ANNALS OF MATHEMATICS
Vol. 71, No. 2, March, 1960
Printed in Japan

ISOGENIES AND DUALITY OF ABELIAN VARIETIES

BY PIERRE CARTIER

(Received September 29, 1959)

TABLE OF CONTENTS

Introduction

The purpose of this paper is to prove two theorems on abelian varieties (cf., Theorems 1 and 2 in Chapter III, §§ 6 and 7). The first one is known as the duality hypothesis for abelian varieties and implies that a certain canonical homomorphism from an abelian variety to the Picard variety of its own Picard variety is indeed an isomorphism. This theorem has been proved by Weil and Chow up to inseparability in characteristic $p \neq 0$. I have given (in [5]) the sketch of a proof for the characteristic $p \neq 0$ using very peculiar methods; but the argument was quite complicated and

assumed a thorough examination of many particular cases.

Using a result by Matsusaka [10], the second asserted theorem implies that on an abelian variety numerical and algebraic equivalence for divisors are identical. Here we prove that for any divisor D on an abelian variety and any integer $m \neq 0$, the relation $m \cdot D \approx 0$ implies $D \approx 0$, that is D algebraically equivalent to zero. This result was first proved by I. Barsotti [2, 3] then by J.-P. Serre [14] in characteristic $p \neq 0$, the case of characteristic 0 being an immediate corollary of Weil's results [16].

Both theorems will be proved at the same time in our Chapter III. We use mainly a theory of isogenies disregarding any separability assumption. For separable isogenies, our results are a very sophisticated elaboration of the usual Galois theory. The main idea is the linearization of Galois theory, undertaken first by E. Artin [1], and under a less transparent form by N. Bourbaki [4].

A brief résumé of the different chapters is as follows:

In Chapter I, we give the formal definition of a k-structure for a vector space. The idea of working on a vector space with two scalar fields at the same time is largely taken from algebraic geometry, and the author owes this to A. Weil. We have attempted to give a convenient intrinsic language, the results being all trivial; the aim to be intrinsic, apart from aesthetic considerations, is mainly motivated by our methods of dealing with isogenies, where there is no privileged basis. Once a k-structure is given on a vector space, one can speak of rationality for a vector, a subspace, or a linear function, with respect to a field k' containing k. If A is such an object, the main properties are the following:

(1) There exists a field $k(A)$ such that A is rational over k' if and only if k' contains $k(A)$.

(2) If $\sigma : k' \to k''$ is a k-isomorphism, and A is rational over k', there is defined A^σ rational over k'' in such a way that $k(A^\sigma) = k(A)^\sigma$, and $A^\sigma = A$ if and only if σ induces the identity on $k(A)$.

(3) If $\tau : k'' \to k'''$ is another k-isomorphism, one gets $(A^\sigma)^\tau = A^{\tau\sigma}$. From these properties it follows for instance that if k is the field of invariants of some group G of automorphisms, A is rational over k if and only if it is invariant under G.

The remainder of the chapter introduces the notion of a group operating at the same time on a field and a vector space, and gives a criterion for lowering the field of definition, generalized from Weil [19].

In Chapter II, we study an algebraic group operating on a vector space over the function field of some transformation space for it. The general result asserting that there exist enough invariants under certain

conditions is taken from S. Lang and E. Kolchin [8], but the proof given here is rather different from theirs. We apply this result to give a new proof for the existence of invariant differential operators. This enables us to give (at least theoretically) a classification of isogenies. This question could also be explored by means of algebraic coherent sheaves, and we hope sometime to elaborate this point of view.

In Chapter III, we study abelian varieties. The main idea comes from Hasse [7] and Roquette [11]. It is to associate to a divisor class a certain commutative algebra whose characters are in one-to-one correspondence with some other divisor classes. Roquette's investigations were limited to the separable case in order to apply Galois and Kummer theory; once this difficulty is overcome by the methods developed in our Chapter II, the remainder follows immediately and gives the principal result without further effort. The main point, due to Roquette, is to consider a generic divisor class instead of the zero class as suggested by Weil in § 11 of his book [16].

Our main source of reference for abelian varieties will be Lang's book [9]; we shall refer to it by the following abbreviations: L-III$_3$, Th. 3 means "Theorem 3 in § 3 of Chapter III of Lang's book." The appearance of this book greatly helped the author, concerned for a long time by the fact that some of the main results on abelian varieties remained hidden in "secret" papers.

CHAPTER I

FIELD OF DEFINITION OF A VECTOR SPACE

Notation. We consider a field K and a subfield k of K; by a field, we mean a subfield of K containing k. A vector space, unless otherwise specified, is a vector space over K, and a linear map is a K-linear map. If k' is a field, any vector space becomes by restricting the scalars a vector space over k'; we shall use a prefix "k'-" when referring to this structure over k'.

1. Definition of a k-structure

Let V be a vector space. A k-subspace V_k of V is said to define a *k-structure on V* if the following equivalent conditions hold.

(a) *At least one k-basis of V_k is a basis of V.*

(b) *Any k-basis of V_k is a basis of V.*

(c) *A subset of V_k linearly independent over k is still linearly independent over K; moreover, V_k generates the vector space V.*

(d) *Let W be a vector space and f a k-linear map from V_k to W. Then f admits a unique extension to a linear map from V to W.*

(e) *The additive map* λ *from*

$$K \bigotimes_k V_k$$

to V *defined by* $\lambda(\xi \otimes v) = \xi \cdot v$ *is bijective.*

Proof of equivalence:

(a) $\Rightarrow$ (d): Assuming (a), let $\{e_i\}$ be a k-basis of V_k which is still a basis for V. If f and W are as in (d), there exists a unique linear map from V to W which agrees with f on the e_i, that is on V_k.

(d) $\Rightarrow$ (e): Assuming (d), there exists a linear map μ from V to $K \bigotimes_k V_k$ such that $\mu(x) = 1 \otimes x$ for x in V_k; clearly λ and μ are reciprocal maps, and this proves that λ is bijective.

(e) $\Rightarrow$ (b): If $\{e_i\}$ is a k-basis of V_k, it follows from the standard properties of tensor products that any element in $K \bigotimes_k V_k$ can be uniquely written in the form $\sum \xi_i \otimes e_i$ with $\xi_i \in K$ for all i. Assuming (e), the map λ is bijective and any element in V can be uniquely written in the form $\lambda\left(\sum \xi_i \otimes e_i\right) = \sum \xi_i \cdot e_i$; therefore $\{e_i\}$ is a basis of V.

(b) $\Rightarrow$ (c): Assuming (b), it is clear that V_k generates V. Moreover a subset of V_k linearly independent over k is contained in a k-basis of V_k, that is, a basis of V by virtue of (b), and is therefore linearly independent over K.

(c) $\Rightarrow$ (a): Assuming (c), any k-basis of V_k is still linearly independent over K, and generates V since V_k does.

Let V_k be a k-structure on V. For any field k', let us define $V_{k'}$ as the k'-subspace $k' \cdot V_k$ of V generated by V_k. A k-basis of V_k is a basis of V by (b); being linearly independent over K by (c), this basis is *a fortiori* the same over k' and is therefore a k'-basis of $V_{k'}$. This shows that $V_{k'}$ is a k'-structure on V. When we shall refer to a k'-structure, for V, it will always be understood, without further specification, that this structure is defined by $V_{k'}$.

2. Rationality for a vector

Let V *be a vector space with a* k*-structure* V_k. A vector v in V is said to be *rational over* k if it is contained in V_k; a basis of V is said to be rational over k if all of its elements are rational over k.

Let $\{e_i\}$ be a basis of V, rational over k. The elements e_i are linearly independent over K and *a fortiori* over k. Let v be in V_k; the subset of V consisting of v and the e_i is not linearly independent over K, and therefore is not so over k, by property (c) of a k-structure; therefore, one gets a relation $v = \sum \xi_i \cdot e_i$ with $\xi_i \in k$ for all i, and $\{e_i\}$ is a k-basis of V_k. Conversely, any k-basis of V_k is a basis of V by (b), and such a basis is rational over k.

Let k' be a field and v a vector in V. If $\{e_i\}$ is a basis of V rational over k, that is a k-basis of V_k and therefore a k'-basis of $V_{k'}$. If $v = \sum \xi_i \cdot e_i$, the vector v is rational over k' if and only if the field k' contains all the ξ_i, that is the field $k(v)$ generated over k by these elements. Therefore the field $k(v)$ is indeed independent of the choice of the basis $\{e_i\}$ rational over k. This follows also from the fact that $k(v)$ is generated over k by all the values $f(v)$ for the linear forms f on V such that $f(V_k) \subset k$.

3. Rationality for a subspace

Let V be a vector space with a k-structure V_k. A vector subspace W of V is said to be *rational over k* if it is generated by a set of rational vectors over k; this being so, one has *a fortiori* $W = K \cdot (W \cap V_k)$, and since any subset of $W \cap V_k$ linearly independent over k is linearly independent over K, the set $W \cap V_k$ is a k-structure on W, called the *induced k-structure* on W.

Let $\{c_\alpha\}$ be a basis of K considered as a vector space over k. By standard properties of tensor products and property (e) in § 1, any vector in V has a unique expression in the form:

$$v = \sum_\alpha c_\alpha \cdot v_\alpha \qquad (v_\alpha \in V_k). \tag{1}$$

Furthermore, one can assume $c_0 = 1$ for some index $\alpha = 0$; therefore, V_k consists of those elements v of the form (1) with $v_\alpha = 0$ for $\alpha \neq 0$. This result implies two things:

(a) Let T be a k-subspace of V_k; the vectors in $K \cdot T$ are those elements of the form (1) with $v_\alpha \in T$ for all α; therefore, $K \cdot T \cap V_k$ consists of those vectors with $v_\alpha = 0$ for $\alpha \neq 0$, that is $v = 1 \cdot v_0$ with $v_0 \in T$. We have proved the formula

$$K \cdot T \cap V_k = T;$$

together with the formula

$$W = K \cdot (W \cap V_k)$$

valid for any subspace W of V rational over k, this shows that *the reciprocal maps $W \to W \cap V_k$ and $T \to K \cdot T$ define a one-to-one correspondence between the set of subspaces W of V rational over k and the set of k-subspaces T of V_k.*

(b) Let T be a k-subspace of V_k, intersection of a family of k-subspaces T_i of V_k. The vectors in $K \cdot T$ are the vectors $v = \sum_\alpha c_\alpha \cdot v_\alpha$ with $v_\alpha \in T$ for all α, that is $v_\alpha \in T_i$ for all α and i; since T_i is the set of vectors $v = \sum_\alpha c_\alpha \cdot v_\alpha$ with v_α in T_i for all α, one gets the formula

$$K \cdot T = \bigcap_i K \cdot T_i$$

from

$$T = \bigcap_i T_i .$$

Together with the preceding result, this shows that *any intersection of subspaces of V rational over k is itself rational over k.*

Let k' be a field. If W is a subspace of V rational over k, let us put $T = W \cap V_k$ in such a way that $W = K \cdot T$; therefore $W = K \cdot (k' \cdot T)$ and one gets $W \cap V_{k'} = k' \cdot T$ by applying the result (a) proved before to k' instead of k and to the k'-subspace $k' \cdot T$ of V_k. In other words, W is rational over k' and $W \cap V_{k'} = k' \cdot (W \cap V_k)$ in such a way that the two k'-structures obtainable on W by inducing or extending the scalars are identical.

We shall now characterize the fields over which a given subspace is rational.

PROPOSITION 1. *Let V be a vector space with a k-structure. For any subspace W of V there exists a field $k(W)$ such that the relations "W is rational over k'" and "$k(W)$ is contained in k'" are equivalent for any field k'.*

Let $\{e_i\}_{i \in I}$ be a basis of V rational over k; by standard results, there is a subset I'' of I such that the vectors e_j for j in I'' form a basis of V modulo W. This means that V is the direct sum of W and the subspace V'' having $\{e_j\}_{j \in I''}$ as a basis; but V is the direct sum of V'' and the subspace V' having as a basis the e_i for i in $I' = I - I''$. Therefore there exists a unique isomorphism f of V' onto W such that $f(v') - v' \in V''$ for any v' in V'. If one puts $v_i = f(e_i)$ for $i \in I'$, the vectors v_i form a basis of W and they are of the following type

$$v_i = e_i - \sum_{j \in I''} \xi_{ij} \cdot e_j \qquad (i \in I') \tag{2}$$

for some scalars ξ_{ij} in K ($i \in I'$ and $j \in I''$). Moreover, no nonzero linear combination of the e_j for $j \in I''$ is in W since $W \cap V'' = 0$.

Let $k(W)$ be the field generated over k by the ξ_{ij}. If a field k' contains $k(W)$, the vectors v_i are rational over k' and so is W. Conversely, suppose that W is rational over some field k'. Let $\{c_\alpha\}$ be a basis of K over k' such that $c_0 = 1$ for some index $\alpha = 0$; put $\xi_{ij} = \sum_\alpha \eta_{ij\alpha} \cdot c_\alpha$ with some $\eta_{ij\alpha}$ in k'; one gets therefore:

$$v_i = c_0 \cdot (e_i - \sum_j \eta_{ij0} \cdot e_j) - \sum_{\alpha \neq 0} c_\alpha \cdot (\sum_j \eta_{ij\alpha} \cdot e_j) . \tag{3}$$

Since W is rational over k' and the v_i are in W, the considerations in (a) above show that the coefficient of each c_α in (3) belongs to W and is rational over k'; for $\alpha \neq 0$ the form of the coefficient of c_α implies therefore $\eta_{ij\alpha} = 0$ for $i \in I'$ and $j \in I''$ since no nonzero linear combination of the e_j is in W. Therefore $\xi_{ij} = \eta_{ij0}$ is in k', and k' contains $k(W)$. q.e.d.

When V is finite dimensional, it follows easily from the previous proof that $k(W)$ is generated by the mutual ratios of the Plücker coordinates of W with respect to any given basis of V rational over k.

4. Rationality for linear and multilinear maps

We shall investigate in this paragraph the question of rationality for the multilinear maps. Two particular cases are worth mentioning; the first one concerns the linear maps; the second one the multilinear and linear forms, that is, the case of functions with values in K endowed with the k-structure defined by k.

Let V_i for $1 \leqq i \leqq r$ and W be vector spaces, each one endowed with a k-structure. A multilinear map f from $V_1 \times \cdots \times V_r$ to W is called *rational over* k if $f(v_1, \cdots, v_r)$ is rational over k when the v_i are so. It is clear that any multilinear map obtained by composition of some multilinear maps rational over k is itself rational over k.

Let $\{e_\alpha^{(i)}\}$ be a basis of V_i rational over k (for $1 \leqq i \leqq r$); since any vector in V_i rational over k is a linear combination with coefficients in k of the basic elements, a multilinear function f as before is rational over k if and only if $f(e_{\alpha_1}^{(1)}, \cdots, e_{\alpha_r}^{(r)})$ is rational over k for all choices of the indices $\alpha_1, \cdots, \alpha_r$; if $\{e'_j\}$ is a basis of W rational over k and if one puts

$$f(e_{\alpha_1}^{(1)}, \cdots, e_{\alpha_r}^{(r)}) = \sum_j f^j_{\alpha_1, \cdots, \alpha_r} \cdot e'_j \tag{4}$$

the function f is rational over k if and only if the components $f^j_{\alpha_1, \cdots, \alpha_r}$ are in k. From that follow two facts:

(a) Let k' be a field. *In order that f be rational over k', it is necessary and sufficient that k' contain the field $k(f)$ generated over k by the elements $f^j_{\alpha_1, \cdots, \alpha_r}$*; in fact, the bases $\{e_\alpha^{(i)}\}$ and $\{e'_j\}$ are rational over k, and *a fortiori* over k'.

(b) Let us assume the spaces $V_1, \cdots, V_r$ to be finite-dimensional. Let $\mathcal{L}$ be the space of all multilinear maps from $V_1 \times \cdots \times V_r$ to W, and $\mathcal{L}_k$ be the subset of $\mathcal{L}$ consisting of the maps rational over k. The correspondence $f \to (f^j_{\alpha_1, \cdots, \alpha_r})$ is linear and one-to-one between $\mathcal{L}$ and the set of all families of elements in K with only a finite number of nonzero components; since $\mathcal{L}_k$ is mapped in this way on the set of all families with components in k, one sees that $\mathcal{L}_k$ is a k-structure on $\mathcal{L}$. Furthermore, for any field k', the set $\mathcal{L}_{k'}$ of the multilinear maps rational over k' is equal to $k' \cdot \mathcal{L}_k$.

Let finally V and W be two vector spaces with respective k-structures V_k and W_k and let f be a linear map from V to W rational over k. If a subspace S of V is rational over k, it is generated by $S \cap V_k$ and therefore $f(S)$ being generated by $f(S \cap V_k) \subset W_k$ is rational over k. Let

now T be a subspace of W rational over k; for a k-basis $\{c_\alpha\}$ of K, any vector v in V is uniquely expressed as $\sum_\alpha c_\alpha \cdot v_\alpha$ for some v_α in V_k, and such a vector is in $f^{-1}(T)$ if and only if $f(v_\alpha)$ is in T for all α since $f(v) = \sum_\alpha c_\alpha \cdot f(v_\alpha)$; therefore $f^{-1}(T)$ is generated by $f^{-1}(T) \cap V_k$ and is rational over k.

From the previous results, we shall deduce that *the linear map f is rational over k if and only if its graph Γ is a subspace of $V \times W$ rational over k* (for the k-structure $V_k \times W_k$ on $V \times W$). Indeed, Γ is the image of the map $g : v \to (v, f(v))$ of V into $V \times W$ and if f is rational over k, so is g and so is its image Γ. Conversely, assume Γ rational over k; there exists therefore a basis of Γ consisting of vectors of $V \times W$ rational over k; such a basis is of the form $\{(e_i, f(e_i))\}$ where e_i and $f(e_i)$ are rational over k for all i; but since the projection from Γ to V is an isomorphism of vector spaces, the e_i form a basis of V rational over k, and since the $f(e_i)$ are rational over k, so is f.

5. Conjugates

Let V be a vector space with a k-structure V_k and let σ be a k-isomorphism from a field k' onto a field k''.

We shall study the behavior under σ of the vectors, the subspaces and the multilinear maps. To begin with, we contend that there exists a unique map $v \to v^\sigma$ from $V_{k'}$ onto $V_{k''}$ such that:

$$f(v^\sigma) = f(v)^\sigma \tag{5}$$

for all linear forms f on V rational over k. Indeed, if $\{e_i\}$ is a basis of V rational over k, the only map satisfying this condition is given explicitly by the formula

$$\left(\sum \xi_i \cdot e_i\right)^\sigma = \sum \xi_i^\sigma \cdot e_i \tag{6}$$

(note that the ξ_i are in k' and therefore the ξ_i^σ are defined and belong to k''). From formula (6) one deduces the following properties:

$$(v + v')^\sigma = v^\sigma + v'^\sigma \tag{7}$$

$$(\xi \cdot v)^\sigma = \xi^\sigma \cdot v^\sigma \ . \tag{8}$$

Moreover, the map $v \to v^\sigma$ is bijective, one has $k(v^\sigma) = k(v)^\sigma$ and in order that $v = v^\sigma$, it is necessary and sufficient that $\xi_i^\sigma = \xi_i$ for all i, that is σ to induce the identity on $k(v)$ (note that $k(v)$ is contained in k' for v rational over k').

If W is a subspace of V rational over k', we shall denote by W^σ the subspace of V *generated* by the vectors v^σ for v in $W \cap V_{k'}$; therefore W is a subspace of V rational over k''. Moreover, any subspace of V rational

over k' is uniquely written as $K \cdot T'$ where T' is a k'-subspace of $V_{k'}$, and a similar statement holds for k''; since $(K \cdot T')^\sigma = K \cdot T'^\sigma$ where T'^σ is the k''-subspace of $V_{k''}$ deduced from T' by $v \to v^\sigma$, one easily sees that $W \to W^\sigma$ is a bijection from the set of subspaces of V rational over k' onto the similar set for the field k''. We contend that the *relation* $W^\sigma = W$ *holds if and only if* σ *is the identity on the field* $k(W)$. For the proof of this statement, we keep the notations of the proof of Proposition 1. If σ induces the identity on $k(W)$, one gets $\xi_{ij}^\sigma = \xi_{ij}$ for all i and j, and therefore $v_i^\sigma = v_i$ for all i; since the v_i form a basis of W and the v_i^σ a basis of W^σ, one has indeed $W^\sigma = W$. Conversely, assuming $W^\sigma = W$, one gets $v_i^\sigma - v_i \in W$ for all i; since $v_i^\sigma - v_i$ is equal to $\sum_{j \in I''} (\xi_{ij}^\sigma - \xi_{ij}) \cdot e_j$ by (2) and since W does not contain any nonzero linear combination of the e_j, one gets $\xi_{ij}^\sigma = \xi_{ij}$ for all i and j, that is σ induces the identity on $k(W)$. The same argument shows that for any subspace W of V rational over k' one has $k(W^\sigma) = k(W)^\sigma$.

Let $V_1, \cdots, V_r$ and W be vector spaces, each one endowed with a k-structure. For any multilinear function f from $V_1 \times \cdots \times V_r$ to W rational over k', we contend that there exists a unique multilinear function f^σ from $V_1 \times \cdots \times V_r$ to W such that:

$$f^\sigma(v_1^\sigma, \cdots, v_r^\sigma) = f(v_1, \cdots, v_r)^\sigma \tag{9}$$

for v_i in V_i rational over k', and that any such f^σ is rational over k''. Indeed introduce for all vector spaces in question rational bases over k, as in § 4; the coordinates of f introduced by (4) are in k' since f is rational over k'; moreover, for vectors v_i in V_i with coordinates $\xi_\alpha^{(i)}$, the coordinates of $f(v_1, \cdots, v_r)$ are given by:

$$\eta_j = \sum_{\alpha_1, \cdots, \alpha_r} f^j_{\alpha_1, \cdots, \alpha_r} \xi^{(1)}_{\alpha_1} \cdots \xi^{(r)}_{\alpha_r} \tag{10}$$

and if the v_i are rational over k', the coordinates of v_i^σ are the $\{\xi_\alpha^{(i)}\}^\sigma$; from these formulas, it follows that the multilinear map f^σ with the coordinates $(f^j_{\alpha_1, \cdots, \alpha_r})^\sigma$ is the only one satisfying (9). Since the field $k(f)$ is generated over k by the $f^j_{\alpha_1, \cdots, \alpha_r}$, one sees that $f^\sigma = f$ if and only if σ induces the identity on $k(f)$, that $k(f^\sigma) = k(f)^\sigma$, and that for finite dimensional V_i the definition of f^σ agrees with the definition deduced from the k-structure defined in § 4 (b) on the space $\mathcal{L}$ of all multilinear maps. Finally, one gets the formulas:

$$(f + f')^\sigma = f^\sigma + f'^\sigma \tag{11}$$

$$(\xi \cdot f)^\sigma = \xi^\sigma \cdot f^\sigma \,. \tag{12}$$

From the axiomatic characterization of f^σ, one deduces the following formula for composable linear maps rational over k':

$$(f' \circ f)^\sigma = f'^\sigma \circ f^\sigma \ . \tag{13}$$

If τ is any k-isomorphism from k'' to a field k''', it follows from (6) that

$$(v^\sigma)^\tau = v^{\tau\sigma} \tag{14}$$

for any vector v in V rational over k'. This implies the relation $(W^\sigma)^\tau = W^{\tau\sigma}$ for any subspace W of V rational over k', and from (9) and (14) one infers $(f^\sigma)^\tau = f^{\tau\sigma}$ for any multilinear map f.

Finally, let G be a group of automorphisms of K, and assume the field of invariants of G in K to be k. Then v^σ is defined for any v in V and any σ in G; by one of the previous criteria, one has $v^\sigma = v$ if and only if σ induces the identity on $k(v)$; therefore v is invariant under G if and only if any element in G induces the identity on $k(v)$, that is $k(v) = k$; but this in turn means that v is rational over k. Therefore V_k *is the set of invariants of* G *in* V. Since criteria similar to those just used for vectors are valid for subspaces of V and multilinear maps, the same reasoning shows that a subspace of V, or a multilinear map from $V_1 \times \cdots \times V_r$ to W is rational over k if and only if it is invariant under G.

6. Definition of a G-K-module

Let G be a group operating on the field K and assume that k is the fixed field of G in K. More precisely, to any σ in G there is associated an automorphism $\xi \to \xi^\sigma$ of the field K, one has $(\xi^\sigma)^\tau = \xi^{\tau\sigma}$ for ξ in K and σ, τ in G, and k is the set of ξ in K such that $\xi^\sigma = \xi$ for all σ in G.

By a *G-K-module*, we mean a vector space V (over K) on which G operates so to satisfy the following rules:

$$(v + v')^\sigma = v^\sigma + v'^\sigma \tag{15}$$

$$(\xi \cdot v)^\sigma = \xi^\sigma \cdot v^\sigma \tag{16}$$

$$(v^\sigma)^\tau = v^{\tau\sigma} \tag{17}$$

for all v, v' in V, ξ in K and σ, τ in G. According to the results of the preceding paragraph, there is a unique action of G on a vector space V with a k-structure V_k which gives to V a structure of G-K-module, and for which V_k is the set of invariants of G in V. The next proposition is devoted to prove the converse.

PROPOSITION 2. *Let V be a G-K-module and E the set of invariants of G in V. Then E is a k-subspace of V and any subset of E linearly independent over k is the same over K. Assume now that E generates V. Then E is a k-structure on V and the maps $W \to W \cap E$ and $T \to K \cdot T$ define a one-to-one correspondence between the set of all subspaces W of*

V invariant under G and the set of all k-subspaces T of E.

It is obvious that E is a k-subspace of V.

Let $B \subset E$ be linearly independent over k. Among the subsets of B linearly independent over K, there exists by Zorn's lemma a maximal one, say B'. Assume $B' \neq B$; for v in B not in B', there exist some scalars ξ_b in K such that:

$$v = \sum_{b \in B'} \xi_b \cdot b \ . \tag{18}$$

Since v is in E, that is invariant under G, one infers from (18) the following identity:

$$\sum_{b \in B'} (\xi_b^\sigma - \xi_b) \cdot b = v^\sigma - v = 0 \qquad (\sigma \in G). \tag{19}$$

Since B' is linearly independent over K, (19) implies $\xi_b^\sigma = \xi_b$ for b in B' and σ in G, and therefore $\xi_b \in k$ for b in B' since k is the field of invariants of G in K. Since B is linearly independent over k by hypothesis, one gets therefore a contradiction from (18); therefore $B' = B$ and B is linearly independent over K.

Assume that E generates V. Then E is a k-structure by the last result and criterion (c) in § 1. We have seen in § 5 (cf., last statement) that the subspaces of V invariant under G are precisely the subspaces rational over k for the k-structure defined by E on V. The last statement in Proposition 2 follows therefore from the one-to-one correspondence between the subspaces of V rational over k and the k-subspaces of E (cf., § 3, (a)). q.e.d.

7. Criteria for Galois extensions

In the case of finite Galois extensions, we shall now prove that the process of definition of a k-structure explained in Proposition 2 works effectively.

PROPOSITION 3. *Let k' be a finite Galois extension of k with Galois group G. Any G-k'-module is then generated by the set of its invariants.*

Let V be a G-k'-module and let E be the set of invariants of G in V. To show that E generates V, it is enough to prove that any k'-linear form f on V which induces 0 on E is 0. For v in V and ξ in k', it is clear that $w = \sum_{\sigma \in G} (\xi \cdot v)^\sigma$ is in E, and this implies

$$\sum_{\sigma \in G} \xi^\sigma \cdot f(v^\sigma) = f(w) = 0 \qquad (\xi \in k'). \tag{20}$$

By Dedekind's theorem (cf., Bourbaki, Alg. Chap. V, § 7, no. 5, th. 3) this implies $f(v^\sigma) = 0$ for all σ in G, and in particular $f(v) = 0$. q.e.d.

We shall apply this result to give a criterion to "lower" the field of

definition of a vector space with some additional structure.

More precisely, let V be a vector space with a k-structure V_k and let k' be a finite Galois extension of k contained in K; let G be the Galois group of k' over k. If W is another vector space with a k-structure, let f be any isomorphism of W onto V rational over k'; then for any σ in G the linear map f^σ from W to V is defined and rational over k', and since f induces a k'-isomorphism from $W_{k'}$ to $V_{k'}$, so does f^σ; therefore f^σ is an isomorphism from W to V and $a(\sigma) = f^\sigma \circ f^{-1}$ is an automorphism of V rational over k'. Moreover, one gets

$$f^{\tau\sigma} \circ f^{-1} = (f^\sigma)^\tau \circ f^{-1} = (f^\sigma \circ f^{-1})^\tau \circ (f^\tau \circ f^{-1})$$

that is

$$a(\tau\sigma) = a(\sigma)^\tau \circ a(\tau) \qquad (\sigma, \tau \in G). \tag{21}$$

Conversely, suppose an automorphism $a(\sigma)$ of V rational over k' has been given for each σ in G, formula (21) being valid. For v in $V_{k'}$ and σ in G, let $v^{[\sigma]}$ be the vector $a(\sigma)^{-1}(v^\sigma)$ in $V_{k'}$. The formulas $(v + v')^{[\sigma]} = v^{[\sigma]} + v'^{[\sigma]}$ and $(\xi \cdot v)^{[\sigma]} = \xi^\sigma \cdot v^{[\sigma]}$ are immediate consequences of (15) and (16); moreover using (21) one gets the following:

$$\begin{aligned} v^{[\tau\sigma]} = a(\tau\sigma)^{-1}(v^{\tau\sigma}) &= a(\tau)^{-1}\{a(\sigma)^{-1}\}^\tau((v^\sigma)^\tau) \\ &= a(\tau)^{-1}\{a(\sigma)^{-1}(v^\sigma)\}^\tau = a(\tau)^{-1}(v^{[\sigma]})^\tau \\ &= (v^{[\sigma]})^{[\tau]} \end{aligned}$$

for σ, τ in G. Therefore, if G operates on $V_{k'}$ by the rule $v \to v^{[\sigma]}$, the axioms for a G-k'-module are satisfied. By Propositions 2 and 3 the set E of vectors $v \in V$ with $v^{[\sigma]} = v$ for all σ in G is a k-structure on the vector space $V_{k'}$ over k'; therefore, any k-basis of E is a k'-basis of $V_{k'}$ and therefore a basis of V; this implies that E is a k-structure on V. We shall denote by W the vector space V with the new k-structure defined by E; therefore, we shall denote E by W_k; we shall denote by f the identity map from W onto V. Since $V_{k'}$ is the k'-subspace of V generated by E, we have therefore $f(W_{k'}) = V_{k'}$ and the isomorphism f from W to V is rational over k'. Finally, the linear map f^σ from W to V is defined by $f^\sigma(v^{[\sigma]}) = f(v)^\sigma$ for v in V, that is

$$f^\sigma(v^{[\sigma]}) = v^\sigma = a(\sigma)v^{[\sigma]} = a(\sigma)f(v^{[\sigma]})$$

and one gets therefore:

$$a(\sigma) = f^\sigma \circ f^{-1} \qquad (\sigma \in G). \tag{22}$$

If W' is another space with a k'-structure and f' is any isomorphism from W' to V rational over k' such that $a(\sigma) = f'^\sigma \circ f'^{-1}$ for σ in G, one gets

$(f'^{-1} \circ f)^\sigma = f'^{-1} \circ f$ for all σ in G, that is $f'^{-1} \circ f$ is rational over k.

In other words, *if* $\{a(\sigma)\}_{\sigma \in G}$ *is a family of automorphisms of* V *rational over* k' *and satisfying* (21), *there exists a vector space* W *with a* k*-structure and an isomorphism* f *from* W *to* V *rational over* k' *such that* (22) *hold; if* W' *and* f' *satisfy the same relation, there exists a unique isomorphism* u *from* W *to* W' *rational over* k *such that* $f = f' \circ u$.

We shall now consider the case of an additional structure on V. To be specific, assume that to any vector space T there is associated a set $\mathcal{S}(T)$, to any isomorphism $f : T \to T'$ a bijective map $f^* : \mathcal{S}(T) \to \mathcal{S}(T')$ and that $(f' \circ f)^* = f'^* \circ f^*$ for two isomorphisms f and f'; assume furthermore that to any field L and to any L-structure on a vector space T be associated a subset $\mathcal{S}_L(T)$ of $\mathcal{S}(T)$ and that for any isomorphism $f : T \to T'$ rational over L, the image of $\mathcal{S}_L(T)$ under f^* be $\mathcal{S}_L(T')$. Finally assume that the group G operates on $\mathcal{S}_{k'}(T)$ for any vector space T with a k-structure, in such a way that $\mathcal{S}_k(T)$ be the set of invariants of G in $\mathcal{S}_{k'}(T)$ and that the map f^* for any isomorphism f rational over k be compatible with the operations of G. As an example, we can take for $\mathcal{S}(T)$ the set of bilinear associative laws of composition on T, the set $\mathcal{S}_L(T)$ being the subset of the laws rational over L, and the operations of G being defined as in § 5 for multilinear maps; finally f^* will be the obvious map given by "transport de structure".

Now, V and the $a(\sigma)$ being as before, suppose one has given on V an element s of $\mathcal{S}_{k'}(V)$ invariant under the maps $a(\sigma)^*$; stated otherwise, s *is a structure of "species"* $\mathcal{S}$ *on* V *rational over* k' *and the* $a(\sigma)$ *are automorphisms of* V *with this additional structure.* If $f : W \to V$ is an isomorphism rational over k' for which (22) holds, there exists a unique t in $\mathcal{S}_{k'}(W)$ such that $f^*(t) = s$; furthermore, since s is invariant under the $a(\sigma)^*$ and f^* is compatible with the actions of G, it is immediate that t is invariant under G, that is, belongs to $\mathcal{S}_k(W)$. In other words, *there exists a unique structure* t *on* W *of "species"* $\mathcal{S}$ *rational over* k *for which* f *is an isomorphism for the additional structures of "species"* $\mathcal{S}$. In the example explained above, one obtains therefore criteria to lower the field of definition of an algebra.

CHAPTER II

EXISTENCE OF INVARIANTS FOR GROUP VARIETIES

Notation. We follow closely Weil's well-known treatise [15] for the notation and terminology in algebraic geometry, except that by "morphism" we mean "everywhere regular rational map"; $\mathbf{K}$ is the universal domain and k is a subfield of $\mathbf{K}$. By subfield of $\mathbf{K}$ we mean a

subfield k' containing k such that $\mathbf{K}$ be of infinite transcendence degree over k'.

1. Principal homogeneous spaces

Let G be a group variety defined over k. We shall consider in the sequel a *principal homogeneous space* P for G defined over k; by this we mean a variety P together with a morphism α from $P \times G$ to P, both defined over k, the following axioms holding true:

(1) *Let p be in P and g, g' be in G; if e is the unit element in G, one has $p \cdot e = p$ and $p \cdot (g \cdot g') = (p \cdot g) \cdot g'$.*

(2) *The map $(p, g) \to (p, p \cdot g)$ from $P \times G$ to $P \times P$ is an isomorphism of varieties.*

(The value of α at the point (p, g) of $P \times G$ is written $p \cdot g$). (Cf., [17] for this definition.)

According to the previous axioms, given any two points p and p' in P, there exists a unique $g = \beta(p, p')$ in G such that $p \cdot g = p'$. The map β is a morphism from $P \times P$ to G, defined over k; furthermore the following transitivity rule holds:

$$\beta(p, p') \cdot \beta(p', p'') = \beta(p, p'') \ . \tag{1}$$

We denote by L the function field of the variety P; for any field k' of definition for P, the subfield of L consisting of the functions on P which are defined over k' will be called $L_{k'}$. Given any g in G, one defines an automorphism $f \to f_g$ of the field L by the rule:

$$f_g(p) = f(p \cdot g) \tag{2}$$

where p is any point in P such that $f(p \cdot g)$ be defined. Moreover, one has the formula $(f_g)_{g'} = f_{g' \cdot g}$ for any two elements g and g' in G and any function f in L. In other words, the group G operates on the field L; since G is transitive on P, the fixed field of G in L is the field $\mathbf{K}$ of constants.

2. Definition of a rational G-module

The principal homogeneous space P being fixed and L being the function field of P, let us consider a G-L-module V in the sense of § 6 in Chapter I. Assume first that V is generated as L-vector space by its invariant elements; we can therefore choose a basis $\{e_i\}$ for V over L, consisting of invariants. Let V_k be the *vector space over* L_k generated by the e_i.

We shall state the main properties of V_k.

(a) *The subset V_k of V is an L_k-structure for the L-vector space V.*

(b) *Let k' be any subfield of* **K**, *and let $V_{k'}$ be the vector space over $L_{k'}$ generated by V_k. Given any g in G rational over k' and any vector v in $V_{k'}$, the vector v_g is in $V_{k'}$.*

(c) *Let σ be any k-automorphism of the field* **K**; *let σ still denote the unique automorphism of L over L_k which extends σ. Given any g in G and any vector v in V, one gets*:

$$(3) \qquad (v_g)^\sigma = (v^\sigma)_{g^\sigma}$$

where the map $v \to v^\sigma$ in V is defined by means of the L_k-structure V_k for the L-vector space V (cf., § 5 in Chapter I).

Property (a) is obvious according to the definitions.

For any f in $L_{k'}$ and any g in G rational over k', it is obvious that f_g is in $L_{k'}$. Moreover, $V_{k'}$ consists of the vectors $\sum_i f_i \cdot e_i$ with f_i in $L_{k'}$ for any i; since the e_i are invariant under G, one gets $g \cdot v = \sum_i (f_i)_g \cdot e_i$ for $v = \sum_i f_i \cdot e_i$; this implies property (b).

Since the map $(p, g) \to p \cdot g$ from $P \times G$ into P is a morphism defined over k, one gets the formula:

$$(4) \qquad (f_g)^\sigma = (f^\sigma)_{g^\sigma} \qquad\qquad f \in L,\ g \in G$$

where σ is any k-automorphism of **K**. Moreover, from the definitions given in § 5 of Chapter I, one gets:

$$(5) \qquad \left(\sum_i f_i \cdot e_i\right)^\sigma = \sum_i (f_i)^\sigma \cdot e_i \ .$$

Property (c) follows immediately from (4) and (5).

The previous results suggest the following definition.

A *rational G-module* (*defined over k*) is a G-L-module together with a subset V_k of V for which properties (a), (b), and (c) hold true. Strictly speaking, we should have to mention the principal homogeneous space P in the notation, but we shall omit it consistently in the sequel.

With this terminology, we have proved that, given any G-L-module V generated by the set of its invariants, and given any basis of V consisting of invariants, the L_k-subspace V_k of V generated by this basis defines on V a structure of rational G-module (defined over k). We shall prove later that any rational G-module defined over k can be obtained in this way (cf., § 5).

3. Examples: derivations[1]

We shall give a first example of a rational G-module.

Let $\mathfrak{g}$ be the set of **K**-derivations of the field L. On $\mathfrak{g}$ we define a

[1] The results contained in this paragraph shall not be used in the sequel of this paper. Their purpose is mainly expository.

structure of L-vector space by means of the definitions:

$$(6) \qquad (D + D')(f) = D(f) + D'(f)\ , \qquad (h \cdot D)(f) = h \cdot D(f)\ .$$

Moreover, let the group G operate on $\mathfrak{g}$ by the rule:

$$(7) \qquad (D_g)(f) = D(f_{g^{-1}})_g\ .$$

The defining properties of a G-L-module are easily checked and the verification will be omitted (cf., formulas (15) to (17) in Chapter I, § 6).

If k' is any field of definition for P, let $\mathfrak{g}_{k'}$ be the set of all derivations D in $\mathfrak{g}$ such that $D(L_{k'})$ is contained in $L_{k'}$. We contend that $\mathfrak{g}$ *endowed with* $\mathfrak{g}_k$ *is a rational* G*-module defined over* k*, and that* $\mathfrak{g}_{k'} = L_{k'} \cdot \mathfrak{g}$ *for any subfield* k' *of* $\mathbf{K}$.

The field L_k is a regular extension of k, and in particular is separably generated over k. There exist therefore n elements $x_1, \cdots, x_n$ in L_k algebraically independent over k such that L_k is separably algebraic over $k(x_1, \cdots, x_n)$. Since L is generated by L_k and $\mathbf{K}$ which are linearly disjoint over k, the field L is separably algebraic over $\mathbf{K}(x_1, \cdots, x_n)$ and the x_i are algebraically independent over $\mathbf{K}$. By well-known results about derivations of fields, $\mathfrak{g}$ admits a basis $\{D_1, \cdots, D_n\}$ over L such that $D_i(x_j) = \delta_{ij}$ for $1 \leqq i, j \leqq n$ (Kronecker symbol). This definition implies the formula $D = \sum_{1 \leqq i \leqq n} D(x_i) \cdot D_i$ for any D in $\mathfrak{g}$.

Let k' be any subfield of $\mathbf{K}$. If D is in $\mathfrak{g}_{k'}$, the previous formula and the relation $D(x_i) \in L_{k'}$ arising from $D(L_{k'}) \subset L_{k'}$ show that D has coordinates in $L_{k'}$ with respect to the basis $\{D_1, \cdots, D_n\}$ of $\mathfrak{g}$. Conversely, for $D = \sum_i f_i \cdot D_i$ with some f_i in $L_{k'}$, one gets $D(x_i) = f_i$ for all i; this implies that D maps $k'(x_1, \cdots, x_n)$ in $L_{k'}$. Since $L_{k'}$ is generated by L_k and k', it is a separably algebraic extension of $k'(x_1, \cdots, x_n)$, and by the lately proved result, D maps $L_{k'}$ into itself (cf., [4, Chap. V, § 9, prop. 5, cor. 1]). Thus we have proved that $\mathfrak{g}_{k'}$ consists of the linear combinations with respect to $L_{k'}$ of the basic elements $D_1, \cdots, D_n$ of $\mathfrak{g}$. This means that $\mathfrak{g}_k$ is an L_k-structure on the L-vector space $\mathfrak{g}$ and that $\mathfrak{g}_{k'} = L_{k'} \cdot \mathfrak{g}_k$.

Let D be in $\mathfrak{g}_{k'}$ and g in G be rational over k'. For any f in $L_{k'}$, the function $f_{g^{-1}}$ is in $L_{k'}$ since g^{-1} is rational over k'; since D is in $\mathfrak{g}_{k'}$, one gets $D(f_{g^{-1}}) \in L_{k'}$, and finally by the definition (7), one gets $D_g(f) \in L_{k'}$ for any f in $L_{k'}$. By the previous criterion, D_g is in $\mathfrak{g}_{k'}$. This checks property (b) in § 2.

Let σ be any k-automorphism of $\mathbf{K}$ and extend σ to an L_k-automorphism of L. If the map $D \to D^\sigma$ in $\mathfrak{g}$ is defined by means of the L_k-structure $\mathfrak{g}_k$, one gets by definition $D^\sigma = \sum f_i^\sigma \cdot D_i$ for $D = \sum f_i \cdot D_i$; for f in L_k, one gets $D(f)^\sigma = \sum f_i^\sigma \cdot D_i(f)^\sigma = \sum f_i^\sigma \cdot D_i(f) = D^\sigma(f)$ since $D_i(f)$ is in L_k

and σ is the identity on L_k. Moreover, the map $f \to D(f)^\sigma - D^\sigma(f^\sigma)$ from L into itself is a derivation annihilating $\mathbf{K}$; by the last result, this derivation annihilates L_k and since L is generated by $\mathbf{K}$ and L_k, it is identically zero, so that one gets:

$$D(f)^\sigma = D^\sigma(f^\sigma) \qquad D \in \mathfrak{g}, f \in L. \tag{8}$$

This last formula defines completely the derivation D^σ; using this characterization of D^σ, the formula $(D_g)^\sigma = (D^\sigma)_{g^\sigma}$ follows immediately.

Our contention is therefore completely proved. Since $\mathfrak{g}$ is a rational G-module defined over k, the theorem to be proved later in § 5 shall imply the well-known result that $\mathfrak{g}$ admits a basis consisting of G-invariant derivations. In fact, it can be proved that the tangent bundle to P admits n linearly independent regular cross-sections rational over k and G-invariant, where n is the dimension of P; furthermore $\mathfrak{g}$ is the set of all rational cross-sections of this bundle.

4. Examples: isogenies

We give now another example of a rational G-module defined over k. This example will be used in Chapter III, § 4.

Let Q be any transformation space for G defined over k; this means as customary that Q is a variety defined over k and there is given a morphism $(q, g) \to q \cdot g$ defined over k from $Q \times G$ to Q with property (1) in § 1. Furthermore, *let λ be a surjective morphism from P to Q such that:*

$$\lambda(p \cdot g) = \lambda(p) \cdot g \qquad p \in P, g \in G, \tag{9}$$

and assume that P and Q have the same dimension.

An important particular case is the following: let P be G operating on itself by right translations; let H be another group variety defined over k and let λ be any rational group homomorphism from G *onto* H defined over k; we let Q be H with G operating on H by the rule $h \cdot g = h \cdot \lambda(g)$; finally assume G and H to have the same dimension, that is λ to be an isogeny.

Let M be the function field on Q, and for any field k' of definition for Q let $M_{k'}$ be the subfield of M consisting of the functions rational over k'. Since λ is surjective, the composite rational function $f^\lambda = f \circ \lambda$ is defined for any f in M; the map $f \to f^\lambda$ is therefore an isomorphism of M with some subfield M^λ of L. Since P and Q have the same dimension, this isomorphism of M into L defines on L a structure of finite dimensional M-vector space.

We shall denote by $\mathcal{E}$ the set of all endomorphisms of L considered as

an M-vector space as before. On $\mathcal{E}$ one defines a structure of L-vector space by the rules:

$$(t + t')(f) = t(f) + t'(f)\ , \qquad (h \cdot t)(f) = h \cdot t(f) \tag{10}$$

and one lets the group G operate on $\mathcal{E}$ by the formula:

$$(t_g)(f) = t(f_{g^{-1}})_g\ . \tag{11}$$

These definitions are completely similar to those of § 3, and for the same reason they give rise to a structure of G-L-module on $\mathcal{E}$.

For any field k' containing k and contained in $\mathbf{K}$, the set $\mathcal{E}_{k'}$ will consist of all t in $\mathcal{E}$ such that $t(L_{k'})$ be contained in $L_{k'}$. We contend *that $\mathcal{E}$ endowed with $\mathcal{E}_k$ is a rational G-module defined over k and that $\mathcal{E}_{k'} = L_{k'} \cdot \mathcal{E}_k$ for any subfield k' of* $\mathbf{K}$.

Since λ is defined over k, the field M^λ is the compositum of M_k^λ and $\mathbf{K}$ which are linearly disjoint over k; since L is the compositum of L_k and $\mathbf{K}$ linearly disjoint over k and M_k^λ is contained in L_k it follows immediately that L is the compositum of L_k and M^λ which are linearly disjoint over M_k^λ (cf., [4, Chap. V, § 2, prop. 7]); moreover, for any subfield k' of $\mathbf{K}$, the field $L_{k'}$ is the compositum of L_k and $M_{k'}^\lambda$. Therefore if $\{x_1, \cdots, x_d\}$ is any basis of L_k over M_k, this set is also a basis for $L_{k'}$ over $M_{k'}$ and of L over M. It follows that the map $\varphi : t \to (t(x_1), \cdots, t(x_d))$ is an isomorphism of L-vector space of $\mathcal{E}$ onto L^d, and that this isomorphism maps $\mathcal{E}_k$ onto $(L_k)^d$ and $\mathcal{E}_{k'}$ onto $(L_{k'})^d$. This proves that $\mathcal{E}_k$ is an L_k-structure on $\mathcal{E}$ and that $\mathcal{E}_{k'} = L_{k'} \cdot \mathcal{E}_k$.

$$\begin{array}{ccccc}
L_k & \longrightarrow & L_{k'} & \longrightarrow & L \\
\uparrow & & \uparrow & & \uparrow \\
M_k^\lambda & \longrightarrow & M_{k'}^\lambda & \longrightarrow & M^\lambda \\
\uparrow & & \uparrow & & \uparrow \\
k & \longrightarrow & k' & \longrightarrow & \mathbf{K}
\end{array}$$

Let still k' be any subfield of $\mathbf{K}$. For t in $\mathcal{E}_{k'}$ and g in G rational over k', it is obvious from the definition (11) that t_g maps $L_{k'}$ into itself, that is $t_g \in \mathcal{E}_{k'}$.

Finally, let σ be any k-automorphism of $\mathbf{K}$, and extend σ to an L_k-automorphism of L. Let the map $t \to t^\sigma$ in $\mathcal{E}$ be defined by means of the L_k-structure $\mathcal{E}_k$ on $\mathcal{E}$; since φ is an isomorphism of $\mathcal{E}$ onto L^d which maps $\mathcal{E}_k$ onto $(L_k)^d$, the characteristic property of t^σ is by $t^\sigma(x_i) = t(x_i)^\sigma$ for $1 \leqq i \leqq d$, and this in turn implies immediately:

(12) $$t(f)^\sigma = t^\sigma(f^\sigma) \qquad t \in \mathcal{E}, f \in L.$$

Checking $(t_g)^\sigma = (t^\sigma)_{g^\sigma}$ is then obvious and may be left to the reader.

Our contention is therefore completely proved. By means of the theorem in § 5, this implies that $\mathcal{E}$ admits a basis consisting of d elements of $\mathcal{E}_k$ invariant under G. By the way, more precise results using vector bundles over Q could be proved, since $\mathcal{E}$ is the set of rational cross-sections of a certain vector bundle over Q. I hope to return later to this question.

5. Existence of invariants

We give now a proof of the structure theorem for rational G-modules.

THEOREM. *Let V be a rational G-module defined over k. Let I be the set of all invariants of G in V, and put $I_{k'} = I \cap V_{k'}$ for any subfield k' of* **K**. *Then I_k is a k-structure on the L-vector space V and for any subfield k' of* **K** *one gets*

(13) $$I_{k'} = k' \cdot I_k , \qquad V_{k'} = L_{k'} \cdot I_k .$$

The proof is rather long and will be divided into several parts.

(A) *Let k' be a subfield of* **K**; *for v a vector in $V_{k'}$ and g in G generic over k', the relation $v_g = v$ insures that v is invariant under G.*

For, h being any point in G generic over k', there exists an automorphism σ of **K** over k' such that $g^\sigma = h$; let σ denote the unique automorphism of L over $L_{k'}$ extending this automorphism of **K**. From $v_g = v$, one infers $(v^\sigma)_{g^\sigma} = v^\sigma$ by (3), that is $v_h = v$ since $v^\sigma = v$ is in $V_{k'}$. Therefore v is fixed by any point in G generic over k'; but any point in G is the product of two such generic points, according to a well-known elementary result. This proves our contention.

(B) *As a vector space over* **K**, *the set I of invariants is generated by I_k.*

Let A be the subring of L generated by **K** and L_k, and let W be the A-module generated by V_k in V, that is $W = A \cdot V_k$. As a field, L is generated by **K** and L_k and therefore L is the quotient field of A; since $V = L \cdot V_k$, any vector in V can be written as $a^{-1} \cdot w$ with w in W for some nonzero element a of A.

Let u be in I and let $\mathfrak{a}$ be the set of all a in A such that $a \cdot u \in W$. Obviously $\mathfrak{a}$ is an ideal in the ring A. By the previous alinea, there is a nonzero element in $\mathfrak{a}$. Let $\bar{k}$ be the algebraic closure of k in **K** and let $\bar{G}$ be the group of all points in G rational over $\bar{k}$. Since $\bar{k}$ is algebraic over k, the *field* $L_{\bar{k}}$ is the *ring* generated by $\bar{k}$ and L_k and therefore $L_{\bar{k}}$ is contained in A. Finally, one gets $A = \mathbf{K} \cdot L_{\bar{k}}$; since $L_{\bar{k}}$ as a whole is stable under $\bar{G}$, the same is true for A which is in a natural way a $\bar{G}$-$L_{\bar{k}}$-module. Since the set **K** of invariants of $\bar{G}$ in A is large enough, any

vector space over $L_{\bar{k}}$ in A stable under $\bar{G}$ contains a nonzero element in $\mathbf{K}$ unless it be reduced to zero (cf., Prop. 2, Chap. I, § 6).

Moreover $W = A \cdot V_k = \mathbf{K} \cdot L_{\bar{k}} \cdot V_k = \mathbf{K} \cdot V_{\bar{k}}$ is stable under $\bar{G}$ by the defining property (b) for a rational G-module. This implies the stability of $\mathfrak{a}$ under $\bar{G}$; therefore by the previous result the ideal $\mathfrak{a}$ in A is 0 or contains a nonzero element in $\mathbf{K}$; since $\mathfrak{a}$ is not 0 and $\mathbf{K}$ is a field one gets $1 \in \mathfrak{a}$, that is $u \in W$.

Since u is in W, one finds some c_α in $\mathbf{K}$ linearly independent over k and some u_α in V_k such that:

$$u = \sum\nolimits_\alpha c_\alpha \cdot u_\alpha \ . \tag{14}$$

For g in G generic over k, one gets $u_g = u$ and therefore:

$$\sum\nolimits_\alpha c_\alpha \cdot \{(u_\alpha)_g - u_\alpha\} = 0 \tag{15}$$

from (14). Let $f : V_{k(g)} \to L_{k(g)}$ be linear over $L_{k(g)}$; since $V_{k(g)}$ is an $L_{k(g)}$-structure on the L-vector space V, there is a unique L-linear form f' on V extending f. Applying f' to (15) one deduces the identity:

$$\sum\nolimits_\alpha c_\alpha \cdot f((u_\alpha)_g - u_\alpha) = 0 \tag{16}$$

since $(u_\alpha)_g - u_\alpha$ is in $V_{k(g)}$ for each α.

The fields $\mathbf{K}$ and $L_{k(g)}$ are linearly disjoint over $k = k(g) \cap \mathbf{K}$ since g is generic over k. Therefore the linear independence of the c_α over k implies that the coefficient of each c_α in (16) is 0. Since f is arbitrary, one gets $(u_\alpha)_g = u_\alpha$ for each α. By property (A), one infers that each u_α is invariant under G, that is $u_\alpha \in I \cap V_k = I_k$.

Our contention is proved.

(C) *As a vector space over L, the set V is generated by I.*

We choose a point (p, g, h) in $P \times G \times G$ generic over k.

The point $p \cdot g$ in P is generic over $k(g, h)$ *and* over $k(p, h)$. Therefore there exists a unique isomorphism σ from $L_{k(g,h)}$ onto $L_{k(p,h)}$ such that:

$$f^\sigma(p \cdot g) = f(p \cdot g) \qquad (f \in L_{k(g,h)}). \tag{17}$$

For f in $L_{k(h)}$, that is rational over $L_{k(g,h)}$ *and* $L_{k(p,h)}$, one gets $f^\sigma = f$ by (17); in other words, σ is the identity on $L_{k(h)}$ and in particular on L_k.

Using Chap. I, § 5, one defines a bijective mapping $v \to v^\sigma$ from $V_{k(g,h)}$ onto $V_{k(p,h)}$. If $\{v_i\}$ is a basis for V_k over L_k, this set is a basis for $V_{k(g,h)}$ over $L_{k(g,h)}$, and the set $\{g^{-1} \cdot v_i\}$ is another basis[2] for the same space (this follows immediately from the defining properties of a rational G-module). It follows that the set $\{(g^{-1} \cdot v_i)^\sigma\}$ is a basis for $V_{k(p,h)}$ over $L_{k(p,h)}$ and finally for V over L.

[2] From now on, we shall write $g \cdot v$ instead of v_g for typographical reasons.

To prove our contention, it is enough to prove that $w = (g^{-1}\cdot v)^{\sigma}$ is in I for any v in V_k; since w is in $V_{k(p)}$ and h in G is generic over $k(p)$, it is even enough to prove the formula $h\cdot w = w$.

Let us introduce a convenient notation. If X and Y are two algebraic varieties defined over k and F is any function on $X \times Y$ rational over k, the function $F(x, \cdot\ )$ on Y is defined for x in X generic over k by the equality $F(x, \cdot\ )(y) = F(x, y)$ for y in Y generic over $k(x)$; this function $F(x, \cdot\ )$ is rational over $k(x)$ and any function on Y rational over $k(x)$ can be uniquely written in this way for some F on $X \times Y$ rational over k.

In particular, for v in V_k, one gets $g^{-1}\cdot v \in V_{k(g)}$ and there exists an identity:

$$g^{-1}\cdot v = \sum_{\alpha} F_{\alpha}(g, \cdot\ )\cdot v_{\alpha} \tag{18}$$

with some v_{α} in V_k and some functions F_{α} on $G \times P$ rational over k. By definition of a principal homogeneous space, the point $(p, p\cdot g)$ in $P \times P$ is generic over k, and therefore, one defines some functions F'_{α} on $P \times P$ rational over k by the formula:

$$F'_{\alpha}(p, p\cdot g) = F_{\alpha}(g, p\cdot g)\ . \tag{19}$$

Using the definition of σ this identity amounts to the following:

$$F'_{\alpha}(p, \cdot\ ) = F_{\alpha}(g, \cdot\ )^{\sigma} \tag{20}$$

Since gh in G is generic over k there exists a k-automorphism ι of $\mathbf{K}$ such that $gh = g^{\iota}$. Since V_k contains both v and the v_{α}, one gets $v^{\iota} = v$ and $v_{\alpha}^{\iota} = v_{\alpha}$ for each α. By (3) and (18) one gets:

$$\begin{aligned}(gh)^{-1}\cdot v = (g^{-1}\cdot v)^{\iota} &= \sum_{\alpha} F_{\alpha}(g, \cdot\ )^{\iota}\cdot v_{\alpha} = \sum_{\alpha} F_{\alpha}(g^{\iota}, \cdot\ )\cdot v_{\alpha} \\ &= \sum_{\alpha} F_{\alpha}(gh, \cdot\ )\cdot v_{\alpha}\ .\end{aligned} \tag{21}$$

Since V is a G-L-module, one gets therefore:

$$g^{-1}\cdot v = h\cdot(gh)^{-1}\cdot v = \sum_{\alpha} F_{\alpha}(gh, \cdot\ )_h\cdot(h\cdot v_{\alpha})$$

and finally

$$w = (g^{-1}\cdot v)^{\sigma} = \sum_{\alpha}\{F_{\alpha}(gh, \cdot\ )_h\}^{\sigma}\cdot(h\cdot v_{\alpha})$$

(note that $h\cdot v_{\alpha}$ is in $V_{k(h)}$ and σ is the identity on $L_{k(h)}$).

For each α, the function $u_{\alpha} = \{F_{\alpha}(gh, \cdot\ )_h\}^{\sigma}$ on P is rational over $k(p, h)$; moreover the point $p\cdot g$ in P is generic over $k(p, h)$. The following computation insures therefore that u_{α} is equal to the function $F'_{\alpha}(p, \cdot\ )_h$ on P rational over $k(p, h)$.

$$\begin{aligned}u_{\alpha}(p\cdot g) = F_{\alpha}(gh, \cdot\ )_h(p\cdot g) &= F_{\alpha}(gh, \cdot\ )(p\cdot gh) = F_{\alpha}(gh, p\cdot gh) \\ &= F'_{\alpha}(p, p\cdot gh) = F'_{\alpha}(p, \cdot\ )(p\cdot gh) = F'_{\alpha}(p, \cdot\ )_h(p\cdot g)\ .\end{aligned}$$

This implies

$$w = \sum_\alpha u_\alpha \cdot (h \cdot v_\alpha) = h \cdot \left(\sum_\alpha F'_\alpha(p, \cdot\ ) \cdot v_\alpha\right) = h \cdot w\ .$$

This proves our contention (C).

(D) *Conclusion.*

Using (B) and (C) proves that V is generated as L-vector space by I_k. Let us choose a basis $\{v_i\}$ for V over L consisting of elements in I_k, and let k' be any subfield of $\mathbf{K}$. Since the v_i belong to $V_{k'}$ and $V_{k'}$ is an $L_{k'}$-structure on V, the set $V_{k'}$ consists of the vectors with components in $L_{k'}$ (with respect to the basis $\{v_i\}$). Since the vectors v_i are invariant under G, the set I consists of the vectors with components in $\mathbf{K}$. Finally $I_{k'} = V_{k'} \cap I$ consists of the vectors with components in $L_{k'} \cap \mathbf{K} = k'$. Our theorem follows immediately. q.e.d.

CHAPTER III

DIVISORS ON ABELIAN VARIETIES

1. Operations on divisors

Let X be a nonsingular variety. The notation $D \sim 0$ (resp. $D \approx 0$) means that the divisor D on X is linearly (resp. algebraically) equivalent to zero; therefore $D \sim 0$ implies $D \approx 0$. A *divisor class* is a class with respect to linear equivalence; by definition such a class is rational over a field k of definition for X if some divisor in it is rational over k; the class of a divisor D is denoted by $\mathrm{Cl}(D)$. Suppose X is complete; then if a divisor D rational over k is linearly equivalent to 0, there exists a function f on X rational over k such that $D = (f)$; if two functions f' and f'' have the same divisor, their ratio is a nonzero constant.

Let Y be another nonsingular variety and f a morphism from X to Y. For any divisor D on Y whose support does not contain $f(X)$, the divisor $f^{-1}(D)$ on Y is defined by the formula:

$$f^{-1}(D) = \mathrm{pr}_X \Gamma_f \cdot (X \times D) \tag{1}$$

where Γ_f is the graph of f; therefore $f^{-1}(D)$ is defined for any divisor D on Y if f is surjective. The relation $D \sim 0$ implies $f^{-1}(D) \sim 0$; more precisely, if $D = (u)$ where u is a nonzero function on Y, the divisor $f^{-1}(D)$ is defined if and only if the composite function $u \circ f$ is defined and nonzero and one has the formula:

$$f^{-1}(D) = (u \circ f) \qquad \text{for } D = (u). \tag{2}$$

Let $\mathfrak{c}$ be a divisor class on Y; since Y is nonsingular there exists a divisor D in $\mathfrak{c}$ whose support does not contain a given point in $f(X)$; then

$f^{-1}(D)$ is defined and by the preceding result the class of $f^{-1}(D)$ depends only on $\mathfrak{c}$; this class we shall denote by $f^{-1}(\mathfrak{c})$. The mapping $\mathfrak{c} \to f^{-1}(\mathfrak{c})$ from the class group of Y to the class group of X is a group homomorphism.

Let k be a field of definition for X, Y and f. When $f^{-1}(D)$ is defined for a divisor D on Y rational over k, then it is rational over k on X. For a class $\mathfrak{c}$ rational over k on Y, there exists a divisor D in $\mathfrak{c}$ rational over k such that $f^{-1}(D)$ be defined; therefore the class $f^{-1}(\mathfrak{c})$ on X is rational over k.

Finally, let f' be a morphism from Y to a nonsingular variety Z. For a divisor D and a class $\mathfrak{c}$ on Z, one has the transitivity formulas:

$$f^{-1}(f'^{-1}(D)) = (f' \circ f)^{-1}(D) \tag{3}$$

$$f^{-1}(f'^{-1}(\mathfrak{c})) = (f' \circ f)^{-1}(\mathfrak{c}) \tag{4}$$

whenever the divisor to the left in (3) is defined.

2. Divisors on an abelian variety

Let A be an abelian variety. By δ_A we mean the identity endomorphism of A. For a in A, the translation $T_a : x \to x + a$ is an automorphism of the variety underlying A; according to a familiar notation, we use a subscript "a" to denote the transform by T_a of any object attached to the variety A. For instance, one has the formulas:

$$f_a(x) = f(x - a) \tag{5}$$

$$D_a = T_{-a}^{-1}(D) \tag{6}$$

$$\mathfrak{c}_a = T_{-a}^{-1}(\mathfrak{c}) \tag{7}$$

for a function f, a divisor D and a divisor class $\mathfrak{c}$ on A, whenever $f(x - a)$ is defined for x in A.

If $\mathfrak{c}$ is a class on A, the map $\psi_{\mathfrak{c}} : a \to \mathfrak{c}_a - \mathfrak{c}$ is a group homomorphism from A to the class group on A (cf., L-III$_3$, cor. 4 to th. 4); we shall write $\mathfrak{c} \equiv 0$ to mean than $\psi_{\mathfrak{c}}$ is 0, that is $\mathfrak{c}$ invariant by translation; if D is a divisor, we write $D \equiv 0$ when $\mathrm{Cl}(D) \equiv 0$, that is $D_a \sim D$ for all a in A. If λ is a homomorphism from A to an abelian variety B, one checks easily the formula:

$$\lambda \circ T_a = T_{\lambda \cdot a} \circ \lambda \qquad (a \in A) \tag{8}$$

where the notation T refers to A in the left hand side and to B in the right hand side. By (4) and (7) one deduces from this formula the rule:

$$\lambda^{-1}(\mathfrak{c})_a = \lambda^{-1}(\mathfrak{c}_{\lambda \cdot a}) \tag{9}$$

and therefore:

$$\psi_{\lambda^{-1}(\mathfrak{c})}(a) = \lambda^{-1}(\psi_{\mathfrak{c}}(\lambda \cdot a)) \tag{10}$$

for a in A and $\mathfrak{c}$ a class on A.

We shall now prove some properties of the equivalence $\equiv$ (cf., L-IV$_1$).

PROPOSITION 1. *Let $\mathfrak{c}$ be a divisor class on an abelian variety A and let S, p and p' be the morphisms from $A \times A$ to A defined by $S(a, b) = a + b$, $p(a, b) = a$ and $p'(a, b) = b$ respectively. Then the relation $\mathfrak{c} \equiv 0$ is equivalent to*

$$S^{-1}(\mathfrak{c}) = p^{-1}(\mathfrak{c}) + p'^{-1}(\mathfrak{c}) \; . \tag{11}$$

Let $\mathfrak{d}$ be the class $S^{-1}(\mathfrak{c}) - p^{-1}(\mathfrak{c}) - p'^{-1}(\mathfrak{c})$ on $A \times A$. For a in A let q_a be the isomorphism of A onto the subvariety $a \times A$ of $A \times A$ defined by $q_a(b) = (a, b)$; one has $S \circ q_a = T_a$, the morphism $p \circ q_a$ is constant and $p' \circ q_a$ is the identity map of A; by (4) and (7) one gets therefore:

$$q_a^{-1}(\mathfrak{d}) = \mathfrak{c}_{-a} - \mathfrak{c} \qquad (a \in A). \tag{12}$$

In the same way, one proves the relation:

$$q_a'^{-1}(\mathfrak{d}) = \mathfrak{c}_{-a} - \mathfrak{c} \tag{13}$$

where q'_a is defined by $q'_a(b) = (b, a)$. Therefore, $\mathfrak{c} \equiv 0$ means that $\mathfrak{d}$ induces the zero class on $A \times a$ and $a \times A$ for any a in A. The proposition will be proved if we show that the last condition implies $\mathfrak{d} = 0$.

Let E be a divisor in $\mathfrak{d}$ and k be a field of definition for A and E; since the support of E is k-closed, it does not contain $a \times A$ for a generic over k, and therefore the divisor $q_a^{-1}(E)$ is defined on A and rational over $k(a)$; this divisor is linearly equivalent to 0 by hypothesis, and since A is complete, there exists a function f on A rational over $k(a)$ such that $q_a^{-1}(E) = (f)$. For b generic in A over $k(a)$ one has $f(b) \in k(a, b)$ and there exists a function g on $A \times A$ rational over k such that $f(b) = g(a, b)$, that is $f = g \circ q_a$. This relation implies that the divisor induced on $a \times A$ by $E - (g)$ is 0; since the latter divisor is rational over k and a is generic over k, there exists a divisor D on A rational over k such that $E - (g) = D \times A$. This implies $\mathfrak{d} = p^{-1}(\mathfrak{c}')$ where $\mathfrak{c}'$ is the class of D; but $\mathfrak{c}' = q_a'^{-1}(p^{-1}(\mathfrak{c}')) = q_a'^{-1}(\mathfrak{d}) = 0$ and therefore $\mathfrak{d} = 0$. q.e.d.

COROLLARY 1. *For two abelian varieties A and B and two homomorphisms λ and μ from B to A, the following holds:*

$$(\lambda + \mu)^{-1}(\mathfrak{c}) = \lambda^{-1}(\mathfrak{c}) + \mu^{-1}(\mathfrak{c}) \tag{14}$$

for any class $\mathfrak{c}$ on A such that $\mathfrak{c} \equiv 0$.

Let π be the homomorphism from B to $A \times A$ defined by $\pi(b) = (\lambda \cdot b, \mu \cdot b)$ for b in B; since $p \circ \pi = \lambda$, $p' \circ \pi = \mu$ and $S \circ \pi = \lambda + \mu$, formula (14) results from (11) by applying the operation π^{-1}.

COROLLARY 2. *Let A be an abelian variety and $\mathfrak{c}$ a divisor class on A. Then for any integer m, one has:*

$$(m\delta_A)^{-1}(\mathfrak{c}) \equiv m^2\cdot\mathfrak{c}\ . \tag{15}$$

For any class $\mathfrak{d}$ on A such that $\mathfrak{d} \equiv 0$, one gets $(m\delta_A)^{-1}(\mathfrak{d}) = m\cdot\mathfrak{d}$ by (14). We know that $\psi_{\mathfrak{c}}$ is a group homomorphism; therefore one gets $\psi_{\mathfrak{c}}(a+b) = \psi_{\mathfrak{c}}(a) + \psi_{\mathfrak{c}}(b)$ that is

$$\mathfrak{c}_{a+b} - \mathfrak{c}_a - \mathfrak{c}_b + \mathfrak{c} = 0$$

or $(\mathfrak{c}_a - \mathfrak{c})_b = \mathfrak{c}_a - \mathfrak{c}$. Finally, one gets $\psi_{\mathfrak{c}}(a) \equiv 0$ for any a in A. If one uses formula (10) with $\lambda = m\cdot\delta$ one gets therefore

$$\psi_{(m\cdot\delta_A)^{-1}(\mathfrak{c})}(a) = (m\cdot\delta_A)^{-1}(\psi_{\mathfrak{c}}(m\cdot a)) = m\cdot\psi_{\mathfrak{c}}(m\cdot a) = m^2\cdot\psi_{\mathfrak{c}}(a) = \psi_{m^2\cdot\mathfrak{c}}(a)$$

and (15) is a consequence of this relation and the definition of the congruence $\equiv$. q.e.d.

By (10) the relation $\mathfrak{c} \equiv 0$ implies $\lambda^{-1}(\mathfrak{c}) \equiv 0$ for any homomorphism $\lambda : A \to B$ and any divisor class $\mathfrak{c}$ on B. Conversely, one has the following result:

PROPOSITION 2. *Let A and B be abelian varieties and λ a surjective homomorphism from A to B. Then, for any class $\mathfrak{c}$ on B, the relation $\lambda^{-1}(\mathfrak{c}) \equiv 0$ implies $\mathfrak{c} \equiv 0$.*

By Poincaré's theorem of complete reducibility (cf., L-II$_1$, th. 6) there is a homomorphism $\mu : B \to A$ and an integer $m \neq 0$ such that $\lambda \circ \mu = m\cdot\delta_B$. Then $\lambda^{-1}(\mathfrak{c}) \equiv 0$ implies $\mu^{-1}(\lambda^{-1}(\mathfrak{c})) \equiv 0$, that is $(m\cdot\delta_B)^{-1}(\mathfrak{c}) \equiv 0$, or finally $m^2\cdot\mathfrak{c} \equiv 0$ by Corollary 2 to Proposition 1. But this in turn implies $\psi_{\mathfrak{c}}(m^2\cdot a) = m^2\cdot\psi_{\mathfrak{c}}(a) = \psi_{m^2\cdot\mathfrak{c}}(a) = 0$ for all a in A, and since $m^2\cdot\delta_B$ is an isogeny (cf., L-IV$_3$, th. 6), one gets $\psi_{\mathfrak{c}} = 0$, that is, $\mathfrak{c} \equiv 0$. q.e.d.

3. Group associated to a divisor

Let A be an abelian variety and L be the function field on A.

If h is a function $\neq 0$ on A and a is in A, the map $\psi_{h,a} : f \to h\cdot f_a$ is an automorphism of L considered as a vector space over $\mathbf{K}$; furthermore $\psi_{h,a} = \psi_{h',a'}$ implies $h = h'$ and $a = a'$ and the set $\mathcal{G}$ of all maps $\psi_{h,a}$ is a group according to the formulas:

$$\psi_{h,a} \circ \psi_{h',a'} = \psi_{h\cdot h'_a,\, a+a'} \tag{16}$$

$$\psi_{h,a}^{-1} = \psi_{h^{-1}_{-a'},\, -a} \tag{17}$$

of which verification is straightforward. Finally $\bar{h} = \psi_{h,e}$ is nothing but the homothety $f \to h\cdot f$ in L.

Let D be a divisor on A such that $D \equiv 0$. To D we associate the set $\mathcal{S}(D)$ of pairs (h, a) such that:

$$D + (h) = D_a \ . \tag{18}$$

It is easily checked that along with the pairs (h, a) and (h', a') the pairs $(h \cdot h'_a, a+a')$ and $(h^{-1}_{-a}, -a)$ are in $\mathcal{S}(D)$; therefore, the set $\mathcal{G}(D)$ of operators $\psi_{h,a}$ for (h, a) in $\mathcal{S}(D)$ is a subgroup of $\mathcal{G}$ and by (16) the map $\zeta : \psi_{h,a} \to a$ from $\mathcal{G}(D)$ to A is a group homomorphism; ζ is surjective since $D_a \sim D$ for all a in A by hypothesis. Finally the kernel of ζ in $\mathcal{G}(D)$ consists of the homotheties $\bar{h}$ for the functions h such that $D + (h) = D_e = D$, that is $(h) = 0$, or h constant since A is complete.

If D and D' are divisors on A with $D \sim D'$, there exists a function F on A such that $D = D' + (F)$; furthermore, since A is complete, this function is defined up to multiplication by a constant; therefore the map $t \to \overline{F} \cdot t \cdot \overline{F}^{-1}$ is an automorphism $s_{D',D}$ of the ring of $\mathbf{K}$-linear maps in L, independent of the choice of F. The following transitivity formula is immediate for $D \sim D' \sim D''$:

$$s_{D'',D} = s_{D'',D'} \circ s_{D',D} \ . \tag{19}$$

On the other hand, for $D = D' + (F)$ the relations $(h, a) \in \mathcal{S}(D)$ and $(h', a) \in \mathcal{S}(D')$ are equivalent provided that $h' = h \cdot F/F_a$; this in turn is equivalent to

$$\psi_{h',a} = \overline{F} \cdot \psi_{h,a} \cdot \overline{F}^{-1}$$

and therefore $s_{D',D}$ induces an isomorphism from $\mathcal{G}(D)$ to $\mathcal{G}(D')$ if $D \sim D'$.

PROPOSITION 3. *Let D be a divisor on an abelian variety A such that $D \equiv 0$; then the group $\mathcal{G}(D)$ is commutative.*

Up to an isomorphism, the group $\mathcal{G}(D)$ depends only on the class of D; since in any class there exists a divisor, the support of which does not contain e, we can assume that e belongs to the complement U in A of the support of D.

Proposition 1 applied to the class of D insures the existence of a function f on $A \times A$ such that:

$$S^{-1}(D) = D \times A + A \times D + (f) \tag{20}$$

where S is the sum mapping $(a, b) \to a + b$ from $A \times A$ to A; furthermore, since e is not on the support of D, the point (e, e) is not on the support of (f), and since $A \times A$ is complete, there exists a unique function f on $A \times A$ whose divisor is given by (20) and such that $f(e, e) = 1$. Since by (20) the divisor of f is invariant under the symmetry $(a, b) \to (b, a)$, the uniqueness of f shows that the following formula holds:

$$f(a, b) = f(b, a) \qquad (a, b, a + b \text{ in } U). \tag{21}$$

If q_a is the isomorphism $b \to (a, b)$ from A to $a \times A$, formula (20) implies

$$D_{-a} - D = (f \circ q_a) \qquad (a \in U), \tag{22}$$

reasoning as in the proof of Prop. 1. In particular putting $a = e$ in (22), one sees that f induces a constant on $e \times A$ and since $f(e, e) = 1$, one gets $f(e, a) = f(a, e) = 1$ for $a \in U$. For $a \in U$ we shall put $h^a = f \circ q_a$ so that $D_{-a} - D = (h^a)$ and $h^a(e) = 1$; since A is complete, these conditions are characteristic for h^a, and if one puts $t(a) = \psi_{h^a, -a}$ for $a \in U$, one therefore gets

$$\psi_{h, -a} = t(a) \cdot \overline{h(e)} \tag{23}$$

whenever (h, a) is in $\mathcal{S}(D)$ and a in U. By (16) one gets therefore:

$$t(a) \cdot t(b) = t(a + b) \cdot \overline{f(b, a)} \tag{24}$$

for a, b and $a + b$ in U.

The set U' of operators $t(a) \cdot \bar{\xi}$ for a in U and ξ in $\mathbf{K}^*$ is the inverse image of U by the homomorphism ζ from $\mathcal{G}(D)$ to A; by (21) and (24) two elements of U' commute provided their product is in U'. Therefore any g in U' commutes with all $\psi_{h,a}$ in $\mathcal{G}(D)$ such that a and $a + \zeta(g)$ are in U, that is, provided a lies in a certain non-empty open set; but any element in A is the product of two elements in a given non-empty open set, and therefore any g in U' commutes with the whole of $\mathcal{G}(D)$. By the same reasoning, any element in $\mathcal{G}(D)$ is the product of two elements in U', so finally $\mathcal{G}(D)$ is commutative. q.e.d.

REMARK. With the same notations as before, by the one-to-one correspondence $t(a) \cdot \bar{\xi} \rightarrow (a, \xi)$, the group law on $\mathcal{G}(D)$ defines a rational law of composition on $U \times G_m$; it is easily checked that $U \times G_m$ is then a group chunk in the sense of Weil [17]. This in turn enables us to define on $\mathcal{G}(D)$ a structure of group variety, extension of A by G_m. Using a well known result of Rosenlicht [13] one sees easily that, up to an isomorphism, one obtains in this way every extension of A by G_m, and that the isomorphism classes of those extensions are in one-to-one correspondence with the divisor classes $\mathfrak{c}$ such that $\mathfrak{c} \equiv 0$. This would give another proof of a result of Weil-Serre (cf., [14] and [18]).

4. Hasse's algebra

The following notations and assumptions will be in force in this section and the next one.

Let A and B be two abelian varieties, λ an isogeny from A to B, d the degree of λ and $\mathfrak{c}$ a divisor class on A. Moreover, let k be a field of definition for A, B, λ and $\mathfrak{c}$ and let D be a divisor in $\mathfrak{c}$ rational over the field k.

The following definitions are analogous to those of Chap. II, § 4 to which

we refer for the proofs. The function fields on A and B are respectively called L and M; since λ is surjective the composite function $f^\lambda = f \circ \lambda$ is defined for any function f on B and $f \to f^\lambda$ is an isomorphism of M onto a subfield of L; this isomorphism gives rise to a structure of M-vector space on L, and we denote by $\mathcal{E}$ the endomorphism ring of this vector space. Finally the map which associates to an f in L the corresponding homothety $\bar{f}$ is an isomorphism of L with a subfield of $\mathcal{E}$, which in turn defines on $\mathcal{E}$ a structure of left vector space over L (not an algebra!).

The fields L_k and M_k are the subfields of L and M consisting respectively of the functions in L and in M which are rational over the field k; then L_k is an M_k-structure on the M-vector space L; on the L-vector space $\mathcal{E}$, the set $\mathcal{E}_k$ of the maps t with $t(L_k) \subset L_k$ is a L_k-structure. This implies the relations:

$$[\mathcal{E} : L] = [\mathcal{E}_k : L_k] = [L : M] = [L_k : M_k] = d \ . \tag{25}$$

The Hasse algebra $\mathcal{H}(D)$ associated to λ and D is the subring of $\mathcal{E}$ consisting of the M-linear operators in L commuting with every element of the group $\mathcal{G}(D)$; we shall put $\mathcal{H}_k(D) = \mathcal{H}(D) \cap \mathcal{E}_k$. If $D = 0$, the group $\mathcal{G}(D)$ is generated by the translations and the constant homotheties in L, and $\mathcal{H}(D)$ is the algebra we have associated to the isogeny λ in Chap. II, § 4 (set of invariants of G in $\mathcal{E}$).

If one puts

$$t_a(f) = t(f_{-a})_a \tag{26}$$

for $t \in \mathcal{E}$, $f \in L$ and $a \in A$, we have seen in Chap. II, § 4 that t_a is in $\mathcal{E}$ and that the group A operates *rationally* on $\mathcal{E}$ by this law. But for $g = \psi_{h,a}$ in $\mathcal{G}(D)$ one gets the formula:

$$g \cdot t \cdot g^{-1} = \bar{h} \cdot t_a \cdot \bar{h}^{-1} \qquad (t \in \mathcal{E}) \tag{27}$$

and therefore $\mathcal{G}(D)$ operates on $\mathcal{E}$ by the law $(g, t) \to g \cdot t \cdot g^{-1}$; but if g is in the kernel of the homomorphism $\psi_{h,a} \to a$ from $\mathcal{G}(D)$ onto A, it is a homothety by a constant, and therefore commutes with any t in $\mathcal{E}$. Therefore, by (27) one sees that the group A operates on $\mathcal{E}$ by the rule:

$$t_{(a)} = \bar{h} \cdot t_a \cdot \bar{h}^{-1} \tag{28}$$

where h is any function on A such that $D + (h) = D_a$.

We shall prove that in fact A operates rationally on $\mathcal{E}$ by this new law; this will be an easy consequence of the same property of the action $(a, t) \to t_a$. In fact:

(a) For f in L, t in $\mathcal{E}$ and a in A, one has:

$$(\bar{f} \cdot t)_{(a)} = \bar{h} \cdot (\bar{f} \cdot t)_a \cdot \bar{h}^{-1} = \bar{h} \cdot \bar{f}_a \cdot t_a \cdot \bar{h}^{-1} = \bar{f}_a \cdot \bar{h} \cdot t_a \cdot \bar{h}^{-1} = \bar{f}_a \cdot t_{(a)}.$$

(b) With the same hypotheses and a rational over a field k', there exists a function h on A rational over k' such that $D + (h) = D_a$ since D and D_a are rational over k' and A is complete; therefore $\overline{h}$ is in $\mathcal{E}_{k'}$ and since t_a is in $\mathcal{E}_{k'}$, one sees that $t_{(a)}$ is in $\mathcal{E}_{k'}$.

(c) Let now σ be a k-automorphism of $\mathbf{K}$; since D is rational over k, the relation $D + (h) = D_a$ implies $D + (h^\sigma) = D_{a^\sigma}$ and since $(t_a)^\sigma = (t^\sigma)_{a^\sigma}$ (cf., Chap. II, § 4) one gets

$$(t_{(a)})^\sigma = \overline{h^\sigma}(t_a)^\sigma(\overline{h^\sigma})^{-1} = \overline{h^\sigma}(t^\sigma)_{a^\sigma}(\overline{h^\sigma})^{-1} = (t^\sigma)_{(a^\sigma)} .$$

Since $\mathcal{N}(D)$ is obviously the set of all t in $\mathcal{E}$ such that $t_{(a)} = t$ for any a in A, one may use the theorem in Chap. II, § 5; this theorem implies that any basis of $\mathcal{N}(D)_k$ over k, is a basis of $\mathcal{N}(D)$ over $\mathbf{K}$, a basis of $\mathcal{E}_k$ over L_k and a basis of $\mathcal{E}$ over L, and by (25) one gets the following equality:

$$[\mathcal{N}(D) : \mathbf{K}] = [\mathcal{N}(D)_k : k] = d . \tag{29}$$

5. Divisor classes and characters[3]

Let $\mathfrak{d}$ be a divisor class on B such that $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$ and let χ be a character of the Hasse's algebra $\mathcal{N}(D)$. We shall denote by $R(\mathfrak{d}, \chi)$ the following relation between $\mathfrak{d}$ and χ:

"There exists a divisor E of class $\mathfrak{d}$ and a function $f \neq 0$ on B with the properties:

$$\lambda^{-1}(E) = D + (f) \tag{30}$$

$$t(f) = \chi(t) \cdot f \qquad (t \in \mathcal{N}(D)).'' \tag{31}$$

Our purpose is to prove the following statement:

"The relation $R(\mathfrak{d}, \chi)$ is a one-to-one correspondence between $\mathfrak{d}$ and χ. Furthermore, assuming $R(\mathfrak{d}, \chi)$, for any subfield k' of $\mathbf{K}$ the divisor class $\mathfrak{d}$ will be rational over k' if and only if χ maps $\mathcal{N}(D)_k$ into k'."

Let us start first with a divisor class $\mathfrak{d}$ on B rational over a field k' containing k, and such that $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$. Choose a divisor E in $\mathfrak{d}$ rational over k'; since the class of $\lambda^{-1}(E)$ is equal to $\mathfrak{c}$ and A is complete, there exists a function $f \neq 0$ on A rational over k' such that (30) holds; this being done, put $\chi(t) = t(f)/f$ for t in $\mathcal{N}(D)$.

Let now E_1 be a divisor in $\mathfrak{d}$ and f_1 be a function on A such that $\lambda^{-1}(E_1) = D + (f_1)$; since E and E_1 have the same class, there exists a function $r_0 \neq 0$ on B such that $E_1 = E + (r_0)$ and therefore

$$D + (f_1) = \lambda^{-1}(E_1) = \lambda^{-1}(E) + (r_0^\lambda) = D + (f \cdot r_0^\lambda) .$$

Since A is complete, and since the functions f_1 and $f \cdot r_0^\lambda$ have the same

[3] If $\mathcal{E}$ is any algebra over a field K, a *character* of $\mathcal{E}$ will be any K-linear ring homomorphism from $\mathcal{E}$ to K.

divisor, their ratio is a constant ξ, and we get $f_1 = f \cdot r^\lambda$ by putting $r = \xi \cdot r_0$. Since any t in $\mathcal{M}(D)$ is M-linear, we have $t(f_1) = t(f \cdot r^\lambda) = t(f) \cdot r^\lambda = \chi(t) \cdot f \cdot r^\lambda = \chi(t) \cdot f_1$; therefore χ is independent of the choices made for E and f.

By (3) and (8) one proves the formula:

$$\lambda^{-1}(E)_a = \lambda^{-1}(E_{\lambda \cdot a}) \qquad (a \in A) \tag{32}$$

for any divisor E on B. The following formula is obvious:

$$D + (\psi_{h,a}(f)) = \{D + (f)\}_a \tag{33}$$

for $\psi_{h,a}$ in $\mathcal{G}(D)$. Moreover, from $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$ and $\mathfrak{c} \equiv 0$, one deduces $\mathfrak{d} \equiv 0$ using Prop. 2, that is the class $\mathfrak{d}$ is invariant by translation. From this remark, one deduces by (32) and (33) that together with a solution (E, f), the equation (30) admits $(E_{\lambda \cdot a}, \psi_{h,a}(f))$ as a solution for any $\psi_{h,a}$ in $\mathcal{G}(D)$. One has therefore $t(\psi_{h,a}(f)) = \chi(t) \cdot \psi_{h,a}(f)$ for any t in $\mathcal{M}(D)$, and since such a t commutes with every element in $\mathcal{G}(D)$, this last formula can be written $h \cdot t(f)_a = h \cdot \chi(t) \cdot f_a$, that is $h \cdot \chi(t)_a f_a = h \cdot \chi(t) \cdot f_a$ using (31). Finally one gets $\chi(t)_a = \chi(t)$ for every a in A and $\chi(t)$ is a constant. If t is in $\mathcal{M}(D)_k$, one has $t(f) \in L_{k'}$ since $t \in \mathcal{E}_k \subset \mathcal{E}_{k'}$ and $f \in L_{k'}$, and therefore $\chi(t) = t(f)/f$ is in $L_{k'}$; since $\chi(t)$ is a constant, it is therefore contained in k'. Since $\chi(t)$ is in $\mathbf{K}$ for any t in $\mathcal{M}(D)$, formula (31) implies that χ is a character of $\mathcal{M}(D)$.

Finally, we have proved that given any divisor class $\mathfrak{d}$ on B such that $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$, there exists a unique character χ of $\mathcal{M}(D)$ such that $R(\mathfrak{d}, \chi)$ hold; moreover, if $\mathfrak{d}$ is rational over k', one has $\chi(\mathcal{M}(D)_k) \subset k'$.

Let now χ be a character of $\mathcal{M}(D)$ and let k' be a subfield of $\mathbf{K}$ such that χ map $\mathcal{M}(D)_k$ into k'; such a subfield exists, for instance the algebraic closure of k in $\mathbf{K}$ has that property, since $\mathcal{M}(D)_k$ is of finite rank over k. Let $\mathcal{J}$ be the kernel of χ; then $\mathcal{J}$ is the ideal in $\mathcal{M}(D)$ consisting of the elements $t - \chi(t) \cdot 1$ for t in $\mathcal{M}(D)$, and its rank over $\mathbf{K}$ is $d - 1$ since the rank of $\mathcal{M}(D)$ is d. The left ideal of $\mathcal{E}$ generated by $\mathcal{J}$ is $\mathcal{E} \cdot \mathcal{J} = L \cdot \mathcal{M}(D) \cdot \mathcal{J} = L \cdot \mathcal{J}$ since $\mathcal{E} = L \cdot \mathcal{M}(D)$, and since any basis of $\mathcal{M}(D)$ over $\mathbf{K}$ is a basis of $\mathcal{E}$ over L, the rank of $L \cdot \mathcal{J}$ over L is $d - 1$ and is $d(d-1)$ over M. Since $\mathcal{E}$ is the ring of endomorphisms of the M-vector space L of rank d, it is a classical result that the set of all vectors in L annihilated by all operators in the left ideal $L \cdot \mathcal{J}$ of rank $d(d-1)$ over M is a one-dimensional M-subspace V of L; it is clear that V is the set of all f in L annihilated by the operators $t - \chi(t) \cdot 1$, that is the set of solutions of (31). Since V is also the set of solutions of the equations (31) for t in $\mathcal{M}(D)_k$ and since $t - \chi(t) \cdot 1$ is in $\mathcal{E}_{k'}$ for t in $\mathcal{M}(D)_k$, there exists a basis for V over M consisting of elements in $L_{k'}$. In other words, there exists a solution

$f \neq 0$ of the system (31) rational over k', and any other solution is of the form $r^{\lambda} \cdot f$ with a function r on B.

Since the function f is rational over k', so is the divisor $D' = D + (f)$; since D' belongs to the class $\mathfrak{c}$ and $\mathfrak{c} \equiv 0$, it follows from Prop. 1 that there exists a function F' on $A \times A$ rational over k' such that:

$$S^{-1}(D') = D' \times A + A \times D' + (F') \tag{34}$$

where S is the sum mapping $(a, b) \to a + b$ from $A \times A$ to A. If μ is the isogeny from $A \times A$ to $B \times B$ defined by $\mu(a, b) = (\lambda \cdot a, \lambda \cdot b)$, we shall now prove that there exists a function H on $B \times B$ such that $F' = H \circ \mu$.

Let a and b be two points of A generic independent over k', and let h be a function on A rational over $k(a)$ such that $D_{-a} = D + (h)$, so that $\psi_{h,-a}$ belong to $\mathcal{G}(D)$. Since every t in $\mathcal{N}(D)$ commutes with $\mathcal{G}(D)$ and in particular with $\psi_{h,-a}$, the function $\psi_{h,-a}(f)$ is a solution of (31) together with f; therefore the ratio $\psi_{h,-a}(f)/f$ is of the form r^{λ} for some function r on B. Since $D' = D + (f)$, one gets

$$D'_{-a} = D + (\psi_{h,-a}(f)) = D + (f \cdot r^{\lambda}) = D' + (r^{\lambda})$$

on the one hand; using (34) one gets

$$D'_{-a} = D' + (h')$$

on the other hand where the function h' on A rational over $k'(a)$ is defined by $h'(b) = F'(a, b)$, by the same reasoning used to prove Prop. 1. Comparing these two values of D'_{-a}, and using the completeness of A, one infers that h'/r^{λ} is a constant and there exists therefore a function r' on B such that $h' = r'^{\lambda}$; since h' is rational over $k'(a)$ so is r' and therefore $F'(a, b) = h'(b) = r'(\lambda \cdot b)$ is contained in $k'(a, \lambda \cdot b)$. But $F'(a, b) = F'(b, a)$ (cf., the proof of Prop. 3) and therefore $F'(a, b)$ is contained in $k'(a, \lambda \cdot b) \cap k'(\lambda \cdot a, b) = k'(\lambda \cdot a, \lambda \cdot b)$; this obviously proves the existence of H.

Since the function H on $B \times B$ is rational over k', we can write $(H) = -E \times B + E_1$ where E_1 is a divisor on $B \times B$ without component of the form $T \times B$, and where E is a divisor on B rational over k'; on the other hand, one has $(F') = -D' \times A + D_1$ where D_1 is a divisor on $A \times A$ without component of the form $S \times A$. Let Y be a subvariety of codimension one of $B \times B$, not of the form $T \times B$; by the dimension principle for correspondences, any component X of $\mu^{-1}(Y)$ is of codimension one in $A \times A$; if X were of the form $S \times A$, one would get $\lambda(S) \times B \subset Y$; but since the counter-image by λ of any point in B is finite, it follows by standard results that $\lambda(S)$ has the same dimension as S and therefore is

of codimension one in B; from $\lambda(S) \times B \subset Y$ one infers therefore $\lambda(S) \times B = Y$, which is a contradiction. Therefore, from the relation $(F') = \mu^{-1}((H))$, which is a consequence of $F' = H \circ \mu$, one deduces $\mu^{-1}(E \times B) = D' \times A$ and $\mu^{-1}(E_1) = D_1$ and therefore $\lambda^{-1}(E) = D' = D + (f)$.

We have therefore proved that given any solution f of (31) rational over k' there exists a divisor E on B rational over k' such that (30) holds. Now, any other solution of (31) is of the form $f_0 = f \cdot r^{\lambda}$ for some function r on B, and the unique divisor E_0 such that $\lambda^{-1}(E_0) = D + (f_0)$ is obviously given by $E_0 = E + (r)$. Therefore, the set of divisors E on B such that there exists a function $f \neq 0$ on A for which (30) and (31) hold, is a class $\mathfrak{d}$ on B rational over k'; this class $\mathfrak{d}$ is then the unique class on B for which $R(\mathfrak{d}, \chi)$ hold. This completes proof of the statement at the beginning of this paragraph.

Let σ be a k-automorphism of $\mathbf{K}$. This automorphism extends to an automorphism $f \to f^{\sigma}$ of L over L_k and to an automorphism $t \to t^{\sigma}$ of $\mathcal{E}$ inducing the identity on $\mathcal{E}_k$. Moreover, as we have seen in § 4, one has the relation $(t_{(a)})^{\sigma} = t^{\sigma}_{(a^{\sigma})}$ for t in $\mathcal{E}$ and a in A; this shows that $t \in \mathcal{N}(D)$ implies $t^{\sigma} \in \mathcal{N}(D)$, and since the map $t \to t^{\sigma}$ in $\mathcal{N}(D)$ is a ring automorphism inducing σ on $\mathbf{K}$ and the identity on $\mathcal{N}(D)_k$, it is the map associated to the k-structure $\mathcal{N}(D)_k$ on $\mathcal{N}(D)$ (cf., Chap. I, § 5). Therefore, to any character χ of $\mathcal{N}(D)$, one can associate another character χ^{σ} by the following condition:

$$\chi^{\sigma}(t^{\sigma}) = \chi(t)^{\sigma} \qquad (t \in \mathcal{N}(D)). \tag{35}$$

This formula and the relation $t(f)^{\sigma} = t^{\sigma}(f^{\sigma})$ for t in $\mathcal{E}$ and f in L show that *the relations* $R(\mathfrak{d}, \chi)$ *and* $R(\mathfrak{d}^{\sigma}, \chi^{\sigma})$ *are equivalent* (use the fact that D and λ are rational over k).

Let D' be a divisor linearly equivalent to D. We have seen in § 3 that the automorphism $s_{D',D}$ of the ring of all endomorphisms of the $\mathbf{K}$-vector space L induces an isomorphism of $\mathcal{G}(D)$ with $\mathcal{G}(D')$; since $\mathcal{N}(D)$ is defined as the commuting set of $\mathcal{G}(D)$ and similarly for $\mathcal{N}(D')$, it follows that $s_{D',D}$ defines an isomorphism of $\mathcal{N}(D)$ with $\mathcal{N}(D')$. Moreover, if D' is rational over k, there exists a function F on A rational over k such that $D = D' + (F)$; since $\overline{F}$ is then in $\mathcal{E}_k$ and $s_{D',D}$ is the map $t \to \overline{F} \cdot t \cdot \overline{F}^{-1}$, this map sends $\mathcal{N}(D)_k$ onto $\mathcal{N}(D')_k$. Finally, one easily checks in formulas (30) and (31) that if χ is a character of $\mathcal{N}(D)$ and χ' the character $\chi \circ s_{D,D'}$ of $\mathcal{N}(D')$, the relations $R(\mathfrak{d}, \chi)$ and $R(\mathfrak{d}, \chi')$ are indeed equivalent. We see therefore in what sense our constructions depend only on the *class* $\mathfrak{c}$ of D.

6. Duality of abelian varieties

We begin by recalling the characteristic properties of the dual of an abelian variety. For the proofs of the following facts, we refer to Lang's book (cf., L-IV$_4$).

Let A be an abelian variety defined over a field k_0; there exists an abelian variety $\hat{A}$ defined over k_0 and a divisor class $\mathfrak{p}_A$ on $A \times \hat{A}$ rational over k_0 with the following properties:

(a) The divisor class $\mathfrak{p}_A$ induces the zero class on $e \times \hat{A}$ and $A \times e$.

(b) For w in $\hat{A}$, let $\mathfrak{p}_A(w)$ be the divisor class on A which is the reciprocal image of $\mathfrak{p}_A$ by the morphism $a \to (a, w)$ from A to $A \times \hat{A}$. Then $w \to \mathfrak{p}_A(w)$ is an isomorphism of the group of points of $\hat{A}$ onto the group of classes on A consisting of divisors algebraically equivalent to 0. Moreover, for any field k containing k_0, the class $\mathfrak{p}_A(w)$ is rational over k if and only if the point w is rational over k.

These two properties characterize $\hat{A}$ and $\mathfrak{p}_A$ up to a k_0-isomorphism; moreover A and $\hat{A}$ have the same dimension. The abelian variety $\hat{A}$ is called *the dual of* A and the divisor class $\mathfrak{p}_A$ *the Poincaré class.*

Let now λ be a homomorphism from A to another abelian variety B both defined over the field k_0; we define $\hat{B}$ and $\mathfrak{p}_B$ similarly as $\hat{A}$ and $\mathfrak{p}_A$. Then there exists a unique homomorphism ${}^t\lambda$ from $\hat{B}$ to $\hat{A}$, the *transpose of* λ, for which the following relation holds:

$$\lambda^{-1}(\mathfrak{p}_B(w)) = \mathfrak{p}_A({}^t\lambda \cdot w) \qquad (w \in \hat{B}). \tag{36}$$

If λ is rational over a field k containing k_0, ${}^t\lambda$ is also. Moreover one has the formulas:

$$ {}^t(\lambda + \mu) = {}^t\lambda + {}^t\mu\ , \qquad {}^t(\lambda \circ \mu) = {}^t\mu \circ {}^t\lambda\ , \qquad {}^t\delta_A = \delta_{\hat{A}}\ . \tag{37}$$

We shall now apply the results obtained in § 5 to prove the following theorem.

THEOREM 1. *Let A and B be abelian varieties and λ an isogeny from A to B. The transposed homomorphism ${}^t\lambda$ from $\hat{B}$ to $\hat{A}$ is an isogeny, and λ and ${}^t\lambda$ have the same degree.*[4]

Since λ is an isogeny, there exists an isogeny μ from B to A and an integer $m \neq 0$ such that:

$$\mu \circ \lambda = m \cdot \delta_A\ , \qquad \lambda \circ \mu = m \cdot \delta_B \tag{38}$$

[4] *Added in proof.* This last statement is the main result of the present paper. We refer to L-VII for the whole set of implications of this assertion. We mention only that the so called canonical homomorphism χ_A of A into $\hat{\hat{A}}$ is an isomorphism for any abelian variety A.

(cf., L-II$_1$, p. 29). Using the formulas (37), one gets:

$$(39) \qquad {}^t\lambda \circ {}^t\mu = m \cdot \delta_{\hat{A}} , \qquad {}^t\mu \circ {}^t\lambda = m \cdot \delta_{\hat{B}}$$

and therefore ${}^t\lambda$ is an isogeny.

Let now k_0 be a field of definition for A, B and λ and define the divisor class $\mathfrak{c}$ on A by $\mathfrak{c} = \mathfrak{p}_A(v)$ where v in $\hat{A}$ is *generic over* k_0; since ${}^t\lambda$ is an isogeny, there exists a point w in $\hat{B}$ generic over k_0 and such that ${}^t\lambda \cdot w = v$; we put $\mathfrak{d} = \mathfrak{p}_B(w)$ in such a way that $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$ by (36). Moreover, we put $k = k_0(v)$ and choose a divisor D in $\mathfrak{c}$ rational over k; let χ be the unique character of the Hasse's algebra $\mathcal{H}(D)$ for which the relation $R(\mathfrak{d}, \chi)$ hold.

Let k' be a subfield of $\mathbf{K}$ containing k; then on the one hand, the class $\mathfrak{d} = \mathfrak{p}_B(w)$ is rational over k' if and only if the point w of $\hat{B}$ is rational over k', that is if and only if k' contains $k_0(w)$. On the other hand, by the main result in § 5, the class $\mathfrak{d}$ is rational over k' if and only if k' contains the ring $\chi(\mathcal{H}(D)_k)$; and since this ring is a finite-dimensional k-module, it is a field containing k. Since $k_0(w)$ contains $k_0({}^t\lambda \cdot w) = k_0(v) = k$, we have therefore the following equality:

$$(40) \qquad \chi(\mathcal{H}(D)_{k_0(v)}) = k_0(w) .$$

Let d, $\hat{d}$, e and $\hat{e}$ be respectively the degrees of the isogenies λ, ${}^t\lambda$, μ and ${}^t\mu$ and let n be the dimension of A and $\hat{A}$. Since v and w are generic points over k_0 and $v = {}^t\lambda \cdot w$, one gets $\hat{d} = [k_0(w) : k_0(v)]$, and since the algebra $\mathcal{H}(D)_k$ over the field $k = k_0(v)$ is of rank d (cf., § 4, formula (29)), one gets $[k_0(w) : k_0(v)] \leqq d$ by (40), that is $\hat{d} \leqq d$. By the same result applied to the isogeny μ instead of λ, one finds $\hat{e} \leqq e$. But, on the other hand, the degree of the isogeny $m \cdot \delta_A$ is equal to m^{2n} (cf., L-IV$_3$, th. 6) and therefore we get $d \cdot e = m^{2n}$ by (38); for the same reason, one gets $\hat{d} \cdot \hat{e} = m^{2n}$ (since A and $\hat{A}$ have the same dimension).

We have proved the formulas $\hat{d} \leqq d$, $\hat{e} \leqq e$ and $d \cdot e = \hat{d} \cdot \hat{e} = m^{2n}$ and from this follows $d = \hat{d}$ and $e = \hat{e}$; the formula $d = \hat{d}$ is the contention of our theorem. q.e.d.

Let us remark for later use that the equality $d = \hat{d}$, that is $[k_0(w) : k_0(v)] = [\mathcal{H}(D)_{k_0(v)} : k_0(v)]$ implies together with (40) that χ induces a ring isomorphism from $\mathcal{H}(D)_{k_0(v)}$ onto $k_0(w)$; therefore $\mathcal{H}(D)_{k_0(v)}$ is a *field*.

7. Non-existence of torsion on abelian varieties

Let A be an abelian variety. It is known (cf., L-IV$_2$, cor. 3 to th. 4) that for a divisor D on A the relation $D \equiv 0$ holds if and only if there

exists an integer $m \neq 0$ with $m \cdot D \approx 0$. We shall now improve this result.

THEOREM 2. *Let A be an abelian variety and D a divisor on A. The relations $D \approx 0$ and $D \equiv 0$ are equivalent. Moreover, the group of divisor classes with respect to algebraic equivalence on A is a torsion-free commutative group.*

According to the remarks preceding the theorem, the two assertions in the theorem are indeed equivalent. We shall therefore prove the second which means that $m \cdot D \approx 0$ for some integer $m \neq 0$ implies $D \approx 0$.

Since $m \cdot D$ is algebraically equivalent to 0, its class is of the form $\mathfrak{p}_A(x)$ for some x in the dual $\hat{A}$ of A; since $m \cdot \delta_{\hat{A}}$ is an isogeny, there exists a point y in $\hat{A}$ such that $x = m \cdot y$ and therefore $\mathrm{Cl}(m \cdot D) = \mathfrak{p}_A(x) = \mathfrak{p}_A(m \cdot y) = m \cdot \mathfrak{p}_A(y)$. If D' is any divisor of class $\mathfrak{p}_A(y)$ one gets $\mathrm{Cl}(m \cdot D) = m \cdot \mathrm{Cl}(D') = \mathrm{Cl}(m \cdot D')$, that is $m \cdot (D - D') \sim 0$, and D' is algebraically equivalent to 0. Moreover since *a fortiori* $m \cdot (D - D') \approx 0$, one gets $D - D' \equiv 0$ and therefore $(m \cdot \delta_A)^{-1}(D - D') \sim m \cdot (D - D') \sim 0$ by using Corollary 1 to Proposition 2. The following lemma will imply $D - D' \approx 0$ and since one has $D' \approx 0$, we shall finally get $D \approx 0$.

LEMMA. *Let $\lambda : A \to B$ be an isogeny where A and B are abelian varieties. For a divisor E on B, the relation $\lambda^{-1}(E) \sim 0$ implies $E \approx 0$.*

We use the notations introduced in the proof of Theorem 1; moreover we can assume the divisor E rational over k_0. Put $\mathfrak{d}' = \mathfrak{d} + \mathrm{Cl}(E)$; the hypothesis $\lambda^{-1}(E) \sim 0$ implies $\lambda^{-1}(\mathfrak{d}') = \lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$ and there is therefore a unique character χ' of the Hasse's algebra $\mathcal{A}(D)$ for which $R(\mathfrak{d}', \chi')$ hold.

We know by the remark following Theorem 1 that $\mathcal{A}(D)_{k_0(v)}$ is a field. Since $\mathbf{K}$ is a universal domain, there exists therefore a k-automorphism σ of $\mathbf{K}$ such that $\chi'(t) = \chi(t)^\sigma$ for all t in $\mathcal{A}(D)_{k_0(v)}$. This implies $\chi'(t^\sigma) = \chi(t)^\sigma$ for $t \in \mathcal{A}(D)$ by linearity; by formula (35), this means $\chi' = \chi^\sigma$ and therefore $\mathfrak{d}' = \mathfrak{d}^\sigma$ since $R(\mathfrak{d}, \chi)$ and $R(\mathfrak{d}^\sigma, \chi^\sigma)$ are equivalent. We get $\mathrm{Cl}(E) = \mathfrak{d}' - \mathfrak{d} = \mathfrak{d}^\sigma - \mathfrak{d} = \mathfrak{p}_B(w)^\sigma - \mathfrak{p}_B(w) = \mathfrak{p}_B(w^\sigma - w)$ and finally $E \approx 0$. q.e.d.

8. Some remarks about separable isogenies

Let $\lambda : A \to B$ be a separable isogeny where A and B are abelian varieties, let $\mathfrak{c}$ be a divisor class on A such that $\mathfrak{c} \equiv 0$ and let k be a field of definition for A, B, λ, $\mathfrak{c}$ and the different points in the kernel N of λ. We shall investigate the structure of the Hasse's algebra in this particular case. We keep the notations of §§ 4 and 5.

Let D be a divisor in $\mathfrak{c}$ rational over k; since $D \equiv 0$, for each a in N there exists a function $c(a)$ on A rational over k such that $D_a - D = (c(a))$; define $u(a) = \psi_{c(a),a}$ as an element of $\mathcal{G}(D)$. Since a is in the kernel of λ,

it is obvious that $u(a)$ is actually M-linear; but since the group $\mathcal{G}(D)$ is commutative, any $u(a)$ commutes with the whole of $\mathcal{G}(D)$ and is therefore in $\mathcal{M}(D)$, even in $\mathcal{M}(D)_k$ since $c(a)$ and a are rational over k.

Since the automorphisms $f \to f_a$ of the field L for the a's in N are distinct, it follows from Dedekind's theorem that the elements $u(a)$ of $\mathcal{M}(D)_k$ are linearly independent over k; since the rank of the k-algebra $\mathcal{M}(D)_k$ is equal to the degree of the separable isogeny λ, that is to the number of elements of N, one sees that $\mathcal{M}(D)_k$ admits the $u(a)$ (for a in N) as a k-basis. Using formula (16), one finds easily the multiplication table of $\mathcal{M}(D)_k$; in fact, one has:

$$u(a)\cdot u(b) = c(b, a)\cdot u(a + b) \qquad (a, b \in N) \tag{41}$$

where $c(a, b)$ is defined by the formula:

$$c(a, b) = c(a)_b \cdot c(b)/c(a + b)\ . \tag{42}$$

Let $\mathfrak{d}$ be a divisor class on B rational over k such that $\lambda^{-1}(\mathfrak{d}) = \mathfrak{c}$, and let χ be the character of $\mathcal{M}(D)$ associated to $\mathfrak{d}$. Then, for E in $\mathfrak{d}$ and a function f on A such that (30) and (31) hold, one gets $\chi(u(a)) = u(a)(f)/f = c(a)\cdot f_a/f$ and this formula defines χ.

We are now in a position to compare our results with Roquette's constructions in [11]. One has to remark that the translations $f \to f_a$ for a in N form the Galois group of the extension L_k/M_k, and the formulas (41) and (42) show that our algebra $\mathcal{M}(D)_k$ of operators in L is isomorphic to the abstractly defined algebra Γ of Roquette. By the way, it is rather difficult to find in Roquette's paper an explicit statement concerning the relation between a divisor class $\mathfrak{d}$ and the corresponding character χ.

INSTITUTE FOR ADVANCED STUDY AND
UNIVERSITY OF PARIS

REFERENCES

1. E. ARTIN, Galois Theory, Notre Dame lectures, Ann Arbor, 1946.
2. I. BARSOTTI, *Abelian varieties over fields of positive characteristic*, Rend. Circ. Math. Palermo, ser. 2, 5 (1956), 145-169.
3. ———, *Repartitions on abelian varieties*, Illinois J. Math., 2 (1958), 43-70.
4. N. BOURBAKI, Algébre, ch. IV-V: *Polynomes et fonctions rationnelles, Corps commutatifs*. Actualités Sci. Ind., 1102, Hermann, Paris, 1951.
5. P. CARTIER, *Dualité des variétés abéliennes, in* Séminaire Bourbaki, Paris, Mai 1958.
6. ———, Questions de rationalité des diviseurs en géométrie algébrique, Thèse Sci. Maths., Paris, *1958*.
7. H. HASSE, *Der n-Teilungskörper eines abstrakten elliptischen Functionenkörper, nebst Anwendung auf den Mordell-Weilschen Endlichkeitsatz*, Math. Z. 48 (1942), 48-66.
8. E. KOLCHIN and S. LANG, *Existence of invariant bases*, to appear.

9. S. LANG, Abelian varieties, Interscience Tracts no. 7, New York, 1959.
10. T. MATSUSAKA, *The criteria for algebraic equivalence and the torsion group*, Amer. J. Math., 79 (1957), 53-66.
11. P. ROQUETTE, *Über das Hassesche Klassenkörper-Zerlegungsgesetz*, J. Reine Angew. Math., 197 (1957), 49-67.
12. M. ROSENLICHT, *A note on derivations and differentials on algebraic varieties*, Portugal. Math., 16 (1957), 43-55.
13. ———, *Some basic theorems on algebraic groups*, Amer. J. Math., 78 (1956), 401-443.
14. J.-P. SERRE, *Quelques propriétés des variétés abéliennes en caract. p*, Amer. J. Math., 80 (1958), 715-739.
15. A. WEIL, Foundations of algebraic geometry, Colloquium Publ. 1946.
16. ———, Variétès abéliennes et courbes algébriques, Actualités. Sci. Ind. 1064, Hermann, Paris, 1948.
17. ———, *On algebraic groups of transformation*, Amer. J. Math., 77 (1955), 355-391.
18. ———, *Variétés abéliennes*, in Colloque d'algèbre et théorie des nombres, Paris, (1948), 125-128.
19. ———, *Lie groups and algebras with involutions*, to appear.