J. TATE

WC-groups over *p*-adic fields

Séminaire N. Bourbaki, 1958, exp. nº 156, p. 265-277
<http://www.numdam.org/item?id=SB_1956-1958__4__265_0>

Séminaire BOURBAKI
(Décembre 1957)

WC-GROUPS OVER $\mathfrak{p}$-ADIC FIELDS

by J. TATE

Let A be a commutative group variety defined over a field k. Let K be a finite Galois extension of k with group G, and let A_K denote the group of points of A rational over K. F. CHÂTELET, [2], in case A is an elliptic curve, and A. WEIL, [8], in the general case, have demonstrated the importance of the one-dimensional cohomology group $H^1(G, A_K)$ for the theory of diophantine equations. In their honor we designate by $WC(A/k)$ the injective limit of the groups $H^1(G, A_K)$ as K ranges over bigger and bigger finite Galois extensions of K. Although no Galois cohomology appears in [8], it is easy to show that Weil's group of classes of principal homogeneous spaces is isomorphic to $WC(A/k)$, by using Châtelet's methods together with Weil's results [9] on the field of definition of a variety. This has been remarked by SERRE, and details are given in [6].

In [6], LANG and I obtained some preliminary insights into the structure of $WC(A/k)$ and could determine the structure exactly in some special cases where A has a non-degenerate specialization. Here I wish to explain a new approach based on a certain cohomological pairing and to prove : <u>If A is an abelian variety and k a $\mathfrak{p}$-adic number field, then $WC(A/k)$ is canonically isomorphic to the character group $\hat{A}_k^*$ of the compact group $\hat{A}_k$ of points rational over k on the Picard variety $\hat{A}$ of</u> A. In the paragraph 1 we describe a reciprocity law of LANG on which our cohomological pairing (paragraph 2) is based. For $\mathfrak{p}$-adic k there results (paragraph 3) a canonical homomorphism $h_k : WC(A/k) \to \hat{A}_k^*$. The paragraphs 4-8 constitute the proof that h_k is bijective ; the methods used, namely counting, Kummer theory, and induction in cyclic towers, make the proof almost a parody of the class field theory on which it is based. In paragraph 9 we propose a definition of generalized Picard varieties $A_{\mathfrak{n}}$, analogous to Rosenlicht's generalized Jacobians of curves, for certains of which we are able to compute $WC(A_{\mathfrak{n}}/k)$ for $\mathfrak{p}$-adic k. In paragraph 10, an afterthought, we suggest a better way of looking at the cohomological pairing of paragraph 2, and generalize it to arbitrary dimensions. This leads to the conjecture : <u>For finite $\mathfrak{p}$-adic Galois K/k, $H^p(G, A_K)$ is isomorphic to the character group of</u> $H^{1-p}(G, A_K)$. We propose a method of proof involving a spectral homomorphism belonging to the cohomology theory of finite group extensions.

Applying these results to the case $A = \hat{A} = J =$ Jacobian of Γ one can prove : If Γ is an algebraic curve defined over, and with rational point in, a $\mathfrak{p}$-adic field k, and if K/k is a finite Galois extension with group G, then $H^1(G, C_K) = 0$, where C_K is the group of idele classes of the function field $K(\Gamma)$. The ideas are sketched in paragraph 9.

The three underlined statements in this introduction hold true if k is the real field, and (trivially) if k is the complex field, provided we divide $\hat{A}_k$ by its connected component in the first statement. Indeed, the third statement for real k has been knowna long time, for it is the essential content of WITT [10].

For a number field k, the global consequences of these local results on the completions of k have still to be investigated.

1. Lang's reciprocity law for correspondences between abelian varieties.

If A is an abelian variety we shall denote by $Z(A)$ the group of zero cycles of degree 0 on A, and by $Y(A) \subset Z(A)$ the Albanese kernel of A. Thus an exact sequence

$$(1) \qquad 0 \to Y(A) \to Z(A) \xrightarrow{S} A \to 0 ,$$

where S denotes summation of points on A.

Let A and B be abelian varieties. Let $\mathfrak{a} \in Y(A)$ and $\mathfrak{b} \in Z(B)$ and suppose D is a divisor on $A \times B$ such that the support of D does not meet the support of $\mathfrak{a} \times \mathfrak{b}$. Under these circumstances the divisor $D(\mathfrak{a}) = Pr_B(D.(\mathfrak{a} \times B))$ is defined ; since $\mathfrak{a} \in Y(A)$ there is a function g on B such that $D(\mathfrak{a}) = (g)$; moreover g is defined and non-zero at each point of the support of $\mathfrak{b}$. We may therefore define the symbol

$$(2) \qquad D(\mathfrak{a}, \mathfrak{b}) = g(\mathfrak{b}) = \prod_{b \in B} g(b)^{\mathrm{ord}_b(\mathfrak{b})} ,$$

its value being independent of the undetermined constant factor in g since $\mathfrak{b}$ is of degree 0.

LANG [5] has proved the fundamental reciprocity law

$$(3) \qquad D(\mathfrak{a}, \mathfrak{b}) = {}^tD(\mathfrak{b}, \mathfrak{a}) \qquad \text{for } \mathfrak{a} \in Y(A) , \ \mathfrak{b} \in Y(B)$$

where ${}^tD \subset B \times A$ denotes the transpose of D. This law is analogous to and implies the by now familiar rule $f((g)) = g((f))$ for relatively prime functions f and g on a curve. LANG bases his proof on a new theorem of the hypercube. In an appendix he reproduces a proof of CHEVALLEY of the important fact that, for given $\mathfrak{a}$ and $\mathfrak{b}$ one can change an arbitrary D by a linear equivalence so that the symbol $D(\mathfrak{a}, \mathfrak{b})$ is defined, without leaving a given field of definition for the objects in question.

2. The cohomological pairing.

Let A and B be abelian varieties defined over a field k. We wish to explain how there is attached to each correspondence class $\mathfrak{D}$ of divisors on $A \times B$ rational over k a pairing of $WC(A/k)$ and the group B_k of points of B rational over k into the Brauer group $Br(k)$.

Let $\alpha \in WC(A/k)$ and $b \in B_k$. To pair α and b we first represent α by a 1-cocycle $\{a_\sigma\}$ of $G_{K/k}$ in A_K for a suitable finite normal extension K/k. Next, with the exact sequence (1) in mind, represent each a_σ by an $\mathfrak{a}_\sigma \in Z_K(A)$. Then $(\delta\mathfrak{a})_{\sigma\tau} = \sigma\mathfrak{a}_\tau - \mathfrak{a}_{\sigma\tau} + \mathfrak{a}_\sigma \in Y_K(A)$. Finally, select $\mathfrak{b} \in Z_k(a)$ representing the given $b \in B_k$, and put

$$c_{\sigma,\tau} = D((\delta\mathfrak{a})_{\sigma,\tau}, \mathfrak{b}), \tag{5}$$

where D is a divisor rational over k in the given correspondence class $\mathfrak{D}$ such that the right hand side is defined. Then $\{c_{\sigma,\tau}\}$ is a 2-cocycle of $G_{K/k}$ in K^* and represents an element γ of the Brauer group $Br(k)$ which we can safely denote by the suggestive symbol

$$\gamma = \mathfrak{D}(\delta\alpha, b) \tag{6}$$

because γ is independent of the choices of D, $\mathfrak{a}_\sigma$, and $\mathfrak{b}$ as the following remarks show. If we change D by $X \times B + A \times Y + (\varphi)$ then $c_{\sigma,\tau}$ changes by the coboundary of the 1-cochain $e_\sigma = \varphi(\mathfrak{a}_\sigma \times \mathfrak{b})$. If we change $\mathfrak{a}_\sigma$ by $\mathfrak{y}_\sigma + (\sigma - 1)$ with $\mathfrak{y}_\sigma \in Y_K(A)$ and $\mathfrak{y} \in Z_K(A)$, then $c_{\sigma,\tau}$ changes by the coboundary of $e_\sigma = D(\mathfrak{y}_\sigma, \mathfrak{b})$.
If we change $\mathfrak{b}$ by $\mathfrak{y} \in Y_k(B)$ then, applying Lang's reciprocity law (3) to the cycles $(\delta\mathfrak{a})_{\sigma,\tau}$ and $\mathfrak{y}$ we find that $c_{\sigma,\tau}$ changes by the coboundary of $e_\sigma = {}^tD(\mathfrak{y}, \mathfrak{a}_\sigma)$. The linearity of $\mathfrak{D}(\delta\alpha, b)$ in each of its three arguments $\mathfrak{D}, \alpha, b$, follows now immediately from that of $D(\mathfrak{a}, \mathfrak{b})$.

Let K/k be a finite separable, not necessarily normal, extension. Then we may consider the cohomological restriction and transfer mappings (cf. [1], [3])

res : $B_k \to B_K$ (inclusion)	tr : $B_K \to B_k$ (trace)
res : $WC(A/k) \to WC(A/K)$	tr : $WC(A/K) \to WC(A/k)$
res : $Br(k) \to Br(K)$	tr : $Br(K) \to Br(k)$

The formal properties of our pairing with respect to these maps are given by the following formulas, in which (α, b) abbreviates $\mathfrak{D}(\delta\alpha, b)$, $\mathfrak{D}$ being kept fixed and rational over k ;

(7) $(\text{res}\ \alpha, \text{res}\ b) = \text{res}\ (\alpha, b)$; $\alpha \in WC(A/k)$, $b \in B_k$

(8) $(\alpha, \text{tr}\ b) = \text{tr}(\text{res}\ \alpha, b)$; $\alpha \in WC(A/k)$, $b \in B_k$

(9) $(\text{tr}\ \alpha, b) = \text{tr}(\alpha, \text{res}\ b)$; $\alpha \in WC(A/K)$, $b \in B_k$

These rules can be established by straightforward cochain computations, using the cochain formulas underlying the corresponding formal properties of the cup product.

3. The duality for $\mathfrak{p}$-adic k .

From now on we assume that A is an abelian variety defined over a $\mathfrak{p}$-adic number field k and we put $B = \hat{A}$, the Picard variety of A . We define a canonical pairing α , $b \to \langle\alpha, b\rangle$ of $WC(A/k)$ and B_k into $\underset{\sim}{T}$ by putting

(10) $$\langle\alpha, b\rangle = \exp 2\pi i\theta\ (\mathcal{D}(\delta\alpha , b)) ,$$

where $\theta : \text{Br}(k) \approx \underset{\sim}{Q}/\underset{\sim}{Z}$ is the canonical isomorphism of local class field theory which attaches to each 2-dimensional class its numerical invariant, and where $\mathcal{D}$ is the correspondence class containing the Poincaré divisors on $A \times B$. In case of a finite extension K/k the formulas (8) and (9) yield simply

(11) $$\langle\alpha , \text{tr}\ b\rangle = \langle\text{res}\ \alpha, b\rangle$$

(12) $$\langle\text{tr}\ \alpha, b\rangle = \langle\alpha, \text{res}\ b\rangle$$

because the transfer in the Brauer groups preserves the numerical invariant θ .

Since k is a locally compact field and B is complete, B_k is a compact topological group. Furthermore one knows (cf. paragraph 4 below) that the subgroups mB_k , $m = 1 , 2 , 3 , \ldots,$ are a fundamental system of neighborhoods of 0 in B_k . Since WC is a torsion group, it follows that for each fixed $\alpha \in WC(A/k)$ the map $b \to \langle\alpha, b\rangle$ is a continuous character of B_k . Hence our pairing yields a canonical homomorphism

(13) $$h_k : WC(A/k) \to B_k^* ,$$

where B_k^* denotes the (discrete) character group of the compact group B_k . Our aim is to show that h_k is bijective.

4. Index computations.

LUTZ, in the elliptic case, and MATTUCK [7] , in general, have shown that A_k contains a subgroup of finite index A_k' isomorphic to the direct sum of r copies of $\mathcal{O}_k$, the ring of integers in k, where $r = \dim A$. If K/k is a finite Galois extension with group G, a Lutz-Mattuck group A'_K in A_k can be chosen so that the isomorphism $A'_K \approx \mathcal{O}^r_K$ is a G-isomorphism. Using Herbrand's Quotient Q we conclude

(14) $$(H^1(G, A_K) : 0) = (H^0(G, A_K) : 0), \qquad \text{if } K/k \text{ is cyclic,}$$

because

$$Q(A_K) = Q(A'_K) = Q(\mathcal{O}_K)^r = 1 .$$

Let m be a natural number. For any abelian group X, let X_m denote the kernel of $X \xrightarrow{m} X$, and let $q(X) = (X : mX)/(X_m : 0)$ denote the 'trivial action' Herbrand quotient. We find

$$q(A_k) = q(A'_k) = q(\mathcal{O}_k)^r = \frac{1}{|m|^r_k},$$

where $|m|_k = (\mathcal{O}_k : m\mathcal{O}_k)^{-1}$ is the normed absolute value of m in k. Since $(A_m : 0) = m^{2r}$ we conclude

(15) $$(A_k : mA_k) = \left(\frac{m^2}{|m|_k}\right)^r, \quad \text{if } A_m \subset A_k .$$

The exact sequence $0 \to A_m \to A \xrightarrow{m} A \to 0$, in which A is to be interpreted as the group of points algebraic over k, gives rise to the cohomology sequence

$$0 \to A_m \cap A_k \to A_k \xrightarrow{m} A_k \xrightarrow{\delta} WC(A_m/k) \to WC(A/k) \xrightarrow{m} WC(A/k) \to \cdots$$

(cf. [6] for a proof that this exists and is exact for the injective limits). Hence, exactly,

(16) $$0 \to A_k/mA_k \to WC(A_m/k) \to WC_m(A/k) \to 0 .$$

Suppose now $A_m \subset A_k$, and $B_m \subset B_k$. Then the Galois group G_k of the algebraic closure of k operates trivially on A_m, and consequently we have

$$WC(A_m/k) \approx \text{Cont Hom}(G_k, A_m) .$$

This latter group is seen by the reciprocity law correspondence $G_k \to k^*$ of local class field theory to be isomorphic to $\text{Hom}(k^*/k^{*m}, A_m)$, whose order is $(k^* : k^{*m})^{2r}$ because $A_m \approx (\underset{\sim}{Z}/m\underset{\sim}{Z})^r$. Since $A_m \subset A_k$ and $B_m \subset B_k$, the **m-th** roots of unity are in k (cf. paragraph 5 below) and consequently $(k^* : k^{*m}) = m^2/|m|_k$. We conclude that the order of $WC(A_m/k)$ is $(m^2/|m|_k)^{2r}$. This fact, together with (15), (16), and the same results for B yields the equalities

$$(17)\qquad (WC_m(A/k) : 0) = \frac{m^2}{|m|_k} = (B_k : mB_k) \quad , \quad \text{if } A_m \subset A_k \text{ and } B_m \subset B_k .$$

5. Kummer theory.

Recall that the Kummer theory of the covering $B \xrightarrow{m} B$ yields a non-degenerate pairing $(b , a) \to e_m(b , a)$ of B_m and A_m ($= \hat{B}_m$) into the group of m-th roots of unity. (One takes α such that $S(\alpha) = a$, and puts $(g) = D(\alpha)$ where D is a Poincaré divisor. Then there is a function f on B such that $(f(u))^m = g(mu)$, and we have $e_m(b , a) = f(u + b)/f(u))$. LANG [5] has shown if $S(\alpha) = a$ and $S(\mathfrak{b}) = b$, then

$$(19)\qquad e_m(b , a) = \frac{D(m\alpha , \mathfrak{b})}{{}^tD(m\mathfrak{b} , \alpha)}$$

where D is any Poincaré divisor such that the right side is defined. Incidentally, the nondegeneracy of e_m shows that if $A_m \subset A_k$ and $B_m \subset B_k$, then the m-th roots of unity are in k , provided, of course, $r > 0$.

Using the non-degeneracy of e_m we can now prove the following lemma, which is our first indication that the pairing $\langle \alpha , b \rangle$ is non-trivial.

LEMMA 1. - Let m be a prime and suppose $A_m \subset A_k$ and $B_m \subset B_k$. If $b \in B_k$ is such that $\langle \alpha, b \rangle = 1$ for all $\alpha \in WC_m(A/k)$, then $b \in mB_k$.

PROOF, by contradiction. - Suppose $b \notin mB_k$. Select $b' \in B$ such that $mb' = b$. Then $b' \notin B_k$, so there is a k-automorphism σ such that $(\sigma - 1)b' \neq 0$. Hence there is an $a \in A_m$ such that $e_m((\sigma - 1)b' , a) \neq 0$. Choose $\alpha \in Z_k(A)$, $\mathfrak{b} \in Z_k(B)$ and $\mathfrak{b}' \in Z(B)$ representing a , b , and b' respectively, and put

$$c = D(m\alpha , \mathfrak{b}')\, {}^tD(\mathfrak{b} - m\mathfrak{b}' , \alpha) .$$

Using (19) one checks that $c^{\sigma - 1} = e_m((\sigma - 1)b' , a) \neq 1$, hence $c \notin k$. One the other hand, applying (3) to the cycles $m\alpha$ and $m\mathfrak{b}' - \mathfrak{b}$ we find that $c^m = D(m\alpha , \mathfrak{b})$. Since the m-th roots of unity are in k , we conclude that $D(m\alpha , \mathfrak{b}) \notin k^m$. From the existence theorem of local class field theory it follows that there is a cyclic extension K/k of degree m such that $D(m\alpha , \mathfrak{b})$ is not a norm from K .

Let τ be a generator of the Galois group G of K/k . The map $\tau^\nu \to \nu a$ is a 1-cocycle of G in A_K and represents a certain element $\alpha \in WC_m(A/k)$. To complete the proof of our lemma one uses the fact that $D(m\alpha , \mathfrak{b})$ is not a norm from K to show, by a routine cyclic cohomology computation, that $\mathcal{D}(\delta\alpha , b) \neq 0$, i.e. $\langle \alpha , b\rangle \neq 1$.

NOTATION. – Let m be a fixed prime natural number. If U and V are torsion groups and $h : U \to V$ a homomorphism we shall denote by $h(m) : U(m) \to V(m)$ the homomorphism induced by h on the m-primary components $U(m)$ and $V(m)$ of U and V. Similarly we shall denote by $h_m : U_m \to V_m$ the homomorphism induced by h on the elements of order m. Notice that injectivity of h_m implies that of $h(m)$.

Consider now our canonical homomorphism $h_k : WC(A/k) \to B_k^*$ which we are trying to show is bijective (cf.(13) at end of paragraph 3.). The following proposition is an encouraging beginning.

PROPOSITION 1. – <u>If</u> $A_m \subset A_k$ <u>and</u> $B_m \subset B_k$ <u>then</u> $(h_k)_m$ <u>is bijective and</u> $h_k(m)$ <u>is injective</u>.

PROOF. – The index computation (17) shows that the domain and range of

$$(h_k)_m : WC_m(A/k) \to (B^*{}_k)_m = (B_k/mB_k)^*$$

have the same number of elements, namely $(m^2/|m|_k)^r$. On the other hand, lemma 1 implies that $(h_k)_m$ is surjective. Thus $(h_k)_m$ is bijective, and consequently $h(m)$ is injective.

6. <u>Towers of cyclic extensions</u>.

For arbitrary finite Galois K/k with group G , let $h_{K/k}$ be the homomorphism such that the following diagram is commutative

$$\begin{array}{ccc} H^1(G, A_K) & \xrightarrow{\text{inf}} & WC(A/k) \\ {\scriptstyle h_{K/k}}\downarrow & & \downarrow{\scriptstyle h_k} \\ H^0(G, B_K)^* & \longrightarrow & B_k^* \end{array}$$

(Here the bottom row is dual to the canonical map $B_k \to (B_k/\mathrm{tr}\, B_K) = H^0(G , B_K))$. Similarly, let $\hat{h}_{K/k} : H^1(G , B_K) \to H^0(G , A_K)^*$ be the corresponding homomorphism obtained by interchanging the roles of A and B . (Recall that if $B = \hat{A}$, then $A = \hat{B}$, and if $D \subset A \times B$ is a Poincaré divisor then $\hat{D} = {}^tD \subset B \times A$ is also a Poincaré divisor).

LEMMA 2. – <u>If</u> $A_m \subset A_k$ <u>and</u> $B_m \subset B_k$ <u>then</u> $h_{K/k}(m)$ <u>and</u> $\hat{h}_{K/k}(m)$ <u>are bijective for cyclic</u> K/k .

PROOF. – $h_{K/k}(m)$ is injective because inflation is injective, $h_k(m)$ is injective (proposition 1), and (20) is commutative. Similarly $\hat{h}_{K/k}(m)$ is injective. On the other hand, the m-primary part of the index equality (14) shows that the domain of $h_{K/k}(m)$ has the same number of elements as the range of $\hat{h}_{K/k}(m)$, and similarly vice versa. The surjectivity of $h_{K/k}(m)$ and of $\hat{h}_{K/k}(m)$ now follows by counting.

LEMMA 3. – Suppose $k \subset K \subset L$ with K/k cyclic and L/k arbitrary finite Galois. Il $h_{K/k}(m)$, $\hat{h}_{K/k}(m)$, and $h_{L/K}(m)$ are bijective, then $h_{L/k}(m)$ is bijective.

PROOF. – We simply apply the five lemma to the m-primary part of the following diagram

$$\begin{array}{ccccccccccc}
0 \to & H^1(K/k, A) & \xrightarrow{\text{inf}} & H^1(L/k, A) & \xrightarrow{\text{res}} & [H^1(L/K, A)]^G & \xrightarrow{\text{tg}} & H^2(K/k, A) & \underset{\approx}{\overset{\sigma}{}} & H^0(K/k, A) \\
\downarrow & \downarrow h_{K/k} & & \downarrow h_{L/k} & & \downarrow h_{L/K} & & & & \downarrow \hat{h}^*_{K/k} \\
0 \to & H^0(K/k, B)^* & \to & H^0(L/k, B)^* & \to & [H^0(L/K, B)^*]^G & \to & H^{-1}(K/k, B)^* & \underset{\approx}{\overset{\sigma^{-1}}{}} & H^1(K/k, B)^*
\end{array}$$

in which the bottom row is dual to

$$0 \leftarrow B_k/\mathrm{tr}\, B_K \leftarrow B_k/\mathrm{tr}_{L/k}\, B_L \xleftarrow{\mathrm{tr}} [B_K/\mathrm{tr}_{L/K}\, B_L]_G \leftarrow \{b \in B_K \mid \mathrm{tr}\, b = 0\}/(\sigma - 1)B_K .$$

Here we have used the following notations :

$H^r(K/k, A) = H^r(G_{K/k}, A_K)$, etc. ;
inf = inflation from K to L ;
res = restriction from k to K ;
G = = cyclic Galois group of K/k ;
tg = transgression (cf. [4]) ;
σ = cyclic cohomology isomorphism lowering dimension by 2

corresponding to a chosen generator σ of G ;

tr = $\mathrm{tr}_{K/k}$ = trace from K to k ;
U^* = character group of U (as always, except for U = k).

The unlabled arrows are natural homomorphisms. It is well known that the top row is exact. The exactness of the bottom row follows from the trivially verifiable exactness of the sequence of which it is the dual. Commutativity of the first square is trivial. Commutativity of the second square follows from definitions, that of the third square from (11) ; that of the fourth square can be proved by cochain computations in which Lang's reciprocity law is used once more.

PROPOSITION 2. – If $A_m \subset A_k$ and $B_m \subset B_k$ then $h_{L/k}(m)$ is bijective for arbitrary finite Galois L/k.

PROOF. – Since local Galois groups are solvable this follows immediately by induction from lemmas 2 and 3.

7. <u>Surjectivity of</u> $h_k(m)$.

By imitating the proof of the existence theorem of local class field theory we can now prove

PROPOSITION 3. – $h_k(m)$ is surjective for arbitrary k.

PROOF. – We first treat the case $A_m \subset A_k$, $B_m \subset B_k$. By proposition 2, the image of $h_{L/k}(m)$ is the m-primary part of $(B_k/\mathrm{tr}_{L/k} B_L)^*$, for arbitrary finite Galois L/k. Since $h_k(m)$ is the inductive limit, for larger and larger L, of the isomorphisms $h_{L/k}(m)$, we conclude that the image of $h_k(m)$ is the m-primary part of $(B_k/U_k)^*$, where $U_k = \bigcap_L \mathrm{tr}_{L/k} B_L$ is the group of 'universal traces' in B_k. Surjectivity of $h_k(m)$ will therefore follow if we prove $U_k \subset \bigcap_{\nu=1}^{\infty} m^\nu B_k$.

In any case, we know from the surjectivity of $(h_k)_m$ (proposition 1) that $(B_k/mB_k)^*$ is in the image of $h_k(m)$. Hence $U_k \subset mB_k$, and by the same token $U_K \subset mB_K$ for each finite extension K of k. On the other hand I contend $U_k \subset \mathrm{tr}_{K/k} U_K$ for each such K. Namely, if $b \in U_k$, the sets $\mathrm{tr}_{K/k}^{-1}(b) \cap \mathrm{tr}_{L/K}(B_L)$ are compact and have the finite intersection property, as L ranges over all finite extensions of K. We now know $U_k \subset \mathrm{tr}_{K/k} U_K \subset \mathrm{tr}_{K/k} mU_k = m\mathrm{tr}_{K/k} U_K$, for each K. Thus, for each $b \in U_k$, the compact (finite) sets $\frac{1}{m}b \cap \mathrm{tr}_{K/k} U_K$ have the finite intersection property, and this shows finally that $U_k \subset mU_k$, and consequently $U_k \subset m^\nu B_k$ for $\nu = 1, 2, 3, \ldots$ as we wanted to show.

Now let k be arbitrary, and let $K = k(A_m, B_m)$. The diagram

$$\begin{array}{ccc} WC(A/K) & \xrightarrow{\mathrm{tr}} & WC(A/k) \\ {\scriptstyle h_K}\downarrow & & \downarrow{\scriptstyle h_k} \\ B_K^* & \xrightarrow{\mathrm{res}^*} & B_k^* \end{array}$$

is commutative by (12). Moreover res^* is surjective because it is dual to the injective inclusion $\mathrm{res} : B_k \to B_K$. We have just proved the surjectivity of $h_K(m)$ because $A_m \subset A_K$ and $B_m \subset B_K$, and the surjectivity of $h_k(m)$ follows.

8. Conclusion of the demonstration.

We now know that $h_k(m)$ is surjective for all $\mathfrak{p}$-adic k over which A is defined (proposition 3) and that $h_k(m)$ is injective for those k such that $A_m \subset A_k$ and $B_m \subset B_k$ (proposition 1). In order finally to get rid of A_m and B_m we prove

LEMMA 4. – Suppose K/k cyclic, group G. If $h_K(m)$ and $\hat{h}_K(m)$ are injective, then $h_k(m)$ and $\hat{h}_k(m)$ are injective.

PROOF. – Chasing around the following exact and commutative diagram

$$\begin{array}{ccccccc}
0 \to H^1(G, A_K) & \to & WC(A/k) & \xrightarrow{\text{res}} & WC(A/K) \\
\downarrow h_{K/k} & & \downarrow h_k & & \downarrow h_K \\
0 \to H^0(G, B_K)^* & \longrightarrow & B_k^* & \longrightarrow & B_K^*
\end{array}$$

we find that $h_{K/k}(m)$ is surjective because $h_k(m)$ is surjective and $h_K(m)$ injective. Similarly, transposing A and B, we find $\hat{h}_{K/k}(m)$ is surjective. Just as in the proof of lemma 2 it now follows from the index equality (14) that $h_{K/k}(m)$ and $\hat{h}_{K/k}(m)$ are injective as well. Chasing around the diagram again we see that the injectivity of $h_k(m)$ follows now from that of $h_K(m)$ and that of $h_{K/k}(m)$. Similarly for $\hat{h}_k(m)$.

Now climbing down in cyclic steps from $k(A_m, B_m)$ to k, we see that $h_k(m)$ is bijective for each k. Since m was an arbitrary prime we have proved our

THEOREM. – h_k is bijective for all $\mathfrak{p}$-adic fields of definition k of A; we have $WC(A/k) \approx (\hat{A}_k)^*$ canonically.

For an arbitrary finite (not necessarily Galois) extension E/k, let $WC(A/k, E)$ denote the kernel of $\text{res} : WC(A/k) \to WC(A/E)$; it is easy to see that this kernel is isomorphic to the group of classes of principal homogeneous spaces over A, rational over k, and having a rational point in E.

COROLLARY 1. – $WC(A/k, E) \approx (A_k/\text{tr}\ A_E)^*$ canonically.

PROOF. – The kernel of res is dual to the cokernel of tr, by (11).

9. Applications to generalized Picard varieties and idele classes.

Let X be a complete non-singular variety and let A be the Picard variety of X . Suppose we are given a finite set of points $x_0 , \dots , x_n$ on X , to each of which there is assigned a zero-dimensional ideal $\mathfrak{n}_i$ in the local ring O_i of x_i on X . We can use these data, just as in the case X is a curve, to construct exact sequences

(21) $$0 \to E_{\mathfrak{n}} \to A_{\mathfrak{n}} \to A \to 0$$

(22) $$0 \to G_m \to \prod_{i=0}^{n} U_i/(1+\mathfrak{n}_i) \to E_{\mathfrak{n}} \to 0$$

where $A_{\mathfrak{n}}$ is the group of divisors algebraically equivalent to zero and not meeting any of the points x_i on X , modulo the divisors of functions f on X such that $f - 1 \in \mathfrak{n}_i$ for each i , and where U_i is the group of units in O_i . Presumably, one can endow $A_{\mathfrak{n}}$ with an algebraic group structure and thereby define generalized Picard varieties of X . However for the following cohomological considerations the algebraic structure is of course inessential.

Let now $b_1 , \dots , b_n$ be distinct non-zero points on an abelian variety B and apply the preceding construction to the case X = B , $x_0 = 0$, $x_i = b_i$ for $i > 0$, and, $\mathfrak{n}_i = \mathfrak{m}_i$ = the maximal ideal in O_i for each i . We obtain an exact sequence (21) in which A = B and in which $E_{\mathfrak{n}} \approx \prod_{i=1}^{n} M_i$, where $M_i = U_i/(1+\mathfrak{m}_i)$ is a copy of the multiplicative group G_m for each $i > 0$.

If k is any field of definition for B , and $b_i \in B_k$, then the part of (21) rational over the separable closure of k leads to an exact sequence

(23) $$0 \to WC(A_{\mathfrak{n}}/k) \to WC(A/k) \xrightarrow{\delta} \sum_{i=1}^{n} Br_i(k) ,$$

and one readily verifies that for $\alpha \in WC(A/k)$ we have $\delta\alpha = \sum_{i=1}^{n} (\alpha , b_i)$.

For $\mathfrak{p}$-adic k , we conclude from the main theorem that $WC(A_{\mathfrak{n}}/k)$ is isomorphic to $(B_k/F)^*$, where F is the closure of the subgroup of B_k generated by our chosen elements b_i , and in particular we have $WC(A_{\mathfrak{n}}/k) = 0$ if the b_i generate an everywhere dense subgroup of B_k .

Finally, let Γ be an algebraic curve of genus $g > 0$ with rational point in k and apply this result to the case B = A = J = the Jacobian of Γ . Take only sets of points b_i which lie on the canonical image of Γ in J, and which break up into prime rational 0-cycles $\mathfrak{q}$ over k . By taking such b_i in sufficient number so that the points $S(\mathfrak{q})$ generate B_k we can prove the third underlined statement in the introduction to this exposé , namely that $WC(C/k) = 0$, where C is the group of idele classes on Γ . The idea is that C is the inverse limit of the generalized Jacobians of Γ and these generalized Jacobians are isomorphic to the generalized Picard varieties $A_{\mathfrak{n}} = J_{\mathfrak{n}}$ of J which are defined by modules $\mathfrak{n}$ whose support lies in the canonical image of Γ in J. One can also deduce that $WC(C/k) = 0$ by working entirely in the function field of Γ and showing that the map $WC(C/k) \to WC(J/k)$ is an injection whose image is the kernel of

$$h_k : WC(J/k) \to J_k^* .$$

10. Higher dimensional cohomology groups.

After writing paragraph 1-8, I realized that the cohomological pairing (paragraph 2) can be generalized. For finite Galois K/k with group G one pair $\alpha \in H^p(G, A_K)$ and $\beta \in H^q(G, B_K)$ into $(\alpha, \beta) \in H^{p+q+1}(G, K^*)$ for arbitrary integers p and q in the following way. Take a p-cochain $\mathfrak{a}$ of G in $X_K(A)$ and a q-cochain $\mathfrak{b}$ of G in $X_K(B)$ such that $S(\mathfrak{a})$ is a cocycle representing α and $S(\mathfrak{b})$ is a cocycle representing β ; then define (α, β) as the class of the $(p + q + 1)$ cocycle

$$c = D(\delta\mathfrak{a} \cup \mathfrak{b}) / {}^tD(\delta\mathfrak{b} \cup \mathfrak{a})^{(-1)^p}$$

(Here $\cup$ denote cup product with respect to $\otimes$, and D has been extended into $Y(A) \otimes Z(B)$ by linearity so that $D(\mathfrak{y} \otimes \mathfrak{z}) = D(\mathfrak{y}, \mathfrak{z})$, and similarly for ${}^tD$). Lang's reciprocity law (3) shows that we have in fact $c = (D/{}^tD)(S(\mathfrak{a} \cup \mathfrak{b}))$, with suitable definitions, and hence that (6) should be replaced by some notation like

$$\gamma = (\alpha, \beta) = \mathfrak{D}(S(\alpha \cup \beta)) .$$

The validity of (7) , (8) , and (9) for all p , q is now obvious, following from the corresponding rule for the cup product and the commutativity of tr and res with δ .

For $\mathfrak{p}$-adic k and $B = \hat{A}$ we have therefore canonical maps

$$h^p_{K/k} : H^p(G, A_K) \to [H^{1-p}(G, B_K)]^*$$

which generalize the map $h^1_{K/k} = h_{K/k}$ of (20). The natural conjecture that h^p is bijective for all p can probably be proved as follows ; From the main theorem $B_K^* \approx WC(A/K)$ we find

(24) $$[H^{1-p}(G, B_K)]^* = H^{p-2}(G, B_K^*) = H^{p-2}(G, WC(A/K)) .$$

Now it is not unreasonable to seek homomorphisms

$$t^{p-2}_{K/k} : H^{p-2}(G, H^1(A/K)) \to H^p(G, A_K)$$

for which one can prove that $h^p \circ t^{p-2} = \pm 1$ and $t^{p-2} \circ h^p = \pm 1$, if we identify the extremes of (24). For example, t^o induces the transgression used in proving lemma 3, and in general, the t^p in question should be related to the d_2 in the spectral sequence [4] associated with the group extension $G_{K/k} = G_k/G_K$.

BIBLIOGRAPHIE

[1] CARTAN (H.) and EILENBERG (S.). - Homological algebra. - Princeton, Princeton University Press, 1956.

[2] CHÂTELET (François). - Méthode galoisienne et courbes de genre 1, Ann. Univ. Lyon, 3e série, Section A, t.89, 1946, p. 40-49.

[3] CHEVALLEY (Claude). - Class field theory. - Nagoya, Nagoya University, 1953-1954.

[4] HOCHSCHILD (G.) and SERRE (J.-P.). - Cohomology of group extensions, Trans. Amer. math. Soc., t. 74, 1953, p. 110-134.

[5] LANG (Serge). - Reciprocity and correspondences on abelian varieties (to appear).

[6] LANG (S.) and TATE (J.). - On the groups of Châtelet-Weil (to appear).

[7] MATTUCK (Arthur). - Abelian varieties over p-adic ground fields, Annals of Math., Series 2, t. 62, 1955, p. 92-119.

[8] WEIL (André). - On algebraic groups and homogeneous spaces, Amer. J. Math., t. 77, 1955, p. 493-512.

[9] WEIL (André). - The field of definition of a variety, Amer. J. Math., t. 78, 1956, p. 509-524.

[10] WITT (Ernst). - Zerlegung reeler algebraischer Functionen in Quadrate, Schiefkörper über reellem Functionenkörper, J. für reine und ang. Math., t. 171, 1934, p. 4-11.