J. Math. Soc. Japan
Vol. 32, No. 3, 1980

On extensions of Lie algebras by algebras

By Mitsuhiro TAKEUCHI

(Received Sept. 9, 1978)

Introduction.

Let k be a commutative ring of prime characteristic p. Let A be a k-algebra, and let L be a restricted Lie algebra (p-Lie algebra) over k. We assume A and L are finitely generated projective k-modules. The first aim of this article is to establish a categorical correspondence among the following three kinds of objects;

I) Pairs of an extension of affine k-group schemes

$$1 \longrightarrow \mu^A \longrightarrow G \longrightarrow \mathcal{E}(L) \longrightarrow 1$$

and an admissible homomorphism

$$\rho: G \longrightarrow \mathrm{Aut}(A),$$

where μ^A and $\mathrm{Aut}(A)$ denote the k-group functors which send each commutative k-algebra T to

$$T \mapsto \text{the group of units in } T \otimes A,$$

$$T \mapsto \text{the group of } T\text{-algebra automorphisms of } T \otimes A,$$

respectively, and $\mathcal{E}(L)$ denotes the finite k-group scheme associated with L [**2**, p. 277]. By ρ admissible we mean that

$$gxg^{-1} = \rho(g)(x), \qquad \forall g \in G(T), \qquad \forall x \in \mu^A(T),$$

$$xyx^{-1} = \rho(x)(y), \qquad \forall x \in \mu^A(T), \qquad \forall y \in T \otimes A,$$

for each commutative k-algebra T.

II) Exact sequences of restricted Lie algebras

$$0 \longrightarrow A \longrightarrow X \longrightarrow L \longrightarrow 0$$

such that for each $x \in X$,

$$\mathrm{ad}(x) = [x, -]: A \longrightarrow A$$

is a k-algebra derivation.

III) Triples (S, θ, u) where S is a k-algebra,

$$\theta: S \longrightarrow S \otimes U^{[p]}(L)$$

is a right comodule structure and a k-algebra map with $U^{[p]}(L)$ the universal restricted enveloping Hopf algebra of L, and

$$u: A \longrightarrow S$$

is a k-algebra map such that $\theta(u(a)) = u(a) \otimes 1$, $\forall a \in A$. The triple must satisfy 1) the map

$$\bar{\theta}: S \otimes_A S \longrightarrow S \otimes U^{[p]}(L), \qquad \bar{\theta}(x \otimes y) = (x \otimes 1)\theta(y)$$

is an isomorphism, 2) there is an isomorphism

$$f: S \cong A \otimes U^{[p]}(L)$$

which is a left A-module and a right $U^{[p]}(L)$-comodule isomorphism.

The correspondence I $\leftrightarrow$ III follows almost directly from [**5**] [**6**], if we note that all extensions of $\mathcal{E}(L)$ by μ^A are H-extensions [**2**, p. 189], since μ^A is smooth and $\mathcal{E}(L)$ is infinitesimal.

Next, assume A is commutative. If (G, ρ) is an object of I, then the homomorphism ρ factors through $G \to \mathcal{E}(L)$. Similarly, if X is an object of II, then the restricted Lie map

$$\mathrm{ad}: X \longrightarrow \mathrm{Der}_k(A)$$

where $\mathrm{Der}_k(A)$ denotes the restricted Lie algebra of all k-algebra derivations of A, factors through $X \to L$. If (S, θ, u) is an object of III, there is a unique structure of a left $U^{[p]}(L)$-comodule algebra on A such that

$$xa = \sum_{(x)} (x_{(1)} \cdot a) x_{(0)}, \qquad \forall x \in S, \qquad \forall a \in A,$$

where $\theta(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$.

On the other hand, there is a 1-1 correspondence among homomorphisms of group functors

$$\tilde{\alpha}: \mathcal{E}(L) \longrightarrow \mathrm{Aut}(A),$$

restricted Lie maps

$$\alpha: L \longrightarrow \mathrm{Der}_k(A),$$

and measuring homomorphisms

$$\alpha': U^{[p]}(L) \longrightarrow \mathrm{End}_k(A).$$

In each case of the above, we say (G, ρ) is $\tilde{\alpha}$-admissible (resp. X is α-admissible, resp. (S, θ, u) is α'-admissible), if the object determines $\tilde{\alpha}$ (resp. α, resp. α').

We can prove that the correspondence we establish induces a correspondence among $\tilde{\alpha}$-admissible objects, α-admissible objects, and α'-admissible objects.

Thirdly, we fix α. Let

$$\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L),\ \mu^A) \quad (\text{resp. } \mathrm{Ext}_{\alpha}(L,\ A), \text{ resp. } \mathrm{Br}_{\alpha'}(U^{[p]}(L),\ A/k))$$

denote the set of isomorphism classes of all $\tilde{\alpha}$-admissible (resp. α-admissible, resp. α'-admissible) objects of I (resp. II, resp. III). We define the structure of a commutative group on each set, and prove that our correspondence induces an isomorphism of groups

$$\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L),\ \mu^A) \cong \mathrm{Ext}_{\alpha}(L,\ A) \cong \mathrm{Br}_{\alpha'}(U^{[p]}(L),\ A/k)\,.$$

The addition on $\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L),\ \mu^A)$ is given by Baer sum. The addition on $\mathrm{Ext}_{\alpha}(L,\ A)$ is given similarly.

Finally, assume α' gives a canonical isomorphism

$$A \# U^{[p]}(L) \cong \mathrm{End}_k(A)\,.$$

We shall prove in a forthcoming paper that $\mathrm{Br}_{\alpha'}(U^{[p]}(L),\ A/k)$ is isomorphic to the Chase-Rosenberg modified Brauer group

$$\hat{\mathrm{Br}}(A/k)$$

in this case. It follows that

$$\mathrm{Ext}_{\alpha}(L,\ A) \cong \hat{\mathrm{Br}}(A/k)\,.$$

Interestingly enough, Yuan [7] has established an isomorphism which seems to have a close relation to the above. He lets $\mathfrak{g}$ be $\mathrm{Der}_k(A)$ and assumes that $A[\mathfrak{g}] = \mathrm{End}_k(A)$. (This condition is weaker than $A \# U^{[p]}(L) \cong \mathrm{End}_k(A)$). He proves that

$$E(\mathrm{Der}_k(A),\ A) \cong \hat{\mathrm{Br}}(A/k)$$

where the left hand side denotes Hochschild's group of regular restricted Lie algebra extensions. I am not so interested in the concept of 'regular restricted Lie algebra'. It is rather complicated, and I do not think it is useful. But it is interesting to note that it follows that

$$\mathrm{Ext}_{\alpha}(L,\ A) \cong E(\mathrm{Der}_k(A),\ A)$$

in case $A \# U^{[p]}(L) \cong \mathrm{End}_k(A)$. Maybe, this will follow directly from $\mathrm{Der}_k(A) \cong A \# L$. The analysis of this matter is left open.

Throughout the paper we fix a commutative ring k, and denote $\otimes_k$ by $\otimes$.

§ 1. Preliminaries.

1.1. Finite group schemes.

Let k be a commutative ring, and let $\mathbf{M}_k$ be the category of commutative k-algebras. A *k-group functor* is a functor of $\mathbf{M}_k$ into the category of groups. We follow the notation of [2] for group functors. k-Group schemes are called k-groups for short. If R is a commutative Hopf k-algebra, $Sp\,R$ denotes the associated affine k-group. If G is an affine k-group, $O(G)$ denotes its affine Hopf algebra.

We follow the notation of [3] or [1] for Hopf algebras. A *finite Hopf k-algebra* means a Hopf k-algebra which is a finitely generated projective k-module. If A is a finite Hopf k-algebra, then $A^*=\mathrm{Hom}_k(A, k)$ is likewise [1, p. 55]. It is called the *dual* of A. Clearly $A \cong A^{**}$ as finite Hopf algebras, and A is *commutative* if and only if A^* is *cocommutative.*

For a Hopf k-algebra H, let

$$G_k(H)=\{g \in H \mid \Delta(g)=g \otimes g,\ \varepsilon(g)=1\}$$

which is a subgroup of units. If $T \in \mathbf{M}_k$, $T \otimes H$ is Hopf T-algebra. The k-group functor $T \mapsto G_T(T \otimes H)$ is denoted by Sp^*H.

Let R be a commutative finite Hopf k-algebra, and let $H=R^*$ be the dual. There is a canonical isomorphism of group functors

$$Sp\,R \cong Sp^*H\,.$$

Indeed, if $T \in \mathbf{M}_k$, the canonical isomorphism

$$\mathrm{Hom}_k(R, T) \cong \mathrm{Hom}_T(T \otimes R, T) \cong T \otimes H$$

induces a group isomorphism

$$\mathbf{M}_k(R, T) \cong G_T(T \otimes H)\,.$$

1.1.1. DEFINITION. A *finite k-group* is an affine k-group G such that the Hopf algebra $O(G)$ is finite. The dual of $O(G)$ is denoted by $O^*(G)$. Thus

$$G \cong Sp\,O(G) \cong Sp^*O^*(G)\,.$$

The functors $G \mapsto O^*(G)$ and $H \mapsto Sp^*H$ give rise to an equivalence between finite k-groups and cocommutative finite Hopf k-algebras.

A sequence of k-group functors

$$1 \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{p} G_3 \longrightarrow 1$$

is an *H-extension* (of G_3 by G_1) [2, II, § 3, 2.1] if $pi=1$ and there is a morphism of k-functors $s: G_3 \to G_2$ such that $ps=Id$ and $G_1 \times G_3 \cong G_2$ by $(x, y) \mapsto i(x)s(y)$. If this is the case, for each $T \in \mathbf{M}_k$,

$$1 \longrightarrow G_1(T) \longrightarrow G_2(T) \longrightarrow G_3(T) \longrightarrow 1$$

is an exact sequence of groups. The converse is true if G_3 is affine. To define general extensions, the reader should know the $fppf$ topology [2, III, § 1]. Fortunately, all extensions which appear in this paper are H-extensions.

The following are easy examples of non H-extensions.

$$0 \longrightarrow {}_p\alpha_k \xrightarrow{\text{incl.}} \alpha_k \xrightarrow{F} \alpha_k \longrightarrow 0 \qquad [2, \text{III}, \S 6, 5.3]$$

$$0 \longrightarrow (\boldsymbol{Z}/p\boldsymbol{Z})_k \longrightarrow \alpha_k \xrightarrow{F\text{-}Id} \alpha_k \longrightarrow 0 \qquad [2, \text{III}, \S 6, 5.4]$$

where k is a field of characteristic $p>0$, and α_k denotes the additive k-group which associates with each T in $\mathbf{M}_k$ the additive group of T, ${}_p\alpha_k$ the subgroup scheme defined by

$${}_p\alpha_k(T) = \{x \text{ in } T \mid x^p = 0\}$$

$(\boldsymbol{Z}/p\boldsymbol{Z})_k$ the constant k-group associated with $\boldsymbol{Z}/p\boldsymbol{Z}$, and F the Frobenius map.

Let H_i be finite cocommutative Hopf k-algebras. A sequence of Hopf algebras

$$H_1 \xrightarrow{f} H_2 \xrightarrow{g} H_3$$

represents an H-extension of finite k-groups

$$1 \longrightarrow Sp^*H_1 \xrightarrow{Sp^*f} Sp^*H_2 \xrightarrow{Sp^*g} Sp^*H_3 \longrightarrow 1$$

if and only if $g(f(x)) = \varepsilon(x)1, \forall x \in H_1$ and there is a k-coalgebra map $h: H_3 \to H_2$ such that $gh=Id$ and $H_1 \otimes H_3 \cong H_2$ by $x \otimes y \mapsto f(x)h(y)$. This follows immediately from the definition.

1.1.2. PROPOSITION. *Let*

$$1 \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{p} G_3 \longrightarrow 1$$

be an H-extension of finite k-groups, and let $H_i = O^*(G_i)$, $f = O^*(i)$, $g = O^*(p)$. There is a canonical isomorphism

$$\xi: H_2 \otimes_{H_1} H_2 \cong H_2 \otimes H_3$$

given by

$$x \otimes y \mapsto \sum_{(y)} x y_{(1)} \otimes g(y_{(2)}).$$

(We are using the sigma notation

$$\Delta(y)=\sum_{(y)} y_{(1)}\otimes y_{(2)}).$$

PROOF. Let $h: H_3\to H_2$ be a coalgebra section to g. We can take h so that $h(1)=1$. Since f and h induce $H_1\otimes H_3\cong H_2$, we have

$$\zeta: H_2\otimes H_3\cong H_2\otimes_{H_1}H_2, \qquad u\otimes v\mapsto u\otimes h(v).$$

The composite $\xi\zeta$ is $u\otimes v\mapsto \sum_{(v)} uh(v_{(1)})\otimes v_{(2)}$. This has the inverse $u\otimes v \mapsto \sum_{(v)} uS(h(v_{(1)}))\otimes v_{(2)}$, where S denotes the antipode of H_2. Hence ξ is bijective. Q. E. D.

This proposition is valid for (general) extensions of finite k-groups. But the fact will not be used.

Let A be a k-algebra. We define a k-group functor $\mathrm{Aut}(A)$ by $\mathrm{Aut}(A)(T)=\mathrm{Aut}_{T\text{-alg}}(T\otimes A)$. It is affine algebraic, if A is a finitely generated projective k-module [**2**, II, §1, 2.6].

Let H be a Hopf k-algebra. We say that a k-linear map

$$\rho: H\to \mathrm{End}_k(A)$$

is a *measuring homomorphism* if i) ρ is a homomorphism of k-algebras (hence A is a left H-module), and ii)

$$x(ab)=\sum_{(x)}(x_{(1)}a)(x_{(2)}b),$$

$$x1=\varepsilon(x)$$

$\forall x\in H$, $\forall a, b\in A$. The pair (A, ρ) is called a left H-module algebra [**3**, §7.2].

Each measuring homomorphism ρ induces a homomorphism of k-group functors

$$\tilde{\rho}: Sp^*H\to \mathrm{Aut}(A)$$

as follows: For each $T\in \mathbf{M}_k$, $T\otimes A$ is a left $T\otimes H$-module T-algebra. Hence the group $G_T(T\otimes H)$ acts on the left on $T\otimes A$ as T-algebra automorphisms. Let $\tilde{\rho}: G_T(T\otimes A)\to \mathrm{Aut}_{T\text{-alg}}(T\otimes A)$ be the corresponding homomorphism of groups.

1.1.3. PROPOSITION. *Let H be a cocommutative finite Hopf k-algebra, and let A be a k-algebra. Each homomorphism of k-group functors $Sp^*H\to \mathrm{Aut}(A)$ is of the form $\tilde{\rho}$ with a uniquely determined measuring homomorphism $\rho: H \to \mathrm{End}_k(A)$.*

PROOF. Let $R=H^*$. The morphism

$$f: Sp\ R\to \mathrm{Aut}(A)$$

corresponds to an element

$$f'\in \mathrm{Aut}_{T\text{-alg}}(R\otimes A)$$

by Yoneda's lemma. We view f' as a k-algebra map

$$f': A \to R \otimes A \cong \mathrm{Hom}_k(H, A).$$

Define a linear map

$$f'': H \to \mathrm{End}_k(A)$$

by $f''(x)(a) = f'(a)(x)$, $\forall x \in H$, $\forall a \in A$. Then f'' is a measuring homomorphism if and only if f is a homomorphism of group functors. Q.E.D.

1.2. p-Lie algebras.

Let k be a commutative ring of prime characteristic p. See [2, II, §7, n°3] for the definition of p-Lie algebras. The p-map of a p-Lie algebra is denoted by $x \mapsto x^{[p]}$.

With each k-group scheme G, a p-Lie k-algebra $\mathrm{Lie}(G)$ is associated as follows: Let $k[\omega] = k[X]/(X^2)$ with ω the image of X, let $q: k[\omega] \to k$ be the k-algebra map defined by $q(\omega) = 0$, and let

$$\mathrm{Lie}(G) = \mathrm{Ker}(G(q): G(k[\omega]) \to G(k)).$$

For each $x \in \mathrm{Lie}(G)$, we write

$$x = 1 + x\omega .$$

$\mathrm{Lie}(G)$ is an abelian group with addition determined by

$$1 + (x + y)\omega = (1 + x\omega)(1 + y\omega)$$

with inverse

$$1 + (-x)\omega = (1 + x\omega)^{-1}$$

and with zero

$$1 + 0\omega = 1 .$$

$\mathrm{Lie}(G)$ is a k-module with scalar multiplication

$$1 + (\lambda x)\omega = 1 + x(\lambda\omega), \qquad \forall x \in \mathrm{Lie}(G), \qquad \forall \lambda \in k,$$

where $1 + x(\lambda\omega)$ means $G(u_\lambda)(x)$ with the k-algebra map $u_\lambda: k[\omega] \to k[\omega]$ determined by $u_\lambda(\omega) = \lambda\omega$. $\mathrm{Lie}(G)$ is a Lie algebra over k with bracket product determined by

$$1 + [x, y]\omega_1\omega_2 = (1 + x\omega_1)(1 + y\omega_2)(1 + x\omega_1)^{-1}(1 + y\omega_2)^{-1} \quad \text{in } G(k[\omega_1, \omega_2])$$

where $k[\omega_1, \omega_2] = k[X, Y]/(X^2, Y^2)$ with ω_1 the image of X and ω_2 the image of Y. Finally the p-map is defined as follows: Let $k[\omega_1, \cdots, \omega_p] = k[X_1, \cdots, X_p]/(X_1^2, \cdots, X_p^2)$ with ω_i the image of X_i, and let

$$\sigma = \omega_1 + \cdots + \omega_p, \qquad \pi = \omega_1 \cdots \omega_p .$$

For each $x \in \mathrm{Lie}(G)$, we have

$$(1+x\omega_1)\cdots(1+x\omega_p)\in G(k[\sigma,\pi])\subset G(k[\omega_1,\cdots,\omega_p]).$$

Let $s: k[\sigma,\pi]\to k[\pi]$ be defined by $s(\sigma)=0$, $s(\pi)=\pi$. There is a unique $x^{[p]}\in \mathrm{Lie}(G)$ with

$$G(s)((1+x\omega_1)\cdots(1+x\omega_p))=1+x^{[p]}\pi.$$

With these operations, Lie(G) is a p-Lie k-algebra [2, II, §7, 3.4]. Also, $G\mapsto \mathrm{Lie}(G)$ is a functor from the category of k-group schemes into the category of p-Lie k-algebras.

To calculate the Lie(G) for a given G, it is enough to find a p-Lie algebra L and a bijection

$$L\cong \mathrm{Ker}\,(G(q): G(k[\omega])\to G(k))$$

$$x\mapsto 1+x\omega$$

which satisfies the above identities.

1.2.1. EXAMPLES. a) Let V be a finitely generated projective k-module. Then

$$GL(V): T\mapsto GL_T(T\otimes V)$$

is an affine algebraic k-group [2, II, §1, 2.4]. If $f\in \mathrm{End}_k(V)$, then $1+\omega\otimes f$: $k[\omega]\otimes V\cong k[\omega]\otimes V$. The map

$$\mathrm{End}_k(V)\to GL(V)(k[\omega]),\qquad f\mapsto 1+\omega\otimes f$$

gives an isomorphism of p-Lie algebras

$$\mathrm{End}_k(V)\cong \mathrm{Lie}\,(GL(V))$$

[2, II, §4, 4.12].

b) Let A be a k-algebra which is a finitely generated projective k-module. Then

$$\mu^A: T\mapsto (\text{the group of units in } T\otimes A)$$

is an affine algebraic k-group [2, II, §1, 2.3]. If $x\in A$, then $1+\omega\otimes x\in \mu^A(k[\omega])$. The map

$$A\to \mu^A(k[\omega]),\qquad x\mapsto 1+\omega\otimes x$$

gives an isomorphism of p-Lie algebras

$$A\cong \mathrm{Lie}\,(\mu^A).$$

c) With the assumption of b), let $\mathrm{Der}_k(A)$ be the p-Lie algebra of all k-algebra derivations of A. Aut(A) is a closed subgroup scheme of $GL(A)$. The isomorphism of a) induces

$$\mathrm{Der}_k(A)\cong \mathrm{Lie}\,(\mathrm{Aut}\,(A)).$$

The following is obvious.

1.2.2. PROPOSITION. *Let*

$$1 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 1$$

be an H-extension of k-group schemes. Then

$$0 \longrightarrow \mathrm{Lie}\,(G_1) \longrightarrow \mathrm{Lie}\,(G_2) \longrightarrow \mathrm{Lie}\,(G_3) \longrightarrow 0$$

is an exact sequence of p-Lie algebras.

For each p-Lie k-algebra L, let $U^{[p]}(L)$ be the restricted universal enveloping k-algebra of L [2, II, §7, 3.6]. It has the structure of a cocommutative Hopf k-algebra determined by

$$\Delta(x)=x\otimes 1+1\otimes x\,, \qquad \forall x\in L\,.$$

We put

$$\mathcal{E}(L)=Sp^*U^{[p]}(L)\,.$$

If L is a finitely generated projective k-module, then $U^{[p]}(L)$ is a finitely generated projective k-module [2, II, §7, 3.7], hence $\mathcal{E}(L)$ is a finite k-group. For each $x\in L$, we have $1+\omega\otimes x\in G_{k[\omega]}(k[\omega]\otimes U^{[p]}(L))$. The map

$$L\rightarrow\mathcal{E}(L)(k[\omega])\,, \qquad x\mapsto 1+\omega\otimes x$$

gives an isomorphism of p-Lie algebras [2, II, §7, 3.9]

$$L\cong\mathrm{Lie}\,(\mathcal{E}(L))\,.$$

1.2.3. THEOREM. *Let*

$$0 \longrightarrow L_1 \longrightarrow L_2 \longrightarrow L_3 \longrightarrow 0$$

be an exact sequence of p-Lie k-algebras which are finitely generated projective k-modules. Then the induced sequence

$$1 \longrightarrow \mathcal{E}(L_1) \longrightarrow \mathcal{E}(L_2) \longrightarrow \mathcal{E}(L_3) \longrightarrow 1$$

is an H-extension.

We shall prove the theorem in the Appendix.

The finite groups $\mathcal{E}(L)$ have the following universal mapping property: Let L be a p-Lie k-algebra which is a finitely generated projective k-module, and let G be a k-group scheme. There is a bijection between homomorphisms of group schemes

$$f:\ \mathcal{E}(L) \longrightarrow G$$

and homomorphisms of p-Lie algebras

$$\phi:\ L \longrightarrow \mathrm{Lie}\,(G)$$

determined by $f \mapsto \phi = \mathrm{Lie}(f)$ [2, II, §7, 3.5].

1.2.4. COROLLARY. *Let L_1 and L_2 be p-Lie algebras which are finitely generated projective k-modules. There is a bijective correspondence between isomorphism classes of H-extensions of finite k-groups*

$$1 \longrightarrow \mathcal{E}(L_1) \longrightarrow G \longrightarrow \mathcal{E}(L_2) \longrightarrow 1$$

and isomorphism classes of extensions of p-Lie algebras

$$0 \longrightarrow L_1 \longrightarrow X \longrightarrow L_2 \longrightarrow 0$$

given by $G \mapsto \mathrm{Lie}(G)$ and $X \mapsto \mathcal{E}(X)$.

This has been proved in [2, III, §6, 8.5] in case k is a field and L_1 is abelian.

PROOF. We have only to show that $G \mapsto \mathrm{Lie}(G)$ and $X \mapsto \mathcal{E}(X)$ are inverses of each other. If G is an H-extension of $\mathcal{E}(L_2)$ by $\mathcal{E}(L_1)$, then $\mathrm{Lie}(G)$ is a finitely generated projective k-module. Hence there is a canonical homomorphism of finite k-groups

$$\mathcal{E}(\mathrm{Lie}(G)) \longrightarrow G\ ,$$

which corresponds to $Id : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$. It is isomorphic by the commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{E}(L_1) \arrow[r] \arrow[d, equal] & G \arrow[r] & \mathcal{E}(L_2) \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & \mathcal{E}(L_1) \arrow[r] & \mathcal{E}(\mathrm{Lie}(G)) \arrow[r] \arrow[u] & \mathcal{E}(L_2) \arrow[r] & 1\ . \end{tikzcd}$$

On the other hand we have $X \cong \mathrm{Lie}(\mathcal{E}(X))$ as extensions of p-Lie algebras.

Q. E. D.

1.2.5. EXAMPLES. Let L be a p-Lie algebra and let A be a k-algebra. Assume L and A are finitely generated projective k-modules.

a) Let $\phi : L \to A$ be a p-Lie map. Extend it to a k-algebra map $\phi' : U^{[p]}(L) \to A$. Since $\mathcal{E}(L)$ is a subgroup functor of $\mu^{U^{[p]}(L)}$, ϕ' induces a homomorphism of k-group schemes

$$\phi'' : \mathcal{E}(L) \subset \mu^{U^{[p]}(L)} \xrightarrow{\phi'} \mu^A\ .$$

We have $\mathrm{Lie}(\phi'') = \phi$.

b) Let $\psi : L \to \mathrm{Der}_k(A)$ be a p-Lie map. Extend it to a k-algebra map $\psi' : U^{[p]}(L) \to \mathrm{End}_k(A)$. It is a measuring homomorphism. Hence it determines a homomorphism of k-group schemes (1.1.3)

$$\tilde{\psi} : \mathcal{E}(L) \to \mathrm{Aut}(A)$$

We have $\mathrm{Lie}(\tilde{\psi}) = \psi$.

1.2.6. NOTATION. Let A be a k-algebra which is a finitely generated projective k-module. We let

$$\pi : U^{[p]}(A) \longrightarrow A$$

denote the k-algebra map such that $\pi | A = Id$, and

$$\Pi : \mathcal{E}(A) \longrightarrow \mu^A$$

denote the homomorphism such that $\mathrm{Lie}(\Pi) = Id$. Π is determined by π as in a) of (1.2.5).

A submodule I of a p-Lie algebra L is an *ideal* if $[L, I] \subset I$ and $x^{[p]} \in I$ for each $x \in I$. Then L/I is a p-Lie algebra.

Let L_1 and L_2 be p-Lie algebras. We make $L_1 \oplus L_2$ into a p-Lie algebra by

$$[(x_1, x_2), (y_1, y_2)] = ([x_1, y_1], [x_2, y_2]),$$

$$(x_1, x_2)^{[p]} = (x_1^{[p]}, x_2^{[p]})$$

$\forall (x_1, x_2), (y_1, y_2) \in L_1 \oplus L_2$. If L is a p-Lie algebra, the set of p-Lie maps

$$L \longrightarrow L_1 \oplus L_2$$

is identified with the set of couples (g_1, g_2) where $g_i : L \to L_i$ are p-Lie maps. On the other hand, the set of p-Lie maps

$$L_1 \oplus L_2 \longrightarrow L$$

is identified with the set of couples (f_1, f_2) where $f_i : L_i \to L$ are p-Lie maps such that $[f_1(L_1), f_2(L_2)] = 0$.

There is a canonical isomorphism of Hopf algebras

$$U^{[p]}(L_1 \oplus L_2) \cong U^{[p]}(L_1) \otimes U^{[p]}(L_2).$$

Hence we have

$$\mathcal{E}(L_1 \oplus L_2) \cong \mathcal{E}(L_1) \times \mathcal{E}(L_2).$$

1.2.7. LEMMA. *If a and b are in a k-algebra,*

$$\sum_{i=0}^{p-1} a^i b a^{p-1-i} = \mathrm{ad}(a)^{p-1}(b)$$

where $\mathrm{ad}(a)(x) = [a, x] = ax - xa$.

This follows by (*) of [2, p. 275].

1.2.8. DEFINITION. Let L be a p-Lie k-algebra. A k-linear map $d : L \to L$ is a *p-derivation* if

$$d[x, y] = [d(x), y] + [x, d(y)],$$

$$d(x^{[p]}) = \mathrm{ad}(x)^{p-1}(d(x))$$

for each $x, y \in L$.

Let $\mathrm{Der}_p(L)$ denote the set of all k-linear p-derivations of the p-Lie algebra L.

If L is a finitely generated projective k-module, the lemma (1.2.7) admits us to identify $\mathrm{Der}_p(L)$ with the submodule of $d \in \mathrm{Der}_k(U^{[p]}(L))$ such that $d(L) \subset L$. In particular, it is a p-Lie algebra. Also, it is easy to check

$$\mathrm{Der}_p(L) \cong \mathrm{Lie}(\mathrm{Aut}(\mathcal{E}(L))).$$

But this will not be used later.

Let L and X be p-Lie algebras, and let

$$\alpha : X \to \mathrm{Der}_p(L)$$

be a p-Lie map. Let $L \times_s X = L \oplus X$. This is a Lie algebra with bracket product

$$[(a, x), (b, y)] = ([a, b] + \alpha(x)(b) - \alpha(y)(a), [x, y])$$

$\forall a, b \in L$, $\forall x, y \in X$. Hence $s_r(u, v)$ is defined for each $0 < r < p$ and $u, v \in L \times_s X$ [**2**, II, §7, 3.1]. $L \times_s X$ is a p-Lie algebra with p-map

$$(a, x)^{[p]} = (a^{[p]} + \sum_{r=1}^{p-1} s_r(a, x), x^{[p]})$$

$\forall a \in L$, $\forall x \in X$. This is called the semi-direct product of L with X.

1.2.9. PROPOSITION. *Let L and X be p-Lie algebras which are finitely generated projective k-modules. Let $\alpha : X \to \mathrm{Der}_p(L)$ be a p-Lie map. Since* $\mathrm{Der}_p(L) \subset \mathrm{Der}_k(U^{[p]}(L))$, *$\alpha$ can be extended to a k-algebra map*

$$\alpha' : U^{[p]}(X) \longrightarrow \mathrm{End}_k(U^{[p]}(L)).$$

This is associated with an action of $\mathcal{E}(X)$ on $\mathcal{E}(L)$ as automorphisms of group schemes. Let $\mathcal{E}(L) \times_s \mathcal{E}(X)$ denote the semidirect product with respect to this action. Then we have

$$\mathcal{E}(L \times_s X) \cong \mathcal{E}(L) \times_s \mathcal{E}(X).$$

PROOF. We start with the canonical split exact sequence of p-Lie algebras

$$0 \longrightarrow L \xrightarrow{i} L \times_s X \underset{j}{\overset{q}{\rightleftarrows}} X \longrightarrow 0$$

where $i(a) = (a, 0)$, $j(x) = (0, x)$, $q(a, x) = x$. This induces a split exact sequence of finite k-groups

$$1 \longrightarrow \mathcal{E}(L) \longrightarrow \mathcal{E}(L \times_s X) \rightleftarrows \mathcal{E}(X) \longrightarrow 1.$$

$\mathcal{E}(L \times_s X)$ acts on $\mathcal{E}(L)$ by inner automorphisms. Hence $\mathcal{E}(X)$ acts on $\mathcal{E}(L)$ as automorphisms through $\mathcal{E}(j): \mathcal{E}(X)\to\mathcal{E}(L\times_s X)$. With respect to this action we have obviously

$$\mathcal{E}(L\times_s X)\cong\mathcal{E}(L)\times_s\mathcal{E}(X).$$

Now, the above extension arises from the following split exact sequence of Hopf algebras

$$U^{[p]}(L)\xrightarrow{i} U^{[p]}(L\times_s X)\underset{j}{\overset{q}{\rightleftarrows}} U^{[p]}(X).$$

The inner action of $\mathcal{E}(L\times_s X)$ on $\mathcal{E}(L)$ corresponds to the following *adjoint action*

$$U^{[p]}(L\times_s X)\otimes U^{[p]}(L)\longrightarrow U^{[p]}(L)$$

$$g\otimes h\longmapsto \sum_{(g)} g_{(1)}hS(g_{(2)})$$

where S denotes the antipode. If we restrict this action on $U^{[p]}(X)\otimes U^{[p]}(L)$, we get α'. Hence the action of $\mathcal{E}(X)$ on $\mathcal{E}(L)$ arises from α'. Q. E. D.

Conversely, any semi-direct product of k-group schemes has a semi-direct product of p-Lie algebras. Let G_1 and G_2 be k-group schemes. Assume G_1 acts on G_2 as automorphisms of group schemes. Then we can make a semi-direct product $G_2\times_s G_1$. Apply the functor Lie$(-)$ to the canonical split exact sequence

$$1\longrightarrow G_2\longrightarrow G_2\times_s G_1\rightleftarrows G_1\longrightarrow 1.$$

Then we obtain

$$0\longrightarrow \mathrm{Lie}\,(G_2)\longrightarrow \mathrm{Lie}\,(G_2\times_s G_1)\rightleftarrows \mathrm{Lie}\,(G_1)\longrightarrow 0.$$

Hence $\mathrm{Lie}\,(G_2\times_s G_1)\cong\mathrm{Lie}\,(G_2)\oplus\mathrm{Lie}\,(G_1)$. It is easy to see that $[\mathrm{Lie}\,(G_2), \mathrm{Lie}\,(G_1)]\subset\mathrm{Lie}\,(G_2)$ and that

$$\mathrm{ad}:\ \mathrm{Lie}\,(G_1)\longrightarrow \mathrm{End}_k\,(\mathrm{Lie}\,(G_2))$$

$$\mathrm{ad}\,(x)(a)=[x,\ a]$$

induces a p-Lie map

$$\mathrm{ad}:\ \mathrm{Lie}\,(G_1)\longrightarrow \mathrm{Der}_p\,(\mathrm{Lie}\,(G_2)).$$

With respect to this map, we have

$$\mathrm{Lie}\,(G_2\times_s G_1)\cong\mathrm{Lie}\,(G_2)\times_s\mathrm{Lie}\,(G_1).$$

1.3. Smooth groups and infinitesimal groups.

Let k be a commutative ring. A locally algebraic k-scheme X is *k-smooth* if for each $T\in\mathbf{M}_k$ and each *nilpotent* ideal I of T, the projection $T\to T/I$ induces a surjection

$$X(T) \longrightarrow X(T/I)$$

[2, I, §4, 4.6]. The following follows immediately from the definition.

1.3.1. PROPOSITION. *If A is a k-algebra which is a finitely generated projective k-module, then μ^A is a k-smooth affine algebraic k-group.*

If H is a Hopf k-algebra, we put

$$H^+ = \mathrm{Ker}\,(\varepsilon : H \longrightarrow k)\,.$$

1.3.2. DEFINITION. A finite k-group G is infinitesimal if $O(G)^+$ is nilpotent (cf. [2, II, §4, 7.1]).

If k is of prime characteristic p and L is a p-Lie algebra which is a finitely generated projective k-module, then $\mathcal{E}(L)$ is infinitesimal. (For the proof, localize k and use the Poincare-Birkhoff-Witt theorem).

1.3.3. PROPOSITION. *Any extension (in the sense of the fppf topology) of an infinitesimal k-group by a smooth k-group scheme is an H-extension.*

PROOF. Let

$$1 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 1$$

be an exact sequence of k-group schemes, where G_3 is infinitesimal and G_1 is smooth. Consider the diagram

$$\begin{tikzcd} \mathrm{Sp}(O(G_3)/O(G_3)^+)\cong e_k \arrow[r, "\eta"] \arrow[d, "\mathrm{cano}"] & G_2 \arrow[d] \\ \mathrm{Sp}\,O(G_3) \arrow[ur, dashed] \arrow[r, phantom, "\cong"] & G_3 \end{tikzcd}$$

where $e_k = Sp\ k$, and η denotes the unit map. Since the projection $G_2 \rightarrow G_3$ is a smooth map, we can apply [2, I, §4, 4.5]. Hence there is a morphism of k-schemes denoted by the broken arrow making the diagram commute. This shows that the extension is an H-extension. Q. E. D.

1.3.4. COROLLARY. *Let k be of prime characteristic p, let L be a p-Lie algebra, and let A be a k-algebra. Assume L and A are finitely generated projective k-modules. Then each extension of $\mathcal{E}(L)$ by μ^A is an H-extension.*

1.4. Split type comodule algebras.

In this section, Let A be a k-algebra which is a finitely generated projective k-module, and let R be a finite commutative Hopf k-algebra with dual $H=R^*$.

Let

$$1 \longrightarrow \mu^A \longrightarrow G \longrightarrow Sp\ R \longrightarrow 1$$

be an H-extension of finite k-groups. A homomorphism

$$\rho: G \longrightarrow \mathrm{Aut}(A)$$

is called *admissible* if 1) $\rho(g)(x)=gxg^{-1}$, $\forall g \in G(T)$, $\forall x \in \mu^A(T)$, 2) $\rho(x)(y)=xyx^{-1}$, $\forall y \in T \otimes A$, $\forall x \in \mu^A(T)$, for each $T \in \mathbf{M}_k$. In this case, we also say that the extension G *acts on* A *admissibly*. By the theorem (3.12) of [**5**], there is a categorical correspondence between H-extensions G of $Sp\ R$ by μ^A which act on A admissibly and the following objects (C, Δ, ε): C is a left A- and a right $R \otimes A$-bimodule over the same k-module.

$$\Delta: C \longrightarrow C \otimes_A C$$

$$\varepsilon: C \longrightarrow A$$

are A-bimodule maps which satisfy the coalgebra condition. The R-action on C satisfies

$$\Delta(cr)=\sum_{(r)} \Delta(c)(r_{(2)} \otimes r_{(1)})$$

$$\varepsilon(cr)=\varepsilon(c)\varepsilon(r)$$

for each $c \in C$, $r \in R$. Finally we have

$$\bar{\Delta}: C \otimes R \cong C \otimes_A C, \qquad c \otimes r \longmapsto \Delta(c)(1 \otimes r),$$

$$C \cong R \otimes A \quad (\text{as right } R \otimes A\text{-modules}).$$

(The last condition corresponds to the fact that the extension is an H-extension).

We shall not use this concept in the following, but use the following dual concept. For each finitely generated projective right A-module M, let

$$D_r(M)=\mathrm{Hom}_{\cdot A}(M, A)$$

which is a finitely generated projective left A-module. The functor D_r gives a duality from finitely generated projective right A-modules onto finitely generated projective left A-modules.

As is well-known [**1**, p. 56] we can identify R-modules with H-comodules.

Thus, under the duality D_r, the above concept (C, Δ, ε) corresponds to the following concept (S, θ, u): S is a k-algebra and a right H-comodule with structure map

$$\theta: S \longrightarrow S \otimes H$$

which is a k-algebra map. Let

$$S^H = \{x \in S \mid \theta(x) = x \otimes 1\}$$

which is a subalgebra. $u: A \to S^H$ is a k-algebra map. We view S as an A-bimodule by multiplication through u. We have

$$\bar{\theta}: S \otimes_A S \cong S \otimes H, \qquad x \otimes y \longmapsto (x \otimes 1)\theta(y),$$

and there is an isomorphism

$$f: S \cong A \otimes H$$

which is a left A-module and a right H-comodule isomorphism.

The objects (S, θ, u) as above are called *right H-comodule A/k-algebras of split type.*

Let S be a split type H-comodule A/k-algebra. For each $T \in \mathbf{M}_k$, $T \otimes S$ is a split type $T \otimes H$-comodule $(T \otimes A)/T$-algebra. For each $g \in G_k(H) = (Sp^*H)(k)$, let

$$S_g = \{x \in S \mid \theta(x) = x \otimes g\} .$$

If $\sigma \in G_T(T \otimes H) = (Sp^*H)(T)$ with $T \in \mathbf{M}_k$, let

$$T \square_\sigma S = (T \otimes S)_\sigma ,$$

which is a $T \otimes A$-bimodule. For each $\sigma, \tau \in (Sp^*H)(T)$, we have

$$(T \square_\sigma S) \otimes_{T \otimes A} (T \square_\tau S) \cong T \square_{\sigma\tau} S$$

by multiplication and u induces

$$T \otimes A \cong T \square_1 S$$

with unit $1 \in (Sp^*H)(T)$. Hence an element of $T \square_\sigma S$ is a unit of $T \otimes S$ if and only if it is a left (equivalently right) $T \otimes A$-basis for $T \square_\sigma S$.

We define a k-group functor E_S. For each $T \in \mathbf{M}_k$, $E_S(T)$ is the set of pairs (x, σ) where $\sigma \in (Sp^*H)(T)$ and $x \in T \square_\sigma S$ which is a unit of $T \otimes S$. This is a group with multiplication $(x, \sigma)(y, \tau) = (xy, \sigma\tau)$, and $E_S: T \mapsto E_S(T)$ is a k-group functor. There is an H-extension

$$1 \longrightarrow \mu^A \xrightarrow{i} E_S \xrightarrow{p} Sp^*H \longrightarrow 1$$

where $i(a) = (u(a), 1)$ and $p(x, \sigma) = \sigma$. E_S acts on A admissibly as follows. If $(x, \sigma) \in E_S(T)$, x is a left $T \otimes A$-basis for $T \square_\sigma S$. Hence there is a unique

$\rho(x, \sigma)(a) \in T \otimes A$ for each $a \in T \otimes A$ such that

$$xa = \rho(x, \sigma)(a)x .$$

Then $\rho: E_S \to \mathrm{Aut}(A)$ is an admissible homomorphism.

The correspondence $S \mapsto E_S$ gives a categorical correspondence from split type H-comodule A/k-algebras onto H-extensions of Sp^*H by μ^A which act on A admissibly. This follows by dualizing the theorem (3.12) of [**5**]. In case k is a field, we have proved this result in [**6**] without assuming that A and H are finitely generated.

1.4.1. LEMMA. *Let*

$$1 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 1$$

be an H-extension of finite k-groups, and let $H_i = O^*(G_i)$. Then H_2 is a split type right H_3-comodule H_1/k-algebra.

PROOF. Let

$$H_1 \xrightarrow{f} H_2 \xrightarrow{g} H_3$$

be the induced Hopf algebra maps. Put

$$\theta: H_2 \xrightarrow{\Delta} H_2 \otimes H_2 \xrightarrow{1 \otimes g} H_2 \otimes H_3 .$$

We claim that (H_2, θ, f) is a split type right H_3-comodule H_1/k-algebra. Indeed the map of (1.1.2)

$$\xi: H_2 \otimes_{H_1} H_2 \cong H_2 \otimes H_3$$

is the same as $\bar{\theta}$, and if $h: H_3 \to H_2$ is a coalgebra section to g, then the isomorphism

$$H_1 \otimes H_3 \cong H_2, \ x \otimes y \longmapsto f(x)h(y)$$

is a left H_1-module map and a right H_3-comodule map.

1.4.2. LEMMA. *Let S be a split type right H-comodule A/k-algebra. Let J be an ideal of A such that*

$$JS = SJ = \tilde{J} .$$

Then $S/\tilde{J}$ is a split type right H-comodule $(A/J)/k$-algebra (with the quotient structure).

The proof is easy, hence omitted.

§ 2. The non-commutative case.

Throughout the rest of the paper, let k be a commutative ring of prime characteristic p, let L be a p-Lie k-algebra, and let A be a k-algebra. We assume L and A are finitely generated projective k-modules.

In this section we consider the case A is not necessarily commutative.

We define three groupoids (categories where all morphisms are isomorphisms) I, II, and III and prove that they are equivalent with one another.

Ob(I) consists of all pairs of an H-extension of finite k-groups

$$1 \longrightarrow \mu^A \longrightarrow G \longrightarrow \mathcal{E}(L) \longrightarrow 1$$

together with an admissible homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}(A).$$

Let $(G_1, \rho_1), (G_2, \rho_2) \in \mathrm{Ob(I)}$. A morphism : $(G_1, \rho_1) \rightarrow (G_2, \rho_2)$ is a homomorphism $f: G_1 \rightarrow G_2$ making the diagrams

$$\begin{tikzcd}
1 \arrow[r] & \mu^A \arrow[r] \arrow[d, equal] & G_1 \arrow[r] \arrow[d, "f"] & \mathcal{E}(L) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mu^A \arrow[r] & G_2 \arrow[r] & \mathcal{E}(L) \arrow[r] & 1
\end{tikzcd}$$

$$\begin{tikzcd}
G_1 \arrow[dr, "\rho_1"] \arrow[dd, "f"'] & \\
& \mathrm{Aut}(A) \\
G_2 \arrow[ur, "\rho_2"'] &
\end{tikzcd}$$

commute. The morphism f is necessarily isomorphic. Hence the category I is a groupoid.

Ob(II) consists of all extensions of p-Lie algebras

$$0 \longrightarrow A \longrightarrow X \longrightarrow L \longrightarrow 0$$

such that for each $x \in X$, $\mathrm{ad}(x): A \rightarrow A$, $a \mapsto [x, a]$ is a k-algebra derivation. We denote the p-Lie map $x \mapsto \mathrm{ad}(x)$ by

$$\mathrm{ad}: X \longrightarrow \mathrm{Der}_k(A).$$

Let $X_1, X_2 \in \mathrm{Ob(II)}$. A morphism : $X_1 \rightarrow X_2$ is a homomorphism of p-Lie algebras $g: X_1 \rightarrow X_2$ making the diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & X_1 \arrow[r] \arrow[d, "g"] & L \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r] & X_2 \arrow[r] & L \arrow[r] & 0
\end{tikzcd}$$

commute. The map g is also necessarily isomorphic, hence the category II is a groupoid.

Ob(III) consists of all split type $U^{[p]}(L)$-comodule A/k-algebras. Let S_1, $S_2 \in \mathrm{Ob}(\mathrm{III})$. A morphism: $S_1 \to S_2$ is a k-algebra map $h: S_1 \to S_2$ which is a $U^{[p]}(L)$-comodule map and an A-bimodule map. We claim that the category III is a groupoid. Indeed, the comodule structure maps $\theta_i: S_i \to S_i \otimes U^{[p]}(L)$ induce isomorphisms (cf. [6, p. 1464])

$$\bar{\bar{\theta}}_i: S_i \otimes_A S_i \cong S_i \otimes U^{[p]}(L), \ x \otimes y \longmapsto \theta_i(x)(y \otimes 1).$$

Since $\bar{\bar{\theta}}_1$ is right S_1-linear, applying $? \otimes_{S_1} S_2$, we get a commutative diagram

$$\begin{tikzcd} S_1 \otimes_A S_2 \arrow[r, "\bar{\bar{\theta}}_1", "\cong"'] \arrow[d, "h \otimes 1"] & S_2 \otimes U^{[p]}(L) \arrow[d, equal] \\ S_2 \otimes_A S_2 \arrow[r, "\bar{\bar{\theta}}_2", "\cong"'] & S_2 \otimes U^{[p]}(L) \end{tikzcd}$$

which proves that h is an isomorphism, since S_2 ($\cong A \otimes U^{[p]}(L)$) is a left A-progenerator.

We shall define equivalences of groupoids

$$\begin{tikzcd} & \mathrm{I} \arrow[dl, shift right, "(2.2)"'] & \\ \mathrm{II} \arrow[ur, shift right, "(2.4)"'] \arrow[rr, shift right, "(2.3)"'] & & \mathrm{III} \arrow[ul, "(2.1)"'] \arrow[ll, shift right, "(2.5)"'] \end{tikzcd}$$

and the following natural isomorphisms

$$(2.1) \circ (2.3) \cong (2.4),$$

$$(2.2) \circ (2.1) \cong (2.5),$$

$$(2.2) \circ (2.4) \cong (Id \text{ of II}), \qquad (2.4) \circ (2.2) \cong (Id \text{ of I}),$$

$$(2.3) \circ (2.5) \cong (Id \text{ of III}), \qquad (2.5) \circ (2.3) \cong (Id \text{ of II}).$$

2.1. III→I.

If $S \in \mathrm{Ob}(\mathrm{III})$, then $E_S \in \mathrm{Ob}(\mathrm{I})$, together with the canonical action on A. This induces a functor III→I. It follows from the theory of [5][6] that this is an equivalence.

2.2. I→II.

Let $1 \to \mu^A \to G \to \mathcal{E}(L) \to 1$ be an H-extension which acts admissibly on A. Apply the functor Lie(−). Since $A = \mathrm{Lie}(\mu^A)$ and $L = \mathrm{Lie}(\mathcal{E}(L))$, we have an extension of p-Lie algebras

$$0 \longrightarrow A \longrightarrow \mathrm{Lie}(G) \longrightarrow L \longrightarrow 0 .$$

We claim that this is an object of II. Since the homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}(A)$$

induces a p-Lie homomorphism

$$\mathrm{Lie}(\rho) : \mathrm{Lie}(G) \longrightarrow \mathrm{Der}_k(A) ,$$

we have only to prove that $\mathrm{Lie}(\rho)=\mathrm{ad}$.

Let $x \in \mathrm{Lie}(G)$ and $a \in A$. We have

$$\rho(1+\omega x)(a)=a+\omega \,\mathrm{Lie}(\rho)(x)(a)$$

in $k[\omega]\otimes A$, by definition. On the other hand, in $G(k[\omega_1, \omega_2])$, we have

$$\begin{aligned} 1+\omega_1\omega_2[x, a] &= (1+\omega_1 x)(1+\omega_2 a)(1-\omega_1 x)(1-\omega_2 a) \\ &= \{\rho(1+\omega_1 x)(1+\omega_2 a)\}(1-\omega_2 a) \\ &= \{1+\omega_2 a+\omega_1\omega_2 \,\mathrm{Lie}(\rho)(x)(a)\}(1-\omega_2 a) \\ &= 1+\omega_1\omega_2 \,\mathrm{Lie}(\rho)(x)(a) . \end{aligned}$$

Hence $[x, a]=\mathrm{Lie}(\rho)(x)(a)$.

The correspondence $G \mapsto \mathrm{Lie}(G)$ gives rise to a functor I→II in an obvious way.

2.3. II→III.

Let $X \in \mathrm{Ob}(\mathrm{II})$. The p-Lie algebra map

$$\mathrm{ad} : X \longrightarrow \mathrm{Der}_k(A)$$

induces a measuring homomorphism

$$\mathrm{ad}' : U^{[p]}(X) \longrightarrow \mathrm{End}_k(A) ,$$

through which we view A as a left $U^{[p]}(X)$-module algebra. On the other hand, $U^{[p]}(A)$ is a normal sub-Hopf algebra of $U^{[p]}(X)$, correspondingly to the fact that $\mathcal{E}(A)$ is a normal subgroup functor of $\mathcal{E}(X)$. This means that $U^{[p]}(A)$ is stable under the following adjoint action

$$\begin{aligned} U^{[p]}(X)\otimes U^{[p]}(A) &\longrightarrow U^{[p]}(A) \\ x\otimes y &\longmapsto \sum_{(x)} x_{(1)}\, y S(x_{(2)}) \end{aligned}$$

where S denotes the antipode of $U^{[p]}(X)$. We also view $U^{[p]}(A)$ as a left $U^{[p]}(X)$-module by this action.

2.3.1. LEMMA. *The map* $\pi : U^{[p]}(A) \to A$ (1.2.6) *is left* $U^{[p]}(X)$*-linear.*

Indeed, the map π is left X-linear, by definition.

Since the p-Lie extension

$$0 \longrightarrow A \longrightarrow X \longrightarrow L \longrightarrow 0$$

induces an H-extension (1.2.3)

$$1 \longrightarrow \mathcal{E}(A) \longrightarrow \mathcal{E}(X) \longrightarrow \mathcal{E}(L) \longrightarrow 1\,,$$

it follows by (1.4.1), that $U^{[p]}(X)$ has the structure of a split type right $U^{[p]}(L)$-comodule $U^{[p]}(A)/k$-algebra.

Let $J=\mathrm{Ker}\,(\pi)$. Since $[X, J]\subset J$, we have

$$JU^{[p]}(X)=U^{[p]}(X)J=\tilde{J}\,.$$

Hence

$$B(X)=U^{[p]}(X)/\tilde{J}$$

has the quotient structure of a split type right $U^{[p]}(L)$-comodule A/k-algebra, by (1.4.2). Thus $B(X)$ is an object of III.

If $g: X_1\rightarrow X_2$ is a morphism of II, the induced algebra map $g': U^{[p]}(X_1)\rightarrow U^{[p]}(X_2)$ is a map of right $U^{[p]}(L)$-comodule $U^{[p]}(A)/k$-algebras. Hence it induces a map of III $g'': B(X_1)\rightarrow B(X_2)$. Thus $X\mapsto B(X)$ is a functor II$\rightarrow$III.

2.4. II$\rightarrow$I.

Let $0\rightarrow A\rightarrow X\rightarrow L\rightarrow 0$ be an object of II. This induces an H-extension

$$1 \longrightarrow \mathcal{E}(A) \longrightarrow \mathcal{E}(X) \longrightarrow \mathcal{E}(L) \longrightarrow 1\,.$$

The adjoint action of $U^{[p]}(X)$ on $U^{[p]}(A)$ (2.3) induces the inner action

$$\mathcal{E}(X)\times\mathcal{E}(A) \longrightarrow \mathcal{E}(A), \quad (x, a) \longmapsto xax^{-1}$$

as follows: For each $T\in\mathbf{M}_k$, $T\otimes U^{[p]}(A)$ is a left $T\otimes U^{[p]}(X)$-module (with the adjoint action). Hence the group $G_T(T\otimes U^{[p]}(X))=\mathcal{E}(X)(T)$ acts on $T\otimes U^{[p]}(A)$. The group turns out to act as T-Hopf algebra automorphisms. Hence $G_T(T\otimes U^{[p]}(X))$ acts on $G_T(T\otimes U^{[p]}(A))$ as group automorphisms. The inner action of $\mathcal{E}(X)(T)$ on $\mathcal{E}(A)(T)$ is this.

Let

$$\mathrm{Ad}: \mathcal{E}(X) \longrightarrow \mathrm{Aut}\,(A)$$

be the homomorphism corresponding to

$$\mathrm{Lie}\,(\mathrm{Ad})=\mathrm{ad}: X \longrightarrow \mathrm{Der}_k(A)\,.$$

We know (1.2.5) how to construct Ad from the measuring homomorphism

$$\mathrm{ad}': U^{[p]}(X) \longrightarrow \mathrm{End}_k(A)\,.$$

We let $\mathcal{E}(X)$ act on μ^A by

$$\mathcal{E}(X)\times\mu^A \longrightarrow \mu^A, \quad (x, g) \longmapsto \mathrm{Ad}\,(x)(g)\,.$$

The following lemma follows immediately from (2.3.1).

2.4.1. LEMMA. *The homomorphism* $\Pi : \mathcal{E}(A) \to \mu^A$ (1.2.6) *commutes with the* $\mathcal{E}(X)$*-actions.*

2.4.2. LEMMA. *For each* $x \in \mathcal{E}(A)(T)$ *and* $a \in T \otimes A$ *with* $T \in \mathbf{M}_k$, *we have*

$$\mathrm{Ad}\,(x)(a) = \Pi(x) a \Pi(x)^{-1}.$$

PROOF. We compare the following two homomorphisms

$$\mathcal{E}(A) \xrightarrow{\Pi} \mu^A \xrightarrow{\text{inn}} \mathrm{Aut}\,(A)$$

$$\mathcal{E}(A) \xrightarrow{\quad\mathrm{Ad}\quad} \mathrm{Aut}\,(A)$$

where inn denotes the inner action $\mathrm{inn}\,(g)(a) = gag^{-1}$, $\forall g \in \mu^A(T)$, $\forall a \in T \otimes A$. To see that they coincide, we have only to apply the functor Lie (—). Then we get

$$A \xrightarrow{Id} A \xrightarrow{\mathrm{Lie(inn)}} \mathrm{Der}_k(A)$$

$$A \xrightarrow{\quad\mathrm{ad}\quad} \mathrm{Der}_k(A).$$

Since Lie (inn) = ad, the claim follows. Q. E. D.

Let

$$\mu^A \times_s \mathcal{E}(X)$$

be the semidirect product of μ^A with $\mathcal{E}(X)$ with respect to the action of $\mathcal{E}(X)$ on μ^A. Thus the product is given by

$$(a, x)(b, y) = (a\,\mathrm{Ad}\,(x)(b), xy), \quad \forall a, b \in \mu^A(T), \ \forall x, y \in \mathcal{E}(X)(T),$$

for each $T \in \mathbf{M}_k$. There is a homomorphism

$$\rho : \mu^A \times_s \mathcal{E}(X) \longrightarrow \mathrm{Aut}\,(A)$$

given by

$$\rho(a, x)(b) = a\,\mathrm{Ad}\,(x)(b) a^{-1},$$

$\forall (a, x) \in (\mu^A \times_s \mathcal{E}(X))(T)$, $\forall b \in T \otimes A$, $\forall T \in \mathbf{M}_k$. We define a morphism

$$\Phi : \mathcal{E}(A) \longrightarrow \mu^A \times_s \mathcal{E}(X)$$

$$\Phi(z) = (\Pi(z^{-1}), z), \ \forall z \in \mathcal{E}(A)(T), \ \forall T \in \mathbf{M}_k.$$

2.4.3. LEMMA. Φ *is a homomorphism of k-group functors,*

$$(a, x)\Phi(z)(a, x)^{-1} = \Phi(xzx^{-1}),$$

for each $(a, x) \in (\mu^A \times_s \mathcal{E}(X))(T)$, $z \in \mathcal{E}(A)(T)$ *with* $T \in \mathbf{M}_k$, *the composite*

$$\mathcal{E}(A) \xrightarrow{\Phi} \mu^A \times_s \mathcal{E}(X) \xrightarrow{\rho} \mathrm{Aut}\,(A)$$

is trivial, and $\mathrm{Im}(\Phi)$ *is a normal subgroup functor of* $\mu^A \times_s \mathcal{E}(X)$.

This follows directly from (2.4.1) and (2.4.2).

Since $\mathcal{E}(A)$ and $\mu^A \times_s \mathcal{E}(X)$ are *k-group sheaves* with respect to the *fppf* topology, we can form a quotient k-group sheaf [**2**, II, § 3, 3.1]

$$\mathcal{B}(X) = (\mu^A \times_s \mathcal{E}(X)) \tilde{/} \mathrm{Im}(\Phi).$$

The homomorphism ρ induces a homomorphism

$$\rho : \mathcal{B}(X) \longrightarrow \mathrm{Aut}(A).$$

Consider the canonical exact sequence

$$1 \longrightarrow \mu^A \xrightarrow{j} \mu^A \times_s \mathcal{E}(X) \xrightarrow{q} \mathcal{E}(X) \longrightarrow 1$$

where $j(a) = (a, 1)$, $q(a, x) = x$. Since

$$\mathrm{Im}(j) \cap \mathrm{Im}(\Phi) = e_k$$

and $\mathcal{E}(A) = \mathrm{Im}(q\Phi)$, it follows that j and q induce an exact sequence (in the sense of the *fppf* topology)

$$1 \longrightarrow \mu^A \xrightarrow{j} \mathcal{B}(X) \xrightarrow{q} \mathcal{E}(L) \longrightarrow 1.$$

There is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{E}(A) & \longrightarrow & \mathcal{E}(X) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\ & & \downarrow \Pi & & \downarrow \Theta & & \| & & \\ 1 & \longrightarrow & \mu^A & \xrightarrow{j} & \mathcal{B}(X) & \xrightarrow{q} & \mathcal{E}(L) & \longrightarrow & 1 \end{array}$$

where Θ is the composite of $\mathcal{E}(X) \to \mu^A \times_s \mathcal{E}(X)$, $x \mapsto (1, x)$ with the projection $\mu^A \times_s \mathcal{E}(X) \to \mathcal{B}(X)$. The homomorphisms j and Θ commute with the action on A (μ^A acting on A by inner automorphisms).

2.4.4. LEMMA. *($\mathcal{B}(X)$, ρ) is an object of* I.

PROOF. By (1.3.4), $\mathcal{B}(X)$ is an H-extension of $\mathcal{E}(L)$ by μ^A. If $(a, x) \in (\mu^A \times_s \mathcal{E}(X))(T)$ and $b \in \mu^A(T)$, we have

$$\begin{aligned} (a, x)(b, 1)(a, x)^{-1} &= (a\, \mathrm{Ad}(x)(b) x^{-1}, 1) \\ &= (\rho(a, x)(b), 1) \end{aligned}$$

in $(\mu^A \times_s \mathcal{E}(X))(T)$. Hence ρ is admissible. Q. E. D.

The correspondence $X \mapsto \mathcal{B}(X)$ defines a functor II $\to$ I. If $g : X_1 \to X_2$ is a morphism in II,

$$(1, \mathcal{E}(g)) : \mu^A \times_s \mathcal{E}(X_1) \longrightarrow \mu^A \times_s \mathcal{E}(X_2)$$

is a homomorphism which induces a morphism $\mathcal{B}(X_1) \to \mathcal{B}(X_2)$ in I.

2.5. III$\rightarrow$II.

Let S be a split type $U^{[p]}(L)$-comodule A/k-algebra. Let $\mathfrak{a}$ be the kernel of the unit map $k\rightarrow A$. (We are not assuming A is a faithful k-algebra). Thus $k/\mathfrak{a}\subset A$, hence $k/\mathfrak{a}\otimes L\subset A\otimes U^{[p]}(L)$, since $U^{[p]}(L)/L$ is a projective k-module. Put

$$\omega(S)=\{x\in S \mid \theta(x)-x\otimes 1\in k/\mathfrak{a}\otimes L\}$$

which is a p-Lie subalgebra of S. $\mathfrak{a}L$ is an ideal of L, hence $L/\mathfrak{a}L$ is a p-Lie k-algebra.

2.5.1. LEMMA. *There is an exact sequence of p-Lie algebras*

$$0\longrightarrow A\xrightarrow{u}\omega(S)\xrightarrow{\gamma}L/\mathfrak{a}L\longrightarrow 0$$

where u denotes the map induced from the structure map $u: A\rightarrow S$, and γ is given by $\gamma(x)=\theta(x)-x\otimes 1\in(k/\mathfrak{a})\otimes L$.

PROOF. Since

$$u:\ A\cong\{x\in S \mid \theta(x)=x\otimes 1\}$$

we have only to prove that γ is surjective. Let

$$h:\ A\otimes U^{[p]}(L)\cong S$$

be an isomorphism of left A-modules and right $U^{[p]}(L)$-comodules. We can assume $h(1\otimes 1)=1$. Then $h(k/\mathfrak{a}\otimes L)\subset\omega(S)$, and $h: k/\mathfrak{a}\otimes L\rightarrow\omega(S)$ is a section to γ. Q.E.D.

Let

$$\begin{array}{ccc}\Omega(S) & \longrightarrow & (L)\\ \downarrow & & \downarrow\\ \omega(S) & \xrightarrow{\gamma} & L/\mathfrak{a}L\end{array}$$

be the fibre product of p-Lie algebras. Thus, $\Omega(S)$ is the p-Lie subalgebra of $\omega(S)\oplus L$ consisting of all (x, l) with $\gamma(x)=\bar{l}$ (the class of l). Then we have an extension of p-Lie algebras

$$0\longrightarrow A\xrightarrow{\bar{u}}\Omega(S)\longrightarrow L\longrightarrow 0$$

where $\bar{u}(a)=(u(a), 0)$. Since

$$[(x, l), (u(a), 0)]=([x, u(a)], 0)$$

for each $(x, l)\in\Omega(S)$ and $a\in A$, and

$$[x, ?]:\ u(A)\longrightarrow u(A)$$

is a k-algebra derivation for each $x\in\omega(S)$, it follows that $\Omega(S)$ is an object of II.

The correspondence $S\mapsto\Omega(S)$ is obviously a functor III$\rightarrow$II.

2.6. Natural isomorphisms

We define the isomorphisms of functors above (2.1). This will prove that each functor is an equivalence.

2.6.1. $(2.1)\circ(2.3)\cong(2.4)$.

Let $X\in \mathrm{Ob}(\mathrm{II})$. Let

$$q: U^{[p]}(X) \longrightarrow B(X)$$

$$r: U^{[p]}(X) \longrightarrow U^{[p]}(L)$$

be the canonical projections. Since q is a $U^{[p]}(L)$-comodule map, if $\sigma\in G_T(T\otimes U^{[p]}(X))$, with $T\in \mathbf{M}_k$, and $\bar{\sigma}=(I\otimes r)(\sigma)\in G_T(T\otimes U^{[p]}(L))$, then

$$(I\otimes q)(\sigma)\in(T \square_{\bar{\sigma}} B(X))\cap\mu^{B(X)}(T).$$

If we put $\Psi(\sigma)=((I\otimes q)(\sigma),\ \sigma)\in E_{B(X)}(T)$,

$$\Psi:\ \mathcal{E}(X) \longrightarrow E_{B(X)}$$

is a homomorphism of k-group functors, and we have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{E}(A) & \longrightarrow & \mathcal{E}(X) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \Pi} & & \downarrow{\scriptstyle \Psi} & & \| & & \\
1 & \longrightarrow & \mu^{A} & \longrightarrow & E_{B(X)} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1,
\end{array}$$

where the first row is induced from $0\to A\to X\to L\to 0$. We claim that Ψ commutes with the action on A. Indeed, if $\sigma\in G_T(T\otimes U^{[p]}(X))$ and $a\in T\otimes U^{[p]}(A)$, we have

$$\sigma a=\sigma(a)\sigma \qquad \text{in } T\otimes U^{[p]}(X)$$

where $\sigma(a)$ means the adjoint action of $U^{[p]}(X)$ on $U^{[p]}(A)$. Applying $I\otimes q$, we get

$$(I\otimes q)(\sigma)(I\otimes\pi)(a)=(I\otimes\pi)(\sigma(a))(I\otimes q)(\sigma)$$

where

$$(I\otimes\pi)(\sigma(a))=\sigma(I\otimes\pi)(a)$$

by (2.3.1). Since π is surjective, this means that Ψ commutes with the action on A.

It follows that the morphism

$$\Gamma:\ \mu^{A}\times_{s}\mathcal{E}(X) \longrightarrow E_{B(X)},\ \Gamma(a,\ x)=a\Psi(x)$$

is a homomorphism of *k-group sheaves*, which commutes with the operation on A. Since $\Gamma\Phi=1$, Γ induces a homomorphism

$$\tilde{\Gamma}:\ \mathcal{B}(X) \longrightarrow E_{B(X)}$$

which also commutes with the operation on A, and we have a commutative diagram of extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu^A & \longrightarrow & \mathcal{B}(X) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\ & & \| & & \downarrow \tilde{\Gamma} & & \| & & \\ 1 & \longrightarrow & \mu^A & \longrightarrow & E_{B(X)} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1\,. \end{array}$$

It is easy to prove that $\tilde{\Gamma}$ is natural with respect to $X \in \mathrm{Ob}(\mathrm{II})$. Thus $\tilde{\Gamma}$ gives rise to an isomorphism of functors

$$(2.1)\circ(2.3) \cong (2.4)\,.$$

2.6.2. $(2.2)\circ(2.4) \cong (Id \text{ of } \mathrm{II})$, $(2.4)\circ(2.2) \cong (Id \text{ of } \mathrm{I})$.

Let $X \in \mathrm{Ob}(\mathrm{II})$. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{E}(A) & \longrightarrow & \mathcal{E}(X) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\ & & \downarrow \Pi & & \downarrow \Theta & & \| & & \\ 1 & \longrightarrow & \mu^A & \longrightarrow & \mathcal{B}(X) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1\,. \end{array}$$

Since $\mathrm{Lie}\,(\Pi) = Id\colon A \to A$, it follows that

$$\mathrm{Lie}\,(\Theta)\colon X \longrightarrow \mathrm{Lie}\,(\mathcal{B}(X))$$

is a morphism of II.

Let $G \in \mathrm{Ob}\,(\mathrm{I})$. $\mathrm{Lie}\,(G)$ is a finitely generated projective k-module, since $\mathrm{Lie}\,(G) \in \mathrm{Ob}\,(\mathrm{II})$. Let

$$\Xi : \mathcal{E}(\mathrm{Lie}\,(G)) \longrightarrow G$$

be the homomorphism corresponding to

$$\mathrm{Lie}\,(\Xi) = Id\colon \mathrm{Lie}\,(G) \longrightarrow \mathrm{Lie}\,(G)\,.$$

It is easy to see that Ξ commutes with the operation on A. ($\mathcal{E}(\mathrm{Lie}\,(G))$ acts on A, since $\mathrm{Lie}\,(G) \in \mathrm{Ob}\,(\mathrm{II})$). Moreover, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{E}(A) & \longrightarrow & \mathcal{E}(\mathrm{Lie}\,(G)) & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\ & & \downarrow \Pi & & \downarrow \Xi & & \| & & \\ 1 & \longrightarrow & \mu^A & \longrightarrow & G & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1\,. \end{array}$$

Just as (2.6.1), this induces an isomorphism in I

$$\mathcal{B}(\mathrm{Lie}\,(G)) \xrightarrow{\sim} G\,.$$

The above are functorial, and we have the required isomorphisms of functors.

2.6.3. $(2.5)\circ(2.3) \cong (Id \text{ of } \mathrm{II})$, $(2.3)\circ(2.5) \cong (Id \text{ of } \mathrm{III})$.

Let $X \in \mathrm{Ob}(\mathrm{II})$. The projection $q\colon U^{[p]}(X) \to B(X)$ induces a p-Lie map $q\colon X \to \omega(B(X))$ which makes the following diagram commute.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & X & \longrightarrow & L & \longrightarrow & 0 \\ & & \| & & \downarrow q & & \downarrow \mathrm{cano} & & \\ 0 & \longrightarrow & A & \longrightarrow & \omega(B(X)) & \longrightarrow & L/\mathfrak{a}L & \longrightarrow & 0\,. \end{array}$$

Hence there is an isomorphism of II

$$X \cong \Omega(B(X)).$$

Let $S \in \mathrm{Ob}(\mathrm{III})$. The projection $\Omega(S) \to \omega(S)$ composed with the inclusion $\omega(S) \hookrightarrow S$ is extended to a k-algebra map $U^{[p]}(\Omega(S)) \to S$ which is seen to be a map of III.

The above maps, which are functorial, give the required natural isomorphisms.

2.6.4. $(2.2)\circ(2.1) \cong (2.5)$.

Let $S \in \mathrm{Ob}(\mathrm{III})$, and let $(x, l) \in \Omega(S)$. Thus $x \in S$ and $l \in L$ which satisfy

$$\theta(x) = x \otimes 1 + 1 \otimes l \qquad \text{in } S \otimes U^{[p]}(L).$$

Let $k[\omega] = k[X]/(X^2)$. Then we have

$$1 + \omega \otimes x \in (k[\omega] \square_{1+\omega\otimes l} S) \cap \mu^S(k[\omega]).$$

The map

$$(x, l) \longmapsto 1 + \omega \otimes x, \qquad \Omega(S) \longrightarrow \mathrm{Lie}(E_S)$$

is a p-Lie map which makes the following diagram commute.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \Omega(S) & \longrightarrow & L & \longrightarrow & 0 \\ & & \wr\| & & \downarrow & & \wr\| & & \\ 0 & \longrightarrow & \mathrm{Lie}(\mu^A) & \longrightarrow & \mathrm{Lie}(E_S) & \longrightarrow & \mathrm{Lie}(\mathcal{E}(L)) & \longrightarrow & 0. \end{array}$$

Since this is natural in S, we have the required isomorphism.

§ 3. The commutative case.

Let k, L, and A be as in § 2. We assume A is commutative, throughout the section.

3.1. PROPOSITION. (a) *Let $(G, \rho) \in \mathrm{Ob}(\mathrm{I})$. The homomorphism*

$$\rho : G \longrightarrow \mathrm{Aut}(A)$$

factors through the projection $G \to \mathcal{E}(L)$.

(b) *Let $X \in \mathrm{Ob}(\mathrm{II})$. The p-Lie map*

$$\mathrm{ad} : X \longrightarrow \mathrm{Der}_k(A)$$

factors through the projection $X \to L$.

(c) *Let $S \in \mathrm{Ob}(\mathrm{III})$. There is a unique structure of a left $U^{[p]}(L)$-module algebra on A such that*

$$xa = \sum_{(x)} (x_{(1)} \cdot a) x_{(0)}, \ \forall x \in S, \ \forall a \in A,$$

where $\theta(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$.

PROOF. (a) and (b) are obvious, since $\rho|\mu^A$ and $\mathrm{ad}|A$ are trivial. (c) Let $H=U^{[p]}(L)$ and $R=H^*$. We can view S as a left $A\otimes R$- and right A-bimodule. Since S is a rank 1 free left $A\otimes R$-module and A is commutative, we have

$$A\otimes R\cong \mathrm{End}_{A\otimes R^-}(S)$$

by left multiplication. Hence there is a unique k-linear map $\gamma: A\to A\otimes R$ such that

$$xa=\gamma(a)x,\ \forall x\in S,\ \forall a\in A.$$

We define a left H-operation on A by the condition that

$$g\cdot a=\sum_{(a)}\langle g,\ a_{(1)}\rangle a_{(0)},\ \forall g\in H,\ \forall a\in A,$$

where $\gamma(a)=\sum_{(a)} a_{(0)}\otimes a_{(1)}$. Then

$$\sum_{(x)}(x_{(1)}\cdot a)x_{(0)}=\sum_{(x,a)}\langle x_{(1)},\ a_{(1)}\rangle a_{(0)}x_{(0)}$$

$$=(\sum_{(a)} a_{(1)}\otimes a_{(0)})x=xa,$$

for each $x\in S$, $a\in A$. Conversely, each such operation determines a linear map γ as above, since

$$A\otimes R\cong \mathrm{Hom}_k(H,\ A).$$

To prove that this makes A into a left H-module algebra, it is enough to show that γ is a k-algebra map and the structure of a right R-comodule. It is clear that γ is an algebra map. To prove that γ is the structure of a right R-comodule, consider the canonical isomorphism

$$\bar\theta:\ S\otimes_A S\cong S\otimes H$$
$$\bar\theta(x\otimes y)=\sum_{(y)} xy_{(0)}\otimes y_{(1)}$$

which is A-bilinear and *semicolinear* over the coalgebra isomorphism

$$H\otimes H\cong H\otimes H,\ g\otimes h\longmapsto \sum_{(h)} gh_{(1)}\otimes h_{(2)}.$$

This means that $\bar\theta^{-1}$ is *semilinear* over the dual algebra isomorphism

$$R\otimes R\cong R\otimes R,\ u\otimes v\longmapsto \sum_{(u)} u_{(1)}\otimes u_{(2)}v.$$

For $z\otimes h\in S\otimes H$ and $a\in A$, we have

$$(z\otimes h)a=za\otimes h$$
$$=\gamma(a)z\otimes h=(\gamma(a)\otimes 1)(z\otimes h),$$

hence, in $S\otimes_A S$, we have

$$\bar{\theta}^{-1}(z\otimes h)a=\sum_{(a)}(a_{(0)}\otimes\Delta(a_{(1)}))\bar{\theta}^{-1}(z\otimes h).$$

On the other hand, for $x\otimes y\in S\otimes_A S$ and $a\in A$, we have

$$\begin{aligned}(x\otimes y)a=x\otimes\gamma(a)y&=\sum_{(a)}xa_{(0)}\otimes a_{(1)}y\\&=\sum_{(a)}(\gamma(a_{(0)})\otimes a_{(1)})(x\otimes y).\end{aligned}$$

Comparing the two identities, we conclude that

$$\sum_{(a)}a_{(0)}\otimes\Delta(a_{(1)})=\sum_{(a)}\gamma(a_{(0)})\otimes a_{(1)},\ \forall a\in A.$$

Letting $x\in A$ in $xa=\gamma(a)x$, we have

$$\sum_{(a)}\varepsilon(a_{(1)})a_{(0)}=a,\ \forall a\in A.$$

Hence A is a right R-comodule. Q.E.D.

Throughout the rest of the paper, we fix a p-Lie map

$$\alpha:\ L\longrightarrow \mathrm{Der}_k(A).$$

Let

$$\alpha':\ U^{[p]}(L)\longrightarrow \mathrm{End}_k(A)$$

be the corresponding measuring homomorphism. We view A as a left $U^{[p]}(L)$-module algebra through α'. Let

$$\tilde{\alpha}:\ \mathcal{E}(L)\longrightarrow \mathrm{Aut}\,(A)$$

be the homomorphism of k-group schemes such that

$$\mathrm{Lie}\,(\tilde{\alpha})=\alpha.$$

We fix these notations.

3.2. DEFINITION. (a) An object (G,ρ) of I is *$\tilde{\alpha}$-admissible* if

$$\rho:\ G\xrightarrow{\text{cano}}\mathcal{E}(L)\xrightarrow{\tilde{\alpha}}\mathrm{Aut}\,(A).$$

(b) An object X of II is *α-admissible* if

$$\mathrm{ad}:\ X\xrightarrow{\text{cano}}L\xrightarrow{\alpha}\mathrm{Der}_k(A).$$

(c) An object S of III is *α'-admissible* if

$$sa=\sum_{(s)}(s_{(1)}\cdot a)s_{(0)},\ \forall s\in S,\ \forall a\in A,$$

where $u\cdot a=\alpha'(u)(a)$, $\forall u\in U^{[p]}(L)$.

3.3. THEOREM. *The equivalences of* §2 *induce equivalences among the following subcategories:*

The $\tilde{\alpha}$-admissible objects of I,

The α-admissible objects of II,

The α'-admissible objects of III.

PROOF. We have only to prove that the equivalences of (2.1), (2.2), and (2.3) preserve the admissible objects.

(2.1) If $S\in\mathrm{Ob}(\mathrm{III})$ is α'-admissible, we have

$$xa=\sigma(a)x,\ \forall x\in T\square_{\sigma}S,\ \forall a\in T\otimes A,$$

$$\forall\sigma\in\mathcal{E}(L)(T),\ \forall T\in\mathbf{M}_k,$$

where $\sigma(a)=\tilde{\alpha}(\sigma)(a)$. Hence, for $(x,\sigma)\in E_S(T)$, we have

$$xa=\sigma(a)x.$$

This proves that E_S is $\tilde{\alpha}$-admissible.

(2.2) If $(G,\rho)\in\mathrm{Ob}(\mathrm{I})$ is $\tilde{\alpha}$-admissible, then

$$\mathrm{Lie}(\rho):\mathrm{Lie}(G)\xrightarrow{\text{cano}}L\xrightarrow{\alpha}\mathrm{Der}_k(A)$$

since $\alpha=\mathrm{Lie}(\tilde{\alpha})$. Hence $\mathrm{Lie}(G)$ is α-admissible.

(2.3) follows from a series of the following lemmas.

3.3.1. LEMMA. *Let*

$$H_1\longrightarrow H_2\longrightarrow H_3$$

be a sequence of finite cocommutative Hopf k-algebras which represents an H-extension of finite k-groups. Assume H_1 is commutative. The adjoint action

$$H_2\otimes H_1\longrightarrow H_1,\ x\otimes a\longmapsto\sum_{(x)}x_{(1)}aS(x_{(2)})$$

factors through $H_2\to H_3$, and we have

$$xa=\sum_{(x)}\bar{x}_{(1)}(a)x_{(2)},\ \forall x\in H_2,\ \forall a\in H_1$$

where we denote by $x\mapsto\bar{x}$ the projection $H_2\to H_3$, and we use the induced action of H_3 on H_1.

PROOF. Let

$$1\longrightarrow G_1\longrightarrow G_2\longrightarrow G_3\longrightarrow 1$$

be the corresponding H-extension. Then we have

$$yb=\bar{y}(b)y,\ \forall y\in G_2(T),\ \forall b\in G_1(T)$$

for each $T\in\mathbf{M}_k$. If is enough to translate this into the language of cocommutative Hopf algebras.

3.3.2. LEMMA. *Let*

$$0\longrightarrow L_1\longrightarrow L_2\longrightarrow L_3\longrightarrow 0$$

be an exact sequence of p-Lie algebras which are finitely generated projective k-modules. Assume L_1 is abelian. The adjoint action

$$\mathrm{ad}: L_2 \longrightarrow \mathrm{Der}_p(L_1),\ \mathrm{ad}(x)=[x, -]$$

factors through $L_2 \to L_3$. If we extend the induced p-Lie map $L_3 \to \mathrm{Der}_p(L_1) \subset \mathrm{Der}_k(U^{[p]}(L_1))$ to a measuring homomorphism

$$U^{[p]}(L_3) \longrightarrow \mathrm{End}_k(U^{[p]}(L_1))$$

then the action of $U^{[p]}(L_3)$ on $U^{[p]}(L_1)$ is associated in the sense of (3.3.1) *with the H-extension of finite cocommutative Hopf algebras*

$$U^{[p]}(L_1) \longrightarrow U^{[p]}(L_2) \longrightarrow U^{[p]}(L_3).$$

This is almost obvious.

We prove that the functor of (2.3) preserves admissible objects. Let $X \in \mathrm{Ob}(\mathrm{III})$ be α-admissible. Extend

$$L \xrightarrow{\alpha} \mathrm{Der}_k(A) \subset \mathrm{Der}_p(A) \subset \mathrm{Der}_k(U^{[p]}(A))$$

to a measuring homomorphism

$$'U^{[p]}(L) \longrightarrow \mathrm{End}_k(U^{[p]}(A)).$$

With respect to this action, we have

$$(*) \qquad xa = \sum_{(x)} \bar{x}_{(1)}(a) x_{(2)}, \quad \forall x \in U^{[p]}(X),\ \forall a \in U^{[p]}(A)$$

where $x \mapsto \bar{x}$ denotes the projection $U^{[p]}(X) \to U^{[p]}(L)$. Since this action is induced by the adjoint action of $U^{[p]}(X)$ on $U^{[p]}(A)$, it follows from (2.3.1) that

$$\pi: U^{[p]}(A) \longrightarrow A$$

is left $U^{[p]}(L)$-linear, where we let $U^{[p]}(L)$ act on A by α'. Applying the projection $q: U^{[p]}(X) \to B(X)$ to the formula (*), we conclude immediately that $B(X)$ is α'-admissible. Q.E.D.

3.4. DEFINITION. Let

$$\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L), \mu^A) \text{ (resp. } \mathrm{Ext}_{\alpha}(L, A), \text{ resp. } \mathrm{Br}_{\alpha'}(U^{[p]}(L), A/k))$$

be the set of isomorphism classes of $\tilde{\alpha}$-admissible objects in I (resp. α-admissible objects in II, resp. α'-admissible objects in III).

We shall make these into abelian groups and prove that they are isomorphic with one another.

3.5. The Baer sum.

3.5.1. $\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L), \mu^A)$.

The homomorphism $\tilde{\alpha}: \mathcal{E}(L) \to \mathrm{Aut}(A)$ induces an action

$$\mathcal{E}(L)\times\mu^A \longrightarrow \mu^A,\ (x, a)\longmapsto \tilde{\alpha}(x)(a)$$

and $\tilde{\alpha}$-admissible objects of I are the same as H-extensions

$$1 \longrightarrow \mu^A \longrightarrow G \longrightarrow \mathcal{E}(L) \longrightarrow 1$$

such that the inner action of G on μ^A induces the above action of $\mathcal{E}(L)$ on μ^A. Hence the isomorphism classes $\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L), \mu^A)$ form an abelian group by Baer sum [**2**, III, §6, 1.9] which is isomorphic to the Hochschild cohomology $H_0^2(\mathcal{E}(L), \mu^A)$ [**2**, III, §6, 2.1]. The unit is supplied by the semidirect product $\mu^A\times_s\mathcal{E}(L)$.

3.5.2. $\mathrm{Ext}_\alpha(L, A)$.

Let X_i, $i=1, 2$, be α-admissible objects in II. We can make an exact sequence of p-Lie algebras

$$0 \longrightarrow A\oplus A \longrightarrow X_1\oplus X_2 \longrightarrow L\oplus L \longrightarrow 0\,.$$

The diagonal map

$$\delta:\ L \longrightarrow L\oplus L,\ \delta(l)=(l, l)$$

is a p-Lie map. Let $X_1\times_L X_2$ by the inverse image of $\delta(L)$ in $X_1\oplus X_2$. Then we have an exact sequence of p-Lie algebras

$$0 \longrightarrow A\oplus A \longrightarrow X_1\times_L X_2 \longrightarrow L \longrightarrow 0$$

which is admissible with respect to the action

$$L\times(A\oplus A) \longrightarrow A\oplus A\,,$$

$$l\cdot(a, b)=(la, lb)\,.$$

The addition $(a, b)\mapsto a+b$, $A\oplus A\to A$ is a p-Lie map which is left L-linear. Hence the kernel N is an ideal such that $[X_1\times_L X_2, N]\subset N$. This means that N is an ideal of $X_1\times_L X_2$. Hence we have an exact sequence of p-Lie algebras

$$0 \longrightarrow A \longrightarrow (X_1\times_L X_2)/N \longrightarrow L \longrightarrow 0$$

which is α-admissible. Denoting by [ ] the isomorphism class, we define an addition on $\mathrm{Ext}_\alpha(L, A)$ by

$$[X_1]+[X_2]=[(X_1\times_L X_2)/N]\,.$$

It is easy to prove directly that this makes $\mathrm{Ext}_\alpha(L, A)$ into an abelian group, but unnecessary, since we shall prove later that $\mathrm{Ext}_\alpha(L, A)\cong\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L), \mu^A)$.

With respect to α, we can make the semidirect product $A\times_s L$ of p-Lie algebras, and we have the canonical extension (1.2.9)

$$0 \longrightarrow A \xrightarrow{\ i\ } A\times_s L \xrightarrow{\ q\ } L \longrightarrow 0$$

which is admissible. We shall prove later that this is the unit.

3.5.3. $\mathrm{Br}_{\alpha'}(U^{[p]}(L), A/k)$.

Let S_i, $i=1, 2$, be α'-admissible objects in III, and let $H=U^{[p]}(L)$. $S_1\otimes S_2$ has the structure of a split type right $H\otimes H$-comodule $(A\otimes A)/k$-algebra, where each structure of comodule, bimodule, and algebra is the tensor product. It is admissible with respect to the module algebra structure

$$(H\otimes H)\otimes(A\otimes A) \longrightarrow A\otimes A$$
$$(g\otimes h)(a\otimes b)=ga\otimes hb\,.$$

Let $S_1\square_H S_2$ denote the inverse image of $S_1\otimes S_2\otimes\Delta(H)$ by the comodule structure

$$\theta\colon S_1\otimes S_2 \longrightarrow S_1\otimes S_2\otimes H\otimes H\,.$$

It has the structure of a split type right H-comodule $(A\otimes A)/k$-algebra, which is admissible with respect to the action

$$H\otimes(A\otimes A) \longrightarrow A\otimes A$$
$$g\cdot(a\otimes b)=\sum_{(g)} g_{(1)}a\otimes g_{(2)}b\,.$$

Let M be the kernel of the product $a\otimes b\mapsto ab$, $A\otimes A\to A$. It is an ideal of $A\otimes A$ stable by H. Hence

$$(S_1\square_H S_2)M=M(S_1\square_H S_2)=\tilde{M}$$

is an ideal of $S_1\square_H S_2$. Just as we have constructed $B(X)$ for $X\in\mathrm{Ob(II)}$, we can make

$$(S_1\square_H S_2)/\tilde{M}$$

into a split type H-comodule A/k-algebra, which is α'-admissible. Define an addition on $\mathrm{Br}_{\alpha'}(H, A/k)$ by

$$[S_1]+[S_2]=[(S_1\square_H S_2)/\tilde{M}]\,.$$

There is another equivalent construction of $(S_1\square_H S_2)/\tilde{M}$. Let

$$\tilde{\tilde{M}}=M(S_1\otimes S_2)\,.$$

Then $(S_1\otimes S_2)/\tilde{\tilde{M}}$ is a left A- and a right $A\otimes A$-bimodule. It is also an $H\otimes H$-comodule satisfying

$$z(a\otimes b)=\sum(z'_{(1)}(a)z'_{(2)}(b))z_{(0)}$$

for each $z\in(S_1\otimes S_2)/\tilde{\tilde{M}}$, $a\otimes b\in A\otimes A$, where

$$\theta(z)=\sum z_{(0)}\otimes z'_{(1)}\otimes z'_{(2)}\,.$$

Let $S_1 * S_2$ be the inverse image of

$$\{(S_1\otimes S_2)/\tilde{\tilde{M}}\}\otimes\Delta(H)$$

by the comodule structure

$$\theta:(S_1\otimes S_2)/\tilde{\tilde{M}}\longrightarrow\{(S_1\otimes S_2)/\tilde{\tilde{M}}\}\otimes H\otimes H.$$

We can prove that S_1*S_2 is a subalgebra of $S_1\times_A S_2$ [4] containing A. It is an α'-admissible split type H-comodule A/k-algebra. The projection

$$S_1\otimes S_2\longrightarrow(S_1\otimes S_2)/\tilde{\tilde{M}}$$

induces $S_1\square_H S_2\rightarrow S_1*S_2$ which factors through the projection $S_1\square_H S_2\rightarrow(S_1\square_H S_2)/M$. The resulting map

$$(S_1\square_H S_2)/M\longrightarrow S_1*S_2$$

is a morphism in III, hence is isomorphic.

We do not prove that $\mathrm{Br}_{\alpha'}(H, A/k)$ is in fact an abelian group either. It will be shown that the unit is supplied by the smash product $A\#H$ [3, § 7.2] where the comodule structure is given by

$$\theta(a\#g)=\sum_{(g)}a\#g_{(1)}\otimes g_{(2)}.$$

3.6. THEOREM. *The equivalences of* § 2 *induce isomorphisms of abelian groups*

$$\mathrm{Ext}_{\tilde{\alpha}}(\mathcal{E}(L),\mu^A)\cong\mathrm{Ext}_{\alpha}(L, A)\cong\mathrm{Br}_{\alpha'}(U^{[p]}(L), A/k).$$

The proof divides into two parts.

3.6.1. I$\rightarrow$II.

Let (G_i, ρ_i), $i=1, 2$, be $\tilde{\alpha}$-admissible objects in I, and let $X_i=\mathrm{Lie}(G_i)$. The p-Lie extension

$$0\longrightarrow A\oplus A\longrightarrow X_1\oplus X_2\longrightarrow L\oplus L\longrightarrow 0$$

is induced from

$$1\longrightarrow\mu^A\times\mu^A\longrightarrow G_1\times G_2\longrightarrow\mathcal{E}(L)\times\mathcal{E}(L)\longrightarrow 1$$

by applying the functor Lie$(-)$. Since the functor Lie$(-)$ preserves fibre products, the Lie$(-)$ of the extension

$$1\longrightarrow\mu^A\times\mu^A\longrightarrow G_1\times_{\mathcal{E}(L)}G_2\longrightarrow\mathcal{E}(L)\longrightarrow 1$$

is

$$0\longrightarrow A\oplus A\longrightarrow X_1\times_L X_2\longrightarrow L\longrightarrow 1.$$

Let $\Sigma:\mu^A\times\mu^A\rightarrow\mu^A$ be $(a, b)\mapsto ab$. Then

$$\mathrm{Lie}(\Sigma): A\oplus A\longrightarrow A,\quad (u, v)\longmapsto u+v.$$

Apply the functor Lie$(-)$ to the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu^A\times\mu^A & \longrightarrow & G_1\times_{\mathcal{E}(L)}G_2 & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\Sigma} & & \downarrow & & \| & & \\
1 & \longrightarrow & \mu^A & \longrightarrow & G_1+G_2 & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1
\end{array}$$

where the bottom row denotes the Baer sum. We get

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A\oplus A & \longrightarrow & X_1\times_L X_2 & \longrightarrow & L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \text{addition}} & & \downarrow & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & \mathrm{Lie}\,(G_1+G_2) & \longrightarrow & L & \longrightarrow & 0\,.
\end{array}$$

This yields $\mathrm{Lie}\,(G_1+G_2)\cong(X_1\times_L X_2)/N$ in II.

3.6.2. III$\to$I.

Let S_i, $i=1, 2$, be α'-admissible objects in III. As we have seen in (3.5.3), $S_1\otimes S_2$ is a split type $U^{[p]}(L)\otimes U^{[p]}(L)$-comodule $(A\otimes A)/k$-algebra. Hence $E_{S_1\otimes S_2}$ is an H-extension of $\mathcal{E}(L)\times\mathcal{E}(L)$ by $\mu^{A\otimes A}$. If σ, $\tau\in\mathcal{E}(L)(T)$ with $T\in\mathbf{M}_k$, the canonical isomorphism

$$T\otimes S_1\otimes S_2\cong(T\otimes S_1)\otimes_T(T\otimes S_2)$$

induces

$$T\,\square_{(\sigma,\tau)}(S_1\otimes S_2)\cong(T\,\square_\sigma S_1)\otimes_T(T\,\square_\tau S_2)\,.$$

which is $T\otimes A\otimes A$-bilinear. If $(x, \sigma)\in E_{S_1}(T)$, $(y, \tau)\in E_{S_2}(T)$, let $x*y$ be the element of $T\,\square_{(\sigma,\tau)}(S_1\otimes S_2)$ which corresponds to $x\otimes_T y$. Then $(x*y, (\sigma, \tau))\in E_{S_1\otimes S_2}(T)$. There is a commutative diagram of extensions

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu^A\times\mu^A & \longrightarrow & E_{S_1}\times E_{S_2} & \longrightarrow & \mathcal{E}(L)\times\mathcal{E}(L) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\eta} & & \downarrow{\scriptstyle\zeta} & & \| & & \\
1 & \longrightarrow & \mu^{A\otimes A} & \longrightarrow & E_{S_1\otimes S_2} & \longrightarrow & \mathcal{E}(L)\times\mathcal{E}(L) & \longrightarrow & 1
\end{array}$$

where $\eta(a, b)=a\otimes_T b$, $\zeta((x, \sigma), (y, \tau))=(x*y, (\sigma, \tau))$, $\forall a$, $b\in\mu^A(T)$, $\forall(x, \sigma)\in E_{S_1}(T)$, $\forall(y, \tau)\in E_{S_2}(T)$, $\forall T\in\mathbf{M}_k$. Taking pullback along the diagonal $\mathcal{E}(L)\to\mathcal{E}(L)\times\mathcal{E}(L)$, we obtain a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu^A\times\mu^A & \longrightarrow & E_{S_1}\times_{\mathcal{E}(L)}E_{S_2} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\eta} & & \downarrow{\scriptstyle\zeta} & & \| & & \\
1 & \longrightarrow & \mu^{A\otimes A} & \longrightarrow & E_{S_1\square S_2} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1
\end{array}$$

where $S_1\square S_2=S_1\square_H S_2$ with $H=U^{[p]}(L)$. Also, there is a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu^{A\otimes A} & \longrightarrow & E_{S_1\square S_2} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\psi} & & \| & & \\
1 & \longrightarrow & \mu^A & \longrightarrow & E_{(S_1\square S_2)/\widetilde{M}} & \longrightarrow & \mathcal{E}(L) & \longrightarrow & 1
\end{array}$$

where ϕ is induced by the product $a\otimes b\mapsto ab$, $A\otimes A\to A$, and ψ by the projection

$S_1 \square S_2 \to (S_1 \square S_2)/\tilde{M}$. Since $\phi\eta = \Sigma$ with the notation of (3.6.1), we conclude that $E_{(S_1 \square S_2)/\tilde{M}}$ is isomorphic to the Baer sum of E_{S_1} and E_{S_2}, by composing the last two diagrams. Q. E. D.

3.7. REMARK. We verify the description of the units in (3.5). The Lie$(-)$ of the canonical extension

$$1 \longrightarrow \mu^A \longrightarrow \mu^A \times_s \mathcal{E}(L) \longrightarrow \mathcal{E}(L) \longrightarrow 1$$

is

$$0 \longrightarrow A \longrightarrow A \times_s L \longrightarrow L \longrightarrow 0$$

by the paragraph following (1.2.9). Hence $A \times_s L$ is the unit of $\mathrm{Ext}_\alpha(L, A)$. Next, to prove that

$$E_{A \# H} \cong \mu^A \times_s \mathcal{E}(L)$$

where $H = U^{[p]}(L)$, it is enough to prove that the projection $E_{A\#H} \to \mathcal{E}(L)$ has a section which is a homomorphism of k-group functors. Indeed, we can identify

$$T \otimes (A \# H) \cong (T \otimes A) \#_T (T \otimes H) .$$

If $\sigma \in G_T(T \otimes H)$, this gives

$$T \square_\sigma (A \# H) \cong (T \otimes A) \#_T T\sigma .$$

The map $\sigma \mapsto (1 \otimes 1) \#_T \sigma$ gives the required section.

Appendix. The proof of (1.2.3).

We prove the theorem (1.2.3). Let k be a commutative ring of prime characteristic p.

For each Hopf algebra H, let

$$H^+ = \mathrm{Ker}\,(\varepsilon : H \to k) .$$

A.1. LEMMA. *If L is a p-Lie algebra which is a finitely generated projective k-module, then the canonical map $L \to U^{[p]}(L)^+$ is injective, and $U^{[p]}(L)^+/L$ is finitely generated projective as a k-module.*

This can be proved by localizing k and using the PBW theorem, just as [2, II, §7, 3.7] (cf. [7, p. 434, Lemma 9]).

For each k-module V, let $S^{[p]}(V)$ be $U^{[p]}(V)$ where V is given the trivial p-Lie structure (i. e., $[V, V] = V^{[p]} = 0$). Thus $S^{[p]}(V)$ is the quotient of the symmetric algebra $S(V)$ by the ideal generated by v^p, $v \in V$.

Let $V^* = \mathrm{Hom}_k(V, k)$.

A.2. PROPOSITION. *Let L be a p-Lie k-algebra which is a finitely generated projective k-module, and let*

$$f : U^{[p]}(L) \longrightarrow L$$

be a k-linear map such that $f|L=Id$ and $f(1)=0$. The dual map

$$f^*: L^* \longrightarrow U^{[p]}(L)^*$$

induces an isomorphism of k-algebras

$$S^{[p]}(L^*)\cong U^{[p]}(L)^*.$$

PROOF. Since $\varepsilon f^*=0$ and $x^p=0$ for each $x\in U^{[p]}(L)^{*+}$, it follows that f^* induces an algebra map

$$S^{[p]}(L^*) \longrightarrow U^{[p]}(L)^*.$$

To prove that this is isomorphic, we can localize k and assume that L is k-free. By the PBW theorem,

$$U^{[p]}(L)^*\cong k[X_1, \cdots, X_n]/(X_1^p, \cdots, X_n^p)$$

as algebras and $f^*(L^*)$ has a basis

$$X_1', \cdots, X_n'$$

where $X_i'-X_i$ is a polynomial of degree >1 without constant term, for each $1\leqq i\leqq n$. Using the canonical graduation on $k[X_1, \cdots, X_n]/(X_1^p, \cdots, X_n^p)$, we can easily prove that $X_i\mapsto X_i'$ defines an automorphism of it. Hence the homomorphism $S^{[p]}(L^*)\to U^{[p]}(L^*)$ is isomorphic. Q. E. D.

A.3. LEMMA. *Let $r: L_1\to L_2$ be a surjective homomorphism of p-Lie algebras which are finitely generated projective k-modules. If $f: U^{[p]}(L_2)\to L_2$ is a k-linear map such that $f|L_2=Id$ and $f(1)=0$, then there is a k-linear map $F: U^{[p]}(L_1)\to L_1$ such that $F|L_1=Id$, $F(1)=0$, and*

$$\begin{array}{ccc} U^{[p]}(L_1) & \xrightarrow{r'} & U^{[p]}(L_2) \\ \downarrow F & & \downarrow f \\ L_1 & \xrightarrow{r} & L_2 \end{array}$$

commutes, where r' denotes the homomorphism induced by r.

PROOF. Let V be a submodule of L_1 such that $L_1=V\oplus \mathrm{Ker}(r)$. Since

$$U^{[p]}(L_2)=L_2\oplus \mathrm{Ker}(f),$$

we have

$$U^{[p]}(L_1)=V\oplus r'^{-1}(\mathrm{Ker}(f)).$$

Since

$$U^{[p]}(L_1)^+/L_1\cong r'^{-1}(\mathrm{Ker}(f))^+/\mathrm{Ker}(r)$$

is finitely generated projective, there is a submodule W of $r'^{-1}(\mathrm{Ker}(f))^+$ such that

$$r'^{-1}(\mathrm{Ker}(f))^+=\mathrm{Ker}(r)\oplus W,$$

hence

$$U^{[p]}(L_1)^+ = L_1 \oplus W.$$

We have only to define F by $F|L_1 = Id$, $F|W = 0$, and $F(1) = 0$. Q.E.D.

A.4. PROPOSITION. *Let $r: L_1 \to L_2$ be a surjective homomorphism of p-Lie algebras which are finitely generated projective k-modules. Then the induced Hopf algebra map*

$$r' : U^{[p]}(L_1) \longrightarrow U^{[p]}(L_2)$$

has a coalgebra section.

PROOF. Let $f: U^{[p]}(L_2) \to L_2$ be a k-linear map such that $f(1)=0$, $f|L_2 = Id$. Lift f to F as in (A.3). We have a commutative diagram

$$\begin{tikzcd} U^{[p]}(L_1)^* & U^{[p]}(L_2)^* \arrow[l, "r'^*"'] \\ S^{[p]}(L_1^*) \arrow[u, "F^*", "\wr"'] & S^{[p]}(L_2^*) \arrow[l, "r^*"] \arrow[u, "f^*", "\wr"'] \end{tikzcd}.$$

Since a k-linear retract for $r^*: L_2^* \to L_1^*$ induces a k-algebra retract for $r^*: S^{[p]}(L_2^*) \to S^{[p]}(L_1^*)$, the k-algebra map r'^* has a retract. This means that r' has a coalgebra section. Q.E.D.

Note that each coalgebra map $U^{[p]}(L_1) \to U^{[p]}(L_2)$ sends L_1 into L_2, if L_i are finitely generated projective p-Lie algebras.

A.5. LEMMA. *Let L_1 and L_2 be finitely generated projective p-Lie algebras. A coalgebra map*

$$c: U^{[p]}(L_1) \longrightarrow U^{[p]}(L_2)$$

is an isomorphism if $c: L_1 \cong L_2$.

PROOF. We can assume $c(1)=1$. Also, we can assume $L_1 = L_2 = L$ and $c|L = Id$. Let

$$f: U^{[p]}(L) \longrightarrow L$$

be a k-linear map such that $f(1)=0$, $f|L = Id$. Then fc also satisfies the same condition. Thus

$$\begin{tikzcd} & S^{[p]}(L^*) \arrow[dl, "(fc)^*"', "\wr"] \arrow[dr, "f^*", "\wr"'] & \\ U^{[p]}(L)^* & & U^{[p]}(L)^* \arrow[ll, "c^*"'] \end{tikzcd}$$

which proves that c^* is an isomorphism. Q.E.D.

A.6. PROPOSITION. *Let*

$$0 \longrightarrow L_1 \longrightarrow L_2 \xrightarrow{r} L_3 \longrightarrow 0$$

be an exact sequence of p-Lie algebras which are finitely generated projective k-modules. Let $s: U^{[p]}(L_3) \to U^{[p]}(L_2)$ *be a section to* $r': U^{[p]}(L_2) \to U^{[p]}(L_3)$. *Then*

$$\xi: U^{[p]}(L_1) \otimes U^{[p]}(L_3) \cong U^{[p]}(L_2)$$

$$\xi(x \otimes y) = x s(y).$$

PROOF. $s(L_3) \subset L_2$, and $s: L_3 \to L_2$ is a section to r. If we identify

$$U^{[p]}(L_1 \oplus L_3) \cong U^{[p]}(L_1) \otimes U^{[p]}(L_3),$$

then $\xi | L_1 \oplus L_3$ gives

$$L_1 \oplus L_3 \cong L_2, \ (x, y) \longmapsto x + s(y).$$

Hence ξ is an isomorphism by (A.5). Q. E. D.

The last proposition proves (1.2.3).

References

[1] S.U. Chase and M.E. Sweedler, Hopf algebras and Galois theory, Springer Lecture Notes, **97** (1969).

[2] M. Demazure and P. Gabriel, Groupes algébriques, tome I, North-Holland, Amsterdam, 1970.

[3] M.E. Sweedler, Hopf algebras, Benjamin, Inc., New York, 1969.

[4] M.E. Sweedler, Groups of simple algebras, I.H.E.S. Publ. Math., **44** (1975), 79-189.

[5] M. Takeuchi, On extensions of affine groups by μ^A, Com. Alg., **5**(13) (1977), 1401-1437.

[6] M. Takeuchi, On extensions of formal groups by μ^A, Com. Alg., **5**(13) (1977), 1439-1481.

[7] S. Yuan, Central separable algebras with purely inseparable splitting rings of exponent one, Trans. A.M.S., **153** (1971), 427-450.

Mitsuhiro TAKEUCHI
The Institute for Advanced Study
Princeton, N.J. 08540
U.S.A.
and
University of Tsukuba
Ibaraki 305
Japan