Structure theorems for group-varieties (*).

by IACOPO BARSOTTI (a Los Angeles, Calif., U.S.A.).

Introduction and summary. - In the present paper we present certain results which describe with some detail the structure of group-varieties. For comments on what is *not* proved here we refer the reader to section 7 of this paper; we shall briefly mention here the results which are proved. First of all, we deal exclusively with group-varieties which are subvarieties of a projective space; that this is not a limitation is proved in a previous paper [4] (1); incidentally, the definitions of the terms and symbolism referring to group-varieties are given in such paper.

Section 2 of the present paper contains the obvious extension to group-varieties of the three « homomorphism theorems » of the theory of groups; the only feature which breaks the analogy with group-theory is the existence of homomorphisms of inseparability > 1; a particular case of the first homomorphism theorem is contained also in [6].

Section 3 deals with commutative group-varieties (called quasi-abelian varieties in [15]), and the main result states that any such variety is birationally equivalent (but not necessarily isomorphic) to the product of an abelian variety and a rational group-variety; in the language of group-theory, any commutative group-variety is the extension or a rational group-variety by an abelian variety. This analogy can be carried very far, and the extension can be described in terms of factor sets. As for the structure of rational commutative group-varieties, in the case of characteristic 0 this is very simply described by stating that any rational commutative group-variety over a field of characteristic 0 is the direct product of finitely many straight lines, each having either an additive or a multiplicative law of composition; this result seems to be in accordance with the main result of [15]. If the characteristic of the ground field is $p > 0$, the structure of rational commutative group-varieties is complicated by the existence of certain group-varieties (the periodic varieties) which are obtained by piecing together additive straight lines in a manner different from the construction of their direct product.

(*) This paper was presented in its present form (but for a correction submitted April 16, 1954) to a meeting held in Princeton in honor of S. LEFSCHETZ, on April 8, 1954. Results which largely overlap with sections 1, 2, 3 of this paper were announced at the same meeting by M. ROSENLICHT. *(This note added August 22, 1954).*

(1) Numbers in brackets refer to the bibliography at the end of the paper.

The commutative group-varieties, which extend a given rational group-variety by means of a given abelian variety, form a set which can be turned into a group by a suitable law of composition; according to the results of section 4, and to incomplete results mentioned in section 7, such group is isomorphic to the group of the points of a commutative group-variety, at least in the case of characteristic zero.

Section 6 deals with noncommutative group-varieties. Essentially, the noncommutativity is due to the existence of group-varieties which are the representative varieties of linear groups; we prefer to call such varieties « Vessiot varieties », since the natural alternate expression « linear-group varieties » is too easily misinterpreted as « linear group-varieties ». In the same manner as the structure of commutative group-varieties depends on the closed invariant differentials of the second and third kind, so the structure of noncommutative group-varieties depends on certain differentials which are invariant, but not closed, or, equivalently, on the noncommutativity of the invariant derivations; while the structure of the set of the derivations (Lie algebra) is known to describe completely the structure of the group-variety in the case of characteristic 0, this is not so when the characteristic is $p \neq 0$, and additional information must be obtained from the structure of the set of the invariant derivations of higher order; this is substantially what is done in section 6, although a more direct method is used, and the derivations play only a minor role. The main result of this section (Theorem 6.4) gives a considerable amount of information on the structure of noncommutative group-varieties, but not as much as would be desirable; it is quite evident that this result could stand improvement.

The ground field is assumed to be algebraically closed throughout this paper (with the exception of a few definitions); ouf course this assumption could be abandoned if one were prepared to extend the ground field whenever necessary, a device of which there are abundant examples in the literature (see for instance [16]). According to our definition of group-variety [4], the existence of group-varieties with singular points is not excluded; almost all of the results of this paper are stated for nonsingular group-varieties (see definition in section 1), as this shortens the proofs; a cursory reading will convince the reader that such hypothesis is not essential.

1. **Definitions and preliminary results.** - The definition of a group-variety is given in [4]; the terminology adopted throughout this paper is the one used in [1], [2], [3], [4]. A group-variety G over the field k, with degeneration locus F, shall be called ***nonsingular*** if every point of the extension $\bar{G}$ of G over the algebraic closure $\bar{k}$ of k, which does not belong to the extension $\bar{F}$ of F over $\bar{k}$, is simple on $\bar{G}$; if k is algebraically closed, and G is a normal group-variety over k, then G is nonsingular, by Theorem 1

of [4]. If k is algebraically closed, and $P \in G - F$, then σ_P and T_P^1 have the meanings stated in Theorem 1 of [4]; if v is a place of G with center P on G, we shall denote σ_P also by σ_v; the automorphism of $k(G)$ over k which is related to T_P^2 as σ_P is to T_P^1 shall be denoted by τ_P, or τ_v. The rules of operation for σ_P, τ_P are:

$$\sigma_{PQ} = \sigma_P\sigma_Q, \qquad \tau_{PQ} = \tau_Q\tau_P, \qquad \sigma_P\tau_Q = \tau_Q\sigma_P,$$

$$\sigma_{\sigma_P v} = \sigma_P\sigma_v, \qquad \sigma_{\tau_P v} = \sigma_v\sigma_P, \qquad \tau_{\sigma_P v} = \tau_v\tau_P, \qquad \tau_{\tau_P v} = \tau_P\tau_v;$$

here v is a place of G whose center on G is not on F. A group-variety G over k is said to be *commutative* if the law of composition on G is commutative. From now on, the ground field k shall be algebraically closed unless specifically stated otherwise. The point P of G such that $\sigma_P = 1$ (or $\tau_P = 1$) shall be denoted by E_G, or simply E if this does not generate confusion, and called the *identity of* G. Let G be a group-variety over the arbitrary field k, with the degeneration locus F; a subvariety V of G is a *group-subvariety of* G if (1) no component of V is a subvariety of F, (2) each component of V is absolutely irreducible, and (3) if P, $Q \in \overline{V} - (\overline{V} \cap \overline{F})$ (the bar denoting extension over the algebraic closure of k), then PQ and P^{-1} belong to $\overline{V}$; $\overline{V}$ has a component V_0 which contains the identity of $\overline{G}$. Let V_1, V_2 be components of $\overline{V}$, and let P_i ($i = 1, 2$) be a point of $\overline{V} - (\overline{V} \cap \overline{F})$ such that the only component of $\overline{V}$ containing P_i is V_i; then the smallest subvariety of $\overline{G}$ containing all the points $Q_iP_i^{-1}P_j$ ($j = 1, 2$; $j \neq i$), when Q_i ranges in $V_i - (V_i \cap \overline{F})$, is an irreducible sub-variety of $\overline{V}$ containing P_j, so that it is a subvariety of V_j. This proves that $\dim V_i = \dim V_j$, or that each component of V has the same dimension as V_0. But then the same construction can be repeated after abandoning the assumption that P_i be contained only in V_i, and assuming, instead, $P_1 = P_2 \notin \overline{F}$; this leads to the conclusion that $V_1 = V_2$, impossible. Hence V_0 is the only component of $\overline{V}$ which contains the identity, and will be called *the component of the identity in* V; two distinct components of $\overline{V}$ have no point in common ouside $\overline{F}$, and if V_0, $V_1, \dots, V_r$ are all the distinct components of V, then $V_0 - (V_0 \cap \overline{F})$ is a group, and the sets $V_i - (V_i \cap \overline{F})$ are the left and right cosets of this group in the group $\overline{V} - (\overline{V} \cap \overline{F})$; hence $V_0 - (V_0 \cap \overline{F})$ is an invariant subgroup of $\overline{V} - (V \cap \overline{F})$, and the factor group $(\overline{V} - (\overline{V} \cap \overline{F}))/(V_0 - V_0 \cap \overline{F})$ has finite order $r + 1$. Let V, W be group-subvarieties of G, and assume W to be a subvariety of V; then W is said to be *invariant in* V if the group $\overline{W} - (\overline{W} \cap \overline{F})$ is invariant in $\overline{V} - (\overline{V} \cap \overline{F})$. The group-variety G is said to be *simple* if $\overline{G}$ has no proper invariant (in $\overline{G}$) group-subvariety of positive dimension.

Let G, G' be group-varieties over the arbitrary field k, with degeneration loci F, F' respectively. A *homomorphism of* G *into* G is a rational mapping α of G into G' such that (1) $\bar{\alpha}[P]$ is a point of $\overline{G}' - \overline{F}'$ whenever $P \in \overline{G} - \overline{F}$, and (2) $\bar{\alpha}[PQ]=(\bar{\alpha}[P])(\bar{\alpha}[Q])$ if P, $Q\in\bar{G}-\bar{F}$. The subvariety G'' of G' on which α operates is an irreducible group-subvariety of G'. The integer ins $\alpha\{G''\}$ is called the *inseparability of* α, and α is said to be *separable* if its inseparability is 1. If $G''=G'$, then α is called a *homomorphism of* G *onto* G'. If E' is the identity of G', the join of all the components of $\alpha[E']$ which are not subvarieties of F has all the properties of a group-subvariety of G, except possibly the one stating that each of its components is absolutely irreducible; such join is called the *kernel of* α. If V is an irreducible subvariety of G, but not of F, and $\alpha'=[\alpha;\ V,\ G'']$, the subvariety of G'' on which α' operates is irreducible, and is not a subvariety of F'; it will be called the *image of* V *in* α, and denoted by αV; it has the property that its extension over $\bar{k}$ is the smallest subvariety of $\bar{G}$ containing all the $\bar{\alpha}[P]$ when P ranges over $\bar{V}-(\bar{V}\cap\bar{F})$. On the other hand, if V' is an irreducible subvariety of G'', but not of F', and $\alpha'=[\alpha;\ G,\ V']$, let $V_1,\dots,V_s$ be those, among the components of the subvariety of G on which α' operates, which are not subvarieties of F; the join of $V_1,\dots,V_s$ will be called the *inverse image of* V' *in* α, and denoted by $\alpha^{-1}V'$. The meaning of the symbols αV, $\alpha^{-1}V'$ is extended in an obvious manner to the cases in which V or V' is reducible. The *degree of* α is 0 if $\dim G''<\dim G$, and equals ord $\alpha\{G''\}$ if $\dim G''=\dim G$. If there exists a homomorphism of G onto G', then G' is said to be a *homomorphic image of* G. We say that G and G' are *isomorphic*, and write $G\cong G'$, if there exists a homomorphism of G onto G' which is also a homomorphism of G' onto G; such homomorphism is then a birational correspondence. The *product* of homomorphisms (as well as of rational mappings) is defined in the usual operatorial manner; the degree of the product of two homomorphisms equals the product of the degrees of the factors. An *endomorphism of* G is a homomorphism of G into a copy G' of G; the endomorphisms of degree 1, which are the isomorphisms of G onto itself, are called the *automorphisms of* G; they form a group with respect to the law of multiplication. If $\mathbf{G}$ has the same meaning as in Corollary 3 to Theorem 1 of [4], then an automorphism γ of $k(G)$ over k is related to an automorphism of G (as automorhisms of $k(G)$ are related to birational mappings of G onto itself) if and only if $\gamma\mathbf{G}\gamma^{-1}=\mathbf{G}$. The group-varieties G, G' over the arbitrary field k are said to be *isogenous* if each is a homomorphic image of the other; the relation of being isogenous is clearly reflexive, symmetrical and transitive. Let G, A be group-varieties over the arbitrary field k, with degeneration loci F, B respectively; the pseudo-variety $G\times A$ is birationally biregularly equivalent to a variety, which we shall still denote by $G\times A$. If P, P' are points of $\bar{G}-\bar{F}$, and Q, Q' of $\bar{A}-\bar{B}$, set $(P\times Q)(P'\times Q')=PP'\times QQ'$; this defines a law of composition on $G\times A$, and under such law $G\times A$ is a group-variety with the degeneration locus $(F\times A)\cup(G\times B)$. This group-variety is called the *direct product of* G *and* A.

Let G be a nonsingular group-variety over the arbitrary field k, with degeneration locus F, and let X be an irreducible cycle of G but not of F; let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G, as specified in section 1 of [4]; assume $k(G_i)$ $(i = 1, 2, 3)$ to be a subfield of $k(D)$ as prescribed by D; then a birational correspondence is established between $(G_2)_{k(G_1)}$ and $(G_3)_{k(G_1)}$, and in such correspondence the modified extension of X_2 over $k(G_1)$ corresponds to exactly one irreducible cycle Γ_X of $(G_3)_{k(G_1)}$, having the same dimension as X; this definition of Γ_X can be extended, by linearity, to any cycle X of G having no component variety on F. We shall also set $T_X = D_{\Gamma_X, G_1}$ (see section 3 of [1]); this notation is in accordance with the notation used in the proof of Theorem 3 of [4], and will be used consistently throughout this paper. We shall now assume, in order to simplify the notations, k to be algebraically closed; if X has the previous meaning and is irreducible, and if $P \in G - F$, the transform of X_2 according to the birational correspondence T_P^1 is an irreducible cycle of G_3 having the same dimension as X; we shall denote it by $(\sigma_P X)_3$, and this notation will be extended by linearity to the case in which X is reducible. The radical of $\sigma_P X$ is the smallest subvariety of G containing all the points PQ when Q ranges oves $\mathrm{rad}\, X - (F \cap \mathrm{rad}\, X)$. Let v be a place of G whose center on G is P, and let R be a point of $\mathrm{rad}\, \sigma_P X$ but not of F; then $Q = P^{-1}R \in \mathrm{rad}\, X - (F \cap \mathrm{rad}\, X)$. Let u be a place of G with center Q on G, compounded with a valuation w of $k(G)$ having as center on G one of the components of $\mathrm{rad}\, X$, say X', which contain Q; then the place (u_2, v_1) of $G_1 \times G_2$ (see Step 3 of the proof of Theorem 3 of [4] for the definition of this symbol) has on $G_1 \times G_2$ the center $P_1 \times Q_2$, and therefore has on G_3 the center R_3. Let w' be the extension of w_2 over $k(G_1)$; then (u_2, v_1) is compounded with w' and with a place of $K_{w'}$; this, in turn, induces a place of $k(T_{X'})$ which induces v_1 in $k(G_1)$, and which has on G_3 the center R_3; as a consequence, $R_3 \in \Gamma_X[v_1]$, and this fact proves that every component of $(\sigma_P X)_3$ is a component of $\Gamma_X[v_1]$. These steps can be retraced, and the result is that $\Gamma_X[v_1]$ is the join of $(\sigma_P X)_3$ and, possibly, of a subvariety of F_3; this last one may actually occur only if $F \cap \mathrm{rad}\, X$ is nonempty. Now assume X to be irreducible, and consider the birational correspondence β_X between $(X_2)_{k(G_1)}$ and Γ_X induced by the birational correspondence $D\{G_1\}$ between $(G_2)_{k(G_1)}$ and $(G_3)_{k(G_1)}$. Then β_X can also be considered as an algebraic correspondence between $k(G_1)$ and $X_2 \times G_3$; if this is done, set $B_X = D_{\beta_X, G_1}$, and consider B_X as an algebraic correspondence between $G_1 \times X_2$ and G_3. For a point $P_1 \times Q_2$ of $G_1 \times X_2$ such that $P, Q \notin F$, we have that $(\sigma_P X)_3$ appears in $T_X\{P_1\}^*$ with the same multiplicity e with which the correspondent component of $B_X[P_1]$ appears in $B_X\{P_1\}^*$. But then the multiplicity of $R_3 = D[P_1 \times Q_2]$ in $D\{P_1 \times Q_2\}^* = B_X\{P_1 \times Q_2\}^*$ is a multiple of e; since such multiplicity is 1, we conclude that $e = 1$, or that

$(\sigma_P X)_3$ appears with multiplicity 1 in $T_X\{P_1\}^*$. We shall make use of these results without specific reference to them. Another result of frequent use is the following one:

LEMMA 1.1. - *Let K be an algebraic function field over the arbitrary field k; let F, V be irreducible varieties over k, and let D be a rational mapping of F into V; let P be a rational point of F_K such that $D_K[P]$ is a rational point Q of V_K; let v be a place of K over k such that $K_v = k$, and set $P' = P[v]$, $Q' = Q[v]$, so that P', Q' are rational points of F, V respectively. Then $Q' \in D[P']$.*

PROOF. - We may assume D to be onto V; if $k(V)$ is then considered to be a subfield of $k(F)$ as prescribed by D, each place of F_K with center P on F_K has the center Q on V_K; let u be such a place, and let w be compounded with u and with the extension of v to K_u. Then P', Q' are the centers of w on F, V respectively, Q. E. D..

As a particular consequence of Lemma 1.1 we may consider the following case: let G be a group-variety over the arbitrary field k, with degeneration locus F; let K be an algebraic function field over k, and let P, Q, R be rational simple points of G_K but not of F_K, such that $PQ = R$; let v be a place of K over k such that $K_v = k$, and assume $P' = P[v]$ and $Q' = Q[v]$ to be simple points of G but not of F, and $R' = R[v]$ to be a simple point of G; then $R' \notin F$, and $R' = P'Q'$.

LEMMA 1.2. - *Let G be a group-variety over k, and let V be an irreducible group-subvariety of G, simple on G. Then V is a group-variety.*

PROOF. - Let F be the degeneration locus of G, and let G_1, G_2, G_3 be copies of G, and V_1, V_2, V_3 be the corresponding copies of V. If D is the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G, then $D\{V_1 \times V_2\}^* = \Delta'$ exists and is a rational point of $(G_3)_{k(V_1 \times V_2)}$, since $V_1 \times V_2$ is simple on $G_1 \times G_2$; set $D' = D_{\Delta', V_1 \times V_2}$; then D' operates on V_3. Since D' is the only component of $D \cap V_1 \times V_2 \times G_3$ which is not a subvariety of $F_1 \times G_2 \times G_3 \cup G_1 \times F_2 \times G_3 \cup G_1 \times G_2 \times F_3$, it also can be obtained by operating with $D\{V_1 \times V_3\}^*$ or $D\{V_2 \times V_3\}^*$; hence D' defines a normal law on V, Q. E. D..

LEMMA 1.3. - *Let G be a nonsingular group-variey over k, and let V be an irreducible group-subvariety of G. Then V is a nonsingular group-variety.*

PROOF. - V is a group-variety by Lemma 1.2. Let F be the degeneration locus of G, and let P be a point of $V - (V \cap F)$, simple on V; set $\mathbf{O} = Q(P/G)$, $\mathbf{P} = \mathbf{P}(V/G)$, $\mathbf{p} = \mathbf{P} \cap \mathbf{O}$; the fact that P is simple on V means that $\mathbf{O}/\mathbf{p}$ is a regular geometric domain. If P' is any point of $V - (V \cap F)$, and $\mathbf{O}'$, $\mathbf{P}'$, $\mathbf{p}'$ are related to P' as $\mathbf{O}$, $\mathbf{P}$, $\mathbf{p}$ are to P, we have $\mathbf{O}' = \sigma\mathbf{O}$, $\mathbf{P}' = \sigma\mathbf{P} = \mathbf{P}$, if $\sigma = \sigma_{P'}\sigma_P^{-1}$; hence $\mathbf{p}' = \sigma\mathbf{p}$, and therefore $\mathbf{O}'/\mathbf{p}'$ is isomorphic to $\mathbf{O}/\mathbf{p}$, and is consequently a regular geometric domain, Q. E. D..

2. **The homomorphism theorems.** - Let α, β be homomorphisms of a group-variety G over k onto group-varieties A, B respectively; we shall say that α, β are *equivalent* if there exists an isomorphism γ of A onto B such that $\beta = \gamma\alpha$; the relation of equivalence is reflexive, symmetrical and transitive. A *class* of homomorphisms means a class with respect to equivalence. Equivalent homomorphisms have the same kernel, degree and inseparability; they will be called respectively the *kernel, degree*, and *inseparability of* their *class*; a *separable class* is the class of a separable homomorphism.

THEOREM 2.1. (FIRST HOMOMORPHISM THEOREM). - *Let G be a nonsingular group-variety over k, with degeneration locus F; there exists a one-to-one correspondence between the set of the invariant group-subvarieties of G, and the set of the separable classes of homomorphisms of G onto group-varieties over k. The group-subvariety V and the class A correspond to each other if and only if V is the kernel of A; if β is a homomorphism of G onto G' of inseparability e and kernel V, and if α is a homomorphism of G onto B belonging to the class A which corresponds to V, there exists a homomorphism γ of B onto G', of inseparability e and kernel E_B, such that $\beta = \gamma\alpha$. Finally,* $\dim V + \dim G' = \dim G$, *and the group of the points of B which do not belong to the degeneration locus of B is isomorphic to the group* $(G - F)/(V - (V \cap F))$.

If V, A, α, B have the meanings just stated, then B (which is determined but for an isomorphism) is called the *factor variety of V in G*, and denoted by G/V, while α (which is determined but for equivalence) is called the *natural homomorphism of G onto B*. We shall always select a nonsingular B.

PROOF. - Let V be given; let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Set $L_1 = G_{\Gamma_V}$ (see the definition preceding Theorem 4.1 of [1] for the symbol G_{Γ_V}), so that $k(L_1)$ is a subfield of $k(G_1)$; we assume L_2, L_3 to be copies of L_1, related to G_2, G_3 respectively as L_1 is to G_1. Let Λ_1 be the irreducible algebraic correspondence between $k(L_1)$ and G_1 generated by the embedding of $k(L_1)$ in $k(G_1)$. Let v_1, w_1 be nondegenerate places of G_1 which induce in $k(L_1)$ the same place u_1; then $\Gamma_V[v_1] = \Gamma_V[w_1]$, and therefore $\sigma_v V = \sigma_w V$; in particular, $\sigma_w E_G \in \sigma_v V$, so that the center of w on G belongs to $\sigma_v V$. This proves that the components of $\Lambda_1[u_1]$ which are not subvarieties of F_1 are necessarily subvarieties of $(\sigma_v V)_1$. On the other hand, let v be a nondegenerate place of G whose center on G is generic, and let u be induced by v in $k(L)$; let w be a nondegenerate place of G whose center on G is on $\sigma_v V$; then $\sigma_w V = \sigma_v V$. But in this case, $(\sigma_v V)_3 = \Gamma_V\{v_1\}^*$, and therefore w_1 has on L_1 the same center as v_1. This proves that if the center of u_1 on L_1 is generic, then $\Lambda_1[u_1]$ has, outside F_1, the same components as $(\sigma_v V)_1$. Now, each component variety of Γ_V has inseparability 1, and therefore Γ_V is the modified extension, over $k(G_1)$, of a cycle Γ of $(G_3)_{k(L_1)}$, and each component variety of Γ has inseparability 1; if $T' = D_{\Gamma, L_1}$, we have that a generic $P_3 \in G_3$ belongs to exactly one $(\sigma_v V)_3$, so that $T'[P_3]$ is a point of L_1. As a consequence, Γ is irreducible, and $k(T')$ is a purely inseparable finite extension of $k(G_3)$; on the other hand, if X is any component of V, $k(T_X)$ contains $k(T')$, and ins $(k(T_X) : k(G_3)) = 1$; hence $k(T')$ is separable over $k(G_3)$, or $k(T') = k(G_3)$, and $k(L_1) \subseteq k(G_3)$. It now follows, from ins $\Gamma = 1$, that ins $(k(T') : k(L_1)) = 1$, so that also ins $(k(G_1) : k(L_1)) = 1$. We now consider $k(G_i)$, $k(L_i)$ $(i = 1, 2, 3)$ as subfields of $k(D)$. Let w be a place of D with centers P_1, Q_2, R_3, P_1', Q_2', R_3' on, respectively, G_1, G_2, G_3, L_1, L_2, L_3, and assume $P_1 \times Q_2$ to be generic on $G_1 \times G_2$. Set $Z_i = D_{\Lambda_i, L_i}$; then $P_1 \in Z_1[P_1'] = (\sigma_P V)_1$, $Q_2 \in Z_2[Q_2'] = (\sigma_Q V)_2$, $R_3 \in Z_3[R_3'] = (\sigma_R V)_3$; but, since V is invariant, $\sigma_R V = \sigma_P \sigma_Q V$ depends only on $\sigma_P V$ and $\sigma_Q V$; hence R' depends only on P', Q', a fact which shows that each element of $k(L_3)$ is purely inseparable over $k(L_1 \times L_2)$; since ins $(k(G_1 \times G_2) : k(L_1 \times L_2)) = 1$, this implies that $k(L_3) \subseteq k(L_1 \times L_2)$. Similar results can be obtained for any permutation of the indices 1, 2, 3; hence the embedding of $k(L_i)$ into $k(D)$ generates a rational mapping D' of $L_i \times L_j$ onto L_h, for any permutation (i, j, h) of $(1, 2, 3)$, and it is quite easily seen that D' gives a normal law on L. According to Theorem 3 of [4], L is birationally equivalent to a variety B which is a group-variety, with a degeneration locus C, under the law Y induced by D'.

Let α be the rational mapping of G onto B generated by the embedding of $k(B)$ into $k(G)$. We contend that α is a homomorphism with kernel V. First of all, if $P \in G - F$ and $P' \in \alpha[P]$, let v be a place of G with centers P, P' on G, B respectively; if v' is the extension of v_1 over $k(G_2)$, then v' is a valuation of $k(D)$ which induces the trivial valuation in $k(G_3)$, hence in $k(B_3)$, a fact which proves that $P' \notin C$; in addition, σ_P induces $\sigma_{P'}$ in $k(B)$, and this shows that $P' = \alpha[P]$. Moreover, if $Q \in G - F$ and $Q' = \alpha[Q]$, we have that $\sigma_{PQ} = \sigma_P \sigma_Q$ induces $\sigma_{P'} \sigma_{Q'} = \sigma_{P'Q'}$ in $k(B)$, so that $\alpha[PQ] = (\alpha[P])(\alpha[Q])$, as requested. Finally, $P \notin F$ belongs to the kernel of α if and only if σ_P induces the identical automorphism in $k(B)$, or in $k(L)$; and this is so if and only if, for a generic Q of G, $\sigma_P \sigma_Q V = \sigma_Q V$, that is, if and only if $P \in V - (V \cap F)$. Hence V is the kernel of α.

Now let β and G' be given as in the statement of the theorem. Let P' be a generic point of G', so that $\beta[P']$ has no component on F; if P, Q belong to $\beta[P']$ but not to F, then $\beta[P^{-1}Q] = E_{G'}$, so that $Q \in \sigma_P V$. Viceversa, if $Q \in \sigma_P V - (F \cap \sigma_P V)$, then $\beta[Q] = P'$. Hence $\beta[P'] = \sigma_P V$. This proves that the algebraic system of the $(\beta\{G'\})\{u\}$, when u ranges over the places of G', coincides with the set of the multiples, according to a fixed integer, of the elements of the algebraic system of the $(\alpha\{B\})\{v\}$, when v ranges over the places of B; hence there exists an algebraic correspondence γ between G' and B such that $k(\gamma)$ is a purely inseparable finite extension of $k(G')$ and $k(B)$, and such that if P' is a generic point of G', then $\gamma[P']$ is the point P

of B such that $\beta[P'] = \alpha[P]$. Now, $B \times G'$ is birationally biregularly equivalent to a variety, which will still be denoted by $B \times G'$; then γ is an irreducible subvariety of $B \times G'$. Consider $\alpha\{G\}$ and $\beta\{G\}$ as rational points of $B_{k(G)}$, $G'_{k(G)}$ respectively, so that $\alpha\{G\} \times \beta\{G\}$ is a rational point X of $(B \times G')_{k(G)}$. For a place v of G, with generic center P on G, we have $X[v] = \alpha[P] \times \beta[P] \in \gamma$; conversely, we have seen that a generic point of γ is of the type $X[v]$. Hence γ is the subvariety of $B \times G'$ on which X operates, so that we can assume $k(\gamma) \subseteq k(G)$. As no element of $k(G)$ is purely inseparable over $k(B)$, we conclude that $k(\gamma) = k(B)$, and that $k(B)$ is a purely inseparable extension of $k(G')$. Moreover, $[k(B) : k(G')] = \text{ins}\,(k(G) : k(G')) = e$. Now it is clear that γ is a homomorphism of B onto G', of inseparability e and kernel E_B, and that $\gamma\alpha = \beta$. The one-to-one correspondence $V \to A$ (where A is the class of α) is obtained by setting $e = 1$, Q. E. D..

A particular case of this result forms the object of [6]. From the previous proof, it is easily seen that if α is a homomorphism of the group-variety G over k onto the group-variety G', and V' is an irreducible subvariety of G', but not of its degeneration locus, then $V = \alpha^{-1}V'$ is the smallest subvariety of G which contains all the $P \in G - F$ (F being the degeneration locus of G) such that $\alpha[P] \in V'$; moreover, any $P \in \alpha^{-1}V' - (F \cap \alpha^{-1}V')$ is such that $\alpha[P] \in V'$.

Lemma 2.1. - *Let G be a group-variety over k, with degeneration locus F, and let V be an invariant group-subvariety of G; let $H = k(G/V)$ be considered as a subfield of $K = k(G)$ as prescribed by the natural homomorphism of G onto G/V. Then H is the set of the elements $x \in K$ such that $\sigma_P x = x$ for every $P \in V - (V \cap F)$. And if $\sigma_P x = x$ for each $x \in H$, then $P \in V - (V \cap F)$.*

Proof. - We may assume G to be nonsingular. Let α be the natural homomorphism of G onto $B = G/V$; let $P \in G - F$, and set $P' = \alpha[P]$. We have seen in the course of the proof of Theorem 2.1 that σ_P induces $\sigma_{P'}$ in H; hence $\sigma_P x = x$ for each $x \in H$ if and only if $\sigma_{P'} = 1$, i. e. if and only if $P \in V$. Let now $x \in K$ be such that $\sigma_P x = x$ for each $P \in V - (V \cap F)$, and set $H' = H(x)$. Let B' be a model of H' over k, and let Q be a generic point of B; let Z be the rational mapping of B' onto B generated by the embedding of H into H'. There exists a nondegenerate place v' of K over k with center Q on B; let Q' be the center of v' on B'; let Q'' be another point of B' obtained from Q by means of another nondegenerate place v''. Then Q', $Q'' \in Z[Q]$, and there exist points P', P'' of $G - F$ such that Q', Q'' correspond to P', P'' respectively in the rational mapping T of G onto B' generated by the embedding of H' into K. As Q is generic, we may select P' to be such that $Q' = T[P']$; since $\alpha[P'] = \alpha[P''] = Q$, we have $P' = \sigma_P P''$ for a $P \in V - (V \cap F)$; hence $\sigma_P v''$ has the center P' on G, and the center Q' on B'. But $\sigma_P v''$ and v'' induce the same valuation in H'; therefore $Q' = Q''$. This proves that for a generic Q of B, $Z[Q]$ is a point of B', a fact which indicates that H' is a purely inseparable extension of H. Since ins $(K:H) = 1$, we conclude that $H' = H$, $x \in H$, Q. E. D..

LEMMA 2.2. - *Let G, A be group-varieties over k, with degeneration loci F, B respectively, and let α be a homomorphism of G onto A. Assume $H = k(A)$ to be a subfield of $K = k(G)$ as prescribed by α. Then, for any $P \in G - F$, we have $\sigma_P H = H$, and σ_P induces in H the automorphism $\sigma_{P'}$, if $P' = \alpha[P]$.*

PROOF. - We may assume G to be nonsingular. Let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Consider $k(G_i)$ as a subfield of $k(D)$ as prescribed by D; let A_i, α_i be copies of A, α respectively, and let $k(A_i)$ be considered as a subfield of $k(G_i)$ as prescriaed by α_i $(i = 1, 2, 3)$. Then the smallest subfield of $k(D)$ containing $k(A_1)$ and $k(A_2)$ also contains $k(A_3)$, and the embedding of $k(A_i)$ in such a field generates a rational mapping D' of $A_1 \times A_2$ onto A_3 which gives the law of composition on A. If v is a nondegenerate place of G, and w is induced in $k(A)$ by v, let v', w' be the extensions of v_1, w_1 over $k(G_2)$, $k(A_2)$ respectively, so that v' induces w' in $k(D')$. If $x \in k(A)$, we have $x_3 - (\sigma_v^{-1} x)_2 \in \mathbf{P}_{v'}$, and also $x_3 - (\sigma_w^{-1} x)_2 \in \mathbf{P}_{w'} \subseteq \mathbf{P}_{v'}$, so that $(\sigma_v^{-1} x - \sigma_w^{-1} x)_2 \in \mathbf{P}_{v'} \cap k(G_2)$, or $\sigma_v^{-1} x = \sigma_w^{-1} x$, Q. E. D..

LEMMA 2.3. - *Let G, A be nonsingular group-varieties over k, with degeneration loci F, B respectively; let α be a rational mapping of G into A such that $\alpha[PQ] = (\alpha[P])(\alpha[Q])$ for a generic pair of points P, Q of G. Then α is a homomorphism of G into A.*

PROOF. - Let A_1, A_2, A_3 be copies of A, and let D be the rational mapping of $A_1 \times A_2$ onto A_3 which gives the law of composition on A; let G_1, G_2, G_3, D' be similarly related to G; consider $k(G_i)$ to be a subfield of $k(D')$ as prescribed by D' $(i = 1, 2, 3)$. The rational mapping $\alpha' = \alpha\{G\}$ is a rational point of $A_{k(G)}$; we shall consider the copies α_i' of α' on $(A_i)_{k(G_i)}$ $(i = 1, 2, 3)$, and the modified extensions α_i of α_i' over $k(D')$. Our assumption implies that if D^* is the modified extension of D over $k(D')$, then $D^*[\alpha_1 \times \alpha_2] = \alpha_3$; Lemma 1.1 yields that if w is a place of D', and u_1, v_2, z_3 are the places induced by w in $k(G_1)$, $k(G_2)$, $k(G_3)$ respectively, we have $(\alpha'[z])_3 \in D[(\alpha'[u])_1 \times (\alpha'[v])_2]$. The set of the centers on G of the places v such that $\alpha'[v] \in B$ is a proper subvariery C of G; if $C \subseteq\!\!|\!\!\equiv F$, it is possible to select w in such a manner that the centers of u and z on G are not on $C \cup F$, while the center of v on G is on C but not on F; the previous relation implies, however, that $\alpha'[z] \in B$ if $\alpha'[u] \notin B$ and $\alpha'[v] \in B$ (for nondegenerate u, v, z); as this is a contradiction, we conclude that $C \subseteq F$. But then we can state, more precisely, that $\alpha'[z] = (\alpha'[u])(\alpha'[v])$ if u, v, z are nondegenerate. Now, the fundamental locus of α on G is also a proper subvariety C' of G; if $C' \subseteq\!\!|\!\!\equiv F$, it is possible to select w in such a manner that the centers P, Q of, respectively, u, v on G are not on $C' \cup F$, while the center R of z on G is on C' but not on F; this contradicts the previous relation, since such relation implies that $\alpha'[z]$ depends only on P and Q, hence only on the center $R = PQ$ of z. Therefore $C' \subseteq F$, Q. E. D..

THEOREM 2.2. (SECOND HOMOMORPHISM THEOREM). - *Let G be a nonsingular group-variety over k, with degeneration locus F, and let V, W be invariant group-subvarieties of G, such that $W \subseteq V$; set $B = G/W$, and let α be the natural homomorphism of G onto B; set $A = \alpha V$. Then A is an invariant group-subvariety of B; set $C = B/A$, and let β be the natural homomorphism of B onto C; let γ be the natural homomorphism of G onto G/V; then γ is equivalent to $\beta\alpha$.*

PROOF. - We may assume $k(B) \subseteq k(G)$ as prescribed by α; the fact that A is an invariant group-subvariety of B is a consequence of group-theoretical considerations. We can further assume $k(C) \subseteq k(B)$ as prescribed by β. Then Lemma 2.1 shows that $k(C)$ is the set of the elements of $k(G)$ which are invariant under all the σ_P for $P \in V - (V \cap F)$, so that C is birationally equivalent to G/V, and the inseparability of $\beta\alpha$ is 1. But then, since γ and $\beta\alpha$ have the same kernel V, Theorem 2.1 implies that γ is equivalent to $\beta\alpha$, Q. E. D..

Let A, B be irreducible subvarieties of a group-variety G over k, but not of the degeneration locus F of G. Let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. The irreducible subvariety C of G such that C_3 is the subvariety of G_3 on which $[D; A_1 \times B_2, G_3]$ operates will be denoted by (A, B); we have $(A, B) \subseteq\!\!|\!\!\sqsubseteq F$, and (A, B) is the smallest subvariety of G containing all the points PQ, when P ranges over $A - (A \cap F)$ and Q ranges over $B - (B \cap F)$. If A, B are not irreducible, but none of their components is a subvariety of F, (A, B) can be defined by means of an obvious generalization of the previous definition. If A, B are group-subvarieties of G, then (A, B) is a group-subvariety of G if and only if $(A, B) = (B, A)$. The symbol $(A, B, C, ...)$ is the natural generalization of (A, B).

THEOREM 2.3. (THIRD HOMOMORPHISM THEOREM). - *Let G be a nonsingular group-variety over k, with degeneration locus F; let A, B be irreducible group-subvarieties of G such that (A, B) is a group-variety of which B is an invariant group-subvariety (this being the case, in particular, if B is invariant in G). Let C be the join of those components of $A \cap B$ which are not subvarieties of F. Then there exists an integer e such that eC is part of the intersection $(A \cap B, (A, B))$; C is an invariant group-subvariety of A, and there exists a homomorphism β of A/C onto $(A, B)/B$ whose kernel is the identity, and whose degree is e.*

PROOF. - By Lemma 1.3, we may assume $(A, B) = G$. The fact that C is an invariant group-subvariety of A is proved by an elementary group-theoretical argument. Let α be the natural homomorphism of G onto $G' = G/B$; then $\alpha' = [\alpha; A, G']$ is a homomorphism of A onto G', whose kernel is evidently C. Therefore C has the pure dimension $\dim A - \dim G' = \dim A + \dim B - \dim G$, so that, if C' is any component of C, the intersection multiplicity $i(C', A \cap B, G)$ exists and is a positive integer, by Theorem 5.11 of [3]. By Theorem 2.1, there exists a homomorphism β of $A' = A/C$ onto G' whose kernel is the identity; then the degree of β equals $e = \operatorname{ins} \alpha'\{G'\}$. Let A^* be the modified extension of $1A$ over $k(G')$; then, by the definition preceding Lemma 1.2 of [3], $\alpha'\{G'\}$ is the only part of $(\alpha\{G'\} \cap A^*, G_{k(G')})$ which operates on the whole A; and since no point of $A - (A \cap F)$ is fundamental for α', we also have that if $\operatorname{rad} \alpha\{G'\} \cap \operatorname{rad} A^*$ has components which do not operate on the whole A, then each one of them must operate on a subvariety of $A \cap F$. If v is a place of G' whose center on G' is $E_{G'}$, we have seen that $(\alpha\{G'\})\{v\}^*$ coincides, but for component varieties on F, with B, so that the law of the conservation of the number (Theorem 5.7 of [3]) implies that $(\alpha'\{G'\})\{v\}^*$ coincides, but for component varieties on F, with $(A \cap B, G)$; therefore $(A \cap B, G) = eC$, but for component varieties on F, Q. E. D..

COROLLARY. - *Let G be a nonsingular group-variety over k, with degeneration locus F, and let A, B be irreducible group-subvarieties of G such that $G = (A, B)$, and that $PQ = QP$ whenever P, Q are points of A, B respectively, but not of F. Assume $(A \cap B, G) = E_G$; then $G \cong A \times B$.*

PROOF. - Set $A' = G/B$, and let α be the natural homomorphism of G onto A'; from Theorem 2.3 and its proof, and under the present conditions, we obtain that $A' \cong A/E_G \cong A$, and that α induces an isomorphism between A and A'; in like manner the natural homomorphism β of G onto $B' = G/A$ induces an isomorphism between B and B'. Set $\alpha' = \alpha\{G\}$, $\beta' = \beta\{G\}$, $\gamma' = \alpha' \times \beta'$, $\gamma = D_{\gamma', G}$, so that γ is a homomorphism of G onto the direct product $A' \times B'$, with kernel E_G. We shall consider $k(A' \times B')$ to be a subfield of $k(G)$ as prescribed by γ. Since α and β are separable, we have that $\operatorname{ins}(k(G) : k(A')) = \operatorname{ins}(k(G) : k(B')) = 1$; the definition of inseparability (section 1 of [2]), and the fact that the smallest perfect extension of $k(A' \times B')$ is the quotient field of the direct product, over k, of the smallest perfect extensions of $k(A')$, $k(B')$, imply then that $\operatorname{ins}(k(G) : k(A' \times B')) = 1$, or that γ is an isomorphism, Q. E. D..

3. Commutative group-varieties. - Let G be an n-dimensional projective space over the arbitrary field k, with n. h. g. p. $\{x_1, \ldots, x_n\}$, and let us define a law of composition on G by means of the rational mapping D of $G_1 \times G_2$ onto G_3 given by $(x_i)_3 = (x_i)_1 + (x_i)_2$ $(i = 1, \ldots, n)$. Then G becomes a commutative group-variety, with the hyperplane at infinity (for $\{x\}$) as degeneration locus; such group-variety, or any one isomorphic to it, is called an n-dimensional *vector variety*; if $n > 0$, it is isomorphic to the direct product of n 1-dimensional vector varieties. If D is defined by

$(x_i)_3 = (x_i)_1(x_i)_2$, G becomes a commutative group-variety, whose degeneration locus consists of the hyperplane at infinity, and of the n hyperplanes $x_i = 0$; such group-variety, or any isomorphic to it, is called a *logarithmic variety,* and is isomorphic, if $n > 0$, to the direct product of n 1-dimensional logarithmic varieties.

LEMMA 3.1. - *Let G be a simple commutative group-variety over k, of dimension > 1; then G is an abelian variety.*

PROOF. - We may assume G to be nonsingular. Let F, n be, respectively, the degeneration locus and the dimension of G; we shall assume $n > 1$, and F to be nonempty, and prove that G cannot be simple. Let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Let X be an $(n-1)$-dimensional unmixed effective (integral) cycle on G, none of whose component varieties is a subvariety of F, and set $(H_X)_1 = G_{\Gamma_X}$ (see section 1). Let V be the set of all the $P \in G - F$ such that $\sigma_P X = X$; then V is a group, and the smallest subvariety V_X of G containing V is a group-subvariety of G, and has the property that $V_X - V \subseteq F$. Since G is commutative, V_X is invariant in G, so that $B_X = G/V_X$ exists. The embedding of $k(B_X)$ and $k(H_X)$ into $k(G)$ generates an algebraic correspondence D' between B_X and H_X. Given a generic $P \in H_X$, there exists a $Q \in G - F$ such that the nondegenerate places v of G whese center on H_X is P are all and only those for which $(\sigma_v X)_3 = \Gamma_X[v_1] = (\sigma_Q X)_3$; such v's are also all and only those for which $\sigma_v^{-1} Q \in V_X$, hence also all and only those for which $\sigma_v V_X = \sigma_Q V_X$, and finally all and only those which have on B_X a certain fixed center. The argument can be retraced, and proves that $D'[P]$ is a point whenever P is a generic point of either H_X or B_X. Hence the smallest subfield of $k(G)$ which contains $k(B_X)$ and $k(H_X)$ is a purely inseparable extension of $k(B_X)$ and $k(H_X)$. But $\operatorname{ins}(k(G) : k(B_X)) = 1$ by Theorem 2.1, so that $k(B_X)$ is a purely inseparable extension of $k(H_X)$. These notations will be maintained in the rest of this proof. Assume now G to be simple; then for each $(n-1)$-dimensional effective cycle X of G, with no component variety on F, V_X is zero-dimensional. Let X be such a cycle, and suppose that there exists a degenerate place v of G such that $\Gamma_X\{v_1\}^*$ has component varieties which are not subvarieties of F; let, for instance, $\Gamma_X\{v_1\}^* = \Sigma_{i=1}^r a_i(X_i)_3 + \Sigma_{j=1}^s b_j(X_j')_3$, where no X_i is a subvariety of F, while each X_j' is a subvariety of F, hence a component of F. Set $Y = \Sigma_i a_i X_i$; for any nondegenerate place u of G, there exists an automorphism ρ_u of $k(D)$ over $k(G_2)$ which induces $(\sigma_u)_1$, $(\sigma_u)_3$ in $k(G_1)$, $k(G_3)$ respectively. Then, if the center of u on G is generic, we have

$$\begin{aligned}(1)\qquad \Gamma_X\{(\sigma_u v)_1\}^* &= \Gamma_X\{\rho_u v_1\}^* = \rho_u \Sigma_i a_i(X_i)_3 + \\ &+ (\text{cycle of } F_3) = (\sigma_u Y)_3 + (\text{cycle of } F_3) = \\ &= \Gamma_Y\{u_1\}^* + (\text{cycle of } F_3).\end{aligned}$$

Let G' be a normal model of $k(G)$, and let T_X', T_Y' be the algebraic correspondences between G_1' and G_3 induced by, respectively, T_X and T_Y; let G' be selected in such a way that T_X' and T_Y' have no fundamental point on G_1' (see Theorem 4.3 of [1]); let likewise G'' be a normal model of $k(G)$, let D'' be the rational mapping of $G_1' \times G_2''$ onto G_3' induced by D, and select G'' in such a way that D'' has no fundamental point on G_2''. Let Q be the center of v on G'', and let T be the only component of $D''[Q_2]$ which operates on the whole G_1' (see Theorem 1 of [4]). Then for a place u whose center on G' is a generic P, the center of $(\sigma_u v)_3$ on G_3' is $T[P_1]$, and this is a generic point R_3 of the proper subvariety F_3' of G_3' on which T operates. Hence for such u we have $\Gamma_X\{(\sigma_u v)_1\}^* = T_X'\{R_1\}^*$, and $\Gamma_Y\{u_1\}^* = T_Y'\{P_1\}^*$, so that formula (1) implies that $T_X'\{R_1\}^* = T_Y'\{P_1\}^* +$ (cycle of F_3). If $T'' = \{T_X'; F_1', G_3\}^*$ (see section 1 of [2]), this can be written $T''\{R_1\}^* = T_Y'\{P_1\}^* +$ (cycle of F_3). This indicates that a generic element of the algebraic system whose elements are the $T''\{R_1\}^*$ is the sum of $T_Y'\{P_1\}^*$ and of the cycle denoted by (cycle of F_3), which can vary among finitely many cycles only. Hence (cycle of F_3) is fixed, and the algebraic system formed by the $T_Y'\{P_1\}^*$ has dimension $\leq \dim F' < n$, so that $\dim B_Y < n$, and $\dim V_Y > 0$. This contradicts the assumption that G be simple, and we must conclude that *if G is simple, for each $(n-1)$-dimensional unmixed effective cycle X of G, with no component variety on F, and for each degenerate place v of G, every component of $\Gamma_X[v_1]$ is a component of F_3*; this also shows that $\dim F = n - 1$. According to the proof of Theorem 3 of [4], it is possible to select X in such a way that H_X is a model of $k(G)$, and is a group-variety isomorphic to G under the law of composition induced by D, in which case we can select $B_X = H_X \cong G$. A place v of H_X is such that its center P on H_X belongs to the degeneration locus of H_X if and only if $\Gamma_X[v_1]$ is a join of components of F_3; since this may happen only for finitely many points P, we conclude that the degeneration locus of H_X is zero-dimensional. But H_X is simple, so that is degeneration locus must be $(n-1)$-dimensional, as previously shown. Since $n > 1$, this contradiction proves that G is not simple, Q. E. D..

The following result, and its proof, are generalizations of Proposition 25 of [16] and its proof:

THEOREM 3.1. - *Let G be a nonsingular group-variety over k, and let A be an abelian group-subvariety of G; then there exists a homomorphism α of G onto A; if B is the component of the identity in the kernel of α, then $\dim (A \cap B) = 0$, and $G = (A, B)$.*

PROOF. - Set $n = \dim G$, $r = \dim A$, and assume $0 < r < n$ (otherwise the result would be trivial). Let F be the degeneration locus of G, and let P be a fixed (simple) point of A. Since P is simple on G, it is possible to find an $(n-r)$-dimensional irreducible cycle X of G, containing P, and such that $i(P, A \cap X, G) = 1$. Let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Set $E = E_G = E_A$; because of the properties of T_X, $[T_X;\ G_1,\ A_3]$ has exactly one component T' such that the subvariety of G_1 on which it operates is not a subvariety of F_1; we have $\dim T' = \dim T_X - n + r = n$; and $T'[R_3]$, for $R \in A$, coincides, but for components on F_1, with $T_X[R_3]$. Therefore, if W_1 is the subvariety of G_1 on which T' operates, we have $E_1 \in W_1$, and P_3 is a component of $T'[E_1]$. If $n' = \dim W$, each component of $T'[E_1]$ has dimension $\geq \dim T' - n' = n - n'$; since P_3 is one of such components, we conclude that $n' = n$, i. e. that T' operates on the whole G_1. But then $\Lambda = T'\{G_1\} = \Gamma_X \cap (A_3)_{k(G_1)}$. Since Λ is a simple point of $(G_3)_{k(G_1)}$, we conclude that $\Lambda'' = (\Gamma_X \cap (A_3)_{k(G_1)},\ (G_3)_{k(G_1)})$ exists and is a multiple of Λ. The condition $i(P,\ A \cap X,\ G) = 1$, and the law of the conservation of the number (Theorem 5.7 of [3]), imply then that $\Lambda'' = \Lambda$, and that $\operatorname{ins} \Lambda = 1$; as a consequence, there exists a normal separable extension K of $k(G_1)$ such that the extension Λ' of Λ over K has the form $\Lambda' = \Sigma_i \Lambda_i$, each Λ_i being a rational simple point of $(G_3)_K$, not on $(F_3)_K$. Set $\theta' = \Pi_i \Lambda_i$ (the order in which the product is performed being immaterial since $\Lambda_i \in (A_3)_K$); then, by Corollary 3 to Theorem 1 of [4], θ' is a rational point of $(A_3)_K$; but any automorphism of K over $k(G_1)$ simply interchanges the Λ_i, so that it leaves θ' invariant; hence θ' is the extension over K of a rational point θ of $(A_3)_{k(G_1)}$, that is, a rational mapping of $k(G_1)$ into A_3. But then, by the remarks opening No 19 of [16], there exist a homomorphism α of G_1 into A_3, and a point Q_3 of A_3, such that $\theta = (Q_3)_{k(G_1)} \alpha\{G_1\}$. For a place v of G whose center R on G is generic, $(\sigma_v X \cap A,\ G)_3$ exists and coincides with $\Lambda\{v_1\}^*$, while $\theta\{v_1\}^* = \Pi_i \Lambda_i\{v'\}^*$, if v' is any place of K over k which induces v_1 in $k(G_1)$; since the $\Lambda_i\{v'\}^*$ are all the intersections of $\sigma_v X$ and A, we conclude that, for any point S of A, we have $\theta\{(\sigma_S v)_1\}^* = (S^d)_3 \theta\{v_1\}^*$, if $d = \operatorname{ord} \Lambda$. This means that $Q_3 \alpha[S_1 R_1] = S_3{}^d Q_3 \alpha[R_1]$; then $\alpha[S_1 R_1] = S_3{}^d \alpha[R_1]$, or $(\alpha[S_1])(\alpha[R_1]) = S_3{}^d \alpha[R_1]$, and $\alpha[S_1] = S_3{}^d$. Therefore α is a homomorphism onto A_3 (see Proposition 24 of [16]). If B_1 is the component of the identity in the kernel of α, for each S_1 of $B_1 \cap A_1$ we have $\alpha[S_1] = E_3$, hence $S_3{}^d = E_3$, so that S_1 also belongs to the zero-dimensional kernel of the homomorphism β of A_1 onto A_3 such that $\beta[S_1] = S_3{}^d$; therefore $B_1 \cap A_1$ is zero-dimensional, Q. E. D..

Let G, G' be nonsingular commutative group-varieties over k, with the degeneration loci F, F' respectively. Let G_1, G_2 be copies of G, and let γ be a rational mapping of $G_1 \times G_2$ into G', operating on a subvariety of G' but not of F'; we say that γ is a *factor set of G into G'* if $(\gamma[P_1 \times Q_2 R_2])(\gamma[Q_1 \times R_2]) = (\gamma[P_1 Q_1 \times R_2])(\gamma[P_1 \times Q_2])$ and $\gamma[P_1 \times Q_2] = \gamma[Q_1 \times P_2]$ for a generic set $\{P,\ Q,\ R\}$ of points of G, and if, in addition, $\gamma[E_{G_1} \times E_{G_2}]$ is a point of $G' - F'$. By setting $P = E_G$ we obtain that $\gamma[E_{G_1} \times Q_2]$ is independent of Q if Q is generic. If γ, γ' are two factor sets of G into G', set $\Delta = (\gamma\{G_1 \times G_2\})(\gamma'\{G_1 \times G_2\})$, and $\delta = D_{\Delta,\, G_1 \times G_2}$; Lemma 1.1 implies then that δ is a factor set of G into G', which we shall call the *product of* γ *and* γ', and denote by $\gamma\gamma'$; in like manner the *inverse* γ^{-1} *of* γ is defined. It thus appears that the factor sets of G into G' form a group, isomorphic to a subgroup of $G'_{k(G_1 \times G_2)} - F'_{k(G_1 \times G_2)}$; such group will be denoted by $\Gamma(G, G')$. Let G_3 be another copy of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G; consider $k(G_3)$ as a subfield of $k(D) = k(G_1 \times G_2)$ as prescribed by D. Let μ be a rational mapping of G into G' such that $\mu[E_G]$ is a point not on F'; denote by μ_i $(i = 1, 2, 3)$ the modified extension over $k(D)$ of the copy of $\mu\{G\}$ which maps $k(G_i)$ into G'; set $\gamma' = \mu_1\mu_2\mu_3^{-1}$, and $\gamma = D_{\gamma', G_1 \times G_2}$. Then γ is clearly a factor set; all the factor sets of this type form a subgroup of $\Gamma(G, G')$, which we shall denote by $\Gamma_0(G, G')$. If $\gamma, \gamma' \in \Gamma(G, G')$, we shall say that they are *associate* (*to* each other) if $\gamma^{-1}\gamma' \in \Gamma_0(G, G')$.

Let A, G, G' be nonsingular commutative group-varieties over k, with degeneration loci B, F, F' respectively; we say that A is a *crossed product of* G *and* G' (in this order) if: (1) there exists a separable homomorphism α of A onto G, with a kernel V which is isomorphic to G' in an isomorphism β; (2) there exists a rational mapping λ of G into A, such that $\alpha[\lambda[P]] = P$ for a generic $P \in G$, and that $\lambda[E_G]$ is a point not on B. Let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G; consider $k(G_3)$ as a subfield of $k(D) = k(G_1 \times G_2)$ as prescribed by D, and let Λ_i be the modified extension over $k(D)$ of the copy of $\lambda\{G\}$ on $A_{k(G_i)}$; set $\Gamma = \Lambda_1\Lambda_2\Lambda_3^{-1}$, $\gamma_0 = D_{\Gamma, G_1 \times G_2}$. For a generic point $P_1 \times Q_2$ of $G_1 \times G_2$, we have $\alpha[\gamma_0[P_1 \times Q_2]] = \alpha[(\lambda[P])(\lambda[Q])(\lambda[PQ])^{-1}] = PQ(PQ)^{-1} = E_G$; therefore γ_0 operates on a subvariety of V. It is easily seen that γ_0 is a factor set of G into V, so that γ_0 corresponds, according to β, to a factor set γ of G into G'; we shall sometimes denote γ by γ_λ, in order to indicate its dependence on λ. There exists a rational mapping δ_0 of A onto V such that, for a generic $P \in A$, we have $\delta_0[P] = P(\lambda[\alpha[P]])^{-1}$; we shall denote by δ the corresponding rational mapping of A onto G' (that is, $\delta = \beta\delta_0$). Let $k(G)$ and $k(G')$ be considered as subfields of $k(A)$ as prescribed by α, δ respectively; for generic points P, P' of G, G' respectively, the point $Q = (\lambda[P])(\beta[P'])$ exists, and is such that $\alpha[Q] = P$, $\delta[Q] = P'$. Hence the smallest subfield of $k(A)$ which contains $k(G)$ and $k(G')$ is $k(G \times G')$; but the same relation also shows that $k(A) = k(G \times G')$, since $\mathrm{ins}\,(k(A) : k(G)) = 1$; therefore A is birationally equivalent to $G \times G'$. The birational mapping of $k(G \times G')$ onto A thus established is $\lambda^*\beta^*$, where λ^*, β^* are the modified extensions over $k(G \times G')$ of, respectively, $\lambda\{G\}$ and $\beta\{G'\}$; the (inverse) birational mapping of $k(A)$ onto $G \times G'$ is $\alpha\{A\} \times \delta\{A\}$.

Conversely, let the nonsingular commutative group-varieties G, G' over k, with degeneration loci F, F' respectively, and $\gamma \in \Gamma(G, G')$ be given, and define a law of composition L' on $G \times G'$ (not a direct product !), as a rational mapping of $G_1 \times G_1' \times G_2 \times G_2'$ onto $G_3 \times G_3'$ in the following manner: let D, D' be the laws on G, G' respectively, and let Δ, Δ' be the modified extensions, over $K = k(G_1 \times G_1' \times G_2 \times G_2')$, of $D\{G_1 \times G_2\}$, $D'\{G_1' \times G_2'\}$ respectively; let γ_3 be the copy of γ in $\Gamma(G, G_3')$, and let Γ be the modified extension of $\gamma_3\{G_1 \times G_2\}$ over K. Then L' is defined by setting $L'\{G_1 \times G_1' \times G_2 \times G_2'\} = \Delta \times \Delta'\Gamma$. It is readily seen that L' is a normal law on $G \times G'$, so that, by Theorem 3 of [4], $G \times G'$ is birationally equivalent, in a birational correspondence β', to a nonsingular commutative group-variety A, with a degeneration locus B, whose law of composition L is induced by L'; such group-variety, defined but for an isomorphism, will be denoted by $\{G, G', \gamma\}$. For any point P' of $G' - F'$, $L'[E_{G_1} \times P_1']$ has as a component the birational correspondence between $G_2 \times G_2'$ and $G_3 \times G_3'$ which gives, as a correspondent of a generic point $Q_2 \times Q_2'$ of $G_2 \times G_2'$, the point $Q_3 \times P_3'Q_3'\gamma_3[E_{G_1} \times Q_2]$; therefore $E_G \times P'$ is not fundamental for β'; moreover, $L'[E_{G_1} \times P_1'] \neq L'[E_{G_1} \times R_1']$ if $P' \neq R' \in G' - F'$; hence β' is biregular at each point of $E_G \times G'$, not on $E_G \times F'$, and induces a birational correspondence β^* between G' and an irreducible subvariety V of A; such correspondence is biregular outside F'. If P' $Q' \in G' - F'$, we have $(\beta'[E_G \times P'])(\beta'[E_G \times Q']) = \beta'[E_G \times P'Q'\gamma[E_{G_1} \times E_{G_2}]] \in V$. We shall accordingly denote by β the isomorphism between G' and V such that $\beta[P'] = \beta^*[P'(\gamma[E_{G_1} \times E_{G_2}])^{-1}]$ for $P' \in G' - F'$. Let α be the rational mapping of A onto G generated by the embeddiug of $k(G)$ into $k(A)$; then, for generic P, $Q \in A$, we have $\alpha[PQ] = (\alpha[P])(\alpha[Q])$; Lemma 2.3 implies then that α is a separable homomorphism of A onto G. For a generic point P of G, we have that $L'[P_1 \times E_{G_1'}]$ has as a component the birational correspondence between $G_2 \times G_2'$ and $G_3 \times G_3'$ which gives, as a correspondent of a generic point $Q_2 \times Q_2'$ of $G_2 \times G_2'$, the point $P_3Q_3 \times Q_3'\gamma_3[P_1 \times Q_2]$; hence $\beta'[P \times E_{G'}]$ is a point of $A - B$, and therefore $[\beta'; G \times E_{G'}, A]$ is a rational mapping λ of G into A, and we have, for a generic P of G: $\alpha[\lambda[P]] = \alpha[\beta'[P \times E_{G'}]] = P$; finally, $\lambda[E_G] \subseteq \beta'[E_G \times E_{G'}] = \beta^*[E_{G'}] = \beta[\gamma[E_{G_1} \times E_{G_2}]]$, and this is a point of V, not on B, so that the same is true of $\lambda[E_G]$. It thus appears that A is a crossed product of G and G', and that β, λ play the same role as in the definition of a crossed product. It is readily verified that $\gamma = \gamma_\lambda$.

We have thus seen that $\gamma \in \Gamma(G, G')$ determines, but for an isomorphism, a crossed product $A = \{G, G', \gamma\}$, and that any such crossed product, determined by means of G, G', α, and λ, determines a $\gamma_\lambda \in \Gamma(G, G')$. We have a mapping $\gamma \to \{G, G', \gamma\}$, and the natural question is: what is the necessary and sufficient condition in order that $\{G, G', \gamma'\} \cong \{G, G' \gamma\}$, for $\gamma' \in \Gamma(G, G')$? We may select $\{G, G', \gamma\} = \{G, G', \gamma'\} = A$, so that there are two rational mapping λ, λ' of G into A with the following properties: (1) $\alpha[\lambda[P]] = \alpha[\lambda'[P]] = P$ for a generic $P \in G$, (2) $\lambda[E_G]$ and $\lambda'[E_G]$ are points of $A - B$, and (3) $\gamma = \gamma_\lambda$, $\gamma' = \gamma_{\lambda'}$. Let μ be the rational mapping of G into G' such that

$\lambda'[P] = (\lambda[P])(\mu[P])$ for a generic $P \in G$; then it is easily verified that γ and γ' are associate to each other, and that μ has the role which the same symbol has in the definition of associate factor sets. The argument can be retraced, and shows that *there is a one-to-one correspondence between the set of the (classes of) crossed products of G and G', and the factor group $\Gamma(G, G')/\Gamma_0(G, G')$, the correspondence being given by* $\{G, G', \gamma\} \rightarrow \gamma$. This, of course, establishes a group structure in the set of the classes of crossed products of G and G', but we shall not enter into details on this topic, as it is not needed for the purpose of this paper.

LEMMA 3.2. - *Let G be a nonsingular commutative group-variety over k, and let V be a rational irreducible 1-dimensional group-subvariety of G; then G is a crossed product of G/V and V.*

PROOF. - Set $A = G/V$; let G_1, G_2, G_3 be copies of G, and let D be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Let V_i be the copy of V which is a subvariety of G_i; if α is the natural homomorphism of G onto A, consider $k(A_1)$ to be a subfield of $k(G_1)$ as prescribed by the copy α_1 of α. Since V_2 is a simple subvariety of G_2, there exists a valuation w_2 of $k(G_2)$, whose center on G_2 is V_2, and such that $K_{w_2} = k(V_2)$; set $\Delta = D\{G_2\}$. Then $\Delta\{w_2\}^*$ has a component variety T which operates on the whole G_1 and the whole G_3, and appears in $\Delta\{w_2\}^*$ with multiplicity 1; moreover, $T' = D_{T, V_2}$ has the following property: if P, Q are generic points of, respectively, G and V, then $T'\{P_1 \times Q_2\}^*$ is a point of $(\sigma_P V)_3$. Let u be a degenerate place of V, and let v be the degenerate place of G compounded with w and u; then $\Delta\{v_2\}^*$ has a unique component variety S which operates on the whole G_1, and S appears in $\Delta\{v_2\}^*$ with multiplicity 1 (Theorem 1 of [4]). As a consequence, S is a component variety of $T\{u_2\}^*$, and appears in $T\{u_2\}^*$ with multiplicity 1; moreover, for a generic point P of G, $S\{P_1\}^*$ is a point of $(\sigma_P V)_3$, necessarily on the degeneration locus of F_3 of G_3, by Theorem 1 of [4]. Since $\sigma_P V$ is not a subvariety of F, it follows that $S\{P_1\}^* = S\{(PQ)_1\}^*$ if Q is a generic point of V. Set $S' = S\{G_1\}$, $W = G_{S'}$, $H = k(W)$, so that $H \subseteq k(G_1)$; the last result proves that $S\{P_1\}^*$ depends only on $\alpha_1 P_1$ when this is generic, and that therefore the smallest subfield of $k(G_1)$ containing H and $k(A_1)$ is a purely inseparable extension of $k(A_1)$. Since α_1 is separable, it follows that $H \subseteq k(A_1)$, and that consequently S' is the modified extension over $k(G_1)$ of a rational point S'' of $(G_3)_{k(A_1)}$. If now α is considered as operating between A_1 and G_3, we have also seen that for a generic $P \in A_1$, and for any place z of A_1 whose center on A_1 is P, $S''[z]$ belongs to $\alpha^{-1}P$, so that S'' is a rational point of $\alpha\{A_1\}$. It is thus proved that $\alpha\{A_1\}$ contains a rational point.

Now, the proof of Theorem 2.1 shows that the modified extension of $\alpha\{A_1\}$ over $k(G_1)$ is birationally equivalent to the modified extension of V_3 over $k(G_1)$, and is therefore a rational curve, hence a curve of genus zero.

Since the genus remains the same under the separable extension $k(A_1) \to k(G_1)$, we conclude that $\alpha\{A_1\}$ is also a curve of genus zero; as it contains a rational point, it follows that $\alpha\{A_1\}$ is a rational curve. We shall now identify A_1 with A, G_3 with G, so that $\alpha\{A\}$ is a rational curve; it is therefore possible to select a rational point λ' of $\alpha\{A\}$, not on $F_{k(A)}$, and such that, after setting $\lambda = D_{\lambda', A}$, $\lambda[E_A]$ is a point not on F. Then λ is a rational mapping of A into G, such that $\lambda[E_A]$ is a point not on F, and that $\alpha[\lambda[P]] = P$ for a generic $P \in A$; the existence of λ with these properties proves that G is a crossed product of A and V, Q. E. D..

LEMMA 3.3. - *Let $G^1, \dots, G^m$, $A^1, \dots, A^n$ be commutative group-varieties over k, and set $G = G^1 \times \dots \times G^m$, $A = A^1 \times \dots \times A^n$; then $\Gamma(G, A)/\Gamma_0(G, A)$ is isomorphic to the direct product of all the $\Gamma(G^i/A^j)/\Gamma_0(G^i, A^j)$.*

PROOF. - If $\gamma \in \Gamma(G, A)$, then $\gamma\{G_1 \times G_2\} = \gamma_1' \times \dots \times \gamma_n'$, where γ_i' is a rational point of $(A^i)_{k(G_1 \times G_2)}$; quite clearly, $\gamma_i = D_{\gamma_i', G_1 \times G_2}$ belongs to $\Gamma(G, A^i)$, and the mapping $\gamma \to \gamma_i$ is a homomorphism of $\Gamma(G, A)$ onto $\Gamma(G, A^i)$; moreover, the set $\{\gamma_1, \dots, \gamma_n\}$ determines γ, so that such homomorphism induces an isomorphism between $\Gamma(G, A)$ and the direct product of the $\Gamma(G, A^i)$; finally, $\gamma \in \Gamma_0(G, A)$ if and only if $\gamma_i \in \Gamma_0(G, A^i)$ for each i. Therefore it is sufficient to prove that, for any i, $\Gamma(G, A^i)/\Gamma_0(G, A^i)$ is isomorphic to the direct product of the $\Gamma(G^j, A^i)/\Gamma_0(G^j, A^i)$; we shall denote A^i simply by A. If $\gamma \in \Gamma(G, A)$, set $\gamma_j = [\gamma;\ G_1^j \times G_2^j,\ A]$; this belongs to $\Gamma(G^j, A)$ since $\gamma[E_{G_1} \times E_{G_2}]$ is a point not on the degeneration locus of A. The mapping $\gamma \to \gamma_j$ is a homomorphism β_j; now, given a quite arbitrary γ_i in each $\Gamma(G^i, A)$, set $\gamma_i' = \gamma_i \times$ (the direct product of all $G_1^j \times G_2^j$ for $j \neq i$), so that $\gamma_i' \in \Gamma(G, A)$, and set $\gamma = \gamma_1'\gamma_2' \dots \gamma'_m$; then $\gamma \in \Gamma(G, A)$, and $\beta_i\gamma = \gamma_i$; this proves that the mapping $\gamma \to \beta\gamma = \{\beta_1\gamma, \dots, \beta_m\gamma\}$ is a homomorphism of $\Gamma(G, A)$ onto the direct product of the $\Gamma(G^i, A)$; if $\gamma \in \Gamma_0(G, A)$, then $\beta\gamma$ belongs to the direct product of the $\Gamma_0(G^i, A)$; viceversa, if $\gamma_i \in \Gamma_0(G^i, A)$ for each i, then $\gamma_1' \dots \gamma'_m \in \Gamma_0(G, A)$. The lemma will thus be proved if we show that the kernel of β is a subgroup of $\Gamma_0(G, A)$. The proof of this fact will be achieved by induction on the number m.

The assertion is true for $m = 1$; set $G' = G^2 \times \dots \times G^m$; if the assertion is true for $m = 2$, then $\Gamma(G, A)/\Gamma_0(G, A) = (\Gamma(G', A)/\Gamma_0(G', A)) \times (\Gamma(G^1, A)/\Gamma_0(G^1, A))$; but, for our induction assumption, the first factor of this direct product is isomorphic to the direct product of the $\Gamma(G^i, A)/\Gamma_0(G^i, A)$, for $i = 2, \dots, m$, and this proves the result for the given value of m. We have thus seen that it is sufficient to give the proof for the case $m = 2$. In this case, let $\gamma \in \Gamma(G, A)$ be such that $\beta_1\gamma = \gamma_1$ and $\beta_2\gamma = \gamma_2$ coincide with the identities $E_A \times G_1^1 \times G_2^1$, $E_A \times G_1^2 \times G_2^2$ respectively. Let μ be the rational mapping of $G^1 \times G^2$ into A such that, for a generic pair of points P, Q of G^1, G^2 respectively, we have $\mu[P \times Q] = \gamma[(P_1 \times E_{G_1^2}) \times (E_{G_2^1} \times Q_2)]$; then $\mu[E_{G^1} \times E_{G^2}]$ is a point of A, but not of its degeneration locus. From the definition of factor set we have, for a generic set of points $P, Q \in G^1$, $R, S \in G^2$: $(\gamma[P_1 \times S_1) \times (Q_2 \times R_2)])(\mu[Q \times R]) = (\gamma[(P_1 \times S_1 R_1) \times (Q_2 \times E_{G^2_2})]) \times (\gamma[(P_1 \times S_1) \times \times (E_{G^1_2} \times R_2)])$; on the other hand, from the same definition we also have $(\gamma[(P_1 \times S_1 R_1) \times (Q_2 \times E_{G^2_2})])(\mu[P \times SR]) = (\mu[PQ \times SR])(\gamma_1[P_1 \times Q_2])$; the last factor is E_A by assumption, so that this reduces to $\gamma[(P_1 \times S_1 R_1) \times (Q_2 \times E_{G^2_2})] = (\mu[(P \times S)(Q \times R)])(\mu[P \times SR])^{-1}$. In like manner we have $(\gamma[(P_1 \times S_1) \times (E_{G^1_2} \times R_2)])(\mu[P \times S]) = (\mu[P \times SR])(\gamma_2[S_1 \times R_2])$, or $\gamma[(P_1 \times S_1) \times (E_{G^1_2} \times R_2)] = (\mu[P \times SR])(\mu[P \times S])^{-1}$; hence $\gamma[(P_1 \times S_1) \times (Q_2 \times R_2)] = (\mu[(P \times S)(Q \times R)])(\mu[P \times S])^{-1}(\mu[Q \times R])^{-1}$, which proves that $\gamma \in \Gamma_0(G, A)$, Q. E. D..

LEMMA 3.4. - *Let G be a nonsingular commutative group-variety over k which is not abelian; then G hav some positive dimensional irreducible rational group-subvariety.*

PROOF. - If $\dim G = 1$, this is a consequence of Proposition 14 of [16]; we shall prove the lemma by induction on $\dim G$; assume the lemma to be true if $\dim G < n$, and let us consider the case in which $\dim G = n$. Since G is not abelian, by Lemma 3.1 it contains a proper positive dimensional irreducible group-subvariety A. Should the lemma be false for G, A would not contain any positive dimensional irreducible rational group-subvariety, and therefore A would be abelian, since $\dim A < n$. Theorem 3.1 then implies the existence of an irreducible proper group-subvariety B of G, of positive dimension, such that $G = (A, B)$; B would also be abelian, and consequently G would be abelian, a contradiction, Q. E. D..

LEMMA 3.5. - *Let G be a nonsingular commutative group-variety over k; (a) if V is an irreducible rational group-subvariety of G, then G is a crossed product of G/V and V; (b) G contains an irreducible rational group-subvariety B containing all the irreducible rational group-subvarieties of G; moreover, G/B is abelian.*

The group-subvariety B will be called the *maximal rational group-subvariety of G*.

PROOF. - We shall denote by S_n (for any nonnegative integer n) the following statement: *statement (a) of the lemma is true, for any G, when* $\dim V \leq n$. We shall denote by S_n' the following statement: *G being as in the statement of the lemma, let B be an irreducible rational group-subvariety of G which is not properly contained in any irreducible rational group-subvariety of G; if $\dim B \leq n$, then G/B is abelian.* We shall prove that S_n implies S_n', and that S_n' and S_n (for $n \geq 1$) imply S_{n+1}. Since S_0 and S_0' are trivially true, and S_1 is true by Lemma 3.2, this will prove S_n and S_n' for each n, and will therefore prove assertion (a) of the lemma, and also the last statement of assertion (b), under the condition that B be as specified in S_n'. But then, if B' is an irreducible rational group-subvariety of G, and α is the natural homomorphism of G onto the abelian variety $A = G/B$, $\alpha B'$ is a point by the Corollary to Theorem 8 of [16]; since $E_G \in B'$, we must have $\alpha B' = E_A$, or $B' \subseteq B$, which completes the proof of (b).

We shall now prove that S_n implies S_n' for $n \geq 1$. Let B be as stated in S_n', and assume $\dim B \leq n$; set $A = G/B$, and let C be a positive dimensional irreducible rational group-subvariety of A, if any exists; let α be the natural homomorphism of G onto A. Set $C^* = \alpha^{-1}C$; then $C = C^*/B$, so that, by S_n, C^* is a crossed product of C and B; as a consequence, C^* is birationally equivalent to $C \times B$, and is therefore rational. Since $B \subset C^*$, this is a contradiction, and we conclude that A has no positive dimensional irreducible rational group-subvariety, and is therefore abelian by Lemma 3.4. Thus S_n' is true. We shall now prove that S_n' and S_n imply S_{n+1}, for $n \geq 1$. Let G, V be as in S_{n+1}, and assume $\dim V = n + 1$. V contains no positive dimensional abelian group-subvariety, as this, by Theorem 3.1, would contradict the Corollary to Theorem 8 of [16]; hence Lemma 3.1, applied to V and to its proper irreducible group-subvarieties, implies that V contains a 1-dimensional irreducible rational group-subvariety W. Set $G' = G/W$, and let α be the natural homomorphism of G onto G'; set also $V' = \alpha V = V/W$. Let B be an irreducible rational group-subvariety of V' which is not properly contained in any irreducible rational group-subvariety of V'; since $B \leq \dim V' = n$, we have that V'/B is abelian by S_n'. If β is the natural homomorphism of V' onto V'/B, then $\beta\alpha$ induces a homomorphism of V onto V'/B. The Corollary to Theorem 8 of [16] implies that $\dim V'/B = 0$, and this proves that $V' = B$ is rational. If $A = G'/V' = G/V$, S_n implies that G' is a crossed product of A and V'. We shall denote by α' the natural homomorphism of G' onto A, and by λ' the rational mapping of A into G' which appears in the definition of crossed products; the choice of λ' is not unique, and we shall select it in such a manner that $\lambda'[E_A] = E_{G'}$. On the other hand, G is a crossed product of G' and W by Lemma 3.2, so that there exists a rational mapping λ of G' into G such that $\alpha[\lambda[P]] = P$ for a generic $P \in G'$. But then $\lambda\lambda'$ is a rational mapping of A into G, such that $\alpha'\alpha[\lambda\lambda'[P]] = P$ for a generic $P \in A$, and that $\lambda\lambda'[E_A] = \lambda[E_{G'}]$ is a point of G, but not of its degeneration locus. This proves that G is a crossed product of A and V, so that S_{n+1} is true, Q. E. D..

Lemma 3.5 can now be stated in the following form:

THEOREM 3.2. - *Let G be a nonsingular commutative group-variety over k, and let B be the maximal rational group-subvariety of G; set $A = G/B$. Then A is abelian, and G is a crossed product of A and B. Conversely, given an abelian variety A and a rational commutative group-variety B, both over k and both nonsingular, any crossed product of A and B has a maximal rational group-subvariety isomorphic to B.*

We shall now devote our attention to the structure of rational commutative group-varieties. If G is any nonsingular commutative group-variety over k, there exists an irreducible vector group-subvariety V of G which is not properly contained in any irreducible vector group-subvariety of G: any such V we shall call *a maximal vector subvariety of* G; we shall see later that V is unique, but for the moment we do not need this result.

A group-variety G over k, with degeneration locus F, is said to be *periodic* if there exists a positive integer e such that $P^e = E_G$ for any $P \in G - F$; the smallest such e is called the *period of* G. Let G be periodic, positive dimensional, and commutative; then, by Theorem 3.2, and by Proposition 24 of [16], G is rational; as a consequence, and by Lemma 3.1, G has proper irreducible group-subvarieties of positive dimension, and any of these is periodic; the argument can be iterated, and shows that G has some irreducible 1-dimensional periodic group-subvariety. This is possible only if the characteristic p of k is $\neq 0$, in which case any such subvariety is a vector variety; this fact shows that any maximal vector subvariety V of G is positive dimensional. By induction, from G/V to G, we obtain that the period of G is a power of p, with positive integral exponent. This being established, we can prove the following result:

LEMMA 3.6. - *Let G be a commutative nonsingular positive dimensional periodic group-variety over the (algebraically closed) field k of characteristic p; then $p \neq 0$, the period of G is p^e for some positive integer e, and G is rational. Let G_i be the smallest subvariety of G containing all the points P of G, but not of its degeneration locus F, such that $P^{p^i} = E_G$ $(i = 1, 2, \ldots, e)$; then G_i is a periodic group-variety of period p^i, and G_i/G_{i-1}, G_1 $(i = 2, \ldots, e)$ are positive dimensional vector varieties.*

PROOF. - The first three statements have already been proved. G_i has period $p^{i'}$, with $i' \leq i$, and G_i/G_{i-1} $(i = 2, \ldots, e)$ is either zero-dimensional, or is positive dimensional and has period p, the first possibility occurring when and only when $i' < i$. The variety G_1 is positive dimensional, since it contains any maximal vector subvariety of G, and has therefore period p. Let j be the largest value of i such that $i' < i$; then $j < e$, and for any P of G_{j+1}, but not of F, we have $P^p \in G_j$, hence $P^{p^{j'+1}} = E_G$, so that the period of G_{j+1} is $\leq j' + 1 < j + 1$, a contradiction; hence $i' = i$ for each i. The lemma will therefore be completely proved if we prove that any commutative group-variety over k, of period p, is a vector variety. Where it not so, there would exist a group-variety G over k of period p, and such that, if V is a maximal vector subvariety of G, G/V is a vector variety of dimension $< \dim G$ and > 0. Lemma 3.3, applied to the $\gamma \in \Gamma(G/V, V)$ such that $G \cong \{G/V, V, \gamma\}$, implies the existence of a variety G having the described properties, and such that, in addition, $\dim V = \dim G/V = 1$. We shall now disprove the existence of such a variety. Set $A = G/V$, and let $G \cong \{A, V, \gamma\}$; let x, y be n. h. g. p. of V, A respectively such that the laws of composition on V, A are given, respectively, by $x_3 = x_1 + x_2$, $y_3 = y_1 + y_2$. We shall identify A with A_1, and consider a copy z of y in $k(A_2)$. The rational mapping γ of $A_1 \times A_2$ into V operates on the whole V, since by assumption $\gamma \notin \Gamma_0(A, V)$;

hence γ prescribes an embedding of $k(x)$ into $k(y, z)$, which we shall express by writing $x = x(y, z)$ in the functional notation. The fact that γ is a factor set implies that $x(0, 0)$ exists (i. e. that $x \in \mathbf{P}(E_{G_1 \times G_2}/G_1 \times G_2)$, and coincides with $x(y, 0)$ and $x(0, y)$, and that, for an indeterminate t, $x(y, z+t) + x(z, t) = x(y+z, t) + x(y, z)$; moreover, $x(y, z) = x(z, y)$. Upon derivating the preceding formula with respect to t, and setting $t = 0$, one finds that the equality $\dfrac{\partial x(y, z)}{\partial z} = \left[\dfrac{\partial x(y+z, t)}{\partial t}\right]_{t=0} - \left[\dfrac{\partial x(z, t)}{\partial t}\right]_{t=0}$ is meaningful and true; hence, if $\varphi(z) = [\partial x(z, t)/\partial t]_{t=0}$, we have $\partial x(y, z)/\partial z = \varphi(y+z) - \varphi(z)$. Now, $\varphi(z)$ can be decomposed in partial fractions, in the form $\varphi(z) = \Sigma_{i=0}^{l} a_i z^i +$ (sum of fractions with numerator in k, and denominator of the form $(z-a)^h$, $a \in k$, h a positive integer), where $a_i \in k$. If $b/(z-a)^h$ is one of the fractions, then $\varphi(y+z) - \varphi(z)$ contains $(b/(z+y-a)^h) - (b/(z-a)^h)$; this shows, first of all, that $a \neq 0$; since $x(y, z)$ can also be decomposed in partial fractions as an element of $K(z)$, K being the algebraic closure of $k(y)$, it follows that $h \not\equiv 1 \pmod p$; as a consequence, $x' = x(y, z) + b(h-1)^{-1}[(y+z-a)^{1-h} - (z-a)^{1-h} - (y-a)^{1-h}]$ defines a factor set associate to γ, and has the property that the φ obtained from x' equals the φ obtained from x, except for the fact that the former does not contain $b(z-a)^{-h}$. Since this can be repeated for each fraction, we conclude that, by replacing γ with an associate factor set, we may assume $\varphi(z) = \Sigma_{i=0}^{l} a_i z^i$. In this expression, consider a term $a_i z^i$ with $i \not\equiv -1 \pmod p$; the polynomial $\varphi(y+z) - \varphi(z)$ contains $a_i(y+z)^i - a_i z^i$; hence $x' = x(y, z) - a_i(i+1)^{-1}[(y+z)^{i+1} - y^{i+1} - z^{i+1}]$ defines a factor set associate to γ, and such that the corresponding φ equals the φ obtained from x, except for the fact that, in the former, the coefficient of z^i vanishes. We conclude that, after replacing γ with an associate factor set, we may assume φ to have the form $\varphi(z) = \Sigma_{j=1}^{r} c_j z^{jp-1}$. The coefficient of z^{jp-1} in $\varphi(y+z) - \varphi(z)$ is then $\Sigma_{i=j+1}^{r} c_i \binom{ip-1}{jp-1} y^{(i-j)p}$, and this must be zero in the expression of $\partial x(y, z)/\partial z$; hence $c_i = 0$ for $i = 2, 3, \ldots, r$, and $\varphi(z) = cz^{p-1}$, where $c = c_1$. But then, since $x(y, z)$ is symmetrical in y, z, it follows that $x(y, z) = cf(y, z) + x'(y', z')$, where $x' \in k(y', z')$, $y' = y^p$, $z' = z^p$, and $f(y, z) = \Sigma_{i=1}^{p-1} (-)^i i^{-1} y^i z^{p-i}$. Now, $f(y, z)$ defines a factor set of A into V, so that $x'(y', z')$ must have the same property; the same analysis can thus be repeated on $x'(y', z')$, and so on finitely many times; the final result will be the existence of a set of elements $c_0, c_1, \ldots, c_s$ of k, such that the factor set determined by $x(y, z) = \Sigma_{i=0}^{s} c_i (f(y, z))^{p^i}$ is associate to the given γ. As $\gamma \notin \Gamma_0(A, V)$, we also have $c_i \neq 0$ for at least one value of i. A direct computation now shows that if the correspondent on $V \times A$ of a point P of G has the co-ordinates $x = \xi$, $y = \eta$, then the point P^p corresponds on $V \times A$, to the point having the co-ordinates $x = \Sigma_{i=0}^{s} c_i \eta^{p^{i+1}}$, $y = 0$; hence $P^p \neq E_G$ for a generic P; this is the contradiction, Q. E. D..

The preceding proof, and Lemma 3.3, furnish the explicit construction of all the commutative periodic varieties of period p^2; explicit constructions of periodic commutative varieties of period p^e, with $e > 2$, are more complicated, and we shall not give them here.

In the notation of Lemma 3.6, we see that any maximal vector subvariety of G is contained in G_1, and that G_1 is itself a vector subvariety of G; hence G_1 is the only maximal vector subvariety of G.

LEMMA 3.7. - *Let G be a positive dimensional nonsingular commutative group-variety over k, with degeneration locus F; let V, L be irreducible group-subvarieties of G, such that $G = (V, L)$, and that $V \cap L$ has, outside F, the only component E_G; assume V to be either a vector variety or a periodic variety, and L to be a 1-dimensional logarithmic variety. Then $G \cong V \times L$.*

PROOF. - Let V', L' be copies of V, L respectively, and set $G' = V' \times L'$ (direct product); let F' be the degeneration locus of G'. Let ν, λ be the identical isomorphisms between V', L' and, respectively, V, L; let ν', λ' be the modified extensions over $k(G')$ of, respectively, $\nu\{V'\}$, $\lambda\{L'\}$. Then ν', λ' are rational points of, respectively, $V_{k(G')}$, $L_{k(G')}$; hence they are rational simple points of $G_{k(G')}$, and their product $\alpha' = \nu'\lambda'$ exists and is a rational point of $G_{k(G')}$, by Corollary 3 to Theorem 1 of [4]. Set $\alpha = D_{\alpha', G'}$, so that α is a homomorphism of G' onto G. The co-ordinates of ν', λ', α' are elements of $k(G')$, which generate, over k, subfields of $k(G')$ isomorphic to, respectively, $k(V)$, $k(L)$, $k(G)$; we shall identify such fields with $k(V)$, $k(L)$, $k(G)$ respectively. Moreover, $k(V) = k(V')$, $k(L) = k(L')$. The co-ordinates of any of the points ν', λ', α' are elements of the field over k generated by the co-ordinates of the other two points; this shows, in particular, that if $k(L') = k(y)$ (where $y \in k(L')$), then $k(V') \subseteq k(G)(y)$, so that $k(G)(y) = k(G')$. Since the kernel of α is $E_{G'}$, we have that $k(G')$ is purely inseparable over $k(G)$; this is sufficient to prove the contention if the characteristic of k is 0. We shall assume k to have characteristic $p \neq 0$, but shall treat first the case in which V is a vector variety. Let $\{x_1, \ldots, x_r\}$ be a n. h. g. p. of V such that the law of composition on V is given by $(x_i)_3 = (x_i)_1 + (x_i)_2$; as for y, we shall select it in such a way that the law of composition on L' be given by $y_3 = y_1 y_2$. Let e be the smallest power of p such that $y^e \in k(G)$; if $e = 1$, we have $k(G) = k(G')$ as claimed; we shall accordingly assume $e > 1$. Then, for each i, there are elements $a_{ij} \in k(G)$ $(j = 0, \ldots, e-1)$, uniquely determined, such that $x_i = \Sigma_{j=0}^{e-1} a_{ij} y^j$ $(i = 1, \ldots, r)$. Since $a_{ij} \in k(G')$, we shall express it as a rational function of $x_1, \ldots, x_r, y : a_{ij} = a_{ij}(x, y)$. If P is a point of $G' - F'$ we have $\sigma_P^{-1} x_i = x_i + \xi_i$, $\sigma_P^{-1} y = \eta y$, where ξ_i, $\eta \in k$ are the co-ordinates of P; hence $x_i + \xi_i = \Sigma_j a_{ij}(x + \xi, \eta y)\eta^j y^j$, or $\xi_i + \Sigma_j a_{ij}(x, y) y^j = \Sigma_j a_{ij}(x + \xi, \eta y)\eta^j y^j$; therefore, by Lemma 2.2, $\xi_i + a_{i0}(x, y) = a_{i0}(x + \xi, \eta y)$. These relations being true for arbitrary values $\xi_1, \ldots, \xi_r$, and for any $\eta \neq 0$, they remain true if ξ, η are considered as indeterminates. We can then denote ξ_i, η by x_i, y

respectively, and replace x_i, y by values ξ_i, η in k at which the denominators of the a_{i0} do not vanish. We thus obtain $a_{i0}(\xi, \eta) + x_i = a_{i0}(x + \xi, \eta y)$. This relation implies that $x_i \in k(G)$; but y is contained in $k(G)(x)$, hence $y \in k(G)$, $e = 1$, $G \cong G'$.

We shall now prove the lemma for the case in which V is periodic, by means of an induction on the period e of V; $e = p$, the contention is true; assume it to be true when the period of V is e/p, and consider the case in which such period is e. Let V^* be the maximal vector subvariety of V, and set $G' = G/V^*$; let α be the natural homomorphism of G onto G', and set $V' = \alpha V$, $L' = \alpha L$. Then $G' = (V', L')$, and $E_{G'}$ is the only component of $V' \cap L'$ outside the degeneration locus F' of G'; moreover, the period of V' is $e/1$ by Lemma 3.6, so that $G' \cong V' \times L'$ by our recurrence assumption. Now, by Lemma 3.5, $G \cong \{ G', V^*, \gamma \}$, where $\gamma \in \Gamma(G, V^*)$; by Lemma 3.3 and its proof, γ is associate to a factor set of the type $(\gamma_0 \times L_1' \times L_2')(\gamma_1 \times V_1' \times V_2')$, where $\gamma_0 \in \Gamma(V', V^*)$, $\gamma_1 \in \Gamma(L', V^*)$. Set $A = \{ L', V^*, \gamma_1 \}$, and consider the endomorphism β of A such that $\beta[P] = P^p$ for any P of A, but not of its degeneration locus F_A. Let δ be the natural homomorphism of A onto L', and let L^* be the group-subvariety of A on which β operates. If $P \in V^* \cap L^*$, but $P \notin F_A$, then $P = Q^p$ for some $Q \in A - F_A$, and $\delta Q^p = E_{L'}$, or $(\delta Q)^p = E_{L'}$, $\delta Q = E_{L'}$, $Q \in V^*$, $P = E_A$. It follows that $V^* \cap L^*$ has, outside F_A, the only component E_A. Since the kernel of β is V^*, we have $\dim L^* = 1$, $A = (L^*, V^*)$; also, $\delta L^* = L'$, so that L^* is a logarithmic variety. Hence the first part of this proof applies, and yields $A \cong V^* \times L^* \cong V^* \times L'$, so that $\gamma_1 \in \Gamma_0(L', V^*)$. But then γ is associate to $\gamma_0 \times L_1' \times L_2'$, and $G \cong \{ V', V^*, \gamma_0 \} \times L' \cong$ $\cong \{ V', V^*, \gamma_0 \} \times L$. If G is identified with $\{ V', V^*, \gamma_0 \} \times L$, then $\{ V', V^*, \gamma_0 \}$ and V have in common the property of being the smallest subvariety of G which contains all the $P \in G - F$ of period e; hence $V = \{ V', V^*, \gamma_0 \}$, and $G \cong V \times L$, Q. E. D..

Lemma 3.8. - *Let G be a nonsingular commutative group-variety over the (algebraically closed) field k of characteristic p; let V be an irreducible group-subvariety of G, and set $A = G/V$; assume that each one of the two varieties V, A is either a vector variety, or a logarithmic variety, or a periodic variety; then:*

(1) *if V and A are both periodic varieties, so is G;*

(2) *in all other cases, $G \cong V \times A$ (direct product).*

Proof. - Assertion (1) is self-evident. In order to prove assertion (2), we shall consider first the particular cases in which either V, or A (but not both) is a periodic variety, in which case $p \neq 0$, and the other variety is a logarithmic variety. If V is periodic of period e, and A is logarithmic, by Lemmas 3.6, 3.5, $G = \{ A, V, \gamma \}$ for some $\gamma \in \Gamma(A, V)$; we are requested to prove that $\gamma \in \Gamma_0(A, V)$; by Lemma 3.3, this is true for any value of $\dim A$ if it is true when $\dim A = 1$. Accordingly, assume $\dim A = 1$, and consider the endomorphism β of G such that $\beta P = P^e$ for any point P of G, but not of its degeneration locus F; the same argument used in the last part of the proof of Lemma 3.7 proves that G contains a 1-dimensional logarithmic group-subvariety A' such that $G = (V, A')$, and that $V \cap A'$ has, outside F, the only component E_G. Then Lemma 3.7 applies, and yields $G \cong V \times A' \cong V \times A$, as desired. We shall now consider the case in which V is logarithmic and A is periodic of period e. Also in this case we may assume $\dim V = 1$. If β has the same meaning as before, let A' be the component of the identity in the kernel of β; since $\beta G = V$, and since no element of V has period e, we now have that the only component of $V \cap A'$ outside F is E_G; the same argument previously used proves that $G \cong V \times A'$; hence $A' \cong G/V = A$, so that, again, $G \cong V \times A$.

There remains to be proved the main part of case (2), i. e. the case in which either $p \neq 0$, and V, A are logarithmic varieties, or $p = 0$, and each one of the varieties V, A is a vector or a logarithmic variety. Lemma 3.5 implies, in each case, that $G \cong \{A, V, \gamma\}$ for some $\gamma \in \Gamma(A, V)$; our aim is thus to prove that $\gamma \in \Gamma_0(A, V)$; by Lemma 3.3, this is true if it is true in the particular case in which $\dim V = \dim A = 1$; we shall accordingly limit our discussion to this case. Let x be a n. h. g. p. of V such that the law of composition on V is given by $x_3 = x_1 + x_2$, or $x_3 = x_1 x_2$, depending on whether V is a vector or a logarithmic variety; let y have a similar role for A; we shall identify A with A_1, and shall consider a copy z of y in $k(A_2)$. Then γ prescribes an embedding of $k(x)$ into $k(y, z)$ (unless γ operates on a point of V, in which case there is nothing to be proved), so that we can write $x = x(y, z) \in k(y, z)$. Since γ is a factor set, we have, for an indeterminate t, one of the following four relations:

(2) $x(y, z+t) + x(z, t) = x(y+z, t) + x(y, z)$, if V, A are vector varieties,

(3) $x(y, z+t)x(z, t) = x(y+z, t)x(y, z)$, if V is a logarithmic variety, A a vector variety,

(4) $x(y, zt) + x(z, t) = x(yz, t) + x(y, z)$, if V is a vector variety, A a logarithmic variety,

(5) $x(y, zt)x(z, t) = x(yz, t)x(y, z)$ if V, A are logarithmic varieties.

By derivating (2) with respect to t, and then setting $t = 0$, we obtain

(6) $\partial x(y, z)/\partial z = \varphi(y+z) - \varphi(z)$, where $\varphi(z) \in k(z)$;

operating in like manner on (3), (4), (5) (but setting $t = 1$ in cases (4) and (5)), we obtain respectively:

(7) $(x(y, z))^{-1}\partial x(y, z)/\partial z = \varphi(y+z) - \varphi(z)$,

(8) $z\partial x(y, z)/\partial z = \varphi(yz) - \varphi(z)$,

(9) $z(x(y, z))^{-1}\partial x(y, z)/\partial z = \varphi(yz) - \varphi(z)$.

Case (5) and (9) is the only possible case if $p \neq 0$, and we shall discuss it in detail. Decompose $\varphi(z)$ in partial fractions, in the form $\varphi(z) = P(z) + \Sigma_i A_i(z - a_i)^{-1} +$ (sum of fractions whose denominator is either nonlinear, or $= z$), where $P(z) \in k[z]$, A_i, $a_i \in k$, $a_i \neq 0$. Then $z^{-1}(\varphi(yz) - \varphi(z)) = (P(yz) - P(z))z^{-1} + \Sigma_i A_i a_i^{-1}(z - a_i y^{-1})^{-1} - \Sigma_i A_i a_i^{-1}(z - a_i)^{-1} +$ (sum of fractions whose denominator is nonlinear). On the other hand, if K denotes the algebraic closure of $k(y)$, we have that $(x(y, z))^{-1}\partial x(y, z)/\partial z$ is a sum of fractions with numerators in the prime field of k, and denominators in $K[z]$, linear and monic in z; as a consequence, $a_i \neq 1$ for each i, and $z^{-1}(\varphi(yz) - \varphi(z))$ reduces to the expression $\Sigma_i A_i a_i^{-1}(z - a_i y^{-1})^{-1} - \Sigma_i A_i a_i^{-1}(z - a_i)^{-1}$, so that each $A_i a_i^{-1} = e_i'$ belongs to the prime field of k. If k has characteristic 0, set $e_i = e_i'$; if k has characteristic $p \neq 0$, denote by e_i a rational integer (to be determined more precisely later on) which represents e_i' (mod p). Then $x'(y, z) = x(y, z)\,\Pi_i\,(yz - a_i)^{-e_i}(y - a_i)^{e_i}(z - a_i)^{e_i}$ defines a factor set associate to γ, and has the property that the corresponding $\varphi(z)$ vanishes. Since $x'(y, z)$ is symmetrical in y, z, we conclude that $x'(y, z) \in k(y', z')$, where $y' = y^p$, $z' = z^p$ (or that $x'(y, z) \in k$ if k has characteristic 0). If $p = 0$, this means that $\gamma \in \Gamma_0(A, V)$, as claimed. Otherwise, we have shown that when x is expressed as a product of powers of linear monic polynomials in $K[z]$, times a factor in K, the product of those powers which appear with an exponent not divisible by p differs from an element of $K(z')$ by the factor $\Pi_i\,(yz - a_i)^{-e_i}(y - a_i)^{e_i}(z - a_i)^{e_i}$. Therefore it is possible to select the rational integers e_i in such a manner that $x'(y, z)$ does not contain any of the factors $yz - a_i$. If $x'(y, z) \notin k$, the process can be repeated, and so on; after a finite number of times, one obtains an $x^{(n)}(y, z)$ which determines a factor set, and which is the product of an element of $k(y)$ and an element of $k(z)$. Such $x^{(n)}$ necessarily belongs to k, a fact which proves that $\gamma \in \Gamma_0(A, V)$ also if $p \neq 0$.

Similar reductions can be carried on in each of the cases (2), (3), (4), with the advantage that $p = 0$ in each of these cases; we shall not give the elementary details here, and will only add that in each case one takes advantage of the fact that $\partial x(y, z)/\partial z$, when decomposed in partial fractions as an element of $K(z)$, contains no fraction whose denominator is linear, while $(x(y, z))^{-1}\partial x(y, z)/\partial z$ contains only fractions whose denominator is linear. This completes the proof, Q. E. D..

The following statements are immediate consequences of Lemma 3.8: let G be a nonsingular commutative group-variety over the field k of characteristic p; if $p \neq 0$, the smallest group-subvariety V of G containing all the irreducible periodic group-subvarieties of G is itself periodic; it will be called the *maximal periodic subvariety of* G. The maximal vector subvariety of V is then also the only maximal vector subvariety of G. If $p = 0$, let V be a maximal vector subvariety of G; then G/V contains no positive dimensional vector group-subvariety, because if A were such a subvariety, the inverse image of A on G would be, by Lemma 3.8, a vector group-subvariety of G properly containing V. As a consequence, V is the only maximal vector subvariety of G. Similar results are true for a *maximal logarithmic subvariety of* G (for any value of p), this being defined as a logarithmic group-subvariety L of G which is not properly contained in any logarithmic group-subvariety of G; in fact, G/L contains no logarithmic group-subvariety of positive dimension, since otherwise the inverse image on G of any such subvariety would be, by Lemma 3.8, a logarithmic group-subvariety of G properly containing L. As a consequence, L is the only maximal logarithmic subvariety of G. We are now prepared to prove the following result:

THEOREM 3.3. - *Let G be a nonsingular rational commutative group-variety over the (algebraically closed) field k of characteristic p; let L be the maximal logarithmic subvariety of G, and let V be* (a) *the maximal vector subvariety of G if $p=0$, or* (b) *the maximal periodic subvariety of G if $p \neq 0$. Then $G \cong L \times V$.*

PROOF. - Set $A = G/V$; then A has no positive dimensional vector or periodic group-subvariety, otherwise V would not be maximal. We shall presently prove that A is logarithmic; let L^* be the maximal logarithmic subvariety of A, and set $B = A/L^*$. Since G is rational, so are A and B; if $\dim B > 0$, B has a 1-dimensional irreducible group-subvariety C, by Lemmas 3.4 and 3.1; C is rational, and is not a vector variety, or else its inverse image on A would contain a positive dimensional vector group-subvariety by Lemma 3.8. Hence C is logarithmic, and this contradicts the fact that L^* is maximal. This proves that $\dim B = 0$, and that $A = L^*$, so that $G \cong V \times A$ by Lemma 3.8. Now let α be the natural homomorphism of G onto $V = G/A$; if $\alpha L \neq E_V$, αL contains periodic points $\neq E_V$, with periods prime to p if $p \neq 0$; but this contradicts the relation $\alpha L \subseteq V$, and we conclude that $\alpha L = E_V$, $L \cong A$, Q. E. D..

A number of elementary properties of vector and logarithmic varieties can be deduced from Theorems 3.2 and 3.3 and Lemma 3.8. The « elementary » proofs of such properties are obvious in the case of characteristic zero, but, to the author' s knowledge, far from trivial, and apparently not to be found in the literature, for the case of positive characteristic. The most embracing of these properties is perhaps the one expressed in the following result, whose proof is left to the reader; for sake of generality we include periodic varieties:

COROLLARY. - *Let V be either a vector or a periodic variety over k, and let L be a logarithmic variety over k; let G be a nonsingular group-variety over k, isomorphic to $V \times L$. Then:*

(1) *Let G' be an irreducible group-subvariety of G; then $G' \cap V$ and*

$G' \cap L$ have, outside the degeneration locus of G, exactly one component V', L' respectively; V' is a vector or periodic variety, and L' is a logarithmic variety; moreover, $G' \cong V' \times L'$;

(2) *Let α be a homomorphism of G onto a nonsingular group-variety G' over k; set $V' = \alpha V$, $L' = \alpha L$; then V' is a vector or a periodic variety, and L' is a logarithmic variety; moreover, $G' \cong L' \times V'$.*

(In the previous statement, V and L have been identified with their images on G)..

4. **The group of algebraic equivalence on abelian varieties.** - Let G be an abelian variety of positive dimension n over k; let G' be a normal 1-dimensional vector or logarithmic variety over k, and let γ be a factor set of G into G', operating on $G_1 \times G_2$, where G_1, G_2 are copies of G; we say that γ is a *constant set* if $\gamma\{G_1 \times G_2\}$ is the modified extension over $k(G_1 \times G_2)$ of a point of G', or, equivalently, if $\gamma[P_1 \times Q_2]$ does not depend on P, Q when P, Q are generic points of G. We shall write Γ, Γ_0 in place of $\Gamma(G, G')$, $\Gamma_0(G, G')$ respectively, and shall denote by $\Gamma_c = \Gamma_c(G, G')$ the group of the constant sets; then $\Gamma_c \subset \Gamma_0 \subseteq \Gamma$, and Γ_c is isomorphic to either the additive group of the elements of k, or to the multiplicative group of the nonzero elements of k. We shall denote by $\backsim$ the relation of linear equivalence (on a variety which shall be specified, or tacitly understood, each time), and by $\equiv$ the equivalence of $(n-1)$-dimensional cycles of G defined in section 57 of [16]. If 0 denotes the zero cycle, we shall denote by $\mathfrak{L}_0$ the group of the cycles $X \backsim 0$ of G such that $E_G \notin \operatorname{rad} X$, and by $\mathfrak{A}_0$ the group of the cycles $X \equiv 0$ of G such that $E_G \notin \operatorname{rad} X$, so that $\mathfrak{L}_0$ is a subgroup of $\mathfrak{A}_0$. We have:

THEOREM 4.1. - *Maintain the previous notations, and assume G' to be a logarithmic variety; then Γ/Γ_c is isomorphic to $\mathfrak{A}_0$, and in this isomorphism Γ_0/Γ_c corresponds to $\mathfrak{L}_0$.*

PROOF. - Let x be a n. h. g. p. of G' such that the law of composition on G' is given by $x_3 = x_1 x_2$; let us denote by 0 the point of G' at which $x = 0$, and by ∞ the point at infinity (for x) of G'; then the degeneration locus of G' is the join of 0 and ∞. It is readily seen that the multiplicative notation for the law of composition on G' can be extended to the cases $P\infty = \infty$, $P0 = 0$ if P is a point of G', not 0 or ∞; the associative and commutative properties remain true when meaningful. If γ operates on the whole G', we shall assume $k(x) \subset k(G_1 \times G_2)$ as prescribed γ. Let H_0 and H_∞ be, respectively, the «numerator» and the «denominator» of the divisor of x on $G_1 \times G_2$; this means, by Theorem 3.1 of [2], that $H_0 = \gamma\{0\}^*$, $H_\infty = \gamma\{\infty\}^*$. Let G_3 be another copy of G, and assume $k(G_3) \subset k(G_1 \times G_2)$, in such a manner that this embedding generates the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. For any $(n-1)$-dimensional cycle Z of G, denote by T_Z' the cycle of $G_1 \times G_2$ obtained from Z_3 as T_Z is from Z_2. The relation

$$(10)\qquad (\gamma[P_1 \times Q_2R_2])(\gamma[Q_1 \times R_2]) = (\gamma[P_1Q_1 \times R_2])(\gamma[P_1 \times Q_2])$$

will now have a meaning and be valid when (1) none of the points $P_1 \times Q_2R_2$, $Q_1 \times R_2$, $P_1Q_1 \times R_2$, $P_1 \times Q_2$ belongs to $C = \text{rad}\, H_0 \cap \text{rad}\, H_\infty$ (this being the fundamental locus of γ on $G_1 \times G_2$), and (2) one factor at least an each side is neither H nor ∞. Let H be a component variety of $H_0 + H_\infty$ which operates on the whole G_1 and the whole G_2; we contend that there exists a component variety of $H_0 + H_\infty$ of the type $Y_1 \times G_2$, where Y is an $(n-1)$-dimensional irreducible subvariety of G, such that $H = T'_Y$. For if it were not so, it would be possible to find points P, Q, R of G such that $P_1 \times Q_2 \in H - (C \cap H)$, while $P_1Q_1 \times R_2$, $P_1 \times Q_2R_2$ and $Q_1 \times R_2$ do not belong to $\text{rad}\,(H_0 + H_\infty)$; but this would contradict formula (10). Conversely, let Y be an $(n-1)$-dimensional irreducible subvariety of G such that $Y_1 \times G_2$ is a component variety of $H_0 + H_\infty$, but assume T'_Y not to be a component variety of $H_0 + H_\infty$. Then again it is possible to find points P, Q, R of G such that $P_1Q_1 \times R_2 \in \text{rad}\,(H_0 + H_\infty) - C$, while $P_1 \times Q_2$, $P_1 \times Q_2R_2$, $Q_1 \times R_2$ do not belong to $\text{rad}\,(H_0 + H_\infty)$; this would also contradict (10). Hence, since $\gamma[P_1 \times Q_2]$ is symmetrical in P, Q, we conclude that there are distinct $(n-1)$-dimensional irreducible subvarieties $Z_1, Z_2, \ldots, Z_r$ of G, none of which contains E_G, and nonzero integers $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r$, such that $H_0 - H_\infty = (\Sigma_i a_iZ_i)_1 \times G_2 + (\Sigma_i a_iZ_i)_2 \times G_1 + \Sigma_i b_i T'_{Z_i}$. Hence the divisor of x on $(G_2)_{k(G_1)}$ is $(\Sigma_i a_iZ_i)_2^* + \Sigma_i b_i T'_{Z_i}\{G_1\}$, where $*$ denotes modified extension over $k(G_1)$. From the definition of γ it appears that $\gamma[E_{G_1} \times P_2]$ is a point of G', not 0 or ∞, independent of P when P is a generic point of G; therefore x is a unit of $Q(E_{G_1} \times G_2/G_1 \times G_2)$; if π denotes reduction of this ring modulo the prime of its nonunits, we have that πx is a nonzero element of k, so that its divisor on G_2 is the zero cycle. But it is well known, and easily seen, that such divisor is $H_0\{E_{G_1}\}^* - H_\infty\{E_{G_1}\}^* = (\Sigma_i a_iZ_i)_2 + \Sigma_i b_i T'_{Z_i}\{E_{G_1}\}^* = (\Sigma_i a_iZ_i)_2 + (\Sigma_i b_iZ_i)_2$. Consequently $b_i = -a_i$; by setting $Z = \Sigma_i a_iZ_i$, we conclude that $H_0 - H_\infty = Z_1 \times G_2 + G_1 \times Z_2 - T'_Z$. Hence $Z_2^* \backsim T'_Z\{G_1\}$, and therefore $Z \in \mathfrak{A}_0$. The correspondence $\gamma \to Z$ clearly establishes a homomorphism of Γ into $\mathfrak{A}_0$, if we agree to map on $Z = 0$ any γ operating on only one point of G'; the kernel of this homomorphism is then Γ_c. In order to prove that such homomorphism is onto $\mathfrak{A}_0$, we select a $Z \in \mathfrak{A}_0$; if $Z = 0$, any element of Γ_c corresponds to it; if $Z \neq 0$, we have $Z_2^* \backsim T'_Z\{G_1\}$ by assumption; hence $Z_2 \times G_1 - T'_Z$ is linearly equivalent, on $G_1 \times G_2$, to a cycle of the type $Z_1' \times G_2$; but then $-T'_Z\{G_2\}$ is linearly equivalent, on $(G_1)_{k(G_2)}$, to the modified extension of Z_1' over $k(G_2)$; since also $-T'_Z\{G_2\} \backsim -$(modified extension of Z_1 over $k(G_2)$), we conclude that $Z_1 \times G_2 + Z_2 \times G_1 \backsim T'_Z$. Let t be an element of $k(G_1 \times G_2)$ whose divisor on $G_1 \times G_2$ is $Z_1 \times G_2 + Z_2 \times G_1 - T'_Z$, and let γ be the rational mapping of $G_1 \times G_2$ onto

G' obtained by setting $x = t$. The operation of interchanging G_1 with G_2 transforms t into ht, for a nonzero element h of k; application of the same operation again shows that $h = \pm 1$, so that (co-ordinate of $\gamma[P_1 \times Q_2]$) $=$ $\pm$(co-ordinate of $\gamma[Q_1 \times P_2]$) for generic points P, Q of G; but $\gamma[P_1 \times P_2]$ is a point of G', neither 0 nor ∞, for a generic $P \in G$; hence $\gamma[P_1 \times Q_2] = \gamma[Q_1 \times P_2]$; the point $E_{G_1} \times E_{G_2}$ is not fundamental for γ, since it does not belong to $\mathrm{rad}(Z_1 \times G_2 + Z_2 \times G_1 + T'_Z)$; therefore $\gamma[E_{G_1} \times E_{G_2}]$ is a point of G', not 0 or ∞. For a $P \in G$, let σ_{P_1}, σ_{P_2} be the automorphism of $k(G_1 \times G_2)$ over, respectively, $k(G_2)$ and $k(G_1)$, which induce $(\sigma_P)_1$, $(\sigma_P)_2$ in $k(G_1)$, $k(G_2)$ respectively; if P, $Q \in G$, denote by $x(P_1, Q_2)$ the element of k to which x is congruent mod $\mathbf{P}(P_1 \times Q_2/G_1 \times G_2)$, if $x \in Q(P_1 \times Q_2/G_1 \times G_2)$. Then $x(P_1, Q_2)$ is the co-ordinate of $\gamma[P_1 \times Q_2]$; denote also by $x(P_1)$, $x(P_2)$ the elements of, respectively, $k(G_2)$, $k(G_1)$ to which x is congruent modulo, respectively, $\mathbf{P}(P_1 \times G_2/G_1 \times G_2)$, $\mathbf{P}(G_1 \times P_2/G_1 \times G_2)$; the same notation will be used for any element of $k(G_1 \times G_2)$ other than x. We have that the divisor of $\sigma_{P_1}^{-1}x$ on $(G_2)_{k(G_1)}$ is $Z_2^* - \sigma_{P_1}^{-1}T'_Z\{G_1\} = Z_2^* - T'_{\sigma_P^{-1}Z}\{G_1\}$, while the divisor of $\sigma_{P_2}^{-1}$ is $(\sigma_P^{-1}Z)_2^* - T'_{\sigma_P^{-1}Z}\{G_1\}$; hence the divisor of $(\sigma_{P_1}^{-1}x)/(\sigma_{P_2}^{-1}x)$ is $Z_2^* - (\sigma_P^{-1}Z)_2^*$, which is the modified extension over $k(G_2)$ of $Z_2 - (\sigma_P^{-1}Z)_2$; this, in turn, is also the divisor of $x(P_1)$; we conclude that there exists an element y of $k(G_1)$ such that $y\sigma_{P_1}^{-1}x = (\sigma_{P_2}^{-1}x)x(P_1)$. If P is generic, the elements $(\sigma_{P_1}^{-1}x)(E_{G_2})$, $(\sigma_{P_2}^{-1}x)(E_{G_2})$, $(x(P_1))(E_{G_2})$ exist, and equal respectively $(\sigma_P^{-1})_1(x(E_{G_2}))$, $x(P_2)$, $x(P_1, E_{G_2})$. But $x(E_{G_2}) \in k$, and therefore it coincides with $x(P_1, E_{G_2})$. Hence $y = x(P_2)$, so that $(\sigma_{P_1}^{-1}x)x(P_2) = (\sigma_{P_2}^{-1}x)x(P_1)$ for a generic $P \in G$. If $\{Q, R\}$ is a generic pair of ponts of G, we have therefore $[(\sigma_{P_1}^{-1}x)(Q_1, R_2)][x(Q_1, P_2)] = [(\sigma_{P_2}^{-1}x)(Q_1, R_2)][x(P_1, R_2)]$, or $(\gamma[P_1Q_1 \times R_2])(\gamma[Q_1 \times P_2]) = (\gamma[Q_1 \times P_2R_2])(\gamma[P_1 \times R_2])$, which is precisely relation (10). Hence γ is a factor set of G into G', as claimed, defined but for an element of Γ_c. Finally, it is quite clear that $\gamma \in \Gamma_0$ if and only if $Z \in \mathfrak{L}_0$, Q. E. D..

We shall now denote by $\mathfrak{A}$ the group of the $X \equiv 0$ of G, and by $\mathfrak{L}$ the gronp of the $X \sim 0$ of G. Since each element of $\mathfrak{A}$ is linearly equivalent to an element of $\mathfrak{A}_0$, we have the following corollary:

COROLLARY. - *Notations as in Theorem 4.1; then* Γ/Γ_0 *is isomorphic to* $\mathfrak{A}/\mathfrak{L}$

REMARK. - Let G, G' be commutative group-varieties over k, with degeneration loci F, F' respectively; we shall write the endomorphisms of G in the exponential form: if $P \in G - F$, and α is an endomorphism of G, we shall write $P^\alpha = \alpha P$; then $\alpha + \beta = \gamma$ if $P^\alpha P^\beta = P^\gamma$ for any $P \in G - F$, and $\alpha\beta = \gamma$ if $(P^\beta)^\alpha = P^\gamma$ for $P \in G - F$. The set of the endomorphisms of G thus becomes a ring. If $\gamma \in \Gamma(G, G')$, and α is an endomorhism of G, denote by γ_α the element of $\Gamma(G, G')$ such that $\gamma_\alpha[P_1 \times Q_2] = \gamma[P_1^\alpha \times Q_2^\alpha]$ for a generic pair of points $\{P, Q\}$ of G. Then $(\gamma_\beta)_\alpha = \gamma_{\beta\alpha}$; if $\gamma \in \Gamma_0(G, G')$, then $\gamma_\alpha \in \Gamma_0(G, G')$; more precisely, if $\gamma[P_1 \times Q_2] = (\mu[PQ])(\mu[P])^{-1}(\mu[Q])^{-1}$ (μ being a rational mapping of G into G'), we have $\gamma_\alpha[P_1 \times Q_2] = (\mu_\alpha[PQ])(\mu_\alpha[P])^{-1}(\mu_\alpha[Q])^{-1}$, where μ_α is defined by setting $\mu_\alpha[P] = \mu[P^\alpha]$ for a generic P of G. We contend that $\gamma_{\alpha+\beta}$ is associate to $\gamma_\alpha\gamma_\beta$; in fact, let μ be the rational mapping of G into G' such that, for a generic $P \in G$, we have $\mu[P] = \gamma[P_1^\alpha \times Q_2^\beta]$. Then $(\gamma_{\alpha+\beta}[P_1 \times Q_2])(\mu[Q])(\mu[P]) = (\gamma[P_1^\alpha P_1^\beta \times Q_2^\alpha Q_2^\beta])(\gamma[Q_1^\alpha \times Q_2^\beta])(\gamma[P_1^\alpha \times P_2^\beta]) = (\gamma[P_1^\alpha Q_1^\alpha P_1^\beta \times Q_2^\beta])(\gamma[P_1^\alpha P_1^\beta \times Q_2^\alpha])(\gamma[P_1^\alpha \times P_2^\beta]) = (\gamma[P_1^\alpha Q_1^\alpha P_1^\beta \times Q_2^\beta])(\gamma[P_1^\beta \times P_2^\alpha Q_2^\alpha])(\gamma[P_1^\alpha \times Q_2^\alpha]) = (\gamma[P_1^\alpha Q_1^\alpha \times P_2^\beta Q_2^\beta])(\gamma[P_1^\beta \times Q_2^\beta])(\gamma[P_1^\alpha \times Q_2^\alpha]) = (\gamma_\alpha[P_1 \times Q_2])(\gamma_\beta[P_1 \times Q_2])(\mu[PQ])$, which shows that $\gamma_{\alpha+\beta}\gamma_\alpha^{-1}\gamma_\beta^{-1} \in \Gamma_0(G, G')$. As a consequence, $\Gamma(G, G')/\Gamma_0(G, G')$ can be considered as an abelian group having the ring of endomorphisms of G as ring of operators. In particular, if ε is the identical endomorphism of G, then $\gamma_{n\varepsilon}$ is associate to γ^n, for each nonnegative integer n. The relationship of this fact to the content of § XI of [16], in particular Proposition 32, is quite obvious.

5. **The invariant derivations.** - Let K be an algebraic function field over the arbitrary field k; a *derivation in K over k* is a mapping D of K into itself which maps k into 0, and such that $D(x+y) = Dx + Dy$, $D(xy) = xDy + yDx$ for $x, y \in K$. It is well known that if $n = \operatorname{transc} K/k$ and $\operatorname{ins}(K:k) = 1$, the derivations of K over k form a free K-module of order n. If $x_1, \ldots, x_n$ are elements of K such that K is a finite separable extension of $k(x)$, then a derivation D of K over k is uniquely determined by assigning (arbitrarily) the elements Dx_i of K. If V is an irreducible variety over k, of inseparability 1, the derivations in $k(V)$ over k will also be called the *derivations on V*.

Let G be a nonsingular group-variety over (the algebraically closed field) k, with degeneration locus F. A derivation D on G is said to be *left-invariant* (respectively *right-invariant*) if $\sigma_P Dx = D\sigma_P x$ (respectivey $\tau_P Dx = D\tau_P x$) for each $x \in k(G)$ and each $P \in G - F$. If D is left-invariant and right-invariant, it will simply be called *invariant*. Let G_1, G_2, G_3 be copies of G, and let B be the rational mapping of $G_1 \times G_2$ onto G_3 which gives the law of composition on G. Let $\{x_1, \ldots, x_m\}$ be a n. h. g. p. of G such that $x_i = 0$ at E_G; we shall identify G_1 with G, and shall denote by $\{y\}$, $\{z\}$ the copies of $\{x\}$ in $k(G_2)$, $k(G_3)$ respectively. Consider $k(G_3)$ as a subfield of $k(B) = k(G_1 \times G_2)$ as prescribed by B, and let $\mathbf{O}$ be the quotient ring of the identity of $(G_2)_{k(G_1)}$; then $\mathbf{O}$ is a regular geometric domain; let $\mathbf{P}$ be the ideal of its nonunits. If $n = \dim G$, it is possible to select n linear combinations of $y_1, \ldots, y_m$, with coefficients in k, which form a regular set of parameters of $\mathbf{O}$; after a projective transformation of co-ordinates, we may assume that these are $\{y_1, \ldots, y_n\}$; then $k(G_2)$ is a separable extension of $k(y_1, \ldots, y_n)$. Since $z_i \in \mathbf{O}$, there are elements $\omega_{ij} \in k(G_1)$ such that

$$z_j \equiv x_j + \Sigma_{i=1}^n \omega_{ij} y_i \pmod{\mathbf{P}^2} \tag{11}$$

for $j = 1, \ldots, n$. Since the set $\{z_1 - x_1, \ldots, z_n - x_n\}$ is a regular set of parameters of $\mathbf{O}$, we have $\det(\omega_{ij}) \neq 0$; hence there are n uniquely determined independent derivations $D_1, \ldots, D_n$ on $G_1 = G$ such that $D_i x_j = \omega_{ij}$; we intend to prove that each D_i is left-invariant. In fact, for any $P \in G - F$, there is an automorphism σ_P^* of $k(B)$ over $k(G_2)$ which induces $(\sigma_P)_1$, $(\sigma_P)_3$ in, respectively, $k(G_1)$, $k(G_3)$. Hence $\sigma_P^* \mathbf{O} = \mathbf{O}$, $\sigma_P^* \mathbf{P} = \mathbf{P}$, and therefore

$$\sigma_P^* z_j \equiv \sigma_P^* x_j + \Sigma_{i=1}^n (\sigma_P^* \omega_{ij}) y_i \qquad (\text{mod } \mathbf{P}^2). \tag{12}$$

Now, $\sigma_P^* \omega_{ij} = \sigma_P \omega_{ij} = \sigma_P D_i x_j$; on the other hand, if $\partial/\partial x_i$ denotes the derivation on G such that $\partial x_j/\partial x_i = \delta_{ij}$ (KRONECKER symbol) $(i, j = 1, \ldots, n)$, it is well known (see for instance [8] or [9]) that $(\sigma_P)_3 z_j \equiv \sigma_P x_j + \Sigma_i (\partial \sigma_P x_j/\partial x_i)(z_i - x_i)$ (mod $\mathbf{P}^2$), since $\mathbf{P} = \mathbf{P}(I/G_1 \times G_3)$, I being the identical correspondence between G_1 and G_3. On replacing for $z_i - x_i$ the expression given by (11), we obtain $\sigma_P^* z_j \equiv \sigma_P^* x_j + \Sigma_{ih} (\partial \sigma_P x_j/\partial x_i) \omega_{hi} y_h$ (mod $\mathbf{P}^2$). This, compared with (12), gives $\sigma_P \omega_{hj} = \Sigma_i (\partial \sigma_P x_j/\partial x_i) D_h x_i = D_h \sigma_P x_j$, or $\sigma_P D_h x_j = D_h \sigma_P x_j$, as claimed. A set of n independent right-invariant derivations Δ_i would be defined by $z_j \equiv y_j + \Sigma_{i=1}^n (\Delta_i y_j) x_i$ (mod $\mathbf{P}'^2$), where $\mathbf{P}' = \mathbf{P}((E_{G_1})_{k(G_2)}/(G_1)_{k(G_2)})$. The left-invariant derivations on G form a free k-module of order n.

LEMMA 5.1. - *Let G be a nonsingular group-variety over k, and set $\mathbf{o} = Q(E_G/G)$, $\mathbf{p} = \mathbf{P}(E_G/G)$; let D be any left-invariant derivation on G; then $Dt \in \mathbf{o}$ if $t \in \mathbf{o}$, and $Dt \in \mathbf{p}^{r-1}$ if $t \in \mathbf{p}^r$, $r \geq 1$.*

PROOF. - It is enough to prove the lemma when D is any of the D_i previously defined; in the notation of (11), we shall first prove that $\omega_{ij} \in \mathbf{o}$. And in fact, set $\mathbf{O}^* = Q(E_{G_1} \times E_{G_2}/G_1 \times G_2)$, and let $\mathbf{P}^*$ be the ideal of the nonunits of $\mathbf{O}^*$; then $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ is a regular set of parameters of $\mathbf{O}^*$, and $z_j \in \mathbf{P}^*$; hence there are forms $\varphi_{ji} \in k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ of degree i, for $i = 1, 2, \ldots$, such that, for each integer $r \geq 1$, $z_j \equiv \Sigma_{i=1}^r \varphi_{ji}$ (mod $\mathbf{P}^{*r+1}$); now, set $\mathbf{p}_2^* = \mathbf{P} \cap \mathbf{O}^*$; for each i, write $\varphi_{ji} = \psi_{ji} + \Sigma_{h=1}^n \chi_{jih} y_h + \nu_{ji}$, where: $\psi_{ji} \in k[x_1, \ldots, x_n]$ is a form af degree i; $\chi_{jih} \in k[x_1, \ldots, x_n]$ is a form of degree $i - 1$; $\nu_{ij} \in k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ belongs to $\mathbf{p}_2^{*2}$. Then $z_j \equiv \Sigma_{i=1}^r (\psi_{ji} + \Sigma_{h=1}^n \chi_{jih} y_h)$ (mod $\mathbf{p}_2^{*2} + \mathbf{P}^{*r+1}$). We shall now denote by $\overline{\mathbf{O}}$ the completion of $\mathbf{O}^*$, by $\overline{\mathbf{p}}$ the topological closure of $\mathbf{p}_2^*$ in $\overline{\mathbf{O}}$ (which coincides with $\mathbf{p}_2^* \overline{\mathbf{O}}$), by $\overline{\mathbf{o}}$ the topological closure of $\mathbf{o}$ in $\overline{\mathbf{O}}$, and shall set $\mathbf{Q} = \overline{\mathbf{O}}_{\overline{\mathbf{p}}}$, $\mathbf{q} = \mathbf{p}_2^* \mathbf{Q} = \overline{\mathbf{p}} \mathbf{Q}$. Then there are elements $\psi_j = \Sigma_{i=1}^\infty \psi_{ji}$, $\chi_{jh} = \Sigma_{i=1}^\infty \chi_{jih}$ of $\mathbf{O}$, and the previous relation implies $z_j \equiv \psi_j + \Sigma_{h=1}^n \chi_{ih} y_h$ (mod $\overline{\mathbf{p}}^2$), or also (mod $\mathbf{q}^2$). On the other hand, $\mathbf{Q}$ contains $\mathbf{O} = \mathbf{O}^*_{\mathbf{p}_2^*}$, and $\mathbf{PQ} = \mathbf{p}_2^* \mathbf{Q} = \mathbf{q}$, so that (11) can be written $z_j \equiv x_j + \Sigma_{h=1}^n \omega_{hj} y_h$ (mod $\mathbf{q}^2$); therefore $(\psi_j - x_j) + \Sigma_{h=1}^n (\chi_{jh} - \omega_{hj}) y_h \in \mathbf{q}^2$. Now, $\mathbf{Q}$ is a regular local ring, with the regular set of parameters $\{y_1, \ldots, y_n\}$, and contains as a subring the qnotient field of $\overline{\mathbf{o}}$ to which $\psi_j - x_j$ and $\chi_{jh} - \omega_{hj}$ belong. Hence $\psi_j - x_j = \chi_{jh} - \omega_{hj} = 0$, or $\omega_{hj} = \chi_{jh} \in \overline{\mathbf{o}} \cap k(G) = \mathbf{o}$, ar claimed. Now, define a derivation $\overline{D}_j$ in the quotient field of $\overline{\mathbf{o}}$ (over k) by setting $\overline{D}_j \Sigma_{i=0}^\infty g_i = \Sigma_{h=1}^n (D_j x_h) \Sigma_{i=0}^\infty \partial g_i/\partial x_h$, whenever $g_i \in k[x_1, \ldots, x_n]$ are forms of degree i. It is readily seen that $\overline{D}_j$

induces D_j in $k(G)$, and that, since $D_j x_h \in \mathbf{o}$, we have $D_j t \in \bar{\mathbf{o}}$ if $t \in \mathbf{o}$, and $D_j t \in \bar{\mathbf{p}}^{r-1}$ if $t \in \mathbf{p}^r$, Q. E. D..

Lemma 5.2. - *Notations as in Lemma 5.1. Let $D_1, \ldots, D_n$ be the left-invariant derivations on G defined by* (11); *then $D_i x_j \equiv \delta_{ij}$* (mod $\mathbf{p}$), *where δ_{ij} is Kroneckers' s symbol.*

Proof. - According to the proof of Lemma 5.1, we have $D_i x_j \in \mathbf{o}$; let $a_{ij} \in k$ be such that $D_i x_j \equiv a_{ij}$ (mod $\mathbf{p}$); then $z_j - x_j - \Sigma_{i=1}^n a_{ij} y_i \in \mathbf{p}_2{}^{*2} + \mathbf{p}_1{}^* \mathbf{p}_2{}^* \subseteq \mathbf{P}^{*2}$, if $\mathbf{p}_1{}^* = \mathbf{p}_1 \mathbf{O}^* = \mathbf{p}\mathbf{O}^*$. Operating with the corresponding right-invariant derivations Δ_i, one would find elements $b_{ij} \in k$ such that $z_j - y_j - \Sigma_{i=1}^n b_{ij} x_i \in \mathbf{P}^{*2}$. Hence $x_j - y_j + \Sigma_{i=1}^n (a_{ij} y_i - b_{ij} x_i) \in \mathbf{P}^{*2}$, or $\Sigma_i (\delta_{ij} - b_{ij}) x_i - (\delta_{ij} - a_{ij}) y_i \in \mathbf{P}^{*2}$; since $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ is a regular set of parameters of $\mathbf{O}^*$, this implies $\delta_{ij} - b_{ij} = \delta_{ij} - a_{ij} = 0$, Q. E. D..

6. Noncommutative group-varieties.

Lemma 6.1. - *Let G be a group-variety over k, with the degeneration locus F; let S be a set of points of G. Then there exists a group-subvariety V of G such that the points of $V - (V \cap F)$ are all and only the points P of $G - F$ which satisfy the relation $PQ = QP$ for each $Q \in S - (S \cap F)$.*

Proof. - Given a $Q \in G - F$, there exists a rational mapping α of G into a copy G_1 of G such that, for any $P \in G - F$, we have $\alpha[P] = (PQP^{-1})_1$; set $V_Q = \alpha[Q_1]$; then $P \in V_Q - (V_Q \cap F)$ if and only if $PQ = QP$. Let V' be the intersection of all the V_Q when Q ranges over $S - (S \cap F)$, and let V be the join of all the components of V' which are not subvarieties of F; then V has the required property, Q. E. D..

If, in particular, $S = G$, V is called the *center of G*; we say that G is *central* if the center of G is E_G.

Lemma 6.2. - *Let V be an n-dimensional nonsingular vector variety over k, and let V_1, V_2 be copies of V; then there exist a nonsingular group-variety G over k, with degeneration locus F, and an algebraic correspondence D between G and $V_1 \times V_2$, such that:*

(1) $\dim G = n^2$;

(2) *when P ranges over $G - F$, $D[P]$ has exactly one component S_P outside the degeneration locus of $V_1 \times V_2$, and S_P ranges over all the isomorphisms between V_1 and V_2;*

(3) *if s_P is the automorphism of $k(V)$ over k which is related to S_P (as automorphisms of $k(V)$ are related to isomorphisms of V), then the correspondence $P \rightarrow s_P$ is a group-isomorphism;*

(4) *$D\{G\}$ and $D\{V_1 \times V_2\}$ are absolutely irreducible.*

The group-variety G is unique, but for isomorphisms.

Proof. - We may assume V to have a n. h. g. p. $\{x_1, \ldots, x_n\}$ such that the law of composition on V is given by $(x_i)_3 = (x_i)_1 + (x_i)_2$. Denote by X the one-column matrix $(x_1, \ldots, x_n)$, and by X_1, X_2 the copies of X related to, respectively, V_1 and V_2. Let G be an n^2-dimensional projective space over k, with n. h. g. p. $\{y_{ij}\}$ $(i, j = 1, ..., n)$, and let Y be the matrix (y_{ij}); define a law of composition on G by setting $Y_3 = Y_1 Y_2$ (matrix-product). Then G becomes a group-variety whose degeneration locus F is the radical of the divisor of $\det Y$ on G. For a $P \in G - F$, denote by $Y(P)$ the matrix obtained by mapping the elements of Y into k, $\bmod \mathbf{P}(P/G)$. Let D be the algebraic correspondence between G and $V_1 \times V_2$ such that a basis of the ideal $\wp(D/k[(x)_1, (x)_2, y])$ is formed by the elements of the matrix $X_2 - YX_1$. Then, for any $P \in G - F$, the only component of $D[P]$ which is not a subvariety of the degeneration locus of $V_1 \times V_2$ is the S_P such that $\wp(S_P/k[(x)_1, (x)_2])$ has as a basis the set of the elements of the matrix $X_2 - Y(P)X_1$; clearly, S_P is an isomorphism of V_1 onto V_2. Conversely, if S is an isomorphism of V_1 onto V_2, it is readily seen that there exist elements η_{ij} of k such that $\det(\eta_{ij}) \neq 0$, and that a basis of $\wp(S/k[(x)_1, (x)_2])$ is given by the set of the $(x_i)_2 - \Sigma_j \eta_{ij}(x_j)_1$ $(i = 1, ..., n)$; if P is the point of G whose co-ordinates are the η_{ij}, then $S = S_P$. Statements (3) and (4) are easily verified, and the uniqueness of G is a consequence of the fact that G is the representative variety of a certain algebraic system of cycles on $V_1 \times V_2$, Q. E. D..

Any group-variety isomorphic to an irreducible group-subvariety of the group-variety G (for some value of n) of Lemma 6.2 will be called a *Vessiot variety.* The nature of the degeneration locus of the group-variety G shows that no VESSIOT variety of positive dimension is an abelian variety. The direct product of two VESSIOT varieties is a VESSIOT variety; vector varieties and logarithmic varieties are VESSIOT varieties.

Let G be a nonsingular group-variety over k, with degeneration locus F; set $\mathbf{o} = Q(E_G/G)$, $\mathbf{p} = \mathbf{P}(E_G/G)$; let G_1 be a copy of G, and set $\mathbf{O} = Q(E_{G_1} \times G/G_1 \times G)$, $\mathbf{P} = \mathbf{P}(E_{G_1} \times G/G_1 \times G)$. If $n = \dim G$, let $\{y_1, ..., y_m\}$ be a n. h. g. p. of G_1 such that $y_i \in \mathbf{p}_1$, and that $\{y_1, ..., y_n\}$ is a regular set of parameters of $\mathbf{o}_1$; for any positive integer r, let υ_r be the homomorphic mapping of $\mathbf{o}_1$ onto $\mathbf{o}_1/\mathbf{p}_1^{r+1}$ whose kernel is $\mathbf{p}_1^{r+1}$; if $\mathbf{o}_1/\mathbf{p}_1$ is identified with k, it is well known that $\upsilon_r\mathbf{p}_1 = \mathbf{p}_1/\mathbf{p}_1^{r+1}$ is a k-module isomorphic to the direct sum of the k-modules $\mathbf{p}_1^{i}/\mathbf{p}_1^{i+1}$ $(i = 1, 2, ..., r)$; for each positive integer i, let $\{y_{i1}, ..., y_{iN_i}\}$ be a k-basis for the forms of $k[y_1, ..., y_n]$ of degree i, and take in particular $y_{1j} = y_j$ $(j = 1, ..., n)$; then a k-basis for $\upsilon_r\mathbf{p}_1$ is the set of the $\upsilon_r y_{ij}$ for i $= 1, 2, ..., r$, and for all the possible values of j. We shall now introduce the operator $\rho_P = \sigma_P\tau_P^{-1}$, defined whenever σ_P, τ_P have a meaning; we have $\rho_{PQ} = \rho_P\rho_Q$. Let $\{x\}$ be a copy of $\{y\}$ in $k(G)$, and let X be the point of $(G_1)_{k(G)}$ whose co-ordinates are $x_1, ..., x_m$; then, for $i = 1, ..., n$, we have $\rho_X y_i \in \mathbf{P}$, hence $\rho_X y_{ij} \in \mathbf{P}$. Now, $\mathbf{O}/\mathbf{P}^{r+1}$ can be identified with the extension of $\mathbf{o}_1/\mathbf{p}_1^{r+1}$ over $k(G)$; we shall accordingly extend υ_r to the homomorphic mapping of $\mathbf{O}$ onto $\mathbf{O}/\mathbf{P}^{r+1}$ whose kernel is $\mathbf{P}^{r+1}$. Write

(13) $$\upsilon_r \rho_X y_{ij} = \Sigma_{hl}\, b_{ijhl} \upsilon_r y_{hl},$$

where Σ_{hl} is extended over the values $1, 2, \ldots, r$ of h, and over all the possible values of l; we have $b_{ijhl} \in k(G)$. We remark that a change in the choice of the y_{ij} (including a different choice of n. h. g. p.) does not affect the ring $k[\ldots, b_{ijhl}, \ldots]$. The matrix (b_{ijhl}), where i and j remain fixed on each column, has a nonzero determinant, since the elements $\upsilon_r \rho_X y_{ij}$ form a basis for $\upsilon_r \mathbf{P}$. Let $P \in G - F$; then there exist elements $\bar{b}_{ijhl}$ of k such that

(14) $$\upsilon_r \rho_{P_1} y_{ij} = \Sigma_{hl}\, \bar{b}_{ijhl} \upsilon_r y_{hl}.$$

Let π_P denote the homomorphic mapping of $Q(P/G)$ onto k whose kernel is $\mathbf{q} = \mathbf{P}(P/G)$. Set $\mathbf{q}' = \mathbf{P}(P \times G_1 / G \times G_1)$, and consider a third copy G_2 of G, with n. h. g. p. $\{z\} = \{\rho_X y\}$; the embedding of $k(G_2)$ into $k(G \times G_1)$ generates a rational mapping D of $G \times G_1$ onto G_2, such that if $P \times Q_1$ is a generic point of $G \times G_1$, we have $D[P \times Q_1] = (P^{-1}QP)_2$. As a consequence, this relation is true whenever P, Q are points of $G - F$. But then, for $P \in G - F$, we have $z_i - \rho_{P_1} y_i \in \mathbf{q}'$, or $\rho_X y_i - \rho_{P_1} y_i \in \mathbf{q}'$. Let $P \in G - F$ be such that z_i and b_{ijhl} belong to $\mathbf{O}^* = Q(P \times E_{G_1} / G \times G_1)$ for $i, h = 1, \ldots, r$; let $\mathbf{P}^*$ be the ideal of the nonunits of $\mathbf{O}^*$; then $\rho_{P_1} y_{ij} - \rho_X y_{ij} \in \mathbf{O}^* \cap \mathbf{q}' = \mathbf{q}^* = \mathbf{q}\mathbf{O}^*$, and (14) gives $\rho_{P_1} y_{ij} - \Sigma_{hl}\, \bar{b}_{ijhl} y_{hl} \in \mathbf{P}^{*^{r+1}}$, while (13) gives $\rho_X y_{ij} - \Sigma_{hl}\, b_{ijhl} y_{hl} \in \mathbf{P}^{r+1} \cap \mathbf{O}^* \subset \mathbf{P}^{*^{r+1}}$; hence $\Sigma_{hl}(b_{ijhl} - \bar{b}_{ijhl}) y_{hl} + (\rho_{P_1} y_{ij} - \rho_X y_{ij}) \in \mathbf{P}^{*^{r+1}}$, or $\Sigma_{hl}(b_{ijhl} - \bar{b}_{ijhl}) y_{hl} \in \mathbf{q}^* + \mathbf{P}^{*^{r+1}}$; hence $\Sigma_{hl}(\pi_P b_{ijhl} - \bar{b}_{ijhl}) y_{hl} \in \pi_P \mathbf{P}^{*^{r+1}}$, if π_P is naturally extended to a homomorphic mapping of $\mathbf{O}^*$ onto $\mathbf{o}_1$ with kernel $\mathbf{q}^*$. But $\pi_P \mathbf{P}^* = \mathbf{p}_1$, and $\pi_P \mathbf{P}^{*^{r+1}} = \mathbf{p}_1^{\,r+1}$; hence $\Sigma_{hl}(\pi_P b_{ijhl} - \bar{b}_{ijhl}) y_{hl} \in \mathbf{p}_1^{\,r+1}$, a fact which proves that $\pi_P b_{ijhl} = \bar{b}_{ijhl}$ if P is generic.

Denote by $X(P)$ the point of $(G_1)_{k(G)}$ whose co-ordinates are $\sigma_P^{-1} x_1, \ldots, \sigma_P^{-1} x_m$; the element $\rho_{X(P)} y_{ij}$ is obtained by applying to $\rho_X y_{ij}$ the automorphism of $k(G \times G_1)$ over $k(G_1)$ which induces σ_P^{-1} in $k(G)$; such automorphism we shall denote by σ_P^*. On the other hand, $\rho_{X(P)} y_{ij}$ is also obtained by applying to y_{ij} the automorphism of $k(G \times G_1)$ over $k(G)$ given by $\rho_{X(P)} \rho_X^{-1} = \rho_{X(P)X^{-1}}$; now, $X(P)X^{-1} = P_1$, so that $\rho_{X(P)} \rho_X^{-1} = \rho_{P_1}$. Accordingly, $\sigma_P^* \rho_X y_{ij} = \rho_{P_1} \rho_X y_{ij}$, or, by (13), $\Sigma_{hl}(\sigma_P^{-1} b_{ijhl}) y_{hl} \equiv \Sigma_{pq}\, b_{ijpq} \rho_{P_1} y_{pq} \pmod{\mathbf{P}^{r+1}}$, and by (14): $\Sigma_{hl}(\sigma_P^{-1} b_{ijhl}) y_{hl} \equiv \Sigma_{hl} \Sigma_{pq}\, b_{ijpq} \pi_P b_{pqhl} y_{hl} \pmod{\mathbf{P}^{r+1}}$, if P is generic; this means that $\sigma_P^{-1} b_{ijhl} = \Sigma_{pq}\, b_{ijpq} \pi_P b_{pqhl}$. This implies that the matrix $(\pi_P b_{pqhl})$, where p, q remain constant in each column, has a nonvanishing determinant.

Let B be the Vessiot variety with n. h. g. p. $\{B_{ijhl}\}$ ($i, h = 1, \ldots, r$; j, l compatibe with these), where the B_{ijhl} are indeterminates, with the law of composition given by $(B_{ijhl})_3 = \Sigma_{pq}(B_{pqhl})_1 (B_{ijpq})_2$; let α_r' be the rational point of $B_{k(G)}$ at which B_{ijhl} has the value b_{ijhl}, and set $\alpha_r = D_{\alpha_r', G}$. Then the previous formula indicates that, for a generic pair of points $\{P, Q\}$ of G, we have $(\alpha_r[P])(\alpha_r[Q]) = \alpha_r[PQ]$. Hence, by Lemma 2.3, α is a homomorphism of G into B, and operates on a VESSIOT variety B_r; this shows also that $\bar{b}_{ijhl} = \pi_P b_{ijhl}$ for any $P \in G - F$. Since $k(B_r) \subseteq k(B_{r+1})$, there exists a positive integer s such that $k(B_r) = k(B_s)$ if $r \geq s$, but not if $r < s$. If C is the kernel of α_s, we have, from (14), that $\rho_P x_{ij} = x_{ij}$ for all i, j, and for a $P \in G - F$, if and only if $P \in C$; hence C is the center of G. We shall express these results in the following theorem:

THEOREM 6.1. - *Let G be a nonsingular group-variety over k, and let C be the center of G; then there exists a homomorphism α of G onto a Vessiot variety B, such that the kernel of α is C.*

We remark that if k has characteristic 0, then $B \cong G/C$; otherwise, this is not necessarily true; however, a particular B and a particular α satisfying Theorem 6.1, and uniquely determined but for, respectively, isomorphism and equivalence, have been constructed in the course of the previous analysis; they will be called, respectively, the *stem* and the *stem-homomorphism of G*. The method of construction of the variety B, denoted by B_s in the preceding proof, gives some further information: in the previous notation, and for $i = 1, 2, \ldots$, we shall define r_i by recurrence in the following manner: r_1 is the integer such that $\dim B_{r_1} > 0$, but $\dim B_{r_1 - 1} = 0$ if $r_1 > 1$; r_i, for $i > 1$, is the integer such that $k(B_{r_{i-1}}) = k(B_{r_i - 1}) \subset k(B_{r_i})$, if such r_i exists; the largest existing r_i, say r_ν is s. If G is not commutative, there is a finite sequence $\{r_1, r_2, \ldots, r_\nu = s\}$ of integers, which we call the *first*, *second* ..., *ν-th index of G*; if G is commutative, we shall define ∞ to be the only index of G; the integer ν will be called the *rank of G*, and we set $\nu = 0$ by definition if G is commutative. If $1 \leq i < \nu$, the embedding of $k(B_{r_i})$ into $k(B_{r_{i+1}})$ generates a rational mapping β_{i+1} of $B_{r_{i+1}}$ onto B_{r_i}; β_{i+1} is clearly a homomorphism such that $\alpha_{r_i} = \beta_{i+1}\alpha_{r_{i+1}}$; the kernel V_{i+1} of β_{i+1} is the join of the components, outside the degeneration locus of $B_{r_{i+1}}$, of the subvariety of $B_{r_{i+1}}$ given by the equations $b_{pjhl} = \delta_{ph}\delta_{jl}$ (KRONECKER's symbols) for p, $h = 1, \ldots, r_{i+1} - 1$, and for all the possible values of j, l. If P is a point of $G - F$ such that $\alpha_{r_{i+1}-1}P$ is the identity, equation (14), because of the meaning of the y_{pj}, indicates also that $\pi_P b_{pjhl}$ equals: 0 if $p = r_{i+1}$ and $h < r_{i+1}$; δ_{jl} if $p = h = r_{i+1}$. Therefore the matrix $M = (b_{pjhl})$ (for p, $h = 1, \ldots, r_{i+1}$), where h, l remain constant on each row, acquires at P the form $M(P) = \left(\begin{array}{c|c} I & O \\ \hline M'(P) & I \end{array}\right)$, where I designates any identical matrix, O any (rectangular) matrix whose elements are all 0, and $M'(P)$ is the value at P of a rectangular matrix M'; if Q is another point of $G - F$ such that $\alpha_{r_{i+1}-1}Q$ is the identity, we have $M(P)M(Q) = \left(\begin{array}{c|c} I & O \\ \hline M'(P) + M'(Q) & I \end{array}\right)$, a fact which indicates that the component of the identity in V_{i+1} is a vector variety (see the Corollary to Theorem 3.3). The same argument shows that B_{r_1} is a vector variety if $r_1 > 1$.

Theorem 6.2. - *Let G be a nonsingular noncommutative group-variety over the (algebraically closed) field k of characteristic p; if $p=0$, then the rank and the index of G both equal 1; if $p\neq 0$, then each index of G is divisible by p.*

Proof. - We maintain the previous notation, and write a_{ij} for $b_{[i]j}$ $(i, j=1, \ldots, n)$. If X has the same meaning as in the symbol ρ_X, the element z_j of formula (11) coincides with $\sigma_X^{-1}y_j$, so that (11) can be written

$$\sigma_X^{-1}y_j \equiv x_j + \Sigma_i (D_i x_j)y_i \qquad (\mathrm{mod}\ \mathbf{P}^2); \tag{15}$$

on the other hand, a basis $\{\Delta_1, \ldots, \Delta_n\}$ for the right-invariant derivations on G is obtained by setting

$$\tau_X^{-1}y_j \equiv x_j + \Sigma_i (\Delta_i x_j)y_i \qquad (\mathrm{mod}\ \mathbf{P}^2); \tag{16}$$

by applying σ_X to (15) we obtain $y_j \equiv x_j + \Sigma_i (D_i x_j)\sigma_X y_i$ $(\mathrm{mod}\ (\sigma_X \mathbf{P})^2)$, and by applying τ_X^{-1} to this: $\tau_X^{-1}y_j \equiv x_j + \Sigma_i (D_i x_j)\rho_X y_i$ $(\mathrm{mod}\ \mathbf{P}^2)$, or, by (16): $\Sigma_i (\Delta_i x_j)y_i \equiv \Sigma_i (D_i x_j)\rho_X y_i$ $(\mathrm{mod}\ \mathbf{P}^2)$; this, by (13) for $r=1$, becomes $\Sigma_i (\Delta_i x_j)y_i = \Sigma_{ih} (D_i x_j)a_{ih}y_h$, or $\Delta_h = \Sigma_i a_{ih}D_i$, a fact which proves that the matrix (a_{ij}) transforms the k-module of left-invariant derivations on G into the k-module of the right-invariant derivations on G. If we assume the first index of G to be $r_1 > 1$, it follows that each left-invariant derivation is invariant. Let then $D_1', \ldots, D_n'$ be copies of $D_1, \ldots, D_n$ on G_1, and let the same symbols denote also their extensions over $k(G)$. Formula (13) gives

$$\rho_X y_i \equiv y_i + \varphi_i \qquad (\mathrm{mod}\ \mathbf{P}^{r_1+1}), \tag{17}$$

where $\varphi_i \in k[y_1, \ldots, y_n]$ is a form of degree r_1, and $\varphi_i \neq 0$ for at least one value of i. Application of D_j' to this congruence yields, by Lemma 5.1: $\rho_X D_j' y_i \equiv D_j' y_i + D_j' \varphi_i$ $(\mathrm{mod}\ \mathbf{P}^{r_1})$. Now, by Lemma 5.2, we have $D_j'\varphi_i \equiv \partial\varphi_i/\partial y_j$ $(\mathrm{mod}\ \mathbf{P}^{r_1})$, so that $\rho_X D_j' y_i \equiv D_j' y_i + \partial\varphi_i/\partial y_j$ $(\mathrm{mod}\ \mathbf{P}^{r_1})$. If $p=0$, or if $p\neq 0$ but r_1 is not divisible by p, we have that $\partial\varphi_i/\partial y_j \neq 0$ for at least one value of i, j, so that $\rho_X D_j' y_i - D_j' y_i \notin \mathbf{P}^{r_1}$. On the other hand, set $D_j' y_i = t$, so that, by Lemma 5.1, $t \in \mathbf{O}$; then $t \equiv f(y)$ $(\mathrm{mod}\ \mathbf{P}^{r_1})$, where $f(y) \in k[y_1, \ldots, y_n]$ is a polynomial of degree $< r_1$; from (17) we obtain $\rho_X f(y) \equiv f(y)$ $(\mathrm{mod}\ \mathbf{P}^{r_1})$, so that $\rho_X t - t \in \mathbf{P}^{r_1}$, a contradiction. We conclude that $r_1 = 1$ if $p=0$, and that r_1 is divisible by p if $p\neq 0$. Now, assume $p=0$, and let r_2 be the second index of G, if it exists. We have seen that $\Delta_h = \Sigma_i a_{ih}D_i$, so that $\Delta_h x_j = \Sigma_i a_{ih}D_i x_j$, and therefore, for $P \in G - F$, $\sigma_P^{-1}\Delta_h x_j = \sigma_P^{-1}\Sigma_i a_{ih}D_i x_j = \Sigma_i (\sigma_P^{-1}a_{ih})(D_i \sigma_P^{-1}x_j)$. Now, in the discussion which led to Theorem 6.1 we proved that $\sigma_P^{-1}a_{ih} = \Sigma_s a_{is}\pi_P a_{sh}$; if P belongs to the kernel of α_1, we have therefore $\sigma_P^{-1}a_{ih} = a_{ih}$, so that $\sigma_P^{-1}\Delta_h x_j = \Sigma_i a_{ih}D_i\sigma_P^{-1}x_j = \Delta_h \sigma_P^{-1}x_j$; hence $\rho_P \Delta_h x_j = \Delta_h \rho_P x_j$ for such P. Formula (14) gives, for such P:

$$\rho_P x_j \equiv x_j + \psi_{jP} \qquad (\mathrm{mod}\ \mathbf{p}^{r_2+1}), \tag{18}$$

where ψ_{jP} is obtained from a form $\psi \in k(G)[y_1, ..., y_n]$, of degree r_2, by first replacing each coefficient with its image according to π_P (which exists), and then replacing $\{y_1, ..., y_n\}$ with $\{x_1, ..., x_n\}$; moreover, the fact that r_2 is the second index of G indicates that $\psi_{jP} \neq 0$ for at least one $P \notin F$ of the kernel of α_1. Since $\rho_P \Delta_h x_j = \Delta_h \rho_P x_j$, we can operate on the last congruence as we did on (17), with the result that $\rho_P \Delta_h x_j - \Delta_h x_j \notin \mathbf{p}^{r_2}$ for at least one value of h. Set again $t = \Delta_h x_j \in \mathbf{o}$, and write $t \equiv f(x) \pmod{\mathbf{p}^{r_2}}$, where $f(x) \in k[x_1, ..., x_n]$ has degree $< r_2$; then (18) implies that $\rho_P f - f \in \mathbf{p}^{r_2}$, hence $\rho_P t - t \in \mathbf{p}^{r_2}$, a contradiction. This proves that the second index of G does not exist, or that G has rank 1.

Finally, assume $p \neq 0$, and assume the s-th index r_s of G to exist: we shall prove by recurrence on i that r_i is divisible by p. This is true for $i = 1$; assume it to be true for $i = 1, 2, ..., s-1$; then a formula similar to (18), with r_2 replaced by r_s, is true, and the relation $\rho_P \Delta_h x_j = \Delta_h \rho_P x_j$ is true for any $P \notin F$ of the kernel of $\alpha_{r_{s-1}}$. Then the same type of proof previously applied would lead to a contradiction unless r_s is a multiple of p, Q, E. D..

We shall now give two examples in order to illustrate the substantial difference between the two cases of Theorem 6.2. Assume $p \neq 0, 2$, and let G be the 3-dimensional projective space over k with n. h. g. p. $\{x_1, x_2, x_3\}$; define a law of composition on G by setting $(x_1, x_2, x_3)(y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3 + (x_1 y_2 - x_2 y_1)^p)$; then G becomes a noncommutative group-variety, with the plane at infinity as degeneration locus. It is readily seen that $\rho_X y_1 = y_1$, $\rho_X y_2 = y_2$, $\rho_X y_3 = 2^p (y_1 x_2 - x_1 y_2)^p$, so that the rank of G is 1, the index is p, and the inseparability of the stem-homomorphism of G is p^2. As another example, consider the 2-dimensional projective space G over k (of characteristic $p \neq 0$), with n. h. g. p. $\{x_1, x_2\}$, and define a law of composition on G by setting $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_1^p + y_2)$; then G becomes a noncommutative group-variety whose degeneration locus is the line at infinity, and whose center is the point $(1, 0)$. In the notation of (13) we have $b_{1111} = 1$, $b_{1112} = b_{1211} = 0$, $b_{1212} = x_1^p$, so that the kernel of α_1 is the group-subvariety of G defined by the equation $x_1 = 1$. Therefore G has the first index $= 1$, but rank > 1.

THEOREM 6.3. - *Any abelian group-subvariety of a nonsingular group-variety G over k is a subvariety of the center of G.*

PROOF. - If G is not commutative, let B be the stem of G, and let α be the stem-homomorphism of G. If A is an abelian group-subvariety of G, then αA is an abelian group-subvariety of B, and is therefore 0-dimensional since B is a VESSIOT variety. Hence A is a subvariety of the kernel of α, which is the center of G, Q. E. D..

The previous result is a generalization of Theorem 5 of [16], and its proof depends only on the fact that the degeneration locus of an abelian variety is empty. Theorem 6.3 could also be obtained, if it were known a priori that A is an invariant group-subvariety of G, by observing that each ρ_P, for $P \in G - F$ ($F =$ degeneration locus of G), induces an automorphism of A; as the set of the automorphisms of A is discrete, by [16], it follows that each ρ_P induces the identical automorphism on A; the same proof can be used to show that *any invariant logarithmic group-subvariety of G, and any 0-dimensional invariant group-subvariety of G is a subvariety of the center of G;* we will not develop the proof since no use will be made of these results in the present work.

Theorems 6.3 and 3.1 give:

COROLLARY. - *Let A be an abelian group-subvariety of the nonsingular group-variety G over k; then G contains an invariant irreducible group-subvariety B such that G is the homomorphic image, in a homomorhism of finite degree, of the direct product $A \times B$.*

THEOREM 6.4. - *Let G be a nonsingular group-variety over k; let C be the component of the identity in the center of G; let B be the maximal rational group-subvariety of C. Then G contains aninvariant irreducible group-subvariety H such that:*

(1) *G/H is an abelian variety;*

(2) *there exists a homomorphism α of H onto a Vessiot variety, and the kernel of α is a group-subvariety B' of the center of G, such that B is the component of the identity in B'.*

PROOF. - If G is commutative, this is a consequence of Theorems 3.2 and 3.3. If G is not commutative, let S, β be, respectively, the stem and the stem-homomorphism of G. By Theorem 6.1, C is the component of the identity in the kernel of β; let γ be the natural homomorphism of G onto G/B; then, by Theorem 2.2, there exists a homomorphism β' of G/B onto S such that $\beta = \beta'\gamma$. By Theorem 3.2, γC is abelian, so that, by the Corollary to Theorem 6.3, there exists an invariant irreducible group-subvariety H' of G/B such that $G/B = (\gamma C, H')$; since γC is a component of the kernel of β', we have that $\beta' H' = S$, and that $\alpha' = [\beta'; H', S]$ has finite degree. Let H be the component of the identity in $\gamma^{-1}H'$, and let δ be the homomorphism of G/B onto γC (whose existence is asserted by Theorem 3.1) such that H' is the component of the identity in the kernel of δ. Then $\delta\gamma$ is a homomorphism of G onto γC, and the component of the identity in the kernel of $\delta\gamma$ is H; since γC is abelian, it follows that G/H is also abelian, as asserted. Now set $\gamma' = [\gamma; H, G/B]$, so that γ' is a homomorphism of H onto H', and set $\alpha = \alpha'\gamma'$; then α is a homomorphism of H onto the VESSIOT variety S; on the other hand, we have $\alpha = [\beta; H, S]$, so that the kernel of α is the join of the components, outside the degeneration locus of G, of the intersection of H with the center of G. As α' has finite degree, one of these components is B, Q. E. D..

7. Remarks. - Let G be an n-dimensional abelian variety over k, and tet G' be a 1-dimensional vector variety over k. Let γ be a factor set of G into G'; let G_1, G_2 be copies of G, with the n. h. g. p. $\{x_i\}$, $\{y_i\}$ (copies of each other). As seen in section 4, if γ operates on the whole G', it prescribes an embedding of $k(G')$ into $k(x, y)$. It t is a n. h. g. p. of G, such that the law of composition on G' is given by $t_3 = t_1 + t_2$, we can write $t = t(x, y)$ as a rational function of x, y. We shall assume $x_i = 0$ at E_{G_1}, so that $y_i = 0$ at E_{G_2}. As seen in the proof of Theorem 4.1, formula (10) can be written $t(\sigma_{P_1}^{-1} x, y) + t(x, z) = t(x, \sigma_{P_2}^{-1} y) + t(z, y)$ if $\{z\}$ are the co-ordinates of P_1 or P_2. We can consider $\{z\}$ as the n. h. g. p. of a third copy G_3 of G, and write $\sigma_{P_1}^{-1} x_i = g_i(z, x) = g_i(x, z)$, g_i being symbol of a rational function with coefficients in k; then the previous formula becomes

$$t(g(z, x), y) + t(x, z) = t(x, g(z, y)) + t(z, y). \tag{19}$$

Let $\{D_1', \ldots, D_n'\}$ be a basis for the invariant derivations on G_1, which we shall consider extended over $k(y, z)$, and let D_i be the copy of D_i' on G_3, which we shall consider extended over $k(y)$, and D_i^* be the copy of D_i' on G_2, which we shall consider extended over $k(z)$. Then $[D_i' g_j(y, x)]_{x=0} = D_i z_j$; therefore, if we apply D_i' to formula (19), and then set $x = 0$, we obtain $D_i t(z, y) + [D_i' t(x, z)]_{x=0} = D_i' t(x, g(z, y))]_{x=0}$, or, after setting $[D_i' t(x, z)]_{x=0} = \varphi_i(z)$: $D_i t(z, y) = \varphi_i(g(z, y)) - \varphi_i(z)$. Therefore $D_j^* D_i t(z, y) = D_j^* \varphi_i(g(z, y))$, and for $z = 0$, $D_j^* \varphi_i(y) = [D_j^* D_i t(z, y)]_{z=0}$; but the previous formula, for $y = 0$, gives $D_j \varphi_i(z) = [D_j^* \varphi_i(g(z, y))]_{y=0} = [D_j^* D_i t(z, y)]_{y=0} = [D_i D_j^* t(z, y)]_{y=0}$; hence $D_j^* \varphi_i(y) = [D_i^* D_j t(y, z)]_{z=0} = D_i^* \varphi_j(y)$. Let d be the differential operator on $(G_3)_{k(G_2)}$, and let $\{\omega_1, \ldots, \omega_n\}$ be a k-basis for the invariant differentials on G_3 (which are all of the first kind [2]), selected in such a way that $\Sigma_i \omega_i D_i z_j = dz_j$. We shall write $\omega_i(z)$ in place of ω_i, so that $\omega_i(y)$ has an obvious meaning; then the previous formula indicates that $\omega(z) = \Sigma_i \varphi_i(z) \omega_i(z)$ is a closed differential, and we can write $dt(z, y) = \omega(g(z, y)) - \omega(z)$. If G' were a logarithmic 1-dimensional variety, this formula should be replaced by $dt(z, y)/t(z, y) = \omega(g(z, y)) - \omega(z)$. It is not difficult to see that $\omega(z)$ is a differential of the second kind if G' is a vector variety, and of the third kind if G' is a logarithmic variety. If we set $\omega = 0$ when γ does not operate on the whole G', the mapping $\gamma \rightarrow \omega$ is a homomorphism of the group $\Gamma = \Gamma(G, G')$ into the group of the differentials of, respectively, the second or the third kind on G_3 which are finite at E_{G_3}; the element $\gamma \in \Gamma$ belongs to $\Gamma_0 = \Gamma_0(G, G')$ if and only if the corresponding ω is (1) an exact differential, plus a differential of the first kind, if G' is a vector variety, or (2) of the type da/a, for $0 \neq a \in k(G_3)$, plus a differential of the first kind, if G' is a logarithmic variety.

(2) The word *differential* is used in any of the equivalent meanings recently appeared in the literature; see for instance [10] or [12].

Denote by $\mathfrak{D}$, $\mathfrak{D}_2$, $\mathfrak{D}_1$, $\mathfrak{D}_e$, $\mathfrak{D}_l$ the additive groups of, respectively, the closed differentials on G_3, the closed differentials of the second kind, the differentials of the first kind, the exact differentials, and the differentials of the type da/a, for $0 \neq a \in k(G_3)$. If G' is a logarithmic variety, and k has characteristic 0, it can be proved, by transcendental means, that the mapping $\gamma \rightarrow \omega$ induces an isomorphism between Γ/Γ_0 and $\mathfrak{D}/(\mathfrak{D}_2 + \mathfrak{D}_l)$; the algebraic equivalent of this fact is expressed by Theorem 4.1, and is valid for any characteristic. If G' is a vector variety, and k has characteristic 0, it can be proved, by transcendental means, that the mapping $\gamma \rightarrow \omega$ induces an isomorphism between Γ/Γ_0 and $\mathfrak{D}_2/(\mathfrak{D}_1 + \mathfrak{D}_e)$; since, in this case, it is also known that $\mathfrak{D}_2/(\mathfrak{D}_1 + \mathfrak{D}_e)$ is a free k-module of order n, it follows that Γ/Γ_0 has the same structure. There are indications that this result could follow, without any use of the differentials, from the considerations which close section 4, but the author has been unable to supply the complete proof; if the characteristic of k is positive, then each element of Γ/Γ_0 is periodic, and each $\{G, G', \gamma\}$ contains a group-subvariety isogenous to G.

Lemma 3.6 does not give complete information on commutative periodic group-varieties; the type of argument used in its proof can, however, be extended to yield the complete structure of any such variety, but the result is unduly complicated; an example of a periodic commutative variety G of period 8 over a field of characteristic 2 is the following: G is the 3-dimensional projective space with n. h. g. p. $\{x, y, z\}$, with the law of composition given by $x_3 = x_1 + x_2$, $y_3 = y_1 + y_2 + x_1x_2$, $z_3 = z_1 + z_2 + y_1y_2 + x_1x_2(y_1 + y_2 + x_1^2 + x_2^2)$.

The points of contact of section 6 with the method of LIE algebras are obvious. It has been known (see for instance [5]) that such a method is highly unsatisfactory for the case of positive characteristic; as seen in the proof of Theorem 6.2, the method of LIE algebras depends on the study of the module $\mathfrak{p}/\mathfrak{p}^2$ (in the notation of that proof), and on the effect of the left-invariant derivations on the field $k(\ldots, b_{1j11}, \ldots)$; its failure in the positive characteristic case is due to two distinct reasons, namely: (1) $\mathfrak{p}/\mathfrak{p}^{r+1}$ may yield more information for some $r > 1$ than for $r = 1$; (2) the stem-homomorphism may have inseparability > 1. Our method takes care of the first difficulty, but does not overcome the second; if this second difficulty could be overcome, a more precise formulation of Theorem 6.4 could be given, and would probably state that H is a VESSIOT variety.

The investigation of $\mathfrak{p}/\mathfrak{p}^{r+1}$ rather than $\mathfrak{p}/\mathfrak{p}^2$ corresponds, approximately, to the consideration of invariant derivations of higher order, as defined in [8] or [9], instead of just those of order 1, as the LIE method does; this, in turn, is made necessary by the fact that derivations of higher order are not iterated derivations of the first order when the characteristic is positive.

We close by remarking that our definition of factor sets is tailored to the commutative case; some of the results of section 6, and perhaps more precise results, could be expressed in terms of factor sets, after the definition of these is generalized in an obvious manner in order to apply to the noncommutative case. The content of section 6 can also be improved after learning more about the structure of VESSIOT varieties. This can be achieved by methods similar to those of section 3; in fact, a minor modification of the proof of Lemma 3.1 yields the result: *any nonabelian n-dimensional group-variety over k contains some positive dimensional proper group-subvariety if* $n > 1$. Application of this result to VESSIOT varieties establishes the existence of the well known « one-parameter groups ». The author plans to deal with these questions in the future.

BIBLIOGRAPHY

[1] I. BARSOTTI, *Algebraic correspondences between algebraic varieties*, « Ann. of Math. », 52, 1950, p. 427. See also *Errata*, ibid., 53, 1951, p. 587.

[2] —— *Local properties of algebraic correspondences*, « Amer. Math. Soc. Trans. », 71, 1951, p. 349).

[3] —— *Intersection theory for cycles of an algebraic variety*, « Pacific Journ. of Math. », 2, 1952, p. 473, (3).

[4] —— *A note on abelian varieties*, « Rend. Circ. Mat. di Palermo », 2, 1953, p. 236.

[5] C. CHEVALLEY, *Théorie des groupes de Lie; II, Groupes algébriques*, « Act. Scien. Ind. », No. 1152, Paris, 1951).

[6] W. L. CHOW, *On the quotient variety of an abelian variety*, « Proc. Nat. Acad. Scie. U.S.A. », 38, 1952, p. 1039).

[7] F. CONFORTO, *Funzioni abeliane e matrici di Riemann*, « Corsi R. Ist. Naz. Alta Mat. », Roma, 1942.

[8] H. HASSE and F. K. SCHMIDT, *Noch eine begründung der theorie der höheren differentialquotienten in einem algebraischen funktionenkörper einer unbestimmten*, « Journ. Reine Angew. Math. », 177, 1937, p. 215.

[9] A. JAEGER, *Eine algebraische theorie vertauschbarer differentiationen für körper beliebiger charakteristik*, « Journ. Reine Angew. Math. », 190, 1952, p. 1.

[10] S. KOIZUMI, *On the differential forms of the first kind on algebraic varieties*, « Journ. Math. Soc. Japan », 2, 1951, p. 273).

[11] E. R. KOLCHIN, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, « Ann. of Math. », 49, 1948, p. 1.

[12] S. NAKANO, *On invariant differential forms on group varieties*, « Journ. Math. Soc. Japan », 2, 1951, p. 216.

[13] M. ROSENLICHT, *Equivalence relations on algebraic curves*, « Ann. of Math. », 56, 1952, p. 169.

[14] —— *Differentials of the second kind for algebraic function fields of one variable*, « Ann. of Math. », 57, 1953, p. 517.

[15] F. SEVERI, *Funzioni quasi abeliane*, « Pontif. Acad. Scien. Scripta Varia », 4, 1947.

[16] A. WEIL, *Variétés abéliennes et courbes algébriques*, « Act. Scien. Ind. », No. 1064, Paris, 1948.

(3) On p. 486 of [3] (proof of Lemma 2.3), delete the portion of line 2 from bottom which follows the word « have ». Also replace m^{-1} by m^{-2} in the 5th line of p. 499.