Canonical Height Pairings via Biextensions

B. Mazur and J. Tate

To I.R. Shafarevich

The object of this paper is to present the foundations of a theory of p-adic-valued height pairings

$$(*) \qquad A(K) \times A'(K) \to \mathbb{Q}_p,$$

where A is a abelian variety over a global field K, and A' is its dual. We say "pairings" in the plural because, in contrast to the classical theory of $\mathbb{R}$-valued) canonical height, there may be many canonical p-adic valued pairings: as we explain in § 4, up to nontrivial scalar multiple, they are in one-to-one correspondence with $\mathbb{Z}_p$-extensions L/K whose ramified primes are finite in number and are primes of ordinary reduction (1.1) for A.

When A also has good reduction at the primes of ramification for L/K, then a different method, introduced by Schneider (cf. [22] for the case of the cyclotomic $\mathbb{Z}_p$-extension) enables one to associate to L/K a p-adic valued pairing (*). We show this to be the same as our pairing.

Our method for the construction of the pairing is first to express the duality between A and A' via the "canonical biextension" of (A, A') by $\mathbb{G}_m$, and then to develop a theory of "canonical local splittings" of biextensions. Our pairings are then defined in a manner analogous to Bloch's definition of the classical $\mathbb{R}$-valued pairing. Whereas for Bloch it suffices to split certain local extensions, to obtain uniqueness we must ask for an especially coherent family of splittings of the local extensions, i.e., a splitting of the local biextension.

We treat simultaneously the $\mathbb{R}$-valued and p-adic valued theories, and express our results in a "uniform" manner in terms of the notion of a Y-valued canonical pairing for a general value group Y satisfying some axioms.

The connection between biextensions and heights is, to be sure, not surprising.

Firstly, Zarhin [24] pointed out that arbitrary (not necessarily canonical) splittings of the canonical biextension are equivalent to Néron type pairings between zero cycles and divisors.

Secondly, biextensions have been used to define theta (and sigma-) functions, as is explained of Breen [5] and in a manuscript in preparation by

Norman [19]. Both of these authors point out that, although the concept of biextensions is not explicitly mentioned in the theories of p-adic theta functions of Mumford, and of Barsotti [2] (see also Cristante [6]) it is directly related to these theories (via the theorem of the cube). One might also try to relate Néron's approach to p-adic theta functions [16], [17], [18] directly to biextensions.

Thirdly, the theory of p-adic heights for elliptic curves of complex multiplication (and p a prime of ordinary reduction) has been developed by Perrin-Riou [20] and Bernardi [4], using a p-adic version of the sigma-function. Here the p-adic sigma-function plays a role analogous to that of the classical sigma-function in Néron's theory [15] for archimedean primes.

Néron has also developed a theory of p-adic valued height pairings using his p-adic theta functions [18]. In the case of elliptic curves of complex multiplication, an explicit connection between Néron's definition and Bernardi's has not yet been made (to our knowledge). What is the relation (if any) between Néron's p-adic height and ours?

Since the explicit expression for the local terms of our canonical p-adic pairing involves the canonical p-adic theta functions (of Mumford and Barsotti), we would find it useful to have a practical algorithm for computing these functions. In a subsequent paper we will discuss this issue in the case of elliptic curves.

In this connection, one should also note that the beginnings of a (mod p)-valued theory of height for general elliptic curves (with ordinary reduction at p) can be found in [21].

Our construction of p-adic valued canonical heights requires ordinary reduction at the primes of ramification of the chosen $\mathbb{Z}_p$-extension. Can one find a generalization or replacement of our construction valid for all $\mathbb{Z}_p$-extensions? For elliptic curves with complex multiplication, B. Gross has some ideas on this; see J. Oesterlé, *Construction de hauteurs archimédiennes et p-adiques suivant la méthode de Bloch*, p. 175–192, in Séminaire de Theorie des Nombres (Séminaire Delange-Pisot-Poitou), Paris, 1980–81; Progress in Math., Vol. 22, Birkhäuser Boston, Basel, Stuttgart, 1982.

We are grateful to M. Artin, L. Breen, J. Coates, L. Moret-Bailly, P. Norman and B. Perrin-Riou for pleasant and informative conversations concerning algebraic spaces, biextensions, theta-functions, and p-adic heights.

We also thank O. Gabber for providing us with significant help in working out §5.

§ 1. Local Splittings

Let K be a field complete with respect to a place v which is either archimedean or discrete. If v is discrete, let $\mathfrak{o} = \mathfrak{o}_K$ denote the ring of v-integers in K, π a prime element in $\mathfrak{o}$ and $k = \mathfrak{o}/\pi\mathfrak{o}$ the residue field.

If $A_{/K}$ is an abelian variety over K, and v is discrete, we denote by A (or sometimes: $A_{/\mathfrak{o}}$) the Néron model of $A_{/K}$ over $\mathfrak{o}$. If v is archimedean, we let A denote $A_{/K}$.

In the non-archimedean case, A^o (or $A^o_{/\mathfrak{o}}$) denotes the connected component of zero in A, i.e., the open subgroupscheme of $A^o_{/\mathfrak{o}}$ whose closed fiber A^o_0 is connected. If $U_{/\mathfrak{o}}$ is any scheme over $\mathfrak{o}$, its closed fiber $U \times_{\mathfrak{o}} k$ is denoted U_0.

(1.1) Ordinary abelian varieties.

A and $A_{/K}$ are called *ordinary* if v is discrete, the characteristic of k is $\neq 0$, and the special fiber of A satisfies the following equivalent conditions.

(i) The formal completion A_0^f of A_0 at the origin is of multiplicative type, i.e., is isomorphic to a product of copies of $\mathbb{G}_m^f$ over the algebraic closure $\overline{k}$ of k.

(ii) For $p = \operatorname{char} k$, the connected component of the kernel of the homomorphism $p\colon A^o_0 \longrightarrow A^o_0$ is the dual of an étale group scheme over k.

(iii) A^o_0 is an extension of an ordinary abelian variety by a torus T_A.

If L/K is a finite field extension and $A_{/K}$ is ordinary, so is $A_{/L}$ and formation of A^o commutes with the base change of rings $\mathfrak{o}_K \to \mathfrak{o}_L$.

If $A_{/K}$ is ordinary, then $A_{/K}$ has good reduction over k (equivalently: $A_{/\mathfrak{o}}$ is an abelian scheme) if an only if $T_A = 0$.

(1.2) Exponents.

By the *exponent* of a finite abelian group G we mean the smallest integer $m > 0$ such that $mG = 0$.

In this paragraph, suppose that v is discrete. Let $m_A = m_{A/K}$ denote the exponent of $A_0(k)/A^o_0(k)$. Now suppose that k is finite. Let T_A denote the "maximal torus" in A_0 which exists by, e.g., [SGA 3] exposé XIV, Thm. 1.1. Let $n_A = n_{A/K}$ denote the exponent of $A^o_0(k)/T_A(k)$.

We refer to the numbers m_A and n_A as the *exponents* of A.

The exponents are sensitive to isogenous change of A.

As for their dependence on the base field K, $m_{A/K'}$ admits a finite upper bound for all finite *unramified extensions* K'/K, while $n_{A/K'}$ is independent of K' provided A is ordinary and K'/K is a finite *totally ramified extension*. If we drop the assumption that A be ordinary, then $n_{A/K'}$ admits a finite upper bound for all finite totally ramified extensions K'/K.

(1.3) Biextensions and paired abelian varieties.

For an introduction to the concept of biextension, we suggest reading §2 and §3 of [12]. For a fuller treatment of this notion, see exposés VII and VIII of [SGA 7I]. A useful and pleasantly written introduction to this fuller treatment may be found in the first $5\frac{1}{2}$ pages of §1 of [5].

Let $A'_{/K}$ denote the dual of $A_{/K}$ and $E^{A}_{/K}$ the canonical biextension of $(A_{/K}, A'_{/K})$ by $\mathbb{G}_{m/K}$ expressing the duality ([SGA 7 I] Exposé VII, 2.9). If v is archimedean, let E^A denote the canonical biextension $E^{A}_{/K}$. If v is discrete, let E^A (or $E^{A}_{/\mathcal{O}}$) denote the canonical biextension of (A^o, A') by $\mathbb{G}_{m/\mathcal{O}}$, i.e., the unique such biextension whose general fiber is $E^{A}_{/K}$ (whose existence and uniqueness follow from [SGA 7 I] Exposé VII, 7.1b).

If $B_{/K}$ is any abelian variety, to give a biextension $E_{/K}$ of $(A_{/K}, B_{/K})$ by $\mathbb{G}_{m/K}$ is equivalent to giving a K-homomorphism $\lambda: B_{/K} \longrightarrow A'_{/K}$ (and $E_{/K}$ is the pullback of $E^{A}_{/K}$ by $(1, \lambda)$), or to giving a K-homomorphism $\lambda': \longrightarrow A_{/K} B'_{/K}$ (the dual of λ).

Again, if v is archimedean, let E denote $E_{/K}$, while if v is discrete, E (or $E_{/\mathcal{O}}$) will denote the pullback of $E^{A}_{/\mathcal{O}}$, viewed as biextension of (A^o, B) by $\mathbb{G}_{m/\mathcal{O}}$.

The abelian varieties $A_{/K}, B_{/K}$ will be said to be *paired*, if a biextension $E_{/K}$ of $(A_{/K}, B_{/K})$ by $\mathbb{G}_{m/K}$ (equivalently: a K-homomorphism $\lambda: B_{/K} \longrightarrow A'_{/K}$) is fixed.

In what follows, we suppose $A_{/K}, B_{/K}$ are paired abelian varieties over K, with $E_{/K}$ the biextension expressing the pairing.

In all cases, archimedean or non-archimedean, the set $E(K)$ of points of E with coordinates in K is a set theoretical biextension of the groups $(A(K), B(K))$ by $\mathbb{G}_m(K) = K^*$. Our aim is to introduce canonical splittings of biextensions obtained from this one via various types of homomorphisms $\rho: K^* \longrightarrow Y$.

(1.4) ρ-splittings

Let U, V, W, and Y be abelian groups, X a biextention of (U, V) by W and ρ: $W \longrightarrow Y$ a homomorphism. A *ρ-splitting* of X is a map

$$\psi: X \longrightarrow Y$$

such that

(i) $\psi(w + x) = \rho(w) + \psi(x)$ for $w \in W$, $x \in X$.

(ii) For each $u \in U$ (resp. $v \in V$) the restriction of ψ to ${}_uX$ (resp. X_v) is a group homomorphism.

(Here ${}_uX$ (resp. X_v) denotes the part of X above $\{u\} \times V$ (resp. $U \times \{v\}$) and is a group extension of V (resp. U) by W.) Note that we are expressing the action of W on X additively. We will continue to do so even when $W = \mathbb{G}_m$.

(1.5) Canonical ρ-splittings.

Let Y be an abelian group and ρ: $K^* \longrightarrow Y$ a homomorphism.

Theorem. *There exists a canonical ρ-splitting*[1]

$$\psi_\rho: E(K) \longrightarrow Y,$$

in the following three cases:

(1.5.1) *v is archimedean and $\rho(c) = 0$ for c such that $|c|_v = 1$.*

(1.5.2) *v is discrete, ρ is unramified (i.e., $\rho(\mathfrak{o}^*) = 0$), and Y is uniquely divisible by m_A.*

(1.5.3) *v is discrete, k is finite. A is ordinary, and Y is uniquely divisible by $m_A m_B n_A n_B$.*

If both (1.5.2) and (1.5.3) hold, they yield the same ψ_ρ.

The image of ψ_ρ satisfies the following inclusion relations:

$$\psi_\rho(E(K)) \subset \begin{cases} \rho(K^*) & \text{in case (1.5.1)} \\ \frac{1}{m_A}\rho(K^*), & \text{in case (1.5.2)} \\ \frac{1}{m_A}\rho(K^*) + \frac{1}{m_A m_B n_A n_B}\rho(\mathfrak{o}^*), & \text{in case (1.5.3).} \end{cases}$$

---

[1]The properties characterizing this ρ-splitting uniquely are explained in (1.9) below.

Before beginning the proof of the theorem, we give some lemmas on set-theoretical biextensions. Let U, V, W and X be as in (1.4), i.e., X a biextension of (U, V) by W. For integers m and n we define a map

$$(m, n)\colon X \longrightarrow X$$

which for each $(u, v) \in U \times V$ takes the fiber ${}_uX_v$ of X over (u, v) to the fiber ${}_{mu}X_{nv}$. The map $(m, 1)$ is defined as multiplication by m in the group X_v for each $v \in V$, the map $(1, n)$ is defined as multiplication by n in the group ${}_uX$ for each $u \in U$, and finally,

$$(m, n) \stackrel{\text{defn}}{=} (m, 1) \circ (1, n) = (1, n) \circ (m, 1);$$

the commutativity of $(1, n)$ and $(m, 1)$ results from the compatibility axiom for the two laws of composition in a biextension. We have the rules

$$(m_1, n_1)(m, n) = (m_1 m, n_1 n)$$

and

$$(m, n)(x + w) = (m, n)x + mn\, w \qquad \text{for } w \in W.$$

If $\rho\colon W \longrightarrow Y$ is a homomorphism and ψ is a ρ-splitting, then

$$\psi\big((m, n)x\big) = mn\, \psi(x).$$

In particular, if Y is uniquely divisible by m and n, then we have

$$\psi(x) = \frac{1}{mn}\psi\big((m, n)x\big).$$

This leads to

(1.6) Lemma. *Suppose U^o and V^o are subgroups of U and V, and that m and n are integers > 0 such that $mU \subset U^o$ and $nV \subset V^o$. Let X^o be the part of X lying over $U^o \times V^o$ and let $\rho\colon W \longrightarrow Y$ be a homomorphism of W into a group Y which is uniquely divisible by mn. Then a ρ-splitting $\psi_o\colon X^o \longrightarrow Y$ extends uniquely to a ρ-splitting ψ of X.*

Indeed $(m, n)X \subset X^o$. Hence, if ψ extends ψ_o we must have

$$\psi(x) = \frac{1}{mn}\psi_o\big((m, n)x\big).$$

On the other hand, it is easy to check that this formula defines a ρ-splitting ψ on all of X, if ψ_o is a ρ-splitting of X^o.

Another case of unique extendibility of ρ-splittings is given by

(1.7) Lemma. *Suppose W' is a subgroup of W and X' a subset of X such that X' is a biextension of (U,V) by W'. Let ρ: $W \longrightarrow Y$ be a homomorphism and let $\rho' = \rho \mid W'$. A ρ'-splitting ψ' of W' extends uniquely to a ρ-splitting ψ of W.*

Let $W = \bigcup_i (w_i + W')$ be the expression of W as disjoint union of cosets of W'. Then $X = \bigcup (w_i + X')$ is a disjoint union because this is true on each fiber over $U \times V$. If $x = w_i + x' \in w_i + X'$ and ψ extends ψ', we must have

$$\psi(x) = \rho(w_i) + \psi'(x').$$

On the other hand, it is easy to check that this formula defines a ρ-splitting ψ of X, if ψ' is a ρ'-splitting of X'.

(1.8) Proposition. *Suppose U and V are compact topological abelian groups and X a topological biextension of (U,V) by $\mathbb{R}$, such that the projection pr: $X \longrightarrow U \times V$ has local sections. Then X has a unique continuous splitting ψ: $X \longrightarrow \mathbb{R}$.*

Since the space of points of a projective variety over a locally compact field is compact, an immediate consequence of 1.8 is:

(1.8.1) Corollary. *Define v: $K^* \longrightarrow \mathbb{R}$ by $v(x) = -\log|x|$. If K is locally compact, then $E(K)$ has a unique v-splitting which is continuous from the v-topology in $E(K)$ to the usual topology in $\mathbb{R}$.*

Proof of 1.8. Since the projection $X \to U \times V$ has continuous local sections and its fiber is real affine 1-space, we can use a partition of unity of $U \times V$ to obtain a continuous global section s: $U \times V \longrightarrow X$.

Unicity: If ψ_1 and ψ_2 are two splittings, then $(\psi_1 - \psi_2) \circ s$ is a continuous biadditive map of $U \times V$ into $\mathbb{R}$. The image of such a map is bounded and closed under multiplication by 2, so is 0.

Existence: Define $f_0 \colon X \longrightarrow \mathbb{R}$ by

$$f_0(x) = x - s(pr(x)).$$

It is easy to check that

$$\psi(x) \overset{\text{defn}}{=} \lim_{n \to \infty} \frac{1}{2^n}\big(f_0(2^n, 1)x\big) \overset{\text{thm.}}{=} \lim_{n \to \infty} \frac{1}{2^n} f_0\big((1, 2^n)x\big)$$

is the desired splitting.

(1.9) Reduction of the theorem of (1.5) to §5.
We treat the three cases separately.

Case (1.5.1). (v is archimedean and $\rho(c) = 0$ if $|c|_v = 1$.) Then $K = \mathbb{R}$ or $\mathbb{C}$, and the homomorphism $v \colon K^\bullet \longrightarrow \mathbb{R}$ defined by $v(c) = -\log|c|$ is surjective. Since $\rho(c)$ depends only on $v(c)$, it follows that there is a (unique) homomorphism $\rho_1 \colon \mathbb{R} \longrightarrow Y$ such that $\rho(c) = \rho_1(v(c))$ for $c \in K^\bullet$. We put then

$$\psi_\rho(x) = \rho_1(\psi_v(x)) \qquad \text{for } x \in E(K),$$

where

$$\psi_v \colon E(K) \longrightarrow \mathbb{R}$$

is the *unique v-splitting of $E(K)$ which is continuous* (cf. 1.8.1). Clearly, $\psi_\rho(E(K)) \subset \rho(K^\bullet)$.

Case (1.5.2). (v is discrete, ρ is unramified (i.e., $\rho(\mathfrak{o}^\bullet) = 0$), and Y is uniquely divisible by m_A). Since $A^o(\mathfrak{o})$ is the subgroup of $A(\mathfrak{o}) = A(K)$ consisting of those points $P \in A(\mathfrak{o})$ whose reduction mod π is contained in $A^o(k)$, we have $m_A \cdot A(K) \subset A^o(\mathfrak{o})$. Let $E^o(K)$ denote that part of $E(K)$ which lies over $A^o(\mathfrak{o}) \times B(K)$. We have then a tower of three biextensions as follows:

$$\begin{array}{ccccc}
\mathfrak{o}^\bullet & \subset & K^\bullet & = & K^\bullet \\
\cap & & \cap & & \cap \\
E(\mathfrak{o}) & \subset & E^o(K) & \subset & E(K) \\
\downarrow & & \downarrow & & \downarrow \\
A^o(\mathfrak{o}) \times B(\mathfrak{o}) & = & A^o(\mathfrak{o}) \times B(K) & \subset & A(K) \times B(K)
\end{array}$$

Since $\rho(\mathfrak{o}^\bullet) = 0$, the constant function 0 (i.e., neutral element in Y) is a $(\rho \mid \mathfrak{o}^\bullet)$-splitting of $E(\mathfrak{o})$. Applying (1.7) with $W' = \mathfrak{o}^\bullet$ and $W = K^\bullet$, then

(1.6) with $U^\circ = A^\circ(\mathfrak{o})$, $U = A(K)$, $V = V^\circ = B(K)$, we see that this $(\rho \mid \mathfrak{o}^*)$-splitting of $E(\mathfrak{o})$ extends uniquely to $E(K)$. We can therefore, and do, define in this case ψ_ρ to be the *unique ρ-splitting of $E(K)$ such that $\rho(E(\mathfrak{o})) = 0$.*

Looking at the explicit constructions in the proofs of (1.7) and (1.6) we find that for $x \in E(K)$ there is a unique integer ν such that $(m,1)x \in \pi^\nu + E(\mathfrak{o})$, where $m = m_A$, and for this ν we have

$$\psi(x) = \frac{1}{m}\psi((m,1)x) = \frac{\nu}{m}\rho(\pi) \in \frac{1}{m}\rho(K^*).$$

Case (1.5.3). (v is discrete, k is finite, A is ordinary, and Y is uniquely divisible by $m_A n_A m_B n_B$.) Let T_A and T_B denote the maximal tori in the special fibers of A and B respectively. Let A^t (resp. B^t) denote the formal completion of A (resp. B) along the torus T_A (resp. T_B), and let E^t denote the formal completion of E along the inverse image of $T_A \times T_B$ in E. Then E^t is a biextension (in the category of formal group schemes over $\hat{\mathfrak{o}}$) of (A^t, B^t) by $\hat{\mathbb{G}}_m$. (Here $\hat{\mathfrak{o}}$ denotes $\mathfrak{o}$ viewed as adic-ring. See the technical description of adic-rings in §5. The formal spectrum of $\hat{\mathfrak{o}}$ is denoted by $\hat{S}$. By $\hat{\mathbb{G}}_m$ we mean the formal completion of $\mathbb{G}_{m/\mathfrak{o}}$ along its special fiber $\mathbb{G}_{m/k}$.) Since A is ordinary, it follows from 5.11.1 or 5.12 below that the formal group scheme biextension E^t has a unique splitting, $\psi: E^t \longrightarrow \hat{\mathbb{G}}_m$. Taking points with coordinates in $\hat{\mathfrak{o}}$ we obtain a canonical splitting $\psi_{\mathfrak{o}}: E^t(\hat{\mathfrak{o}}) \longrightarrow \hat{\mathbb{G}}_m(\hat{\mathfrak{o}}) = \mathfrak{o}^*$ of the set-theoretic biextension $E^t(\hat{\mathfrak{o}})$ of $\big(A^t(\hat{\mathfrak{o}}), B^t(\hat{\mathfrak{o}})\big)$ by $\mathfrak{o}^*$, and we define in this case ψ_ρ to be the *unique ρ-splitting of $E(K)$ such that $\psi_\rho \mid E^t(\mathfrak{o}) = \rho \circ \psi_{\mathfrak{o}}$.* Again, the existence and uniqueness of such a ρ-splitting follows from (1.6) and (1.7), once we note (cf. (5.1.1)) that $A^t(\hat{\mathfrak{o}})$ (resp. $B^t(\hat{\mathfrak{o}})$) is the subgroup of points $P \in A(\mathfrak{o})$ (resp. $P \in B(\mathfrak{o})$) whose reduction mod π is contained in $T_A(k)$ (resp. $T_B(k)$), and that $E^t(\hat{\mathfrak{o}})$ is simply the part of $E(\mathfrak{o})$ lying over $A^t(\hat{\mathfrak{o}}) \times B^t(\hat{\mathfrak{o}})$. Thus we can add a still smaller biextension to the left of the diagram under case 1.5.2:

$$\begin{array}{ccc} \mathfrak{o}^* & = & \mathfrak{o}^* \\ \cap & & \cap \\ E^t(\hat{\mathfrak{o}}) & \subset & E(\mathfrak{o}) \\ \downarrow & & \downarrow \\ A^t(\hat{\mathfrak{o}}) \times B^t(\hat{\mathfrak{o}}) & \subset & A^\circ(\mathfrak{o}) \times B(K) \end{array}$$

By (1.7), (1.6) and (1.7) in succession we extend the $\rho \mid \mathfrak{o}^*$-splitting $\rho \circ \psi_{\mathfrak{o}}$ of $E^t(\hat{\mathfrak{o}})$ to $E(\mathfrak{o})$, then to $E^\circ(K)$ and then to $E(K)$ obtaining finally our canonical ρ-splitting ψ_ρ. For $x \in E(K)$ there is an integer ν such that $(m_A, 1)x \in \pi^\nu + E(\mathfrak{o})$; writing $(m_A, 1)x = \pi^\nu + y$, we have

$$(n_A, m_B n_B)y \in E^t(\hat{\mathfrak{o}})$$

and then $\psi_\rho(x)$ is given explicitly by the formula

$$\psi_\rho(x) = \frac{1}{m_A}\left(\nu\rho(\pi) + \frac{1}{m_B n_A n_B}\rho\Big(\psi_{\mathfrak{o}}((m_A, m_B n_B)y)\Big)\right).$$

Hence

$$\psi_\rho(x) \in \frac{1}{m_A}\rho(K^*) + \frac{1}{m_A m_B n_A n_B}\rho(\mathfrak{o}^*).$$

If we are simultaneously in case (1.5.2) and (1.5.3), then $\rho \circ \psi_{\mathfrak{o}} = 0$, hence the ψ_ρ we have just defined in case (1.5.3) does indeed coincide with that defined for (1.5.2). This concludes the proof of 1.5, or rather its reduction to our result (5.11, 5.12) on the existence of unique splittings of certain formal group scheme biextensions.

Remark. At the cost of increasing n_A and n_B a bit, one can avoid some of the technical complications of 5.11.1 by replacing the "toric completions" A^t, B^t, E^t by the formal completions A^f, B^f, E^f of A, B and E at the zero points of their special fibers. Then E^f is a biextension of (A^f, B^f) by $\mathbb{G}_m^f$ in the category of formal groups over $\hat{\mathfrak{o}}$, and the existence of a unique splitting for it is given by a proposition of Mumford; see (5.11.5). But then instead of n_A, n_B one must take integers N_A, N_B such that

$$N_A \circ A^o(k) = 0 = N_B \circ B^o(k).$$

(1.10) Functorial properties of ψ_ρ.

In this paragraph, without stating it explicitly, we suppose that, in each situation considered, the canonical ρ-splittings which occur in formulae are defined, i.e., that we are in one of the three cases (1.5.1-3). If no indication of a proof is given, it is because the stated formula follows immediately from the unique characterization of canonical ρ-splittings given in (1.9).

(1.10.1) *Change of value group, and linearity in ρ.*

Let $\rho\colon K^* \longrightarrow Y$ and $c\colon Y \longrightarrow Y'$ be homomorphisms. Then

$$\psi_{c\rho} = c\psi_\rho.$$

Let $\rho, \rho' : K^* \to Y$ be homomorphisms and $c, c' \in \operatorname{End} Y$. Then

$$\psi_{c\rho+c'\rho'} = c \cdot \psi_\rho + c' \psi_{\rho'}.$$

(1.10.2) *Change of field.*
Suppose $\sigma\colon K \longrightarrow L$ is a continuous homomorphisms of local fields. Let

$$\rho\colon L^* \longrightarrow Y$$

be a homomorphism. Then

$$\psi_{\rho\circ\sigma} = \psi_\rho \circ \sigma,$$

i.e., the diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\sigma} & E(L) \\ {\scriptstyle \psi_{\rho\circ\sigma}} \downarrow & & \downarrow {\scriptstyle \psi_\sigma} \\ Y & = & Y \end{array}$$

is commutative. Indeed, the right side has the characterizing properties of the left, in each of the three cases.

(1.10.3) *Change of abelian variety.*
First, let A_1, B_1 be abelian varieties over K and $f\colon A_1 \longrightarrow A$, $g\colon B_1 \longrightarrow B$ K-homomorphisms. Let E_1 be the biextension of (A_1, B_1) by $\mathbb{G}_{m/K}$ obtained from E by pullback via (f, g), so that we have a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E \\ \downarrow & & \downarrow \\ A_1 \times B_1 & \xrightarrow{f\times g} & A \times B \end{array}$$

Let $\rho\colon K^* \longrightarrow Y$ be a homomorphism and ψ_ρ (resp. $\psi_{1\rho}$) the canonical ρ-splitting of E (resp. of E_1). Then

$$\psi_{1\rho} = \psi_\rho \circ \varphi.$$

(1.10.4) *Symmetry.*
If E is the biextension pairing A and B, then its "mirror-image" ${}^{s}E$ (cf. [SGA 7 I], exp. VII, 2.7) is a biextension, pairing B and A. Moreover, there

is a canonical identification of sets ${}^{s}E(K) = E(K)$. Any ρ-splitting of E is a ρ-splitting of ${}^{s}E$.

(1.10.5) *Trace.*

Suppose $L \supset K$ is a finite extension, which we assume Galois for simplicity. Let $G = \mathrm{Gal}(L/K)$ and suppose $\rho: L^{\bullet} \longrightarrow Y$ is a homomorphism. Let $E(L, K)$ be the part of E which lies over $A(L) \times B(K)$, and define a map Tr: $E(L,K) \longrightarrow E(K)$ as the map which is the *trace* $E_b(L) \to E_b(K)$ on the fibers of $E \to B$ for $b \in B(K)$. Then for $x \in E(L, K)$,

$$\psi_{(\rho|K^{\bullet})}(\mathrm{Tr}\, x) = \psi_{\sum_{\tau\in G}\rho\circ\tau}(x).$$

Indeed, if $x \in E_b$, $b \in B(K)$,

$$\psi_{(\rho|K^{\bullet})}(\mathrm{Tr}\, x) = \psi_{(\rho|K^{\bullet})}\Big(\sum_{\tau\in G}\tau x\Big) \qquad \text{(sum in } E_b(L)).$$

By (1.10.2) and (1.10.1) this equals

$$\psi_{\rho}\Big(\sum_{\tau}\tau x\Big) = \sum_{\tau}\psi_{\rho}(\tau x) = \sum_{\tau}\psi_{\rho\tau}(x)$$
$$= \psi_{\sum_{\tau}\rho\tau}(x).$$

In particular, if $\rho\tau = \rho$ for all $\tau \in G$, then

$$\psi_{(\rho|K^{\bullet})}(\mathrm{Tr}\, x) = [L : K]\psi_{\rho}(x). \tag{1.10.5.2}$$

And if $\rho = \theta \circ \mathrm{N}_{L/K}$, where $\theta: K^{\bullet} \longrightarrow Y$, then this becomes

$$[L : K]\psi_{\theta}(\mathrm{Tr}\, x) = [L : K]\psi_{\theta\circ\mathrm{N}_{L/K}}(x),$$

whence, if Y has no $[L : K]$-torsion,

$$\psi_{\theta}(\mathrm{Tr}\, x) = \psi_{\theta\circ\mathrm{N}_{L/K}}(x). \tag{1.10.5.3}$$

(1.11) Local universal norms.

In [22] Schneider defined a p-adic height pairing using an approach modelled on Bloch's definition of the archimedean height pairing. To define his pairing, Schneider makes use of "local splittings" obtained by consideration of local universal norms. In this paragraph we investigate the connection between the canonical biextension splittings of (1.5) and Schneider's splittings.

(1.11.1) *Local $\mathbb{Z}_p$-extensions.* Let K be a complete local field with finite residue field. Let $\rho: K^* \longrightarrow \mathbb{Q}_p$ be a non-trivial continuous homomorphism. Such a homomorphism extends uniquely to the profinite completion of K^*

$$\hat{\rho}: \hat{K}^* \longrightarrow \mathbb{Q}_p$$

and by local class field theory, $\hat{\rho}$ determines a $\mathbb{Z}_p$-extension L/K whose $\nu^{\underline{th}}$ layer K_ν/K is the unique cyclic extension of degree p^ν such that

$$\rho(N_{K_\nu/K}K_\nu^*) = p^\nu \cdot \rho(K^*) \subseteq \mathbb{Q}_p.$$

(1.11.2) *Universal ρ-norms.*

Fix a ρ as in (1.11.1). If $G_{/K}$ is any commutative group scheme, let the subgroup of *universal ρ-norms*, $\tilde{G}(K) \subset G(K)$, be defined as the intersection of the images

$$\mathrm{Tr}_{K_\nu/K}: G(K_\nu) \longrightarrow G(K)$$

for all ν.

Examples. If $G = \mathbb{G}_m$, then $\tilde{\mathbb{G}}_m(K)$ is the kernel of the homomorphism ρ: $\mathbb{G}_m(K) = K^* \longrightarrow \mathbb{Q}_p$. The group of universal ρ-norms $\tilde{A}(K)$ for our abelian variety A is of finite index in $A(K)$ if either $A_{/\mathbb{O}}$ is ordinary of good reduction or L/K is unramified, ([11] 4.39; and if L/K is unramified, 4.2 and 4.3).

(1.11.3) *Biextensions of universal ρ-norms.*

Recall that $E(K_\nu, K) \subset E(K_\nu)$ is the set of points which project to $A(K_\nu) \times B(K)$. Define the subset $\tilde{E}(K) \subset E(K)$ to be the intersection of the images of

$$\mathrm{Tr}_{K_\nu/K}: E(K_\nu, K) \longrightarrow E(K)$$

for all ν, (cf. 1.10.5).

(1.11.4) Lemma. *If $\tilde{A}(K)$ is of finite index in $A(K)$, then $\tilde{E}(K)$ inherits the structure of a biextension of $(\tilde{A}(K), B(K))$ by $\tilde{\mathbb{G}}_m(K)$ via the natural inclusion*

$$\begin{array}{ccc} \tilde{\mathbb{G}}_m(K) & \subset & \mathbb{G}_m(K) \\ \downarrow & & \downarrow \\ \tilde{E}(K) & \subset & E(K) \\ \downarrow & & \downarrow \\ \tilde{A}(K) \times B(K) & \subset & A(K) \times B(K). \end{array}$$

Proof. For each $b \in B(K)$ we must show that

$$0 \to \tilde{\mathbb{G}}_m(K) \to \tilde{E}_b(K) \to \tilde{A}(K) \to 0$$

is exact. This is (essentially) lemma 3 of §2 of [22].

Schneider's method for constructing his p-adic analytic height may be phrased in terms of biextensions as follows:

(1.11.5) Lemma. *Let $\tilde{A}(K)$ be of finite index in $A(K)$. Then there is a unique ρ-splitting of the biextensions $E(K)$ which takes $\tilde{E}(K)$ to zero.*

Proof. An easy application of (1.6) and (1.7). We refer to the above ρ-splitting (which exists when $\tilde{A}(K)$ is of finite index in $A(K)$) as *Schneider's ρ-splitting.*

(1.11.6) Proposition. *Suppose that either*

(a) *L/K is unramified,*

or

(b) *$A_{/\mathbb{O}}$ and $B_{/\mathbb{O}}$ have good reduction, and are ordinary.*

Then $\tilde{A}(K)$ is of finite index in $A(K)$ and the canonical ρ-splitting of $E(K)$ is equal to Schneider's ρ-splitting.

Proof. By (1.11.2), $\tilde{A}(K)$ is indeed of finite index in $A(K)$. For each $\nu \geq 1$, let

$$\rho_\nu = \rho \circ \mathrm{N}_{K_\nu/K} \colon K_\nu^* \longrightarrow \mathbb{Q}_p$$

and $\psi_\nu = \psi_{\rho_\nu}$, the canonical ρ_ν-splitting of $E(K_\nu)$. We have by (1.10.5.3) a commutative diagram:

$$(1.11.6.1)\qquad \begin{array}{ccc} E(K_\nu, K) & \xrightarrow{\psi_\nu} & \mathbb{Q}_p \\ \downarrow \mathrm{Tr}_{K_\nu/K} & & \downarrow id. \\ E(K) & \xrightarrow{\psi} & \mathbb{Q}_p \end{array}$$

where $\psi = \psi_1$ is the canonical ρ-splitting of $E(K)$.

(1.11.7) *Claim.*
There is an integer $c \in \mathbb{Z}$, such that, for all ν,

$$\psi_\nu E(K_\nu) \subseteq p^{-c}\rho_\nu(K_\nu^*).$$

Our proposition follows from (1.11.5) because

$$\rho_\nu(K_\nu^*) = p^\nu \rho(K^*) \subseteq \mathbb{Q}_p$$

and consequently by (1.11.6.1), $\psi\tilde{E}(K)$ is contained in $p^{\nu-c}\cdot\rho(K^*)$ for all ν, hence is zero.

To prove the claim, let $\mathfrak{o}_\nu = \mathfrak{o}(K_\nu)$ be the ring of integers in K_ν. Note that the Néron model of $A_{/K_\nu}$ over $\mathfrak{o}_\nu$ is, under assumption (a) or (b), the base-change to $\mathfrak{o}_\nu$ of A. Let $m_\nu = m_{A/K_\nu}$, $n_\nu = n_{A/K_\nu}$ and $m'_\nu = m_{B/K_\nu}$, $n'_\nu = n_{B/K_\nu}$ be the exponents of $A_{/K_\nu}$ and $B_{/K_\nu}$.

By the theorem in (1.5),

$$\psi_\nu E(K_\nu) \subset \frac{1}{m_\nu}\rho_\nu(K_\nu^*)$$

if L/K is unramified, and

$$\psi_\nu E(K_\nu) \subset \rho_\nu(K_\nu^*) + \frac{1}{n_\nu n'_\nu}\rho_\nu(\mathfrak{o}_\nu^*)$$

if $A_{/K}$ and $B_{/K}$ have good, ordinary reduction.

Note that, in case (a), m_ν is bounded independent of ν (by the number of components of $A_{/\bar{k}}$). If we are not in case (a), then $m_\nu = m'_\nu = 1$ and n_ν, (resp. n'_ν) is bounded independent of ν (by the number of points of A (resp. B) in the residue field of L). Our claim follows.

§ 2. Interpretation in Terms of Zero-Cycles and Divisors; Relation with Néron's Canonical Quasi-Functions

(2.1) The symbol $[\mathfrak{a}, D, c]$.

In the next two paragraphs, K can be any field; $A_{/K}$ is an abelian variety over K, $A'_{/K}$ its dual, and $E = E^A$, cf. (1.3).

Consider the set T of triples $(\mathfrak{a}, D, c)$ consisting of:

(i) A zero cycle of degree zero, $\mathfrak{a} = \sum_i n_i(a_i)$, $a_i \in A(K)$, on A_K, all of whose components are points a_i of A rational over K.

(ii) A divisor D algebraically equivalent to zero on $A_{/K}$, whose support is disjoint from $\mathfrak{a}$.

(iii) An element $c \in K^\bullet$.

A triple $(\mathfrak{a}, D, c) \in T$ determines a point $[\mathfrak{a}, D, c] \in E(K)$ in a well-known manner, and every point of $E(K)$ is of this form. The symbol $[\mathfrak{a}, D, c]$ obeys the following rules.

(2.1.1) $[\mathfrak{a}, D, c]$ lies over the point $(a, b) \in A(K) \times B(K)$, where

$$a = S(\mathfrak{a}) \stackrel{\text{defn}}{=} \sum_i n_i a_i$$

and

$$b = Cl(D) \stackrel{\text{defn}}{=} \text{The point in } A'(K) \text{ representing the class of the divisor } D.$$

(2.1.2) $$[\mathfrak{a}, D, c] = c + [\mathfrak{a}, D, 1] \quad \text{for } c \in K^\bullet.$$

(2.1.3) Addition in ${}_aE(K)$ for $a = S(\mathfrak{a})$ is given by

$$[\mathfrak{a}, D_1, 1] + [\mathfrak{a}, D_2, 1] = [\mathfrak{a}, D_1 + D_2, 1].$$

(2.1.4) Addition in $E_b(K)$ for $b = Cl\, D$ is given by

$$[\mathfrak{a}_1, D, 1] + [\mathfrak{a}_2, D, 1] = [\mathfrak{a}_1 + \mathfrak{a}_2, D, 1].$$

(2.1.5) If f is a rational function on A_K whose support is disjoint from $\mathfrak{a}$ we have

$$[\mathfrak{a}, (f), 1] = [\mathfrak{a}, 0, f(\mathfrak{a})],$$

where

$$f(\mathfrak{a}) = \prod_i f(a_i)^{n_i}, \quad \text{if} \quad \mathfrak{a} = \sum n_i(a_i).$$

(2.1.6) For each D and each $a_0 \in (A - \operatorname{Supp} D)(K)$ there is a K-morphism

$$g = g_{a_0,D}\colon (A_{/K} - \operatorname{Supp} D) \longrightarrow E$$

such that

$$g(a) = [(a) - (a_0), D, 1].$$

The properties (2.1.1)-(2.1.6), for K and its algebraic extensions, *characterize* the symbol $[\mathfrak{a}, D, c]$. Indeed, suppose $[\quad]_1$ and $[\quad]_2$ are two such symbols with those properties. Let their difference be

$$\delta(\mathfrak{a}, D, c) = [\mathfrak{a}, D, c]_1 - [\mathfrak{a}, D, c]_2 \in K^*.$$

This makes sense by (2.1.1). By (2.1.2), $\delta(\mathfrak{a}, D, c)$ is independent of c, and by (2.1.5), it depends only on the class of D. Choosing divisors D_j in this class such that none of them passes through zero, and whose supports have an empty intersection, we find using (2.1.6) that there are morphisms

$$h_i\colon (A - \operatorname{Supp} D_i) \longrightarrow \mathbb{G}_m$$

such that

$$h_i(a) = \delta\big((a) - (0), D_i, 1\big).$$

These fit together to make a morphism

$$h\colon A \longrightarrow \mathbb{G}_m.$$

This h is constant since A is complete, and $h = 0$ because $h(0) = 0$. Since the elements $(a) - (0)$ generate the group of zero cycles of degree 0, this shows that $\delta(\mathfrak{a}, D, c) = 0$ for all $(\mathfrak{a}, D, c)$ and proves unicity.

A further property of the symbol is invariance under translation

(2.1.7) $$[\mathfrak{a}_a, D_a, c] = [\mathfrak{a}, D, c],$$

if $\mathfrak{a}_a$ and D_a denote the images of $\mathfrak{a}$ and D under translation by a. Indeed, the left side has the properties characterizing the right.

(2.2) Interpretations of splittings as pairings between disjoint zero cycles and divisors.

In this paragraph we recall the connection between ρ-splittings and Néron type pairings; cf. Zarhin [24], where also conditions are given for ρ to admit some splitting.

Let P be the set of all pairs $(\mathfrak{a}, D)$ such that $(\mathfrak{a}, D, 1) \in T$. Suppose now $\rho: K^{\bullet} \longrightarrow Y$ is a homomorphism, and $\psi: E(K) \longrightarrow Y$ is a ρ-splitting of $E(K)$. Put

$$[\mathfrak{a}, D]_{\psi} \overset{\text{defn}}{=} \psi([\mathfrak{a}, D, 1]).$$

Then it is easy to check that the symbol $[\mathfrak{a}, D]_{\psi}$, which is defined for $(\mathfrak{a}, d) \in P$, and takes values in Y, satisfies the rules

(2.2.1) $$[\mathfrak{a}, D] \text{ is biadditive.}$$

(2.2.2) $$[\mathfrak{a}, (f)] = \rho(f(\mathfrak{a})).$$

(2.2.3) $$[\mathfrak{a}_a, D_a] = [\mathfrak{a}, D].$$

Conversely, given a symbol satisfying (2.2.1), (2.2.2), and (2.2.3), we obtain a ρ-splitting ψ of $E(K)$ by putting

(2.2.4) $$\psi([\mathfrak{a}, D, c]) = \rho(c) + [\mathfrak{a}, D].$$

This is clear, once one proves that $\psi(x)$ is well defined, i.e., that (2.2.4) is independent of the representation of x as a triple $x = [\mathfrak{a}, D, c]$. We leave the details of this to the reader. *Thus, a ρ-splitting of $E(K)$ is the same as a pairing $[\mathfrak{a}, D]$ satisfying the above three properties.*

(2.3) Canonical pairings.

Now suppose we are in the situation of the theorem of (1.5). In particular, we suppose that K is local as in §1. Define the *canonical ρ-pairing* (on P, with values in Y) by

$$[\mathfrak{a}, D]_{\rho} = \psi_{\rho}([\mathfrak{a}, D, 1])$$

where ψ_{ρ} is the *canonical ρ-splitting* of (1.5).

(2.3.1) Proposition. *Suppose $v(x) = -\log|x|$. Then the canonical v-pairing $[\mathfrak{a}, D]_v$ coincides with Néron's symbol $(D, \mathfrak{a})_v$, defined in §9 of [15].*

Indeed, our conditions (2.2.1). (2.2.2), (2.2.3) are Néron's conditions (i), (ii) and (iii′), and according to Néron's Theorem 3 and his remark (d) after its proof, his symbol is characterized by those three conditions together with his condition (iv), which states that the function $a \mapsto [(a)-(a_o), D]_\rho$ is bounded on bounded subsets of $(A - \text{Supp } D)(K)$. We have (cf. 2.16)

$$[(a)-(a_o), D]_\rho = \psi_v\big((a)-(a_o), D, 1\big) = g_{a_o,D}(a).$$

A morphism like $g_{a_o,D}$ takes bounded sets to bounded sets. It suffices therefore to show that our canonical splitting ψ_v is bounded on bounded subsets of $E(K)$. In the archimedean case (1.5.1) this is true because bounded sets are compact and ψ_v is continuous. In case (1.5.2), it is a consequence of the following lemma, whose proof we leave to the reader.

(2.3.2) **Lemma.** *A bounded subset T of $E(K)$ which lies in $E^0(K) = \bigcup_{\nu\in\mathbf{Z}}(\pi^\nu + E(R))$ is contained in a finite union of the sets $\pi^\nu + E(R)$.*

In cases (1.5.1) and (1.5.2) the canonical ρ-splitting ψ_ρ is determined by ψ_v, because $\rho(x)$ depends only on $v(x)$. Hence, those two cases of the theorem of 1.5 are simply the expression in terms of biextensions of Bloch's interpretation in terms of extensions of Néron's theory of canonical quasi-functions and his pairing $(X, \mathfrak{a})_v$. Thus these two cases are not really new; nor are biextensions essential for them, since the characterizing properties of ψ_v can be expressed in terms of single extensions.

§ 3. Global Fields

In this section K denotes a "global" field, by which we mean at first only this, that there is given a set $\mathcal{V}$ of places of K such that each $v \in \mathcal{V}$ is either archimedean or discrete, and such that, for each $c \in K^*$, we have $|c|_v = 1$ for all but a finite number of $v \in \mathcal{V}$. In particular, the set $\mathcal{V}_\infty$ of archimedean places in $\mathcal{V}$ is finite.

For each $v \in \mathcal{V}$, let K_v denote the completion of K at v, and for $v \notin \mathcal{V}_\infty$, let $\mathfrak{o}_v$ be the ring of integers in K_v, π_v a uniformizer and $k(v) = \mathfrak{o}_v/\pi_v\mathfrak{o}_v$.

Let $A_{/K}$ and $B_{/K}$ be abelian varieties and fix $E_{/K}$ a biextension of $(A_{/K}, B_{/K})$ by $\mathbb{G}_{m/K}$, i.e., $A_{/K}$ and $B_{/K}$ are paired abelian varieties. For each v of $\mathcal{V}$, we consider the local theory for $A_{/K_v}$ discussed in §1, and let the symbols A_v, E_v, for all $v \in \mathcal{V}$; A_v^o, m_{A_v}, for $v \notin \mathcal{V}_\infty; T_{A,v}, n_{A_v}$ for v

such that $k(v)$ is finite have the meanings explained in the beginning of §1; and similarly for the abelian variety $B_{/K}$.

Let Y be a commutative group, and suppose that we are given a family $\rho = (\rho_v)_{v\in\mathcal{V}}$ of homomorphisms $\rho_v\colon K_v^\bullet \longrightarrow Y$, such that $\rho_v(\mathcal{O}_v^\bullet) = 0$ for all but a finite number of v's, and such that the "sum formula" $\sum_{v\in\mathcal{V}} \rho_v(c) = 0$ holds for all $c \in K^\bullet$.

Define the topological ring $\mathbb{A}_K$ as the restricted product $\prod'_{v\in\mathcal{V}} K_v$ where a vector $x = (x_v)_{v\in\mathcal{V}}$ is in $\mathbb{A}_K$ if $x_v \in \mathfrak{o}_v$ for all but a finite number of $v \in \mathcal{V} - \mathcal{V}_\infty$. We have a canonical homomorphism $K \to \mathbb{A}_K$. It is convenient to view a family $\rho = (\rho_v)$ as above, as a homomorphism

$$\rho\colon \mathbb{A}_K^\bullet \longrightarrow Y$$

which annihilates the image of $\mathfrak{o}_v^\bullet$ for all but a finite number of $v \in \mathcal{V} - \mathcal{V}_\infty$ as well as the image of $K^\bullet$.

Suppose that we are given for each $v \in \mathcal{V}$ a ρ_v-splitting, ψ_v, of $E(K_v)$, and that $\psi_v(E(\mathfrak{o}_v)) = 0$ for all but a finite number of v's:

(3.1) **Lemma.** *Let $\rho = (\rho_v)$ and let (ψ_v) be as just described. There is a unique pairing*

$$(\ ,\ )\colon A(K) \times B(K) \longrightarrow Y$$

such that if $x \in E(K)$ lies above $(a, b) \in A(K) \times B(K)$, then

$$(a, b) = \sum_{v\in\mathcal{V}} \psi_v(x_v), \tag{3.1.1}$$

where $x_v \in E(K_v)$ is the image of x under the inclusion $K \subset K_v$.

Proof. We first note that (3.1.1) is a finite sum. Indeed, our abelian varieties A, B and the biextension E come from abelian schemes $A_{/R}$, $B_{/R}$ and a biextension E of $(A_{/R}, B_{/R})$ by $\mathbb{G}_{m/R}$ for some finitely generated subring $R \subset K$.

This R is contained in $\mathfrak{o}_v$ for almost all v by the fact that $|c|_v = 1$ for almost all v, for $c \in K^\bullet$. We have $A(K) = \bigcup A(R)$, the union over all such R's, and for $x \in E(R)$ we have $x_v \in E(\mathfrak{o}_v)$ for all but a finite number of v.

We can therefore define a map $\psi\colon E(K) \longrightarrow Y$ by

$$\psi(x) = \sum_{v\in\mathcal{V}} \psi_v(x_v).$$

For each $c \in K^*$ we have then

$$\psi(x+c) = \psi(x)$$

because $\psi_v(x_v + c) = \psi_v(x_v) + \rho_v(c)$ and $\sum_v \rho_v(c) = 0$. Thus the right side of (3.1.1) is independent of the choice of $x \in E(K)$ above (a, b). Moreover, the map $E(K) \to A(K) \times B(K)$ is surjective, because there are local sections (E is a line bundle on $A \times B$, minus its 0-section). Hence (3.1.1) defines a map $A(K) \times B(K) \to Y$. The map so defined is biadditive, because the ψ_v are splittings.

(3.2) *Definition.* If, in the situation of (3.1), the ρ_v-splitting ψ_v is the canonical ρ_v-splitting of Theorem 1.3, for each v, then the pairing (3.1.1) is called the *canonical ρ-pairing*, and is denoted by $(\ ,\ )_\rho$.

(3.3) Thus, the conditions for the canonical ρ-pairing

$$A(K) \times B(K) \to Y$$

to be defined for a family $\rho = (\rho_v)$ of homomorphisms $\rho_v \colon K_v^* \longrightarrow Y$ are

(3.3.1) For each $v \in \mathcal{V}_\infty$, we have $\rho_v(c) = 0$ if $|c|_v = 1$.

(3.3.2) There is a finite subset $S \subset \mathcal{V} - \mathcal{V}_\infty$ (possibly empty) such that $\rho_v(\mathfrak{o}_v^*) = 0$ for $v \notin S \cup \mathcal{V}_\infty$ and such that A_v is ordinary and $k(v)$ finite for $v \in S$.

(3.3.3) *Sum formula* $\sum_{v \in \mathcal{V}} \rho_v(x) = 0$ for $x \in K^*$.

(3.3.4) Y is uniquely divisible by MN, where

$$M = \prod_{v \notin \mathcal{V}_\infty} m_{A_v} \quad \text{and}$$

$$N = \prod_{v \in S} m_{B_v} \cdot n_{A_v} \cdot n_{B_v}.$$

A homomorphism $\rho \colon \mathbb{A}_K^* \longrightarrow Y$ defined by such a family (ρ_v) where (3.3.1-4) are satisfied is called *admissible*. This notion depends upon the "global" field K with its $\mathcal{V}$, $A_{/K}$, $B_{/K}$ and Y. If Y is a uniquely divisible group, then the notion does not depend on $B_{/K}$.

The values of the canonical ρ-pairing are in the following subgroup of Y:

$$\sum_{v \in \mathcal{V}_\infty} \rho_v(K_v^*) + \sum_{v \in S} \frac{1}{m_{A_v}} \left[\rho_v(K_v^*) + \frac{1}{m_{B_v} n_{A_v} n_{B_v}} \rho_v(\mathfrak{o}_v^*) \right] + \sum_{v \notin S, \mathcal{V}_\infty} \frac{1}{m_{A_v}} \rho_v(K_v^*).$$

(3.4) Functorial Properties.

In this paragraph, we let A, B be paired abelian varieties over a "global" field K, and without stating it explicitly we suppose that, in each situation considered, the canonical ρ-pairings which occur in formulae are defined, i.e., that the ρ's which occur are all admissible. Each subparagraph follows directly from its local counterpart in (1.10).

(3.4.1) *Change of value group, and linearity in* ρ.

Let $\rho\colon \mathbb{A}_K^* \longrightarrow Y$ and $c\colon Y \longrightarrow Y'$ be homomorphisms. Then

$$c \cdot (a,b)_\rho = (a,b)_{c\rho}$$

for $a \in A(K)$, $b \in B(K)$.

The group of homomorphisms

$$\rho\colon \mathbb{A}_K^* \longrightarrow Y$$

which are admissible for A, B form an $\mathrm{End}(Y)$-module, and we have:

$$(a,b)_{c\rho + c'\rho'} = c \cdot (a,b)_\rho + c' \cdot (a,b)_{\rho'}$$

for $c, c' \in \mathrm{End}(Y)$, $a \in A(K)$, $b \in B(K)$.

(3.4.2) *Change of field*

Let $\sigma\colon K \longrightarrow L$ be a homomorphism of "global" fields such that L is of finite degree over K, and the chosen set of places $\mathcal{V}_L$ for L is the full "inverse image" of the chosen set of places $\mathcal{V}_K$ for K.

Denote by the same letter σ the induced mapping $\mathbb{A}_K^* \to \mathbb{A}_L^*$ and also the mappings induced on groups of rational points.

Then for an admissible $\rho\colon \mathbb{A}_L^* \longrightarrow Y$ we have

$$(a,b)_{\rho\sigma} = (\sigma a, \sigma b)_\rho$$

for $a \in A(K)$, $b \in B(K)$.

(3.4.3) *Change of abelian variety.*

First, let A_1, B_1 be abelian varieties over K and $f\colon A_1 \longrightarrow A$, $g\colon B_1 \longrightarrow B$ K-homomorphisms. Let E_1 be the biextension of $(A_{1/K}, B_{1/K})$ by $\mathbb{G}_{m/K}$ obtained from E via pullback via (f,g). Then

$$(fa_1, gb_1)_\rho = (a_1, b_1)_\rho$$

for $a_1 \in A_1(K)$, $b_1 \in B_1(K)$.

An important corollary of this rule is the following. Suppose A and B are abelian varieties over K, A' and B' their duals, and E^A (resp. E^B) the biextension of (A, A') (resp. (B, B')) by $\mathbb{G}_m$ expressing the duality. Suppose $f\colon A \longrightarrow B$ is a homomorphism and $f'\colon B' \longrightarrow A'$ its dual. This means that the pullbacks $(f \times 1_{B'})^*E^B$ and $(1_A \times f')^*E^A$ are canonically isomorphic biextensions of (A, B') by $\mathbb{G}_m$. Hence for $a \in A(K)$ and $b' \in B'(K)$ we have

$$(fa, b')_\rho = (a, f'b')_\rho,$$

where the canonical ρ-pairing on the left is relative to E^B and that on the right is relative to E^A.

(3.4.4) *Symmetry.*
Let ${}^sE$ be the "mirror-image" of the biextension E (cf. [SGA 7 I] exp. VII 2.7). Thus ${}^sE$ is a biextension of $(B_{/K}, A_{/K})$ by $\mathbb{G}_{m/K}$. Then

$$(a, b)_\rho = (b, a)_\rho$$

for $a \in A(K)$, $b \in A(K)$, where the left-hand side refers to the canonical ρ-pairing $A(K) \times B(K) \to Y$ (coming from E) and the right-hand side refers to the canonical ρ-pairing $B(K) \times A(K) \to Y$ (coming from ${}^sE$).

If A is *symmetrically paired* with itself (by a biextension E of $(A_{/K}, A_{/K})$ by $\mathbb{G}_{m/K}$ such that there is an isomorphism of biextension $E \cong {}^sE$) then the canonical ρ-pairing

$$A(K) \times A(K) \to Y$$
$$(a_1, a_2) \mapsto (a_1, a_2)_\rho$$

is a symmetric bilinear form.

Remark. This is notably the case when A is the jacobian of a smooth projective curve $X_{/K}$ and the biextension E is the one determined by the canonical θ-divisor (cf. [13], §2, §3).

(3.4.5) *Trace.*
Let $K \subset L$ be a finite Galois extension of "global" fields. Assume again that $\mathcal{V}_L$ is the full inverse image of $\mathcal{V}_K$. We have a natural norm homomorphism $N_{L/K}\colon \mathbb{A}_L^* \longrightarrow \mathbb{A}_K^*$ compatible with local norms $N_{L_w/K_v}\colon L_w^* \longrightarrow K_v^*$

for $v \in \mathcal{V}_K$ and $w \in \mathcal{V}_L$ "lying above" v, and with the global norm $N_{L/K}\colon L^* \to K^*$. Assume that Y has no $[L:K]$-torsion. Then for $a \in A(L)$ and $b \in B(K)$

$$(\mathrm{Tr}_{L/K} a, b)_\rho = (a, b)_{\rho \circ N_{L/K}}.$$

(3.5) Examples of canonical ρ-pairings.

(3.5.1) *The Néron pairing*: Suppose our places v have absolute values $c \mapsto |c|_v$ satisfying the product formula

$$\prod_{v \in \mathcal{V}} |c|_v = 1.$$

Taking $Y = \mathbb{R}$ and $\rho_v(c) = -\log|c|_v$ for each v we obtain a canonical pairing

$$A(K) \times B(K) \to \mathbb{R}.$$

This is Néron's canonical pairing, as follows immediately from 2.3.1.

(3.5.2) A slight refinement of (3.5.1) which uses essentially the same local splittngs and therefore is in some sense an old story, but which does not seem to have been considered much and whose value we are unable to estimate, is obtained as follows. *Suppose that each* $m_v = 1$. Let

$$W = \bigoplus_{v \in \mathcal{V}} \mathbb{R} e_v$$

be a real vector space with basis elements e_v in one-one correspondence with the places $v \in \mathcal{V}$. Let

$$W_0 = \sum_{v \in \mathcal{V}_\infty} \mathbb{R} e_v + \sum_{v \notin \mathcal{V}_\infty} \mathbb{Z} \log|\pi_v| e_v$$

and let Z denote the subgroup of elements of W of the form

$$\sum_{v \in \mathcal{V}} \log|c|_v e_v, \qquad c \in K^*.$$

Put

$$Y = (W_0/Z)$$

and for each $v \in \mathcal{V}$, put

$$\rho_v(c) = -\log|c|_v + Z \in Y.$$

Then the canonical ρ-pairing

$$A(K) \times B(K) \to Y$$

is defined. Note that if K is a number field, $\mathcal{V}$ the set of all places, and $|c|_v$ the normed absolute value at $v \in \mathcal{V}$, then "dividing" the exact sequence

$$0 \to \sum_{v \in \mathcal{V}_\infty} \mathbb{R}e_v \to W_0 \to (\text{ideal group of } K) \to 0$$

by the sequence

$$0 \to \frac{\text{units of } K}{\text{roots of } 1} \to \frac{K^*}{\text{roots of } 1} \to \begin{pmatrix}\text{principal ideals} \\ \text{of } K\end{pmatrix} \to 0$$

we obtain an exact sequence

$$0 \to \frac{\bigoplus_{v \in \mathcal{V}_\infty} \mathbb{R}}{\text{image of units of } K} \to Y \to (\text{ideal class group of } K) \to 0.$$

Thus Y is (non-canonically) a product of a finite group, a real line, and (card $\mathcal{V}_\infty - 1$) circles.

(3.5.3) *Remarks.* 1) Y maps canonically to the ideal class group, so we get a canonical pairing

$$A(K) \times B(K) \to (\text{ideal class group of } K).$$

This pairing is not new; see [10], [23] for a function field version, and for something in number fields, see Duncan Buell's paper *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. (2), 15, (1977), 19–25.

2) Let us specialize (3.5.2) to the case of K a real quadratic field of class number one, and $A_{/\mathbb{Q}}$, $B_{/\mathbb{Q}}$ paired abelian varieties over $\mathbb{Q}$.

Then $\mathrm{Gal}(K/\mathbb{Q})$ operates on $A(K)$, $B(K)$ and Y. Let the superscript $^+$ or $^-$ refer to the maximal subgroup on which the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts as multiplication by $+1$ or -1. Thus $B(K)^+ = B(\mathbb{Q})$, and the canonical ρ-pairing induces a pairing

$$A(K)^- \times B(\mathbb{Q}) \to Y^- \cong \mathbb{R}/\mathbb{Z}.$$

What is the meaning of this pairing?

§ 4. p-adic Height Pairings

Fix paired abelian varieties $A_{/K}, B_{/K}$ and suppose that K is a global field in the strict sense, i.e., is either a finite extension of $\mathbb{Q}$ or of $F(T)$, F a finite field. Let $\mathcal{V}$ be the set of all places of K.

(4.1) Let $\rho\colon \mathbb{A}_K^* \longrightarrow \mathbb{Q}_p$ be a continuous admissible homomorphism, (for A, K) so that the canonical pairing

$$\begin{aligned} A(K) \times B(K) &\to \mathbb{Q}_p \\ (a,b) &\mapsto (a,b)_\rho \end{aligned}$$

is defined. The space of such homomorphisms forms a $\mathbb{Q}_p$-vector space $V_p = V_p(A, K)$. If $p \neq \operatorname{char} K$, then V_p is finite-dimensional.

The canonical pairing $(\ ,\ )_\rho$ induces a trilinear functional

$$\begin{aligned} A(K) \otimes \mathbb{Q}_p \times B(K) \otimes \mathbb{Q}_p \times V_p &\to \mathbb{Q}_p \\ (\alpha, \beta, \rho) &\mapsto (\alpha, \beta)_\rho . \end{aligned}$$

For $a \in A(K)$, $b \in B(K)$ we have:

(4.1.1) $$(a,b)_\rho \in p^{-\nu} \cdot \rho(\mathbb{A}_K^*) \subset \mathbb{Q}_p$$

where ν is the maximum of the two numbers

(4.1.2) $$\underset{v\, finite}{\operatorname{Max}} (ord_p m_{A_v}) \quad \text{and} \quad \underset{v \in S}{\operatorname{Max}} (ord_p m_{A_v} m_{B_v} n_{A_v} n_{B_v})$$

where S is as in (3.3.2).

(4.2) *Admissible $\mathbb{Z}_p$-extensions.*
Let

$$\rho_{\mathrm{Gal}}\colon G_K \longrightarrow \mathbb{Q}_p$$

be a continuous homomorphisms of the Galois group G_K of an algebraic closure $\overline{K}$ of K into the additive group of p-adic numbers. Then by the reciprocity law, ρ_{Gal} induces a continuous homomorphism

$$\rho\colon \mathbb{A}_K^* \longrightarrow \mathbb{Q}_p .$$

We say that ρ_{Gal} is *admissible* (for A, K) if ρ is.

Since $\mathbb{Q}_p$ is totally disconnected and 2-torsion free, $\rho_v = 0$ for archimedean v. For nonarchimedean v, ρ_v is unramified unless $p = \text{char}\,(k(v))$, because otherwise $\mathfrak{O}_v^*$ has no infinite pro-p-group as quotient.

The homomorphism ρ (and ρ_{Gal}) is admissible for A, if and only if A is ordinary at v if ρ_v is ramified (and if, in the function field case, such places are finite in number).

If ρ_{Gal} is nontrivial, then ρ_{Gal} cuts out a $\mathbb{Z}_p$-extension L/K defined by the condition that ρ_{Gal} factors:

$$\begin{array}{ccc} G_K & \xrightarrow{\ \rho_{\text{Gal}}\ } & \mathbb{Q}_p \\ & \searrow \quad \nearrow & \\ & \text{Gal}(L/K) & \end{array}$$

Such a $\mathbb{Z}_p$-extension is called *admissible for* A if ρ_{Gal} is admissible. Thus a $\mathbb{Z}_p$-extension L/K is admissible for A if and only if it is ramified at only a finite set S of places of K, and A_v is ordinary for each $v \in S$. The admissible $\mathbb{Z}_p$-extensions are in $(1:1)$-correspondence with one-dimensional subspaces of $V_p(A,K)$.

(4.3) The determinant form.

For this paragraph and the next, let $B = A'$, and $E = E^A$.

By the Mordell-Weil theorem, the groups $A(K)$ and $A'(K)$ are finitely generated. They are of the same rank since A and A' are isogenous.

Let the common rank be r and let $(P_i)_{1\le i\le r}$, (resp. $(Q_j)_{1\le j\le r}$) be a basis for $A(K)$ (resp. $A'(K)$) mod torsion.

Then for admissible ρ the determinant

$$\delta(A,\rho) \stackrel{\text{defn}}{=} det_{1\le i,j\le r}(P_i, Q_j)_\rho$$

is defined, and is, up to sign, an invariant of A and ρ. Since $(\ ,\ )_\rho$ is linear in ρ, the determinant $\delta(A)$ is a homogeneous form of degree r on the $\mathbb{Q}_p$-vector space V_p. A line in this space, and also the corresponding $\mathbb{Z}_p$-extension is called *singular (for A)* if $\delta(A,\rho) = 0$ for ρ in the line.

(4.4) Schneider's p-adic analytic height.

Suppose, in this paragraph, that K is a number field and that A has good, ordinary reduction at all places v of K, of residual characteristic p.

Then Schneider [22] has defined a height pairing

$$A(K) \times A'(K) \to \mathbb{Q}_p$$
$$(a,b) \mapsto \langle a,b\rangle_p$$

using "local splittings" defined by universal norms in the cyclotomic $\mathbb{Z}_p$-extension. Define the homomorphism ρ_c: $G_K \longrightarrow \mathbb{Q}_p$ cutting out the cyclotomic $\mathbb{Z}_p$-extensions by $\rho_c(\sigma) = \log_p(u)$ where $u = u(\sigma) \in \mathbb{Z}_p^*$ is defined by $\varsigma^\sigma = \varsigma^u$ for all p-power roots of unity $\varsigma \in \overline{K}$. Here $\log_p$ is the p-adic logarithm.

From (1.11.6) and the definition of Schneider's height pairing $\langle\ ,\ \rangle_p$ we immediately have:

Proposition. *Schneider's height pairing is equal to our canonical ρ_c-pairing.*

Schneider conjectures that this height pairing is nondegenerate.

Remark. Schneider's construction of a p-adic height pairing generalizes immediately to the following kind of ρ_{Gal}: $G_K \longrightarrow \mathbb{Q}_p$; for K any global field.

(4.4.1) *The homomorphism ρ_{Gal} is ramified only at a finite set of valuations v of k, and for each such v, A has good ordinary reduction.*

Then (1.11.6) again insures that Schneider's ρ-pairing coincides with the canonical ρ-pairing.

(4.5) Global universal norms.

Let Γ be a topological group isomorphic to $\mathbb{Z}_p$, and written multiplicatively. Let $\Gamma_n = \Gamma^{p^n}$. Let W be a $\mathbb{Z}_p$-module admitting an action of Γ such that if $W_n = W^{\Gamma_n}$ (the fixed submodule under the action of Γ_n) then W_n is a $\mathbb{Z}_p$-module of finite type for each $n \geq 0$, and $W = \bigcup_n W_n$.

Let

$$N_{m,n} = \sum_{\sigma \in \Gamma_n/\Gamma_m} \sigma \in \mathbb{Z}_p[\Gamma_n/\Gamma_m]$$

for integers $m \geq n \geq 0$. Set $N_m = N_{m,0}$

Form the projective limit $\varprojlim_m W_m$, compiled via the mappings

$$N_{m,n}\colon W_m \longrightarrow W_n \qquad (m \geq n \geq 0).$$

(4.5.8) **Proposition:** *Let $w \in W_0 = W^{\Gamma}$. These conditions are equivalent.*

(1) *The element w is in the image of the natural projection*

$$\varprojlim_m W_m \to W_0.$$

(1′) *There is a family of elements $w_m \in W_m$ such that $N_{m,n}w_m = w_n$ for $m \geq n \geq 0$, and $w_0 = w$.*

(2) *For each $m \geq 0$ there is an element $w_m \in W_m$ such that $N_m w_m = w$.*

Proof. (1) and (1′) are clearly equivalent, and (1′) ⇒ (2) trivially. A standard compactness argument gives that (2) ⇒ (1′).

Call an element $w \in W_0$ satisfying the above conditions a *universal norm.*

Let K be a global field.

If $\rho_{\mathrm{Gal}}: G_K \longrightarrow \mathbb{Q}_p$ is a nontrivial continuous homomorphism cutting out the $\mathbb{Z}_p$-extension L/K set $\Gamma = \mathrm{Gal}(L/K)$ and let K_n/K denote the $n^{\underline{th}}$ layer, so that $\Gamma_n = \mathrm{Gal}(L/K_n)$.

Suppose that $A_{/K}$ is an abelian variety; set

$$W = A(L) \otimes \mathbb{Z}_p; \quad W_n = A(K_n) \otimes \mathbb{Z}_p.$$

The universal norms (for the Γ-module W) in $W_0 = A(K) \otimes \mathbb{Z}_p$ form a $\mathbb{Z}_p$-submodule:

$$U_\rho(A_{/K}) \subseteq A(K) \otimes \mathbb{Z}_p$$

which we refer to as the module of ***universal* ρ*-norms*.** Fix $B_{/K}$ an abelian variety and $E_{/K}$ a biextension of (A, B) by $\mathbb{G}_m$.

(4.5.2) **Proposition.** *Let ρ satisfy (4.4.1). The universal ρ-norms are degenerate for the canonical ρ-pairing:*

$$(u, \beta)_\rho = 0$$

for all $u \in U_\rho(A_{/K})$ and $\beta \in B(K) \otimes \mathbb{Z}_p$.

Proof. By the functorial property (3.4.3) we may assume that B is the dual of A and $E = E^{\wedge}$. For each $n \geq 0$, let $a_n \in A(K_n) \otimes \mathbb{Z}_p$ be such that

$Tr_{K_n/K}(a_n) = u$. By (3.4.5)

$$(u,\beta)_\rho = (a_n,\beta)_{\rho_n}$$

where $\rho_n = \rho \circ N_{K_n/K}$.

By (4.1.1), $(a_n,\beta)_{\rho_n} \in \frac{1}{p^{\nu_n}}\rho_n(\mathbb{A}^*_{K_n})$, where ν_n is given in terms of the exponents for $A_{/K_n}$, $B_{/K_n}$ as in (4.1.2). By the same reasoning as in (1.11.7) ν_n admits an upper bound (say N) of n, giving:

$$(u,\beta)_\rho \in p^{n-N}\rho(\mathbb{A}^*_K)$$

for all n.

Remarks. 1. Let $\mathcal{K}$ be a quadratic imaginary field, and p a prime number. The *anti-cyclotomic* $\mathbb{Z}_p$*-extension* of $\mathcal{K}$ is the unique $\mathbb{Z}_p$-extension $\mathcal{L}/\mathcal{K}$ such that $\mathcal{L}/\mathbb{Q}$ is Galois with non-abelian (necessarily "dihedral") Galois group. By considering Birch-Heegner points on factors of jacobians of modular curves one may produce (for any quadratic imaginary field $\mathcal{K}$) examples of prime p, abelian varieties $A_{/\mathbb{Q}}$ and finite field extensions $K/\mathcal{K}$ such that if ρ: $G_K \longrightarrow \mathbb{Q}_p$ cuts out the anti-cyclotomic $\mathbb{Z}_p$-extension L/K (where $L = \mathcal{L}\cdot K$) the $\mathbb{Z}_p$-module $U_\rho(A_{/K})$ of universal ρ-norms is of positive rank. ([7], [9]).

We have no examples where $rank_{\mathbb{Z}_p} U_\rho(A_{/K})$ is positive, and ρ cuts out a $\mathbb{Z}_p$-extension different from (a base-change of) an anti-cyclotomic $\mathbb{Z}_p$-extension.

2. Let $D_\rho(A_{/K})$ denote the left-kernel of the canonical ρ-pairing, where ρ is admissible. By (4.5.2)

$$rank_{\mathbb{Z}_p} U_\rho(A_{/K}) \leq rank_{\mathbb{Z}_p} D_\rho(A_{/K}).$$

Although at present, we have no examples where $B = A'$, $E = E^A$ and where this is a strict inequality, we expect that such examples exist.

3. An interesting special case to investigate is that in which A is an elliptic curve over $\mathbb{Q}$, with rank $A(\mathbb{Q}) = 1$. Let $P \in A(\mathbb{Q})$ be a generator mod torsion. Let p be a prime of ordinary reduction for A.

Let K be a quadratic imaginary field and $\rho_{a,K}\colon G_K \longrightarrow \mathbb{Q}_p$ a continuous homomorphism which cuts out the anti-cyclotomic $\mathbb{Z}_p$-extension of K.

Note that $V_p(A,K)$ is 2-dimensional, generated by ρ_c (cf. 4.4) and $\rho_{a,K}$.

Using the behavior of our canonical pairing under the action of Gal$(K/\mathbb{Q})$ (cf. (3.4.2)) one sees that

$$(P,P)_{\rho_{a,K}} = 0.$$

Consider these two special cases.

CASE 1. *rank* $A(K) = 1$.
Then the anti-cyclotomic canonical pairing $(\ ,\ )_{\rho_{a,K}}$ is totally degenerate. What are the universal norms? If $(P,P)_{\rho_c} \neq 0$ it follows that the anti-cyclotomic $\mathbb{Z}_p$-extension is the *only* $\mathbb{Z}_p$-extension of K, singular for A.

CASE 2. *rank* $A(K) = 2$.
Let $Q \in A(K)$ be such that P, Q generate $A(K)$ mod torsion, and $\sigma Q = -Q$ for $\sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$.
Writing $\rho = u\rho_c + v\rho_{a,K} \in V_p$ for $(u,v) \in \mathbb{Q}_p \times \mathbb{Q}_p$, the determinant, $\delta(A,\rho)$, defined in (4.3), is easily seen to be this quadratic form:

$$(P,P)_{\rho_c} \cdot (Q,Q)_{\rho_c} \cdot u^2 - (P,Q)^2_{\rho_{a,K}} \cdot v^2,$$

which represents zero if $(P,Q)_{\rho_{a,K}} = 0$ or if $(P,P)_{\rho_c} \cdot (Q,Q)_{\rho_c}$ is a square in $\mathbb{Q}_p$. It would be interesting to have some cases where $(P,Q)_{\rho_{a,K}} \neq 0$ and $(P,P)_{\rho_c} \cdot (Q,Q)_{\rho_c}$ is a nonzero square in $\mathbb{Q}_p$.[2] In such a case one would have precisely two $\mathbb{Z}_p$-extensions of K which are singular for A. It would then be especially interesting to investigate the arithmetic of A over the various finite layers of these singular $\mathbb{Z}_p$-extensions.

§ 5. Biextensions of Formal Group Schemes

(5.1) Review of formal schemes.
Our references for this paragraph are [EGA I] §10 and Knutson's [8], Ch. V, §1. All our rings are assumed to be *noetherian* (and our schemes, formal schemes, etc., will be locally noetherian).

A (noetherian) topological ring A is called *adic* if A has an ideal I (called an *ideal of definition*) such that the topology on A is the I-adic topology, and A is separated and complete for its topology. Since A is noetherian,

[2] In this regard, see forthcoming publications of Gudrun Brattström.

A has a largest ideal of definition I (which is the radical of any ideal of definition).

If A is adic, the topological space $\mathrm{Spec}(A/I)$ (for I any ideal of definition) is independent of I, and is called the *formal spectrum* of A.

The formal spectrum of A may be endowed with a canonical local adic-ringed space structure $(\mathcal{X}, \mathfrak{o}_{\mathcal{X}})$, denoted $\mathrm{Spf}(A)$ such that there is a canonical isomorphism $\Gamma(\mathcal{X}, \mathfrak{o}_{\mathcal{X}}) \cong A$ and such that the functor $A \mapsto \mathrm{Spf}(A)$ is a fully faithful functor from the category of adic rings to the category of local adic-ringed spaces. By definition, an *affine formal scheme* is a local adic-ringed space isomorphic to $\mathrm{Spf}(A)$ for some adic A.

The topological ring A is called the *affine coordinate ring* of the affine formal scheme $\mathrm{Spf}(A)$.

The category of *formal schemes* is the (fully faithful) subcategory of local (adic) ringed spaces "modelled on" affine formal schemes. (Cf. [8], [EGA I] §10.)

Recall that $\mathfrak{o}$ is a complete discrete valuation ring with uniformizer π. Let $S = \mathrm{Spec}\,\mathfrak{o}$, and $S_n = \mathrm{Spec}\,\mathfrak{o}/\pi^{n+1}\mathfrak{o}$ for $n \geq 0$. In particular, $S_0 = \mathrm{Spec}(\mathfrak{o}/\pi\mathfrak{o}) = \mathrm{Spec}\,k$ where k is the residue field of $\mathfrak{o}$.

We let $\hat{\mathfrak{o}}$ denote the adic ring $\mathfrak{o}$ with $\pi\mathfrak{o}$ as ideal of definition, and $\hat{S} = \mathrm{Spf}(\hat{\mathfrak{o}})$.

Let $X_{/S}$ be an S-scheme and set $X_n = X \times_S S_n$, viewed as S_n-scheme. Let $Y \subset X_0$ be a closed subscheme.

If X^Y denotes the completion of X along Y, then X^Y is a formal $\hat{S}$-scheme. Let R be a local $\mathfrak{o}$-algebra separated and complete for the π-adic topology.

Let $\hat{R}$ be R viewed as adic local $\hat{\mathfrak{o}}$-algebra with ideal of definition $\pi\hat{R}$.

Then $\mathrm{Spf}\,\hat{R}$ is an affine formal scheme and it makes sense to consider $X^Y(\hat{R})$, the $\hat{R}$-valued points of the formal $\hat{S}$-scheme X^Y. This set may be viewed in a natural way as a subset of $X(R)$, the set of R-valued points of the S-scheme X. Which subset? Since R is local, one can reduce this question to the case where X is affine, where it is easily resolved. Specifically, if $x \in X(R)$, denote by $x \times_S S_0 \in X_0(R_0)$ its specialization to the closed fiber. Then

$$X^Y(\hat{R}) = \{x \in X(R) \mid x \underset{S}{\times} S_0 \in Y(R_0)\}.$$

(5.2) Formal group schemes and formal groups.

If S is a formal scheme, a *formal group scheme over* S is a group-object in the category of formal schemes over S. From now on, *formal group scheme* means commutative formal group scheme.

If $\mathcal{G}_{/S}$ is a (formally) *smooth* formal group scheme over the formal scheme S such that the structural morphisms $\mathcal{G} \to S$ induces an isomorphism on underlying topological spaces, we say that $\mathcal{G}$ is a *formal group over* S.

(5.3) *Examples.*
Most of our examples of formal schemes can be obtained by completing a scheme X along a closed subscheme Y.

(5.3.1) *Completion along the closed fiber.*
Let $X_{/S}$ be an S-scheme locally of finite type and set $X_n = X \times_S S_n$. Let $Y = X_{0/S_0}$ be the closed fiber.

Denote by $\hat{X}$ the completion of X along Y. Then $\hat{X}$ is a formal $\hat{S}$-scheme. In the notation of ([EGA I] §10) it is given as an *adic* (S_n)*-system of schemes* $(X_{n/S_n})_n$.

If $X'_{/S}$ is another S-scheme locally of finite type, we have a bijection

$$\mathrm{Hom}_{\hat{S}}(\hat{X}, \hat{X}') \to \varprojlim_n \mathrm{Hom}_{S_n}(X_n, X'_n).$$

(5.3.2) *Formal completion at zero.*
Let $X_{/S}$ be a smooth commutative group scheme of dimension d. Let e_0 denote the identity element of the closed fiber X_{0/S_0}. Form X^f, the completion of X at the point e_0. Then X^f is a formal group over the formal scheme $\hat{S}$. Moreover, X^f is an affine formal scheme whose affine coordinate ring is isomorphic to a power series ring in d variables over $\hat{\mathcal{O}}$ with the maximal ideal as ideal of definition.

(5.3.3) *Formal completion along subtori.*
Let $X_{/S}$ be a smooth (commutative) group scheme, and $T_0 \subset X_0$ a torus over k, contained in the closed fiber. Let X^t denote the formal group scheme over $\hat{S}$ obtained by completing X along T_0. Since T_0 is an affine k-group scheme, a straightforward application of Serre's criterion (also compare [8] V thm. 2.5) shows that X^t is an affine formal group scheme over $\hat{S}$.

There are natural homomorphisms of formal group schemes

$$X^f \to X^t \to \hat{X}.$$

(5.4) *Tori.*
By definition, a *torus* (of dimension d) over any base scheme S is a group scheme over S which, locally for the étale topology, is isomorphic to a product of d copies of $\mathbb{G}_m$.

Let k^s be a separable algebraic closure of k, and $G = \mathrm{Gal}(k^s/k)$. Let R be a local 'artinian ring' with k as residue field. If T is a torus over R, let $T_{0/k}$ denote its closed fiber. The category of tori over R is equivalent to the category of tori over k, the equivalence being given by passage to closed fiber $T \mapsto T_0$; the latter category is anti-equivalent to the category of free abelian groups of finite rank endowed with continuous G-module structures, the anti-equivalence being given by $\mathbb{G}_m$-duality (cf. [SGA 3], exp. VIII).

Consequently, given $T_{0/k}$, for each $n \geq 0$, there is a torus T_{n/S_n} given up to canonical isomorphism, such that $T_n \times_{S_n} S_0 = T_0$.

The system of tori $\left(T_{n/S_n}\right)_{n\geq 0}$ has the property that $T_n \times_{S_n} S_m \cong T_m$ for $n \geq m$, and determines a formal group scheme $\hat{T}_{/\hat{S}}$ [3] which we refer to as the *formal torus over* $\hat{S}$ determined by $T_{0/k}$.

(5.5) **The geometry of toric completions.**

Let $X_{/S}$ be a commutative smooth group scheme over S, $T_{0/k}$ a torus, and

$$\varphi_0 \colon T_0 \longrightarrow X_0$$

a closed immersion of k-group schemes. Let $\hat{T}_{/\hat{S}} = \left(T_{n/S_n}\right)_{n\geq 0}$ be the formal torus over $\hat{S}$ determined by $T_{0/k}$ as discussed in (5.4).

For each $n \geq 0$, there is a unique closed immersion

$$\varphi_n \colon T_n \longrightarrow X_n$$

of S_n-group schemes extending φ_0 (SGA 3 exp. VIII thm. 5.1).

Invoking [SGA 3] exp VI, we may form the quotient group scheme X_n/T_n. The sequence

$$0 \to T_n \xrightarrow{\varphi_n} X_n \xrightarrow{\rho_n} X_n/T_n \to 0 \tag{5.5.1}$$

is exact in the sense that ρ_n is faithfully flat (it is, in fact, smooth) with kernel T_n.

The sequence (5.5.1) induces a sequence:

$$0 \to T_n \to (X_n)^t \to Y_n^f \to 0 \tag{5.5.2}$$

---

[3] The notation is not misleading. This $\hat{T}$ is, in fact, the completion along the closed fiber of a torus T over S (determined uniquely up to canonical isomorphism), but this is irrelevant to us.

where $(X_n)^t$ is the formal completion of X_n along T_0 and Y_n^f is the formal completion at zero in X_n/T_n.

Since $(X_n)^t$ is canonically $(X^t)_n$, passage to the limit gives a sequence of affine formal group schemes over $\hat{S}$:

(5.5.3) $$0 \to \hat{T} \to X^t \to Y^f \to 0.$$

The sequence is exact in the sense that the morphism $X^t \to Y^f$ is formally smooth, with kernel $\hat{T}$. The affine coordinate ring of the $\hat{S}$-formal group Y^f[4] is a power series ring over $\mathfrak{o}$ in ν variables where ν is the codimension of T_0 in X_0.

(5.5.4) *Split tori.*

If T_0 is a split torus over k, then the affine coordinate ring of X^t is isomorphic to an $\mathfrak{o}$-algebra of the form:

$$\varprojlim_n \ \mathfrak{o}/(\pi^n)[[y_1, \ldots, y_\nu]][\tau_1, \tau_1^{-1}, \ldots, \tau_\mu, \tau_\mu^{-1}]$$

where μ is the dimension of T_0. Since T_0 is split $\mathrm{Pic}(T_0) = 0$, and hence $\mathrm{Pic}(X^t) = 0$ ([SGA 2] exp. XI prop. 1.1, plus the fact that T_0 is affine).

(5.6) Biextensions of formal group schemes over $\hat{S}$.

Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be formal group schemes over $\hat{S}$ and E a biextension of $(\mathcal{A}, \mathcal{B})$ by C over $\hat{S}$. Thus E is a formal $\hat{S}$-scheme which is a $\mathcal{C}$-torsor over $\mathcal{A} \times_{\hat{S}} \mathcal{B}$, locally trivial for the Zariski topology and, moreover, E is endowed with *two* group-extensions structures

(5.6.1) $$(\epsilon_B)\colon 0 \to \mathcal{C}_{\mathcal{B}} \to E_{(\mathcal{B})} \to \mathcal{A}_{\mathcal{B}} \to 0$$
$$(\epsilon_A)\colon 0 \to \mathcal{C}_{\mathcal{A}} \to E_{(\mathcal{A})} \to \mathcal{B}_{\mathcal{A}} \to 0$$

where $\mathcal{A}_{\mathcal{B}} = \mathcal{A} \times_{\hat{S}} \mathcal{B}$ viewed as formal group scheme over $\mathcal{B}$, and $E_{(\mathcal{B})}$ denotes E as $\mathcal{B}$-formal scheme via its natural projection to $\mathcal{B}$, etc.

The group-extensions $(\epsilon_{\mathcal{A}})$, $(\epsilon_{\mathcal{B}})$ are required to be compatible with the $\mathcal{C}$-torsor structure of E, and with each other (cf. [SGA 7 I] exp. VII).

---

[4]The notation is not *totally* misleading. If X_0/T_0 is an abelian variety, there is, in fact, an abelian variety over S whose formal completion at the zero part of the closed fiber is Y^f. See ([SGA 7 I] exp. IX §7). However, we make no use of this fact.

In the specific case that the C-torsor E admits a global section $\sigma : \mathcal{A} \times_{\hat{S}} \mathcal{B} \to E$ (in the category of formal $\hat{S}$-schemes) the biextension structure on E determines, and is determined by two 2-cocycles

$$\text{(5.6.2)} \qquad \begin{aligned} \varphi_\sigma &: (\mathcal{A} \times \mathcal{A})_{\mathcal{B}} \longrightarrow C_{\mathcal{B}} \\ \psi_\sigma &: (\mathcal{B} \times \mathcal{B})_{\mathcal{A}} \longrightarrow C_{\mathcal{A}} \end{aligned}$$

where φ_σ is a morphism in the category of formal $\mathcal{B}$-schemes (a 2-cocycle) determining the group-law in the usual way on the $C_{\mathcal{B}}$-torsor

$$\begin{aligned} \mathcal{A}_{\mathcal{B}} \times_{\mathcal{B}} C_{\mathcal{B}} &\xrightarrow{\sim} E_{(\mathcal{B})} \\ (\alpha, \gamma) &\mapsto (\gamma \cdot \sigma\alpha) \end{aligned}$$

and ψ_σ is similar. For more details, see §2 of [12]. The 2-cocycles $\varphi_\sigma, \psi_\sigma$ satisfy the relations (a), (b), (c) of §2 of [12].

(5.7) **The category of biextensions.**

Let $\mathrm{BIEXT}_{\hat{S}}(\mathcal{A}, \mathcal{B}; C)$ denote the category of biextensions (of formal S-schemes) of $(\mathcal{A}, \mathcal{B})$ by C. See ([5], [SGA 7 I] exp. VII) for a discussion of this category.

Let $\mathrm{Biext}^1_{\hat{S}}(\mathcal{A}, \mathcal{B}; C)$ denote the group of isomorphisms classes of biextensions of $(\mathcal{A}, \mathcal{B})$ by C, and let $\mathrm{Biext}^0_{\hat{S}}(\mathcal{A}, \mathcal{B}; C)$ be the group of automorphisms of the trivial biextension.

(5.7.1) In general, we have that $\mathrm{Biext}^0_{\hat{S}}(\mathcal{A}, \mathcal{B}; C)$ is the group of $\hat{S}$-morphisms h: $\mathcal{A} \times \mathcal{B} \longrightarrow C$ which are bilinear in the sense that the induced mappings

$$h_{\mathcal{B}} : \mathcal{A}_{\mathcal{B}} \longrightarrow C_{\mathcal{B}}; \quad h_{\mathcal{A}} : \mathcal{B}_{\mathcal{A}} \longrightarrow C_{\mathcal{A}}$$

are homomorphisms (of formal $\mathcal{B}$-groups, and $\mathcal{A}$-groups, respectively).

(5.8) **Canonical trivializations.**

These statements are equivalent:

(5.8.1) $\mathrm{BIEXT}_{\hat{S}}(\mathcal{A}, \mathcal{B}; C)$ is equivalent to the punctual category.

(5.8.2) $\mathrm{Biext}^i_{\hat{S}}(\mathcal{A}, \mathcal{B}; C) = 0$, for $i = 0, 1$.

(5.8.3) Every biextensions E of $(\mathcal{A}, \mathcal{B})$ by C in the category of $\hat{S}$-schemes admits a unique trivialization (i.e., a 1_C-splitting ψ: $E \longrightarrow C$; cf. (1.4).

(5.9) Biextensions by $\hat{\mathbb{G}}_{m/\hat{S}}$.

Recall that $\hat{\mathbb{G}}_{m/\hat{S}}$ is the formal completion of $\mathbb{G}_{m/S}$ along its closed fiber $\mathbb{G}_{m/k}$. It is determined by the system $(\mathbb{G}_{m/S_n})_{n\geq 0}$.

If E is a biextension of $(\mathcal{A}, \mathcal{B})$ by $\hat{\mathbb{G}}_m$, the $\hat{\mathbb{G}}_m$-torsor E may be taken to be the complement of the zero-section in a line bundle $\mathcal{L}$ over $\mathcal{A} \times_{\hat{S}} \mathcal{B}$.

In particular, if $\mathrm{Pic}(\mathcal{A} \times \mathcal{B}) = 0$, as is the case if $\mathcal{A}$ and $\mathcal{B}$ are toric completions A^t, B^t along *split* tori, any such E admits a section $\sigma\colon \mathcal{A} \times \mathcal{B} \longrightarrow E$, and hence can be described by the 2-cocyles $\varphi_\sigma, \psi_\sigma$ as in (5.6).

(5.10) Canonical Reductions.

Let U, V be two smooth group schemes over S *with connected fibers.* Let $T(U)_0 \subset U_0$, $T(V)_0 \subset V_0$ denote k-tori contained in the special fibers. Let U^t, V^t be the completions of U, V along $T(U)_0$, and $T(V)_0$ respectively.

Let

$$0 \to \hat{T}(U) \to U^t \to Y^f \to 0 \tag{5.10.1}$$

$$0 \to \hat{T}(V) \to V^t \to Z^f \to 0 \tag{5.10.2}$$

denote the exact sequences of formal group schemes over $\hat{S}$ as provided by (5.5.3).

(5.10.3) **Propositions.** *The functor "inverse image of biextensions" induces an equivalence of categories*

$$\mathrm{BIEXT}_{\hat{S}}(Y^f, Z^f; \hat{\mathbb{G}}_m) \xrightarrow{\sim} \mathrm{BIEXT}_{\hat{S}}(U^t, V^t; \hat{\mathbb{G}}_m).$$

Note that this proposition is very close to the statement of Corollary 3.5 of ([SGA 7 I] exp. VIII). Indeed, it is identical except that we are dealing with formal group schemes rather than group schemes. We shall adapt the proof of that corollary to our situation.

Here we rely on some of the results and notions explained in [8], (especially chapter V). In particular, we shall consider the *global etale topology* of formal $\hat{S}$-schemes (as in loc. cit. V §1) and its induced topos, which we denote $\mathcal{T}$. We also shall consider *formal algebraic spaces* over $\hat{S}$ (loc. cit. II §2) and group objects in that category (*formal group algebraic spaces* over $\hat{S}$).

We may also consider biextensions for the topos $\mathcal{T}$ ([SGA 7 I] exp. VII §2). For example, $\mathrm{BIEXT}_{\mathcal{T}}(U^t, V^t; \hat{\mathbb{G}}_m)$ means the category of biextensions of (U^t, V^t) by $\hat{\mathbb{G}}_m$ in the topos $\mathcal{T}$, i.e., a biextensions E in this category is a *sheaf in* $\mathcal{T}$ (and consequently a formal algebraic space over $\hat{S}$) endowed with the structure of biextension.

A key step in the proof of (5.10.3) is:

(5.10.4) **Proposition.** $\mathrm{BIEXT}_{\mathcal{T}}(\hat{T}(U), V^t; \hat{\mathbb{G}}_m)$ *is equivalent to the punctual category.*

We prepare for its proof.

(5.10.5) **Proposition.** *Any formal group algebraic space over* $\hat{S}$ *is a formal group scheme over* $\hat{S}$.

Proof. Let $\mathcal{B}$ be a formal group algebraic space over $\hat{S}$, and, keeping to the notation of loc. cit., let $\mathcal{B}_1$ denote its *first truncation* (loc. cit. V Defn. 2.4). Then $\mathcal{B}_1$ is an algebraic space over S_0 and it inherits an algebraic space-group structure from that of $\mathcal{B}$. By Murre's theorem ([1], Theorem 4.1, [14]), $\mathcal{B}_1$ is a group scheme over S_0. By (loc. cit. V Theorem 2.5) $\mathcal{B}$ is a formal group scheme.

(5.10.6) **Corollary.** *Let* G_1, G_2 *be formal group schemes over* $\hat{S}$ *(commutative, as always). Then any element* e *in* $\mathrm{Ext}^1_{\mathcal{T}}(G_1, G_2)$ *is representable by an extension* $0 \to G_2 \to \mathcal{E} \to G_1 \to 0$ *in the category of formal group schemes over* $\hat{S}$.

Now form

$$\hat{M} = \underline{\mathrm{Hom}}_{\mathcal{T}}(\hat{T}(U), \hat{\mathbb{G}}_m)$$
$$\hat{N} = \underline{\mathrm{Ext}}^1_{\mathcal{T}}(\hat{T}(U), \hat{\mathbb{G}}_m),$$

where the *underline* means as sheaves for the étale topology over $\hat{S}$. One easily sees that $\hat{M}$ (the "Cartier dual" of $\hat{T}(U)$) is representable by an adic (S_n)-system of locally constant group schemes (torsion-free of finite rank). But $\hat{N} = 0$. To see this, we may suppose that k is separably algebraically closed, and (using (5.10.6)) we are reduced to proving that if

$$(e) \qquad 0 \to \hat{\mathbb{G}}_m \to \mathcal{E} \to \hat{T}(U) \to 0$$

is an exact sequence of formal $\hat{S}$-group schemes, then (e) splits. But, for each $n \geq 0$, $(e_n) = (e) \times_{\hat{S}} S_n$ may be seen to be an exact sequence of group schemes over S_n, and splits by ([SGA 7 I]exp. VIII, Prop. 3.3.1). Moreover, a splitting of (e_o) determines uniquely a compatible splitting of (e_n) for all n. Thus $\hat{N} = 0$.

It then follows from the general fact ([SGA 7 I] exp. VIII 1.5.2) that

$$\mathrm{Biext}^1_{\mathcal{T}}(\hat{T}(U), V^t; \hat{\mathbb{G}}_m) \cong \mathrm{Ext}^1_{\mathcal{T}}(V^t, \hat{M}).$$

To show that $\mathrm{Biext}^1_{\mathcal{T}}(\hat{T}(U), V^t; \hat{\mathbb{G}}_m)$ vanishes, we note that (5.10.2) represents an exact sequence of sheaves in the topos $\mathcal{T}$ and hence our problem is reduced to the following two vanishing statements:

(5.10.7) $$\mathrm{Ext}^1_{\mathcal{T}}(\hat{T}(V), \hat{M}) = 0.$$

(5.10.8) $$\mathrm{Ext}^1_{\mathcal{T}}(Z^f, \hat{M}) = 0.$$

But (5.10.7) follows immediately from (5.10.6) and the argument of proposition 3.4 of [SGA 7 I], ext. VIII. To see (5.10.8), consider an exact sequence of formal group schemes over $\hat{S}$.

(5.10.9) $$0 \to \hat{M} \to \mathcal{E} \to Z^f \to 0.$$

Since $Z^f(k) = 0$, and $\mathcal{E} \to Z^f$ is formally étale, there is a unique lifting $\gamma \colon Z^f \longrightarrow \mathcal{E}$ sending the k-valued point of Z^f to zero in $\mathcal{E}(k)$. It is immediate that γ provides a splitting of (5.10.9).

Since the "Cartier dual," $\hat{M} = \underline{\mathrm{Hom}}_{\mathcal{T}}(\hat{T}(U), \hat{\mathbb{G}}_m)$ is étale, one easily sees that $\mathrm{Biext}^0_{\hat{S}}(\hat{T}(U), V^t; \hat{\mathbb{G}}_m) = 0$. The proposition then follows from (5.8).

(5.10.10) *Conclusion of the proof of the proposition* (5.10.3).
By ([SGA 7 I] VII 3.7.6) and the exact sequence (5.10.1), one sees that the category $\mathrm{BIEXT}_{\mathcal{T}}(Y^f, V^t; \hat{\mathbb{G}}_m)$ may be identified up to equivalence with the category whose objects are $\hat{S}$-biextensions E of (U^t, V^t) by $\hat{\mathbb{G}}_m$ supplied with trivializations of the induced biextensions $\mathcal{E}'$ of $(\hat{T}(U), V^t)$ by $\hat{\mathbb{G}}_m$. Morphisms are defined evidently. By (5.10.4) we then have an equivalence of categories

$$\mathrm{BIEXT}_{\mathcal{T}}(Y^f, V^t; \hat{\mathbb{G}}_m) \xrightarrow{\sim} \mathrm{BIEXT}_{\mathcal{T}}(U^t, V^t; \hat{\mathbb{G}}_m)$$

and a symmetrical reduction of V^t to Z^f establishes our proposition.

(5.11) **Canonical trivializations.**
Let $U, V, T(U)_0, T(V)_0$ be as in (5.10). Thus $U_{/S}, V_{/S}$ are smooth group schemes with connected fibers.

(5.11.1) **Proposition.** *Suppose that U^f (equivalently: Y^f) is of multiplicative type. Then* $\mathrm{BIEXT}_{\mathcal{T}}(U^t, V^t; \hat{\mathbb{G}}_m)$ *is equivalent to the punctual category.*

Proof. Using (5.10.3) it suffices to show

(5.11.2) **Lemma.** *If Y^f is ordinary, then* $\mathrm{BIEXT}_{\mathcal{T}}(Y^f, Z^f; \hat{\mathbb{G}}_m)$ *is punctual.*

This is a simple exercise which can be seen in a variety of ways. For example:

(5.11.3) *Proof of* (5.11.2): In analogy with the proof of (5.10.3), set

$$\begin{aligned}\hat{\hat{M}} &= \underline{\mathrm{Hom}}_{\mathcal{T}}(Y^f, \hat{\mathbb{G}}_m)\\ \hat{\hat{N}} &= \underline{\mathrm{Ext}}^1_{\mathcal{T}}(Y^f, \hat{\mathbb{G}}_m),\end{aligned}$$

Then $\hat{\hat{M}}$ is easily seen to be a projective limit of locally constant finite (formal) group schemes over $\hat{S}$.

Moreover, $\hat{\hat{N}}$ is seen to vanish by the proof of (SGA 7 I exp. VIII, Prop. 3.3.1). Thus $\mathrm{Biext}^1(Y, Z^f; \hat{\mathbb{G}}_m) \xrightarrow{\sim} \mathrm{Ext}^1(Z^f, \hat{\hat{M}})$ and the latter group is seen to be zero by the argument demonstrating (5.10.8).

Finally, since $\mathrm{Hom}_S(Z^f, \hat{\hat{M}}) = 0$, we see that

$$\mathrm{Biext}^0_S(Y^f, Z^f; \hat{\mathbb{G}}_m) = 0$$

as well and (5.11.1) follows from (5.8).

(5.11.4) *Paraphrase of part of the above proof, using cocycles.*

From the fact that $\hat{\hat{M}}$ is a projective limit of locally constant finite (formal) group schemes over $\hat{S}$, and that $\hat{\hat{N}} = 0$, the reader may verify that if E is a biextension of (Y^f, Z^f) by $\hat{\mathbb{G}}_m$, then there is a section $\sigma: Y^f \times Z^f \longrightarrow E$ such that the 2-cocycle (5.6.2)

$$\psi_\sigma: (Y^f \times Y^f)_{Z^f} \longrightarrow \hat{\mathbb{G}}_{m_{Z^f}}$$

is trivial. From the relations satisfied by $\psi_\sigma, \varphi_\sigma$ (cf. [12], §2 (a), (b), (c)) it follows that φ_σ may be viewed as an $\hat{S}$-morphisms from $Z^f \times Z^f$ to

$\hat{M} = \underline{\mathrm{Hom}}_{\hat{S}}(\hat{Y}^f, \hat{\mathbb{G}}_m)$ which takes the unique k-valued point of $Z^f \times Z^f$ to zero. Since $\hat{M}$ is a projective limit of locally constant group schemes, φ_σ is trivial as well and consequently E is the trivial biextension.

(5.11.5) *A mild weakening.*

If one is willing to assume that the formal group Z^f is of "finite height" which is indeed all that occurs in any serious application that we envision, then (5.11.2) also follows immediately from ([12], §5, Prop. 4).

References

[1] M. Artin, *Algebraization of formal moduli*: I, *Global Analysis*. Papers in honor of K. Kodaira. (1970) 21–71. Princeton Univ. Press.

[2] I. Barsotti, *Considerations on theta-functions*, Symposia Mathematica (1970) p. 247.

[3] S. Bloch, *A note on height pairings, Tamagawa numbers and the Birch and Swinnerton-Dyer conjecture*, Inv. Math. *58* (1980), 65–76.

[4] D. Bernardi, *Hauteur p-adique sur les courbes elliptiques*. Séminaire de Théorie des Nombres, Paris 1979-80, Séminaire Delange-Pisot-Poitou. Progress in Math. series vol. 12. Birkhäuser, Boston-Basel-Stuttgart. (1981) 1–14.

[5] L. Breen, *Fonctions thêta et théorème du cube*, preprint of the Laboratoire associé au C.N.R.S. N° 305, Université de Rennes I, 1982.

[6] V. Cristante, *Theta functions and Barsotti-Tate groups*, Annali della Scuola Normale Superiore di Pisa, Serie IV, 7 (1980) 181–215.

[7] M. Harris, *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Inv. Math. *51* (1979) 123–141.

[8] D. Knutson, *Algebraic Spaces*, Lecture Notes in Math. *203*, Springer Berlin-Heidelberg-New York, 1971.

[9] P. F. Kurchanov, *Elliptic curves of infinite rank over* Γ*-extensions*, Math. USSR Sbornik, *19*, 320–324 (1973).

[10] J. Manin, *The Tate height of points on an abelian variety. Its variants and applications*. Izv. Akad. Nauk SSSR Ser. Mat. *28* (1964), 1363–1390. (AMS Translations 59 (1966) 82–110).

[11] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inv. Math. *18* (1972) 183–266.

[12] D. Mumford, *Biextensions of formal groups*, in the *Proceedings of the Bombay Colloquium on Algebraic Geometry*, Tata Institute of Fundamental Research Studies in Mathematics 4, London, Oxford University Press 1968.

[13] D. Mumford, *A remark on Mordell's conjecture*, Amer. J. Math. 87 (1965) 1007–1016.

[14] J. P. Murre, *On contravariant functors from the category of preschemes over a field into the category of abelian groups*, Pub. Math. I. H. E. S. n° 23, 1964.

[15] A. Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Annals of Math. *82*, n° 2, (1965) 249–331.

[16] A. Néron, *Hauteurs et fonctions thêta*. Rend. Sci. Mat. Milano *46* (1976) 111–135.

[17] A. Néron, *Fonctions thêta p-adiques*, Symposia Mathematica, *24* (1981) 315–345.

[18] A. Néron, *Fonctions thêta p-adiques et hauteurs p-adiques*, pp. 149–174, in Séminaire de theorie des nombres (Séminaire Delange-Pisot-Poitou), Paris 1980–81, Progress in Math., Vol 22, Birkhäuser Boston-Basel-Stuttgart (1982).

[19] P. Norman, *Theta Functions*. Handwritten manuscript.

[20] B. Perrin-Riou, *Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe*. To appear in Inv. Math.

[21] M. Rosenblum, in collaboration with S. Abramov, *The Birch-Swinnerton-Dyer conjecture mod p*. Handwritten manuscript.

[22] P. Schneider, *p-adic height pairings I*, to appear in Inv. Math.

[23] J. Tate, *Variation of the canonical height of a point depending on a parameter*. To appear in Amer. J. Math.

[24] Ju. G. Zarhin, *Néron Pairing and Quasicharacters*, Izv. Akad. Nauk. SSSR Ser. Mat. Tom 36 (1972) No. 3, 497–509. (Math. USSR Izvestija, Vol. 6 (1972) No. 3, 491–503.)

[EGA I] A. Grothendieck, *Éléments de géométrie algébrigue*. Publications Mathématiques, I. H. E. S. 4 Paris (1961).

[SGA 2] A. Grothendieck, *Cohomologie locale des faisceaux cohérents et Théorèmes de Lefschetz locaux et globaux*, North-Holland Publishing Company - Amsterdam (1968).

[SGA 3] M. Demazure and A. Grothendieck et al, Séminaire de Géométrie Algébrique du Bois Marie 1962/64. *Schémas en Groupes* II. Lecture Notes in Mathematics. *152*, Springer, Berlin-Heidelberg-New York (1970).

[SGA 7 I] A. Grothendieck et al, Séminaire de Géometrie Algébrique du Bois Marie. 1967/69. *Groupes de Monodromie en Géométrie Algébrique*. Lecture Notes in Mathematics. *288*, Springer, Berlin-Heidelberg-New York (1972).

Received October 13, 1982

Supported by NSF

Professor Barry Mazur
Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138

Professor John Tate
Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138