by (C) in §6 for any f_1 and f_2 in $k(G)$. Therefore, for any u in $R^*=N(\alpha)$, $m_R^*(u)(f_1\otimes f_2)=(uR)(f_1\otimes f_2)=u(f_1f_2)=\Delta_G(u)(f_1\otimes f_2)$. This means that $\Delta_G(u)=m_G^*(u)$ and hence that $\Delta_G|_{N(\alpha)}=m_G^*$. Next we show that $\Delta_R^*=m_G|_{N(\alpha)}$. If $\bar{f}$ is an element of R represented by an element f in $O=O_{e,G}$, $\Delta_R(\bar{f})$ is the class of $\mu^*(f)$ of $O\otimes_k O$ mod. $\mathfrak{a}\otimes O+O\otimes\mathfrak{a}$, where μ is the k-morphism of $G\times G$ onto G defining the multiplication of G. Now we identify the field $k(G\times G)$ with $k(x, y)$, where x and y are independent generic points of G over k. Let $\{t_1, \cdots, t_n\}$ be a regular system of parameters of O and let $\{I_{e_1\cdots e_n}\}$ be the canonical basis of $\mathfrak{H}(G)$ with respect to $\{t_1, \cdots, t_n\}$. Then $\mu^*(f)=f(xy)$ is equal to, by Theorem 2,

$$\sum_{e_i, e_j'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})_e(f)\xi_1^{e_1}\cdots\xi_n^{e_n}\eta_1^{e_1'}\cdots\eta_n^{e_n'}$$

$$+\sum_{i=1}^{n}a_i(x, y)\xi_i^{p^r}+\sum_{i=1}^{n}b_i(x, y)\eta_i^{p^r},$$

and hence $\Delta_R(\bar{f})$ is equal to

$$\sum_{e_i, e_j'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})_e(f)\bar{\xi}_1^{e_1}\cdots\bar{\xi}_n^{e_n}\bar{\eta}_1^{e_1'}\cdots\bar{\eta}_n^{e_n'}$$

for a large r, where $\xi_i=t_i(x)$ and $\eta_i=t_i(y)$ for $i=1, 2, \cdots, n$. Let u and v be in R^*. Then we have

$$\Delta_R^*(u\otimes v)(\bar{f})=(u\otimes v)\Delta_R(\bar{f})$$

$$=\sum_{e_i, e_j'<p^r}(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})_e(f)u(\xi_1^{e_1}\cdots\xi_n^{e_n})v(\eta_1^{e_1'}\cdots\eta_n^{e_n'}).$$

As we see in the proof of Theorem 1, we have $(I_{e_1\cdots e_n})_e(t_1^{e_1}\cdots t_n^{e_n})=1$ and $(I_{e_1\cdots e_n})_e(t_1^{e_1'}\cdots t_n^{e_n'})=0$ for $(e_1, \cdots, e_n)\neq(e_1', \cdots, e_n')$, and hence

$$\Delta_R^*(I_{e_1\cdots e_n}\otimes I_{e_1'\cdots e_n'})(\bar{f})=(I_{e_1\cdots e_n}I_{e_1'\cdots e_n'})_e(f)$$
$$=m_G(I_{e_1\cdots e_n}\otimes I_{e_1'\cdots e_n'})(\bar{f}).$$

This shows that $\Delta_R^*=m_G$, since $\{I_{e_1\cdots e_n}\}$ is a basis of $\mathfrak{H}(G)$. The equalities $\varepsilon_G=\eta_R^*$ and $\eta_G=\varepsilon_R^*$ can be also varified easily, but we omit the proof. q.e.d.

COROLLARY 1. *$\mathfrak{H}(G)=k\oplus\mathfrak{G}(G)$ is a Hopf algebra over k.*

PROOF. $\mathfrak{H}(G)$ is the union of $\mathfrak{H}_r(G)$ $(r=1, 2, \cdots)$, which are equal to $N(\pi_r)$ corresponding to the Frobenius isogeny π_r of height r. By Theorem 4, $N(\pi_r)$ is isomorphic to the linear dual R^D of the Hopf algebra R of Ker π_r. Therefore $N(\pi_r)$ is a Hopf algebra over k with the antipode c_r. Then it is clear that $c_{r'}|_{N(\pi_r)}=c_r$ if $r'>r$. Therefore $\mathfrak{H}(G)$ has an antipode c_G such that $c_G|_{N(\pi_r)}=c_r$. q.e.d.

COROLLARY 2. *Let G, G' and G'' be group varieties defined over k, and let α and β be purely inseparable isogenies of G onto G' and G'' defined over k respectively. Then there exists an isogeny γ of G' onto G'' such that $\beta=\gamma\circ\alpha$ if and only if there exists a k-morphism σ of Ker α to Ker β as group k-schemes such that $j_\alpha=j_\beta\circ\sigma$, where j_α and j_β are the closed immersions of Ker α and Ker β into G respectively.*

PROOF. Assume that there exists an isogeny γ of G' onto G'' such that $\beta=\gamma\circ\alpha$. Then we see that the local homomorphism β^* of $\mathcal{O}''=\mathcal{O}_{e'',G''}$ into $\mathcal{O}=\mathcal{O}_{e,G}$ decomposes into $\alpha^*\circ\gamma^*$. Let $\mathfrak{m}'$ and $\mathfrak{m}''$ be the maximal ideals of $\mathcal{O}'=\mathcal{O}_{e',G'}$ and $\mathcal{O}''$ respectively. If we put $\mathfrak{a}=\alpha^*(\mathfrak{m}')\mathcal{O}$ and $\mathfrak{b}=\beta^*(\mathfrak{m}'')\mathcal{O}$, $\mathfrak{D}$ contains $\mathfrak{B}$, since $\gamma^*(\mathfrak{m}'')\subset\mathfrak{m}'$. Therefore there exists a natural homomorphism ϕ of $S=\mathcal{O}/\mathfrak{b}$ onto $R=\mathcal{O}/\mathfrak{a}$, which defines a k-morphism σ of Ker $\alpha=$ Spec(R) to Ker $\beta=$Spec(S). Then it is easy to see that σ is a morphism of group schemes over k and that $j_\alpha=j_\beta\circ\sigma$. Conversely assume that there exists a morphism σ of Ker $\alpha=$Spec(R) to Ker $\beta=$Spec(S) such that $j_\alpha=j_\beta\circ\sigma$. Then σ^* is a bialgebra homomorphism of S onto R and hence the dual mapping h of σ^* is an injection of R^D into S^D. This means by Theorem 4 that $N(\alpha)$ is a subbialgebra of $N(\beta)$, and hence that there exists an isogeny γ of G' onto G'' such that $\beta=\gamma\circ\alpha$ by (E) in §6. q.e.d.

Next we give a characterization for a group subscheme of a group variety G to be the kernel of a purely inseparable isogeny of G. Let G be as above and X a group k-subscheme of G with the underlying topological space consisting of one point e. Then X is Spec$(\mathcal{O}_{e,G}/\mathfrak{a})$, where $\mathfrak{a}$ is a primary ideal belonging to the maximal ideal of $\mathcal{O}_{e,G}$. Such a group k-subscheme will be called a group k-subscheme with one point. Let g be a closed point of G and τ_g the k-morphism $R_gL_{g^{-1}}=L_{g^{-1}}R_g$ of G onto itself. Denote by τ_g^* the automorphism of $\mathcal{O}_{e,G}$ attached to τ_g. Then $X=$Spec$(\mathcal{O}_{e,G}/\mathfrak{a})$ is called *an invariant group subscheme with one point of G* if $\tau_g^*(\mathfrak{a})=\mathfrak{a}$ for any closed point g of G.

Then we have the following

THEOREM 5. *Let G be a group variety defined over k. Then a group k-subscheme X with one point of G is invariant if and only if X is the kernel of a purely inseparable isogeny of G defined over k.*

PROOF. First we assume that X is $Ker\,\alpha = \mathrm{Spec}(O/\mathfrak{a})$, where $O = O_{e,G}$. If $N(\alpha)$ is the subbialgebra of $\mathfrak{H}(G)$ corresponding to α, $v(\mathfrak{a})$ is contained in $\mathfrak{a}$ for any v in $N(\alpha)$ as seen in the proof of Lemma 14. Moreover if u is in $N(\alpha)$, $R_g^{*-1}uR_g^*$ is in $N(\alpha)$ by Theorem 3. Therefore we see that $R_g^{*-1}uR_g^*(\mathfrak{a}) \subset \mathfrak{a}$ for any u in $N(\alpha)$. This means that $uR_g^*(\mathfrak{a}) \subset R_g^*(\mathfrak{a})$ for any u in $N(\alpha)$. Since u commutes with L_g^* and $\tau_g^* = L_{g^{-1}}^* R_g^*$, we have $u\tau_g^*(\mathfrak{a}) \subset \tau_g^*(\mathfrak{a})$. On the other hand if a proper ideal $\mathfrak{b}$ of O is such that $u(\mathfrak{b}) \subset \mathfrak{b}$ for any u in $N(\alpha)$, $\mathfrak{b}$ is contained in $\mathfrak{a}$. In fact if otherwise, there exists an element f in $\mathfrak{b}$ but not in $\mathfrak{a}$. Then there exists an element u in $N(\alpha)$ such that $u(f)$ is not in the maximal ideal $\mathfrak{m}$ of O, since $N(\alpha)$ is canonically isomorphic to the dual space of $O/\mathfrak{a}$ by Lemma 14. This means that $u(\mathfrak{b})$ is not contained in $\mathfrak{B}$. A contradiction. Therefore $\tau_g^*(\mathfrak{a})$ is contained in $\mathfrak{a}$, and hence $X = \mathrm{Spec}(O_e/\mathfrak{a})$ is invariant.

Conversely we assume that $X = \mathrm{Spec}(O/\mathfrak{a})$ is an invariant group k-subscheme with one point of G. Then $\mathfrak{a}$ is an $\mathfrak{m}$-primary ideal and hence $\mathfrak{a}$ contains the ideal $\mathfrak{a}_r = (t_1^{p^r}, \cdots, t_n^{p^r})O$ for some $r > 0$, where $\{t_1, \cdots, t_n\}$ is a regular system of parameters of O. Then $X_r = \mathrm{Spec}(O/\mathfrak{a}_r)$ is the kernel of the Frobenies morphism π_r of height r and there exists a k-morphism γ of X to X_r which is a morphism of group k-schemes. Then composite morphism $j_{\pi_r} \circ \gamma$ is the natural injection of X into G. On the other hand $\mathfrak{H}_r(G) = N(\pi_r)$ is isomorphic to the linear dual of $O/\mathfrak{a}_r$ and hence the bialgebra $(O/\mathfrak{a})^D$ is considered as a subbialgebra of $\mathfrak{H}_r(G)$ which consists of the elements u in $\mathfrak{H}_r(G)$ such that $u(\mathfrak{a}) \subset \mathfrak{m}$. Since X is invariant by our assumption, $\tau_g^*(\mathfrak{a}) = \mathfrak{a}$ for any closed point g of G. Therefore if u is in $(O/\mathfrak{a})^D$, we have $u\tau_g^*(\mathfrak{a}) = u(\mathfrak{a}) \subset \mathfrak{m}$ and hence $\tau_g^{*-1}u\tau_g^*(\mathfrak{N}) \subset \tau_g^{*-1}\mathfrak{m} = \mathfrak{m}$. However we have $\tau_g^{*-1}u\tau_g^* = R_g^{*-1}uR_g^*$, since $\tau_g^* = L_{g^{-1}}^* R_g^*$ and $L_{g^{-1}}^* u = uL_{g^{-1}}^*$. This means that $R_g^{*-1}uR_g^*(\mathfrak{a}) \subset \mathfrak{m}$ and hence $R_g^{*-1}uR_g^*$ is in $(O/\mathfrak{a})^D$. Therefore $(O/\mathfrak{a})^D$ is a subbialgebra of $\mathfrak{H}_r(G)$ which is stable under the adjoint representation of G. By Theorem 3 this shows that $(O/\mathfrak{a})^D$ is $N(\alpha)$ for some purely inseparable isogeny α of G. Then it is clear that $X = \mathrm{Spec}(O/\mathfrak{a})$ in $Ker\,\alpha$. q. e. d.

References

[1] I. Barsotti, "Abelian varieties over fields of positive characteristics," Rend. Circ. Mat. Palermo. vol. **5** (1956), pp. 145-169.

[2] P. Cartier, "Calcul différentiel sur les variétés algébsiques en caractéristique non nulle," Comptes Rendus, vol. **245** (1957), pp. 1109-1111.

[3] ———, "Isogenies des variétés de groupes," Bull. Soc. Math. France, vol. **87** (1959), pp. 191-220.

[4] ———, "Arithmétique des groupes algébriques," Colloque. Theorie des Groupes algébriques à Bruxelles (1962). (Centre belge de Rech. Math.) pp. 87-111.
[5] M. Demazure et A. Grothendieck, "Séminaire de Geom. Alg. 1963-64, Schemas en Groupes," 2A, 2B. Mimeographed Notes of I. H. E. S.
[6] J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique $p > 0$," Comm. Math. Helv. vol. **28** (1954), pp. 87-118.
[7] A. Grothendieck, "Éléments de géometrie algébrique," I, II, ..., Publ. Math. No. **4** (1960), **8** (1961), ...
[8] S. Lang, "Introduction to Algebraic Geometry," Interscience tracts in pure and applied Math. no. **5**, 1958.
[9] M. Nagata, "The theory of multiplicity in general local rings," Proc. Int. Symp. on Alg. Number Theory, Tokyo & Nikko (1955), pp. 191-226.
[10] F. Oort, "Commutative group schemes," Lecture Notes in Math. (1966), Springer-Verlag.
[11] J. -P. Serre, "Quelques propriétés des variétés abéliennes an caractéristique p," Amer. J. Math. vol. **80** (1958), pp. 715-739.
[12] A. Weil, "Foundations of Algebraic Geometry," Amer. Math. Soc. Colloquium Pub. New York, 1962.
[13] ———, "Variétés abéliennes et courbes algébriques," Paris, 1948.

Department of Mathematics,
Faculty of Science,
Hiroshima University.