HIROSHIMA MATH. J.
1 (1971), 227-251

Some Properties of Hopf Algebras Attached to Group Varieties

Hiroshi YANAGIHARA
(Received September 17, 1971)

In the previous paper [8] we developed a theory of invariant semi-derivations on group varieties defined over an algebraically closed field k of a positive characteristic p. Let G be a group variety defined over k and $\mathfrak{g}(G)$ the set of all left invariant semi-derivations of G. Then the direct sum $\mathfrak{H}(G)=k\oplus\mathfrak{g}(G)$ is a subalgebra of $\mathrm{End}_k(k(G))$, where $k(G)$ is the field of the ra-toinal functions on G over k. This structure has a close connection with the group multiplication of G. On the other hand $\mathfrak{H}(G)$ may be identified with the set of point distributions of the local ring $\mathcal{O}$ of G at the neutral element e, and then $\mathfrak{H}(G)$ has a structure of a coalgebra induced dually from that of $\mathcal{O}$ as an algebra over k. These structures give to $\mathfrak{H}(G)$ a Hopf algebra structre over k. Using this structure we obtained some results on purely inseparable isogenies of group varieties in [8].

In this paper we shall show that our theory of the Hopf algebras $\mathfrak{H}(G)$ has more applications not only to the theory of purely insparable isogenies of group varieties, but also to the general theory of algebraic groups over a field of a positive charabteristic p. In particular $\mathfrak{H}(G)$ may play a similar role to that of the Lie algebra of invariant derivations on a group variety in the case of characteristic zero.

In §1 we give some definitions and results on Hopf algebras over a field which are necessary in the later sections. Let $\mathcal{C}$ be the category of commutative and cocommutative Hopf algebras over a field k which are a union of finite dimensional Hopf subalgebras. Then it is shown that $\mathcal{C}$ is an abelian category. In the next section we shall obtain a criterion, in the languages of Hopf algebras, for a morphism of a group variety to another to be separable. For this purpose we give a generalization of the theorem in the paper [4] on the existence of convenient pair of local parameters at the neutral elements for a given purely inseparable isogeny of group varieties. As an application of this criterion we give a modification of Serre's results on the group $\mathrm{Ext}(A, B)$ in §3, where A and B are commutative group varieties. He treated in [6] the case of purely inseparable isogenies of exponent 1 making use of the Galois theory for such isogenies. However we obtain the same result for any purely insepárble isogeny of a commutative group variety using our Hopf algebras. Of course this result may be obtained in a different way if we use the fact that the category of commutative algebraic group schemes over a field is abelian. In §4 we consider a rational representation ϕ of a group variety to the group GL_V of linear transformations of a vector space V over k. Then we give an operation of the Hopf algebra $\mathfrak{H}(G)$ attached to G on V determined by ϕ and show that a subspace W of V is a G-submodule of V if and only if W is a $\mathfrak{H}(G)$-submodule of V. This is a modification, in a positive characteristic case, of the similar result in the case of characteristic zero, where the Lie algebra of invariant derivations works instead of the Hopf algebra $\mathfrak{H}(G)$. In the last section a condition for a Hopf subalgebra of $\mathfrak{H}(G)$ to be an algebraic one is given. For this purpose some results on formal groups over a field k are shown.

The terminologies are the same as in the paper [8], but as to those of Hopf algebras we shall refer to the book [7] freely.

§1 Preliminary results on Hopf algebras

In this section we give some results on Hopf algebras over a field k, which are necessary in the later. Let $(\mathfrak{H}, m, \eta, \Delta, \varepsilon, c)$ be a Hopf algebra over a field k with antipode c, where $(\mathfrak{H}, m, \eta)$ (resp. $(\mathfrak{H}, \Delta, \varepsilon)$) is the algebra structure with multiplication m and unit η (resp. the coalgebra structure with diagonal Δ and augmentation ε). We may sometimes identify k with its image $\eta(k)$ in $\mathfrak{H}$. We denote by $\mathfrak{H}^+$ the kernel $\varepsilon^{-1}(0)$ of the augmentation ε. Let $\mathfrak{H}'$ be another Hopf algebra over k and u a Hopf algebra homomorphism. Then we understand by *the h-kernel of u* the set of the elements x in $\mathfrak{H}$ such such that $(id_{\mathfrak{H}}\otimes u)\,\Delta(x)=x\otimes 1$ and denote it by h-ker u. It is known that h-ker u is a Hopf subalgebra of $\mathfrak{H}$ if $\mathfrak{H}$ is cocommutative (cf. Lemma 16.1.1 in [7]). Similarly we denote by h-coker u the quotent space $\mathfrak{H}'/u(\mathfrak{H}^+)\mathfrak{H}'$, where $u(\mathfrak{H}^+)\mathfrak{H}'$ is the right idal of $\mathfrak{H}'$ generated by $u(\mathfrak{H}^+)$. Then it is also known that h-coker u has a Hopf algebra structure such that the natural homomorphism of H' onto h-coker u is a Hopf algebra homomorphism, if $u(\mathfrak{H}^+)\mathfrak{H}'$ is a two-sided ideal of $\mathfrak{H}'$ (cf. Lemma 16.1.2. in [7]). In particuar if $\mathfrak{H}'$ is commutative, h-coker u is a Hopf algebra.

A sequence

$$\cdots\longrightarrow\mathfrak{H}_{i-1}\xrightarrow{u_{i-1}}\mathfrak{H}_i\xrightarrow{u_i}\mathfrak{H}_{i+1}\xrightarrow{u_{i+1}}\cdots$$

of Hopf algebras $\mathfrak{H}_i$ with Hopf algebra homomorphisms u_i is called *exact* if h-ker u_i is equal to the image of $\mathfrak{H}_{i-1}$ under u_{i-1} for each i. Let $(\mathfrak{H}, m, \eta, \Delta, \varepsilon, c)$ and $(\mathfrak{H}', m', \eta', \Delta', \varepsilon', c')$ be two Hopf algebras ovar k. Then it is easy to see that the tensor product $\mathfrak{H}\otimes_k\mathfrak{H}'$ has a natural Hopf algebra structure $(\mathfrak{H}\otimes_k\mathfrak{H}', \bar{m}, \bar{\eta}, \bar{\Delta}, \bar{c})$ such that the canonical injections j and j' of $\mathfrak{H}$ and $\mathfrak{H}'$ into $\mathfrak{H}\otimes_k\mathfrak{H}'$ given by $j(x)=x\otimes 1$ and $j'(y)=1\otimes y$ are Hopf algebra homomorphisms respectively. Moreover we have the following

PROPOSITION 1. *Let $\mathfrak{H}$ and $\mathfrak{H}'$ be cocommutative Hopf algebras over k. Let*

j be the canonical injection of $\mathfrak{H}$ into $\mathfrak{H}\otimes_k\mathfrak{H}'$ defined by $j(x)=x\otimes 1$ and ρ the linear mapping of $\mathfrak{H}\otimes_k\mathfrak{H}'$ onto $\mathfrak{H}'$ defined by $\rho(x\otimes y)=\varepsilon(x)y$. Then the sequence

$$k\xrightarrow{\eta}\mathfrak{H}\xrightarrow{j}\mathfrak{H}\otimes_k\mathfrak{H}'\xrightarrow{\rho}\mathfrak{H}'\xrightarrow{\varepsilon'}k$$

is exact.

PROOF. It is easy to see that j (resp. ρ) is a Hopf algebra homomorphism (resp. an algebra homomorphism). Let x and y be elements of $\mathfrak{H}$ and $\mathfrak{H}'$ respectivey, and put $\Delta(x)=\sum_{(x)} x_{(1)}\otimes x_{(2)}$ and $\Delta'(y)=\sum_{(y)} y_{(1)}\otimes y_{(2)}$. Then we have $\bar{\Delta}(x\otimes y)=\sum_{(x),(y)} x_{(1)}\otimes y_{(1)}\otimes x_{(2)}\otimes y_{(2)}$, by definition of $\bar{\Delta}$, and $(\rho\otimes\rho)\bar{\Delta}(x\otimes y)=(\rho\otimes\rho)(\sum_{(x),(y)} x_{(1)}\otimes y_{(1)}\otimes x_{(2)}\otimes y_{(2)})=\sum_{(x),(y)}\varepsilon(x_{(1)})y_{(1)}\otimes\varepsilon(x_{(2)})y_{(2)}=\varepsilon(x)\Delta'(y)=\Delta'(\varepsilon(x)y)=\Delta'(\rho(x\otimes y))$. Since we have $\varepsilon'\rho=\bar{\varepsilon}$ and $c'\rho=\bar{c}$, this means that ρ is a Hopf algebra homomorphism. Next we show that h-ker j is $\eta(k)$. Let $\{x_i\}_{i\in I}$ be a basis of $\mathfrak{H}$ over k such that $\eta(1)=x_0$, and let x be an element of h-ker j. If $\Delta(x)=\sum_{i,j\in I}\xi_{ij}x_i\otimes x_j$, we have $\xi_{ij}=\xi_{ji}$ by cocommutativity of $\mathfrak{H}$ and $\sum_{i,j\in I}\xi_{ij}x_i\otimes x_j\otimes 1=(id_{\mathfrak{H}}\otimes j)\Delta(x)=x\otimes 1\otimes 1$. Therefore we have $\xi_{ij}=\xi_{ji}=0$ for $i\neq j$, $\xi_{ii}=0$ for $i\neq 0$ and $x=\xi_{00}x_0=\eta(\xi_{00})\in\eta(k)$. This means thant the sequence $k\xrightarrow{\eta}\mathfrak{H}\xrightarrow{j}\mathfrak{H}\otimes_k\mathfrak{H}'$ is exact. Now let $\sum_i x_i\otimes y_i$ be in h-ker ρ and put $\Delta(x_i)=\sum_{(y_j)} x_{i,(1)}\otimes x_{i,(2)}$ and$\Delta'(y_j)=\sum_{(x_i)} y_{j,(1)}\otimes y_{j,(2)}$. Then we have

$$\begin{aligned}\sum_i x_i\otimes y_i\otimes 1&=(\mathrm{id}_{\mathfrak{H}\otimes\mathfrak{H}'}\otimes\rho)\bar{\Delta}(\sum_i x_i\otimes y_i)\\&=\sum_{i,(x_i),(y_i)} x_{i,(1)}\otimes y_{i,(1)}\otimes\varepsilon(x_{i,(2)})y_{i,(2)}\\&=\sum_{i,(x_i)}\varepsilon(x_{i,(2)})x_{i,(1)}\otimes\Delta'(y_i)\\&=\sum_i x_i\otimes\Delta'(y_i),\end{aligned}$$

since we have $(\varepsilon\otimes id_{\mathfrak{H}})\Delta=id_{\mathfrak{H}}$. We may assume that the set $\{x_i\}$ is linearly independent over k, and hence that $\Delta'(y_i)=y_i\otimes 1$ for each i. This means that y_i is in $k=\eta'(k)$ and that $\sum_i x_i\otimes y_i$ is in the image of j. Conversely it can be seen that h-ker ρ contains the image of j. Therefore the sequence $\mathfrak{H}\xrightarrow{j}\mathfrak{H}\otimes_k\mathfrak{H}'\xrightarrow{\rho}\mathfrak{H}'$ is exact. Lastly the h-kernel of ε' is $\mathfrak{H}'$, since $(id_{\mathfrak{H}'}\otimes\varepsilon')\Delta'=id_{\mathfrak{H}'}$. This completes the proof. q. e. d.

Let $\mathscr{C}$ be the category of commutative and cocommutative Hopf algebras over k such that any object of $\mathscr{C}$ is a union of finite dimensional Hopf subalgebras and that the morphisms of $\mathscr{C}$ are Hopf algebra homomorphisms. It is known that the full subcategory $\mathscr{C}'$ of $\mathscr{C}$ whose objects are of finite dimensions is an abelian category. Using this fact we show that $\mathscr{C}$ is also abelian. Recall that the group composition of $\mathrm{Hom}_{\mathscr{C}}(\mathfrak{H}, H')$ is given by the convolution

$f*g=m'(f\otimes g)\Delta$ for f and g in $\mathrm{Hom}_{\mathscr{C}}(\mathfrak{H}, \mathfrak{H}')$, that the inverse of f is $c'f=fc$ and that the neutral element of $\mathrm{Hom}_{\mathscr{C}}(\mathfrak{H}, \mathfrak{H}')$ is $\eta'\varepsilon$. First we give the following lemmas.

LEMMA 1. *Let $\mathfrak{H}'$ and $\mathfrak{H}''$ be Hopf subalgebras of a Hopf algebra $\mathfrak{H}$ over a field k. Then the intersection $\mathfrak{H}'\cap\mathfrak{H}''$ is also a Hopf subalgebra of $\mathfrak{H}$.*

PROOF. Let $\{x_\lambda\}_{\lambda\in L}$ be a basis of $\mathfrak{H}'\cap\mathfrak{H}''$ over k and let $\{x_\lambda\}_{\lambda\in L}\cup\{x'_\mu\}_{\mu\in M}$ (resp. $\{x_\lambda\}_{\lambda\in L}\cup\{x''_\nu\}_{\nu\in N}$) be a basis of $\mathfrak{H}'$ (resp. of $\mathfrak{H}''$) over k. Then the set $\{x_\lambda\}_{\lambda\in L}\cup\{x'_\mu\}_{\mu\in M}\cup\{x''_\nu\}_{\nu\in N}$ is linearly independent over k. If x is an element of $\mathfrak{H}'\cap\mathfrak{H}''$, $\Delta(x)$ is a linear combination of the elements $x_\lambda\otimes x_{\lambda'}$, $x_\lambda\otimes x'_{\mu'}$, $x'_\mu\otimes x_{\lambda'}$ and $x'_\mu\otimes x'_{\mu'}$ (λ, $\lambda'\in L$, μ, $\mu'\in M$) with uniquely determined coefficients in k since x is in $\mathfrak{H}'$. Similaly $\Delta(x)$ is a linear combination of the elements $x_\lambda\otimes x_{\lambda'}$, $x_\lambda\otimes x''_{\nu'}$, $x''_\nu\otimes x_{\lambda'}$ and $x''_\nu\otimes x''_{\nu'}$ (λ, $\lambda'\in L$ ν, and $\nu'\in N$), since x is in $\mathfrak{H}''$. Therefore $\Delta(x)$ must be a linear combination of the elements $x_\lambda\otimes x_{\lambda'}(\lambda, \lambda'\in L)$, since $x_\lambda\otimes x_{\lambda'}$, $x_\lambda\otimes x'_{\mu'}$, $x_\lambda\otimes x''_{\nu'}$, $x'_\mu\otimes x_{\lambda'}$, $x'_\mu\otimes x'_{\mu'}$, $x''_\nu\otimes x_{\lambda'}$ and $x''_\nu\otimes x''_{\nu'}$ are linearly independent over k. This means that $\mathfrak{H}'\cap\mathfrak{H}''$ is a subcoalgebra of $\mathfrak{H}$ and hence it is easy to see that $\mathfrak{H}'\cap\mathfrak{H}''$ is a Hopf subalgedra of $\mathfrak{H}$. q.e.d.

LEMMA 2. *Let $\mathfrak{H}'$ be a Hopf subalgebra of a Hopf algebra $\mathfrak{H}$ over a field k and I a coideal of $\mathfrak{H}$. Then $\mathfrak{H}'\cap I$ is a coideal of $\mathfrak{H}'$.*

The proof of this lemma is exactly the same as that of Lemma 1 and therefore we omit the detail.

LEMMA 3. *Let u be a Hopf algebra homomorphism of $\mathfrak{H}$ into $\mathfrak{H}'$ and $\mathfrak{K}$ a subcoalgebra of $\mathfrak{H}$ such that $u(\mathfrak{K}^+)=0$, where $\mathfrak{K}^+=\mathfrak{K}\cap\mathfrak{H}^+$. Then $\mathfrak{K}$ is contained in the h-kernel of u.*

PROOF. By assumption we have $u(x)=\varepsilon'u(x)=\varepsilon(x)$ for any element x in $\mathfrak{K}$. Therefore if $\Delta(y)=\sum_{(y)} y_{(1)}\otimes y_{(2)}$ for y in $\mathfrak{K}$, we have

$$\begin{aligned}(id_{\mathfrak{H}}\otimes u)\Delta(y)&=\sum_{(y)}(id_{\mathfrak{H}}\otimes u)\,(y_{(1)}\otimes y_{(2)})\\&=\sum_{(y)}\varepsilon(y_{(2)})y_{(1)}\otimes 1\\&=y\otimes 1.\end{aligned}$$

This means that y is in the h-kernel of u. q.e.d.

PROPOSITION 2. *The category $\mathscr{C}$ is abelian.*

PROOF. It is easy to see that $\mathscr{C}$ is an additive category with 0-object k and that the product (resp. the coproduct) of $\mathfrak{H}_1$ and $\mathfrak{H}_2$ is $\mathfrak{H}_1\otimes_k\mathfrak{H}_2$ with the projections ρ_1 and ρ_2 (resp. with the injections j_1 and j_2) defined as in Proposition 1. We shall show that $\mathscr{C}$ has kernels and cokernels of morphisms in $\mathscr{C}$ and that $\mathscr{C}$ is normal and conormal in the sense of chapter I in [5]. Then $\mathscr{C}$ is an abelian category by Th.20.1 of Chap. I in [5]. Let $u: \mathfrak{H}_1 \to \mathfrak{H}_2$ be a morphism in $\mathcal{C}$, and let $\mathfrak{K}$ and $\mathfrak{K}'$ be the h-kernel and the h-cokernel of u respectively. Then $\mathfrak{K}$ is a Hopf subalgebra of $\mathfrak{H}_1$ and $\mathfrak{K}'$ is a quotient Hopf algebra of $\mathfrak{H}_2$. By assumptions on $\mathcal{C}$ there exist Hopf subalgebras $\mathfrak{N}_\alpha$ of finite dimensions such that $\mathfrak{H}_1 = \bigvee_\alpha \mathfrak{N}_\alpha$, and hence we have $\mathfrak{K} = \bigvee_\alpha \mathfrak{K} \cap \mathfrak{N}_\alpha$. But $\mathfrak{K} \cap \mathfrak{N}_\alpha$ is a finite dimensional Hopf subalgebra of $\mathfrak{K}$ by Lemma 1. Therefore $\mathfrak{K}$ is an object of $\mathcal{C}$. Simlarly there exist Hopf subalgebras of finite dimensions $\mathfrak{M}_\beta$ such that $\mathfrak{H}_2 = \bigvee_\beta \mathfrak{M}_\beta$. Then $I_\beta = \mathfrak{M}_\beta \cap u(\mathfrak{H}_1^+)\mathfrak{H}_2$ is a Hopf ideal of $\mathfrak{M}_\beta$ by Lemma 2, since $u(\mathfrak{H}_1^+)\mathfrak{H}_2$ is a Hopf ideal of $\mathfrak{H}_2$. If we identify $\mathfrak{M}_\beta / I_\beta$ with its canonical image in $\mathfrak{K}' = \mathfrak{H}_2 / u(\mathfrak{H}_1^+)\mathfrak{H}_2$, we have $\mathfrak{K}' = \bigvee_\beta \mathfrak{M}_\beta / I_\beta$, where each $\mathfrak{M}_\beta / I_\beta$ is of finite dimension over k. Therefore $\mathfrak{K}'$ is also an object in $\mathcal{C}$. It is easy to check that $\mathfrak{K}$ and $\mathfrak{K}'$ are the kernel and the cokernel of u in $\mathcal{C}$ from the definitions and Lemma 3. Next we see that $\mathcal{C}$ is normal and conormal. Let $u: \mathfrak{H}_1 \to \mathfrak{H}_2$ be an epimorphism in $\mathcal{C}$. Then u is a surjection as a linear mapping over k. We must show that $(\mathfrak{H}_2, u)$ is a cokernel of a monomorphism in $\mathcal{C}$. In fact let $\mathfrak{K}$ be the h-kernel of u and let x be an element of $\mathfrak{K}^+$. There exists a finite dimensional Hopf subalgebra $\mathfrak{N}$ of $\mathfrak{H}_1$ such that $x \in \mathfrak{N} \cap \mathfrak{K}^+ = \mathfrak{N}^+$, and hence that x is contained in $(u|_{\mathfrak{N}})^{-1}(0) \subset u^{-1}(0)$ by Lemma 16.0.2 in [7]. Since u is an algebra homomorphism, this means that $\mathfrak{K}^+\mathfrak{H}_1$ is contained in $u^{-1}(0)$. Conversely let x be an element of $u^{-1}(0)$ and let $\mathfrak{N}$ be a finite dimensional Hopf subalgebra of $\mathfrak{H}_1$ such that $x \in \mathfrak{N}$. Then x is contained in $\mathfrak{K}_{\mathfrak{N}}^+\mathfrak{N}$ by Lemma 16.0.2 in [7], where $\mathfrak{K}_{\mathfrak{N}}$ is the h-kernel of the morphism $u|_{\mathfrak{N}}$. It is clear that $\mathfrak{K}_{\mathfrak{N}} = \mathfrak{N} \cap \mathfrak{K}$ and in particular that $\mathfrak{K}_{\mathfrak{N}}^+$ is contained in $\mathfrak{K}^+$. Therefore x is contained in $\mathfrak{K}^+\mathfrak{H}_1$. This means that $u^{-1}(0)$ is equal to $\mathfrak{K}^+\mathfrak{H}_1$ and hence $(\mathfrak{H}_2, u)$ is the cokernel of the canonical injection of $\mathfrak{K}$ into $\mathfrak{H}_1$ in $\mathcal{C}$. In other words $\mathcal{C}$ is conormal. Lastly let $j: \mathfrak{H}_1 \to \mathfrak{H}_2$ be a monomorphism in $\mathcal{C}$. Then we may assume that $\mathfrak{H}_1$ is a Hopf subalgebra of $\mathfrak{H}_2$ and $\mathfrak{H}_1^+\mathfrak{H}_2$ is a Hopf ideal of $\mathfrak{H}_2$. If π is the natural mapping of $\mathfrak{H}_2$ onto the quotient space $\mathfrak{L} = \mathfrak{H}_2 / \mathfrak{H}_1^+\mathfrak{H}_2$, π is a Hopf algebra homomorphism. We must show that $(\mathfrak{H}_1, j)$ is the kernel of π in $\mathcal{C}$. If $\mathfrak{H}$ is the h-kernel of j, we see that $\mathfrak{H}^+\mathfrak{H}_2 = \mathfrak{H}_1^+\mathfrak{H}_2 = \pi^{-1}(0)$ from the result just obtained in the above. Let x be in $\mathfrak{H}^+$ and let $\mathfrak{M}$ be a finite dimensional Hopf subalgebra of $\mathfrak{H}_2$ such that x is in $\mathfrak{M}$. By Lemma 1 there exists the smallest Hopf subalgebra $\mathfrak{M}_0$ of $\mathfrak{H}_2$ containing x. If $\{x_0 = x, x_1, \cdots, x_s\}$ is a basis of $\mathfrak{M}_0^+$ over k, each x_i is in $\mathfrak{H}^+ \subset \mathfrak{H}_1^+\mathfrak{H}_2$ and hence we have $x_i = \sum_j y_{ij} z_{ij}$ for $y_{ij} \in \mathfrak{H}_1^+$ and $z_{ij} \in \mathfrak{H}_2$. Then we may assume that $\mathfrak{M}$ contains these elements y_{ij} and z_{ij}, replaceing it with larger one if necessary. Therefore we have $\mathfrak{M}_0^+ \subset \mathfrak{M}_1^+\mathfrak{M}$, where $\mathfrak{M}_1 = \mathfrak{H}_1 \cap \mathfrak{M}$, and the composition of the canonical injection of $\mathfrak{M}_0$ into $\mathfrak{M}$ and the canonical projection of $\mathfrak{M}$ onto $\mathfrak{M}/\mathfrak{M}_1^+\mathfrak{M}$ is the zero-morphism in $\mathcal{C}$. Since the full subcategory $\mathcal{C}'$ of $\mathcal{C}$ is abelian, $\mathfrak{M}_1$ is the kernel of the morphism $\pi: \mathfrak{M} \to \mathfrak{M}/\mathfrak{M}_1^+\mathfrak{M}$ in $\mathcal{C}'$ and hence $\mathfrak{M}_0$ is contained in $\mathfrak{M}_1$ by Lemma 3. This means that $\mathfrak{H}$ is contained in $\mathfrak{H}_1$. Conversely $\mathfrak{H}$ contains $\mathfrak{H}_1$ by Lemma 3, since $\mathfrak{H}$ is the h-kernel of π and $\pi \cdot j$ is O-morphism in $\mathcal{C}$. Therefore $\mathfrak{H}$ is equal to $\mathfrak{H}_1$ and $\mathcal{C}$ is normal. q.e.d.

§2 Separability of morphisms of group varieties

In the following let k be an algebraically closed field of a positive characteristic p. Let G and G' be group varieties defined over k and denote by $\mathcal{O}$ and $\mathcal{O}'$ the local rings $\mathcal{O}_{e,G}$ and $\mathcal{O}_{e',G'}$ of G and G' at the neutral elements e and e' respectively. If α is an algebraic homomorphism of G into G' defined over k, there exists a local homomorphism α^* of $\mathcal{O}'$ into $\mathcal{O}$. First we give a generalization of Theorem in [4].

PROPOSITION 3. *Let α be an algebraic homomorphism of a group variety G of dimension n into a group variety G' of dimension m. Let G'' be the kernel of α and $\mathcal{O}''$ the local ring of G'' at e. Then if the image $\alpha(G)$ is of dimension r, there exist regular systems $\{t_1,\cdots, t_n\}$ and $\{s_1,\cdots, s_m\}$ of parameters of $\mathcal{O}$ and $\mathcal{O}'$ respectively satisfying the following conditions:*

(i) $\alpha^*(s_i)=t_i^{p^{e_i}}$ *for* $i=1, 2,\cdots, r$,

(ii) $\alpha^*(s_j)=0$ *for* $j=r+1,\cdots, m$,

and (iii) $\{\bar{t}_{r+1},\cdots, \bar{t}_n\}$ *is a regular system of parameters of $\mathcal{O}''$, where $\bar{t}_j$ is the image of t_j under the natural homomorphism of $\mathcal{O}$ onto $\mathcal{O}''$.*

PROOF. First we assume that α is a separable homomorphism of G onto G'. Then we see that there exist regular systems $\{t_1,\cdots, t_n\}$ and $\{s_1,\cdots, s_m\}$ of parameters of $\mathcal{O}$ and $\mathcal{O}'$ respectively such that $\alpha^*(s_i)=t_i$ for $i=1, 2,\cdots, m$ (cf. the proof of Proposition 14 in [8]). From this if $\{s_1',\cdots, s_m'\}$ is any regular system of parameters of $\mathcal{O}'$, we can easily see that $\{\alpha^*(s_1'),\cdots,\alpha^*(s_m'), t_{m+1},\cdots, t_n\}$ is a regular system of parameters of $\mathcal{O}$. Next we assume that α is a surjective morphism. If we denote by G_1 the quotient group variety G/G'' and by π the canonical homomorphism of G onto G_1, there exists a purely inseparable isogeny α_1 of G' onto G_1 such that $\alpha=\alpha_1\pi$. If $\mathcal{O}_1$ is the local ring of G_1 at the neutral element e_1, there exist regular systems $\{u_1,\cdots, u_m\}$ of parameters of $\mathcal{O}_1$ and $\{s_1,\cdots, s_m\}$ of $\mathcal{O}'$ respectively such that $\alpha_1^*(s_i)=u_i^{p^{e_i}}$ for $i=1, 2,\cdots, m$ by Theorem in [4]. Since π is a separable morphism, there exists a subset $\{t_{m+1},\cdots, t_n\}$ of $\mathcal{O}$ such that $\{t_1=\pi^*(u_1),\cdots, t_m=\pi^*(u_m), t_{m+1},\cdots, t_n\}$ is a regular system of parameters of $\mathcal{O}$ as shown in the above. Therefore these $\{t_1,\cdots, t_n\}$ and $\{s_1,\cdots, s_m\}$ are our solution in this case. In fact we see easily $\{\bar{t}_{m+1},\cdots, \bar{t}_n\}$ is a regular system of parameters of $\mathcal{O}''$. In general cases let G_2 be the image $\alpha(G)$ and $\mathcal{O}_2$ the local ring of G_2 at e'. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}'$ corresponding to the subvariety G_2 of G', $\mathcal{O}'/\mathfrak{p}$ is isomorphic to $\mathcal{O}_2$. In particular $\mathcal{O}'/\mathfrak{p}$ is a regular local ring. Therefore $\mathfrak{p}$ is generated by a subset $\{s_{r+1},\cdots, s_m\}$ of a regular system of parameters of $\mathcal{O}'$ by Theorem 26, Chap. VIII in [9]. Moreover we see that $\{s_1,\cdots, s_r, s_{r+1},\cdots, s_m\}$ is a regular system of parameters of $\mathcal{O}'$ for any subset $\{s_1,\cdots, s_r\}$ of $\mathcal{O}'$ such that the image of $\{s_1,\cdots, s_r\}$ in $\mathcal{O}'/\mathfrak{p}$ is that of $\mathcal{O}'/\mathfrak{p}$. Combining this with the results obtained in the above for a special case, we see that our assertion is true. q.e.d.

REMARK. (i) The notation being as in Proposition 3, let $\{t'_{r+1},\cdots, t'_n\}$ be any regular system of parameters of $\mathcal{O}''$. Then we can find $\{t_1,\cdots, t_n\}$ in Proposition 3 satisfying $\bar{t}_i=t'_i$ for $i=r+1,\cdots, n$. In fact we may replace $\{t_{r+1},\cdots, t_n\}$ by any set of $m-r$ elements in $\mathcal{O}$ whose image in $\mathcal{O}''$ is a regular system of parameters of $\mathcal{O}''$, since the ideal $(t_1,\cdots, t_r)\mathcal{O}$ is the prime ideal corresponding to the subvariety G'' such that $\mathcal{O}''$ is isomorphic to $\mathcal{O}/(t_1,\cdots, t_r)\mathcal{O}$.

(ii) Similarly if $\alpha(G)$ is a normal subgroup of G', $\{s_{r+1},\cdots, s_m\}$ may be replaced with any regular system of parameters of the local ring of the quotient group variety $G'/\alpha(G)$ at the neutral element.

COROLLARY. *In Proposition* 3, α *is a separable morphism if and only if* $e_i=0$ *for* $i=1,2,\cdots, r$.

PROOF. Let G_1 be the quotient group variety G/G', and π the canonical homomorphism of G onto G_1. Then there exists a purely inseparable isogeny α_1 of G_1 onto $\alpha(G)$ such that $\alpha=\alpha_1\pi$. Then α is a separable morphism if and only if α_1 is an isomorphism. On the other hand we know that $e_1+\cdots+e_r=s$, where $[k(G_1)\colon k(\alpha(G))]=[k(G)\colon k(\alpha(G_1)]_i=p^s$ by Theorm in [4]. This completes the proof. q.e.d.

Let G be a group variety defined over k. Then recall that the Hopf algebra $\mathfrak{H}(G)$ attached to G is the subalgebra $k\oplus\mathfrak{g}(G)$ of the algebra $\mathrm{Hom}_k(k(G), k(G))$ over k, where $\mathfrak{g}(G)$ consists of all the left invariant semi-derivations of G. Moreover if $\{t_1,\cdots, t_n\}$ is a regular system of parameters of $\mathcal{O}$, then there exists a basis $\{I_{e_1\dots e_n}\mid c_i\geqslant 0, \sum_i e_i>0\}$ of $\mathfrak{g}(G)$, which is uniquely determined by the condition that $I_{e_1\dots e_n}(t_1^{e_1}\cdots t_n^{e_n})-1$ and $I_{e_1\dots e_n}(t_1^{e'_1}\cdots t_{n'}^{e_n'})$ for $(e_1,\cdots, e_n)\neq(e'_1,\cdots e'_n)$ are in the maximal ideal of $\mathcal{O}$ (cf. Theorem l in [8]). For convenience' sake we denote by $I_{0\dots 0}$ the identity mapping of $k(G)$. Then $\{I_{e_1\dots e_n}\mid e_i\geqslant 0$ for each $i\}$ is called *the canonical basis of* $\mathfrak{H}(G)$ *with respect to* $\{t_1,\cdots, t_n\}$. Now we have the following

THEOREM 1. *Let α be an algebraic homomorphism of a group variety G into a group variety G' defined over k, and assume that $\{t_1,\cdots, t_n\}$ and $\{s_1,\cdots, s_m\}$ are reguar systems of parameters of $\mathcal{O}$ and $\mathcal{O}'$ satisfying the conditions* (i), (ii) *and* (iii) *in Proposition* 3. *Let $\{I_{a_1\dots a_n}\}$ be the canonical basis of the Hopf algebra $\mathfrak{H}(G)$ attached to G with respect to $\{t_1,\cdots, t_n\}$. Then the h-kernel of the Hopf algebra homomorphism α_* of $\mathfrak{H}(G)$ into $\mathfrak{H}(G')$ induced from α is the linear subspace of $\mathfrak{H}(G)$ generated by the elements $I_{a_1\dots a_n}$ such that $a_i<p^{e_i}$ for $i=1,2,\cdots, r$.*

PROOF. Let $\{I'_{b_1\dots b_m}\mid b_i\geqslant 0\}$ be the canonical basis of $\mathfrak{H}(G')$ with respect to $\{s_1,\cdots, s_m\}$. Since $\alpha_*(D)(x)=D(\alpha^*(x))$ for any element x in $\mathcal{O}'$ and any element D in $\mathfrak{H}(G)$, we see that

$$\alpha_*(I_{a_1p^{e_1}\dots a_rp^{e_r}0\dots 0})=I'_{a_1\dots a_r0\dots 0}$$

and $$\alpha_*(I_{b_1\dots b_n})=0 \quad\text{for}\quad (b_1,\cdots, b_n)\neq(a_1p^{e_1},\cdots, a_rp^{e_r}, 0,\cdots, 0)$$

from the definition of the canonical basis and the condition in Proposition 3 satisfied by $\{t_1,\cdots, t_n\}$ and $\{s_1,\cdots, s_m\}$. If we denote by Δ the diagonal of the Hopf algebra $\mathfrak{H}(G)$, we know that $\Delta(I_{a_1\dots a_n})=\sum_{(a')+(a'')=(a)} I_{a'_1\dots a'_n}\otimes I_{a''_1\dots a''_n}$ (cf. §5 in [8]). Therefore we have

$$(id_{\mathfrak{H}(G)}\otimes\alpha_*)\Delta(I_{a_1\dots a_n})=\sum_{(a')+(a'')=(a)} I_{a'_1\dots a'_n}\otimes\alpha_*(I_{a''_1\dots a''_n})$$

$$=\sum_{(a')+(bp^e)=(a)}' I_{a'_1\dots a'_n}\otimes I'_{b_1\dots b_r0\dots0},$$

where $\sum'_{(a')+(bp^e)=(a)}$ runs over all pairs $((a'), (b))$ such that

$$(a'_1,\cdots, a'_n)+(b_1p^{e_1},\cdots, b_rp^{e_r}, 0,\cdots, 0)=(a_1,\cdots, a_n).$$

This means that

$$(id_{\mathfrak{H}(G)}\otimes\alpha_*)\Delta(I_{a_1\dots a_n})\neq I_{a_1\dots a_n}\otimes 1$$

if $a_i\geqslant p^{e_i}$ for some $i<r$, since $\{I_{a_1\dots a_n}\otimes I'_{b_1\dots b_m}\}$ is a basis of $\mathfrak{H}(G)\otimes_k\mathfrak{H}(G')$ over k. On the other hand if $a_i<p^{e_i}$ for any $i\leqslant r$, we have $(id_{\mathfrak{H}(G)}\otimes\alpha_*)\Delta(I_{a_1\dots a_n})=I_{a_1\dots a_n}\otimes 1$ and hence $I_{a_1\dots a_n}$ is contained in the h-kernel of α_*. In general if $D=\sum_{(a)}\gamma_{a_1\dots a_n}I_{a_1\dots a_n}$, we have

$$(id_{\mathfrak{H}(G)}\otimes\alpha_*)\Delta(D)=\sum_{(a)}\gamma_{a_1\dots a_n}\sum_{(a')+(bp^e)=(a)}' I_{a'_1\dots a'_n}\otimes I'_{b_1\dots b_r0\dots0}.$$

Now it is easy to see that $((a'), (bp^e))\neq((a'_1), (b_1p^e))$ if $(a')+(bp^e)\neq(a'_1)+(b_1p^e)$. Therefore we see

$$(id_{\mathfrak{H}(G)}\otimes\alpha_*)\Delta(D)\neq D\otimes 1,$$

if $\gamma_{a_1\dots a_n}\neq 0$for such $(a_1,\cdots, a_n)$ that $a_i\geqslant p^{e_i}$ for some $i\leqslant r$. This means that the h-kernel of α_* is generated by the elements $I_{a_1\dots a_n}$ such that $a_i<p^{e_i}$ for any $i\leqslant r$. q.e.d.

THEOREM 2. *Let G_1, G_2 and G_3 be group varieties defined over k and let α_i be an algebraic homomorphism of G_i into G_{i+1} defined over k for $i=1, 2$ such that the image of G_1 into G_2 is equal to the connected component of the kernel of α_2 containing the neutral element. Then α_2 is a separable morphism if and only if the sequence $\mathfrak{H}(G_1)\xrightarrow{\alpha_{1*}}\mathfrak{H}(G_2)\xrightarrow{\alpha_{2*}}\mathfrak{H}(G_3)$ of Hopf algebras is exact.*

PROOF. We may assume that G_1 is a group subvariety of G_2 and that α_1 is the canonical injection. In fact if α is a surjective algebraic homomorphism of G onto G' in Proposition 3, we have $\alpha^*(s_i)=t_i^{p^{e_i}}$ for $i=1, 2,\cdots, m$. Then we have $\alpha_*(I_{a_1p^{e_1}\dots a_mp^{e_m}0\dots0})=I'_{a_1\dots a_m}$ for any $(a_1,\cdots, a_m)$, where $\{I_{a_1\dots a_n}\}$ and $\{I'_{b_1\dots b_m}\}$ are the canonical basis of $\mathfrak{H}(G)$ and $\mathfrak{H}(G')$ with respect to $\{t_1,\cdots, t_n\}$

and $\{s_1,\cdots, s_m\}$ respectively (cf. the proof of Theorem 1). This means that α_* is also a surjection and we may replace G_1 with the image $\alpha_1(G_1)$.

Therfore we assume that G_1 is the connected component of the kernel of α_2 containing the neutral element e_2. Then, from Proposition 3 and Remark (i) below it, there exists a regular system $\{t_1,\cdots, t_n\}$ of parameters of $\mathcal{O}_{e_2,G_2}$ and that $\{s_1,\cdots, s_m\}$ of $\mathcal{O}_{e_3,G_3}$ satisfying the following conditions:

(i) $\alpha_2^*(s_i)=t_i^{p^{e_i}}$ *for* $i=1,\cdots, r=\dim \alpha_2(G_2)$,

(ii) $\alpha_2^*(s_j)=0$ *for* $j=r+1,\cdots, m$

and (iii) $\{\bar{t}_{r+1,\dots,}\bar{t}_n\}$ *is a regular system of parameters of* $\mathcal{O}_{e_1,G_1}$, *where* $\bar{t}_n$ *is the canonical image of* t_n *in* $\mathcal{O}_{e_1,G_1}$. By Corollary of Proposition 3, α_2 is separable if and only if $e_i=0$ for $i=1, 2,\cdots, r$. On the other hand if $\{\bar{I}_{a_1\dots a_n}\}$ is the canonical basis of $\mathfrak{H}(G_2)$ with respect to $\{t_1,\cdots, t_n\}$, we easily see that $\alpha_{1_*}(\mathfrak{H}(G_1))$ is the subspace of $\mathfrak{H}(G_2)$ generated by the elements $\bar{I}_{0\dots 0a_{r+1}\dots a_n}$ for $a_i\geqslant 0$ as seen in the proof of Theorem 1 and that the h-kernel of α_{2_*} is the subspace of $\mathfrak{H}(G_2)$ generated by the elements $\bar{I}_{a_1\dots a_n}$ such that $a_i<p^{e_i}$ for any $i\leqslant r$. This means that $e_1=\cdots=e_r=0$ if and only if $\alpha_{1_*}(\mathfrak{H}(G_1))$ is the h-kernel of α_{2_*}. Therefore our assertion is proved. q.e.d.

§3 Groups Ext(A,B) for purely inseparable isogenies

The aim of this section is to give a generalization of Serre's result on groups Ext(A,B) for purely inseparable isogenies of exponent 1 in §3, $n^\circ 8$ in [6] for cases of higher exponents. Let A and B be two commutative group varieties defined over k. Now recall that Ext(A,B) is the set of isomorphism classes of extensions C of A by B, i.e., the set of isomorphism classes of strictly exact sequences $0\to B\to C\to A\to 0$ of commutative group varieties defined over k, and that Ext(A,B) is an additive functor in both A and B into abelian groups (cf. §3, $n^\circ 7$ in [6]). More generally let $\mathcal{A}$ be an abelian category and let A and B be two objects in $\mathcal{A}$. Then there exists an abelian group Ext(A,B) called "the group of Yoneda extensions of A by B" (cf. Chap. VII in [5]). In particular the Hopf algebra $\mathfrak{H}(A)$ attached to a commutative group variety A defined over k is in the abelian category $\mathcal{C}$ given in §l, and hence Ext($\mathfrak{N}$,$\mathfrak{H}(A)$) is defined for any object $\mathfrak{N}$ in $\mathcal{C}$.

Let ρ be a purely inseparable isogeny of a commutative group variety A onto A' defined over k and $N=N(\rho)$ the Hopf subalgebra of $\mathfrak{H}(A)$ corresponding to ρ in the sense of Theorem 4 in [8]. Then we have

LEMMA 4. *The sequence*

$$k\longrightarrow N(\rho)\xrightarrow{i}\mathfrak{H}(A)\xrightarrow{\rho_*}\mathfrak{H}(A')\longrightarrow k$$

of Hopf algebras is exact in $\mathcal{C}$.

PROOF. By Theorem in [4], there exists a regular system $\{t_1,\cdots, t_n\}$ of parameters of $\mathcal{O}_{e,A}$ such that $\{t_1^{p^{e_1}},\cdots, t_n^{p^{e_n}}\}$ is that of $\mathcal{O}_{e',A'}$, where we identify $\mathcal{O}_{e',A'}$ with the subring $\rho^*(\mathcal{O}_{e',A'})$ of $\mathcal{O}_{e,A}$. Then the h-kernel $\mathfrak{K}$ of ρ_* has a basis $\{I_{a_1\ldots a_n} | a_i < p^{e_i}$ for $i=1, 2,\cdots, n\}$ by Theorem l, where $\{I_{a_1\ldots a_n} | a_i \geqslant 0\}$ is the canonical basis of $\mathfrak{H}(A)$ with respect to $\{t_1,\cdots, t_n\}$. By the definition of $N(\rho)$ and Proposition 15 in [8], we see $D(k(A'))=0$ for any element D in $N(\rho)^+$. This means that $\mathfrak{K}$ is contained in $N(\rho)$ by Lemma 3. But we know that $\dim_k N(\rho)=[k(A): k(A')]=p^{\sum_{i=1}^{n} e_i}=\dim_k\mathfrak{K}$, and hence we see $N(\rho)=\mathfrak{K}$.

q.e.d.

If B is another commutative group variety defined over k, we denote by Hom(A,B) (resp. Hom(A',B)) the group of algebraic homomorphisms of A (resp. A') into B defined over k. Then there exists a group homomorphism $\tilde{\rho}$ of Hom (A', B) into Hom (A, B) defined dy $\tilde{\rho}(\alpha)=\alpha\rho$. Similary we define a mapping $\tilde{i}$ of Hom(A,B) into $\mathrm{Hom}_{\mathcal{C}}(N(\rho), \mathfrak{H}(B))$ by $\tilde{i}(\alpha)=\alpha_* i$ for α in Hom(A,B), where α_* is the tangential mapping of $\mathfrak{H}(A)$ to $\mathfrak{H}(B)$ induced by α. Then $\tilde{i}$ is a group homomorphism. In fact, let δ_A be the diagonal mapping of A into $A\times A$ given by $\delta_A(x)=x\times x$ and μ_B the multiplication of $B\times B$ onto B given by $\mu_B(y\times z)=y+z$. If f and g are in Hom(A,B), we have $f+g=\mu_B(f\times g)\delta_A$ and hence $(f+g)_*=\mu_{B*}(f\times g)_*\delta_{A*}=m_{\mathfrak{H}(B)}(f_*\otimes g_*)\Delta_{\mathfrak{H}(A)}=(f_*)*(g_*)$. This means that $\tilde{i}(f+g)=(f+g)_* i=(f_* i)*(g_* i)=\tilde{i}(f)*\tilde{i}(g)$. Then we have

LEMMA 5. *The sequence*

$$0\longrightarrow \mathrm{Hom}(A',B)\xrightarrow{\tilde{\rho}}\mathrm{Hom}(A,B)\xrightarrow{\tilde{i}}\mathrm{Hom}_{\mathcal{C}}(N(\rho),\mathfrak{H}(B))$$

of abelian groups is exact.

PROOF. It is clear that $\tilde{\rho}$ is injective. Let g be an element of Hom(A',B) and put $f=\tilde{\rho}(g)=g\cdot\rho$. If i^* is the natural homomorphism of $\mathcal{O}_{e,A}$ onto $R=N(\rho)^D$, we have $i^*\rho^*(\mathfrak{m}')=0$, where $\mathfrak{m}'$ is the maximal ideal of $\mathcal{O}_{e,A'}$ (cf. §7 in [8]). From this we easily see that $\tilde{i}(f)=f_* i=g_*\rho_* i$ is the zero morphism of $N(\rho)$ into $\mathfrak{H}(B)$ in $\mathcal{C}$, since $\mathfrak{H}(B)$ and $N(\rho)$ may be considerd as subspaces of the dual spaces of $\mathcal{O}_{e,B}$ and $R=N(\alpha)^D$ over k respectively. This means that the image of $\tilde{\rho}$ is contained in the kernel of $\tilde{i}$. Conversely assume that $\tilde{i}(f)=0$ and put $f(A)=B'$. If j is the canonical injection of B' into B, we have $f=j\cdot f'$, where f' is a surjective homomorphism of A to B'. Now we identify the fields $k(A')$ and $k(B')$ with the subfields $\rho^*(k(A'))$ and $f'^*(k(B'))$ of $k(A)$. Then we have $f'_*(D)=D|_{k(B')}$ for any D in $\mathfrak{H}(A)$ by Proposition 15 in [8]. Since j_* is injective, we have $f'_*\tilde{i}=0$ by the hypothesis $\tilde{i}(f)=f_* i=0$. Therefore we have $D|_{k(B')}=0$ for any element D in $N(\rho)^+$. On the other hand $k(A')$ is the set of the elements x in $k(A)$ such that $D(x)=0$ for any D in $N(\rho)^+$ by (D) in §6 of [8], and hence $k(A')$ contains $k(B')$. From this we see that there exists an algebraic homomorphism g' of A' onto B' such that $f'=g'\cdot\rho$ and hence $f=jf'=(jg')\rho=\tilde{\rho}(jg')$. q.e.d.

Let g be an element of $\mathrm{Hom}_{\mathcal{C}}(N(\rho), \mathfrak{H}(B))$. Then there exists the push-out $\mathfrak{H}_g$ of $\mathfrak{H}(A)$ and $\mathfrak{H}(B)$ over $N(\rho)$ with respect to (i,g), since $\mathcal{C}$ is an abelian category (cf. TH. 20.1. of Chap. I in [5]). Let p_1 and p_2 be the canonical morphisms of $\mathfrak{H}(A)$ and $\mathfrak{H}(B)$ into $\mathfrak{H}_g$ such that $p_1 i = p_2 g$. Recall that $\mathfrak{H}_g$ is constructed as follows: let μ be a morphism of $N(\rho)$ into $\mathfrak{H}(A)\otimes_k\mathfrak{H}(B)$ defined by $\mu=(i_A\cdot i)*(c i_B g)$, where c is the antipode of the direct sum $(\mathfrak{H}(A)\otimes_k\mathfrak{H}(B)$, i_A, $i_B)$ of $\mathfrak{H}(A)$ and $\mathfrak{H}(B)$ in $\mathcal{C}$. Then if $(\mathfrak{H}_g, \nu)$ is the cokernel of μ, $(\mathfrak{H}_g, p_1=\nu i_A$, $p_2=\nu i_B)$ is the push-out of $\mathfrak{H}(A)$ and $\mathfrak{H}(B)$ over $N(\rho)$. If we put $N'=\mu(N(\rho))$, N' is a Hopf subalgebra of $\mathfrak{H}(A)\otimes_k\mathfrak{H}(B)=\mathfrak{H}(A\otimes B)$ of a finite dimension. Therefore there exists a purely inseparable isogeny π of $A\times B$ onto a commutative group variety C_g such that $\mathrm{Spec}(N'^D)$ is the kernel of π by Theorems 3 and 4 in [8]. It is clear by Lemma 4 that $\mathfrak{H}_g$ and ν may be identified with $\mathfrak{H}(C_g)$ and π_* respectively. Moreover $\pi^*(k(C_g))$ is the set of y in $k(A\times B)$ such that $D(y)=0$ for any D in N'^+. On the other hand if $k(A)$ is identified with the subfield $p_A^*(k(A))$ of $k(A\times B)$, we have $D(x)=\mu D(x)$ for x in $k(A)$ and D in N by the definition of the morphism μ. Therefore $\pi^*(k(C_g))$ contains $\rho^*(k(A'))$ and hence there exist an algebraic homorphism ϕ of C_g onto A' such that $\phi\pi=\rho p_A$. On the other hand it is easy to see that g gives a morphism g_1 of $\mathrm{Spec}(N(\rho)^D)$ to B as k-group schemes such that $(g_1)_*=g$. Similarly i gives a morphism i_1 of $\mathrm{Spec}(N(\rho)^D)$ to A such that $(i_1)_*=i$. Then we have

LEMMA 6. *The diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Spec}(N(\rho)^D) & \xrightarrow{i_1} & A & \xrightarrow{\rho} & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle \pi i_A} & & \downarrow{\scriptstyle id_{A'}} & & \\ 0 & \longrightarrow & B & \xrightarrow{\pi i_B} & C_g & \longrightarrow & A' & \longrightarrow & 0 \end{array}$$

of k-schemes is commutative and the second row is strictly exact.

PROOF. Since $(\pi i_A)_*=p_1$ and $(\pi i_B)_*=p_2$, we have $(\pi i_B g_1)_*=p_2 g=p_2 i=(\pi i_A i_1)_*$ and hence $\pi i_B g_1=\pi i_A i_1$. Therefore the first assertion is seen, and from this we have a commutative diagram of Hopf algebras:

$$\begin{array}{ccccccccc} k & \longrightarrow & N(\rho) & \xrightarrow{i} & \mathfrak{H}(A) & \xrightarrow{\rho_*} & \mathfrak{H}(A') & \longrightarrow & k \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle id_{\mathfrak{H}(A')}} & & \\ k & \longrightarrow & \mathfrak{H}(B) & \xrightarrow{p_2} & \mathfrak{H}_g=\mathfrak{H}(C_g) & \xrightarrow{\phi_*} & \mathfrak{H}(A') & \longrightarrow & k \end{array}$$

Then the second row is also exact in $\mathcal{C}$ by the dual of Corollary 20.3 of Chap. I in [5], since $\mathfrak{H}(C_g)$ is the push-out of $\mathfrak{H}(A)$ and $\mathfrak{H}(B)$ over $N(\rho)$. From this we see that the sequence $0\longrightarrow B\xrightarrow{\pi i_B} C_g\xrightarrow{\phi} A'\longrightarrow 0$ is strictly exact by Theorem 2. q.e.d.

LEMMA 7. *Let C be a commutative group variety defined over k satisfying the commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Spec}(N(\rho)^D) & \xrightarrow{i'} & A & \longrightarrow & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle q_1} & & \downarrow{\scriptstyle id_{A'}} & & \\ 0 & \longrightarrow & B & \xrightarrow{q_2} & C & \xrightarrow{\phi} & A' & \longrightarrow & 0, \end{array}$$

where the second row is strictly exact. Then there exists an isomorphism λ *of* C_g *onto* C *satisfying the following commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{\pi i_B} & C_g & \xrightarrow{\phi} & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_B} & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle id_{A'}} & & \\ 0 & \longrightarrow & B & \xrightarrow{q_2} & C & \xrightarrow{\psi} & A' & \longrightarrow & 0. \end{array}$$

PROOF. By hypothesis we have a commutative diagram of Hopf algebras with exact rows:

$$\begin{array}{ccccccccc} k & \longrightarrow & N(\rho) & \xrightarrow{i} & \mathfrak{H}(A) & \xrightarrow{\rho^*} & \mathfrak{H}(A') & \longrightarrow & k \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle (q_1)_*} & & \downarrow{\scriptstyle \mathfrak{H}(A')} & & \\ k & \longrightarrow & \mathfrak{H}(B) & \xrightarrow{(q_2)_*} & \mathfrak{H}(C) & \xrightarrow{\phi_*} & \mathfrak{H}(A') & \longrightarrow & k. \end{array}$$

Then, by the dual of Corollary 1.2. of Chap. VII in [5], there exists an isomorphism σ of $\mathfrak{H}(C_g)$ onto $\mathfrak{H}(C)$ such that $\sigma p_1=(q_1)_*$, $\sigma p_2=(q_2)_*$ and $\psi_*\sigma=\phi_*$, since C_g satisfies also the condition for C by Lemma 6. Let p_A and p_B be the canonical projections of $A\times B$ onto A and B respectively and put $\alpha=q_1p_A+q_2p_B$. Then we can easily see that $\alpha_*=\pi_*$. Therefore there exists an isomorphism λ of C_g onto C such that $\alpha=\lambda\pi$. Then it is clear that we may replace σ by λ_* and it is seen that $q_1=\lambda p_1$ and $q_2=\lambda p_2$, since $(q_1)_*=(\lambda p_1)_*$ and $(q_2)_*=(\lambda p_2)_*$. The equality $\psi\lambda=\phi$ is also obtained easily. q.e.d.

From Lemmas 6 and 7, there exists a uniquely determined element (C, q_2, ψ) in $\mathrm{Ext}(A',B)$ satisfying the condition of Lemma 7 for any element g in $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))$. Now we define a morphism d of $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))$ to $\mathrm{Ext}(A',B)$ by $d(g)=(C, q_2, \psi)=C$. Then *d is a group homomorphism.* In fact let g_1 and g_2 be two elements in $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))$, and put $C_{g_i}=d(g_i)$ for $i=1, 2$. Then by the definition of the sum in the group $\mathrm{Ext}(A',B)$, there exists the following commutative diagram of group varieties:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B\times B & \longrightarrow & C_{g_1}\times C_{g_2} & \longrightarrow & A'\times A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle m_B} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & B & \longrightarrow & \bar{C} & \xrightarrow{\eta} & A'\times A' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle id_B} & & \uparrow{\scriptstyle \xi} & & \uparrow{\scriptstyle \Delta_{A'}} & & \\ 0 & \longrightarrow & B & \longrightarrow & C_{g_1}+C_{g_2} & \xrightarrow{\zeta} & A' & \longrightarrow & 0, \end{array} \qquad (1)$$

where $\bar{C}$ is the push-out of B and $C_{g_1}\times C_{g_2}$ over $B\times B$ and where $C_{g_1}+C_{g_2}$ is the pull-back of $\bar{C}$ and A' over $A'\times A'$. On the other hand by the definition of C_{g_1} we have diagrams

$$\begin{array}{ccccccccc} 0 \to & \mathrm{Spec}(N(\rho)^D) & \xrightarrow{i_1} & A & \xrightarrow{\rho} & A' & \longrightarrow 0 \\ & \downarrow{\scriptstyle (g_i)_1} & & \downarrow{\scriptstyle r_i} & & \downarrow{\scriptstyle id_{A'}} & \\ 0 \longrightarrow & B & \longrightarrow & C_{g_i} & \xrightarrow{\phi_i} & A' & \longrightarrow 0 \end{array}$$

From this and (1) we have a diagram

$$\begin{array}{ccccccccc} 0 \to & \mathrm{Spec}(N(\rho)^D) & \xrightarrow{i_1} & A & \xrightarrow{\rho} & A' & \longrightarrow 0 \\ & \downarrow{\scriptstyle \sigma_1} & & \downarrow{\scriptstyle \sigma_2} & & \downarrow{\scriptstyle \varDelta_{A'}} & \\ 0 \longrightarrow & B & \longrightarrow & \bar{C} & \xrightarrow{\eta} & A'\times A' & \longrightarrow 0 \end{array} \tag{2}$$

where $\sigma_1 = m_B((g_1)_1\times(g_2)_1)\varDelta_N D$ and $\sigma_2=\tau(r_1\times r_2)\varDelta_A$. Since $C_{g_1}+C_{g_2}$ is the pull-back of A' and $\bar{C}$ over $A'\times A'$, there exists an algebraic homomorphism ω of A to $C_{g_1}+C_{g_2}$ satisfying the following diagram

$$\begin{array}{ccccccccc} 0 \to & \mathrm{Spec}(N(\rho)^D) & \xrightarrow{i_1} & A & \xrightarrow{\rho} & A' & \longrightarrow 0 \\ & & & \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle id_{A'}} & \\ 0 \longrightarrow & B & \longrightarrow & C_{g_1}+C_{g_2} & \xrightarrow{\zeta} & A' & \longrightarrow 0 \\ & \downarrow{\scriptstyle id_B} & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \varDelta_{A'}} & \\ 0 \longrightarrow & B & \longrightarrow & \bar{C} & \xrightarrow{\eta} & A'\times A' & \longrightarrow 0 \end{array} \tag{3}$$

such that $\sigma_2=\xi w$. Hence we have a commutative diagram of Hopf algebras:

$$\begin{array}{ccccccccc} k\longrightarrow & N(\rho) & \xrightarrow{i} & \mathfrak{H}(A) & \xrightarrow{\rho_*} & \mathfrak{H}(A') & \longrightarrow k \\ & \vdots{\scriptstyle g_1*g_2} & & \downarrow{\scriptstyle \omega*} & & \downarrow{\scriptstyle id} & \\ k\longrightarrow & \mathfrak{H}(B) & \longrightarrow & \mathfrak{H}(C_{g_1}+C_{g_2}) & \xrightarrow{\zeta_*} & \mathfrak{H}(A') & \longrightarrow k \\ & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \xi*} & & \downarrow & \\ k\longrightarrow & \mathfrak{H}(B) & \longrightarrow & \mathfrak{H}(\bar{C}) & \xrightarrow{\eta_*} & \mathfrak{H}(A')\otimes_k\mathfrak{H}(A') & \longrightarrow k. \end{array} \tag{4}$$

Since each row of this diagram is exact in $\mathscr{C}$, $\mathfrak{H}(C_{g_1}+C_{g_2})$ is the push-out of $\mathfrak{H}(A')$ and $\mathfrak{H}(\bar{C})$ over $\mathfrak{H}(A'\times A')$. Then using the commutative diagrams of Hopf algebras obtained from (1) and (2), we can easily see by Lemma 1. 1. of Chap. VII in [5] that we may add the morphism $g_1*g_2=m_{\mathfrak{H}(B)}(g_1\otimes g_2)\varDelta_N$ of N into $\mathfrak{H}(B)$ in (4) without breaking the commutativity, and hence we may add in (3) the morphism $(g_1*g_2)_1=m_B((g_1)_1\times(g_2)_1)\varDelta_{ND}$ of Spec $(N(\rho)^D)$ into B. This means that $d(g_1*g_2)=C_{g_1}+C_{g_2}=d(g_1)+d(g_2)$. Now we have

LEMMA 8. *The sequence*

$$\mathrm{Hom}(A,B)\xrightarrow{\tilde{i}}\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))\xrightarrow{d}\mathrm{Ext}(A',B)$$

is exact.

PROOF. Let f be an element of $\mathrm{Hom}(A,B)$ and put $g=\tilde{i}(f)=f_*i$ and $\sigma=\pi(i_A-i_Bf)$, where i_A and i_B are the canonical injection of A and B into

$A\times B$ resspectively and where π is the isogeny of $A\times B$ onto C_g defined in the above. Recall that $(\mathfrak{H}(C_g), \pi_*)$ is the cokernel of the morphlsm $\mu=((i_A)_*i)*(c(i_B)_*g)$, and hence we see that $\sigma_*i=\pi_*(i_A-i_Bf)_*i=\pi_*\mu$ is the zero-morphism of $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(C_g))$. This means that there exists a uniquely determined algebraic homomorphism σ_1 of A' into C_g such that $\sigma=\sigma'\rho$ by Lemma 5. If ϕ is the homomorpism of C_g onto A' defined in Lemma 6, we see from the definition of σ that $\phi\sigma_1$ is the identity of A'. This means that the sequence $0\longrightarrow B\longrightarrow C_g\xrightarrow{\phi}A'\longrightarrow 0$ is split, i.e., $d(g)=0$. Conversely assume that $d(g)=0$ for g in $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))$. Then the sequence $0\longrightarrow B\xrightarrow{\pi i_B}C_g\xrightarrow{\phi}A'\longrightarrow 0$ is split and hence there exists an algebraic homomorphism h of C_g onto B such that $h\pi i_B=id_B$. If we put $f=h\pi i_A$, we see easily that $g=f_*i=\tilde{i}(f)$. This completes the proof. q.e.d.

Now we denote by $\tilde{\rho}_1$ the group homomorphism of $\mathrm{Ext}(A',B)$ into $\mathrm{Ext}(A,B)$ induced from ρ. Then we have

LEMMA 9. *The sequence*

$$\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))\xrightarrow{d}\mathrm{Ext}(A',B)\xrightarrow{\tilde{\rho}}\mathrm{Ext}(A,B)$$

is exact.

PROOF. If we put $C=\tilde{\rho}_1(C_g)$ for g in $\mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B))$, we have, by the definition of $\tilde{\rho}_1$, the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C & \xrightarrow{\alpha} & A & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle id_B} & & \big\downarrow{\scriptstyle \beta} & & \big\downarrow{\scriptstyle \rho} & & \\ 0 & \longrightarrow & B & \xrightarrow{\pi i_B} & C_g & \xrightarrow{\phi} & A' & \longrightarrow & 0. \end{array}$$

Moreover C is the pll-back of A and C_g over A' and hence there exists an algebraic homomorhism h of A into C such that $\alpha h=id_A$ and $\beta h=\pi i_A$. This means that the sequence $0\longrightarrow B\longrightarrow C\xrightarrow{\alpha}A'\longrightarrow 0$ is split. Conversely let (C', γ, ρ') be an element of $\mathrm{Ext}\,(A', B)$ satisfying the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{i_B} & A\times B & \underset{i_A}{\overset{p_A}{\rightleftarrows}} & A & \longrightarrow & 0 \\ & & \big\downarrow & & \big\downarrow{\scriptstyle \beta} & & \big\downarrow{\scriptstyle \rho} & & \\ 0 & \longrightarrow & B & \xrightarrow{\gamma} & C' & \xrightarrow{\rho'} & A' & \longrightarrow & 0. \end{array}$$

If we put $h=\beta i_A$, we see $\rho=\rho' h$ and hence have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} k & \longrightarrow & N & \xrightarrow{i} & \mathfrak{H}(A) & \xrightarrow{\rho_*} & \mathfrak{H}(A') & \longrightarrow & k \\ & & & & \big\downarrow{\scriptstyle h_*} & & \big\downarrow{\scriptstyle id_{\mathfrak{H}(A')}} & & \\ k & \longrightarrow & \mathfrak{H}(B) & \xrightarrow{\gamma_*} & \mathfrak{H}(C') & \xrightarrow{\rho'_*} & \mathfrak{H}(A') & \longrightarrow & k. \end{array}$$

Therefore there exists a morphism g of N into $\mathfrak{H}(B)$ subh that $\gamma_* g = h_* i$. From this we see that $C' = C_g$ q.e.d.

If (C, γ, ϕ) is an element of $\mathrm{Ext}(A,B)$, $(\mathfrak{H}(C), \gamma_*, \psi_*)$ is in $\mathrm{Ext}(\mathfrak{H}(A),\mathfrak{H}(B))$ by Theorem 2. Denoting by i_1 the homomorphism of $\mathrm{Ext}(\mathfrak{H}(A),\mathfrak{H}(B))$ into $\mathrm{Ext}(N(\rho),\mathfrak{H}(B))$ induced from the morphism i of $N(\rho)$ into $\mathfrak{H}(A)$, we define $\tilde{i}_1$ of $\mathrm{Ext}(A,B)$ into $\mathrm{Ext}(N(\rho),\mathfrak{H}(B))$ by $\tilde{i}_1(C) = i_1(\mathfrak{H}(C))$. Then we have

Lemma 10. *The sequence*

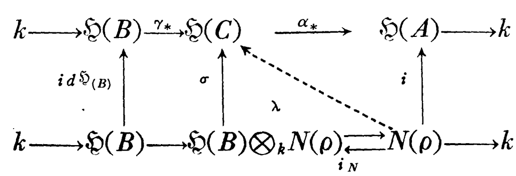
$$\mathrm{Ext}(A',B) \xrightarrow{\tilde{\rho}_1} \mathrm{Ext}(A,B) \xrightarrow{\tilde{i}_1} \mathrm{Ext}(N(\rho),\mathfrak{H}(B))$$

is exact.

Proof. Since the sequence

$$\mathrm{Ext}(\mathfrak{H}(A'),\mathfrak{H}(B)) \xrightarrow{(\rho_*)_1} \mathrm{Ext}(\mathfrak{H}(A),\mathfrak{H}(B)) \xrightarrow{i_1} \mathrm{Ext}(N(\rho),\mathfrak{H}(B))$$

is exact by Prop. 2.2. of Chap. VII in [5], we can easily see that the image of $\tilde{\rho}_1$ is contained in the kernel of $\tilde{i}_1$. Conversely let (C, γ, α) be an element of $\mathrm{Ext}(A,B)$ such that $\tilde{i}_1(C) = 0$. Then we have the following commutative diagram



with split second row. Since $\lambda = \sigma i_N$ is a monomorphism in $\mathscr{C}$, $\lambda(N)$ may be identified with N. If ψ is a purely inseparable isogeny of C onto a group variety C' corresponding to $N = \lambda(N)$, there exists an algebraic homomorphism ϕ of C' into A' such that $\phi\psi = \rho\alpha$ by Lemma 5, since $\rho_* \alpha_* \lambda_* (N^+) = \rho_* i(N^+) = 0$. Then the sequence $0 \longrightarrow B \xrightarrow{\psi\gamma} C' \xrightarrow{\phi} A' \longrightarrow 0$ is strictly exact. For we can easily see that the sequence $0 \longrightarrow \mathfrak{H}(B) \xrightarrow{(\psi\gamma)_*} \mathfrak{H}(C') \xrightarrow{\phi_*} \mathfrak{H}(A') \longrightarrow 0$ is exact in $\mathscr{C}$. Moreover we see, from the definition of C and C', $C = \tilde{\rho}_1(C')$. q.e.d.

In conclusion we have the following

Theorem 3. *The notation being as above, we have the following exact sequene*:

$$0 \longrightarrow \mathrm{Hom}(A',B) \xrightarrow{\tilde{\rho}} \mathrm{Hom}(A,B) \xrightarrow{\tilde{i}} \mathrm{Hom}_{\mathscr{C}}(N(\rho),\mathfrak{H}(B)) \xrightarrow{d} \mathrm{Ext}(A',B)$$

$$\xrightarrow{\rho_1} \mathrm{Ext}(A,B) \xrightarrow{\tilde{i}_1} \mathrm{Ext}(N(\rho),\mathfrak{H}(B)).$$

§4 Hopf algebras and rational representations

First we give some results on Hopf subalgebras of the Hopf algebra $\mathfrak{H}(G)$

attached to a group variety G corresponding to group subvarieties of G. In this section we identify the Hopf algebra $\mathfrak{H}(H)$ attached to a group subvariety H of G with Hopf subalgebra $i_*(\mathfrak{H}(H))$ of $\mathfrak{H}(G)$, where i_* is the tangential homomorphism of $\mathfrak{H}(H)$ to $\mathfrak{H}(G)$ induced by the canonical injection i of H into G.

PROPOSITION 4. *Let H and K be two group subvarieties of a group variety G. Then K is a group subvariety of H if and only if $\mathfrak{H}(H)$ contains $\mathfrak{H}(K)$.*

PROOF. Let $\mathfrak{a}$ and $\mathfrak{b}$ be the prime ideals of the local ring $\mathcal{O}=\mathcal{O}_{e,G}$ corresponding to H and K respectively. By Lemma 14 and Proposition 16 in [8] we know that $\mathfrak{H}(G)$ may be identified with the set of continuous k-linear homomorphismm of $\mathcal{O}$ with the $\mathfrak{m}$-adic topology to k with the discrete topology where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$. Then we easily see that $\mathfrak{H}(H)$ (resp. $\mathfrak{H}(K)$) consists of the elements D of $\mathfrak{H}(G)$ such that $D(\mathfrak{a})=0$ (resp. $D(\mathfrak{b})=0$). On the other hand $\mathfrak{a}$ (resp. $\mathfrak{b}$) consists of the elements x of $\mathcal{O}$ such that $D(x)=0$ for any D in $\mathfrak{H}(H)$ (resp. $\mathfrak{H}(K)$), since $\mathfrak{a}=\bigcap_{n=0}^{\infty}(\mathfrak{m}^n+\mathfrak{a})$ and $\mathfrak{b}=\bigcap_{n=0}^{\infty}(\mathfrak{m}^n+\mathfrak{b})$. Therefore $\mathfrak{a}$ is contained in $\mathfrak{b}$ if and only if $\mathfrak{H}(H)$ contains $\mathfrak{H}(K)$. This completes the proof. q.e.d.

COROLLARY. *Let G, H and K be as in Proposition 4. Let $\mathfrak{a}$ be the prime ideal of the local ring $\mathcal{O}=\mathcal{O}_{e,G}$ corresponding to the group subvariety H of G and $\{t_1,\cdots,t_n\}$ be a regular system of parameters of $\mathcal{O}$ such that $\mathfrak{a}$ is generated by a subset $\{t_1,\cdots,t_r\}$ of $\{t_1,\cdots,t_n\}$. If $\{I_{a_1\dots a_n}\mid a_i\geqslant 0\}$ is the canonical basis of $\mathfrak{H}(G)$ with respect to $\{t_1,\cdots,t_n\}$, then the following three conditions are equivalent:*

(i) *K is a group subvariety of H.*
(ii) *If $D=\sum_{(a)}\alpha_{a_1\dots a_n}I_{a_1\dots a_n}$ is in $\mathfrak{H}(K)$ and if $i\leqslant r$, we have $\alpha_{a_1\dots a_n}=0$ for $a_i=1$ and $a_j=0$ $(i\neq j)$.*
(iii) *If $D=\sum_{(a)}\alpha_{a_1\dots a_n}I_{a_1\dots a_n}$ is in $\mathfrak{H}(K)$ and if $i\leqslant r$, we have $\alpha_{a_1\dots a_n}=0$ for $a_i\neq 0$.*

PROOF. First we assume the condition (i). Then, as shown in the proof of Proposition 4, we see $D(\mathfrak{a})=0$ for any D in $\mathfrak{H}(K)$ if $\mathfrak{H}(G)$ is identified with the set of continuous k-linear homomorphisms of $\mathcal{O}$ into k. Since $t_1^{a_1}\cdots t_n^{a_n}$ is contained in $\mathfrak{a}$ if $a_i\neq 0$ for some $i\leqslant r$, this means that $\alpha_{a_1\dots a_n}=D(t_1^{a_1}\cdots t_n^{a_n})=0$ and hence the condition (iii) is satisfied. It is trivial the condition (ii) is satisfied if (iii) is so. Lastly assume that the condition (ii) is true. If K is not a group subvariety of H, then there exists an element t_i contained in $\mathfrak{a}$ such that t_i does not belong to the prime ideal $\mathfrak{b}$ of $\mathcal{O}$ corresponding to K. As seen in the proof of Proposition 4 there exists an element D in $\mathfrak{H}(G)$ such that $D(t_i)\neq 0$ and $D(\mathfrak{b})=0$. If $D=\sum_{(a)}\alpha_{a_1\dots a_n}I_{a_1\dots a_n}$, this means that $D(t_i)=\alpha_{0\cdots 0\overset{i}{1}0\cdots 0}\neq 0$. This is a contradiction. q.e.d.

Now we denote by G_n the general linear group GL_n whose affine ring over k is $k[t_{11},\cdots, t_{nn}, D^{-1}]$, where $D=\det(t_{ij})$. Then we have $XY=(\sum_{h=1}^{n}\xi_{ih}\eta_{hj})$ for $X=(\xi_{ij})$ and $Y=(\eta_{ij})$ in G_n. If we put $s_{ij}=t_{ij}-\delta_{ij}$ for $i, j=1, 2,\cdots, n$, where $\delta_{ij}=0$ for $i\neq j$ and $\delta_{ii}=1$, we see that $\{s_{11},\cdots s_{nn}\}$ is a regular system of parameters of the local ring $\mathcal{O}_{e,G_n}$ of G_n at the point $E=(\delta_{ij})$. Let $\{I_{a_{11}\cdots a_{nn}}|a_{ij}\geqslant 0\}$ be the canonical basis of $\mathfrak{H}(G_n)$ with respect to $\{s_{11},\cdots, s_{nn}\}$. In particular we denote dy $I_{ij}^{(r)}$ the element $I_{a_{11}\cdots a_{nn}}$ such that $a_{ij}=p^r$ and $a_{hl}=0$ for $(h, l)\neq(i, j)$ and call it *a distinguished element of height* r. Then we have

LEMMA 11. *Let* $\{s_{11},\cdots, s_{nn}\}$ *and* $\{I_{a_{11}\cdots a_{nn}}|a_{ij}\geqslant 0\}$ *be as above. Then we have*

(i) $I_{ij}^{(r)}(s_{lm}^{p^u})=(s_{li}^{p^u}+\delta_{li})\delta_{jm}\delta_{ru}$,

and (ii) $I_{a_{11}\cdots a_{nn}}(s_{lm}^{p^u})=0$ *if* $I_{a_{11}\cdots a_{nn}}$ *is not a distinguished element.*

PROOF. Let X and Y be two independent generic points of G_n over k and put $s_{ij}(X)=\xi_{ij}$ and $s_{ij}(Y)=\eta_{ij}$ for $i, j=1, 2,\cdots, n$. Since we have

$$s_{ij}(XY)+\delta_{ij}=\sum_{h=1}^{n}(s_{ih}(X)+\delta_{ih})\,(s_{hj}(Y)+\delta_{hj}),$$

it is easily see that

$$s_{ij}(XY)^{p^u}-s_{ij}(X)^{p^u}=\sum_{h=1}^{n}(\xi_{ih}^{p^u}+\delta_{ih})\eta_{hj}^{p^u}.$$

From this equality, we see that (i) and (ii) in our lemma are given from the definition of $\{I_{a_{11}\cdots a_{nn}}\}$ (cf. §4 in [8]). q.e.d.

Now let $M_n(k)$ be the ring of all the square matrices of degree n with elements in the field k. Then we define a mapping ρ_r of $\mathfrak{H}(G_n)$ to $M_n(k)$ by $\rho_r(D)=(D_e(s_{ij}^{p^r}))$ for D in $\mathfrak{H}(G_n)$, where D_e is the local component of D at e defined in §3 of [8]. If $D=\sum_{(a)}\alpha_{a_{11}\cdots a_{nn}}I_{a_{11}\cdots a_{nn}}$, we see that $\rho_r(D)=(\alpha_{ij}^{(r)})$ by the definition of the canonical basis $\{I_{a_{11}\cdots a_{nn}}|a_{ij}\geqslant 0\}$ of $\mathfrak{H}(G_n)$, where $\alpha_{ij}^{(r)}$ is the element $\alpha_{a_{11}\cdots a_{nn}}$, for each (i, j) and r, such that $a_{ij}=p^r$ and $a_{hl}\neq 0$ for $(h, l)\neq(i, j)$. Now we show the following

PROPOSITION 5. *The notation being as above,* ρ_r *is a k-algebra homomorphism of* $\mathfrak{H}(G_n)$ *to* $M_n(k)$ *for any non-negative integer* r.

PROOF. It is clear that ρ_r is a k-linear mapping, and hence it is sufficient to show that

$$\rho_r(I_{a_{11}\cdots a_{nn}}I_{b_{11}\cdots b_{nn}})=\rho_r(I_{a_{11}\cdots a_{nn}})\,\rho_r(I_{b_{11}\cdots b_{nn}}).$$

If one of $I_{a_{11}\cdots a_{nn}}$ and $I_{b_{11}\cdots b_{nn}}$ is not a distinguished element of height r, we see by Lemma 11

$$\rho_r(I_{a_{11}\cdots a_{nn}}I_{b_{11}\cdots b_{nn}})=\rho_r(I_{a_{11}\cdots a_{nn}})\,\rho_r(I_{b_{11}\cdots b_{nn}})=0.$$

Thus we may assume that $I_{a_{11}\cdots a_{nn}}=I_{ij}^{(r)}$ and $I_{b_{11}\cdots b_{nn}}=I_{lm}^{(r)}$. Let $E_{ij}=(\varepsilon_{\lambda\mu})$ be the square matrix of degree n such that $\varepsilon_{ij}=1$ and $\varepsilon_{\lambda\mu}=0$ for $(\lambda, \mu)\neq(i, j)$. By Lemma 11, we have

$$I_{ij}^{(r)}I_{lm}^{(r)}(s_{\lambda\mu}^{p^r})=I_{ij}^{(r)}((s_{\lambda l}^{p^r}+\delta_{\lambda l})\delta_{m\mu})$$
$$=\delta_{m\mu}\delta_{lj}(s_{\lambda i}^{p^r}+\delta_{\lambda i}), \qquad (*)$$

and hence $\qquad I_{ij}^{(r)}I_{lm}^{(r)}(s_{\lambda\mu}^{p^r})=0 \qquad \text{if } j\neq l.$

This means that

$$\rho_r(I_{ij}^{(r)}I_{lm}^{(r)})=0=\rho_r(I_{ij}^{(r)})\rho_r(I_{lm}^{(r)}) \qquad \text{for } j\neq l,$$

since $\rho_r(I_{ij}^{(r)})=E_{ij}$ and $\rho_r(I_{lm}^{(r)})=E_{lm}$. If $j=l$, we have

$$\rho_r(I_{ij}^{(r)}I_{jm}^{(r)})=E_{im}=E_{ij}E_{jm}=\rho_r(I_{ij}^{(r)})\rho_r(I_{jm}^{(r)}),$$

since $(I_{ij}^{(r)}I_{jm}^{(r)})_e(s_{\lambda\mu}^{p^r})=\delta_{\lambda i}\delta_{m\mu}$ by the epuality $(*)$. This completes the the proof. q.e.d.

Let V be a vector space of dimension n over k and GL_V the group of linear automorphisms of V which has a structure of a group variety defined over k. Precisely if $\{v_1,\cdots, v_n\}$ is a basis of V over k, GL_V may be identified with the general linear group G_n naturally such that an element l in GL_V corresponds to (λ_{ij}), where $l(v_i)=\sum_{j=1}^{n}\lambda_{ij}v_j$.

Now let G be a group variety over k and assume that there exists a rational representation ϕ of G to GL_V defined over k. Then we show that V has a structure of $\mathfrak{H}(G)$-module determined depending on ϕ. In fact let ϕ_* be the tangential mapping of $\mathfrak{H}(G)$ to $\mathfrak{H}(GL_V)=H(\mathfrak{G}_n)$ induced by ϕ and ρ_0 the k-algebra homomorphism of $\mathfrak{H}(G_n)$ to $M_n(k)$ defined in the above. Moreover we consider any element $A=(\alpha_{ij})$ of $M_n(k)$ as a linear endomorphism of V such that $A(v_i)=\sum_{j=1}^{n}\alpha_{ij}v_j$ for each $i=1, 2,\cdots, n$. Then if we denote by $D(v)$ the element $\rho_0(\phi_*(D))(v)$ of V for D in $\mathfrak{H}(G)$ and v in V, we see by Proposition 4 that

$$(\alpha D+\alpha' D')(v)=\alpha D(v)+\alpha' D'(v)$$

$$(DD')(v)=D(D'(v))$$

$$D(\alpha v+\alpha' v')=\alpha D(v)+\alpha' D(v')$$

$$1(v)=v$$

for D and D' in $\mathfrak{H}(G)$, v and v' in V, and α and α' in k. It is easy to see that this structure is determined independently of the choice of the basis

$\{v_1,\cdots, v_n\}$ of V over k.

A vector subspace W of V is called a G-submodule of V, if $\phi(g)W$ is equal to W for any element g of G. Then a rational representation ϕ' of G to GL_W is obtained naturally from ϕ. Similarly W is called a $\mathfrak{H}(G)$-submobule if $D(W)$ is contained in W for any element D of $\mathfrak{H}(G)$. If $\mathfrak{g}_0$ is the Lie algebra of G consising of left invaiant derivations of G, we can also give the definition of $\mathfrak{g}_0$-submodules of V, and it is known, in characteristic 0, that W is a G-submodule of V if and only if it is a $\mathfrak{g}_0$-submodule of V (cf. e. g., Proposition 3.31 in [3]). The following theorem is a modification of this fact in a positive characteristic p.

THEOREM 4. *Let V be a finite dimensional vector space over k, and let ϕ be a rational representation of a group variety G to GL_V. Then a subspace W of V is a G-submodule of V if and only if it is a $\mathfrak{H}(G)$-submodule of V.*

PROOF. Let H be the group subvariety of GL_V which consists of the elements x of GL_V such that xW is contained in W. Then we show that $\rho_0(\mathfrak{H}(H))$ is the set of the elements A in $M_n(k)$ such that $AW\subset W$. For let $\{v_1,\cdots, v_n\}$ be a basis of V such that $\{v_1,\cdots, v_r\}$ is that of W, and we identify GL_V with G_n using this basis as seen in the above. Then H is the subgroup of G_n consisting of the elements $\begin{pmatrix} A & 0 \\ B & C\end{pmatrix}$ of G_n, where A and C are square matrices of degree r and $n-r$ respectively and $\{\bar{s}_{ij}\,|\,i>r+1 \text{ or } j<r\}$ is a regular system of parameters of the local ring $\mathcal{O}_{e,H}$, where $\bar{s}_{ij}$ is the image of s_{ij} under the canonical mapping of $\mathcal{O}_{e,G}$ to $\mathcal{O}_{e,H}$. Therefore if we denote by $\{I'_{a_{11}\cdots a_{nn}}\,|\,a_{ij}\geqslant 0 \text{ and } a_{hl}=0 \text{ if } 1\leqslant h\leqslant r \text{ and } r+1\leqslant l\leqslant n\}$ the canonical basis of $\mathfrak{H}(H)$ with respect to $\{\bar{s}_{ij}\}$, we see $j_*(I'_{a_{11}\cdots a_{nn}})=I_{a_{11}\cdots a_{nn}}$, where j_* is the tangential mapping of $\mathfrak{H}(H)$ to $\mathfrak{H}(\mathrm{GL}_V)$ induced by the canonical injection j of H into GL_V. Then by the definition of ρ_0 we see easily $\rho_0(\mathfrak{H}(H))=\{A\in M_n(k)\,|\,AW\subset W\}$.

First we assume that W is a G-submodule. Then $\phi(G)$ is contained in H and hence $\phi_*(\mathfrak{H}(G))$ is contained in $\mathfrak{H}(H)$. Since $\rho_0(\mathfrak{H}(H))W$ is equal to W, this means that W is a $\mathfrak{H}(G)$-submodule of V by the definition of the operation of the operation of $\mathfrak{H}(G)$ on V. Conversely assume that W is a $\mathfrak{H}(G)$-submodule of V. If G_1 is the image $\phi(G)$ of G, G_1 is a group subvariety of GL_V and ϕ_* maps $\mathfrak{H}(G)$ onto $\mathfrak{H}(G_1)$. This means that W is also a $\mathfrak{H}(G_1)$-submodule of V. On the other hand W is a G-submodule of V if and only if it is a G_1-submodule of V. Therefore we may assume that G is a group subvariety of GL_V and that ϕ is the canonical injection. Let $D=\sum_{(a)}\alpha_{a_{11}\cdots a_{nn}}I_{a_{11}\cdots a_{nn}}$ be an element in $\mathfrak{H}(G)$ and let (i, j) be such a pair that $1\leqslant i\leqslant r$ and $r+1\leqslant j\leqslant n$. Since $\rho_0(\mathfrak{H}(G))$ is contained in $\rho_0(\mathfrak{H}(H))$ by assumption, we see that $\alpha_{a_{11}\cdots a_{nn}}=0$ if $a_{ij}=1$ and $a_{hl}=0$ for $(h, l)\neq(i, j)$. It is clear that the prime ideal of $\mathcal{O}_{e,G_n}$ corresponding to H is generated by the subset $\{s_{ij}\,|\,0\leqslant i\leqslant r, r+1\leqslant j\leqslant n\}$ of the regular system $\{s_{ij}\,|\,1\leqslant i, j\leqslant n\}$ of parameters, and therefore H contains G by Corollary of Proposition 4. This means that W is a G-submodule of V. q.e.d.

COROLLARY. *Let G, V and ϕ be as above. Then V is a completely reducible G-module if and only if it is a completely reducible $\mathfrak{H}(G)$-module.*

§5 Formal groups and algebraic Hopf algebras

Let G be a group variety defined over k. If we identify the Hopf algebra $\mathfrak{H}(G)$ of G with the set of continuous k-linear homomorphisms of $O_{e,G}$ to k, the Hopf algebra $\mathfrak{H}(H)$ of a group subvariety H of G may be identified with the Hopf subalgebra of $\mathfrak{H}(G)$ which consists of the elements D in $\mathfrak{H}(G)$ such that D annihilates the prime ideal of $O_{e,G}$ corresponding to H. Therefore the set of group subvarieties of G defined over k corresponds injectively to a subset of Hopf subalgebras of $\mathfrak{H}(G)$ by Proposition 4. Now we understand by *an algebraic Hopf subalgebra of* $\mathfrak{H}(G)$ a Hopf subalgebra corresponding to a group subvariety of G in this way. The aim of this section is to give a condition for a Hopf subalgebra of $\mathfrak{H}(G)$ to be algebraic.

For this purpose we give some results on Hopf algebras attached to formal groups which are already known (cf. §1 and §10 in [2], and [1]). Here we understand by *a formal group over a field* k a noetherian complete local ring R with maximal ideal $\mathfrak{m}$ satisfying the following conditions:

(i) R contains k and $R/\mathfrak{m}$ is canonically isomorphic to k.

(ii) There exists a continuous k-algebra homomorphism Δ of R with the $\mathfrak{m}$-adic topology to the complete tensor product $R\hat{\otimes}_k R$ such that $(\Delta\hat{\otimes} id_R)\Delta=(id_R\hat{\otimes}\Delta)\Delta$.

(iii) If ε is the canonical homomorphism of R to $k=R/\mathfrak{m}$, $(\varepsilon\otimes id_R)\Delta$ and $(id_R\otimes\varepsilon)\Delta$ are the natural isomorphism of R to $k\otimes R$ and $R\otimes k$ respectively.

(iv) There exists a continuous k-algebra automorphism c of R such that $\hat{m}(id_R\hat{\otimes}c)\Delta=\eta\varepsilon$ and $\hat{m}(c\hat{\otimes}id_R)\Delta=\eta\varepsilon$, where $\hat{m}$ is the completion of the multiplication of R and η is the canonical injection of k into R.

Now we denote by $\mathfrak{H}(R)$ the set of continuous k-linear mappings of R with the $\mathfrak{m}$-adic topology to k with the discrete topology. Then the vector space $\mathfrak{H}(R)$ over k is a Hopf algebra over k. In fact the coalgeba structure $(\tilde{\Delta}, \tilde{\varepsilon})$ of $\mathfrak{H}(R)$ is naturally defined by the algebra structure (m, η) of R by $\tilde{\Delta}(D)(x\otimes y)=D(xy)$ and $\tilde{\varepsilon}(D)=D(\eta)$ for D in $\mathfrak{H}(R)$ and x, y in R by Proposition 6.0.2 in [7], if we identify $\mathfrak{H}(R)\otimes_k\mathfrak{H}(R)$ with a subspace of the dual space of $R\otimes_k R$. As to the algebra structure of $\mathfrak{H}(R)$ we define the multiplicaton $\tilde{m}(D\otimes D')=D\cdot D'$ by $D\cdot D'(x)=(D\otimes D')(\Delta(x))$. It is easy to see that $D\cdot D'$ is contained in $\mathfrak{H}(R)$ and that this composition satisfies the associative law. Moreover we see that $\varepsilon\cdot D=D\cdot\varepsilon=D$ for any D in $\mathfrak{H}(R)$. If we define $\tilde{\eta}$ of k to $\mathfrak{H}(R)$ by $\tilde{\eta}(\alpha)=\alpha\varepsilon$, $(\tilde{m}, \tilde{\eta})$ is an algebra structure of $\mathfrak{H}(R)$. The antibode $\tilde{c}$ of $\mathfrak{H}(R)$ is given by $\tilde{c}(D)=Dc$ for any D in $\mathfrak{H}(R)$. Then it is easy to check that

$(\mathfrak{H}(R), \tilde{m}, \tilde{\eta}, \tilde{\varDelta}, \tilde{\varepsilon}, \tilde{c})$ is a Hopf algebra over k.

PROPOSITION. 6. *Let R be a formal group over k, and let $\mathfrak{H}_i$ be the subspace of $\mathfrak{H}(R)$ consisting of the elements D such that $D(\mathfrak{m}_i)=0$, where $\mathfrak{m}_i$ is the ideal of R generated by all the p^i-th exponents x^{p^i} of x in the maximal ideal $\mathfrak{m}$. Then $\mathfrak{H}_i$ is a Hopf subalgebra of $\mathfrak{H}(R)$ and $\mathfrak{m}_i$ is the set of all elements x in R such that $D(x)=0$ for any D in $\mathfrak{H}_i$.*

PROOF. Let $\{D_s \mid s \in S\}$ be a basis of $\mathfrak{H}_i$ and let $\{D'_t \mid t \in T\}$ be a subset of $\mathfrak{H}(R)$ such that the union $\{D_s \mid s \in S\} \cup \{D'_t \mid t \in T\}$ is a basis of $\mathfrak{H}(R)$. Then, for any element D in $\mathfrak{H}_i$, we have

$$\tilde{\varDelta}(D)=\sum_{j=1}^{m} E_{s_j} \otimes D_{s_j}+\sum_{h=1}^{n} E'_{t_h} \otimes D'_{t_h},$$

where E_{s_j} and E'_{t_h} are non-zero elements of $\mathfrak{H}(R)$. If $n>0$, there exists an element x of $\mathfrak{m}_i$ such that $D'_{t_1}(x) \neq 0$ and $D'_{t_h}(x)=0$ for $h \neq 1$. Therefore if y is an element of R such that $E'_{t_1}(y) \neq 0$, we have

$$\tilde{\varDelta}(D)(y \otimes x)=E'_{t_1}(y) D'_{t_1}(x) \neq 0.$$

But by the definition of $\tilde{\varDelta}$, we have $\tilde{\varDelta}(D)(y \otimes x)=D(yx)=0$, since D is in $\mathfrak{H}_i$. This is a contradiction. Therefore we see that $\tilde{\varDelta}(D)=\sum_{j=1}^{m} E_{s_j} \otimes D_{s_j}$. Similarly we see from this that $\tilde{\varDelta}(D)=\sum_{j,h} \alpha_{jh} D_j \otimes D_h$ fof α_{ij} in k. This means that $\mathfrak{H}_i$ is a subcoalgebra of $\mathfrak{H}(R)$. On the other hand we see eaaily that $\varDelta(\mathfrak{m}_i)$ is contained in the ideal of $R \hat{\otimes} R$ generated by $(\mathfrak{m}_i \otimes R+R \otimes \mathfrak{m}_i)$, since $\varDelta(\mathfrak{m})$ is contained in $(\mathfrak{m} \otimes R+R \otimes \mathfrak{m}) R \hat{\otimes} R$. Hence we heve $D \cdot D'(y)=(D \hat{\otimes} D')(\varDelta(y))=0$ for y in $\mathfrak{m}_i$ and D, D' in $\mathfrak{H}_i$. This means that $\mathfrak{H}_i$ is subalgebra of $\mathfrak{H}(R)$. It is clear that $\tilde{c}(\mathfrak{H}_i)=\mathfrak{H}_i$. Therefore $\mathfrak{H}_i$ is a Hopf subalgebra of $\mathfrak{H}(R)$. Moreover $\mathfrak{H}_i$ is the dual space of $R/\mathfrak{m}_i$ and hence the last assertion is seen, since $R/\mathfrak{m}_i$ is of fiinite dimension. q.e.d.

By Proposition 6, $R/\mathfrak{m}_i$ is also a formal group over k and $\mathfrak{H}_i$ may be identified with the Hopf algebra $\mathfrak{H}(R/\mathfrak{m}_i)$ of $R/\mathfrak{m}_i$. Then $\mathfrak{H}(R)$ is the inductive limit of $\mathfrak{H}(R/\mathfrak{m}_i)$. Now we denote by R_i the formal group $R/\mathfrak{m}_i$ and call it the formal subgroup of R of exponent i. In general we call a residue class ring $R/\mathfrak{a}$ of R *a formal subgroup of* R if $R/\mathfrak{a}$ has a structure $(R/\mathfrak{a}, \varDelta_{\mathfrak{a}}, \varepsilon_{\mathfrak{a}}, c_{\mathfrak{a}})$ of a formal group over k such that $(\pi \hat{\otimes} \pi)\varDelta=\varDelta_{\mathfrak{a}}\pi$, $\varepsilon=\pi\varepsilon_{\mathfrak{a}}$ and $c_{\mathfrak{a}}\pi=\pi c$, where π is the canonical homomorphis of R onto $R/\mathfrak{a}$. Then if we define a mapping π_* of $\mathfrak{H}(R/\mathfrak{a})$ to $\mathfrak{H}(R)$ by $\pi_*(D)=D\pi$ for D in $\mathfrak{H}(R/\mathfrak{a})$, we can easily see that π_* is a Hopf algebra homomorphism. Moreover we see that π_* is a monomorphism and that $\pi_*(\mathfrak{H}(R/\mathfrak{a}))$ consists of the elements D in $\mathfrak{H}(R)$ such that $D(\mathfrak{a})=0$. In the following we identify $\mathfrak{H}(R/\mathfrak{a})$ with $\pi_*(\mathfrak{H}(R/\mathfrak{a}))$. Then we have

THEOREM 5. *Let R be a formal group over k and let $\mathfrak{H}$ be a Hopf subalgebra* of $\mathfrak{H}(R)$. *Then there exists a unique formal subgroup* $R/\mathfrak{a}_{\mathfrak{H}}$ *of* R *such that* $\mathfrak{H}=\mathfrak{H}(R/\mathfrak{a}_{\mathfrak{H}})$.

PROOF. We denote by $\mathfrak{a}_{\mathfrak{H}}$ the set of the elements x in R such that $D(x)=0$ for any D in H. We shall see that $R/\mathfrak{a}_{\mathfrak{H}}$ is a formal subgroup of R. Let $\mathfrak{H}_i'$ be the intersection of $\mathfrak{H}$ and $\mathfrak{H}_i$, and let $\mathfrak{a}_i$ be the set of elements x in R such that $D(x)=0$ for any D in $\mathfrak{H}_i'$. Then $\mathfrak{H}_i'$ is a Hopf subalgebra of $\mathfrak{H}(R)$ for any i by Lemma 1 and proposition 6, and we have $\mathfrak{H}=\bigcup_{i=1}^{\infty}\mathfrak{H}_i'$. On the other hand $R/\mathfrak{m}_i$ is a Hopf algebra over k and $\mathfrak{H}_i=\mathfrak{H}(R/\mathfrak{m}_i)$ is the dual Hopf algebra of $R/\mathfrak{m}_i$, since $R/\mathfrak{m}_i$ is a formal group with the discrete topology by Proposition 6. Then we easily see that the annihilator $\mathfrak{a}_i/\mathfrak{m}_i$ of $\mathfrak{H}_i'$ is a Hopf ideal of $R/\mathfrak{m}_i$ by Proposition 1. 4. 3. and Proposition 1. 4. 6 in [7]. This means that $R/\mathfrak{a}_i$ is a Hopf algebra over k. Denote by $\varDelta_i$ and c_i the diagonal and the antipode of $R/\mathfrak{a}_i$. Then if π_{ij} is the natural homomorpism of $R/\mathfrak{a}_i$ to $R/\mathfrak{a}_j$ for $i\geqslant j$, we easily see that $(\pi_{ij}\otimes\pi_{ij})\varDelta_i=\varDelta_j\pi_{ij}$ and $\pi_{ij}c_i=c_j\pi_{ij}$. Now we easily see that $\mathfrak{a}_{\mathfrak{H}}$ is contained in $\mathfrak{a}'=\bigcap_{i=1}^{\infty}\mathfrak{a}_i$, since $\mathfrak{H}$ contains $\mathfrak{H}_i'$ for any i. Conversely let x be any element of $\mathfrak{a}'$. Then x is contained in $\mathfrak{a}_i$ for any i and hence we see that $D(x)=0$ for any element D in $\mathfrak{H}_i'$. Since $\mathfrak{H}=\bigcup_{i=1}^{\infty}\mathfrak{H}_i'$, x must be contained in $\mathfrak{a}_{\mathfrak{H}}$. Therefore $\mathfrak{a}_{\mathfrak{H}}$ is equal to $\mathfrak{a}'=\bigcap_{i=1}^{\infty}\mathfrak{a}_i$. Moreover the family $\{\mathfrak{a}_i/\mathfrak{a}_{\mathfrak{H}}\mid i=1, 2,\cdots\}$ is a fundamental basis of neighbourhoods of 0 in the $\mathfrak{m}/\mathfrak{a}_{\mathfrak{H}}$-adic topology of $\bar{R}=R/\mathfrak{a}_{\mathfrak{H}}$ by Theorem 13 of Chap. VIII in [9], since $\bar{R}$ is a complete local ring with a descending chain of ideals $\{\mathfrak{a}_i/\mathfrak{a}_{\mathfrak{H}}\}$ such that $\bigcap_{i=1}^{\infty}\mathfrak{a}_i/\mathfrak{a}_{\mathfrak{H}}=0$. Since $R/\mathfrak{a}_{\mathfrak{H}}=\varprojlim_i R/\mathfrak{a}_i$, there exists a unique mapping $\varDelta_{\mathfrak{H}}$ (resp. $c_{\mathfrak{H}}$) of $R/\mathfrak{a}_{\mathfrak{H}}$ to $R/\mathfrak{a}_{\mathfrak{H}}\hat{\otimes}R/\mathfrak{a}_{\mathfrak{H}}=\varprojlim_i R/\mathfrak{a}_i\otimes R/\mathfrak{a}_i$ (resp. $R/\mathfrak{a}_{\mathfrak{H}}$) induced by $\varDelta_i$ (resp. c_i) $(i=1. 2,\cdots)$. Then it is easy to see that $(R/\mathfrak{a}_{\mathfrak{H}}, \varDelta_{\mathfrak{H}}, c_{\mathfrak{H}})$ is a formal subgroup of R and that $\mathfrak{H}$ corresponds to $R/\mathfrak{a}_{\mathfrak{H}}$. q.e.d.

Now we consider a group variety G defined over k with the local ring $\mathcal{O}=\mathcal{O}_{e,G}$ at the neutral element e. Then if $\mathfrak{m}$ is the maxinal ideal of $\mathcal{O}$, it is well known that the completion $R=\bar{\mathcal{O}}$ of $\mathcal{O}$ with respect to the $\mathfrak{m}$-adic topology is a formal group over k whose diagonal $\varDelta_R$ and the antipode c_R is naturally obtained from the group structure of G. We call this formal group R *the formalization of* G. The Hopf algebra $\mathfrak{H}(R)$ of R is isomorphic to $\mathfrak{H}(G)$ and hence we may identify them. If $\mathcal{O}'$ is the local ring $\mathcal{O}_{e\times e,G\times G}$ of $G\times G$ at the point $e\times e$, it is the quotient ring $(\mathcal{O}\otimes_k\mathcal{O})_S$ of $\mathcal{O}\otimes_k\mathcal{O}$ with respect to the multiplicatively closed set S which is the complement of the maximal ideal $\mathfrak{m}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{m}$ in $\mathcal{O}\otimes_k\mathcal{O}$. The comorphism $\varDelta_G$ of $k(G)$ to $k(G\times G)$ defined by the multiplication of $G\times G$ to G induces a homomorphism $\varDelta$ of $\mathcal{O}$ to $\mathcal{O}'$. Then $\varDelta$ is the restriction of the diagonal $\varDelta_R$ of R to $\mathcal{O}$ by the definition of the formalization R, if we identify $\mathcal{O}'$ with a subring of $R\hat{\otimes}R$. Moreover we denote by c the restriction of c_R to $\mathcal{O}$.

Proposition 7. *Let G, $\mathcal{O}$, $\mathcal{O}'$ and R be as above, and let $\mathfrak{H}$ be a Hopf subalgebra of $\mathfrak{H}(R)$. If $\mathfrak{a}$ is the set of the elements x of $\mathcal{O}$ such that $D(x)=0$ for any D in $\mathfrak{H}$. Then $\mathfrak{a}$ is an ideal of $\mathcal{O}$. Moreover if $\mathfrak{H}$ is the set of the elements D in $\mathfrak{H}(R)$ such that $D(\mathfrak{a})=0$, $\Delta(\mathfrak{a})$ is contained in the ideal of $\mathcal{O}'$ generated by $\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a}$ and $c(\mathfrak{a})$ is equal to $\mathfrak{a}$.*

Proof. By Theorem 5 it is clear that $\mathfrak{a}=\mathcal{O}\cap\mathfrak{a}_{\mathfrak{H}}$ is an ideal of $\mathcal{O}$. Moreover if $\mathfrak{H}$ is the set of the elements D in $\mathfrak{H}(R)$ such that $D(\mathfrak{a})=0$, the closure $\bar{\mathfrak{a}}$ of $\mathfrak{a}$ in R is $\mathfrak{a}_{\mathfrak{H}}$. In fact if there exists an element x in $\mathfrak{a}_{\mathfrak{H}}$ but not in $\bar{\mathfrak{a}}$, x is not contained in $\mathfrak{a}+m^{p^s}$ for a sufficiently large s. Then there exists an element D in $\mathfrak{H}(R)$ such that $D(x)\neq 0$ and $D(\mathfrak{a}+\mathfrak{m}^{p^s})=0$. By assumption D is contained in $\mathfrak{H}$. But this is a contradiction to the fact that x is in $\mathfrak{a}_{\mathfrak{H}}$.

Now let x be in $\mathfrak{a}$. Using the notations of the proof of Theorem 5, x is contained in $\mathfrak{a}_i$ for any i. Since $R/\mathfrak{a}_i$ is a Hopf algeba over k, it is seen that $\Delta_R(x)$ is contained in $\mathfrak{b}_i=(\mathfrak{a}_i\otimes R+R\otimes\mathfrak{a}_i)R\hat{\otimes}R$. On the other hand the set of the ideals $\mathfrak{b}_i(i=1.\ 2,\cdots)$ is a fundamental system of neighbourhoods of $\mathfrak{a}_{\mathfrak{H}}\otimes R+R\otimes\mathfrak{a}_{\mathfrak{H}}$ in the completion $\bar{\mathcal{O}}'=R\hat{\otimes}R$ of $\mathcal{O}'$, we have

$$\bigcap_{i=1}^{\infty}((\mathfrak{a}_i\otimes R+R\otimes\mathfrak{a}_i)R\hat{\otimes}R)=\overline{\mathfrak{a}_{\mathfrak{H}}\otimes R+R\otimes\mathfrak{a}_{\mathfrak{H}}}$$
$$=\overline{\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a}}\qquad \text{in } R\hat{\otimes}R,$$

since $\mathfrak{a}$ is dense in $\mathfrak{a}_{\mathfrak{H}}$ as seen in the above. It is clear that $\Delta(x)$ is in $\mathcal{O}'$. Therefore $\Delta(x)$ belongs to $\overline{(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})}\cap\mathcal{O}'=(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\mathcal{O}'$. This means that $\Delta(\mathfrak{a})$ is contained in $(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\mathcal{O}'$. Similarly $\Delta(\mathfrak{a})$ is contained in $\Delta_R(\mathfrak{a}R)=\mathfrak{a}_{\mathfrak{H}}$ and hence in $\mathfrak{a}=\mathfrak{a}\bar{R}\cap\mathcal{O}=\mathfrak{a}_{\mathfrak{H}}\cap\mathcal{O}$. q.e.d.

Lemma 12. *Let G be a group variety over k and H a closed subset of G saatisfying the following conditions:*

(i) *there exists a dense open subset U of H such that $U\cdot U$ is contained in H.*

and (ii) *there exists a dense open subset V of H such that V^{-1} is contained in H.*

Then H is an algebraic subgroup of G.

The proof is easy and hence we omit it.

Corollary. *Let G, $\mathcal{O}$ and $\mathcal{O}'$ be as in proposition 7 and let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ such that $\Delta(\mathfrak{a})\subset(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\mathcal{O}'$ and $c(\mathfrak{a})\subset\mathfrak{a}$. Then if $\mathfrak{a}$ is equal to its radical $\sqrt{\mathfrak{a}}$, $\mathfrak{a}$ is a prime ideal of $\mathcal{O}$ corresponding to a group subvariety of G.*

Proof. If H is the algebraic subset of G defined by $\mathfrak{a}$, any component of H contains the neutral element e of G. On the other hand if $V=\mathrm{Spec}(B)$ is an affine open set of G containing e, there exists an affine open set $U=\mathrm{Spec}(A)$ of G containing e such that $U\cdot U\subset V$ and $U^{-1}\subset V$. Then the restriction Δ_B

(resp. c_B) of the diagonal Δ of $\mathcal{O}$ to $\mathcal{O}'$ (resp. the antipode c of $\mathcal{O}$ to $\mathcal{O}$) to B is a homomorphism of B to $A\otimes_k A$ (resp. to A). Now recall that if $\mathfrak{p}$ and $\mathfrak{p}'$ are two prime ideals of $\mathcal{O}$, $\mathfrak{p}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{p}'$ is also a prime ideal of $\mathcal{O}\otimes_k\mathcal{O}$. On the other hand we can easily see in a similar way to the proof of Lemma 1 that $(\mathfrak{a}_1\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{b})\cap(\mathfrak{a}_2\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{b})=(\mathfrak{a}_1\cap\mathfrak{a}_2)\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{b}$ for any ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{b}$ of $\mathcal{O}$. Therefore if $\mathfrak{a}$ is an intersection of prime ideals $\mathfrak{p}_i$ $(i=1, 2,\dots, s)$, $\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a}$ is the intersection of prime ideals $\mathfrak{p}_i\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{p}_j(i, j=1, 2,\dots, s)$. In particular we see that $(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\mathcal{O}'\cap(\mathcal{O}\otimes\mathcal{O})=\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a}$, since S and $\mathfrak{p}_i\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{p}_j$ have the empty intersection for any i, j. By assumption we have

$$\begin{aligned}\Delta_B(\mathfrak{a}\cap B)&\subset(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\mathcal{O}'\cap(A\otimes_k A)\\&=(\mathfrak{a}\otimes\mathcal{O}+\mathcal{O}\otimes\mathfrak{a})\cap(A\otimes_k A)\\&=(\mathfrak{a}\cap A)\otimes_k A+A\otimes_k(\mathfrak{a}\cap A)\end{aligned}$$

and $c_B(\mathfrak{a}\cap B)\subset\mathfrak{a}\cap A$. This means that

$$(H\cap U)(H\cap U)\subset H\cap V\subset H \text{ and } (H\cap U)^{-1}\subset H\cap V\subset H.$$

Therefore, by Lemma 12, H is an algebraic subgroup of G, since $H\cap U$ is a dense open subset of H. Then $\mathfrak{a}$ must be a prime ideal, because a connected algebraic group is irreducible. q.e.d.

Now we have the last

THEOREM 6. *Let G be a group variety defined over k and $\mathfrak{H}(G)$ the Hopf algebra attached to G. Then a Hopf subalgebra $\mathfrak{H}$ of $\mathfrak{H}(G)$ is an algebraic one if and only if $\mathfrak{H}$ satisfies the following conditions:*

(i) *the ideal $\mathfrak{a}$ of $\mathcal{O}_{e,G}$ consisting of the elements x such that $D(x)=0$ for any D in $\mathfrak{H}$ is equal to its radical $\sqrt{\mathfrak{a}}$,*

and (ii) *$\mathfrak{H}$ is the set of the elements D in $\mathfrak{H}(G)$ such that $D(\mathfrak{a})=0$.*

PROOF. It is sufficient to see the "if" part. We assume that $\mathfrak{H}$ satisfies (i) and (ii) in our theorem. Then, by Proposition 7, $\mathfrak{a}$ satisfies the condition in Corollary of Lemma 12 and hence, by the collorary, $\mathfrak{a}$ is a prime ideal corresponding to a group subvariety H of G, since $\mathfrak{a}=\sqrt{\mathfrak{a}}$. This means that $\mathfrak{H}$ is a Hopf algebra attached to H by the condition (ii). q.e.d.

References

[1] P. Cartier, "Hyperalgèbes et groupes de Lie formels", Séminaire "Sophus Lie", 2e année: 1955/56.

[2] P. Cartier, "Arithmétique des groupes algébriques", Colloque. Thèorie des Groupes algébriques à Bruxelles (1962). (Centre bélge de Rech. Math. 87-111.

[3] J. Fogarty, "Invariant Theory", W. A. Beniamin, Inc., (1969), New York and Amsterdam.

[4] K. Kosaki and H. Yanagihara, "On purely inseparable Extensions of Algebraic Function Fields", J. Sci. Hiroshima Univ. Ser. A-I. **34** (1970), 69-72.

[5] B. Mitchell, "Theory of Categories", Academic Press (1965), New York and London.
[6] J. -P. Serre, "Quélque propriétés des variétés abéliennes en caractéristique p", Amer. J. Math. **80** (1958), 715-739.
[7] M. E. Sweedler, "Hopf Algebras", W. A. Benjamin, Inc., (1969), New York.
[8] H. Yanagihara, "On the structure of bialgebras attached to group varieties", J. Sci. Hirohsima Univ. Ser. A-I. **34** (1970), 29-58.
[9] O. Zariski and P. Samuel, "Commutative Algebra Vol. II", D. Van Nostrand Co. Inc. (1960), Princeton.

Department of Mathematics,
Faculty of Science,
Hiroshima University.