PRINCIPAL HOMOGENEOUS SPACES OVER ABELIAN VARIETIES.*

By Serge Lang and John Tate.[1]

Let A be a commutative group variety defined over a field k. If K/k is a Galois extension, the group A_K of points of A rational over K is a module for the Galois group $G(K/k)$, and we denote the associated cohomology groups simply by $H^r(K/k,A)$ or by $H^r(k,A)$ in case K is the separable closure of k. In case K/k is infinite, we mean of course the cohomology groups constructed with cochains of finite type, i.e. coming by inflation from finite extensions.

In § 1, we have carried over to the infinite case the basic propositions of Galois cohomolgy which are familiar in the finite case [2]. This generalization is essentially trivial, but it furnishes a good review for the non-expert, it fixes our notation, and mainly, it is urgently called for when one studies algebraic groups for the following reason: If $A \rightarrow B \rightarrow C$ is an exact sequence of (separable) homomorphisms defined over k, then $A_K \rightarrow B_K \rightarrow C_K$ is not necessarily exact but *is* exact if K is the (separable) algebraic closure of k. Actually, in the remainder of the paper, we require the cohomological results only for dimension 1, and most of our applications are based on the special "Kummer sequence" discussed at the end of § 1.

In § 2 we discuss systematically the representation of principal homogeneous spaces for A over k by elements of the 1-dimensional cohomology group (a set if A is non-commutative) $H^1(k,A)$. One establishes an injection of the classes of k-isomorphic spaces into $H^1(k,A)$, and as Serre has remarked, using Weil's theorems concerning the field of definition of a variety, one sees immediately that one actually gets a bijection. Since this representation has been carried out in special cases by F. Chatelet, we call $H^1(k,A)$ the Chatelet group.

Although the rest of the paper is essentially independent of the principal homogeneous space interpretation, it is mainly this interpretation and the consequent relation of the cohomology to diophantine problems which motivates our study of $H^1(k,A)$. For example, as Chatelet has shown, an

* Received January 7, 1958.

[1] Fulbright and Sloan Fellows respectively.

elliptic curve Γ is a homogeneous space over its Jacobian A, and the question whether Γ has a rational point in an extension field K is the same as whether its cohomology class $\alpha(\Gamma) \in H^1(k,A)$ is split by K.

The essential content of this paper is contained in the theorems of the last two sections, which concern the structure of $H^1(k,A)$ when A is an abelian variety.

We first consider the case where k is a local field. After recalling in § 3 some basic facts concerning reduction mod $\mathfrak{p}$, we treat in § 4 the case when A has a non-degenerate reduction. We show (Theorem 1) how the study of elements of order prime to p in $H^1(k,A)$ can be reduced to a study of the reduced variety. There results (Theorem 2) a complete description of the part of $H^1(k,A)$ prime to p when k is a $\mathfrak{p}$-adic number field. In particular, it is a finite group.

In § 5, we deal with global fields, essentially number fields, function fields over algebraically closed fields, or fields of finite type, and obtain various qualitative results. Theorem 3 gives a new variant of the proof that A_k/mA_k is finite. (For another variant, cf. Roquette [10].) From it, we deduce the finiteness of $H^r(K/k,A)$ for finite K/k and all $r > 0$, in Theorem 4. We then consider the subgroup of $H^1(k,A)$ consisting of those elements which split at all primes. Although it is known that this group is not necessarily trivial, we can show that for each integer m (prime to the characteristic of k), its subgroup of elements of period m is finite.

Theorems 6 and 7, which are independent of the preceding five, show on the other hand that $H^1(k,A)$ is large, in different senses. From Theorem 7, it is a corollary that given any positive integer m one can construct a function field in one variable of genus 1, over a suitable algebraic number field k, the degrees of whose divisors rational over k are exactly the multiples of m. One still does not have such examples when $k = \boldsymbol{Q}$ is the field of rational numbers.

1. Galois cohomology.

Let k be a field and Ω an algebraically closed field containing k. In Galois cohomology, one deals with a functor A which attaches to each field K between k and Ω a group $A(K)$ and to each k-isomorphism $\phi\colon K \to K^{\phi}$, an isomorphism $A(\phi) : A(K) \to A(K^{\phi})$. The functor is subjected to three axioms:

(A1) For each K we have $A(K) = \bigcup A(F)$, the union being taken over all finitely generated subextensions F/k of K/k.

Notice that (A1) implies that all of our groups $A(K)$ are subgroups of one big group, namely $A(\Omega)$, and that we have $A(K) \subset A(L)$ whenever $K \subset L$.

(A2) If ψ prolongs ϕ, then $A(\psi)$ prolongs $A(\phi)$. If ψ and ϕ can be composed, then $A(\psi \circ \phi) = A(\psi) \circ A(\phi)$. $A(\text{identity}) = \text{identity}$.

From (A2) it follows that any group of k-automorphisms of a field L operates on $A(L)$.

(A3) If L/K is a Galois extension, then $A(K)$ is the set of fixed points for the operation of the Galois group on $A(L)$.

In most of our applications, A will be (the functor derived from) an algebraic group defined over k, for which $A(K) = A_K$ is the group of points of A which are rational over K, i. e. whose coordinates lie in K, and $A(\phi)$ is the map obtained by applying ϕ to the coordinates.

From now on in this section, we assume that our functor A is commutative, that is, each $A(K)$ is a commutative group. Let K/k be a (possibly infinite) Galois extension. Then $A(K)$ is a module for the Galois group $G(K/k)$, and we can consider the standard r-cochains $a = a(\sigma_1, \cdots, \sigma_r)$ of $G(K/k)$ with values in $A(K)$. We shall say that such a cochain is of *finite type* if there exists a finite sub-extension F such that $a(\sigma_1, \cdots, \sigma_r)$ depends only on the effects of the automorphisms σ_i on F. The cochains of finite type, which are the only ones arising from the usual algebraic processes, form a subcomplex of the standard cochain complex. We shall denote this subcomplex simply by $C(K/k, A)$ and its cohomology groups by $H^r(K/k, A)$. These latter are what we mean by Galois cohomology groups. Of course, if K/k is a finite extension then every cochain is of finite type, and we have achieved nothing but a simplification of notation: $H^r(K/k, A) = H^r(G(K/k), A(K))$. Also, even for infinite K, we have $H^0(K/k, A) = H^0(G(K/k), A(K))$ and this group is just $A(k)$ because of (A3). However, for $r > 0$ and K/k infinite, our groups may differ from the usual ones. For example, if $A(k) = A(K)$, that is, if $G(K/k)$ operates trivially on $A(K)$, then $H^1(K/k, A)$ is the group of continuous homomorphisms of $G(K/k)$ (Krull topology) into $A(K)$ (discrete topology), whereas $H^1(G(K/k), A(K))$ is the group of all homomorphisms.

Let K'/k' be another Galois extension, such that $K' \supset K$ and $k' \supset k$. Then each cochain $a \in C(K/k, A)$ determines a cochain $a' \in C(K'/k', A)$ by the rule $a'(\cdots, \sigma', \cdots) = a(\cdots, \sigma'_K, \cdots)$, where σ'_K denotes the effect on K of $\sigma' \in G(K'/k')$. The cochain map $a \rightarrow a'$ induces a homomorphism

$H^r(K/k,A) \to H^r(K'/k',A)$ which we simply call the *canonical* homomorphism. However, in the extreme case $k=k'$, it goes by the name of *inflation* (inf), and in the other extreme case $K=K'$, it is known as *restriction* (res).

PROPOSITION 1. *Let K/k be Galois and let k' be an arbitrary subfield. Then*

$$H^r(K/k',A) = \lim_F \{H^r(F/F\cap k',A)\},$$

the limit being taken inductively with respect to the canonical homomorphisms, as F runs over the finite subextensions of K.

Since passage to (co)homology commutes with inductive limits (cf. [2], Ch. V, Prop. 9.3*), our proposition will follow if we can show that the corresponding formula holds for the cochain groups. Each of the canonical maps $C^r(F/F\cap k',A) \to C^r(K/k',A)$ is an injection, because the inclusion $A(F\cap k') \to A(k')$ is injective and the natural map $G(K/k') \to G(F/F\cap k')$ is surjective. Thus we have only to show that each element $a\in C^r(K/k',A)$ is in the image of $C^r(F/F\cap k',A)$ for some F depending on a. Since a is of finite type, it has only a finite set of distinct values and by Axiom (A1), it follows that we can find a finitely generated, hence finite, sub-extension F/k of K/k such that all valuesof a lie in $A(F)$. Enlarging F, if necessary, so that $a(\sigma_1,\cdots,\sigma_r)$ depends only on the effects of the σ_i on Fk', we can well-define a cochain $b\in C^r(F/F\cap k',A)$ whose image is a by putting $b(\cdots,\sigma_F,\cdots) = a(\cdots,\sigma,\cdots)$, where σ_F denotes the effect of σ on F.

Taking the special case $k'=k$, we find as a corollary

$$H^r(K/k,A) = \lim_F \{H^r(F/k,A)\} = \lim_F \{H^r(G(F/k),A(F))\}.$$

Thus our cohomology groups are just the inductive limits, under inflation, of the ordinary cohomology groups of the finite subextensions.

Let L/K be a Galois extension. A k-isomorphism $\phi\colon L\to L^\phi$ induces an isomorphism $C(L/K,A)\to C(L^\phi/K^\phi,A)$ by the rule $a^\phi(\cdots,\sigma,\cdots) = \phi a(\cdots,\phi^{-1}\sigma\phi,\cdots)$, and it is a fact that the induced cohomology map $H^r(L/K,A)\to H^r(L^\phi/K^\phi,A)$, called *conjugation*, depends only on the effect of ϕ on K. In particular, if L and K are Galois extensions of k, then the Galois group $G(K/k)$ operates on $H^r(L/K,A)$.

Although there is no doubt that the whole spectral sequence of Hochschild-Serre carries over to the case of infinite Galois extensions we are content here to discuss only a small corner of it, namely:

PROPOSITION 2. *Let $K \supset k'$ be Galois extensions of k. Then there exists* *a canonical transgression homomorphism* (tg) *such that the following sequence is exact:*

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(K/k, A) \xrightarrow{\text{res}} H^1(K/k', A)^{G(k'/k)}$$
$$\xrightarrow{\text{tg}} H^2(k'/k, A) \xrightarrow{\text{inf}} H^2(K/k, A).$$

Indeed, this proposition is known in the case of ordinary cohomology groups (Cf. Hochschild, G. and Serre, J-P., "Cohomology of Group Extensions," *Trans. A. M. S.*, Vol. 74, 1953). Consequently, for each finite Galois subfield F of K, we have, exactly, with obvious abbreviations of notation:

$$0 \to H^1(F \cap k'/k) \to H^1(F/k) \to H^1(F/F \cap k')^{G(F\cap k'/k)}$$
$$\xrightarrow{\text{tg}} H^2(F \cap k'/k) \to H^2(F/k).$$

The commutativities required for passing to the inductive limit over F are satisfied and, by Proposition 1, the limit sequence is the one we are looking for. The superscript G on the middle term carries over to the limit because each $(F \cap k'/k)$ is finite.

It is easy to see that our limiting transgression map cap be characterized in the same way as the ordinary one, namely, we have $\alpha = \text{tg}\,\beta$ if and only if there is a cochain $b \in C^1(K/k, A)$ whose restriction to $C^1(K/k', A)$ is a cocycle representing β and whose coboundary δb is the inflation to $C^2(K/k, A)$ of a cocycle $a \in C^2(k'/k, A)$ representing α.

If K/k is Galois and E a finite (not necessarily Galois) subextension, there exists a *transfer* map

$$\text{tr}\colon H^r(K/E, A) \to H^r(K/k, A)$$

going in the opposite direction from restriction, whose definition we recall here, although we have little use for it in the sequel. Let Φ be the set of $[E\colon k]$ distinct k-isomorphisms of E. For each $\phi \in \Phi$, let $\phi_* \in G(K/k)$ be a chosen prolongation of ϕ to K. Then for $\sigma \in G(K/k)$, both $\sigma\phi_*$ and $(\sigma\phi)_*$ have the same effect on E, and, consequently, the automorphism $(\sigma\phi)_*^{-1}\sigma\phi_*$, which we shall denote by (σ, ϕ) leaves E elementwise fixed, i. e. belongs to $G(K/E)$. The cohomology transfer is that induced by the cochain transfer $a \to \text{tr}(a)$ defined by

$$(\text{tr}(a))(\sigma_1, \cdots, \sigma_r)$$
$$= \sum_{\phi \in \Phi} (\sigma_1\sigma_2 \cdots \sigma_r\phi)_* a((\sigma_1, \sigma_2 \cdots \sigma_r\phi),\ (\sigma_2, \sigma_3 \cdots \sigma_r\phi), \cdots, (\sigma_r, \phi)).$$

Although this cochain transfer depends on the choice of prolongations, the induced cohomology map does not. The main relation between transfer and restriction is the rule $\mathrm{tr} \circ \mathrm{res} = [E: k]$. This and all other such relations can be guessed from the case of dimension 0, where the transfer $A(E) \to A(k)$ is just the *trace*: $a \to \sum \phi a$, and the restriction $A(k) \to A(E)$ is just the inclusion map.

The relation $\mathrm{tr} \circ \mathrm{res} = [E: k]$ shows that if an element $\alpha \in H^r(K/k)$ restricts to 0 in $H^r(K/E)$, then $[E: k]\alpha = 0$. Applying this remark in case $E = K$ is a finite Galois extension of k, we see that $H^r(E/k)$ is a torsion group of exponent $[E: k]$ for $r > 0$, because $H^r(E/E, A) = 0$ for positive r. From Proposition 1, it now follows that the Galois cohomology groups in positive dimension are torsion groups for arbitrary K/k.

We conclude this section by considering the cohomology maps induced by a *homomorphism* $f: A \to B$ of one of our functors into another. By this we mean a collection of homomorphisms $f(K): A(K) \to B(K)$ satisfying

(f1) If $L \supset K$, then $f(K)$ is the restriction of $f(L)$ to $A(K)$.

(f2) If $\phi: K \to K^\phi$ is a k-isomorphism, then

$$f(K^\phi) \circ A(\phi) = B(\phi) \circ f(K).$$

For example, suppose A and B are algebraic groups defined over k. Then a k-homomorphism $f: A \to B$ (that is, an everywhere defined rational map over k which is a group homomorphism) yields a homomorphism of the functor A into the functor B. We simply let $f(K)$ denote the restriction of f to $A(K)$. Condition (f2) is satisfied because f is defined over k.

A functor homomorphism $f: A \to B$ gives rise to cohomology homomorphisms

$$H^r(K/k, A) \to H^r(K/k, B),$$

namely, those induced by the cochain map $a \to f \circ a$, and these induced cohomology maps obviously commute with canonical maps, conjugations, and transfers. A sequence of functor homomorphisms $A' \to A \to A''$ is said to be *K-exact* if the sequence $A'(K) \to A(K) \to A''(K)$ is exact in the ordinary sense.

PROPOSITION 3. *Let K/k be Galois. A K-exact sequence*

$$0 \to A' \to A \to A'' \to 0$$

gives rise to an infinite exact cohomology sequence

$$\cdots \to H^r(K/k, A) \to H^r(K/k, A'') \xrightarrow{\delta} H^{r+1}(K/k, A') \to H^{r+1}(K/k, A) \to \cdots.$$

This proposition follows as usual from the lemma: *If $A' \to A \to A''$ is K-exact, then the cochain sequence*

$$C(K/k, A') \to C(K/k, A) \to C(K/k, A'')$$

is exact. If a cochain $a \in C(K/k, A)$ goes to 0 in $C(K/k, A'')$, then each of its values goes to 0 in $A''(K)$. Hence, by K-exactness, we can pick a pre-image in $A'(K)$ for each of these values and thereby define a cochain a' whose image is a. Moreover, a' will be of finite type, provided we select one single pre-image for each of the distinct values of a, because of Axiom (A1).

In many applications, we shall deal with the case where K is the separable closure k_s of k, and where the sequence of Proposition 3 is k_s-exact. The resulting cohomology sequence involves the cohomology groups $H^r(k_s/k, A)$ which we shall simply write $H^r(k, A)$ since they occur so frequently.

Such a sequence arises from commutative algebraic groups. As a matter of notation, if X is an abelian group and m a natural number, we shall denote by X_m the kernel of the map $X \xrightarrow{m} X$. Let A be a commutative group variety defined over k. If m is prime to the characteristic, the sequence

$$0 \to A_m \to A \xrightarrow{m} A \to 0$$

is k_s-exact. Writing A_K instead of $A(K)$, our cohomology sequence becomes

$$0 \to A_m \cap A_k \to A_k \xrightarrow{m} A_k \to H^1(k, A_m) \to H^1(k, A) \xrightarrow{m} H^1(k, A) \to \cdots.$$

A portion of this exact sequence may be written more simply as follows.

$$0 \to A_k/mA_k \to H^1(k, A_m) \to H^1(k, A)_m \to 0.$$

The group A_k/mA_k is well known to be of interest in arithmetical questions, and we shall investigate it from this point of view in § 5. For the moment, we assume further that $A_m \subset A_k$, and let G_k be the Galois group of k_s over k, i.e. $G_k = G(k_s/k)$. Then G_k operates trivially on A_m, and our sequence becomes

$$0 \to A_k/mA_k \to \operatorname{Hom}(G_k, A_m) \to H^1(k, A)_m \to 0,$$

where Hom means, of course, the continuous homomorphisms as always. We shall have many applications for this sequence, and we shall call it the *Kummer* sequence, because, in case A is the multiplicative group, we have

$H^1(k, A) = 0$ by Hilbert's Theorem 90, so that we find the familiar Kummer duality

$$k^*/k^{*m} \approx \mathrm{Hom}(G_k, A_m),$$

always provided that the group of m-th roots of unity A_m is contained in $A_k = k^*$.

2. Principal homogeneous spaces. Let A be a functor of the type described in the first paragraph of § 1. If the groups $A(K)$ are not commutative, we cannot define cohomology groups $H^r(K/k, A)$ for Galois extensions K/k. The best we can do is define cohomology *sets* in dimension *one*, as follows. We consider 1-cochains a of finite type and we call 1-cocycles those satisfying the identity $a_\sigma a_\tau{}^\sigma = a_{\sigma\tau}$. Here we write $A(K)$ multiplicatively and write a_σ instead of $a(\sigma)$ for $\sigma \in G(K/k)$. We do not attempt to multiply 1-cocycles, but we explain when two 1-cocycles a and a' are cohomologous, namely, when there exists an element $b \in A(K)$ such that $a'_\sigma = b^{-1}a_\sigma b^\sigma$. The cohomology thus defined is an equivalence relation, and we denote the set of equivalence classes by $H^1(K/k, A)$. This set is not a group but it does have a distinguished element, namely the class of coboundaries of the form $a_\sigma = b^{-1}b^\sigma$, which we call the trivial class.

The reader will easily verify that the canonical maps, in particular, restriction and inflation, the conjugation maps, and the induced maps make sense for this non-commutative cohomology.

Proposition 1 holds in dimension 1.

Proposition 2 holds in a weaker form, namely, in the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(K/k, A) \xrightarrow{\text{res}} H^1(K/k', A)^{G(k'/k)}$$

inf is an injection whose image is the inverse image of the trivial class under restriction.

Proposition 3 collapses to the exactness of the sequence

$$0 \to A(k) \to B(k) \to C(k) \xrightarrow{\delta} H^1(K/k, A) \to H^1(K/k, B) \to H^1(K/k, C),$$

where we now deal with a K-exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

Here exactness means that the image of each map is the inverse image of the trivial element under the succeeding map, and there is the additional feature that δ injects the right coset space $C(k)/gB(k)$ into $H^1(K/k, A)$.

Suppose now that A is a group variety defined over k. We wish to explain the connection between the 1-dimensional cohomology sets and the right principal homogeneous spaces for A. To recall the definition of this latter object, a right phs for A over k is a variety V defined over k on which A operates simply and transitively, in such a way that the map $(v, w) \rightarrow v^{-1}w$ of $V \times V$ into A is an everywhere defined rational map over k. Here we use the symbol $v^{-1}w$ to denote the uniquely determined element of A which carries the point v into the point w, so that the formula $v(v^{-1}w) = w$ becomes an identity. Two phs's V and V' are said to be *k-isomorphic* if there exists a birational biholomorphic transformation $f\colon V \rightarrow V'$ such that $f(va) = f(v)a$ for $v \in V$ and $a \in A$. Among the k-isomorphism classes, there is a distinguished class, namely, the class of spaces which are k-isomorphic to A itself, viewed as phs under right multiplication. A space is in this class if and only if it has a rational point in k. In case A is commutative, Weil [13] has defined a geometric law of composition which makes the classes of phs's into a commutative group.

The following proposition has been proved by F. Chatelet [3], [4] for various special groups.

PROPOSITION 4. *Let K/k be a Galois extension. There is a canonical bijection between the first cohomology set $H^1(K/k, A)$ and the set of k-isomorphism classes of principal homogeneous spaces for A over k which have rational points in K. This bijection is a group isomorphism when A is commutative.*

Proof. Let V be a phs with a rational point v in K. Each such point gives rise to a 1-cocyle $a_\sigma = v^{-1}v^\sigma$. The different choices of v lead to cocycles filling out a cohomology class. Denote this class by $\alpha(V)$. If V and V' are k-isomorphic, then points v and v' which correspond under a k-isomorphism yield the same cocycle; hence $\alpha(V) = \alpha(V')$. Conversely, if V and V' are given such that $\alpha(V) = \alpha(V')$, then there do exist points v and v' yielding the same cocycle. When this is the case, the map $x \rightarrow v'(v^{-1}x)$ is a k-isomorphism of V onto V'. Indeed, it is a K-isomorphism, and a simple computation shows that it is invariant under all $\sigma \in G(K/k)$. We have thus obtained an injection of the classes of spaces into the cohomology set.

As Serre has observed, it follows immediately from Weil's theorems concerning the field of definition of a variety that every cocycle comes from a space. Indeed, consider the transformations $f_\sigma : A \to A$ defined by $f_\sigma(x) = a_\sigma x$. They satisfy the identity $f_\sigma \circ f_\tau{}^\sigma = f_{\sigma\tau}$. Since the cocycle a is of finite type, it follows from [14] that there exists a variety V defined over k and a birational biholomorphic transformation $F : A \to V$ defined over K such that $f_\sigma = F^{-1} \circ F^\sigma$. The operation $vb = F(F^{-1}(v)b)$ for $v \in V$ and $b \in A$ makes V into a phs for A over k, not only over K, because a simple computation shows that $(v^{-1}w)^\sigma = ((v^\sigma)^{-1}w^\sigma)$. Finally, one sees that the cocycle a with which we started is that arising from the point $v = F(1)$ on V.

If A is commutative, let U, V, W be phs's and suppose $f : U \times V \to W$ is an everywhere defined rational map over k which exhibits the fact that the class of W is the product of the classes of U and V (cf. [13], prop. 5). Select $u \in U$, $v \in V$ rational over K and put $w = f(u, v)$. Using the characteristic property of f, namely $f(ua, vb) = f(u, v)ab$, one finds that the cocycle derived from w is the product of those derived from u and v. This concludes the proof.

Since every variety defined over k has a point whose coordinates lie in the separable algebraic closure k_s of k, it follows from Proposition 4 that the set (group) of all principal homogeneous spaces for A over k is isomorphic to $H^1(k_s/k, A)$ which we have agreed to write $H^1(k, A)$, and which we shall call the *Chatelet set* (*group*) for A over k.

If k' is an extension field of k, it is obvious that the canonical cohomology map $H^1(k, A) \to H^1(k', A)$ reflects the homogeneous space operation of extending the ground field from k to k'. The cohomology classes in the kernel of this map are said to be *split* by k', and the same terminology is applied to the corresponding homogeneous spaces. Thus a phs for A over k is *split* by an extension k' if and only if it is k'-isomorphic to A, or what is the same, if and only if it has a rational point in k'. In case k'/k is a Galois extension, the exactness of the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(k, A) \xrightarrow{\text{res}} H^1(k', A)$$

is obvious from the point of view of homogeneous spaces, for the cohomology inflation map simply reflects the inclusion of the set of phs's split by k' in the set of all phs's for A over k.

Let X be a variety defined over k. We define the *index* of X over k ($\operatorname{ind} X$) to be the greatest common divisor of the degrees of the 0-cycles on X which are prime rational over k. The degree of a prime rational 0-cycle is equal to the degree of the extension generated over k by the coordinates of one of its points. Thus, in the case of a principal homogeneous space V

for A over k, we see that $\operatorname{ind} V$ is the greatest common divisor of the degrees of the finite extensions of k which split V, and is consequently subject to a cohomological analysis.

From now on, we assume that A is commutative. Defining the *separable index* of V ($\operatorname{ind}_s V$) as the greatest common divisor of the degrees of the finite separable splitting extensions, and the *period* of V ($\operatorname{per} V$) as the period of V in the group of classes of principal homogeneous spaces for A over k, we have

PROPOSITION 5. *Let V be a principal homogeneous space for A over k. Then* $\operatorname{per} V$ *divides* $\operatorname{ind} V$ *divides* $\operatorname{ind}_s V$, *and all three numbers have the same prime factors.*

Proof. It is trivial that the index divides the separable index. Let v_0 be a rational point of V in some Galois extension of k. Let $f\colon V \rightarrow A$ be the map $v \rightarrow v_0^{-1}v$, and let $a_\sigma = v_0^{-1}v^\sigma$ be the cocycle determined by v_0. Then for any point $v \in V$, we have $a_\sigma(f(v))^\sigma = f(v^\sigma)$, and consequently, by linearity, we have

$$a_\sigma^{\deg(\mathfrak{v})}(f(\mathfrak{v}))^\sigma = f(\mathfrak{v}^\sigma)$$

for any 0-cycle $\mathfrak{v}$ on V. If $\mathfrak{v}$ is rational over k and of degree d, then $\mathfrak{v}^\sigma = \mathfrak{v}$, and the d-th power of the cocycle a_σ is split by the coboundary of $f(\mathfrak{v})$. This proves that the period divides the index.

Finally, let p be a prime number not dividing the period. We must show that p does not divide the separable index, that is, we must construct a finite separable splitting extension E_p whose degree is not divisible by p. To this effect, we simply take any finite Galois splitting extension K/k and let E_p be the subextension cut out by a p-Sylow subgroup of $G(K/k)$. If $\alpha \in H^1(K/k, A)$ is the cohomology class of V, then the period of $\operatorname{res} \alpha \in H^1(K/E, A)$ divides the p-power $[K\colon E]$ on the one hand, and divides $\operatorname{per} V$ on the other. Consequently, $\operatorname{res} \alpha = 0$, i.e. E splits V.

The reader will have noticed the analogy between the Chatelet group of classes of principal homogeneous spaces for A over k and Brauer's group of classes of central simple algebras over k. We have in fact taken over Proposition 5 and its proof almost word for word from the theory of algebras. In the case of algebras, the period is not in general equal to the index as a counterexample of Albert [1] shows. We have found a similar counterexample in the case of principal homogeneous spaces (end of § 4). Nevertheless, our counterexample, like Albert's, involves a comparatively complicated ground field k, and over number fields and their completions, all examples which we have satisfy the condition period $=$ index.

The theory of algebras suggests other questions. Since every central division algebra contains a separable splitting field, it is true for algebras that (1) the index equals the separable index, and (2) the index is not only the greatest common divisor, but is actually the minimum of the degrees of the finite splitting fields. We have not investigated the corresponding statements for homogeneous spaces, except to notice that (2) is true in case A is an elliptic curve, for in that case, the Riemann-Roch theorem shows that every divisor class of positive degree contains positive diivsors.

The divisibilities of Proposition 5 imply

COROLLARY. *Suppose $\alpha \in H^1(k, A)$ is of period m and is split by an extension E/k of degree m. Then the corresponding homogeneous space has index m.*

This corollary will enable us to construct, with abelian varieties A, over various ground fields k, examples of spaces whose index is a preassigned integer m (cf. Theorem 7, § 5). These examples are of particular interest in case A is an elliptic curve. Then V, which becomes birationally equivalent to A over an extended ground field, is also a curve of genus 1. The point is that the index of a curve of genus $g \neq 1$ is bounded by, and in fact divides, $2g - 2$, for the Riemann-Roch theorem shows the existence of divisors rational over k of degree $2g - 2$. On the other hand, our examples show that the index is completely arbitrary for $g = 1$, a fact conjectured by Artin, but unknown until now.

3. Non-degenerate reduction. Throughout this section, we assume that we have a field k and a place of k onto a field k' such that any two extensions of it to the algebraic closure $\bar{k}$ of k are conjugate over k'. In terms of valuations, this means that the extension of the valuation is unique, and this condition is certainly satisfied if k is complete, and the valuation discrete.

We denote by θ a definite extension of our place to $\bar{k}$. An automorphism σ of $G(\bar{k}/k)$ induces an automorphism σ' of the algebraic closure of k', characterized by the relation $\theta\sigma = \sigma'\theta$. The map $\sigma \rightarrow \sigma'$ is a homomorphism of $G(\bar{k}/k)$ onto $G(\bar{k}'/k')$.

We shall also assume that the valuation is discrete, although this can presumably be dispensed with. If Z is a cycle rational over an algebraic extension K of k (say in some projective space), then it has a reduction, or, as we shall also say, a specialization Z' in the reduced projective space determined by θ, and rational over K' (Shimura [12]). The only facts concerning the specialization $Z \to Z'$ which we shall use in the sequel is that it commutes with projections and intersections, i. e. under suitable hypotheses, $(\operatorname{pr} Z)' = \operatorname{pr}(Z')$, and for two positive cycles X, Y, we have $(X \cdot Y)' = X' \cdot Y'$. We refer to [12] for the proof.

Our place θ induces a mapping of points P of our projective space, algebraic over k, onto points P', algebraic over k'. We shall also write $P' = \theta P$. We have for any automorphism σ of $\bar{k}/k$, $(\sigma P)' = \sigma' P'$. If Z is a positive cycle, then $\operatorname{supp}(Z') = (\operatorname{supp} Z)'$.

We shall now list a few properties of reduction of cycles, and especially varieties in non-degenerate cases.

To begin with, we have a result which will serve as Hensel's lemma for points on varieties.

LEMMA. *Let $\mathfrak{a}$ be a positive 0-cycle rational over k. Let P' be a point of $\mathfrak{a}'$ which occurs in $\mathfrak{a}'$ with multiplicity 1. Then there exists a unique point P of $\mathfrak{a}$ specializing to P', and P is rational over k.*

Proof. Note that P' is rational over k' since $\mathfrak{a}'$ is rational over k'. Let P be in $\mathfrak{a}$, specializing to P'. Then obviously P occurs with multiplicity 1, so that P is separable over k. If σ is any automorphism of $\bar{k}$ over k, then $(\sigma P)' = (\sigma' P') = P'$, and hence σP also specializes to P'. Since $\mathfrak{a}$ is rational over k, it follows that σP also occurs in $\mathfrak{a}$, and since P' has multiplicity 1, we conclude that $\sigma P = P$, and hence that P is rational over k.

We now have the surjectivity of θ, whose proof is due to Chow.

PROPOSITION 6. *Let the cycle Z be a variety V, and assume that Z' is also a variety V', i. e. consists of one component with multiplicity 1. Let P' be a simple point of V', rational over k'. Then there exists a point P of V rational over k which specializes to P'.*

Proof. Our statement being local, we may assume that V' is affine. There exists a linear variety L' defined over k' such that $V' \cdot L'$ is defined and contains P' with multiplicity 1. Lift L' to a linear variety L over k, such that $V \cdot L$ is defined. Then $V \cdot L$ contains a point P specializing to P'. Since $V \cdot L$ is rational over k, we need merely apply the lemma and the compatibility of specializations with intersections to conclude the proof.

For the applications, we are principally interested in abelian varieties. Let A be an abelian variety defined over k. Its specialization A' is then a cycle. If this cycle has one component with multiplicity 1, which is an abelian variety whose law of composition is obtained by reduction of that of A, then we shall say that the specialization $A \to A'$ is *non-degenerate*. (The uniqueness of non-degenerate specializations has been proved in [5].) In that case, if a, b are two points of A algebraic over k, then $(a + b)' = a' + b'$, the first $+$ referring to addition on A and the second on A'. In view of Proposition 6, we have an exact sequence

$$0 \rightarrow S_k \rightarrow A_k \rightarrow A'_{k'} \rightarrow 0,$$

where S_k is simply the kernel of the specialization homomorphism θ. If K is a finite Galois extension of k with group G then each one of the groups S_K, A_K, $A'_{K'}$ is a G-module, in view of the relation $(\sigma x)' = \sigma' x'$. It is to the exact sequence

$$0 \rightarrow S_K \rightarrow A_K \rightarrow A'_{K'} \rightarrow 0$$

that we shall apply the cohomology theory in the next section.

Suppose for a moment that k is a p-adic field $\boldsymbol{Q}_p$ and A is an elliptic curve of the type considered by Lutz [8]. Then A_k contains a subgroup isomorphic to the integers of $\boldsymbol{Q}_p$, which is none other than our kernel S_k when A' is non-degenerate. More generally, if k is an arbitrary $\mathfrak{p}$-adic field, and A an abelian variety of dimension r, then Mattuck [9] has shown that A_k contains a subgroup isomorphic to r copies of the integers of k. We can always choose such a subgroup M_k of Lutz-Mattuck such that $M_k \subset S_k$. We shall prove below that S_k is uniquely divisible by an integer m prime to p. From this one sees that $(S_k\colon M_k)$ is a power of p.

We return to an arbitrary field k subject to the conditions stated at the beginning of this section. Let m be an integer not divisible by the characteristic p of k'. Let a be a point of A rational over k. The cycle

$$(m\delta)^{-1}(a) = \mathrm{pr}_1\{\Gamma \cdot (A \times (a))\},$$

where Γ is the graph of $m\delta$, consists of the points x on A such that $mx = a$, each one occurring with multiplicity 1. Specializing, we see that

$$[(m\delta)^{-1}(a)]' = (m\delta')^{-1}(a'),$$

where δ' is the identity on A'. Taking $a = 0$, this shows in particular that θ induces an isomorphism of the points of finite order prime to p on A onto those points on A', i.e. of A_m onto A'_m. Actually, from Hensel's lemma, we get

PROPOSITION 7. *Assume that the specialization $A \rightarrow A'$ is non-degenerate. Let m be an integer prime to p. Then the homomorphism θ induces an isomorphism of $A_m \cap A_k$ onto $A'_m \cap A'_{k'}$.*

Furthermore, we also get information concerning the kernel S_k in our exact sequence above.

PROPOSITION 8. *Assume that the specialization $A \rightarrow A'$ is non-degenerate. Let m be an integer prime to p. Then S_k is uniquely divisible by m.*

Proof. Let a be in S_k, so that $a' = 0'$. The cycle $(m\delta)^{-1}(a)$ specializes to the cycle $(m\delta')^{-1}(a') = (m\delta')^{-1}(0')$ which consists of the points of order m on A'. Since $(0')$ occurs with multiplicity 1 in the reduced cycle, it follows by Hensel's lemma that there is exactly one point on $(m\delta)^{-1}(a)$ which specializes to $0'$ and that this point is rational over k.

PROPOSITION 9. *Assume that the specialization $A \rightarrow A'$ is non-degenerate. Let m be an integer prime to p. Let a be a point of A_k, and let $K = k(1/m \cdot a)$ be the field obtained by adjoining all points x such that $mx = a$. Then K is unramified over k, and $K' = k'(1/m \cdot a')$.*

Proof. This is again an immediate consequence of Hensel's lemma. Taking into account the fact that the points in $(m\delta')^{-1}(a')$ are all separable over k', we see that K is in fact the uniquely determined unramified extension of k such that $K' = k'(1/m \cdot a')$.

We conclude this section by a remark on the reduction of principal homogeneous spaces. Let V be such a space over A, defined over k. Suppose that V' has one component with multiplicity 1. Then V' has a simple rational point in some separable extension of k', and hence, by Proposition 6, V has a point in, and is split by, an unramified extension of k.

4. Cohomology and non-degenerate reduction. Let k be a field complete with respect to a discrete valuation and let A be an abelian variety defined over k which has a non-degenerate reduction A' modulo the prime in k. The only fields we consider are the algebraic extensions K of k and their residue class fields K'. From the preceding section we know the following facts:

(R1) The reduction map $\theta_K\colon A_K \rightarrow A'_{K'}$ is surjective for each K and its kernel S_K is uniquely divisible by an integer m prime to the residue class characteristic, p.

(R2) If K' is separably closed, then $A'_{K'}$ is divisible by m and contains A'_m for m prime to p.

The following cohomological analysis makes no reference to the details of the reduction process itself, nor even to abelian varieties. It applies to any pair of commutative functors A and A' of the fields K and K' (in the sense of § 1) which are linked by a natural homomorphism $\theta\colon A \rightarrow A'$ so that conditions (R1) and (R2) are satisfied. Note that (R1) implies, trivially,

(R1′) θ_K induces a bijection $A_m \cap A_K \rightarrow A'_m \cap A'_{K'}$ for each K, and m prime to p.

Let k_u denote the maximal unramified extension of k. Then the residue class field of k_u is the separable closure of the residue class field of k, or in symbols, $(k_u)' = (k')_s$.

For the rest of this section, we let m be an integer prime to p. Our goal is now Theorem 1 below.

LEMMA 1. *If $K \supset k_u$, then A_K is divisible by m and contains A_m.*

Proof. K' is separably closed because $K \supset k_u$. Hence, by (R2), we know the divisibility by m of the factor group $A_K/S_K \approx A'_{K'}$. Since from (R1), we know S_K is also divisible by m, we conclude that A_K is. We also know from (R2) that $A'_m \subset A'_{K'}$. This together with (R1′) implies that $A_m \cap A_K$ is independent of K for $K \supset k_u$, and consequently, $A_m \subset A_K$.

The group Ω_m of m-th roots of unity is contained in k_u, and the group of units in k_u is divisible by m. Therefore the maximal abelian extension of k_u of exponent m is the field $k_u(\pi^{1/m})$ obtained by adjoining the m-th root of any prime element π of k_u. The Galois group of this extension is canonically isomorphic to Ω_m. Indeed, the map $\sigma \rightarrow \zeta_\sigma = (\pi^{1/m})^{\sigma-1}$ is a homomorphism of G_{k_u} onto Ω_m, whose kernel cuts out $k_u(\pi^{1/m})$, and this homomorphism is independent of π and its chosen m-th root.

LEMMA 2. *There is a canonical isomorphism*

$$\operatorname{Hom}(\Omega_m, A_m) \approx H^1(k_u, A)_m$$

which attaches to each homomorphism $\chi\colon \Omega_m \rightarrow A_m$ the cohomology class of the cocycle $\sigma \rightarrow \chi(\zeta_\sigma)$, $\sigma \in G(k_s/k_u)$.

Proof. Since A_{k_s} is divisible by m, the Kummer sequence at the end of § 1 is applicable, and since A_{k_u} is divisible by m, it yields an isomorphism

$$\operatorname{Hom}(G_{k_u}, A_m) \approx H^1(k_u, A)_m.$$

Since A_m is commutative of exponent m, any homomorphism $h\colon G_{k_u} \rightarrow A_m$ will have the property that $h(\sigma)$ depends only on the effect of σ on an abelian extension of exponent m. Consequently, according to the discussion preceding this lemma, we can factor h through $\sigma \rightarrow \zeta_\sigma$, i.e. we can write $h(\sigma) = \chi(\zeta_\sigma)$ for some $\chi\colon \Omega_m \rightarrow A_m$.

The Galois group G_k of k_s/k operates on $H^1(k_u, A)$ as explained in § 1. It also operates on Ω_m and on A_m, and consequently, on $\operatorname{Hom}(\Omega_m, A_m)$ in the usual manner, so that

$$(\chi^\phi)(\zeta^\phi) = \phi(\chi(\zeta))$$

for $\phi \in G_k$.

LEMMA 3. *The isomorphism of Lemma 2 is a G_k-isomorphism.*

Proof. Let $\chi \in \operatorname{Hom}(\Omega_m, A_m)$ and let $a_\sigma = \chi(\zeta_\sigma)$ be the corresponding cocycle. Let $\phi \in G_k$. Then for $\sigma \in G_{k_u}$, we have

$$(a^\phi)_\sigma = \phi a_{\phi^{-1}\sigma\phi} = \phi\chi(\zeta_{\phi^{-1}\sigma\phi}) = \chi^\phi(\zeta_{\phi^{-1}\sigma\phi}{}^\phi) = \chi^\phi(\zeta_\sigma)$$

because

$$\zeta_{\phi^{-1}\sigma\phi}{}^\phi = (\pi^{1/m})^{\sigma\phi-\phi} = ((\pi^\phi)^{1/m})^{\sigma-1} = \zeta_\sigma.$$

Note that because of the way G_k is defined to operate on $\operatorname{Hom}(\Omega_m, A_m)$, we have

$$\operatorname{Hom}(\Omega_m, A_m)^{G_k} = \operatorname{Hom}_{G_k}(\Omega_m, A_m)\ ;$$

in other words, a homomorphism is left fixed by the operation of G_k if and only if it is a G_k-isomorphism.

LEMMA 4. *The sequence*

$$0 \to H^1(k_u/k, A)_m \xrightarrow{\text{inf}} H^1(k, A)_m \xrightarrow{\text{res}} [H^1(k_u, A)_m]^{G_k} \to 0$$

is exact.

Proof. Of course, it is only necessary to prove that the restriction is surjective. By the preceding lemmas, an element $\alpha \in H^1(k_u, A)_m$ which is invariant under G_k will be represented by a cocycle of the form $a_\sigma = \chi((\pi^{1/m})^{\sigma-1})$, $\sigma \in G_{k_u}$, where $\chi\colon \Omega_m \to A_m$ is a G_k-homomorphism. Here π is an arbitrary prime in k_u. Choosing π in k, and choosing a definite m-th root, we see that that the expression for a_σ makes sense for all $\sigma \in G_k$, not only for $\sigma \in G_{k_u}$. Now

$$\sigma \to (\pi^{1/m})^{\sigma-1}$$

is a cocycle in Ω_m (it is a coboundary in Ω), and since $\chi\colon \Omega_m \to A_m$ is a G_k-homomorphism, it follows that a_σ is still a cocycle. By construction, its class $\beta \in H^1(k, A)_m$ restricts to α.

Since k_u/k is unramified, its Galois group may be identified with the Galois group of its residue class extension. We shall make this identification from now on, and will designate both groups by the simpler symbol $G_{k'}$. Of course, $\theta\colon A_{k_u} \to A'_{k'_s}$ is a $G_{k'}$-homomorphism.

LEMMA 5. *θ induces an isomorphism $H^1(k_u/k, A)_m \approx H^1(k', A')_m$.*

Proof. Since A_{k_u} and A'_{k_s} are divisible by m, we can apply the Kummer sequence to the extensions k_u/k and k'_s/k', obtaining the exact horizontal rows in the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_k/mA_k \arrow[r] \arrow[d, "\theta"'] & H^1(k_u/k, A_m) \arrow[r] \arrow[d, "\theta"'] & H^1(k_u/k, A)_m \arrow[r] \arrow[d, "\theta"'] & 0 \\
0 \arrow[r] & A'_{k'}/mA'_{k'} \arrow[r] & H^1(k', A'_m) \arrow[r] & H^1(k', A')_m \arrow[r] & 0
\end{tikzcd}$$

The left vertical arrow is surjective by (R1). The middle is bijective because A_m is $G_{k'}$-isomorphic to A'_m (recall that $G_k = G(k_u/k)$). Consequently, the right vertical arrow is bijective as contended.

Putting our results together, we see that we have proved a good part of

THEOREM 1. *Let k be a field complete with respect to a discrete valuation with residue class field k' of characteristic $p \geqq 0$. Let A and A' be two commutative functors as in § 1, satisfying* (R1) *and* (R2). *Then for each natural number m not divisible by p, there exists a canonical exact sequence*

$$0 \to H^1(k', A')_m \to H^1(k, A)_m \to \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m) \to 0,$$

where Ω'_m is the group of m-th roots of unity in the residue field. Furthermore, if K is a finite extension of k with ramification index e, the following diagram is commutative:

$$\begin{tikzcd}
H^1(k', A')_m \arrow[r] \arrow[d, "\mathrm{res}"'] & H^1(k, A)_m \arrow[r] \arrow[d, "\mathrm{res}"'] & \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m) \arrow[d, "e"'] \\
H^1(K', A')_m \arrow[r] & H^1(K, A)_m \arrow[r] & \mathrm{Hom}_{G_K}(\Omega'_m, A'_m).
\end{tikzcd}$$

Proof. The indicated exact sequence results from the preceding two lemmas and the trivial replacement of Ω_m and A_m by the isomorphic Ω'_m and A'_m. The commutativity of the left square is obvious. That of the right follows from the relationship

$$\chi((\pi^{1/m})^{\sigma-1}) = \chi^e((\pi_1^{1/m})^{\sigma-1})$$

for $\sigma \in G_{K_u}$, where π_1 is a prime in K_u and $\pi \sim \pi_1^e$ is a prime in k_u.

Naturally, we are interested here in the case where the functors are given by an abelian variety A defined over k, and a non-degenerate reduction A'. Theorem 1 gives especially precise information when $H^1(k', A') = 0$. This is the case, for example, if k' is algebraically closed, or finite [7]. Then we obtain simply an isomorphism

$$H^1(k, A)_m \approx \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m).$$

From the commutative diagram of the theorem, we obtain the following corollaries.

COROLLARY 1. *Assume k' is either finite or algebraically closed. Let A be an abelian variety defined over k, with a non-degenerate reduction A'. Then a finite extension K/k splits an element $\alpha \in H^1(k, A)_m$ if and only if the ramification index $e(K/k)$ is divisible by the period of α.*

In terms of homogeneous spaces, this means that the homogeneous space

V corresponding to α has a rational point in K if and only if $e(K/k)$ is divisible by its period.

COROLLARY 2. *Let A, A' be as in Corollary 1. Let V be a principal homogeneous space of A defined over k, of period prime to p. Then the index of V is equal to its period.*

Proof. There exist ramified extensions, e.g. $k(\pi^{1/e})$, with preassigned ramification index, whose degree is equal to that index.

To describe $\mathrm{Hom}(\Omega'_m, A'_m)$ more concretely is, of course, easy. We choose a generator ζ for Ω'_m. Then a homomorphism χ is determined by the image $\chi(\zeta)$ of ζ, and this may be any element of A'_m. In order that χ be a $G_{k'}$-homomorphism, it is necessary and sufficient that $\chi(\zeta^\sigma) = \sigma\chi(\zeta)$ for each $\sigma \in G_{k'}$. Defining the integer $\nu_\sigma \pmod m$ by $\zeta^\sigma = \zeta^{\nu_\sigma}$, we see that the condition becomes $\nu_\sigma\chi(\zeta) = \sigma\chi(\zeta)$. Thus, $\mathrm{Hom}_{G_k}(\Omega'_m, A'_m)$ is isomorphic to the group of solutions $x \in A'_m$ of the equations $\sigma x = \nu_\sigma x$, $\sigma \in G_{k'}$. The isomorphism is not canonical, but depends on the choice of a primitive m-th root of unity ζ.

In particular, suppose that k' is a finite field with q elements. Then $G_{k'}$ has a canonical generator, namely the Frobenius automorphism $\xi \to \xi^q$. Its effect on an element x of A' is denoted by $x^{(q)}$. We may therefore express our result in this case as follows.

THEOREM 2. *Let A be an abelian variety defined over k with a non-degenerate reduction A', and suppose k' is a finite field with q elements. Then the group of elements of order prime to p in $H^1(k, A)$ is isomorphic to the group of solutions of $x^{(q)} = qx$ on A', of order prime to p.*

We observe that $x \to x^{(q)} - qx$ is an endomorphism of A'. Furthermore, if π denotes the Frobenius endomorphism of A', then its transpose ${}^t\pi$ on the Picard variety is easily seen to be given by the formula

$$ {}^t\pi y = qy^{(1/q)}. $$

Consequently, the transpose of $\pi - \delta$ is given by the endomorphism $y \to qy^{(1/q)} - y$ on $\hat{A}'$. Raising the kernel of this endomorphism to the q-th power, we see that the kernel is isomorphic to the subgroup of $\hat{A}'$ satisfying $y^{(q)} = qy$. In particular, we see that the group of solutions of $x^{(q)} = qx$ on A', of order prime to p, is dual to the group of rational points of $\hat{A}'$ in k', of order prime to p.

We close this section with an example of a homogeneous space whose index is not equal to its period. Suppose first of all that we could construct an abelian variety A over a field k such that $A_m \subset A_k$ and such that A_K is divisible by m for each algebraic extension K of k. Then the Kummer sequence gives isomorphisms

$$\operatorname{Hom}(G_k, A_m) \approx H^1(k, A)_m$$

and, moreover, for each K/k, a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}(G_k, A_m) \arrow[r, phantom, "\approx"] \arrow[d, "\text{res}"'] & H^1(k, A)_m \arrow[d, "\text{res}"] \\
\operatorname{Hom}(G_K, A_m) \arrow[r, phantom, "\approx"] & H^1(K, A)_m,
\end{tikzcd}$$

where the left hand res means restriction of homomorphisms from G_k to G_K. If $f\colon G_K \rightarrow A_m$ is a homomorphism, we see that K splits the corresponding cohomology class if and only if G_K is in the kernel of f. Thus the index of the corresponding homogeneous space would be the *order* of the group $f(G_k)$, whereas its period would be the *exponent* of the group $f(G_k)$. In particular, if k has an abelian extension whose group is isomorphic to A_m, i. e. to the direct product of $2r$ cyclic groups of order m ($r = \dim A$), then we can construct a homogeneous space with index m^{2r} and period m.

An actual example can be constructed easily enough. Let A be defined over an algebraically closed field k_0. Define $k_i = k_{i-1}((t_i))$ (power series in one variable) for $1 \leqq i \leqq 2r$. One proves by induction that $A_{k_i} = mA_{k_i}$, and a similar divisibility statement for finite extensions. Then we can construct our example with $k = k_{2r}$ and the abelian extension $k(t_1^{1/m}, \cdots, t_{2r}^{1/m})$.

One could also construct a similar example over a purely transcendental function field in $2r$ variables. Incidentally, we note that the Kummer sequence shows, for any A and k, that if $A_m \subset A_k$ and $\operatorname{per}_k V = m$, then $\operatorname{ind}_k V$ divides m^{2r}. Thus our example is as bad as possible under the conditions $A_m \subset A_k$.

5. Global fields. Let k be a field with a fixed set of (inequivalent) discrete valuations $\mathfrak{p}$ which we shall call primes. By a prime in a finite algebraic extension K of k, we mean, of course, a valuation of K which extends a prime of k. Let m be a natural number not divisible by the characteristic of k. We shall say that k is an *m-global field* if each finite extension K of k has the following two properties.

(Gl1) If A is an abelian variety defined over K, then A has a non-degenerate reduction at all but a finite set of primes $\mathfrak{p}$ of K.

(Gl2, m) The set of primes of K dividing m is finite, and if S is any finite set of primes of K, there is only a finite number of abelian extensions of K of exponent m which are unramified outside S.

By well known elementary properties of number fields, one sees immediately that an algebraic number field of finite degree is m-global for every m, if we take as primes all the inequivalent discrete valuations.

The same remark applies to a field of algebraic functions of one variable over a finite constant field, and shows that it is m-global for m prime to its characteristic.

More generally, let k be an algebraic function field in n variables (the case $n=0$ is not excluded) over a constant field k_0 such that $k_0{}^*/(k_0{}^*)^m$ is finite, for instance, a $\mathfrak{p}$-adic field, or an algebraically closed field. Choose as set of primes of k those arising from the prime divisors rational over k_0 of a projective normal model of k. Then it is easy to see (using results of algebraic geometry) that k is m-global.

Finally, if k is a function field over an algebraic number field of finite degree, then k is m-global for every m. The set of primes is then to be the set of prime divisors on a "mixed characteristic" model. This can easily be seen by reducing the proof to a geometric statement. As this, and the above fields are meant mostly to give concrete examples of m-global fields to the reader, we do not go in detail into the proofs that they are m-global, since they are essentially well known.

For the convenience of the reader, we indicate very briefly a sketch of the manner in which the above fields can be proved to satisfy our two global axioms.

(Gl 1) actually depends on the fact that an element of the field k has only a finite number of zeros and poles. To check that a reduction is non-degenerate, one checks that each property entering into the definition of an abelian variety has a non-degenerate reduction. For instance, we have: the absolute irreducibility (say of the Chow form if the variety is in projective space); the non-singularity (which depends on the non-vanishing of a determinant which is an element of k); the fact that some mappings are everywhere defined; associativity; etc.

As for (Gl 2), say for number fields, one may look at it either from the point of view that there is only a finite number of unramified extensions of degree m (abelian or non-abelian), a fact already stated in Hilbert's *Zahlbericht*, or from the point of view of Kummer theory: After adjoining the m-th roots of unity, the extension can be obtained by extracting radicals, and one uses the finiteness of class number and unit theorem. In the geometric case, one uses the analogous facts, which involve the Jacobian for the case of curves, and the Picard variety as well as the torsion part of the Neron-Severi group in higher dimension.

We shall now reprove for global fields the weak part of the Mordell-Weil theorem, i. e. Theorem 3 below.

PROPOSITION 10. *Let A be an abelian variety defined over a field k. Let m be prime to the characteristic of k and let $K = k(1/m \cdot A_k)$. Then $(A_k \colon mA_k)$ is finite if and only if $[K \colon k]$ is finite.*

Proof. It is trivial that if $(A_k \colon mA_k)$ is finite, then $[K \colon k]$ is finite. Conversely, consider the exact sequence

$$0 \to A_m \to A_K \to mA_K \to 0$$

Let $G = G(K/k)$. We have the cohomology sequence

$$0 \to A_m \cap A_k \to A_k \to mA_K \cap A_k \to H^1(G, A_m).$$

By assumption, $mA_K \cap A_k = A_k$, and thus we get the injection

$$0 \to A_k/mA_k \to H^1(G, A_m)$$

which shows that A_k/mA_k is finite.

COROLLARY. *Let A be an abelian variety defined over a field k, and let m be a natural number prime to the characteristic of k. Let L be a finite extension of k. If A_L/mA_L is finite then so is also A_k/mA_k.*

Proof. By the proposition, $L(1/m \cdot A_L)$ is finite over L. This implies a fortiori that $k(1/m \cdot A_k)$ is finite over k. Using the proposition once more, we get what we want.

THEOREM 3. *Let A be an abelian variety defined over an m-global field k. Then A_k/mA_k is finite.*

Proof. By the corollary, we may assume that $A_m \subset A_k$. Let $K = k(1/m \cdot A_k)$. By Proposition 9, we know that K/k is unramified at every prime $\mathfrak{p}$ not dividing m at which A has a non-degenerate reduction. From the definition of m-global, it follows that K is finite over k because it is abelian of exponent m over k. We now apply Proposition 10, to conclude the proof.

If K is a finite Galois extension of k, and if A is an abelian variety defined over k such that its group of rational points A_K in K is finitely generated (i. e. satisfies the strong Mordell-Weil theorem), then obviously $H^r(K/k, A)$ is finite for $r > 0$. However, Theorem 3 will suffice to prove the analogous result for m-global fields. For use in the statement of our next theorem, we recall that the m-primary part of an abelian group consists of those elements whose period divides a power of m.

THEOREM 4. *Let A be an abelian variety defined over an m-global* *field k. If K/k is a finite Galois extension, then the m-primary part of the group $H^r(K/k, A)$ is finite for each $r > 0$.*

Proof. This is an immediate consequence of the following general cohomological fact.

LEMMA. *Let G be a finite group and X a G-module such that X/mX and X_m are finite. Then the m-primary part of $H^r(G, X)$ is finite for each $r > 0$.*

Proof. Since $H^r(G, X)$ is a torsion group of bounded exponent $(G\colon 1)$, it is enough to prove $H^r(G, X)_m$ finite. The map $m\colon X \rightarrow X$ can be written as a product $m = g \circ h$ of the maps g and h in the exact sequences

$$0 \rightarrow X_m \rightarrow X \xrightarrow{h} mX \rightarrow 0$$

$$0 \rightarrow mX \xrightarrow{g} X \rightarrow X/mX \rightarrow 0.$$

For the induced cohomology maps in dimension r, we have $m_* = g_* h_*$. From the exact cohomology sequences derived from our two exact sequences, we see that the kernels of h_* and g_* are finite, being homomorphic images of $H^r(G, X_m)$ and $H^{r-1}(G, X/mX)$ respectively. Consequently, the kernel of m_* is finite, which is what we wanted to prove.

If A is an abelian variety defined over an m-global field k, we say that an element $\alpha \in H^1(k, A)$ *splits at a prime* $\mathfrak{p}$ of k if α is in the kernel of the canonical map $H^1(k, A) \rightarrow H^1(k_\mathfrak{p}, A)$, where $k_\mathfrak{p}$ denotes the completion of k at $\mathfrak{p}$. In other words, α splits at $\mathfrak{p}$ if the corresponding homogeneous space has a rational point in $k_\mathfrak{p}$.

Selmer [11] has given examples of principal homogeneous spaces for abelian varieties of dimension 1 over the rational number field $\boldsymbol{Q}$ which split at all primes p but do not split in $\boldsymbol{Q}$. The elliptic curve $3X^3 + 4Y^3 + 5Z^3 = 0$ is such a space over its Jacobian. On the other hand, we can show that the number of such spaces with given period is finite. More precisely, let us denote by $H^1(k, A, S)$ the subgroup of $H^1(k, A)$ consisting of the elements which split at all primes outside a finite set S. We have

THEOREM 5. *Let A be an abelian variety defined over an m-global field k. Then $H^1(k, A, S)_m$ is finite.*

Proof. Without loss of generality, we may assume $A_m \subset A_k$. Indeed, the restriction of $H^1(k, A)$ to $H^1(K, A)$, where $K = k(A_m)$, has finite kernel by Theorem 4, and a fortiori that of $H^1(k, A, S)_m$ to $H^1(K, A, S)_m$. Furthermore, we may enlarge S until it contains all primes $\mathfrak{p}$ dividing m

and all primes $\mathfrak{p}$ where A does not have a non-degenerate reduction. Now for $\mathfrak{p} \notin S$, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_k/mA_k \arrow[r] \arrow[d] & \mathrm{Hom}(G_k, A_m) \arrow[r] \arrow[d] & H^1(k, A)_m \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_\mathfrak{p}/mA_\mathfrak{p} \arrow[r] & \mathrm{Hom}(G_\mathfrak{p}, A_m) \arrow[r] & H^1(k_\mathfrak{p}, A)_m \arrow[r] & 0.
\end{tikzcd}$$

Here we have abbreviated by $A_\mathfrak{p}$ the group $A_{k_\mathfrak{p}}$ and by $G_\mathfrak{p}$ the decomposition group $G_{k_\mathfrak{p}}$ which we may view as a subgroup of G_k, uniquely determined up to a conjugation. The horizontal arrows are the exact Kummer sequences and the vertical arrows are the canonical maps, the middle one therefore denoting simply the operation of restricting to $G_\mathfrak{p}$ a homomorphism of G_k. What we shall actually prove is that the inverse image of $H^1(k, A, S)_m$ in $\mathrm{Hom}(G_k, A_m)$ is finite. To this effect, it will be enough to show that if $\chi\colon G_k \to A_m$ is a homomorphism whose cohomology class in $H^1(k, A)$ splits outside S, then the abelian extension K_χ/k of exponent m which is cut out by the kernel of χ is unramified outside S. By the commutativity of the right square of the above diagram we know that the restriction of χ to G_p is of the form $\chi(\sigma) = (\sigma - 1)(1/m \cdot a)$ for some $a \in A_\mathfrak{p}$. Thus we have $K_\chi \subset k_\mathfrak{p}(1/m \cdot a)$, and, by Proposition 9, it follows that K_χ is unramified at $\mathfrak{p}$. This completes the proof of Theorem 5.

It is natural to raise the question whether, given an element of $H^1(k_\mathfrak{p}, A)$, there exists an element of $H^1(k, A)$ which restricts to it. We can prove this in a special case.

THEOREM 6. *Let k be any field with a discrete valuation $\mathfrak{p}$ and let $k_\mathfrak{p}$ be its completion. Let m be prime to the characteristic of k and assume that the group of m-th roots of unity Ω_m lies in k. Let A be an abelian variety defined over k such that $A_m \subset A_k$. Then given $\alpha_\mathfrak{p} \in H^1(k_\mathfrak{p}, A)_m$, there exists an element $\alpha \in H^1(k, A)_m$ whose canonical image in $H^1(k_\mathfrak{p}, A)$ is $\alpha_\mathfrak{p}$.*

Proof. We use the Kummer sequence again, and the exact commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(G_k, A_m) \arrow[r] \arrow[d] & H^1(k, A)_m \arrow[r] \arrow[d] & 0 \\
\mathrm{Hom}(G_\mathfrak{p}, A_m) \arrow[r] & H^1(k_\mathfrak{p}, A)_m \arrow[r] & 0.
\end{tikzcd}$$

We are trying to prove that the right hand vertical arrow is surjective. To do so, it is enough to prove the left hand vertical arrow is surjective. Since

A_m is isomorphic as an abstract group to the direct sum of $2r$ copies of Ω_m $(r=\dim A)$, we have

$$\operatorname{Hom}(G,A_m)\approx(\operatorname{Hom}(G,\Omega_m))^{2r},$$

and, consequently, it is enough if we show the surjectivity of

$$\operatorname{Hom}(G_k,\Omega_m)\rightarrow\operatorname{Hom}(G_{\mathfrak{p}},\Omega_m).$$

Recall now that Hom means here continuous homomorphisms, so that by the usual Kummer duality, we have $\operatorname{Hom}(G_k,\Omega_m)\approx k^*/(k^*)^m$, and similarly for $k_{\mathfrak{p}}$. Thus, we must simply show the surjectivity of $k^*/(k^*)^m\rightarrow k_{\mathfrak{p}}{}^*/(k_{\mathfrak{p}}{}^*)^m$. This is now obvious since $(k_{\mathfrak{p}}{}^*)^m$ is an open subgroup of $k_{\mathfrak{p}}{}^*$, m being prime to the characteristic.

Remark. Under the same hypotheses as in the theorem, one can deal with a finite number of discrete valuations, and use the approximation theorem to show that there is an α restricting simultaneously to a finite number of given $\alpha_{\mathfrak{p}_i}$.

In analogy with Grunwald's theorem in class field theory, one may conjecture that if k is an algebraic number field and $\mathfrak{p}$ a given prime, then given $\alpha_{\mathfrak{p}}\in H^1(k_{\mathfrak{p}},A)$, there exists $\alpha\in H^1(k,A)$ restricting to $\alpha_{\mathfrak{p}}$.

Finally, we prove a result indicating that $H^1(k,A)$ is usually a large group when k is a global field.

THEOREM 7. *Let m be a natural number and let k be a field with an infinite number of abelian extensions of exponent exactly m. Let A be an abelian variety defined over k such that* (1) *A_k/mA_k is finite and* (2) *A_k contains at least one element a of exact period m. Then $H^1(k,A)$ contains an infinite number of elements of period m, and, in fact, an infinite number such that the corresponding homogeneous spaces have index m as well as period m.*

Proof. Let $L=k(1/m\cdot A_k)$. Since we have assumed A_k/mA_k finite, L is a finite extension of k. Consequently, by our hypothesis about the existence of abelian extensions of exponent m, there exists a Galois extension K of k linearly disjoint from L whose group $G=G(K/k)$ is the direct product of an arbitrarily large number of cyclic groups of order m. For each homomorphism χ of G into the cyclic group $\langle a\rangle$ of order m generated by a, let $\alpha_\chi\in H^1(K/k,A)\subset H^1(k,A)$ denote the cohomology class of the 1-cocycle $\sigma\rightarrow\chi(\sigma)$. We claim that the map $\chi\rightarrow\alpha_\chi$ is an injection. Indeed, if $\chi(\sigma)=(\sigma-1)b$, $b\in A_K$, $\sigma\in G$, then $m\chi(\sigma)=(\sigma-1)mb=0$ for all σ; hence $mb\in A_k$. Since K is disjoint from L, it follows that $b\in A_k$ and $\chi=0$.

Thus, $H^1(k, A)$ contains a subgroup isomorphic to $\mathrm{Hom}(G, \langle a \rangle)$, that is, to the direct product of arbitrarily many cyclic groups of order m. Moreover, for each element of this subgroup, the corresponding homogeneous space has index $=$ period. This follows from the Corollary of Proposition 5, § 2 because, since $\langle a \rangle$ is cyclic, the index in G of the kernel of the homomorphism χ: $G \rightarrow \langle a \rangle$ is equal to the period of χ, and the subfield of K cut out by this kernel splits α.

PARIS.

REFERENCES.

[1] A. Albert, "On primary normal division algebras of degree 8," *Bulletin of the American Mathematical Society*, vol. 39 (1933), pp. 265-272.

[2] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1956.

[3] F. Chatelet, "Méthode Galoisienne et courbes de genre 1," *Annales de l'Universite de Lyon*, Section A., t. 89 (1946), pp. 40-49.

[4] ———, "Variations sur un thème de Poincaré," *Annales de l'Ecole Normale superieure*, vol. 59 (1944), pp. 249-300.

[5] W. L. Chow and S. Lang, "On the birational equivalence of curves under specialization," *American Journal of Mathematics*, vol. 79, No. 3 (1957), pp. 649-652.

[6] J. Igusa, "Fibre systems of Jacobian varieties, II," *American Journal of Mathematics*, vol. 78 (1956), pp. 745-760.

[7] S. Lang, "Algebraic groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[8] E. Lutz, "Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques," *Journal für die reine und angewandte Mathematik*, Bd. 177 (1937), pp. 238-247.

[9] A. Mattuck, "Abelian varieties over p-adic ground fields," *Annals of Mathematics*, Series 2, vol. 62 (1955), pp. 92-119.

[10] P. Roquette, "Uber das Hassesche Klassenkorper-Zerlegungesetz," *Journal für die reine und angewandte Mathematik*, Bd. 197 (1957), pp. 49-67.

[11] E. Selmer, "The diophantine equation $ax^3 + by^3 + cz^3 = 0$," *Acta Mathematika*, vol. 85 (1951), pp. 203-362.

[12] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[13] A. Weil, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955), pp. 493-512.

[14] ———, "The field of definition of a variety," *American Journal of Mathematics*, vol. 78 (1956), pp. 509-524.