J. Math. Soc. Japan
Vol. 19, No. 1, 1967

On the extensions of linear groups by abelian varieties over a field of positive characteristic p

By Masayoshi MIYANISHI

(Received Feb. 20, 1965)

Contents.

Introduction.

In this paper, we denote by k a fixed algebraically closed field of characteristic $p > 0$. All algebraic varieties, algebraic groups and homomorphisms etc., are those defined over k, unless the contrary is explicitly mentioned. We denote by $\mathcal{A}$ the category of commutative algebraic groups. If we consider the case over a field of the characteristic zero, then such category is an abelian category, but in our case, since the characteristic p is positive, $\mathcal{A}$ is not abelian category. However $\mathcal{A}$ can be mapped into the abelian category Q of quasi-algebraic groups, Q being embedded into the abelian category $\mathcal{P} \cong \mathrm{Pro}(Q)$ of proalgebraic groups. Considering the completions of algebraic groups at their neutral elements, $\mathcal{A}$ also can be mapped into the category of reduced formal groups $\mathcal{F}$ which is not abelian, and $\mathcal{F}$ can be embedded into the abelian category $\tilde{\mathcal{F}}$ formed by formal groups whose coordinate rings may have nilpotent elements.

The purpose of this paper is to study the groups of isomorphism classes of extensions of a linear group by an abelian variety A in $\mathcal{A}$, $\mathcal{P}$, $\mathcal{F}$, especially the groups, $\mathrm{Ext}_{\mathcal{A}}(G_m, A)$, $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$, $\mathrm{Ext}_{\mathcal{P}}(G_m, A)$, $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$ and $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$, where $\mathcal{A}$, $\mathcal{P}$ or $\mathcal{F}$ shows the category in which above groups are considered.

The results which we obtain are as follows:

(1) $\mathrm{Ext}_{\mathcal{A}}(G_m, A) \cong \bigoplus_{l:\,\mathrm{prime}} A_{[l]} \cong$ *the torsion subgroup of* A *(isomorphism of abelian groups), where* $A_{[l]}$ *means the group formed by elements* a *of* A *such that* $l^N a = 0$ *for some integer* $N \geqq 0$, *and* l *runs over all prime numbers* > 0.

(2) $\mathrm{Ext}_{\mathcal{A}}(G_a, A) \cong \bigoplus_{i=1}^{n} k$ *(isomorphism of k-vector spaces), that is,* $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ *is endowed with the structure of k-vector space of dimension* $n = \dim A$.

(3) $\mathrm{Ext}_{\mathcal{P}}(G_m, A) \cong \bigoplus_{\substack{l \neq p \\ l:\,\mathrm{prime}}} A_{[l]}$, *(isomorphism of abelian groups), where* p *is the characteristic of* k, *and* l *runs over all positive prime numbers except* p.

(4) $\mathrm{Ext}_{\mathcal{P}}(G_a, A) \cong \bigoplus_{i=1}^{f} k$, *(isomorphism of k-vector spaces), where* f *is the integer* $\geqq 0$ *such that* p^f *is the order of the kernel of* $p\delta_A$.

(5) $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A}) \cong \bigoplus_{i=1}^{n-f} k$, *(isomorphism of k-vector spaces).*

For these descriptions, we use the theories of pro-algebraic groups and of formal groups, and above all, the theory of Dieudonné modules. We prove that any Dieudonné module M is of (projective) dimension $\leqq 2$, and the dimension is equal to 1 if M is reduced. These results are interesting if we recall the groups, $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$ and $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$, which are given the definite descriptions by I. Barsotti, [1], P. Cartier, [5], M. Rosenlicht, [16] and J. P. Serre, [17] etc.. Moreover, there exists a duality between $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$ and $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$. (See the forthcoming paper by H. Matsumura and M. Miyanishi.) To complete the description, we shall recall some results without proof by Serre's book, [19]. Now, the author would like to express his gratitude to Professor H. Matsumura for his advices and valuable conversations. (Added in August 1966.) F. Oort has obtained the same result on $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ which has been published with many other results on commutative group schemes as n°15 in Springer Lecture Note series.

Chapter I. Preliminaries.

§ 1. Definitions and some fundamental results.

1. For all the definitions and the results which appear here without definite descriptions, the readers will be sent to Serre's book, [**19**].

Let A, B, C be elements of $\mathcal{A}$. A strictly exact sequence $0 \to B \to C \to A \to 0$ is also exact in $\mathcal{A}$ in the sense of the category and is called an *extension* of A by B. We shall denote by $\mathrm{Ext}_{\mathcal{A}}(A, B)$ the set of isomorphism classes of extensions of A by B in the category $\mathcal{A}$.

In the following, for the abbreviation of notation, when we write $C \in \mathrm{Ext}_{\mathcal{A}}(A, B)$, we mean that the isomorphism class of the extension C of A by B belongs to $\mathrm{Ext}_{\mathcal{A}}(A, B)$.

Then $\mathrm{Ext}_{\mathcal{A}}(A, B)$ can be endowed with a structure of abelian group and $\mathrm{Ext}_{\mathcal{A}}(*, B)$ (resp. $\mathrm{Ext}_{\mathcal{A}}(A, *)$) is a contravariant (resp. covariant) functor from $\mathcal{A}$ to the category of abelian groups. For the details, see Serre's book [**19**].

We shall mention some results for the convenience of later applications.

PROPOSITION 1.1. *For a strictly exact sequence* $0 \to A' \to A \to A'' \to 0$ *in* $\mathcal{A}$ *and for* $B \in \mathcal{A}$, *we have the following exact sequence of abelian groups;*

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A'', B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A', B)$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{A}}(A'', B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A', B).$$

PROPOSITION 1.2. *For a strictly exact sequence* $0 \to B' \to B \to B'' \to 0$ *in* $\mathcal{A}$ *and for* $A \in \mathcal{A}$, *we have the following exact sequence of abelian groups;*

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B') \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B'')$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B') \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B'').$$

2. When k is of characteristic $p > 0$, the class of purely inseparable isogeny of height 1, A' of A corresponds bijectively to the restricted sub-p-Lie algebra $\mathfrak{N}$ of $t(A)$, where $t(A)$ means the tangent space of A at the neutral element. If $\mathfrak{N}$ is a sub p-Lie algebra of $t(A)$, we denote by $A/\mathfrak{N}$ the group which is associated to $\mathfrak{N}$ and defined as follows. We have $A/\mathfrak{N} = A$ in the set-theoretic sense, and the rational functions of $A/\mathfrak{N}$ are those of A which are annihilated by the derivations of $\mathfrak{N}$. If $\varphi : A \to A'$ is a purely inseparable isogeny of height 1, there is a mapping $t(\varphi) : t(A) \to t(A')$, which is a homomorphism of restricted p-Lie algebras. We associate to φ the kernel of $t(\varphi)$, which is a sub p-Lie algebra of $t(A)$. Especially, if $\mathfrak{N} = t(A)$, $A/t(A) \cong A^p$, the image of Frobenius endomorphism of A, and if $\mathfrak{N} = 0$, $A/\mathfrak{N} = A$. Then we have the following.

PROPOSITION 1.3. *For a sub p-Lie algebra* $\mathfrak{N}$ *of* $t(A)$ *and for* $B \in \mathcal{A}$, *we have the following exact sequence,*

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A/\mathfrak{N}, B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Hom}(\mathfrak{N}, t(B))$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{A}}(A/\mathfrak{N}, B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}(\mathfrak{N}, t(B)),$$

where Hom $(\mathfrak{N}, t(B))$, Ext $(\mathfrak{N}, t(B))$ *are taken in the category of restricted abelian p-Lie algebras defined over k. In particular, we have the exact sequence,*

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A^p, B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Hom}(t(A), t(B))$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{A}}(A^p, B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}(t(A), T(B)).$$

§ 2. On $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$ and $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$.

Letting A be an abelian variety in $\mathcal{A}$, we cite the results on $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$ and $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$ which are well known and which we do not use in our subsequent theory. These are inserted here for comparison.

1. The case of $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$.

PROPOSITION 2.1. *If A is an abelian variety, the group $\mathrm{Ext}_{\mathcal{A}}(A, G_a)$ is isomorphic onto $H^1(A, \mathcal{O}_A)$, the group of isomorphism classes of locally trivial fibre spaces of the base A and of the structure group G_a.*

PROPOSITION 2.2. (Cf. P. Cartier [5].) *Let A be an abelian variety defined over k and let A^* be its Picard variety. Then there exists a linear isomorphism from the tangent space $t(A^*)$ at the neutral element of A^* to the cohomology group $H^1(A, \mathcal{O}_A)$.*

For the proof of this result, we use the following fact:
the dimension of k-vector space $H^1(A, \mathcal{O}_A)$ is equal to the dimension of A.

2. The case of $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$.

We only mention a principal result, and for the proof of the result and other detailed results, the readers will be sent to P. Cartier [**6**], J. P. Serre [**17**] and I. Barsotti [**1**].

PROPOSITION 2.3. *Let A be an abelian variety defined over k. Then the group $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$ is isomorphic to the additive group of the Picard variety A^* of A.*

§ 3. The concept of the extensions of groups in $\mathcal{F}$.

1. Let G, H be two commutative formal Lie groups of finite dimension. We say that a formal group G' and a pair of homomorphisms $H \xrightarrow{u} G' \xrightarrow{v} G$ constitute an *extension* of G by H if u is a monomorphism and v is an epimorphism, and if the kernel of v is equal to the image of u.

We say, as usual, that two extensions (G', u, v), (G_1, u_1, v_1) are equivalent if there exists an isomorphism $f: G' \to G_1$ such that the diagram,

$$\begin{array}{ccccc} H & \xrightarrow{u} & G' & \xrightarrow{v} & G \\ \downarrow \text{id.} & & \downarrow f & & \downarrow \text{id.} \\ H & \xrightarrow[u_1]{} & G_1 & \xrightarrow[v_1]{} & G \end{array}$$

is commutative. The set of all isomorphism classes of extensions of G by H is denoted by $\mathrm{Ext}_{\mathscr{F}}(G, H)$.

2. Let (G, φ) and (H, ψ) be formal groups of dimension n and m with formal group laws $\varphi=(\varphi_i)_{1\leqq i\leqq n}$ and $\psi=(\psi_j)_{1\leqq j\leqq m}$. We call a system of indeterminates $x=(x_1, \cdots, x_n)$ a *generic point* of G.

Let $x^{(1)}, \cdots, x^{(k)}$ be independent generic points of G. We define *k-cochain* g on G with values in H as a system of formal power series $g=(g_j(x^{(1)}, \cdots, x^{(k)}))_{1\leqq j\leqq m}$ with respect to $x^{(1)}, \cdots, x^{(k)}$. The sum of k-cochains g and g' is defined by

$$(g \dotplus g')_j(x^{(1)}, \cdots, x^{(k)})=\psi_j(g(x^{(1)}, \cdots, x^{(k)}), g'(x^{(1)}, \cdots, x^{(k)})), \qquad 1\leqq j\leqq m.$$

By this sum $(\dotplus)$, the k-cochains on G with values in H form an abelian group $C^k(G, H)$. We next define the *coboundary operator* $d_{k+1}: C^k(G, H)\rightarrow C^{k+1}(G, H)$ by $(d_{k+1}g)(x^{(1)}, \cdots, x^{(k+1)})=g(x^{(2)}, \cdots, x^{(k+1)})\dotplus \sum_{i=1}^{k}(-1)^i g(x^{(1)}, \cdots, x^{(i-1)}, x^{(i)}\dotplus x^{(i+1)}, x^{(i+2)}, \cdots, x^{(k+1)})\dotplus(-1)^{k+1}g(x^{(1)}, \cdots, x^{(k)})$. It is easy to see $d_{k+2}\cdot d_{k+1}=0$. We can define as usual the subgroup $Z^k(G, H)\subset C^k(G, H)$ of *k-cocycles* for $k\geqq 1$ and the subgroup $B^k(G, H)\subset Z^k(G, H)$ of *k-coboundaries* for $k\geqq 2$. Hence the definition of k-cohomology group,

$$H^k(G, H)=Z^k(G, H)/B^k(G, H) \qquad \text{for} \quad k\geqq 2,$$

and

$$H^1(G, H)=Z^1(G, H).$$

If 2-cochain $g=(g_j)_{1\leqq j\leqq m}$ satisfies,

$$g_j(x^{(1)}, x^{(2)})=g_j(x^{(2)}, x^{(1)}), \qquad 1\leqq j\leqq m,$$

we call g *symmetric* and denote the set of symmetric 2-cochains (resp. 2-cocycles, 2-coboundaries) by $C^2(G, H)_s$ (resp. $Z^2(G, H)_s$, $B^2(G, H)_s$). And we define $H^2(G, H)_s$ as the quotient $Z^2(G, H)_s/B^2(G, H)_s$. It is proved in J. Dieudonné [**11**] that $H^2(G, H)_s$ corresponds bijectively to the set $\mathrm{Ext}_{\mathscr{F}}(G, H)$ of the isomorphism classes of extensions of G by H. In the following, $\mathrm{Ext}_{\mathscr{F}}(G, H)$ are considered with the structure of abelian group induced from $H^2(G, H)_s$.

3. Let A be an algebraic group of dimension n defined over k with the neutral element e_A. Then we can associate to A a formal group $\hat{A}$ of dimension n defined over k, by the process of completing the local ring $\mathcal{O}_A$ of A at the point e_A with respect to its topology defined by its maximal ideal $\mathfrak{M}_A$. For the details, see J. Dieudonné [**10**]. $\hat{A}$ is sometimes called the *completion* of A.

Let A, B be algebraic groups and let $u: A \to B$ be a homomorphism. Suppose that A, B and u are defined over k. Then we can associate to u a homomorphism $\hat{u}: \hat{A} \to \hat{B}$ of the formal groups defined over k. See also [**10**].

4. Let A, B be commutative group varieties and let C be an extension of B by A,

$$0 \longrightarrow A \underset{\alpha}{\longrightarrow} C \underset{\beta}{\longrightarrow} B \longrightarrow 0. \tag{1}$$

Let $k(A)$ (resp. $k(B)$, $k(C)$) be the k-rational functions field of A (resp. B, C) and let $k\{A\}$ (resp. $k\{B\}$, $k\{C\}$) be the quotient field of the completion of $\mathcal{O}_A$ (resp. $\mathcal{O}_B$, $\mathcal{O}_C$) with respect to its $\mathfrak{M}_A$ (resp. $\mathfrak{M}_B$, $\mathfrak{M}_C$)-adic topology. As easily shown, $\beta^*: k(B) \to k(C)$ is injective and $\alpha^*: k(C) \to k(A)$ is surjective. Therefore $\beta^*: k\{B\} \to k\{C\}$ is injective and $\alpha^*: k\{C\} \to k\{A\}$ is surjective. Then by the homomorphism theorem of J. Dieudonné [8], we have the next exact sequence of formal groups,

$$0 \longrightarrow \hat{A} \underset{\hat{\alpha}}{\longrightarrow} \hat{C} \underset{\hat{\beta}}{\longrightarrow} \hat{B} \longrightarrow 0,$$

which defines an extension $\hat{C}$ of $\hat{B}$ by $\hat{A}$ in the category $\mathcal{F}$. If we fix group laws of $\hat{A}$ and $\hat{B}$, the isomorphism class of $\hat{C}$ is defined depending only on the sequence (1). Thus we obtained a map $\sigma: \mathrm{Ext}_{\mathcal{A}}(B, A) \to \mathrm{Ext}_{\mathcal{F}}(\hat{B}, \hat{A})$. From the definition, σ is evidently a homomorphism of abelian groups.

5. For the concept of extensions of proalgebraic groups, we shall send the readers to Serre's book, [**20**].

Let A, B be elements of $\mathcal{A}$, and G be an extension of B by A. If we consider A, B as elements of $\mathcal{P}$, then G is an extension of B by A in $\mathcal{P}$. Hence the definition of a homomorphism of abelian groups $\rho: \mathrm{Ext}_{\mathcal{A}}(B, A) \to \mathrm{Ext}_{\mathcal{P}}(B, A)$.

§ 4. Some remarks.

1. Let A, B be elements of $\mathcal{A}$, and G be an extension of B by A. For a generic point x of B over k, the set of elements of G which are mapped to x is an algebraic variety defined over $k(x)$ and is endowed with the structure of principal homogeneous space with respect to A. We will quote the result concerning the principal homogeneous space from A. Weil, [**21**].

LEMMA 4.1. *Let G be a commutative group defined over a field K. Let H_i for $1 \leqq i \leqq n$, be principal homogeneous spaces with respect to G, defined over K. Then there is a principal homogeneous space H with respect to G defined over K, and an everywhere defined mapping f of $H_1 \times H_2 \times \cdots \times H_n$ into H, defined over K, such that*

$$f(s_1 a_1, \cdots, s_n a_n) = s_1 \cdots s_n f(a_1, \cdots, a_n),$$

for all $s_i \in G$ *and* $a_i \in H_i$. *Moreover* H *and* f *are uniquely determined up to an isomorphism of* H.

Let G and G' be extensions of B by A. Then we shall recall the sum $\{G\}+\{G'\}$ of the classes $\{G\}$ and $\{G'\}$ which are determined by G and G' respectively. First $G \times G'$ is considered as an extension of $B \times B$ by $A \times A$. Then, we consider the transfered extension $d^*(G \times G')$ by the diagonal map $d: B \to B \times B$. If x is a generic point of B over k, $G_x \times G'_x$, where G_x (resp. G'_x) is the inverse image of x, is considered as a principal homogeneous space with respect to $A \times A$, defined over $k(x)$. Next we transfer $d^*(G \times G')$ to $s_* d^*(G \times G')$ by the composition law s of A. Then we have the following commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \times A & \longrightarrow & d^*(G \times G') & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow s_A & & \downarrow \varphi & & \downarrow id & & \\ 0 & \longrightarrow & A & \longrightarrow & s_* d^*(G \times G') & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

For points g_1, g_2 of G_x and G'_x, and points a_1, a_2 of A, $\varphi(a_1 g_1, a_2 g_2) = a_1 a_2 \varphi(g_1, g_2)$, and $\varphi(g_1, g_2)$ is contained in the set G''_x of elements of $s_* d^*(G \times G')$ which are mapped onto x. As G''_x is also considered as a principal homogeneous space with respect to A defined over $k(x)$, from Lemma 4.1 the birational equivalence class $[G''_x]$ is the sum of the birational equivalence classes $[G_x]$ and $[G'_x]$. If y is another generic point of B over k, the classes $[G_x]$ and $[G_y]$ are identical, therefore we denote this class by $[G]$. For G, G' such that $\{G\} = \{G'\}$, we have $[G]=[G']$. Therefore we can associate to every class $\{G\}$ of $\mathrm{Ext}_{\mathcal{A}}(B, A)$ the element $[G]$ of the commutative group $\mathcal{PH}(A)$ composed by the birational equivalence classes of principal homogeneous spaces with respect to A (we denote this map by π).

PROPOSITION 4.1. *π is a homomorphism of which kernel is* $H^2_{\mathrm{rat.}}(B, A)_s$. *(For the notation of* $H^2_{\mathrm{rat.}}(B, A)_s$, *see Serre's book,* [**19**].)

PROOF. Let x be a generic point of B over k, and G be an extension of B by A such that $\pi(\{G\})=0$. Then G_x has a $k(x)$-rational point $g=\varphi(x)$. Then φ is a rational section of B to G. Conversely if G has a k-rational section, G_x is $k(x)$-trivial.

COROLLARY.

(1) *If B is a linear group, and A is an abelian variety, then* $H^2_{\mathrm{rat.}}(B, A)_s = 0$, *that is, π is injective.*

(2) *If A is linear, then π is trivial.*

The demonstration is easy, so we omit it.

2. Let A, B, C be abelian varieties defined over k. If $0 \to B \to C \to A \to 0$ is a strictly exact sequence, the transposed sequence $0 \to A^* \to C^* \to B^* \to 0$ is also strictly exact. This fact is proved in S. Lang, [13], Theorem 10, p. 216. Thence we have,

$$0 \longrightarrow t(A^*) \longrightarrow t(C^*) \longrightarrow t(B^*) \longrightarrow 0.$$

By virtue of the results of § 2,

$$0 \longrightarrow \mathrm{Ext}_{\mathcal{A}}(A, G_a) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(C, G_a) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(B, G_a) \longrightarrow 0,$$

or

$$0 \longrightarrow H^1(A, \mathcal{O}_A) \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow H^1(B, \mathcal{O}_B) \longrightarrow 0.$$

3. As $(A^*)^* \cong A$ (biregular isomorphism), we get bijective maps

$$(*)_1: \quad \mathrm{Hom}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(B^*, A^*),$$

$$(*)_2: \quad \mathrm{Ext}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(B^*, A^*).$$

Both $(*)_1$ and $(*)_2$ are isomorphisms.

4. Let G be a commutative algebraic group, and $\mathfrak{N}$ be a sub p-Lie algebra of $t(G)$. Then for any commutative algebraic group H, $\mathrm{Hom}_{\mathcal{A}}(H, G) \to \mathrm{Hom}_{\mathcal{A}}(H, G/\mathfrak{N})$ is injective. If G, H are abelian varieties A, B respectively, we define $\mathfrak{N}^*$ corresponding to $\mathfrak{N}$ as follows. Since $A/\mathfrak{N}$ is a purely inseparable isogeny of A, A^* is also a purely inseparable isogeny of $(A/\mathfrak{N})^*$. We define $\mathfrak{N}^*$ as the kernel of the homomorphism,

$$t((A/\mathfrak{N})^*) \longrightarrow t(A^*).$$

Then we have the following exact sequence,

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(B, A) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(B, A/\mathfrak{N}) \longrightarrow \mathrm{Hom}(\mathfrak{N}^*, t(B^*))$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{A}}(B, A) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(B, A/\mathfrak{N}) \longrightarrow \mathrm{Ext}(\mathfrak{N}^*, t(B^*)).$$

Chapter II. On $\mathrm{Ext}_{\mathcal{A}}(G_m, A)$.

§ 1. On $\mathrm{Ext}_{\mathcal{P}}(G_m, A)$.

1. Let A be an abelian variety defined over an algebraically closed field k of characteristic $p > 0$ and G_m be the multiplicative group. We can consider A and G_m objects of the category $\mathcal{P}$ of proalgebraic groups. With the notations of Serre's book, [20], we can consider the universal covering $\overline{G}_m$ of G_m, where $\pi_1(\overline{G}_m) = \pi_0(\overline{G}_m) = \pi_0(G_m) = 0$. Moreover, $\overline{G}_m$ is a projective object in $\mathcal{P}$.

LEMMA 1.1. (1) *The l-primary component of $\pi_1(G_m)$ is isomorphic to $\mathbf{Z}_l$, the ring of l-adic integers, when l is a prime number different from p, and is zero, when $l = p$.*

(2) *We have the following exact sequence in $\mathcal{P}$,*

$$0 \longrightarrow \pi_1(G_m) \longrightarrow \overline{G}_m \longrightarrow G_m \longrightarrow 0. \tag{1}$$

2. $\pi_1(G_m)$ belongs to the category $\mathcal{P}_0$ of profinite groups, which is a subcategory of $\mathcal{P}$. Using the exact sequence (1), we have,

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{P}}(G_m, A) \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\bar{G}_m, A) \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\pi_1(G_m), A)$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{P}}(G_m, A) \longrightarrow \mathrm{Ext}_{\mathcal{P}}(\bar{G}_m, A).$$

LEMMA 1.2.

(1) $\mathrm{Hom}_{\mathcal{P}}(G_m, A) = \mathrm{Hom}_{\mathcal{P}}(\bar{G}_m, A) = 0$,

(2) $\mathrm{Ext}_{\mathcal{P}}(\bar{G}_m, A) = 0$.

PROOF. The category of quasi-algebraic groups Q is a full subcategory of $\mathcal{P}$. Therefore $\mathrm{Hom}_{\mathcal{P}}(G_m, A) = \mathrm{Hom}_Q(G_m, A) = 0$, for G_m is linear and A is an abelian variety. As for $\mathrm{Hom}_{\mathcal{P}}(\bar{G}_m, A)$, at first, $\bar{G}_m$ is represented as a projective limit $\varprojlim_n G^{(n)}$, where $G^{(n)}$ is a quasi-algebraic group and satisfies the following sequences,

$$0 \longrightarrow N^{(n)} \longrightarrow G^{(n)} \xrightarrow{\varphi^{(n)}} G_m \longrightarrow 0,$$

$N^{(n)}$ being a finite group, and satisfying $\varprojlim_n N^{(n)} = \pi_1(G_m)$. These $G^{(n)}$ really exist from the definition of the proalgebraic group $\bar{G}_m$. Then, with some algebraic group structure of $G^{(n)}$ and a morphism $\varphi^{(n)}$, $G^{(n)}$ are isogenous to G_m, hence linear, because the isogeny preserves the linearity. Consequently $\mathrm{Hom}_{\mathcal{P}}(\bar{G}_m, A) = \varinjlim \mathrm{Hom}_Q(G^{(n)}, A) = 0$, by virtue of Proposition 14 of [20]. As for (2), the proof is trivial, because $\bar{G}_m$ is a projective object in $\mathcal{P}$.

3. Therefore we have the isomorphism of abelian groups,

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_m), A) \cong \mathrm{Ext}_{\mathcal{P}}(G_m, A).$$

Taking Lemma 1.1 into consideration, $\pi_1(G_m) = \prod_{\substack{l \neq p \\ l:\,\text{prime}}} \varprojlim_n (\mathbf{Z}/l^n\mathbf{Z})$. Hence,

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_m), A) = \bigoplus_{\substack{l \neq p \\ l:\,\text{prime}}} \mathrm{Hom}_{\mathcal{P}}(\varprojlim_n \mathbf{Z}/l^n\mathbf{Z}, A) = \bigoplus_{\substack{l \neq p \\ l:\,\text{prime}}} \varinjlim_n \mathrm{Hom}(\mathbf{Z}/l^n\mathbf{Z}, A).$$

We shall denote by a symbol $A_{[l]}$, l: prime number, the set of elements a of A such that $l^n a = 0$ for some positive integer n. Then we have:

THEOREM 1.1.

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_m), A) = \bigoplus_{\substack{l \neq p \\ l:\,\text{prime}}} A_{[l]},$$

where l runs over all positive prime number except p.

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_m), A) \cong \mathrm{Ext}_{\mathcal{P}}(G_m, A).$$

§ 2. On $\mathrm{Ext}_{\mathcal{A}}(G_m, A)$.

1. We use Proposition 1.3 of § 1, Chapter I. $t(G_m)$ has an element $Y = t\dfrac{\partial}{\partial t}$ as a base, where t is a generic point of G_m over k, and Y satisfies

$Y^p = Y$. Then we have,

$$0 \longrightarrow \mathrm{Hom}\,(t(G_m), t(A)) \longrightarrow \mathrm{Ext}_{\mathcal{A}}\,(G_m^p, A) \longrightarrow \mathrm{Ext}_{\mathcal{A}}\,(G_m, A) \longrightarrow \mathrm{Ext}\,(t(G_m), t(A)) . \qquad (1)$$

2. Let A be an abelian variety. First we have the next Lemma.

LEMMA 2.1. *The restricted p-Lie algebra $t(A)$ is the direct sum of the sub p-Lie algebras $\mathfrak{H}$ and $\mathfrak{F}$, where $\mathfrak{H}$ is the subalgebra with a basis $X_1, \cdots, X_f$ such that $X_1^p = X_1, \cdots, X_f^p = X_f$ and $\mathfrak{F}$ is pseudo-nilpotent, i.e. $\mathfrak{F}^{p^N} = 0$, for some integer $N \geqq 0$.*

REMARK. The above integer f is associated to A as follows:

(a) The order of the kernel of $p\delta_A$ is p^f.

(b) By J. Dieudonné, [**9**]. Let $\hat{A}$ be the completion of A, $t(A)$ its Lie algebra, $\mathfrak{H}$ the core and $\mathfrak{F}$ the p-radical of $t(A)$. Then $\mathfrak{H}$ has dimension f and $\hat{A}$ is isomorphic to the direct product of f groups isomorphic to $\hat{G}_m$ and of a group having $\mathfrak{F}$ as its Lie algebra. Here $\hat{G}_m$ is the completion of G_m and has the composition law, $(x, y) \rightarrow x+y+xy$.

LEMMA 2.2. *Let $\mathfrak{A}$ be a restricted abelian p-Lie algebra of one of the following types.*

(1) $\mathfrak{A}$: *pseudo-nilpotent, that is, there exists a positive integer N such that $\mathfrak{A}^{p^N} = 0$.*

(2) $\mathfrak{A}$: *restricted abelian p-Lie algebra generated by a basis $X_1, \cdots, X_f$ such that $X_1^p = X_1, \cdots, X_f^p = X_f$.*

Let $\mathfrak{B}$ be a restricted p-Lie algebra generated by only one element such that $Y^p = Y$. Then we have $\mathrm{Ext}\,(\mathfrak{B}, \mathfrak{A}) = 0$.

PROOF.

Case (1): Let $\mathfrak{C}$ be an element of $\mathrm{Ext}\,(\mathfrak{B}, \mathfrak{A})$, then a sequence $0 \longrightarrow \mathfrak{A} \longrightarrow \mathfrak{C} \xrightarrow{\varphi} \mathfrak{B} \longrightarrow 0$ is exact in the category of restricted p-Lie algebras. Take an element Z in $\mathfrak{C}$, such that $\varphi(Z) = Y$. As $\varphi(Z^p) = (\varphi(Z))^p = Y^p = Y = \varphi(Z)$, $Z^p - Z \in \mathfrak{A}$. Then $Z^{p^{N+1}} - Z^{p^N} = 0$. If we put $Z' = Z^{p^N}$, we have $Z'^p = Z'$, and $\varphi(Z') = \varphi(Z)^{p^N} = Y$. Then a map $\psi: \mathfrak{B} \rightarrow \mathfrak{C}$, determined by $\psi(Y) = Z'$ is a morphism and satisfies $\varphi \cdot \psi = id_{\mathfrak{B}}$. Hence, $\mathrm{Ext}\,(\mathfrak{B}, \mathfrak{A}) = 0$.

Case (2): Choose also an element Z in $\mathfrak{C}$ such that $\varphi(Z) = Y$. We can write

$$Z^p = Z + \alpha_1 X_1 + \cdots + \alpha_f X_f,\ \alpha_1, \cdots, \alpha_f \in k .$$

Put $Z' = Z + \beta_1 X_1 + \cdots + \beta_f X_f$. Here $\beta_1, \cdots, \beta_f$ are indeterminates. If $Z'^p = Z'$ is satisfied, then

$$Z'^p = Z^p + \beta_1^p X_1^p + \cdots + \beta_f^p X_f^p = Z + (\beta_1^p + \alpha_1) X_1 + \cdots + (\beta_f^p + \alpha_f) X_f$$
$$= Z' = Z + \beta_1 X_1 + \cdots + \beta_f X_f .$$

Hence, we have equations $\beta_i^p + \alpha_i = \beta_i$, $1 \leqq i \leqq f$. Since k is algebraically closed, the above equations can be solved in k. Therefore we can find an element Z' in $\mathfrak{C}$ such that $Z'^p = Z'$. We can define a morphism $\psi : \mathfrak{B} \to \mathfrak{C}$ by $\psi(Y) = Z'$. Hence, $\mathrm{Ext}(\mathfrak{B}, \mathfrak{A}) = 0$. q. e. d.

Taking account of the sequence (1) and Lemma 2.1, we have the following.

PROPOSITION 2.1. *For an abelian variety A and for the multiplicative group G_m, we have the following exact sequence of abelian groups,*

$$0 \longrightarrow \mathrm{Hom}(t(G_m), t(A)) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m^p, A) \xrightarrow{\varphi} \mathrm{Ext}_{\mathcal{A}}(G_m, A) \longrightarrow 0,$$

$\mathrm{Hom}(t(G_m), t(A))$ *being isomorphic to* $\bigoplus_{i=1}^{f} \mathbf{Z}/\mathrm{p}\mathbf{Z}$.

PROOF. The proof of the last assertion is left, but it is easily verified that $\mathrm{Hom}(t(G_m), t(A)) \cong \mathrm{Hom}(t(G_m), \mathfrak{H}) \cong \bigoplus_{i=1}^{f} \mathbf{Z}/p\mathbf{Z}$, because

$$\psi(Y^p) = (\psi(Y))^p \quad \text{for} \quad \psi \in \mathrm{Hom}(t(G_m), t(A)). \qquad \text{q. e. d.}$$

Now we shall consider the homomorphism $\varphi : \mathrm{Ext}_{\mathcal{A}}(G_m^p, A) \to \mathrm{Ext}_{\mathcal{A}}(G_m, A)$. Since G_m^p the image of the Frobenius endomorphism of G_m is identical with G_m, we can identify the Frobenius endomorphism with the multiplication of an element of G_m by itself p-times. Then we can assume φ the multiplication by p to elements of $\mathrm{Ext}_{\mathcal{A}}(G_m^p, A)$. We can apply the analogous argument for $G_m^{p^n}$ which is the image of n-iterated Frobenius endomorphism of G_m for a positive integer n. We have the following exact sequence,

$$0 \longrightarrow \bigoplus_{i=1}^{f} \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m^{p^{n+1}}, A) \xrightarrow{\varphi} \mathrm{Ext}_{\mathcal{A}}(G_m^{p^n}, A) \longrightarrow 0.$$

It is easy to show that the kernel of φ^n is isomorphic to $\bigoplus_{i=1}^{f} \mathbf{Z}/p^n\mathbf{Z}$. Therefore we have an exact sequence,

$$0 \longrightarrow \bigoplus_{i=1}^{f} \mathbf{Z}/p^n\mathbf{Z} \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m^{p^n}, A) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m, A) \longrightarrow 0.$$

Substituting G_m by $G_m^{p^{-n}}$, we have an exact sequence,

$$0 \longrightarrow \bigoplus_{i=1}^{f} \mathbf{Z}/p^n\mathbf{Z} \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m, A) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m^{p^{-n}}, A) \longrightarrow 0.$$

As the inductive limit is the exact functor in the category of abelian groups, finally we have an exact sequence,

$$0 \longrightarrow \varinjlim_n \bigoplus_{i=1}^{f} \mathbf{Z}/p^n\mathbf{Z} \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m, A) \longrightarrow \varinjlim_n \mathrm{Ext}_{\mathcal{A}}(G_m^{p^{-n}}, A) \longrightarrow 0.$$

LEMMA 2.3.

(1) *It is verified in J.P. Serre,* [**20**], *Proposition* 13, *that* $\mathrm{Ext}_{\mathcal{P}}(G_m, A) \cong \varinjlim_n \mathrm{Ext}_{\mathcal{A}}(G_m^{p^{-n}}, A)$.

(2) *By the property of an abelian variety,*

$$A_{[p]}=\varinjlim_{n}\bigoplus_{i=1}^{f}\mathbf{Z}/p^n\mathbf{Z}\,.$$

Therefore we have an exact sequence,

$$0\longrightarrow A_{[p]}\longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_m, A)\longrightarrow \mathrm{Ext}_{\mathcal{P}}(G_m, A)\longrightarrow 0\,.$$

However, as $A_{[p]}$ is a p-torsion group and $\mathrm{Ext}_{\mathcal{P}}(G_m, A)$ has no p-torsion, we have, $\mathrm{Ext}_{\mathcal{A}}(G_m, A)\cong A_{[p]}\oplus \mathrm{Ext}_{\mathcal{P}}(G_m, A)$. By virtue of Thorem 1.1 of § 1, we have:

THEOREM 2.1. $\mathrm{Ext}_{\mathcal{A}}(G_m, A)\cong \bigoplus_{l:\text{ prime}} A_{[l]}$, *where l runs over all positive prime numbers.*

REMARK. (1) Any extension G of G_m by A is isogenous to $A\times G_m$.

(2) Let G be an extension of A by G_m. If G has the maximal abelian subvariety isogenous to A, G is isogenous to the direct product $A\times G_m$. Then the isomorphism class to which G belongs is a torsion element in $\mathrm{Ext}_{\mathcal{A}}(A, G_m)$. Conversely any extension $G\in \mathrm{Ext}_{\mathcal{A}}(A, G_m)$ of which class is a torsion element has the maximal abelian subvariety isogenous to A.

Chapter III. On $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$.

§ 1. On $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$.

1. Let A be an abelian variety. For any $\lambda\in k$, we denote by λ the multiplication $x\rightarrow\lambda x$, for $x\in k$. We know that the Frobenius endomorphism $\boldsymbol{p}$ of G_a is identified with the endomorphism of $G_a: x\rightarrow x^p$. Then if we associate to any extension $G\in \mathrm{Ext}_{\mathcal{A}}(G_a, A)$ (resp. $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$) the extensions $\lambda^*G, \boldsymbol{p}^*G\in \mathrm{Ext}_{\mathcal{A}}(G_a, A)$ (resp. $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$), with these operations, $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ (resp. $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$) is considered an abelian p^{-1}-Lie algebra over k. And the map $\rho: \mathrm{Ext}_{\mathcal{A}}(G_a, A)\rightarrow \mathrm{Ext}_{\mathcal{P}}(G_a, A)$ defined in Chapter I, § 3, 5, is a homomorphism of p^{-1}-Lie algebras.

2. We shall use the notations of § 3, Chapter I. Let g be k-cochain on $\hat{G}_a$ with values in $\hat{A}$ and let $x^{(1)}, \cdots, x^{(k)}$, be independent indeterminates. If we associate to g a system of formal power series $g'=(g'_j)_{1\leqq j\leqq n}$ such that

$$g'_j(x^{(1)}, \cdots x^{(k)})=g_j(\lambda x^{(1)}, \cdots, \lambda x^{(k)})\,,\qquad 1\leqq j\leqq n\,,\qquad \lambda\in k\,,$$

then g' is also k-cochain $\in C^k(\hat{G}_a, \hat{A})$ which we denote by λg. It is trivial that if g is k-cocycle (resp. k-coboundary), then g' is k-cocycle (resp. k-coboundary). Hence the definition of the scalar multiplication on $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$. If we associate to g a system of formal power series $g''=(g''_j)_{1\leqq j\leqq n}$ defined by

$$g''_j(x^{(1)}, \cdots, x^{(k)})=g_j((x^{(1)})^p, \cdots, (x^{(k)})^p)\,,\qquad 1\leqq j\leqq n\,,$$

g'' is also k-cochain $\in C^k(\hat{G}_a, \hat{A})$, which we denote by $g^{(p)}$. And if $g \in Z^k(\hat{G}_a, \hat{A})$ (resp. $B^k(\hat{G}_a, \hat{A})$), then $g^{(p)} \in Z^k(\hat{G}_a, \hat{A})$ (resp. $B^k(\hat{G}_a, \hat{A})$). Therefore, there exists the mapping $p^*: \mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A}) \to \mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$. This mapping p^* is p^{-1}-semi-linear with respect to the above-defined structure of k-vector space on $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$. Therefore we can consider $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$ an abelian p^{-1}-Lie algebra. Then the map $\sigma: \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to \mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$ is a homomorphism of p^{-1}-Lie algebras.

3. First, we recall the next results.

LEMMA 1.1. (J. P. Serre, [**20**].) *Let $\overline{G}_a$ and $\overline{W}$ be the universal coverings of G_a and W, the Witt group of infinite length. Then we have the following results.*

(1) *There is an exact sequence in $\mathcal{P}$,*

$$0 \longrightarrow \overline{W} \xrightarrow{\bar{p}} \overline{W} \longrightarrow \overline{G}_a \longrightarrow 0, \tag{1}$$

where $\bar{p}$ is the morphism induced by the multiplication by p on W.

(2) *$\overline{W}$ is projective in $\mathcal{P}$. Moreover, we have the exact sequence in $\mathcal{P}$,*

$$0 \longrightarrow \pi_1(G_a) \longrightarrow \overline{G}_a \longrightarrow G_a \longrightarrow 0. \tag{2}$$

By virtue of the sequences (1), (2), for an abelian variety A, we have,

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\overline{G}_a, A) \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\pi_1(G_a), A) \longrightarrow \mathrm{Ext}_{\mathcal{P}}(G_a, A) \longrightarrow \mathrm{Ext}_{\mathcal{P}}(\overline{G}_a, A),$$

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\overline{G}_a, A) \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\overline{W}, A) \longrightarrow \mathrm{Hom}_{\mathcal{P}}(\overline{W}, A) \longrightarrow \mathrm{Ext}_{\mathcal{P}}(\overline{G}_a, A)$$
$$\longrightarrow \mathrm{Ext}_{\mathcal{P}}(\overline{W}, A).$$

Here we have used the fact that $\mathrm{Hom}_{\mathcal{A}}(G_a, A) = 0$, and that

$$\mathrm{Hom}_{\mathcal{P}}(G_a, A) = \varinjlim_n \mathrm{Hom}_{\mathcal{A}}(G_a^{p^{-n}}, A).$$

As G_a and W are linear and A is complete, we have $\mathrm{Hom}_{\mathcal{P}}(\overline{G}_a, A) = \mathrm{Hom}_{\mathcal{P}}(\overline{W}, A) = 0$, by the same argument in Chapter II, § 1. Moreover $\mathrm{Ext}_{\mathcal{P}}(\overline{W}, A) = 0$, by virtue of Lemma 1.1, (2). Therefore we have:

PROPOSITION 1.1.

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_a), A) \cong \mathrm{Ext}_{\mathcal{P}}(G_a, A) (\equiv \varinjlim_n \mathrm{Ext}_{\mathcal{A}}(G_a^{p^{-n}}, A)).$$

4. Let $\mathcal{P}_0$ be the subcategory of $\mathcal{P}$ formed by groups of dimension zero, i.e. profinite groups. If to $G \in \mathcal{P}_0$, we associate $\check{G} = \mathrm{Hom}_{\mathcal{P}}(G, \mathbf{Q}/\mathbf{Z})$ $(\equiv \varinjlim_n \mathrm{Hom}_{\mathcal{P}}(G, \mathbf{Z}/n\mathbf{Z}))$, then $G \rightsquigarrow \check{G}$ is a contravariant functor from $\mathcal{P}_0$ to the category $\mathcal{T}$ of abelian groups of torsion.

LEMMA 1.2. (J. P. Serre, [**20**].) *The above functor $G \rightsquigarrow \check{G}$ determines an equivalence between the dual category of $\mathcal{P}_0$ and $\mathcal{T}$.*

LEMMA 1.3. (J. P. Serre, [20].) *The group* $\pi_1(G_a)$ *is isomorphic to the group* $\mathrm{Hom}_{\mathcal{T}}(k, \mathbf{Z}/p\mathbf{Z})$ *with the simple convergence topology, (k is endowed with the discrete topology).*

THEOREM 1.1. *Let A be an abelian variety defined over the ground field k. Then* $\mathrm{Ext}_{\mathcal{P}}(G_a, A) \cong \bigoplus_{i=1}^{f} k$, *that is, k-vector space of dimension f where f is characterized in Chapter II.*

PROOF. By Lemma 1.1, $\mathrm{Ext}_{\mathcal{P}}(G_a, A) \cong \mathrm{Hom}_{\mathcal{P}}(\pi_1(G_a), A)$. By Lemma 1.3,

$$\mathrm{Hom}_{\mathcal{P}}(\pi_1(G_a), A) \cong \mathrm{Hom}_{\mathcal{P}}(\mathrm{Hom}(k, \mathbf{Z}/p\mathbf{Z}), A) \cong \mathrm{Hom}_{\mathcal{P}}(\mathrm{Hom}(k, \mathbf{Z}/p\mathbf{Z}), A_p)$$

$$\cong \mathrm{Hom}_{\mathcal{P}}(\mathrm{Hom}(k, \mathbf{Z}/p\mathbf{Z}), \bigoplus_{i=1}^{f} \mathbf{Z}/p\mathbf{Z}) \cong \bigoplus_{i=1}^{f} k,$$

where A_p means the set of elements a of A such that $pa=0$.

§ 2. Some results.

1. Now we shall apply the exact sequence of Proposition 1.3 in Chapter I. Then we have,

$$0 \longrightarrow \mathrm{Hom}(t(G_a), t(A)) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_a^p, A) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_a, A) \longrightarrow \mathrm{Ext}(t(G_a), t(A)).$$

Here $t(G_a)$ is the restricted abelian p-Lie algebra generated by $X\left(\equiv \frac{\partial}{\partial x}\right)$ over k such that $X^p=0$. As there is p-operation (we denote it simply by p) in $t(A)$ (i.e. $X \in t(A) \to X^p \in t(A)$), we shall denote by $P(t(A))$ (resp. $Q(t(A))$) the kernel (resp. the cokernel) of p-operation. We have considered in Chapter II the decomposition $t(A) \cong \mathfrak{H} \oplus \mathfrak{F}$, $\mathfrak{H}$ being generated by elements $Y_1, \cdots, Y_f$ such that $Y_1^p = Y_1, \cdots, Y_f^p = Y_f$ and $\mathfrak{F}$ being pseudo-nilpotent (i.e. for some integer $N \geqq 0$, $\mathfrak{F}^{p^N}=0$). Thence, $P(t(A))$ (resp. $Q(t(A))$) is the kernel (resp. the cokernel) of the restriction of p-operation on $\mathfrak{F}$.

2. LEMMA 2.1.

(1) $\mathrm{Hom}(t(G_a), t(A)) \cong P(t(A))$,

(2) $\mathrm{Ext}(t(G_a), t(A)) \cong Q(t(A))$.

PROOF. (1) is trivial. (2) As $t(A) \cong \mathfrak{H} \oplus \mathfrak{F}$, and $\mathrm{Ext}(t(G_a), \mathfrak{H})=0$, (the proof is easy), we have $\mathrm{Ext}(t(G_a), t(A)) \cong \mathrm{Ext}(t(G_a), \mathfrak{F})$. Let $\mathfrak{A}$ represent an element of $\mathrm{Ext}(t(G_a), \mathfrak{F})$. Then

$$0 \longrightarrow \mathfrak{F} \longrightarrow \mathfrak{A} \xrightarrow{\varphi} t(G_a) \longrightarrow 0,$$

hence $\mathfrak{A} \cong t(G_a) \oplus \mathfrak{F}$ as k-vector spaces. If $\mathfrak{A}$ is not trivial, for $Z \in \mathfrak{A}$ such that $\varphi(Z) = X(\in t(G_a))$, $Z^p \notin \mathfrak{F}^p$. If so, there exists $Y \in \mathfrak{F}$ and $Y^p = Z^p$. Putting $Z' = Z - Y$, $Z'^p = 0$ and $\varphi(Z') = X$. Hence the triviality of $\mathfrak{A}$. This contradicts the assumption. The class Z^p modulo $\mathfrak{F}^p$ depends only on the isomorphism class of $\mathfrak{A}$, and the map $\mathfrak{A} \to Z^p$ determines an injective homomorphism from

$\mathrm{Ext}\,(t(G_a), \mathfrak{F})$ to $Q(\mathfrak{F})$ $(\cong \mathfrak{F}/\mathfrak{F}^p)$. Conversely this homomorphism is surjective. Let $Y \in \mathfrak{F}$ represent a class of $Q(\mathfrak{F})$. Putting $\mathfrak{A} = \mathfrak{F} + k\cdot Z$, $Z^p = Y$, $\varphi(Z) = X$, $\mathfrak{A}$ is an extension of $t(G_a)$ by $\mathfrak{F}$. Therefore we have obtained the exact sequence,

$$0 \longrightarrow P(t(A)) \longrightarrow \mathrm{Ext}_{\mathcal{A}}(G_a^p, A) \xrightarrow{\ \boldsymbol{p}^*\ } \mathrm{Ext}_{\mathcal{A}}(G_a, A) \xrightarrow{\ \theta\ } Q(t(A))\,.$$

3. REMARK. Later, we shall see that the dimension of k-vector space $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ is equal to the dimension of A. If we know the finiteness of the dimension of k-vector space $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$, we can conclude that θ is surjective. $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ is considered as the p^{-1}-Lie algebra with p^{-1}-semi-linear operation $\boldsymbol{p}^*$. The above exact sequence shows that the k-dimension of the cokernel of $\boldsymbol{p}^*$ of $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ is equal to the k-dimension of $P(t(A))$. On the other hand, the k-dimension of $P(t(A))$ is equal to the k-dimension of $Q(t(A))$, because the k-dimension of $t(A)$ is finite. Therefore the homomorphism $\theta: \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to Q(t(A))$ is surjective.

§ 3. The decomposition.

$$\mathrm{Ext}_{\mathcal{A}}(G_a, A) \cong \mathrm{Ext}_{\mathcal{P}}(G_a, A) \oplus \mathrm{Ext}_{\mathcal{T}}(\hat{G}_a, \hat{A})\,.$$

1. Let B, C be group-varieties isogenous to a group-variety A and let $\varphi: B \to A$, $\psi: C \to A$ be their isogenies. We denote by D the connected component $(B \times_A C)_0$, where the fibre product is taken in the category $\mathcal{A}$, and by π the composition $D \to B \xrightarrow{\varphi} A$ (or $D \to C \xrightarrow{\psi} A$),

$$\begin{array}{ccc} D & \longrightarrow & C \\ \downarrow & \searrow^{\pi} & \downarrow \psi \\ B & \underset{\varphi}{\longrightarrow} & A\,. \end{array}$$

Then we have the following:

LEMMA 3.1. *If φ and ψ are separable (resp. purely inseparable) then π is also separable (resp. purely inseparable).*

We omit the proof.

LEMMA 3.2. (By I. Barsotti, [1].) *Let A be a group-variety, and let α be a homomorphism of positive degree. Then α is a lowest common multiple of two homomorphisms α_s and α_i which are respectively separable and purely inseparable. A highest common divisor of α_s and α_i is the identity δ_A of A. The equivalence classes to which α_s and α_i belong are uniquely determined by the class to which α belongs. In addition, if we write $\alpha = \beta_i\alpha_s = \beta_s\alpha_i$ β_i is purely inseparable and β_s is separable.*

We omit the proof.

2. Let α be an isogeny of G_a. Then, taking a generic point x of G_a

over k, α can be written in the form, $\alpha(x)=a_s x^{p^s}+a_{s+1}x^{p^{s+1}}+\cdots+a_t x^{p^t}$, for some integers $s, t\geqq 0$ and for $a_s, \cdots, a_t \in k$ such that $a_s \neq 0$. Then writing $a_s=(b_s)^{p^s}$, $a_{s+1}=(b_{s+1})^{p^s}$, $\cdots$, $a_t=(b_t)^{p^s}$, $b_s, \cdots, b_t \in k$, $\alpha(x)=a_s(x^{p^s})+a_{s+1}(x^{p^s})^p+\cdots+a_t(x^{p^s})^{p^{t-s}}=(b_s x+\cdots+b_t x^{p^{t-s}})^{p^s}$. From the above equations, we know that α is decomposed to $\alpha=\alpha_s\cdot\alpha_i$, where $\alpha_i(x)=x^{p^s}$, $\alpha_s(x)=a_s x+\cdots+a_t x^{p^{t-s}}$, or to $\alpha=\beta_i\cdot\beta_s$, where $\beta_s(x)=b_s x+\cdots+b_t x^{p^{t-s}}$, $\beta_i(x)=x^{p^s}$. There α_i, β_i are purely inseparable, and α_s, β_s are separable. Therefore we see that as a purely inseparable isogeny of G_a, we can take no homomorphism but iteration of the Frobenius endomorphism $\boldsymbol{p}$.

3. Let A, B be connected commutative algebraic groups, and G be an extension of A by B. Let $\varphi: A'\to A$ be an isogeny. Putting $G'=\varphi^*(G)$, it is evident that G' is an isogeny of G. More precisely, we have the following results.

LEMMA 3.3.

(1) *If φ is separable, then the induced homomorphism $\psi: G'\to G$ by φ is also separable.*

(2) *If φ is purely inseparable and of height 1, then $\psi: G'\to G$ is also purely inseparable and of height 1.*

PROOF.

(1) We have the following commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & t(B) & \longrightarrow & t(G') & \longrightarrow & t(A') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id.} & & \downarrow{\scriptstyle t(\psi)} & & \downarrow{\scriptstyle t(\varphi)} & & \\ 0 & \longrightarrow & t(B) & \longrightarrow & t(G) & \longrightarrow & t(A) & \longrightarrow & 0. \end{array}$$

As φ is separable, $t(\varphi): t(A')\to t(A)$ is an isomorphism. Therefore $t(\psi): t(G')\to t(G)$ is also an isomorphism. Hence, ψ is separable.

(2) Since φ is a purely inseparable isogeny of height 1, A is characterised by a sub p-Lie algebra $\mathfrak{N}$ of $t(A')$. We have the following commutative diagram,

$$\begin{array}{ccccccccc} & & & & \mathfrak{M} & \longrightarrow & \mathfrak{N} & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & t(B) & \longrightarrow & t(G') & \longrightarrow & t(A') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id.} & & \downarrow{\scriptstyle t(\psi)} & & \downarrow{\scriptstyle t(\varphi)} & & \\ 0 & \longrightarrow & t(B) & \longrightarrow & t(G) & \longrightarrow & t(A) & \longrightarrow & 0, \end{array}$$

where $\mathfrak{M}$ is the kernel of $t(\psi)$. From this diagram, $\mathfrak{M}\cong\mathfrak{N}$. We can construct a purely inseparable isogeny of height 1 $G'/\mathfrak{M}$ of G' by the sub p-Lie algebra $\mathfrak{M}$ of $t(G')$. Then from the commutative diagram,

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & B & \longrightarrow & G' & \longrightarrow & A' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id.} & & \downarrow{\scriptstyle \psi'} & & \downarrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & B & \longrightarrow & G'/\mathfrak{M} & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id.} & & \downarrow{\scriptstyle \psi''} & & \downarrow{\scriptstyle id.} & & \\
0 & \longrightarrow & B & \longrightarrow & G & \longrightarrow & A & \longrightarrow & 0\,.
\end{array}
$$

where $\psi'' \cdot \psi' = \psi$, we obtain that $G'/\mathfrak{M} \cong G$. Therefore G is a purely inseparable isogeny of height 1. q. e. d.

4. Let G be an extension of G_a by A, where A is an abelian variety, and let L be the maximal connected linear subgroup of G. Then $L \cong G_a$, $A \cap L =$ finite group, and $G = A \cdot L$. Therefore there exists an isogeny $\psi : A \times G_a \to G$. We have the following commutative diagram,

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & A \times G_a & \longrightarrow & G_a & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id.} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & G_a & \longrightarrow & 0
\end{array}
$$

where φ is the isogeny induced by ψ. From this diagram, we know that $\varphi^* G = 0$, for $\varphi^* : \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to \mathrm{Ext}_{\mathcal{A}}(G_a, A)$.

DEFINITION[1]. We call G an extension of *separable* type (resp. *purely inseparable* type) if there exists a separable (resp. purely inseparable) isogeny φ such that $\varphi^* G \cong A \times G_a$. We shall denote by E_s (resp. E_i) the set of classes of extensions of separable type (resp. purely inseparable type). Then by Lemma 3.1, E_s and E_i are k-vector spaces of $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$, and by Lemma 3.2, $\boldsymbol{p}^*(E_s) \subset E_s$ and $\boldsymbol{p}^*(E_i) \subset E_i$. It is easily shown that the restriction of $\boldsymbol{p}^*$ on E_s is injective, that is, $E_s \cap E_i = (0)$. Hence $E_s \oplus E_i$ is the vector subspace of $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ closed with respect to $\boldsymbol{p}^*$. On the other hand, $\boldsymbol{p}^*$ is a p^{-1}-semi-linear map on $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$ and $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$, where $p^{-1} : \lambda \in k \to \lambda^{p^{-1}} \in k$. It is evident from the definition that $\boldsymbol{p}^*$ is p^{-1}-semi-linear automorphism on $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$. We have already remarked that the map $\rho : \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to \mathrm{Ext}_{\mathcal{P}}(G, A)$ is the homomorphism of p^{-1}-Lie algebras, i. e. $\rho \cdot \boldsymbol{p}^* = \boldsymbol{p}^* \cdot \rho$.

LEMMA 3.4. *The restriction of $\boldsymbol{p}^*$ on E_s is a p^{-1}-semi-linear automorphism.*

PROOF. See the Appendix.

THEOREM 3.1.

(1) $\mathrm{Ext}_{\mathcal{A}}(G_a, A) \cong E_s \oplus E_i$.

(2) $E_s \cong \mathrm{Ext}_{\mathcal{P}}(G_a, A)$.

PROOF. If $\varphi^* G = 0$, by Lemma 3.2, we can write $\varphi = \boldsymbol{p}^\nu \cdot \varphi_s$, for some integer $\nu \geqq 0$ and some separable isogeny φ_s. Putting $G' = (\boldsymbol{p}^*)^\nu \cdot G$ and $G'' = G - ((\boldsymbol{p}^* | E_s)^{-\nu} \cdot (\boldsymbol{p}^*)^\nu G)$, G' is an extension of separable type and G'' is an ex-

1) This definition is due to H. Matsumura.

tension of purely inseparable type. Hence $\mathrm{Ext}_{\mathcal{A}}(G_a, A) \cong E_s \oplus E_i$. Since the kernel of the homomorphism $\rho: \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to \mathrm{Ext}_{\mathcal{P}}(G_a, A)$ is E_i (the proof is easy), and since $\rho(E_s) = \mathrm{Ext}_{\mathcal{P}}(G_a, A)$, we know that $\rho | E_s$ is the isomorphism onto $\mathrm{Ext}_{\mathcal{P}}(G_a, A)$. q. e. d.

5. Let $u: B \to A$ be an isogeny. Then we can assume $\mathcal{O}_A \subset \mathcal{O}_B$ as prescribed by u^* and $k(B)$ is a finite algebraic extension of $k(A)$. With this situation, we have the following lemma.

LEMMA 3.5.

(1) *If u is separable, then $k\{A\} \cong k\{B\}$. Therefore the completions $\hat{A}$ and $\hat{B}$ are isomorphic.*

(2) *If u is purely inseparable, then $[k(B): k(A)]_i = [k\{B\} : k\{A\}]_i$.*

We omit the proof.

The next lemma is proved in the paper of Ju. I. Manin, [**14**].

LEMMA 3.6. *Let $\hat{B}$ be the completion of an algebraic group B and let $\varphi: \hat{B} \to G$ be an isogeny of formal groups. Then there exists an isogeny $f: B \to A$ of algebraic groups such that G is isomorphic to the completion $\hat{A}$ of A and φ is isomorphic to the completion of f.*

Let A be an abelian variety. We have defined the p^{-1}-semi-linear homomorphism $\sigma: \mathrm{Ext}_{\mathcal{A}}(G_a, A) \to \mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$ which commutes with $\boldsymbol{p}^*$, i. e. $\sigma \cdot \boldsymbol{p}^* = \boldsymbol{p}^* \cdot \sigma$.

Then we have the following results.

THEOREM 3.2.

(1) $\sigma(E_s) = 0$.

(2) *The restriction of σ on E_i is the isomorphism onto* $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A})$.

PROOF. (1) follows from the definition of E_s and Lemma 3.5, (1). As for (2), first, we prove the injectivity. Let G be an extension of which class belongs to E_i and of which completion $\hat{G}$ is trivial,

$$0 \longrightarrow A \xrightarrow{\beta} G \xrightarrow{\alpha} G_a \longrightarrow 0 .$$

Let L be the maximal connected linear subgroup of G. Then $L \cong G_a$, and the restriction α' of α on L is a purely inseparable isogeny of order p^ν, for some integer $\nu \geqq 0$. From the assumption, the completion is isomorphic to $\hat{A} \times \hat{G}_a$, and $\hat{G}_a \cong \hat{L} \subset \hat{G}$. However, as there is no subgroup isogenous to $\hat{G}_a$ in $\hat{A}$, $\hat{L}$ is embedded into $\hat{A} \times \hat{G}_a$ in the form, $x \to (0, x)$. Since the completion $\hat{\alpha}$ is given by $(y, x) \to x$, the order of inseparability p^ν is equal to 1 by Lemma 3.5, (2). Therefore α' is isomorphism, hence the triviality of G.

Next, we prove the surjectivity. Let G^* be an extension in $\mathcal{F}$ of $\hat{G}_a$ by $\hat{A}$. Then from the theory of Dieudonné modules, we know G^* is isogenous to the direct product $\hat{A} \times \hat{G}_a$. Hence the existence of an isogeny $\varphi: \hat{A} \times \hat{G}_a \to G^*$.

As $\varphi(\hat{G}_a)\cong\hat{G}_a$, there exists the maximal unipotent subgroup H^* of G^*, H^* being isomorphic to $\hat{G}_a$. It is easy to see that $H^*\vee\hat{A}=G^*$ and $H^*\wedge\hat{A}=(0)$, following the notation of J. Dieudonné, [10]. Therefore we have the commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{A} & \longrightarrow & \hat{A}\times\hat{G}_a & \longrightarrow & \hat{G}_a & \longrightarrow & 0 \\ & & \downarrow id. & & \downarrow \psi & & \downarrow & & \\ 0 & \longrightarrow & \hat{A} & \underset{\beta^*}{\longrightarrow} & G^* & \underset{\alpha^*}{\longrightarrow} & \hat{G}_a & \longrightarrow & 0. \end{array}$$

By Lemma 3.6, there exist an algebraic group G and an isogeny $f: A\times G_a\rightarrow G$ such that $G^*=\hat{G}$, and $\psi=\hat{f}$. If we write $f=f_s\cdot f_i$, where f_s is separable and f_i is purely inseparable, then $\hat{f}\cong\hat{f}_i\cong\psi$. Therefore, we can suppose that f is purely inseparable. If we define β by the composition $A\rightarrow A\times G_a\xrightarrow{f}G$, then $\beta^*=\hat{\beta}$. Denoting by $t(G^*)$ ($t(\hat{A})$ etc.) the Lie algebra of derivations on G^* ($\hat{A}$ etc.), the homomorphism

$$t(\beta^*):\ t(\hat{A})\rightarrow t(G^*) \text{ is injective}.$$

As $t(\hat{A})\cong t(A)$ and $t(G^*)\cong t(G)$, the induced homomorphism

$$t(\beta):\ t(A)\rightarrow t(G) \text{ is injective}.$$

Hence β is separable. If we define α as the canonical projection from G to $G/A\cong G_a$, then $\hat{\alpha}\cong\alpha^*$. Hence the surjectivity of σ. q. e. d.

COROLLARY.

$$\mathrm{Ext}_{\mathcal{A}}(G_a, A)\cong\mathrm{Ext}_{\mathcal{P}}(G_a, A)\oplus\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A}).$$

§ 4. On $\mathrm{Ext}_{\mathcal{A}}(G_a, A)$.

1. In the following, we shall use the terminology of Ju. I. Manin, [14]. He defines a formal k-scheme as a formal spectrum Spf(A), where A is non-zero local ring with the residue field k and admits nilpotent elements, and defines a formal k-group as a group object in the category of formal k-schemes. Here we will consider only commutative formal groups, so we omit the adjective "commutative". All formal k-groups form an abelian category $\tilde{\mathcal{F}}$. In $\tilde{\mathcal{F}}$, all reduced formal k-groups form a full subcategory, which is identified with the category $\mathcal{F}$ of formal Lie groups defined over k which was first given by J. Dieudonné [8]. $\mathcal{F}$ is not abelian. $\tilde{\mathcal{F}}$ is equivalent to the product of the category of torus groups and the category $\mathcal{D}$ of Dieudonné groups. And each torus group defined over an algebraically closed field k is isomorphic to the subgroup of the direct product of a finite number of multiplicative groups. Especially, any reduced torus group is isomorphic to the direct product of a finite number of multiplicative groups. On the other hand, the dual category $\mathcal{D}^0$ is equivalent to the category $\mathcal{DM}$ of Dieudonné modules, where the equivalence is given by the functor $G \in \mathcal{D} \rightsquigarrow \mathrm{Hom}_{\tilde{\mathcal{F}}}(G, I)$ for the injective envelope I of the simple object of $\tilde{\mathcal{F}}$,

$$S = \mathrm{Spec}\,(k[x]/(x^p))\,, \qquad \triangle x = x \otimes 1 + 1 \otimes x\,.$$

It is easy to see, for any $G, H \in \mathcal{F}$, $\mathrm{Ext}_{\tilde{\mathcal{F}}}(G, H) \cong \mathrm{Ext}_{\mathcal{F}}(G, H)$. We denote by $M(G)$ the Dieudonné module corresponding to $G \in \tilde{\mathcal{F}}$. It is proved that a group $G \in \tilde{\mathcal{F}}$ is *reduced* if and only if for $x \in M(G)$, the equality $Fx = 0$ means $x = 0$. Then we have the following:

PROPOSITION 4.1.

(1) $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_m) = 0$.

(2) *For* $G, H \in \tilde{\mathcal{F}}$, $\mathrm{Ext}_{\tilde{\mathcal{F}}}(G, H) \cong \mathrm{Ext}_{\mathcal{DM}}(M(H), M(G))$.

Let A be an abelian variety defined over k. A can be written $A = (\hat{G}_m)^f \cdot G$ *where G is a Dieudonné group (or coreless group by J. Dieudonné). Then* $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A}) = \mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, G)$. *Therefore we can assume that A is a coreless group. With this assumption* $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{A}) \cong \mathrm{Ext}_{\mathcal{DM}}(M(A), E/EV)$, *where* $E/EV \cong M(\hat{G}_a)$.

2. We shall determine the dimension of the k-vector space $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, G_{n,m})$ where $nm > 0$. $G_{n,m}$, $nm > 0$ is a formal group of dimension n characterized by the Dieudonné module $E/E(V^n - F^m)$. If $(n, m) = 1$, then $G_{n,m}$ is a simple formal group. As we have shown, $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, G_{n,m}) \cong \mathrm{Ext}_{\mathcal{DM}}(E/E(V^n - F^m), E/EV)$. Let M be a Dieudonné module of which isomorphism class belongs to $\mathrm{Ext}_{\mathcal{DM}}(E/E(V^n - F^m), E/EV)$,

$$0 \longrightarrow E/EV \longrightarrow M \xrightarrow{\ \varphi\ } E/E(V^n - F^m) \longrightarrow 0\,. \qquad (1)$$

As left E-module, $E/E(V^n - F^m)$ is generated by an element x over E. Let z be an element of M such that $\varphi(z) = x$. Then $\varphi((V^n - F^m) \cdot z) = (V^n - F^m) \cdot \varphi(z) = (V^n - F^m) \cdot x = 0$. Hence, $(V^n - F^m) \cdot z \in E/EV$. E/EV is also generated by an element y over E such that $V \cdot y = 0$. If $(V^n - F^m) \cdot z = F^m \cdot y'$, for $y' \in E/EV$, tnen $(V^n - F^m) \cdot z = (V^n - F^m)(-y')$. Hence $(V^n - F^m)(z + y') = 0$. If we define a homomorphism $\psi : E/E(V^n - F^m) \to M$ by $\psi(x) = z + y'$, then $\varphi \cdot \psi = 1$. Therefore the sequence (1) splits. If (1) does not split, $(V^n - F^m) \cdot z$ modulo $F^m(E/EV)$ is not zero. Conversely, let y' be an element of E/EV such that y' modulo $F^m(E/EV)$ is not zero. Then if we define $M \cong E \cdot z + E \cdot y'$ and $\varphi(z) = x$, where z satisfies $(V^n - F^m) \cdot z = y'$, M defines an extension of $E/E(V^n - F^m)$ by E/EV. As $E/(EV + EF^m) \cong k + kF + \cdots + kF^{m-1}$, we have the isomorphism of k-vector spaces,

$$\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, G_{n,m}) \cong \mathrm{Ext}_{\mathcal{DM}}(E/E(V^n - F^m), E/EV) \cong k + kF + \cdots + kF^{m-1}.$$

Hence

$$\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G_{n,m}) = m\,.$$

Thus we have proved:

PROPOSITION 4.2. *For a formal group $G_{n,m}$, $nm > 0$,*

$$\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G_{n,m}) = m\,.$$

3. We shall apply this result for one-dimensional formal groups, digressing from our main subject. We know by J. Dieudonné that any one-dimensional formal group is isomorphic to one of $G_{1,m}$, $0 \leqq m \leqq \infty$. Here $G_{1,0} \cong \hat{G}_m$ and $G_{1,\infty} \cong \hat{G}_a$. The Dieudonné module corresponding to $G_{1,m}$ $(0 < m < \infty)$ is $E/E(V-F^m)$, and the Dieudonné module corresponding to $G_{1,\infty} \cong \hat{G}_a$ is E/EV. From the above consequence, we know that $\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G_{1,m}) = m$, above all, that $\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_a) = \infty$ and $\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_m) = 0$.

COROLLARY. *For any one-dimensional abelian variety A,*

$$\dim_k \operatorname{Ext}_{\mathcal{A}}(G_a, A) = 1\,.$$

PROOF. From Ju. I. Manin, [**14**], p. 71, Corollary, we know that all equidimensional formal groups of the form $kG_{n,m}$, where $nm > 1$, are not algebraizable. As for $G_{1,1}$, it is representable as $G_{1,1} \cong \hat{X}$, where X is an elliptic curve with vanishing Hasse invariant. If the Hasse invariant is different from zero, then $\hat{X} \cong G_{1,0} \cong \hat{G}_m$. Hence the requirement. q. e. d.

We can give more precise description of $\operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_a)$. We shall use the results by M. Lazard, [**22**]. For all integer $q \geqq 2$, we denote by $B_q(x, y)$ the polynomial

$$B_q(x, y) = (x+y)^q - x^q - y^q\,.$$

And for all integer $q \geqq 2$, we denote by $C_q(x, y)$ the polynomial: $C_q(x, y) = B_q(x, y)$, if q can not be written in the form $q = p^h$, for any prime number $p > 0$ and any positive integer h, and $C_q(x, y) = \frac{1}{p} B_q(x, y)$, if $q = p^h$ for some prime number p and some integer $h > 0$.

LEMMA 4.1. (M. Lazard.) *For all integer $q \geqq 2$, let $P(x, y) \in k[x, y]$ be a homogeneous polynomial of total degree q satisfying,*

(1) $\delta P(x, y, z) = P(y, z) - P(x+y, z) + P(x, y+z) - P(x, y) = 0$,

(2) $P(x, y) - P(y, x) = 0$.

Then $P(x, y)$ is the polynomial of the form $a \cdot C_q(x, y)$ for $a \in k$.

As $\operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_a) = H^2(\hat{G}_a, \hat{G}_a)_s = Z^2(\hat{G}_a, \hat{G}_a)_s / B^2(\hat{G}_a, \hat{G}_a)_s$, let $g(x, y) \in k[[x, y]]$ be an element of $Z^2(\hat{G}_a, \hat{G}_a)_s$. Then it is easy to see that for $q \geqq 2$, the q-homogeneous part $g_q(x, y)$ of $g(x, y)$ satisfies the conditions (1), (2) of Lemma 4.1, and that $g(x, y)$ has no 1-homogeneous term. Therefore $g(x, y)$ can be written in the form,

$$g(x, y)=\sum_{q\geqq 2}^{\infty} a_q C_q(x, y) \qquad \text{for} \quad a_q \in k\,.$$

If q can not be written in the form $q=p^h$, for some integer $h>0$, where p is the characteristic of k,

$$C_q(x, y)\in B^2(\hat{G}_a, \hat{G}_a)_s\,.$$

Therefore

$$P(x, y)\equiv \sum_{h=1}^{\infty} a_h C_{p^h}(x, y) \ (\text{mod. } B^2(\hat{G}_a, \hat{G}_a)_s)\,.$$

PROPOSITION 4.3. *The k-vector space $\mathrm{Ext}_{\mathcal{F}}(\hat{G}_a, \hat{G}_a)$ has a k-base formed by isomorphism classes of groups which are determined corresponding to $C_{p^h}(x, y)$ where $h=1, 2, \cdots$.*

4. In the category of Dieudonné modules $\mathcal{DM}$, E is a projective object. We shall consider the projective resolutions of $E/E(V^n-F^m)$ and of $E/(EV+EF)$ in $\mathcal{DM}$. We have the following results.

LEMMA 4.2. *The following sequences are exact,*

$$(1)\quad 0\longrightarrow E \xrightarrow{(V^n-F^m)} E\longrightarrow E/E(V^n-F^m)\longrightarrow 0,$$

$$(2)\quad 0\longrightarrow E \xrightarrow{(V,F)} E\oplus E \xrightarrow{(V,-F)} E\longrightarrow E/(EV+EF)\longrightarrow 0.$$

Here (V^n-F^m) means the multiplication of V^n-F^m on E from the right, and (V, F) (resp. $(V, -F)$) means the operation on E (resp. $E\oplus E$) $(V, F): x\in E \to (xV, xF)$ (resp. $(V, -F): (x, y)\in E\oplus E\to xV-yF\in E$).

PROOF. We denote by $W(k)$ the Witt ring with coefficients in k and by σ the homomorphism of $W(k)$, $\sigma: (a_0, a_1, a_2, \cdots)\to(a_0^p, a_1^p, a_2^p, \cdots)$. Then E is isomorphic to the ring $W(k)_\sigma[[F, V]]$ of non-commutative formal power series of the form,

$$u=w+\sum_{r=1}^{\infty} a_r F^r+\sum_{s=1}^{\infty} b_s V^s,\ w,\ a_r,\ b_s\in W(k)\,,$$

with multiplication formulas $VF=FV=p$, $Fw=w^\sigma F$, $wV=Vw^\sigma$. Let Γ be a set of representants of the classes of $W(k)/pW(k)\cong k$. Then we can write uniquely

$$u=\sum_{r,s\geqq 0}^{\infty} a_{r,s}F^rV^s,\ a_{r,s}\in\Gamma\,.$$

With this remark, it is evident that if $uV^n=uF^m$ for $u\in E$, then $u=0$. Hence the verification of (1). As for (2), we have only to show that if for $(a, b)\in E\oplus E$, $aV=bF$, there exists an element c of E such that $b=cV$, $a=cF$. From the above remark, we know that $a=cF$ for some element c of E. Then from the equality $cFV=cVF=bF$, $b=cF$. q.e.d.

Lemma 4.2. can be said that the projective dimension of $E/(EV+EF)$ (resp. $E/E(V^n-F^m)$) is 2 (resp. 1).

5. Let G, H be equidimensional Dieudonné groups in $\mathfrak{F}$ and let $\varphi : G \to H$ be an isogeny. Then φ can be written as $\varphi = \varphi_r \cdot \varphi_{r-1} \cdots \varphi_1$ where each φ_i, $1 \leqq i \leqq r$, is an isogeny of height 1 from $(\varphi_{i-1} \cdots \varphi_1)G$ to $(\varphi_i \cdot \varphi_{i-1} \cdots \varphi_1)G$. We assume that φ is an isogeny of height 1. If we consider that G, H are elements of $\tilde{\mathfrak{F}}$, we have the following exact sequence in $\tilde{\mathfrak{F}}$,

$$0 \longrightarrow \mathrm{Spec}\,(R) \longrightarrow G \xrightarrow{\varphi} H \longrightarrow 0\,,$$

where $\mathrm{Spec}\,(R)$ is the kernel of φ and R is finite dimensional over k. In the category $\mathcal{DM}$, we have the exact sequence,

$$0 \longrightarrow M(H) \longrightarrow M(G) \longrightarrow \mathrm{Hom}_{\tilde{\mathfrak{F}}}\,(\mathrm{Spec}\,(R), I) \longrightarrow 0\,.$$

Hence, $\mathrm{Hom}_{\tilde{\mathfrak{F}}}\,(\mathrm{Spec}\,(R), I) \cong M(G)/M(H)$ (which we denote by M). From the assumption on φ, $FM=0$. Moreover φ is defined by the sub p-Lie algebra $\mathfrak{N}$ of $t(G)$. Since G is the equidimensional Dieudonné module, for some integer $N>0$, $(t(G))^{p^N}=0$. Therefore we can find a series of sub p-Lie algebras of $\mathfrak{N}$, $0=\mathfrak{N}_0 \subsetneqq \mathfrak{N}_1 \subsetneqq \cdots \subsetneqq \mathfrak{N}_l = \mathfrak{N}$ such that $\mathfrak{N}_j^p \subset \mathfrak{N}_{j-1}$, $1 \leqq j \leqq l$. Hence the decomposition of φ, $\varphi = \psi_l \cdot \psi_{l-1} \cdots \psi_1$. Considering ψ_i instead of φ, we can assume that $\mathfrak{N}^p=0$, that is, $VM=0$. Then M is the direct sum, $M \cong \underbrace{E/(EV+EF) \oplus \cdots \oplus E/(EV+EF)}_{t}$, where t is the integer >0 such that p^t is the order of φ.

6. Now we shall prove the next Proposition.

PROPOSITION 4.4. *Let M be a Dieudonné module. Then the projective dimension of M is $\leqq 2$. In particular, the projective dimension of M is 1 if M is reduced.*

PROOF.

(1) Any Dieudonné module M is isogenous to $M' = \sum_i E/E(V^{n_i} - F^{m_i}) \oplus \sum_j E/EV^{r_j}$ of which projective dimension is 1. Then we have a sequence of Dieudonné modules,

$$M' = M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_{t-1} \longrightarrow M_t = M\,,$$

such that

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow E/(EV+EF) \longrightarrow 0\,, \qquad 1 \leqq i \leqq t\,,$$

is exact. Therefore it is sufficient to prove Proposition 4.4 in the case where M satisfies the following exact sequence,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow E/(EV+EF) \longrightarrow 0\,,$$

M' being a Dieudonné module of projective dimension $\leqq 2$. Then with the usual method, the projective dimension of M is $\leqq 2$.

(2) Let M' be a reduced Dieudonné module with the projective dimension 1, and let M be a reduced Dieudonné module such that the following exact

sequence is satisfied,

$$0 \longrightarrow M \longrightarrow M' \longrightarrow E/(EV+EF) \longrightarrow 0\,.$$

Then for any $N \in \mathfrak{DM}$, we have the next exact sequence,

$$\mathrm{Ext}^2_{\mathfrak{DM}}(M', N) \longrightarrow \mathrm{Ext}^2_{\mathfrak{DM}}(M, N) \longrightarrow \mathrm{Ext}^3_{\mathfrak{DM}}(E/(EV+EF), N)\,.$$

From the assumption,

$$\mathrm{Ext}^2_{\mathfrak{DM}}(M', N) = \mathrm{Ext}^3_{\mathfrak{DM}}(E/(EV+EF), N) = 0\,.$$

Hence $\mathrm{Ext}^2_{\mathfrak{DM}}(M, N) = 0$ for any $N \in \mathfrak{DM}$. Hence the projective dimension of M is equal to 1. If M is isogenous to $M'' = \sum_i E/E(V^{n_i} - F^{m_i}) \oplus \sum_j E/EV^{r_j}$, we can construct a sequence of Dieudonné modules,

$$M = M_t \longrightarrow M_{t-1} \longrightarrow \cdots \longrightarrow M_1 \longrightarrow M_0 = M''\,,$$

such that

$$0 \longrightarrow M_j \longrightarrow M_{j-1} \longrightarrow E/(EV+EF) \longrightarrow 0\,, \qquad 1 \leqq j \leqq t\,,$$

is exact. As the projective dimension of M'' is equal to 1, we know that the projective dimension of M is equal to 1. q. e. d.

7. LEMMA 4.3. *We have the following results.*

(1) $\dim_k \mathrm{Ext}_{\mathfrak{DM}}(E/(EV+EF), E/EV) = 1.$

(2) $\dim_k \mathrm{Ext}^2_{\mathfrak{DM}}(E/(EV+EF), E/EV) = 1.$

(3) $\dim_k \mathrm{Ext}_{\mathfrak{DM}}(E/E(V^n - F^m), E/EV) = m.$

PROOF.

(1) Let M be an extension of $E/(EV+EF)$ by E/EV,

$$0 \longrightarrow E/EV \longrightarrow M \overset{\varphi}{\longrightarrow} E/(EV+EF) \longrightarrow 0\,.$$

Let x be a generator of $E/(EV+EF)$ and y be an element of M such that $\varphi(y) = x$. Then $Vy = a \in E/EV$, $Fy = b \in E/EV$, and $Fa = Vb = 0$. Since E/EV is the reduced module, the equation $Fa = 0$ means $a = 0$. If $b = Fb'$, for $b' \in E/EV$, then $F(y - b') = 0$. Replacing y with $y - b' = y'$, $\varphi(y') = x$, $Fy' = 0$ and $Vy' = 0$ because $FVy' = VFy' = 0$. Therefore if M is not trivial, $Fy = b \neq 0$ modulo $F(E/EV)$. Conversely let b be an element of E/EV such that $b \neq 0$ modulo $F(E/EV)$. Then putting $M = E/EV + E \cdot y$ where $F \cdot y = b$, $Vy = 0$ and $\varphi(y) = x$, M is a non-trivial extension of $E/(EV+EF)$ by E/EV. The above correspondence determines a k-vector space isomorphism between $\mathrm{Ext}_{\mathfrak{DM}}(E/(EV+EF), E/EV)$ and $E/EV/F(E/EV) \cong E/(EV+EF) \cong k$. Hence the requirement.

(2) We use the projective resolution of Lemma 4.2, (2). Then we have the complex,

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{DM}}(E, E/EV) \longrightarrow \mathrm{Hom}_{\mathcal{DM}}(E\oplus E, E/EV) \xrightarrow{d} \mathrm{Hom}_{\mathcal{DM}}(E, E/EV) \longrightarrow 0\,,$$

or

$$0 \longrightarrow E/EV \longrightarrow E/EV \oplus E/EV \xrightarrow{d} E/EV \longrightarrow 0\,,$$

where d is given by the formula,

$$f \in \mathrm{Hom}_{\mathcal{DM}}(E\oplus E, E/EV) \rightsquigarrow (df)(1) = f((V, 0)) + f((0, F))\,.$$

Or if f is given by the formula,

$$f((a, b)) = am + bn \quad \text{for} \quad a, b \in E \quad \text{and} \quad m, n \in E/EV\,,$$

d is given by $(m, n) \to Vm + Fn$. Hence,

$$\begin{aligned} &\mathrm{Ext}^2_{\mathcal{DM}}(E/(EV+EF), E/EV) \\ &\quad \cong \mathrm{Hom}_{\mathcal{DM}}(E, E/EV)/d(\mathrm{Hom}_{\mathcal{DM}}(E\oplus E, E/EV)) \\ &\quad \cong (E/EV)/F(E/EV) \cong E/(EV+EF) \cong k\,. \end{aligned}$$

Hence the requirement.

(3) is already proved. q. e. d.

8. Let M, M' be reduced equidimensional Dieudonné modules such that the following exact sequence is satisfied,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow E/(EV+EF) \longrightarrow 0\,.$$

Then we have the exact sequence by virtue of Proposition 4.4,

$$\begin{aligned} 0 &\longrightarrow \mathrm{Ext}_{\mathcal{DM}}(E/(EV+EF), E/EV) \longrightarrow \mathrm{Ext}_{\mathcal{DM}}(M, E/EV) \\ &\longrightarrow \mathrm{Ext}_{\mathcal{DM}}(M', E/EV) \longrightarrow \mathrm{Ext}^2_{\mathcal{DM}}(E/(EV+EF), E/EV) \longrightarrow 0\,. \end{aligned}$$

By Lemma 4.3 (1), (2), we have,

$$\dim_k \mathrm{Ext}_{\mathcal{DM}}(M, E/EV) = \dim_k \mathrm{Ext}_{\mathcal{DM}}(M', E/EV)\,.$$

If a reduced equidimensional Dieudonné module M is isogenous to $M' = \sum_i E/E(V^{n_i} - F^{m_i})$, then we can construct a sequence of Dieudonné modules,

$$M' = M_t \longrightarrow M_{t-1} \longrightarrow \cdots \longrightarrow M_1 \longrightarrow M_0 = M\,,$$

such that

$$0 \longrightarrow M_j \longrightarrow M_{j-1} \longrightarrow E/(EV+EF) \longrightarrow 0\,, \qquad 1 \leqq j \leqq t\,,$$

is exact.

Therefore we have,

$$\dim_k \mathrm{Ext}_{\mathcal{DM}}(M, E/EV) = \dim_k \mathrm{Ext}_{\mathcal{DM}}(M', E/EV) = \sum_i m_i\,.$$

Let A be an abelian variety of dimension n such that $\hat{A} = (\hat{G}_m)^f \cdot H$, where H is isogenous to $G = \sum_i G_{n_i, m_i}$, $n_i m_i > 0$, $\sum_i n_i = \sum_i m_i = n - f$ by Ju. I. Manin, [**14**].

Then

$$\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, H) = \dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G) = \sum_i m_i = n-f .$$

Therefore

$$\dim_k \operatorname{Ext}_{\mathcal{A}}(G_a, A) = n .$$

Thus we have proved Main Theorem.

THEOREM 4.1.

(1) *Let A be an abelian variety of dimension n. Then* $\dim_k \operatorname{Ext}_{\mathcal{A}}(G_a, A) = n$.

(2) *Let G, G' be reduced isogenous equidimensional Dieudonné groups. Then we have,*

$$\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G) = \dim_k \operatorname{Ext}_{\mathcal{F}}(G_a, G') .$$

(3) *When for $s \geqq 1$, we denote by W_s the Witt group of length s, we have*

$$\operatorname{length}_{W(k)} \operatorname{Ext}_{\mathcal{F}}(\hat{W}_s, G) = s \cdot (\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G)) .$$

PROOF. We have only to prove (3). W_s is endowed with the following operations:

(1) The homomorphism $V: W_s \to W_{s+1}$ which maps

$$(x_0, x_1, x_2, \cdots, x_{s-1}) \quad \text{to} \quad (0, x_0, x_1, \cdots, x_{s-1}) ,$$

(2) The homomorphism $R: W_{s+1} \to W_s$ which maps

$$(x_0, x_1, \cdots, x_s) \quad \text{to} \quad (x_0, x_1, \cdots, x_{s-1}) .$$

Then we have the following exact sequence,

$$0 \longrightarrow G_a \xrightarrow{V^{s-1}} W_s \xrightarrow{R} W_{s-1} \longrightarrow 0 .$$

Then we have the exact sequence,

$$0 \longrightarrow \operatorname{Ext}_{\mathcal{F}}(\hat{W}_{s-1}, G) \longrightarrow \operatorname{Ext}_{\mathcal{F}}(\hat{W}_s, G) \longrightarrow \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G) \longrightarrow 0 ,$$

because the projective dimension of $M(G)$ is 1.

Hence,

$$\operatorname{length}_{W(k)} \operatorname{Ext}_{\mathcal{F}}(\hat{W}_s, G) = \operatorname{length}_{W(k)} \operatorname{Ext}_{\mathcal{F}}(\hat{W}_{s-1}, G) + \dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G) .$$

Using the induction on s, we have,

$$\operatorname{length}_{W(k)} \operatorname{Ext}_{\mathcal{F}}(\hat{W}_s, G) = s \cdot (\dim_k \operatorname{Ext}_{\mathcal{F}}(\hat{G}_a, G)) , \qquad \text{q.e.d.}$$

Appendix.

We shall generalize the results of Chapter III, § 3.

1. Let L be a connected linear group, A an abelian variety and G an extension of L by A. We put the next definitions.

DEFINITION. We call G an extension of *separable* type (resp. *purely inseparable* type) if there exists a separable (resp. purely inseparable) isogeny $\varphi: H \to L$ such that $\varphi^* G \cong A \times H$. We denote by $\mathrm{Ext}_{\mathcal{A}}(L, A)_s$ (resp. $\mathrm{Ext}_{\mathcal{A}}(L, A)_i$) the set of classes of extensions of separable type (resp. purely inseparable type). Then by Lemma 3.1, Chapter III, § 3, $\mathrm{Ext}_{\mathcal{A}}(L, A)_s$ and $\mathrm{Ext}_{\mathcal{A}}(L, A)_i$ are subgroups of $\mathrm{Ext}_{\mathcal{A}}(L, A)$. If $G \in \mathrm{Ext}_{\mathcal{A}}(L, A)_s$ (resp. $\mathrm{Ext}_{\mathcal{A}}(L, A)_i$), then the isogeny $\psi: H' \to L$ is separable (resp. purely inseparable) for the maximal connected linear subgroup H' of G. Then it is easy to see that $\mathrm{Ext}_{\mathcal{A}}(L, A)_s \cap \mathrm{Ext}_{\mathcal{A}}(L, A)_i = (0)$. Considering the Frobenius endomorphism $\boldsymbol{p}: L^{(p^{-1})} \to L$, we have

$$\boldsymbol{p}^*(\mathrm{Ext}_{\mathcal{A}}(L, A)_s) \subset \mathrm{Ext}_{\mathcal{A}}(L^{(p^{-1})}, A)_s$$

and

$$\boldsymbol{p}^*(\mathrm{Ext}_{\mathcal{A}}(L, A)_i) \subset \mathrm{Ext}_{\mathcal{A}}(L^{(p^{-1})}, A)_i \,.$$

LEMMA 1. *The restriction of* $\boldsymbol{p}^*$ *on* $\mathrm{Ext}_{\mathcal{A}}(L, A)_s$ *is an isomorphism onto* $\mathrm{Ext}_{\mathcal{A}}(L^{(p^{-1})}, A)_s$.

PROOF. Let G be an extension of L by A such that for a separable isogeny $\varphi: H \to L$, $\varphi^* G \cong A \times H$,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \times H & \longrightarrow & H & \longrightarrow & 0 \\ & & \big\downarrow id. & & \big\downarrow & & \big\downarrow \varphi & & \\ 0 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & L & \longrightarrow & 0\,. \end{array}$$

By Lemma 3.3, Chapter III, § 3, G is the quotient of $A \times H$ by its finite subgroup N, i. e. $G \cong A \times H/N$. Then taking the inverse image N' of N by the homomorphism $A \times H^{(p^{-1})} \to A \times H$, $\boldsymbol{p}^* G \cong A \times H^{(p^{-1})}/N'$. Conversely, let G' be an extension of $L^{(p^{-1})}$ by A such that $\psi^* G' = 0$, for some separable isogeny $H' \xrightarrow{\psi} L^{(p^{-1})}$. Then G' is also written as the quotient $A \times H'/N'$ of $A \times H'$ by its finite subgroup N'. Taking the image N of N' by the homomorphism

$$A \times H' \to A \times H'^{p}\,, \qquad G' \cong \boldsymbol{p}^*(A \times H'^{p}/N)\,.$$

Therefore we have constructed the bijective correspondence from which follows the requirement. q. e. d.

2. Let G be an extension of L by A, H be the maximal connected linear subgroup of G. Then $A \cap H =$ finite group, $G = A \cdot H$ and H is isogenous to L (the isogeny $\varphi: H \to L$). It is easy to see $\varphi^* G \cong A \times H$. We write $\varphi = \varphi_s \cdot \varphi_i$, where φ_s is separable and φ_i is purely inseparable. φ_i is a divisor of an iteration of the Frobenius map $\boldsymbol{p}^N$, for some integer $N \geqq 0$, that is, $\varphi_i \cdot \psi = \boldsymbol{p}^N$, for some purely inseparable isogeny ψ. Then from $\varphi^*\{G\} = 0$, $(\boldsymbol{p}^*)^N \cdot (\varphi_s{}^*\{G\} = 0$. We can write $\varphi_s \cdot \boldsymbol{p}^N = \boldsymbol{p}^N \cdot \varphi'$, where φ' is a separable isogeny. Then $(\varphi')^*(\boldsymbol{p}^*)^N\{G\} = 0$. If we put $G' = ((\boldsymbol{p}^*)^N | \mathrm{Ext}_{\mathcal{A}}(L^{(p^{-N})}, A)_s)^{-1}((\boldsymbol{p}^*)^N G)$ and $G'' =$

$G-G'$, then $G' \in \mathrm{Ext}_{\mathcal{A}}(L, A)_s$ and $G'' \in \mathrm{Ext}_{\mathcal{A}}(L, A)_i$. Moreover we know that $\mathrm{Ext}_{\mathcal{P}}(L, A) \cong \varinjlim_n \mathrm{Ext}_{\mathcal{A}}(L^{p^{-n}}, A)$. Therefore we have proved:

THEOREM 1.

(1) $\mathrm{Ext}_{\mathcal{A}}(L, A) \cong \mathrm{Ext}_{\mathcal{A}}(L, A)_s \oplus \mathrm{Ext}_{\mathcal{A}}(L, A)_i$,

(2) $\mathrm{Ext}_{\mathcal{A}}(L, A)_s \cong \mathrm{Ext}_{\mathcal{P}}(L, A)$.

4. Let U be a connected unipotent group, A an abelian variety. Then we have the following:

THEOREM 2. *The homomorphism* $\sigma: \mathrm{Ext}_{\mathcal{A}}(U, A) \rightarrow \mathrm{Ext}_{\mathcal{F}}(\hat{U}, \hat{A})$ *is surjective, and has* $\mathrm{Ext}_{\mathcal{A}}(U, A)_s$ *as its kernel. Here* σ *means the homomorphism* $G \in \mathrm{Ext}_{\mathcal{A}}(U, A) \rightarrow \hat{G} \in \mathrm{Ext}_{\mathcal{F}}(\hat{U}, \hat{A})$.

PROOF. The last assertion is proved by repeating the argument of the proof of Theorem 3.2 of Chapter III, § 3.

We shall prove the surjectivity. Let G^* be an extension of $\hat{U}$ by $\hat{A}$ in $\mathcal{F}$, and H^* the maximal unipotent subgroup of G^*. Then $G^* = H^* \vee \hat{A}$, $H^* \wedge \hat{A} = (0)$ and H^* is isogenous to $\hat{U}$ (the isogeny $\varphi^*: H^* \rightarrow \hat{U}$). Considering $\hat{U}$, H^* and $\hat{A}$ in $\tilde{\mathcal{F}}$, we denote by $\mathfrak{B}$ (resp. $\mathfrak{A}$) the kernel of $\varphi^*: H^* \rightarrow \hat{U}$ (resp. $\psi: \hat{A} \times H^* \rightarrow G^*$) in the category $\tilde{\mathcal{F}}$ (cf. Chapter III, § 4),

$$\begin{array}{ccccccccc}
 & & & & \mathfrak{A} & \longrightarrow & \mathfrak{B} & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \hat{A} & \longrightarrow & \hat{A} \times H^* & \longrightarrow & H^* & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id.} & & \downarrow & & \downarrow{\scriptstyle \varphi^*} & & \\
0 & \longrightarrow & \hat{A} & \longrightarrow & G^* & \longrightarrow & \hat{U} & \longrightarrow & 0.
\end{array}$$

Then $\mathfrak{A} \cong \mathfrak{B}$. Since $\mathfrak{B}$ is artinian, we can find a unipotent group H and a purely inseparable isogeny $\varphi: H \rightarrow U$ such that $\hat{H} \cong H^*$, $\hat{\varphi} \cong \varphi^*$ and $\mathfrak{B} \cong$ the kernel of φ. As $\mathfrak{A}$ is also artinian, $\mathfrak{A}$ can be considered a sub-group scheme of $A \times H$. Then, for our purpose, it is enough to take $G = A \times H / \mathfrak{A}$. q. e. d.

Kyoto University

Bibliography

[1] I. Barsotti, Abelian varieties over fields of positive characteristic, Rend. Circ. Mat. Palermo, 5 (1956), 1-25.

[2] I. Barsotti, Repartitions on abelian varieties, Illinois J. Math., 2 (1958), 43-70.

[3] I. Barsotti, Gli endomorphismi delle varietà abeliane su corpi di caratteristica positiva, Ann. Scuola Norm. Sup. Pisa, 10 (1956), 1-24.

[4] P. Cartier, Questions de rationalité des diviseurs en géométrie algébrique, Bull. Soc. Math. France, 86 (1958), (Thèse).

[5] P. Cartier, Dualité des variétés abéliennes, Séminaire Bourbaki, No. 164, (1958).
[6] P. Cartier, Isogenies and duality of abelian varieties, Ann. of Math., **71** (1960), 315–351.
[7] P. Cartier, Une nouvelle opération sur les formes differentielles, C. R. Acad. Sci. Paris, **244** (1957), 426–428.
[8] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un caractéristique $p>0$, Comment. Math. Helv., **28** (1954), 87–118.
[9] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$, (II), Amer. J. Math., **77** (1955), 218–244.
[10] J. Dieudonné Lie groups and Lie hyperalgebras over a field of characteristic $p>0$, (VI), Amer. J. Math., **79** (1957), 331–388.
[11] J. Dieudonné Lie groups and Lie hyperalgebras over a field of characteristic $p>0$, (VIII), Amer. J. Math., **80** (1958), 740–772.
[12] J. Frenkel, Cohomologie non abélienne et espaces fibrés, Bull. Soc. Math. France, **85** (1957), 135–220.
[13] S. Lang, Abelian varieties, Interscience Tracts No. 7, New-York, 1959.
[14] Ju. I. Manin, Theory of commutative formal groups over a field of positive characteristic, Uspehi Math. Nauk, **18** (1963), 3–90. Translated into English in Russian Math. Surveys, **18** (1963), 1–80.
[15] M. Rosenlicht, Some basic theorems on algebraic groups, Amer. J. Math., **78** (1956), 401–443.
[16] M. Rosenlicht, Extensions of vector groups by abelian varieties, Amer. J. Math., **80** (1958), 685–714.
[17] J. P. Serre, Quelques propriétés des variétés abéliennes en caractéristique p, Amer. J. Math., **80** (1958), 715–739.
[18] J. P. Serre, Espaces fibrés algébriques, Séminaire C. Chevally, 2 (1958).
[19] J. P. Serre, Groupes algébriques et corps de classes, Act. Sci. Ind., No. 1264, Hermann, Paris, 1959.
[20] J. P. Serre, Groupes proalgébriques, Publication de IHES, No. 7, 1960.
[21] A. Weil, On algebraic groups and homogeneous spaces, Amer. J. Math., **77** (1955), 493–512.
[22] M. Lazard, Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math. France, **83** (1955), 251–274.