ANNALES SCIENTIFIQUES DE L'É.N.S.

J. S. MILNE

Weil-Châtelet groups over local fields

Annales scientifiques de l'É.N.S. 4e série, tome 3, nº 3 (1970), p. 273-284
<http://www.numdam.org/item?id=ASENS_1970_4_3_3_273_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 3, 1970, p. 273 à 284.

WEIL-CHÂTELET GROUPS OVER LOCAL FIELDS

BY J. S. MILNE.

Let K be a local field (i. e. a field which is locally compact for the topology defined by a non-trivial discrete valuation) and let A be an abelian variety over K with Picard variety $\hat{A}$. Tate has defined a continuous pairing of the group of K-rational points on A with the Weil-Châtelet group of $\hat{A}$ into the Brauer group of K, and has proved ([12], [13]) that this pairing is non-degenerate except possibly on the p-primary components of the groups when K has characteristic $p > 0$. We will show that it is always non-degenerate irrespective of the characteristic, when A has potential good reduction.

If A does not have potential good reduction, but is an elliptic curve, then Tate's theory of the p-adic theta functions gives a description of the rational points on A and this enabled Shatz [11] to prove the non-degeneracy in this case also. Thus, the non-degeneracy of the pairing is now completely proved for elliptic curves, and it is to be hoped that, once the appropriate generalization of Tate's description of the rational points is proved, then the non-degeneracy in general will follow from the case proved in this paper.

One immediate consequence of our results is that Lichtenbaum's solution of the period-index problem for elliptic curves [5] holds over any local field.

NOTATION. — K is a local field with separable algebraic closure $\overline{K}$ and ring of integers R. All group schemes are commutative. $H^i(R, -)$ and $H^i(K, -)$ refer to cohomology with respect to the flat (f. p. q. f.) topology on spec R and spec K (if G is a smooth group scheme, then its flat cohomology groups can be computed using the étale topology [1] and, in particular, $H^i(K, -)$ can be identified with the usual Galois cohomology groups). If Z is an abelian group, then Z_m is the subgroup of elements killed by m and $Z(p)$ is the p-primary component of Z.

$\hat{N}$ denotes the Cartier dual of a finite flat group scheme N and Z^* the Pontryagin dual of a locally compact abelian group Z.

Let A be an abelian variety over K, and consider the exact sequences,

$$0 \to Y(A) \to Z(A) \xrightarrow{S} A(\overline{K}) \to 0,$$
$$0 \to Y(\hat{A}) \to Z(\hat{A}) \xrightarrow{S} \hat{A}(\overline{K}) \to 0,$$

where $Z(A)$ and $Z(\hat{A})$ are the groups of zero cycles of degree zero on $A_{\overline{K}}$ and $\hat{A}_{\overline{K}}$ respectively, and S denotes summation of points on A or $\hat{A}$. A Poincaré divisor D on $A \times \hat{A}$ and its transpose ${}^tD$ on $\hat{A} \times A$ define pairings

$$Y(A) \times Z(\hat{A}) \to \overline{K}^*,$$
$$Z(A) \times Y(\hat{A}) \to \overline{K}^*,$$

which agree on $Y(A) \times Y(\hat{A})$ [12]. Hence ([4], chap. V) there are augmented cup products

$$H^r(K, A) \times H^{1-r}(K, \hat{A}) \to H^2(K, \mathbf{G}_m) \approx \mathbf{Q}/\mathbf{Z}.$$

Moreover, for $r = 0, 1$, these are continuous with respect to the canonical compact topology on H^0 and the discrete topology on H^1.

THEOREM. — *(a) The above pairings*

$$H^r(K, A) \times H^{1-r}(K, \hat{A}) \to \mathbf{Q}/\mathbf{Z}$$

are non-degenerate for $r = 0, 1$, except possibly on the p-primary components of the groups when p is the characteristic of K *and* A *is not isogenous to a product of elliptic curves and abelian varieties with potential good reduction.*

(b) $$H^r(K, A) = 0 \quad \text{for} \quad r \geq 2.$$

The pairing defined above for $(A, \hat{A})$ is compatible with that for $(\hat{A}, \hat{\hat{A}})$ in the sense that

$$\begin{array}{ccccc} H^r(K, A) & \times & H^{1-r}(K, \hat{A}) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \downarrow & & \downarrow & & \| \\ H^r(K, \hat{\hat{A}}) & \times & H^{1-r}(K, \hat{A}) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \end{array}$$

commutes up to sign (the first vertical arrow is induced by the canonical isomorphism $A \to \hat{\hat{A}}$). Thus, to prove part (a) of the theorem, it suffices to show that the map

$$\theta_K(A): \quad H^1(K, A) \to \hat{A}(K)^*$$

induced by the first pairing is an isomorphism.

For any positive integer m, there is an exact commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/mA(K) & \longrightarrow & H^1(K, A_m) & \longrightarrow & H^1(K, A)_m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \theta_K(A)_m} & & \\ 0 & \longrightarrow & H^1(K, \hat{A})^*_m & \longrightarrow & H^1(K, \hat{A}_m)^* & \longrightarrow & (\hat{A}(K)/m\hat{A}(K))^* & \longrightarrow & 0 \end{array}$$

where the rows come from the cohomology sequences of

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

and

$$0 \to \hat{A}_m \to \hat{A} \xrightarrow{m} \hat{A} \to 0$$

the two end vertical arrows are induced by the pairings in the theorem, and the middle arrow is induced by cup products from the e_m-pairing $A_m \times \hat{A}_m \to \mathbf{G}_m$. The commutativity of the diagram may be checked directly by using the definition of the e_m-pairing (e. g. [3], p. 173) and the explicit descriptions of cup products. The middle arrow is an isomorphism ([13], th. 2.1; [10], th. 5), and so $\theta_K(A)_m$ is surjective for all m. Since

$$H^1(K, A) = \cup H^1(K, A)_m \quad \text{and} \quad \hat{A}(K) = \varprojlim (\hat{A}(K)/m\hat{A}(K)),$$

this shows that

$$\theta_K(A) : \ H^1(K, A) \to \hat{A}(K)^*$$

is surjective.

This is already sufficient to prove part (b) of the theorem, for consider the exact commutative diagram

$$\begin{array}{ccccccc} H^1(K, A) & \longrightarrow & H^2(K, A_m) & \longrightarrow & H^2(K, A)_m & \longrightarrow & 0 \\ \downarrow{\scriptstyle \theta_K(A)} & & \downarrow & & \downarrow & & \\ \hat{A}(K)^* & \longrightarrow & \hat{A}_m(K)^* & \longrightarrow & 0 & & \end{array}$$

which is just a continuation to the right of the previous diagram. We have seen that the first vertical arrow is surjective, and the middle arrow is an isomorphism by ([13]; [10], *loc. cit.*). A diagram chase now shows that $H^2(K, A)_m = 0$ for all m and this suffices to show that $H^2(K, A) = 0$. Note finally that $H^r(K, A) = 0$ for $r > 2$ because K has strict cohomological dimension 2 [13].

To prove part (a), it remains to show that

$$\theta_K(A) : \ H^1(K, A) \to \hat{A}(K)^*$$

is injective, and for this it suffices to show that, for all primes p, the map

$$\theta_K(A)_p : \ H^1(K, A)_p \to (\hat{A}(K)/p\hat{A}(K))^*$$

is injective.

To do this when $p \neq \mathrm{char}(K)$. Tate used the following counting argument. Let $M = A(\overline{K})_p$. Then,

$$\chi(M) = \frac{1}{(R : pR)^{2d}} = \chi(\hat{M}) \quad ([9], \text{II-35}).$$

From the known structure of $A(K)$ (*see* [6]),

$$\frac{[A(K)/pA(K)]}{[A(K)_p]} = (R : pR)^d = \frac{[\hat{A}(K)/p\hat{A}(K)]}{[\hat{A}(K)_p]}.$$

By considering the cohomology sequence of

$$0 \to M \to A(\overline{K}) \xrightarrow{p} A(\overline{K}) \to 0$$

one gets easily that

$$[H^1(K, A)_p] = [\hat{A}(K)/p\hat{A}(K)],$$

and so the surjectivity of $\theta_K(A)_p$ implies its injectivity.

This argument fails when $p = \mathrm{char}(K)$ because the groups involved are not finite (nor even compact).

Lemma 1. — *If for some finite Galois extension* L *of* K, $\theta_L(A)$ *is injective, then* $\theta_K(A)$ *is injective.*

Proof. — Since K is local, the Galois group G of L over K is soluble, and so we may assume it to be cyclic. There is an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(G, A(L)) \arrow[r] \arrow[d] & H^1(K, A) \arrow[r] \arrow[d, "\theta_K(A)"] & H^1(L, A)^G \arrow[r] \arrow[d, "\theta_L(A)"] & \check{H}^0(G, A(L)) \arrow[r] \arrow[d] & H^2(K, A) = 0 \\
0 \arrow[r] & \check{H}^0(G, \hat{A}(L))^* \arrow[r] & \hat{A}(K)^* \arrow[r] & \hat{A}(L)^{*G} \arrow[r] & H^1(G, \hat{A}(L))^* \arrow[r] & 0
\end{tikzcd}$$

($\check{H}^0$ denotes Tate cohomology [8], p. 136) in which the first vertical arrow is induced by $\theta_K(A)$ and the fourth vertical arrow is the dual of the map induced in the same way by $\theta_K(\hat{A})$. The diagram can be obtained from the diagram in [12] (lemma 3) by passing to the direct limit over the fields denoted there by L.

From the right hand end of the diagram we get that

$$\check{H}^0(G, A(L)) \to H^1(G, \hat{A}(L))^*$$

is an isomorphism and, from the same diagram with A and $\hat{A}$ interchanged, we get that

$$\check{H}^0(G, \hat{A}(L)) \to H^1(G, A(L))^*$$

is an isomorphism. This shows that the first vertical arrow is an isomorphism, and hence that $\theta_K(A)$ is an isomorphism.

LEMMA 2. — *If* A *and* B *are isogenous abelian varieties over* K, *and* $\theta_K(A)$ *is an isomorphism, then* $\theta_K(B)$ *is also an isomorphism.*

Proof. — Let N be the kernel of an isogeny $\varphi : A \to B$. The cohomology sequences of

$$o \to N \to A \xrightarrow{\varphi} B \to o$$

and

$$o \to \hat{N} \to \hat{B} \xrightarrow{\hat{\varphi}} \hat{A} \to o$$

give an exact commutative diagram

$$\begin{tikzcd}
H^1(K, N) \arrow[r] \arrow[d] & H^1(K, A) \arrow[r] \arrow[d, "\theta_K(A)"] & H^1(K, B) \arrow[r] \arrow[d, "\theta_K(B)"] & H^2(K, N) \arrow[r] \arrow[d] & o \\
H^1(K, \hat{N})^* \arrow[r] & \hat{A}(K)^* \arrow[r] & \hat{B}(K)^* \arrow[r] & \hat{N}(K)^* \arrow[r] & o
\end{tikzcd}$$

in which all vertical arrows are induced by cup products or augmented cup products. By [13], [10] or assumption, all the vertical arrows are isomorphisms except possibly $\theta_K(B)$, and it follows that $\theta_K(B)$ must be an isomorphism.

After these two lemmas and theorem 1 of Shatz [11] we may assume in proving (a) that A has good reduction over K. Thus, we are reduced to proving the statement : let A be an abelian variety with good reduction over K, where K has characteristic p. Then, after possibly replacing K by a finite separable extension,

$$\theta_K(A)_p : \quad H^1(K, A)_p \to (\hat{A}(K)/p\,\hat{A}(K))^*$$

is injective.

To say that A has good reduction over K means that there is an abelian scheme $\mathcal{A}$ over the ring of integers R in K whose generic fibre is A. There is an exact sequence over R,

$$o \to \mathcal{A}_p \to \mathcal{A} \xrightarrow{p} \mathcal{A} \to o$$

where $\mathcal{A}_p$ is a finite flat group scheme over R with $\mathcal{A}_p \otimes_R K = A_p$. By ([1], th. 11.7; [2]) $H^i(R, \mathcal{A}) = o$ for $i > o$ and so, from the cohomology sequences of the above short exact sequence and the corresponding sequence over K, we get an exact commutative diagram

$$\begin{tikzcd}
\mathcal{A}(R) \arrow[r, "p"] \arrow[d] & \mathcal{A}(R) \arrow[r] \arrow[d] & H^1(R, \mathcal{A}_p) \arrow[rr] \arrow[d, "\iota(\mathcal{A}_p)"] & & o \arrow[d] \\
A(K) \arrow[r, "p"] & A(K) \arrow[r] & H^1(K, A_p) \arrow[r] & H^1(K, A)_p \arrow[r] & o
\end{tikzcd}$$

in which the vertical arrows are the maps induced on cohomology by the morphism $\mathrm{spec}(K) \to \mathrm{spec}(R)$. The first two vertical arrows are isomorphisms, and so the image of the map $\iota(\mathcal{A}_p)$ in $H^1(K, A_p)$ is equal to the image of $A(K)$ in $H^1(K, A_p)$. Similarly, the image of $\iota(\hat{\mathcal{A}}_p)$ in $H^1(K, \hat{A}_p)$ is equal to the image of $\hat{A}(K)$, and so, to complete the proof of the theorem, we have only to show that $\mathrm{im}(\iota(\mathcal{A}_p))$ is the exact annihilator of $\mathrm{im}(\iota(\hat{\mathcal{A}}_p))$ in the non-degenerate cup product pairing

$$H^1(K, A_p) \times H^1(K, \hat{A}_p) \to H^2(K, \mathbf{G}_m).$$

To do this, we first need to examine the structure of $\mathcal{A}_p$. After possibly replacing K by a finite separable extension, A_p will have a composition series all of whose quotients have rank p [10]. The following easy lemma shows that the same will then be true of $\mathcal{A}_p$.

Lemma 3. — *Let* $\mathcal{N}$ *be a finite flat group scheme over* R, *let* $N = \mathcal{N} \otimes_R K$, *and let*

$$0 \to N' \to N \to N'' \to 0$$

be an exact sequence of finite group schemes over K. *Then there is a unique exact sequence of finite flat group schemes over* R,

$$0 \to \mathcal{N}' \to \mathcal{N} \to \mathcal{N}'' \to 0,$$

whose generic fibre is the first sequence.

We will also need the following lemma of Tate.

Lemma 4. — *For any pair* $a, b \in R$ *with* $ab = 0$, *define* $R_{a,b}$ *to be the* R-*algebra* $\dfrac{R[f]}{f^p - af}$ *and*

$$\delta : \quad R_{a,b} \to R_{a,b} \otimes_R R_{a,b}$$

to be the R-*algebra homomorphism with*

$$\delta(f) = f \otimes 1 + 1 \otimes f + b \sum_{\substack{i+j=p \\ 0<i,j<p}} \frac{f^i \otimes f^j}{i!\,j!}.$$

Then, with respect to the multiplication induced by δ, $\mathcal{N}_{a,b} = \mathrm{spec}\, R_{a,b}$ *is a flat group scheme of rank p over* R *and any flat group scheme of rank p over* R *is isomorphic to such an* $\mathcal{N}_{a,b}$. $\mathcal{N}_{a,b}$ *is isomorphic to* $\mathcal{N}_{a',b'}$ *if and only if there is a unit u in* R *such that*

$$a' = u^{p-1} a, \qquad b' = u^{1-p} a.$$

Proof. — *See* [14].

It follows that we may assume that $\mathcal{C}_p$ has a composition series whose quotients are of the form $\mathcal{N}_{a,b}$. In fact we may assume more. Let $K = k((t))$ (so $R = k[[t]]$). If $a \neq 0$ then $b = 0$, and $a = ut^c$ (say) where u is a unit in R. After the adjunction of a $(p-1)$st root of u and a $(p-1)$st root of t to K, $\mathcal{N}_{a,b}$ becomes isomorphic to $\mathcal{N}_{a',0}$ where a' is of the form $t^{(p-1)c}$. A similar argument applies when $b \neq 0$. Thus, we may assume that $\mathcal{C}_p$ has a composition series over R, each of whose quotients is of the form $\mathcal{N}_{t^{(p-1)c},0}$, $\mathcal{N}_{0,0}$ or $\mathcal{N}_{0,t^{(p-1)c}}$.

Lemma 5. — *Let $\mathcal{N}$ be one of the group schemes $\mathcal{N}_{t^{(p-1)c}}$, $\mathcal{N}_{0,0}$, or $\mathcal{N}_{0,t^{(p-1)c}}$ over* R, *and let $N = \mathcal{N} \otimes_R K$. Then the image of $\iota(\mathcal{N})$ in $H^1(K, N)$ is the exact annihilator of the image of $\iota(\hat{\mathcal{N}})$ in $H^1(K, \hat{N})$ under the cup product pairing*

$$H^1(K, N) \times H^1(K, \hat{N}) \to H^2(K, \mathbf{G}_m).$$

Proof. — The commutativity of the diagram

$$(\star)\qquad \begin{array}{ccccc} H^1(R, \mathcal{N}) & \times & H^1(R, \hat{\mathcal{N}}) & \longrightarrow & H^2(R, \mathbf{G}_m) = 0 \\ \downarrow{\scriptstyle \iota(\mathcal{N})} & & \downarrow{\scriptstyle \iota(\hat{\mathcal{N}})} & & \downarrow \\ H^1(K, N) & \times & H^1(K, \hat{N}) & \longrightarrow & H^2(K, \mathbf{G}_m) \end{array}$$

shows that $\mathrm{im}(\iota(\mathcal{N}))$ and $\mathrm{im}(\iota(\hat{\mathcal{N}}))$ do annihilate each other. [$H^2(R, \mathbf{G}_m) = 0$ because, by ([1], th. 11.7), $H^2(R, \dot{\mathbf{G}}_m) = H^2(k, \mathbf{G}_m) = 0$]. Let $\mathcal{N} = \mathcal{N}_{0,0}$. Then $\mathcal{N} = \boldsymbol{\alpha}_p$ and $\hat{\mathcal{N}} = \boldsymbol{\alpha}_p$. There are exact sequences

$$0 \to \boldsymbol{\alpha}_p \to \mathbf{G}_a \xrightarrow{F} \mathbf{G}_a \to 0$$

over R and K, and their cohomology sequences give a commutative diagram

$$\begin{array}{ccccccc} R & \xrightarrow{F} & R & \longrightarrow & H^1(R, \boldsymbol{\alpha}_p) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \iota(\boldsymbol{\alpha}_p)} & & \\ K & \xrightarrow{F} & K & \longrightarrow & H^1(K, \boldsymbol{\alpha}_p) & \longrightarrow & 0 \end{array}$$

in which $F(a) = a^p$. Hence the diagram $(\star)$ with $\mathcal{N}$ replaced by $\boldsymbol{\alpha}_p$ can be canonically identified with the diagram,

$$\begin{array}{ccccc} R/R^p & \times & R/R^p & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow \\ K/K^p & \times & K/K^p & \longrightarrow & \mathbf{Q}/\mathbf{Z} \end{array}$$

in which the vertical arrows are induced by the inclusion of R in K and the lower pairing is induced by the pairing $K \times K \to \mathbf{F}_p \subset \mathbf{Q}_p/\mathbf{Z}_p$ such that $(f, g) \mapsto \mathrm{tr}_{k/\mathbf{F}_p} \mathrm{res}(f dg)$ (*see* [10], p. 433). It is now easy to check that R/R^p and R/R^p, i. e. $\mathrm{im}(\iota(\boldsymbol{\alpha}_p))$ and $\mathrm{im}(\iota(\hat{\boldsymbol{\alpha}}_p))$, are exact annihilators of each other in the lower pairing.

Let $\mathcal{N} = \mathcal{N}_{t^c(p-1),\,0}$. In this case $\hat{\mathcal{N}} = \mathcal{N}_{0,\,t^c(p-1)}$. There is a homomorphism $\psi : \mathcal{N}_{1,\,0} \to \mathcal{N}$ which, for any ring $R' \supset R$, gives the map

$$(a \mapsto t^c a) : \quad \mathcal{N}_{1,\,0}(R') \to \mathcal{N}(R')$$

and whose dual $\hat{\psi} : \hat{\mathcal{N}} \to \mathcal{N}_{0,\,1}$ gives the map

$$(a \mapsto t^c a) : \quad \hat{\mathcal{N}}(R') \to \mathcal{N}_{0,\,1}(R').$$

$\mathcal{N}_{1,\,0}$ is the étale group scheme $\mathbf{Z}/p\mathbf{Z}$ and $\mathcal{N}_{0,\,1}$ is $\boldsymbol{\mu}_p$ (although that is not the usual representation of $\boldsymbol{\mu}_p$). ψ and $\hat{\psi}$ give isomorphisms ψ_K and $\hat{\psi}_K$ on the generic fibres.

From the exact sequences

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \xrightarrow{\mathfrak{p}} \mathbf{G}_a \to 0,$$
$$0 \longrightarrow \boldsymbol{\mu}_p \longrightarrow \mathbf{G}_m \xrightarrow{F} \mathbf{G}_m \to 0$$

we get isomorphisms

$$\delta : \quad K/\mathfrak{p}K \to H^1(K, \mathbf{Z}/p\mathbf{Z}),$$
$$\delta' : \quad K^*/K^{*p} \to H^1(K, \boldsymbol{\mu}_p).$$

Thus there are isomorphisms

$$\varphi : \quad K/\mathfrak{p}K \to H^1(K, N), \qquad \varphi = \psi_K \circ \delta,$$
$$\varphi' : \quad K^*/K^{*p} \to H^1(K, \hat{N}), \qquad \varphi' = \hat{\psi}_K^{-1} \circ \delta',$$

where we have used ψ_K and $\hat{\psi}_K$ to denote also the maps induced by ψ_K and $\hat{\psi}_K$ on the cohomology groups. In terms of these isomorphisms, the pairing

$$H^1(K, N) \times H^1(K, \hat{N}) \to \mathbf{Q}/\mathbf{Z}$$

can be described as follows (*see* [10], p. 444) : let $a \in H^1(K, N)$ and let $f \in K$ be such that $\varphi(\bar{f}) = a$, where $\bar{f}$ denotes the residue class of f in $K/\mathfrak{p}K$; let $b \in H^1(K, \hat{N})$ and let $g \in K^*$ be such that $\varphi'(\bar{g}) = b$, where $\bar{g}$ denotes the residue class of g in K^*/K^{*p}; then

$$\langle a, b \rangle = \mathrm{tr}_{k/\mathbf{F}_p}\,\mathrm{res}\left(f\frac{dg}{g}\right) \in \mathbf{F}_p \subset \mathbf{Q}/\mathbf{Z}.$$

We shall now explicitly compute $\varphi^{-1}(\mathrm{im}(\iota(\mathcal{N})))$. There is an exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & \mathbf{G}_a & \xrightarrow{\mathfrak{p}} & \mathbf{G}_a & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \\
0 & \longrightarrow & \mathcal{N} & \longrightarrow & \mathbf{G}_a & \xrightarrow{\mathfrak{p}_c} & \mathbf{G}_a & \longrightarrow & 0
\end{array}$$

where (on points) $\mathfrak{p}_c$ is the map $a \mapsto a^p - t^{c(p-1)}a$, α_1 is the map $a \mapsto t^c a$ and α_2 is the map $a \mapsto t^{cp}a$. This yields commutative diagrams,

$$\begin{array}{ccc} R/\mathfrak{p}R & \xrightarrow{\partial} & H^1(R, \mathbf{Z}/p\mathbf{Z}) \\ {\scriptstyle\alpha_2}\downarrow & & \downarrow{\scriptstyle\psi} \\ R/\mathfrak{p}_c R & \longrightarrow & H^1(R, \mathfrak{N}) \end{array} \qquad \begin{array}{ccc} K/\mathfrak{p}K & \xrightarrow{\partial} & H^1(K, \mathbf{Z}/p\mathbf{Z}) \\ {\scriptstyle\alpha_2}\downarrow & & \downarrow{\scriptstyle\psi_K} \\ K/\mathfrak{p}_c K & \longrightarrow & H^1(K, N) \end{array}$$

which are compatible in an obvious sense. It follows that

$$\begin{aligned} \varphi^{-1}(\operatorname{im}(\iota(\mathfrak{N}))) &= t^{-cp}(\partial^{-1}\operatorname{im}(\iota(\mathbf{Z}/p\mathbf{Z}))) = t^{-cp}(R/\mathfrak{p}R) \\ &= t^{-cp}R/((t^{-cp}R) \cap \mathfrak{p}K). \end{aligned}$$

Before we can compute $\varphi'^{-1}(\operatorname{im}(\iota(\hat{\mathfrak{N}})))$ we must give an explicit description of $\partial' : K^*/K^* \to H^1(K, \boldsymbol{\mu}_p)$. For any element a of a ring containing R, we will write

$$l(a) = a - \frac{a^2}{2} + \frac{a^3}{3} - \ldots - \frac{a^{p-1}}{p-1}$$

and

$$e(a) = 1 + a + \frac{a^2}{2!} + \ldots + \frac{a^{p-1}}{(p-1)!}.$$

There is an exact sequence over R,

$$0 \to \boldsymbol{\mu}_p \xrightarrow{\varepsilon} \mathbf{G}_m \xrightarrow{F} \mathbf{G}_m \to 0,$$

where (on points) ε is the map $a \mapsto e(a)$ and F is the map $a \mapsto F(a) = a^p$. If $a \in \mathbf{G}_m(R')$, R′ some ring containing R, and $F(a) = 1$, then $a = e(l(a-1))$.

$H^1(K, \boldsymbol{\mu}_p)$ can be identified with the Čech cohomology group $H^1(K_1/K, \boldsymbol{\mu}_p)$ where $K_1 = k((s))$, $s^p = t$ ([10], prop. 13). Since

$$C^0(K_1/K, \boldsymbol{\mu}_p) = \boldsymbol{\mu}_p(K_1) = 0,$$

$H^1(K_1/K, \boldsymbol{\mu}_p)$ is a subgroup of

$$C^1(K_1/K, \boldsymbol{\mu}_p) = \boldsymbol{\mu}_p(K_1 \otimes_K K_1).$$

An element of this last group is a sum, $\sum(a_i \otimes b_i)$, a_i, $b_i \in K_1$, such that

$$\sum(a_i^p \otimes b_i^p) = \left(\sum a_i^p b_i^p\right) \otimes 1 = 0.$$

Hence, in the isomorphism $(a \otimes b \mapsto a^p \otimes b^p)$: $K_1 \otimes_K K_1 \to K \otimes_{K^p} K$, $\boldsymbol{\mu}_p(K_1 \otimes_K K_1)$ maps into the ideal I of $K \otimes_{K^p} K$ which is the kernel of the map $(a \otimes b \mapsto ab) : K \otimes_K pK \to K$. There is an isomorphism

$$(a \otimes b \mapsto a\,db) : \quad I/I^2 \to \Omega^1_{K/k},$$

where $\Omega^1_{K/k}$ denotes the module of Kähler differentials of K/k. By composing these maps we get an injection $\nu : C^1(K_1/K, \boldsymbol{\mu}_p) \to \Omega^1_{K/k}$. We now claim that the diagram

$$\begin{tikzcd} H^1(K, \boldsymbol{\mu}_p) \subset C^1(K_1/K, \boldsymbol{\mu}_p) \arrow[d, "\nu"] \\ K^*/K^{*p} \arrow[u, "\delta'"] \arrow[r, "d\log"] & \Omega^1_{K/k} \end{tikzcd}$$

commutes, where $d\log(\bar{f}) = \dfrac{df}{f}$ if $\bar{f}$ is the residue class of $f \in K^*$ in K^*/K^{*p}. Indeed, let $a \in K^*$ and choose $a_1 \in K_1^*$ such that $a_1^p = a$; then $\delta'(\bar{a}) = l(a_1^{-1} \otimes a_1 - 1 \otimes 1)$ and $\nu(\delta'(\bar{a})) = \dfrac{da}{a}$.

A principal homogeneous space for a finite flat group scheme over R which has a point in K_1 clearly already has a point in R_1, the integral closure of R in K_1. It follows that, in particular, $H^1(R, \boldsymbol{\mu}_p)$ and $H^1(R, \hat{\mathcal{N}})$ may be identified with the Čech cohomology groups $H^1(R_1/R, \boldsymbol{\mu}_p)$ and $H^1(R_1/R, \hat{\mathcal{N}})$ respectively. Thus there is a commutative diagram with exact rows,

$$\begin{tikzcd} 0 \arrow[r] & H^1(R, \hat{\mathcal{N}}) \arrow[r] \arrow[d, "\hat{\varphi}"] & C^1(R_1/R, \hat{\mathcal{N}}) \arrow[r] \arrow[d] & C^2(R_1/R, \hat{\mathcal{N}}) \arrow[d] \\ 0 \arrow[r] & H^1(R, \boldsymbol{\mu}_p) \arrow[r] \arrow[d, "\iota(\boldsymbol{\mu}_p)"] & C^1(R_1/R, \boldsymbol{\mu}_p) \arrow[r] \arrow[d] & C^2(R_1/R, \boldsymbol{\mu}_p) \arrow[d] \\ 0 \arrow[r] & H^1(K, \boldsymbol{\mu}_p) \arrow[r] & C^1(K_1/K, \boldsymbol{\mu}_p) \arrow[r] & C^2(K_1/K, \boldsymbol{\mu}_p) \end{tikzcd}$$

in which all the vertical arrows are injective. It follows that,

$$d\log(\delta'^{-1}\operatorname{im}(\iota(\boldsymbol{\mu}_p))) = d\log(K^*/K^{*p}) \cap R\, dt$$

and

$$d\log(\varphi'^{-1}\operatorname{im}(\iota(\hat{\mathcal{N}}))) = d\log(K^*/K^{*p}) \cap (t^{cp}R)\, dt.$$

Finally, it is an easy calculation to show that

$$t^{-cp}R/((t^{-cp}R) \cap pK) \quad \text{and} \quad d\log(K^*/K^{*p}) \cap (t^{cp}R\, dt)$$

are exact annihilators of each other in the pairing

$$K/pK \times d\log(K^*/K^{*p}) \to \mathbf{F}_p$$
$$(f, \omega) \mapsto \operatorname{tr}_{k/\mathbf{F}_p}\operatorname{res}(f\omega).$$

The case with $\mathcal{N} = \mathcal{N}_{0, t^c(p-1)}$ follows, by symmetry, from the above result. This completes the proof of lemma 5.

Let $\mathcal{A}_p = \mathcal{N}_{2d} \supset \mathcal{N}_{2d-1} \supset \ldots \supset \mathcal{N}_0 = 0$ be a composition series of $\mathcal{A}_p$, each of whose quotients is of the form $\mathcal{N}_{t^c(p-1), 0}$, $\mathcal{N}_{0,0}$ or $\mathcal{N}_{0, t^c(p-1)}$. We claim that $H^r(R, \mathcal{N}_j) = 0$ for $r > 1$ and all j. Indeed, $\mathcal{N}_j$ is a subgroup scheme of $\mathcal{A}$, and the quotient sheaf $\mathcal{A}'$ is representable by an abelian scheme over R (*cf.* [7]). By ([1], th. 11.7; [2])

$$\mathrm{H}^r(\mathrm{R}, \mathcal{A}) = 0 = \mathrm{H}^r(\mathrm{R}, \mathcal{A}')$$

for $r > 0$, and so $\mathrm{H}^r(\mathrm{R}, \mathcal{N}_j) = 0$ for $r > 1$. $\hat{\mathcal{N}}_j$ fits into a short exact sequence

$$0 \to \widehat{\mathcal{A}_p/\mathcal{N}_j} \to \hat{\mathcal{A}}_p \to \hat{\mathcal{N}}_j \to 0$$

in which $\widehat{\mathcal{A}_p/\mathcal{N}_j}$ and $\hat{\mathcal{A}}_p$ are subgroup schemes of $\hat{\mathcal{A}}$, and so also $\mathrm{H}^r(\mathrm{R}, \hat{\mathcal{N}}_j) = 0$ for $r > 1$.

We are now in a position to complete the proof of the theorem. Lemma 5 shows that $\mathrm{im}(\iota(\mathcal{N}_1))$ is the exact annihilator of $\mathrm{im}(\iota(\hat{\mathcal{N}}_1))$ in

$$\langle\ ,\ \rangle :\quad \mathrm{H}^1(\mathrm{K}, \mathrm{N}_1) \times \mathrm{H}^1(\mathrm{K}, \hat{\mathrm{N}}_1) \to \mathbf{Q}/\mathbf{Z}.$$

We shall assume that $\mathrm{im}(\iota(\hat{\mathcal{N}}_j))$ is the exact annihilator of $\mathrm{im}(\iota(\mathcal{N}_j))$ and prove that the same holds for $\mathcal{N}_{j+1}$.

Consider the exact commutative diagrams,

$$\begin{tikzcd}
\mathrm{H}^1(\mathrm{R}, \mathcal{N}_j) \arrow[r] \arrow[d, "\iota(\mathcal{N}_j)"] & \mathrm{H}^1(\mathrm{R}, \mathcal{N}_{j+1}) \arrow[r] \arrow[d, "\iota(\mathcal{N}_{j+1})"] & \mathrm{H}^1(\mathrm{R}, \mathcal{N}_{j+1}/\mathcal{N}_j) \arrow[r] \arrow[d, "\iota(\mathcal{N}_{j+1}/\mathcal{N}_j)"] & \mathrm{H}^2(\mathrm{R}, \mathcal{N}_j) = 0 \arrow[d] \\
\mathrm{H}^1(\mathrm{K}, \mathrm{N}_j) \arrow[r, "\beta_0"] & \mathrm{H}^1(\mathrm{K}, \mathrm{N}_{j+1}) \arrow[r, "\beta_1"] & \mathrm{H}^1(\mathrm{K}, \mathrm{N}_{j+1}/\mathrm{N}_j) \arrow[r] & \mathrm{H}^2(\mathrm{K}, \mathrm{N}_j)
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[d] & \mathrm{H}^1(\mathrm{R}, \hat{\mathcal{N}}_j) \arrow[l] \arrow[d, "\iota(\hat{\mathcal{N}}_j)"] & \mathrm{H}^1(\mathrm{R}, \hat{\mathcal{N}}_{j+1}) \arrow[l] \arrow[d, "\iota(\hat{\mathcal{N}}_{j+1})"] & \mathrm{H}^1(\mathrm{R}, \widehat{\mathcal{N}_{j+1}/\mathcal{N}_j}) \arrow[l] \arrow[d, "\iota(\widehat{\mathcal{N}_{j+1}/\mathcal{N}_j})"] \\
\mathrm{H}^2(\mathrm{K}, \widehat{\mathrm{N}_{j+1}/\mathrm{N}_j}) & \mathrm{H}^1(\mathrm{K}, \hat{\mathrm{N}}_j) \arrow[l] & \mathrm{H}^1(\mathrm{K}, \hat{\mathrm{N}}_{j+1}) \arrow[l, "\gamma_0"'] & \mathrm{H}^1(\mathrm{K}, \widehat{\mathrm{N}_{j+1}/\mathrm{N}_j}) \arrow[l, "\gamma_1"']
\end{tikzcd}$$

Let $a \in \mathrm{H}^1(\mathrm{K}, \mathrm{N}_{j+1})$, and suppose that $\langle a, b \rangle = 0$ for all $b \in \mathrm{im}(\iota(\hat{\mathcal{N}}_{j+1}))$. We must show that $a \in \mathrm{im}(\iota(\mathcal{N}_{j+1}))$.

$$\langle \beta_1(a), b \rangle = \langle a, \gamma_1(b) \rangle = 0 \qquad \text{for all} \quad b \in \mathrm{im}(\iota(\widehat{\mathrm{N}_{j+1}/\mathrm{N}_j}))$$

and so, by lemma 5, $\beta_1(a) \in \mathrm{im}(\iota(\mathcal{N}_{j+1}/\mathcal{N}_j))$. There is an $a' \in \mathrm{im}(\iota(\mathcal{N}_{j+1}))$ such that $\beta_1(a') = \beta_1(a)$ and so, after subtracting a' from a, we may assume that $a \in \ker(\beta_1)$. Thus, $a = \beta_0(a'')$ for some $a'' \in \mathrm{H}^1(\mathrm{K}, \mathrm{N}_j)$. If $b \in \mathrm{im}(\iota(\hat{\mathcal{N}}_j))$, there exists $ab' \in \mathrm{im}(\iota(\hat{\mathcal{N}}_{j+1}))$ such that $\gamma_0(b') = b$, and so $\langle a'', b \rangle = \langle a, b' \rangle = 0$. Thus $a'' \in \mathrm{im}(\iota(\mathcal{N}_j))$, and the proof is complete.

Corollary. — *If* V *is a principal homogeneous space for the elliptic curve* A *over a local field* K, *then the period of* V *equals its index.*

Proof. — This was proved by Lichtenbaum [5] for local fields of characteristic 0, but exactly the same proof works in non-zero characteristic once one has the above theorem.

REFERENCES.

[1] A. Grothendieck, *Le groupe de Brauer* III, Dix exposés sur la cohomologie des schémas, North-Holland, Amsterdam; Masson, Paris, 1968.
[2] S. Lang, *Algebraic groups over finite fields* (*Amer. J. Math.*, vol. 78, 1956, p. 555-563).
[3] S. Lang, *Abelian varieties*, Interscience Tracts, No. 7, New York, Interscience, 1959.
[4] S. Lang, *Rapport sur la cohomologie des groupes*, New York, Benjamin, 1966.
[5] S. Lichtenbaum, *The period-index problem for elliptic curves* (*Amer. J. Math.*, vol. 90, 1968, p. 1209-1223).
[6] A. Mattuck, *Abelian varieties over p-adic ground fields* (*Ann. of Math.*, vol. 62, 1955, p. 92-119).
[7] M. Raynaud, *Passage au quotient par une relation d'équivalence plate* (*Proceedings of a conference on local fields*, Berlin-Heidelberg-New York, Springer, 1967).
[8] J.-P. Serre, *Corps locaux* (*Act. Sci. Ind.*, No. 1296, Paris, 1962).
[9] J.-P. Serre, *Cohomologie galoisienne* (*Lecture Notes in Math.*, No. 5, Berlin-Heidelberg-New York, Springer, 1964).
[10] S. Shatz, *Cohomology of artinian group schemes over local fields* (*Ann. of Math.*, vol. 79, 1964, p. 411-449).
[11] S. Shatz, *The cohomology of certain elliptic curves over local and quasi-local fields* (*Illinois J. of Math.*, vol. 11, 1967, p. 234-241).
[12] J. Tate, W. C.-*groups over* P-*adic fields* (Séminaire Bourbaki, 1957-1958, exposé 156).
[13] J. Tate, *Duality theorems in Galois cohomology over number fields* (*Proc. Intern. Congress Math.*, Stockholm, 1962, p. 288-295).
[14] J. Tate and F. Oort, *Group schemes of prime order* (*Ann. scient. Éc. Norm. Sup.*, t. 3, fasc. 1, 1970, p. 1-21).

(Manuscrit reçu le 22 mai 1970.)

J. S. Milne,
Department of Mathematics,
University of Michigan,
Ann Arbor,
Mich., 48104, U. S. A.