Journal of the Mathematical Society of Japan Vol. 12, No. 3, July, 1960

# Commutative group varieties.

To the memory of Y. Taniyama.

By Satoshi ARIMA

(Received Nov. 29, 1958)

The purpose of this paper is to generalize some results of Weil [**6**] on abelian varieties to the case of commutative group varieties. An element, of a group, whose order is finite and divides $n$ will be called an *$n$-division point.* In § 1, we first count the number of $n$-division points on a commutative group variety and see that a commutative group variety without affine subgroup is generated by division points. We can introduce therefore a system of $l$-adic coordinates on such a group $G$, and get the $l$-adic representation of the ring of endomorphisms of $G$. Next we shall show the symmetric property of isogenies between divisible commutative group varieties, where an isogeny means a surjective (rational) homomorphism between two group varieties of the same dimension. In § 2, we shall see that a group variety defined over a finite field is generated by an abelian variety and a linear group variety (Theorem 1), and that the algebra of endomorphisms of a divisible commutative group variety defined over a finite field is a semi-simple algebra over the field of rational numbers.

We use the following terminologies and notations throughout the paper. A homomorphism of a group variety into a group variety means always a rational homomorphism; we use " endomorphism " in the corresponding sense. An algebraic subgroup of a group variety is an abstract subgroup which is a closed subset in the sense of Zariski topology. An affine group is a group variety which is biregularly equivalent to an affine space as a variety. $G_a$ denotes the additive group of the universal domain and $G_m$ the multiplicative group of the non-zero elements of the universal domain. A biregular isomorphism between group varieties is a group-isomorphism defined by a birational mapping which we denote by $\cong$. $T \supset S$ means that $T$ contains $S$ but not equals $S$. For a natural number $n$, we denote by $n[G]$ the number of $n$-division points on a group $G$. We denote the characteristic of the universal domain by $p$. We write the (commutative) group-operation additively.

## § 1. Division points.

**1.** Let $G$ be a commutative group variety and $L$ be its maximal linear group subvariety. Then the factor group $A=G/L$ is an abelian variety [**2**, p. 439, Theorem 16]; in this case we shall say that the group variety $G$ is an extension of an abelian variety $A$ by a linear group variety $L$. It is known also that the (commutative) linear group variety $L$ is a direct product of two group varieties $L_1$ and $L_2$ where $L_1$ is biregularly isomorphic to a direct product of a certain number of $G_m$, and $L_2$ is an affine group ([**1**], [**3**]). We first count the number of $n$-division points of a commutative group variety.

Lemma 1. *Let $G$ be a commutative abstract group and $L$ be its subgroup. If $n[L]<\infty$ and $n[G/L]<\infty$, then we have $n[G]\leqq n[L]\ n[G/L]$. Moreover we have $n[G]=n[L]\ n[G/L]$, provided that $nL=L$.*

Proof. Put $\mathfrak{g}=\{x \mid x\in G,\ nx=e\}$, $\mathfrak{h}=\mathfrak{g}\frown L$, $A=G/L$, $\mathfrak{a}=\{a \mid a\in A,\ na=e\}$, and let $\alpha: G\rightarrow A$ be the canonical homomorphism. As $\mathfrak{g}/\mathfrak{h}\cong\mathfrak{g}L/L=\alpha\mathfrak{g}\subseteqq\mathfrak{a}$, we have $n[G]\leqq n[L]\ n[A]$. Moreover if $nL=L$, then we have $\alpha\mathfrak{g}=\mathfrak{a}$. In fact, take an element $a=\alpha x$ of $\mathfrak{a}$ (with $x\in G$). From $na=\alpha nx=e$, it follows that $nx\in L=nL$. Hence there exists an element $\xi$ of $L$ such that $nx=n\xi$, which implies that $x-\xi\in\mathfrak{g}$ and $a=\alpha(x-\xi)\in\alpha\mathfrak{g}$: Lemma 1 is thereby proved.

Proposition 1. *Let $n$ be a natural number coprime to the characteristic $p$. Then the neutral element is the only $n$-division point of an affine group.*

Proof. An affine group $L^m$ is solvable and has a normal chain of affine subgroups: $L^m=H_0\supset H_1^{m-1}\supset\cdots\supset H_{m-1}^1\supset H_m=\{e\}$ with $H_{i-1}/H_i\cong G_a(1\leqq i\leqq m)$ [**3**, p. 155]. Proposition 1 follows immediately from this and the relation $n[H_{i-1}/H_i]=n[G_a]=1$.

Proposition 2. *Let a commutative group variety $G$ be an extension of an abelian variety $A^{n_0}$ by a linear group variety $L=L_1\times L_2$, where $L_1\cong(G_m)^{n_1}$ and $L_2$ is an affine group. Let $n$ be a natural number. If $n$ is coprime to the characteristic $p$, then the number of $n$-division points on $G$ is $n^{2n_0+n_1}$. If $G$ contains no affine group, then the number of $n$-division points is at most $n^{2n_0+n_1}$.*

Proof. Since the $n$-division points of $G_m$ are $n$-th roots of the unity, we have clearly $n[L_1]=n^{n_1}$ for $n$ which is coprime to the characteristic $p$ and $n[L_1]\leqq n^{n_1}$ for arbitrary $n$. We first assume that $n$ is coprime to $p$. From $n[L_1]=n^{n_1}$ and Proposition 1 follows immediately $n[L]=n^{n_1}$, which implies also $nL=L$. It is well known that the number $n[A]$ of the abelian variety $A$ is $n^{2n_0}$, so that we have $n[G]=n^{2n_0+n_1}$ by Lemma 1. The second part of Proposition 2 will be verified analogously.

**2.** We shall show next that division points of a commutative group variety generate, together with its canonical affine subgroup, the whole group.

Proposition 3. *Let $G$ be biregularly isomorphic to a direct product of $G_m$'s, then every group subvariety of $G$ is also biregularly isomorphic to a direct product of $G_m$'s.*

Proof. Let $H$ be a group subvariety of $G \cong (G_m)^n$. Since $H$ and $G/H$ are linear [2, p. 440, Cor. 2 to Th. 16], we have, by the structure theorem of linear group variety, $H = H_1^{t_1} \times H_2^{t_2}$, $G/H = G_1^{s_1} \times G_2^{s_2}$ where $H_1 \cong (G_m)^{t_1}$, $G_1 \cong (G_m)^{s_1}$, and $H_2$ and $G_2$ are affine groups. We take now a natural number $l$ coprime to the characteristic $p$ and count the number of $l$-division points. By Proposition 2 and Lemma 1, we have $l^n = l[G] = l[H]l[G/H] = l^{t_1}l^{s_1}$. From this follows that $n = t_1 + s_1$, $t_2 = s_2 = 0$ and $H \cong (G_m)^{t_1}$, which proves Proposition 3.

Proposition 4. *Let $G$ be a commutative group variety and $F$ an algebraic subgroup of $G$. Suppose that $F$ fulfills the following two conditions:*

(i) *for infinite number of natural numbers $n$ which is coprime to the characteristic $p$, $F$ contains all the $n$-division points of $G$, i.e., $(n\delta)^{-1}(e) \subseteqq F$;*

(ii) *$F$ contains the canonical affine subgroup of $G$.*

*Then we have $F = G$.*

Proof. Assume for a moment that $F \neq G$; let $G$ be an extension of an abelian variety $A^{n_0}$ by a linear group variety $L = L_1 \times L_2$, where $L_1 \cong (G_m)^{n_1}$ and $L_2$ is an affine group. Let $F_0$ and $(F_0 \frown L)_0$ be the identity-components of $F$ and $F_0 \frown L$ respectively. If a natural number $n$ is coprime to $p$, we have, by Lemma 1 and Proposition 1, $n[F] \leqq (F: F_0)\, n[F_0/(F_0 \frown L)_0]\, n[(F_0 \frown L)_0/L_2]$. $F_0/(F_0 \frown L)_0$ is isogenous to $F_0L/L$, which is an abelian subvariety of $G/L = A$. Put $n_0' = \dim F_0/(F_0 \frown L)_0$; then we have $n_0' \leqq n_0$ and $n[F_0/(F_0 \frown L)_0] = n^{2n_0'}$. From $(F_0 \frown L)_0/L_2 \subseteqq L/L_2 \cong (G_m)^{n_1}$ and Proposition 3, it follows $(F_0 \frown L)_0/L_2 \cong (G_m)^{n_1'}$ with $n_1' \leqq n_1$, and $n[(F_0 \frown L)_0/L_2] = n^{n_1'}$. Since the equalities $n_0' = n_0$ and $n_1' = n_1$ lead to $F_0L = F = G$, we must have $2n_0' + n_1' < 2n_0 + n_1$. Now, if $F$ contains all the $n$-division points of $G$, then the number of $n$-division points of $G$ is equal to that of $F$, and we have $n^{2n_0+n_1} = n[G] = n[F] \leqq (F: F_0) n^{2n_0'} n^{n_1'}$, i.e.,

$$n^{(2n_0+n_1)-(2n_0'+n_1')} \leqq (F: F_0)\,.$$

Since $(2n_0 + n_1) - (2n_0' + n_1') > 0$, we see that the number $n$ satisfying the last inequality must be finite, which contradicts the condition (i) and proves our assertion.

**3.** Let $G$ be a commutative group variety and assume that $G$ *contains no affine group*; $G$ is an extension of an abelian variety $A^{n_0}$ by a linear group variety $L \cong (G_m)^{n_1}$. Take a prime number $l$ coprime to the characteristic $p$. We have seen in Proposition 2 that, for a natural number $m$, the group $\mathfrak{g}_m$ of $l^m$-division points of $G$ is a finite group of order $l^m[G] = l^{m(2n_0+n_1)}$. We have then the following proposition which is an analogue of the proposition 11 of [6, p. 45] and proved in the same way.

Proposition 5. *$\mathfrak{g}_m$ is a direct product of $2n_0 + n_1$ cyclic groups of order $l^m$.*

Denote by $\mathfrak{g}_l(G)$ the group of elements of $G$ whose orders are powers of $l$; by virtue of Proposition 5, the structure of $\mathfrak{g}_l(G)$ is determined only by $l$

and $2n_0+n_1$, so by $l$ and $G$; as in [6], we see that $\mathfrak{g}_l(G)$ is isomorphic to the direct product of $2n_0+n_1$ copies of the additive group of the $l$-adic numbers modulo the $l$-adic integers. In other words, we can introduce a system of $l$-adic coordinates in $\mathfrak{g}_l(G)$. Denote by $\mathfrak{a}_m$ and $\mathfrak{b}_m$ the group of $l^m$-division points of $A$ and $L$, respectively; denote by $\mathfrak{g}_l(A)$ and $\mathfrak{g}_l(L)$ the group of elements, respectively, of $A$ and $L$ whose orders are powers of $l$. From Proposition 2 and Lemma 1 it follows that $\mathfrak{g}_m/\mathfrak{b}_m$ is isomorphic to $\mathfrak{a}_m$, and therefore that $\mathfrak{g}_m$ is isomorphic to the direct product $\mathfrak{a}_m \times \mathfrak{b}_m$. It follows from this that $\mathfrak{g}_l(G)$ is isomorphic to $\mathfrak{g}_l(A) \times \mathfrak{g}_l(L)$ (cf. [6, p. 46, Lemma 6]). Therefore we can introduce a system of $l$-adic coordinates in $\mathfrak{g}_l(G)$ in such a way that the first $2n_0$ components of the coordinates are that of $\mathfrak{g}_l(A)$ and the remaining $n_1$ components are that of $\mathfrak{g}_l(L)$.

Let $G'$ be another commutative group variety which is an extension of an abelian variety $A'^{n_0'}$ by a linear group variety $L' \cong (G_m)^{n_1'}$; we introduce a system of $l$-adic coordinates also in $\mathfrak{g}_l(G')$; let $\lambda$ be a homomorphism of $G$ into $G'$. Let $\alpha : G \rightarrow A$ and $\alpha' : G' \rightarrow A'$ be the canonical homomorphisms. As $\alpha'\lambda : G \rightarrow A'$ maps $L$ to $\{e\}$, there exists a homomorphism $\lambda_0 : A \rightarrow A'$ such that $\alpha'\lambda = \lambda_0\alpha$ [2, p. 415, Cor. 1 to Th. 4]. Since $\lambda L \subseteqq L'$ (because $\lambda L$ is linear), $\lambda$ induces a homomorphism of $L$ into $L'$ which we denote by $\lambda_1$. Following the same process as in [6, p. 49, Th. 14], we obtain an $l$-adic representation of $\lambda$ in the following sense. Namely there exists a matrix $M = M_l(\lambda)$ of $2n_0'+n_1'$ rows and $2n_0+n_1$ columns with $l$-adic integral coefficients such that, if $\bar{x}$ and $\bar{y}$ are the $l$-adic representations of $x \in \mathfrak{g}_l(G)$ and $y = \lambda x \in \mathfrak{g}_l(G')$, we have $\bar{y} \equiv M\bar{x}$ (mod. 1). Moreover, $\lambda \rightarrow M_l(\lambda)$ gives a faithful representation of the module of homomorphisms of $G$ into $G'$. To prove this, assume that $\lambda \neq 0$; put $F = \lambda^{-1}(e)$. Since $F \neq G$, Proposition 4 shows that the set $N$ of natural numbers $n$ which is such that $(n\delta)^{-1}(e) \subseteqq F$ and coprime to the characteristic $p$ is a finite set. If $M_l(\lambda) = 0$, we see that

$$l^\nu x = e \quad \Rightarrow \quad \overline{\lambda x} = M_l(\lambda)\bar{x} = 0 \quad \Rightarrow \quad \lambda x = e\,,$$

i. e., $(l^\nu\delta)^{-1}(e) \subseteqq F$, where $\nu$ is an arbitrary natural number. This indicates that $N$ is an infinite set, which is a contradiction.

We now introduce, in the same way as we have described below Proposition 5, the systems of $l$-adic coordinates in $\mathfrak{g}_l(G) \cong \mathfrak{g}_l(A) \times \mathfrak{g}_l(L)$ and $\mathfrak{g}_l(G') \cong \mathfrak{g}_l(A') \times \mathfrak{g}_l(L')$; We denote $l$-adic representations of $\lambda, \lambda_0, \lambda_1$ by $M_l(\lambda), M_l(\lambda_0), M_l(\lambda_1)$, respectively. Then we have clearly $M_l(\lambda) = \begin{pmatrix} M_l(\lambda_0) & 0 \\ * & M_l(\lambda_1) \end{pmatrix}$ since $\lambda L \subseteqq L'$.

**4.** We now prove a symmetric property of isogenies between commutative group varieties.

PROPOSITION 6. *Let $\lambda$ be a homomorphism of a commutative group variety $G$ onto a commutative group variety $H$ with finite kernel. If $G$ is divisible* (*and* *a fortiori $H$ is also divisible), then there exists a homomorphism $\mu$ of $H$ onto $G$ such that $\mu\lambda=\nu(\lambda)\delta_G$, $\lambda\mu=\nu(\lambda)\delta_H$.*

Proof. Separable case: If $\lambda$ is separable, we have $H=G/\lambda^{-1}(e)$. Putting $d=\nu(\lambda)$, we have $(d\delta)^{-1}(e)\supseteqq\lambda^{-1}(e)$. Thus there exists a homomorphism $\mu$ of $H$ onto $dG=G$ such that $\mu\lambda=d\delta_G$ [**2**, p. 415, Cor. 1 to Th. 4].

Purely inseparable case: In this case $\lambda$ is bijective. Denote by $\Gamma$ the graph of $\lambda$ in the product $H\times G$ and let $k$ be a field of definition for $G, H$ and $\Gamma$. Take a generic point $y$ of $H$ over $k$, then the element $x\in G$ with $y=\lambda x$ is a generic point of $G$ over $k$. Put $d=\nu(\lambda)=\nu_i(\lambda)$. Since we have $\Gamma\cdot(y\times G)=y\times d(x)$, the cycle $d(x)$ is rational over $k(y)$, and hence the point $dx\in G$ is also rational over $k(y)$. We can thus define the rational mapping

$$y\to\mu y=dx \qquad (y=\lambda x)$$

of $H$ into $G$. Let $y'$ be another generic point of $H$ over $k$, independent of $y$ over $k$. Clearly we have $\mu y'=dx'$ (with $y'=\lambda x'$). Since we have $y+y'=\lambda x+\lambda x'=\lambda(x+x')$, we have $\mu(y+y')=dx+dx'=\mu y+\mu y'$. Thus $\mu$ is generically a homomorphism, and therefore defines a homomorphism $\mu$ of $H$ into $G$; clearly we have $\mu\lambda x=dx$.

General case: Given $\lambda$, we can decompose $\lambda$ into two homomorphisms $G\xrightarrow{\alpha}G/\lambda^{-1}(e)\xrightarrow{\beta}H$ where $\alpha$ is separable and $\beta$ is purely inseparable and $\nu(\alpha)=\nu_s(\lambda)$, $\nu(\beta)=\nu_i(\lambda)$ [**2**, p. 415, Cor. 1 to Th. 4]; then, applying the above two cases to $\alpha$ and $\beta$ respectively, we obtain a homomorphism $\mu$ of $H$ onto $G$ such that $\mu\lambda=\nu_i(\lambda)\nu_s(\lambda)\delta_G=\nu(\lambda)\delta_G$. $\lambda\mu=\nu(\lambda)\delta_H$ is trivially verified from $\mu\lambda=\nu(\lambda)\delta_G$. Proposition 6 is thereby proved.

## § 2. Groups over finite fields.

**5.** We first prove the following

Proposition 7. *Let $G$ be a commutative group variety containing no abelian subvariety and $L$ be its maximal linear group subvariety. If an endomorphism $\lambda$ of $G$ is zero on $L$, then $\lambda=0$ on $G$.*

Proof. Let $\alpha: G\to A=G/L$ be the canonical homomorphism. Since $\alpha^{-1}(e)=L\subseteqq\lambda^{-1}(e)$, there exists a homomorphism $\mu$ of $A$ into $G$ such that $\lambda=\mu\alpha$. Then the assumption that $G$ contains no abelian variety implies that $\lambda G=\mu\alpha(G)=\mu(A)=\{e\}$, which proves our proposition.

Theorem 1. *Let $G$ be a group variety defined over a finite field. Let $A$ and $L$ be the maximal abelian subvariety and the maximal linear group subvariety of $G$ respectively. Then $G$ is generated by $A$ and $L: G=AL$. (We do not assume the commutativity of $G$.)*

Proof. Let $G$ be defined over a finite field $k$. Then $L$ is also defined over

$k$. As there exists a central group subvariety $D$ of $G$ defined over $k$ such that $G=DL$ and $D$ is divisible and $D$ contains every abelian subvariety of $G$, we can assume without loss of generality that $G$ is commutative and contains no affine subgroup (cf. [**2**, p. 431, Cor. 3 to Th. 12], [**2**, p. 433, Cor. 1 to Th. 13] and [**2**, p. 440, Cor. 5 to Th. 16]).

Let $A$ be the maximal abelian subvariety of $G$, then $A$ is defined over $k$ and there exists a $k$-closed group subvariety $G_1$ of $G$ such that $G=G_1A$ and $G_1 \cap A$ is finite [**2**, p. 443, Cor. to Prop. 4], [**2**, p. 434, Cor. to Th. 14]. Hence it suffices to prove our theorem for $G_1$. Now suppose that $G$ is a commutative group variety defined over the finite field $k$ with $q$ elements and that $G$ contains neither affine subgroup nor abelian subvariety. Under this assumption we shall show that $G$ is biregularly isomorphic to a direct product of $G_m$'s, which will prove the theorem. Let $L \cong (G_m)^{n_1}$ be the maximal linear group subvariety of $G$ and $G/L=B^{n_0}$. We assume $n_0>0$ and show that this leads to a contradiction. $B=G/L$ is defined over $k$ [**2**, p. 413, Th. 4]; replacing $k$ by its finite extension if necessary, we can also assume that the biregular isomorphism $L \cong (G_m)^{n_1}$ is defined over $k$. Let $\pi$ and $\pi_0$ be the $q$-th-power-endomorphisms of $G$ and $B$, respectively. We remark that we have $\pi=q\delta_L$ on $L$ since the biregular isomorphism $L \cong (G_m)^{n_1}$ is defined over $k$. Now we compare the $l$-adic representotions of $\pi$ and $q\delta_G$:

$$M_l(\pi)=\begin{pmatrix} M_l(\pi_0) & 0 \\ * & M_l(q\delta_L) \end{pmatrix}, \qquad M_l(q\delta_G)=\begin{pmatrix} M_l(q\delta_B) & 0 \\ * & M_l(q\delta_L) \end{pmatrix}$$

(cf. § 1, no. 3). Since $\det M_l(\pi_0)=(\sqrt{q}\,)^{2n_0}=q^{n_0}$ [**5**, p. 37] and $\det M_l(q\delta_B)=\nu(q\delta_B)=q^{2n_0}$ [**6**, p. 127, Cor. 1 to Th. 33] and $n_0>0$, we see that $M_l(\pi)\neq M(q\delta_G)$ and $\pi \neq q\delta_G$. Put $\lambda=\pi-q\delta_G$, then we have $\lambda \neq 0$ on $G$ and $\lambda=0$ on $L$. From Proposition 7, it follows that $\lambda=0$ on $G$ since $G$ contains no abelian subvariety; this is a contradicition and completes the proof.

Since a divisible (commutative) linear group variety defined over a field of positive characteristic is a direct product of $G_m$'s and since an abelian variety is completely reducible, we have now at once

COROLLARY 1. *Let $G$ be a divisible commutative group variety defined over a finite field. Then there exist simple group subvarieties $G_1, \cdots, G_h$ of $G$, of dimensions $n_1, \cdots, n_h$ respectively, such that $\sum_{i=1}^{h} n_i=n$ and $G=G_1 \cdots G_h$.*

COROLLARY 2. *Let $G^n$ be a divisible commutative group variety defined over a finite field and $H^r$ be a group subvariety of $G$. Then there exists a group subvariety $F^{n-r}$ of $G$ such that $H \cap F$ is a finite set, and $G=HF$.*

The divisibility assumption on $G$ in Corollaries 1 and 2 is necessary. For example, a Witt group $W_n$ of length $n$ is defined over a prime finite field and contains only $n-1$ proper group subvariety $W_i$ such that $W_n \supset W_{n-1} \supset \cdots$

$\supset W_1 \supset \{e\}$, so that it is immediately verified that the conclusions of Corollaries 1 and 2 do not hold.

We denote by $\mathcal{A}(G)$ the ring of endomorphisms of a commutative group variety $G$. It is clear that, if $G$ is divisible, then the ring $\mathcal{A}(G)$ can be imbedded in the algebra $\mathcal{A}(G)\otimes \boldsymbol{Q}$ over the field $\boldsymbol{Q}$ of rational numbers. We now assume that $G$ is divisible and defined over a finite field; this implies, by Corollary 1 to Theorem 1, that $G$ is isogenous to a direct product $H=A\times L$, where $A$ is an abelian variety and $L=(G_m)^{n_1}$. Making use of the symmetric property of isogeny (Proposition 6), we can see easily that the algebra $\mathcal{A}(G)\otimes \boldsymbol{Q}$ is isomorphic to $\mathcal{A}(H)\otimes \boldsymbol{Q}$. On the other hand, it is easily verified that $\mathcal{A}(H)$ is isomorphic to the direct sum of $\mathcal{A}(A)$ and $\mathcal{A}(L)$, and that $\mathcal{A}(L)$ is isomorphic to the total matric ring of degree $n_1$ over the ring of rational integers, and therefore that $\mathcal{A}(L)\otimes \boldsymbol{Q}$ is the total matric algebra over $\boldsymbol{Q}$; it is well known that $\mathcal{A}(A)\otimes \boldsymbol{Q}$ is a semi-simple algebra over $\boldsymbol{Q}$. We have thus

Corollary 3. *Let $G$ be a divisible commutative group variety defined over a finite field. Then the algebra $\mathcal{A}(G)\otimes \boldsymbol{Q}$ of endomorphisms of $G$ is a semi-simple algebra over $\boldsymbol{Q}$.*

## Added in June 3, 1959.

Previously we have shown that a group variety defined over a finite field is generated by an abelian variety and a linear group variety (Theorem 1). Here we shall show that Theorem 1 can be also proved by using the theory of groups of extensions of abelian varieties [**4**, Chap. VII]. We shall also show the existence of a group variety which is not generated by an abelian variety and a linear group variety.

**6.** We first recall some properties of group extensions due to M. Rosenlicht and J-P. Serre [**4**], and we shall call our special attention to fields of definition of the objects which we are considering; we introduce these as three lemmas.

Let $A, B, C$ be three commutative algebraic groups. An exact sequence of (rational) homomorphisms

$$O \longrightarrow B \longrightarrow C \longrightarrow A \longrightarrow O \tag{1}$$

is called *strictly exact* if the homomorphisms $B\rightarrow C$ and $C\rightarrow A$ are separable. We can then identify $B$ with an algebraic subgroup of $C$, and $A$ with $C/B$. An exact sequence (1) is called an *extension* of $A$ by $B$; we shall often call $C$ itself an extension of $A$ by $B$ when no confusion is possible. Another extension $C'$ of $A$ by $B$ is called *equivalent* to the extension $C$ if there is a commutative diagram

$$\begin{tikzcd}
O \arrow[r] & B \arrow[r] \arrow[d, "id."'] & C \arrow[r] \arrow[d, "f"'] & A \arrow[r] \arrow[d, "id."'] & O \\
O \arrow[r] & B \arrow[r] & C' \arrow[r] & A \arrow[r] & O,
\end{tikzcd}$$

where $f$ is a homomorphism; in this case, $f$ is automatically a biregular isomorphism. The set of equivalence classes of extensions of $A$ by $B$ is denoted by Ext $(A, B)$. This is a functor which is contravariant in $A$, covariant in $B$ and additive in both $A$ and $B$. Especially we have

$$\text{Ext}(A, B\times B')\cong \text{Ext}(A, B)\times \text{Ext}(A, B')\,. \tag{2}$$

Lemma 2. *Assume in* (2) *that $A$, $B$ and $B'$ are defined over a field $k$, and let $C\in$* Ext$(A, B\times B')$ *and* $(C_1, C_2)\in$ Ext$(A, B)\times$Ext$(A, B')$ *be corresponding elements. Then $C$ is defined over $k$ if and only if both $C_1$ and $C_2$ are defined over $k$.*

This can be easily seen in following the proof of (2) in [**4**, VII-3].

We can define a composition law between the elements of Ext$(A, B)$ in a natural way, by which Ext$(A, B)$ becomes a commutative group whose neutral element is the class of trivial extension $A\times B$.

Suppose that $A$ and $B$ are connected, and that $B$ is linear. Then every extension $C$ of $A$ by $B$ has a rational section $s: A\to C$, which determines a symmetric factor system

$$h(x, y) = s(x+y)-s(x)-s(y)\,, \qquad x, y\in A\,, \qquad h(x, y)\in B\,.$$

This is a rational mapping of $A\times A$ into $B$, and satisfies the usual equations of factor systems. If we take another section, then $h$ is modified by a coboundary. Thus a class of symmetric factor systems corresponds to a given extension of $A$ by $B$. Conversely, every factor system $h$ determines a structure of pre-algebraic group on $A\times B$ which is an extension of $A$ by $B$; then, in view of Weil's theorem, there exists a group variety $C$ to which the factor system $h$ corresponds. We denote by $H^2_{rat}(A, B)$ the group of equivalence classes of rational symmetric factor systems from $A\times A$ into $B$. We have then

Lemma 3. *The group* Ext$(A, B)$ *is isomorphic to the group* $H^2_{rat}(A, B)$, *provided that $A$ and $B$ are connected and $B$ is linear* ([**4**, Chap. VII, Prop. 11]).

Suppose now that $A$ is an abelian variety, and consider the group Ext$(A, G_m)$ of equivalence classes of extensions of $A$ by the *multiplicative group* $G_m$. Take an extension $C$ of $A$ by $G_m$. As $G_m$ is linear, there exists a rational section $A\to C$, by which $C$ has a structure of principal fiber space over $A$ with group $G_m$, so that $C$ determines a linear equivalence class of divisors on $A$. Serre has shown, with the help of the absence of torsions of abelian varieites, that a divisor class $\{D\}$ corresponds to an element of Ext$(A, G_m)$ if and only if $D$ is algebraically equivalent to 0. We have thus

$$\text{(3)} \qquad \mathrm{Ext}(A, G_m) \cong P(A),$$

where $P(A)$ is a Picard variety of $A$.

LEMMA 4. *Suppose that $A$, $G_m$ and $P(A)$ in* (3) *are defined over a field $k$, and that an extension $C$ of $A$ corresponds to a point $c$ of $P(A)$. If $C$ is defined over $k$, then the point $c$ is algebraic over $k$.*

This can be easily seen in following the proof of (3) in [**4**, Chap. VII, pp. 5-10].

Clearly, a commutative group variety is generated by an abelian variety and a linear group variety if and only if it is isogenous to a direct product of an abelian variety and a linear group variety.

**7.** We can now prove the following

THEOREM 2. *Let $A$ be an abelian variety, $L$ a commutative linear group variety and $G$ an extension group of $A$ by $L$. Denote by $c = c(G)$ the equivalence class of $G$, $\in \mathrm{Ext}(A, L)$. Then $c$ is of finite order if and only if $G$ is generated by an abelian variety $A'$ and the linear group subvariety $L$. Moreover, when that is so, the order of $c$ divides the degree of the* 0*-cycle $A' \cdot L$.*

PROOF. Assume first that $c$ is of finite order $n$. Take a rational section $s: A \rightarrow G$. Then $h(x_1, x_2) = s(x_1 + x_2) - s(x_1) - s(x_2)$ is a corresponding rational symmetric factor system of $A \times A$ into $L$. In view of Lemma 3, our assumption implies that there exists a rational mapping $k$ of $A$ into $L$ such that

$$\text{(4)} \qquad nh(x_1, x_2) = ns(x_1 + x_2) - ns(x_1) - ns(x_2) = k(x_1) + k(x_2) - k(x_1 + x_2).$$

Put $\sigma(x) = ns(x) + k(x)$. Then $\sigma$ defines a homomorphism of $A$ into $G$, since $\sigma$ is generically a homomorphism by (4).. Calling $\pi$ the canonical homomorphism $G \rightarrow A$, we have $\pi\sigma(x) = n\pi s(x) - \pi k(x) = nx$ for a generic point $x$ of $A$ and so for every $x$ of $A$. If $\sigma(a) = 0$ for an element $a$ of $A$, then we have $\pi\sigma(a) = na = 0$. It follows from this that $\sigma: A \rightarrow \sigma(A)$ is an isogeny, since the number of elements $a$ of $A$ with $na = 0$ is finite. As $A$ is complete, $\sigma(A)$ is complete and an abelian variety. Since $\dim L + \dim \sigma(A) = \dim L + \dim A = \dim G$ and since $L \frown \sigma(A)$ is a finite set, we see that $G = L\sigma(A)$. We have thus proved that, if $c = c(G)$ is of finite order, then $G$ is generated by $L$ and an abelian variety $\sigma(A)$.

Assume conversely that the extension $G$ of $A$ is generated by $L$ and an abelian variety $A'$. Denote by $\lambda$ the restriction to $A'$ of the canonical homomorphism $G \xrightarrow{\pi} A$. It will follow that $\lambda^*(c) = 0$. In fact, $\lambda^*(G)$ is, by definition, the set of elements $(a', g)$ of $A' \times G$ with $\lambda(a') = \pi(a') = \pi(g)$, and $L$ is identified with the subgroup composed of elements $(0, l)$ with $l \in L$. The mapping $s: a' \rightarrow (a', a')$ defines clearly a section homomorphism of $A'$ into $\lambda^*(G)$; hence $\lambda^*(G)$ is biregularly isomorphic to the direct product of $A' \times L$, which implies that $\lambda^*(c) = 0$. Since $\lambda$ is an isogeny of $A'$ onto $A$, there exists an isogeny $\mu$ of $A$ onto $A'$ with $\lambda\mu = d\delta_A$ where $d = \nu(\lambda)$ and $\delta_A$ is the identity automorphism of $A$. As $\delta_A{}^* = 1$, it follows then that $0 = \mu^*\lambda^*(c) = (\lambda\mu)^*(c) = (d\delta_A)^*(c) = dc$. We see easily that $d = \nu(\lambda)$ is equal to the degree of the cycle $A' \cdot L$. Our Theorem is thus completely proved.

We shall now show that Theorem 1 can be obtained as a corollary to Theorem 2. Assume first that $G$ is an extension of an abelian variety $A$ by $(G_m)^n$, and that $G$ is defined over a finite field $k$; we may assume that $A$ and a Picard variety $P(A)$ of $A$ are also defined over $k$. It follows from (2) and (3) that

$$\mathrm{Ext}(A,(G_m)^n) \cong \mathrm{Ext}(A, G_m) \times \cdots \times \mathrm{Ext}(A, G_m) \cong P(A) \times \cdots \times P(A)\,.$$

Call $(c_1, \cdots, c_n)$ the element of $P(A) \times \cdots \times P(A)$ which corresponds to the extension $G$. As $G$ is defined over $k$, it follows from Lemma 2 and 4 that the point $(c_1, \cdots, c_n)$ is algebraic over $k$, which implies that the order of $(c_1, \cdots, c_n)$ is finite since the abelian variety $P(A)$ is defined over the finite field $k$. In view of our Theorem 2, this completes the proof of Theorem 1 in the special case we were considering.

If $G$ is an arbitrary group variety defined over a finite field $k$, then we can, as we have seen in the first proof of Theorem 1, reduce the problem to the special case which we have just proved. Namely, we can see that there exists a central group subvariety $D$ of $G$ defined over $k$ such that $G = DL$ and $D$ is divisible where $L$ is the maximal linear group subvariety of $G$, so that it is sufficient to prove our result in the case which we have already proved. We have thus proved Theorem 1 again.

Theorem 2 will also be applied to show the existence of a group variety which is not generated by an abelian variety and a linear group variety. Let $A$ be an abelian variety, and $P(A)$ a Picard variety of $A$. By (3), we have $\mathrm{Ext}(A, G_m) \cong P(A)$. Since the group $P(A)$ has points of infinite order, Theorem 2 shows that, *for an arbitrary given abelian variety $A$, there is an extension of $A$ by the linear group variety $G_m$ which is not generated by $G_m$ and an abelian variety.*

Musashi Institute of Technology,
Tokyo.

## References

[1] L. Barsotti, Structure theorems for group varieties, Ann. di Mat. (4), **38** (1955), 77-119.

[2] M. Rosenlicht, Some basic theorems on algebraic groups, Amer. J. Math., **78** (1956), 401-443.

[3] M. Rosenlicht, Commutative algebraic group varieties, Algebraic geometry and topology, A symposium in honor of S. Lefschetz, 151-156.

[ 4 ] J-P. Serre, Groupes Algebriques et Théorie du Corps de Classes, mimeographed notes at Collège de France, 1957.

[ 5 ] Y. Taniyama, Jacobian varieties and number fields, Proc. Int. Symp. Alg. Nb. Th. Tokyo-Nikko, 1955, 31-45.

[ 6 ] A. Weil, Variétés abéliennes et courbes algébriques, Paris, 1948.