Invent. math. 79, 329–374 (1985)

Inventiones mathematicae

p-adic height pairings. II

Peter Schneider

Mathematisches Institut, Im Neuenheimer Feld 288, D-6900 Heidelberg, Federal Republic of Germany,
and
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA

Our main concern in this paper is to show that algebraic and analytic p-adic heights which are defined in a completely different way nevertheless are the same. If A is an abelian variety over a number field k, $\tilde{A}$ its dual abelian variety, and p a prime number then p-adic heights are pairings

$$\tilde{A}(k) \times A(k) \to \mathbb{Q}_p.$$

Their definition depends on the choice of a nonzero continuous character κ of the absolute Galois group of k into the group of p-adic 1-units $1+p\mathbb{Z}_p$ such that A has ordinary good reduction at the ramification places of κ. The analytic pairing $(\ ,\ )_\kappa$ associated with κ was defined in Part I of this paper ([19]; but see [24] for a more unified treatment). Its construction is straightforward and is modeled on Bloch's description of the real valued Néron-Tate height which relies on the interpretation of points in $\tilde{A}(k)$ as extensions of A by the multiplicative group $\mathbb{G}_m$. It is called analytic since it also can be expressed in terms of p-adic theta functions.

The algebraic pairing $\langle\ ,\ \rangle_\kappa$ was defined in [20] under the assumption that A fulfills certain arithmetic conditions. The construction was highly indirect and used the global flat duality theorem of Artin/Mazur and the descent theory for the $\mathbb{Z}_p$-extension k_∞/k cut out by κ. In the first paragraph we will refine these methods in order to define a pairing

$$\langle\!\langle\ ,\ \rangle\!\rangle_\kappa\colon H^1(\mathscr{o}, T_p(\tilde{\mathscr{A}})) \times H^1(\mathscr{o}, T_p(\mathscr{A})) \to \mathbb{Q}_p$$

between the p-Selmer groups of A and $\tilde{A}$ (which by restriction to points induces $\langle\ ,\ \rangle_\kappa$) only assuming in addition that p is odd and A has good reduction at all primes of k above p. Furthermore we show that some of the arithmetic conditions on A assumed in [20] hold true if $\langle\!\langle\ ,\ \rangle\!\rangle_\kappa$ is nondegenerate (Theorem 1). The most important one of that conditions is that the Iwasawa L-function $L_p(A, \kappa, s)$ of A with respect to κ is defined. This L-function is given in terms of certain characteristic polynomials and reflects the arithmetic properties of A with respect to the $\mathbb{Z}_p$-extension k_∞/k. Assuming the nondegeneracy of $\langle\!\langle\ ,\ \rangle\!\rangle_\kappa$ we then prove in the second paragraph that an analog of the conjecture of Birch and Swinnerton-Dyer is valid for $L_p(A,\kappa,s)$ at $s=1$: $L_p(A,\kappa,s)$ has a zero of order $\operatorname{rank}_{\mathbb{Z}_p} H^1(o, T_p(\mathscr{A}))$ at $s=1$ and the leading coefficient up to a p-adic unit is equal to the determinant of $\langle\!\langle\ ,\ \rangle\!\rangle_\kappa$ times the order of the p-cotorsion group of the Tate-Šafarevič group $Ш_k(A)$ of A times some other (less important) factors (Theorem 2). If we assume in addition that the p-component $Ш_k(A)(p)$ is finite then we have $\langle\!\langle\ ,\ \rangle\!\rangle_\kappa = \langle\ ,\ \rangle_\kappa$ and $\operatorname{rank}_{\mathbb{Z}_p} H^1(o, T_p(\mathscr{A})) = \operatorname{rank}_{\mathbb{Z}} A(k)$ such that our result becomes very analogous to the usual conjecture (Theorem 2′). But we emphasize that this result indicates that for p-adic L-functions a Birch and Swinnerton-Dyer type conjecture might even be true if $Ш_k(A)$ would turn out not to be finite.

The Iwasawa-L-function $L_p(A,\kappa,s)$ is defined if and only if the p-Selmer group of A over k_∞ has rank $\rho=0$ as module over the completed group ring $\mathbb{Z}_p[\![\mathrm{Gal}(k_\infty/k)]\!]$. In the third paragraph we investigate that rank (using the same methods as before) for any abelian variety A which has good but not necessarily ordinary reduction at the primes of k above p and any $\mathbb{Z}_p$-extension k_∞/k. We show that ρ is the sum of a certain global invariant and certain local invariants corresponding to the ramification primes of k_∞/k. It seems that these local invariants are mainly determined by the p-rank of the reduction of A at the corresponding prime. Using a theorem of Konovalov about universal norms in formal groups we are able to establish this if A is an elliptic curve (Theorem 3). On the other hand, we imagine that the mentioned global invariant behaves rather unpredictably for an arbitrary $\mathbb{Z}_p$-extension. But if k_∞/k is the cyclotomic $\mathbb{Z}_p$-extension we in fact conjecture that it always vanishes, i.e. that ρ is completely given in local terms. This conjecture contains as a special case the conjecture of Mazur that $\rho=0$ if A has ordinary good reduction at the ramification primes of k_∞/k. As already said, in that situation the nondegeneracy of the algebraic height $\langle\!\langle\ ,\ \rangle\!\rangle_\kappa$ would imply $\rho=0$. Indeed, we strongly suspect that nondegeneracy is true for the cyclotomic character κ. As we will see, our conjecture also is related to Iwasawa's "$\mu=0$" conjecture. As a consequence of this discussion and the theorem of Ferrero/Washington about $\mu=0$ for abelian fields we will prove that $\rho=[k:\mathbb{Q}]$ if k is abelian over $\mathbb{Q}$ and A is an elliptic curve which has supersingular reduction at the primes above p and possesses a nonzero k-rational point of order p (Theorem 5).

Section B is devoted to the proof of the comparison theorem between analytic and algebraic heights: We have

$$\langle\ ,\ \rangle_\kappa = -(\ ,\ )_\kappa$$

(Theorem 6). An introduction into the structure of this rather lengthy proof is given at the beginning of Sect. B. As an application we show that the nondegeneracy of $(\ ,\ )_\kappa$ for all finite intermediate layers of k_∞/k implies that the Mordell-Weil group $A(k_\infty)$ is finitely generated if its torsion subgroup is finite (which, for example, is known to be the case for the cyclotomic k_∞; – Theorem 8). In an appendix we finally give a cohomological interpretation of the Néron-Tate height pairing which is very similar to the one of $(\ ,\ )_\kappa$ given in Proposition 1 of the last paragraph.

The reader easily will realize to what a big extent this paper originates from a careful understanding of Mazur's fundamental work in [13]. I want to mention that, for elliptic curves with complex multiplication, the whole theory was developed independently by B. Perrin-Riou ([17]). And I want to thank J. Coates and U. Jannsen for several helpful and inspiring conversations.

Contents

Standard notations

For an abelian group M, let $\mathrm{Tor}\,M$ be the torsion subgroup and $M_{\mathrm{Tor}} := M/\mathrm{Tor}\,M$, let $\mathrm{Div}\,M$ be the maximal divisible subgroup and $M_{\mathrm{Div}} := M/\mathrm{Div}\,M$. We use the same notation for a homomorphism $f\colon M\to N$ between abelian groups, e.g., $\mathrm{Div}\,f$ denotes the induced map $\mathrm{Div}\,M\to\mathrm{Div}\,N$. Furthermore, f is called a quasi-isomorphism if it has finite kernel and cokernel.

For a $\mathbb{Z}_p$-module M, let $M^* := \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontrjagin dual of M. If M^* is a finitely generated $\mathbb{Z}_p$-module we put $\operatorname{corank} M := \operatorname{rank}_{\mathbb{Z}_p} M^*$.

For an abelian group or a commutative group scheme G we put $G_n := \ker(G \xrightarrow{n} G)$ for $n\in\mathbb{N}$ and $G(p) := \varinjlim G_{p^\nu}$ for a prime number p. In case of the multiplicative group we use the slightly different notation $\mu_n := \ker(\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)$, resp. $\mu(p) := \varinjlim \mu_{p^\nu}$. If G is an abelian group we also put $T_p(G) := \varprojlim G_{p^\nu}$.

If not indicated otherwise, all cohomology or Ext-groups are taken with respect to the big $fppf$-site on a scheme S. In Sect. A one might prefer to think of the small $fpqf$-site instead; this is possible since there we only consider the cohomology of quasi-finite flat group schemes. By S_{et}, resp. $H^*_{\mathrm{et}}(S,.)$, resp. $\mathrm{cd}_p S_{\mathrm{et}}$, we denote the small étale site on S, resp. its cohomology, resp. its cohomological p-dimension. Similarly $\mathrm{cd}_p \Gamma$ denotes the cohomological p-dimension of a profinite group Γ.

Finally, the cyclotomic $\mathbb{Z}_p$-extension of a number field k is the unique $\mathbb{Z}_p$-extension of k contained in $k(\mu(p))$.

A. The Iwasawa theory of abelian varieties

Throughout the paper, $A_{/k}$ is an abelian variety over a finite extension k of $\mathbb{Q}$ and p is an odd prime number such that

A has good reduction at all primes of k above p.

We denote by $\mathscr{A}_{/o}$ the Néron model of A over the ring of integers o in k. Furthermore, we fix an arbitrary $\mathbb{Z}_p$-extension k_∞/k; let o_∞ be the ring of integers in k_∞ and put $\Gamma := \mathrm{Gal}(k_\infty/k)$. This Sect. A is concerned with the arithmetic properties of the $\mathbb{Z}_p[[\Gamma]]$-module $H^1(o_\infty, \mathscr{A}(p))$.

§ 1. Algebraic p-adic height pairings

In this paragraph we want to show that under a further assumption about the reduction type of A the structure of $H^1(o_\infty, \mathscr{A}(p))$ to a big extent depends on the properties of a certain pairing we will construct. Let Σ denote the finite set of primes of k which are ramified in k_∞/k (and which therefore lie above p).

Definition. A is called ordinary for k_∞ if A has ordinary good reduction at all primes in Σ (in addition to our general assumption about p).

The two spectral sequences

$$H^i(\Gamma, H^j(o_\infty, \mathscr{A}(p))) \Rightarrow H^{i+j}(o_\infty/o, \mathscr{A}(p))$$

and

$$H^i(o, R^j\pi_\Gamma \mathscr{A}(p)) \Rightarrow H^{i+j}(o_\infty/o, \mathscr{A}(p))$$

and the fact that

$$H^i(o, \mathscr{A}(p)) = H^i(o, \pi_\Gamma \mathscr{A}(p)) \quad \text{for } i \geqq 0$$

which we established in [20] lead to the exact "descent diagram"

$$\begin{array}{c}
0 \\
\downarrow \\
H^1(o, \mathscr{A}(p)) \\
\downarrow \\
0 \longrightarrow H^1(\Gamma, A(k_\infty)(p)) \longrightarrow H^1(o_\infty/o, \mathscr{A}(p)) \longrightarrow H^0(\Gamma, H^1(o_\infty, \mathscr{A}(p))) \longrightarrow 0 \\
\downarrow \\
H^0(o, R^1\pi_\Gamma \mathscr{A}(p)) \\
\downarrow \\
H^2(o, \mathscr{A}(p)) \\
\downarrow \\
0 \longleftarrow H^0(\Gamma, H^2(o_\infty, \mathscr{A}(p))) \longleftarrow H^2(o_\infty/o, \mathscr{A}(p)) \longleftarrow H^1(\Gamma, H^1(o_\infty, \mathscr{A}(p))) \longleftarrow 0.
\end{array}$$

We already have computed the group $H^0(o, R^1\pi_\Gamma \mathscr{A}(p))$ in [20]. Here we should remark that most of the results in [20] (proved there only for the

cyclotomic $\mathbb{Z}_p$-extension) carry over to our more general situation by exactly the same proofs. We therefore will use them in that generality without reformulating the proofs. For any finite prime $\mathfrak{p}$ of k, let $k_\mathfrak{p}$ be the completion of k at $\mathfrak{p}$ and let $o_\mathfrak{p}$, resp. $\kappa_\mathfrak{p}$, be the ring of integers in $k_\mathfrak{p}$, resp. the residue class field of $o_\mathfrak{p}$; (fixing a prime of k_∞ above each $\mathfrak{p}$) we put $k_{\mathfrak{p},\infty} := k_\mathfrak{p} \cdot k_\infty$ and $\Gamma_\mathfrak{p} := \mathrm{Gal}(k_{\mathfrak{p},\infty}/k_\mathfrak{p})$.

Proposition 1.

i) $H^i(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty})) = 0$ *for* $\mathfrak{p} \notin \Sigma$ *and* $i > 0$;

ii) $H^0(o, R^1\pi_\Gamma \mathscr{A}(p)) = \bigoplus_{\mathfrak{p} \in \Sigma} H^1(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty}))$;

iii) *if* A *is ordinary for* k_∞ *then, for* $\mathfrak{p} \in \Sigma$, $H^1(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty}))$ *is finite of order* $(\# \mathscr{A}(\kappa_\mathfrak{p})(p))^2$ *and* $H^2(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty})) = 0$.

Proof. For the assertion i) see [13] (4.2) and (4.4). The other assertions are shown on pp. 282-284 in [20]. Although the vanishing of $H^2(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty}))$ for $\mathfrak{p} \in \Sigma$ is not stated explicitly there it is an immediate consequence of that consideration.

The main additional fact we now want to show is the following result.

Proposition 2. *If* A *is ordinary for* k_∞ *then the map* $H^2(o, \mathscr{A}(p)) \to H^2(o_\infty/o, \mathscr{A}(p))$ *is surjective.*

We reduce the proof to a local problem using

Lemma 3. *In the situation of the appendix to* [20] *we have the commutative diagram of exact relative cohomology sequences*

$$\begin{array}{ccccccccc}
\longrightarrow & H^{i-1}(Y, \mathscr{F}) & \longrightarrow & H^i_Z(o, \mathscr{F}) & \longrightarrow & H^i(o, \mathscr{F}) & \longrightarrow & H^i(Y, \mathscr{F}) & \longrightarrow \\
& \| & & \downarrow & & \downarrow & & \| & \\
\longrightarrow & H^{i-1}(Y, \mathscr{F}) & \longrightarrow & H^i_Z(R/o, \mathscr{F}) & \longrightarrow & H^i(R/o, \mathscr{F}) & \longrightarrow & H^i(Y, \mathscr{F}) & \longrightarrow .
\end{array}$$

Proof. The map $H^0(o, \mathscr{I}) \to H^0(Y, \mathscr{I})$ is surjective for all injective sheaves $\mathscr{I} \in \mathscr{S}(o)$ (SGA4 V 4.7). We thus have the commutative exact diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0_Z(o, \mathscr{I}) & \longrightarrow & H^0(o, \mathscr{I}) & \longrightarrow & H^0(Y, \mathscr{I}) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & H^0_Z(R/o, \mathscr{I}) & \longrightarrow & H^0(R/o, \mathscr{I}) & \longrightarrow & H^0(Y, \mathscr{I}) & \longrightarrow & 0.
\end{array}$$

The assertion now follows by applying these functors to an injective resolution of $\mathscr{F}$ and passing to the associated long exact homology sequences. q.e.d.

From the commutative exact diagram (with $Y := \mathrm{Spec}(o) \setminus \Sigma$)

$$\begin{array}{ccccccc}
H^2_\Sigma(o, \mathscr{A}(p)) & \longrightarrow & H^2(o, \mathscr{A}(p)) & \longrightarrow & H^2(Y, \mathscr{A}(p)) & \longrightarrow & H^3_\Sigma(o, \mathscr{A}(p)) \\
\downarrow & & \downarrow & & \| & & \downarrow \\
H^2_\Sigma(o_\infty/o, \mathscr{A}(p)) & \longrightarrow & H^2(o_\infty/o, \mathscr{A}(p)) & \longrightarrow & H^2(Y, \mathscr{A}(p)) & \longrightarrow & H^3_\Sigma(o_\infty/o, \mathscr{A}(p))
\end{array}$$

and the five lemma we get that it suffices to show that

$$H^3_\Sigma(\mathfrak{o}, \mathcal{A}(p)) = 0 \quad \text{and that}$$

$$H^2_\Sigma(\mathfrak{o}, \mathcal{A}(p)) \to H^2_\Sigma(\mathfrak{o}_\infty/\mathfrak{o}, \mathcal{A}(p)) \quad \text{is surjective.}$$

Using [20] (3.4) and the local flat duality theorem we compute

$$H^3_\Sigma(\mathfrak{o}, \mathcal{A}(p)) = \bigoplus_{\mathfrak{p}\in\Sigma} H^3_\cdot(\mathfrak{o}_\mathfrak{p}, \mathcal{A}(p)) = \bigoplus_{\mathfrak{p}\in\Sigma} (\varprojlim \tilde{\mathcal{A}}(\mathfrak{o}_\mathfrak{p})_{p^v})^* = 0$$

where $\tilde{\mathcal{A}}$ denotes the Néron model of the dual abelian variety $\tilde{A}_{/k}$. On the other hand, in the proof of [20] (7.3) we have identified the map $H^2_\Sigma(\mathfrak{o}, \mathcal{A}(p)) \to H^2_\Sigma(\mathfrak{o}_\infty/\mathfrak{o}, \mathcal{A}(p))$ with the map

$$\bigoplus_{\mathfrak{p}\in\Sigma} (H^1(k_\mathfrak{p}, A)(p) \to H^1(k_{\mathfrak{p},\infty}, A)(p)^{\Gamma_\mathfrak{p}})$$

which is surjective since $H^2(\Gamma_\mathfrak{p}, A(k_{\mathfrak{p},\infty}))$ vanishes according to Proposition 1. q.e.d.

Let $\mathcal{A}^0$ be the connected component of $\mathcal{A}$. We put

$$H^i(\mathfrak{o}, T_p(\mathcal{A})) := \varprojlim H^i(\mathfrak{o}, \mathcal{A}_{p^v}) = \varprojlim H^i(\mathfrak{o}, \mathcal{A}^0_{p^v}).$$

Remark.

$$\mathrm{Hom}_{\mathbb{Z}_p}(H^i(\mathfrak{o}, T_p(\mathcal{A})), \mathbb{Z}_p) = (H^i(\mathfrak{o}, \mathcal{A}^0(p))^*)_{\mathrm{Tor}}.$$

Proof. The projective system of nondegenerate pairings between finite groups

$$H^i(\mathfrak{o}, \mathcal{A}^0_{p^v}) \times \mathrm{Hom}(H^i(\mathfrak{o}, \mathcal{A}^0_{p^v}), \mathbb{Z}/p^v\mathbb{Z}) \to \mathbb{Z}/p^v\mathbb{Z}$$

induces a pairing

$$H^i(\mathfrak{o}, T_p(\mathcal{A})) \times H^i(\mathfrak{o}, \mathcal{A}^0(p))^* \to \mathbb{Z}_p$$

of finitely generated $\mathbb{Z}_p$-modules. From the exact sequences (use SGA 7 IX 2.2.1)

$$H^i(\mathfrak{o}, T_p(\mathcal{A})) \xrightarrow{p^v} H^i(\mathfrak{o}, T_p(\mathcal{A})) \longrightarrow H^i(\mathfrak{o}, \mathcal{A}^0_{p^v}) \longrightarrow \mathrm{Tor}\, H^{i+1}(\mathfrak{o}, T_p(\mathcal{A}))$$

and

$$H^i(\mathfrak{o}, \mathcal{A}^0(p))^* \xrightarrow{p^v} H^i(\mathfrak{o}, \mathcal{A}^0(p))^* \longrightarrow H^i(\mathfrak{o}, \mathcal{A}^0_{p^v})^* \longrightarrow \mathrm{Tor}\, H^{i-1}(\mathfrak{o}, \mathcal{A}^0(p))^*$$

we see that the orders of the cokernels of the injective maps

$$H^i(\mathfrak{o}, T_p(\mathcal{A}))/p^v \to H^i(\mathfrak{o}, \mathcal{A}^0_{p^v})$$

and

$$H^i(\mathfrak{o}, \mathcal{A}^0(p))^*/p^v \to H^i(\mathfrak{o}, \mathcal{A}^0_{p^v})^*$$

are bounded independently of v. This implies the $\mathbb{Z}_p$-unimodularity of the above pairing (modulo torsion). q.e.d.

We thus have

$$(H^1(\mathfrak{o}, \mathcal{A}^0(p))^*)_{\mathrm{Tor}} = \mathrm{Hom}_{\mathbb{Z}_p}(H^1(\mathfrak{o}, T_p(\mathcal{A})), \mathbb{Z}_p)$$

and, according to the global flat duality theorem,

$$H^2(\mathfrak{o}, \mathcal{A}(p))^* = H^1(\mathfrak{o}, T_p(\tilde{\mathcal{A}}))$$

where, as before, $\tilde{\mathcal{A}}$ is the Néron model of the dual abelian variety $\tilde{A}$. Let us consider the sequence of maps

$$\begin{array}{ccc}
H^1(\mathfrak{o}, T_p(\tilde{\mathcal{A}})) & & \mathrm{Hom}_{\mathbb{Z}_p}(H^1(\mathfrak{o}, T_p(\mathcal{A})), \mathbb{Z}_p) \\
\| & & \| \\
 & & (H^1(\mathfrak{o}, \mathcal{A}^0(p))^*)_{\mathrm{Tor}} \\
 & & \uparrow \\
H^2(\mathfrak{o}, \mathcal{A}(p))^* & & H^1(\mathfrak{o}, \mathcal{A}(p))^* \\
\uparrow{\scriptstyle \beta^*} & & \\
H^2(\mathfrak{o}_\infty/\mathfrak{o}, \mathcal{A}(p))^* & & \uparrow{\scriptstyle \alpha^*} \\
\downarrow{\scriptstyle \gamma^*} & & \\
H^1(\Gamma, H^1(\mathfrak{o}_\infty, \mathcal{A}(p)))^* & \xrightarrow{f^*} & H^0(\Gamma, H^1(\mathfrak{o}_\infty, \mathcal{A}(p)))^*
\end{array}$$

where α, β, γ are the obvious maps induced by the descent diagram; furthermore, if we fix a topological generator ϕ of Γ then f is defined to be the map induced by the identity on $H^1(\mathfrak{o}_\infty, \mathcal{A}(p))$ (identifying $H^1(\Gamma, .)$ with the Γ-coinvariants). In the following we assume that A is ordinary for k_∞! From Propositions 1 and 2 and the descent diagram we then know that

α^* is a quasi-isomorphism,

β^* is injective with finite cokernel, and

γ^* is surjective.

The above sequence therefore determines a unique pairing

$$\langle\!\langle\ ,\ \rangle\!\rangle_\phi : H^1(\mathfrak{o}, T_p(\tilde{\mathcal{A}})) \times H^1(\mathfrak{o}, T_p(\mathcal{A})) \to \mathbb{Q}_p$$

which is nondegenerate if and only if γ and f are quasi-isomorphisms; in that case

$$|\det\langle\!\langle\ ,\ \rangle\!\rangle_\phi|_p^{-1} = \frac{\#\ker \mathrm{Div}(\gamma\circ f\circ\alpha)}{\#\ker \mathrm{Div}\,\beta} \cdot I$$

with

$$I := \#\ker(\mathrm{Div}\, H^1(\mathfrak{o}, \mathcal{A}^0(p)) \to \mathrm{Div}\, H^1(\mathfrak{o}, \mathcal{A}(p)))$$

holds true. Later on we will fix a nontrivial continuous character $\kappa\colon \Gamma \to \mathbb{Z}_p^\times$. The modified pairing

$$\langle\!\langle\ ,\ \rangle\!\rangle_\kappa := \langle\!\langle\ ,\ \rangle\!\rangle_\phi \cdot \log_p \kappa(\phi)$$

then is independent of the special choice of $\phi \in \Gamma$.

Lemma 4. *We have the canonical exact sequence*

$$0 \to \mathscr{A}^0(o) \otimes \mathbb{Z}_p \to H^1(o, T_p(\mathscr{A})) \to T_p(Ш_k(A)) \to 0$$

where $Ш_k(A)$ denotes the Tate-Šafarevič group of $A_{/k}$.

Proof. As on p. 279 in [20] we consider the commutative exact diagrams

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{A}_{p^v} \arrow[r] & \mathscr{A} \arrow[r, "\alpha_v"] \arrow[dr, "p^v"'] & \bar{\mathscr{A}} \arrow[r] \arrow[d, "\cong"] & 0 \\ & & & \mathscr{A} & \end{tikzcd}$$

(for v big enough) and as in the proof of loc. cit. (6.7) we derive from them the exact sequences

$$0 \to \mathscr{A}^0(o) \otimes \mathbb{Z}_p \to H^1(o, T_p(\mathscr{A})) \to \varprojlim H^1(o, \mathscr{A})_{\alpha_v = 0} \to 0$$

and

$$0 \to H^1(o, \mathscr{A})_{\alpha_v = 0} \to H^1(o, \mathscr{A})_{p^v} \to \ker(H^1(o, \bar{\mathscr{A}}) \to H^1(o, \mathscr{A})).$$

But $H^1(o, \bar{\mathscr{A}}) \to H^1(o, \mathscr{A})$ is a quasi-isomorphism and therefore

$$\varprojlim H^1(o, \mathscr{A})_{\alpha_v = 0} = \varprojlim H^1(o, \mathscr{A})_{p^v}.$$

Since $Ш_k(A)(p)$ is the image of the quasi-isomorphism $H^1(o, \mathscr{A}^0)(p) \to H^1(o, \mathscr{A})(p)$ (see [13] appendix) we furthermore have

$$\varprojlim H^1(o, \mathscr{A})_{p^v} = T_p(Ш_k(A)). \quad \text{q.e.d.}$$

By restriction and extension $\langle\langle\ ,\ \rangle\rangle_\kappa$ therefore induces a pairing

$$\langle\ ,\ \rangle_\kappa \colon \tilde{A}(k) \times A(k) \to \mathbb{Q}_p$$

which we call the *algebraic p-adic height pairing* associated with κ.

Theorem 1. *Let A be ordinary for k_∞, and suppose that $\langle\langle\ ,\ \rangle\rangle_\phi$ is nondegenerate. We then have:*

i) $H^1(o_\infty, \mathscr{A}(p))^*$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$-torsion module;

ii) $H^2(o_\infty, \mathscr{A}(p))^* = \varprojlim \tilde{A}(k_n)(p)$ is a finitely generated free $\mathbb{Z}_p$-module; $H^2(o_\infty, \mathscr{A}(p))_\Gamma = 0$ and $H^2(o_\infty, \mathscr{A}(p))^\Gamma$ is finite; here k_n is defined to be that intermediate layer of k_∞/k with $[k_n : k] = p^n$;

iii) if $\Sigma = \{\mathfrak{p}/p\}$ and p is unramified in k then $H^1(o_\infty, \mathscr{A}(p))^*$ has no nonzero finite Γ-submodules.

Remark. 1) $H^0(o_\infty, \mathscr{A}(p))^*$ is a finitely generated $\mathbb{Z}_p$-module and $H^i(o_\infty, \mathscr{A}(p)) = 0$ for $i \geqq 3$.

2) Because of Lemma 4 the second assumption in the theorem can be replaced by the following one: $Ш_k(A)(p)$ is finite and $\langle\ ,\ \rangle_\kappa$ is nondegenerate.

3) If k_∞/k is the cyclotomic $\mathbb{Z}_p$-extension then $H^2(o_\infty, \mathscr{A}(p)) = 0$ under the assumptions of the above theorem; according to [5] we namely have $\#\operatorname{Tor} \tilde{A}(k_\infty) < \infty$ in that case. Other $\mathbb{Z}_p$-extensions with that property are discussed in [23].

4) From the local theory (i.e., the considerations on p. 283/284 in [20] and the results of [8]) it seems very likely that in general $H^1(o_\infty, \mathscr{A}(p))^*$ has nonzero finite Γ-submodules even if k_∞ is the cyclotomic $\mathbb{Z}_p$-extension.

For the proof we need a whole series of preliminary results. These sometimes have interest in there own right and we then state them in a more general form than necessary. Let o', resp. o_n, be the ring of p-integers in k, resp. the ring of integers in k_n, and put $\Gamma_n := \operatorname{Gal}(k_\infty/k_n)$.

Lemma 5.

$$\operatorname{cd}_p(o'_{\text{et}}) \leqq 2.$$

Proof. Since any torsion sheaf of abelian groups on o'_{et} is the direct limit of its constructible subsheaves (SGA 4 IX 2.9) it suffices to prove

$$H^i_{\text{et}}(o', \mathscr{F}) = 0 \quad \text{for } i > 2$$

and any constructible p-torsion sheaf $\mathscr{F}$ on o'_{et}. For $i > 3$ this is done in [14] §3 Prop. C. Let $U \subseteq \operatorname{Spec}(o')$ be a nonempty open subscheme such that $\mathscr{F}_{/U}$ is locally constant, and denote by

$$U \xrightarrow{\sigma} \operatorname{Spec}(o') \xrightarrow{j} \operatorname{Spec}(o)$$

the canonical open immersions. We first consider the spectral sequence

$$H^r_{\text{et}}(o', \underline{\operatorname{Ext}}^s_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m)) \Rightarrow \operatorname{Ext}^{r+s}_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m).$$

According to SGA $4\frac{1}{2}$ [Dualité] Theorem 1.3 we have

$$\underline{\operatorname{Hom}}_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m) = \sigma_* \underline{\operatorname{Hom}}_U(\mathscr{F}, \mathbb{G}_m)$$

and

$$\underline{\operatorname{Ext}}^s_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m) = 0 \quad \text{for } s > 0$$

and therefore

$$H^i_{\text{et}}(o', \sigma_* \underline{\operatorname{Hom}}_U(\mathscr{F}, \mathbb{G}_m)) = \operatorname{Ext}^i_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m).$$

On the other hand, from Artin-Verdier duality (and the fact that $j_!$ and j^* are exact and $j_!$ is left adjoint to j^*) we get the nondegenerate pairings of finite groups

$$H^i_{\text{et}}(o, j_! \sigma_*(\mathscr{F}_{/U})) \times \operatorname{Ext}^{3-i}_{o'_{\text{et}}}(\sigma_*(\mathscr{F}_{/U}), \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}.$$

Thus $H^3_{\text{et}}(o', \sigma_*(\mathscr{F}_{/U}))$ is dual to $H^0_{\text{et}}(o, j_! \sigma_*(\check{\mathscr{F}}_{/U}))$ with $\check{\mathscr{F}} := \underline{\operatorname{Hom}}_{o'_{\text{et}}}(\mathscr{F}, \mathbb{G}_m)$. But one easily checks that

$$H^0_{\text{et}}(o, j_! \sigma_*(\check{\mathscr{F}}_{/U})) = 0.$$

Finally, since kernel and cokernel of the canonical homomorphism $\mathscr{F} \to \sigma_*(\mathscr{F}_{/U})$ are skyscraper sheaves, the vanishing of $H^3_{\text{et}}(o', \sigma_*(\mathscr{F}_{/U}))$ implies $H^3_{\text{et}}(o', \mathscr{F}) = 0$. q.e.d.

The next result implicitly is contained in [13].

Lemma 6. *If A has ordinary good reduction at $\mathfrak{p}\in\Sigma$ then $H^1(k_{\mathfrak{p},\infty},A)(p)^*$ is a finitely generated $\mathbb{Z}_p[\![\Gamma_{\mathfrak{p}}]\!]$-module of rank $[k_{\mathfrak{p}}:\mathbb{Q}_p]\cdot\dim A$ with $H^1(\Gamma_{\mathfrak{p}},H^1(k_{\mathfrak{p},\infty},A))=0$. It is free if, moreover, $\mathfrak{p}$ is unramified in $k/\mathbb{Q}$.*

Proof. By the structure theory of $\mathbb{Z}_p[\![\Gamma_{\mathfrak{p}}]\!]$-modules and by change of the base field it suffices to show that

$$\operatorname{corank} H^1(k_{\mathfrak{p},\infty},A)(p)^{\Gamma_{\mathfrak{p}}}=[k_{\mathfrak{p}}:\mathbb{Q}_p]\cdot\dim A$$

in order to prove the first assertion. From Proposition 1 we know that the map

$$H^1(k_{\mathfrak{p}},A)(p)\to H^1(k_{\mathfrak{p},\infty},A)(p)^{\Gamma_{\mathfrak{p}}}$$

is surjective with finite kernel. In addition, the group $H^1(\Gamma_{\mathfrak{p}},H^1(k_{\mathfrak{p},\infty},A))$ always is a subquotient of $H^2(k_{\mathfrak{p}},A)$. On the other hand, according to Tate's local duality theorem, we have

$$H^1(k_{\mathfrak{p}},A)(p)^*=\tilde{A}(k_{\mathfrak{p}})\otimes\mathbb{Z}_p \quad\text{and}\quad H^2(k_{\mathfrak{p}},A)=0.$$

But $\operatorname{rank}_{\mathbb{Z}_p}\tilde{A}(k_{\mathfrak{p}})\otimes\mathbb{Z}_p=[k_{\mathfrak{p}}:\mathbb{Q}_p]\cdot\dim A$. The second assertion is proved in the same way as Corollary 5.12 in [13].

Lemma 7. i) $H^i_\Sigma(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))=0$ *for* $i\neq 2$;

ii) *if A is ordinary for k_∞ and p is unramified in k, then $H^2_\Sigma(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))$ is divisible.*

Proof. Let $\mathfrak{o}_{\infty,\mathfrak{P}}$ be the Henselization of $\mathfrak{o}_\infty$ at $\mathfrak{P}/\mathfrak{p}\in\Sigma$. From the spectral sequence

$$H^i(\Gamma,\bigoplus_{\mathfrak{P}/\mathfrak{p}\in\Sigma}H^j_{\cdot}(\mathfrak{o}_{\infty,\mathfrak{P}},\mathscr{A}(p)))\Rightarrow H^{i+j}_\Sigma(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))$$

and the vanishing of $H^j_{\cdot}(\mathfrak{o}_{\infty,\mathfrak{P}},\mathscr{A}(p))$ for $j\neq 2$ (see [20] (3.5)) follows

$$H^i_\Sigma(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))=\begin{cases}H^0(\Gamma,\bigoplus_{\mathfrak{P}}H^2_{\cdot}(\mathfrak{o}_{\infty,\mathfrak{P}},\mathscr{A}(p))) & \text{for } i=2,\\ H^1(\Gamma,\bigoplus_{\mathfrak{P}}H^2_{\cdot}(\mathfrak{o}_{\infty,\mathfrak{P}},\mathscr{A}(p))) & \text{for } i=3,\\ 0 & \text{for } i\neq 2,3.\end{cases}$$

Because of

$$H^i(\Gamma,\bigoplus_{\mathfrak{P}}H^2_{\cdot}(\mathfrak{o}_{\infty,\mathfrak{P}},\mathscr{A}(p)))=\bigoplus_{\mathfrak{p}\in\Sigma}H^i(\Gamma_{\mathfrak{p}},H^1(k_{\mathfrak{p},\infty},A)(p))$$

(use [13] (5.2)) and the previous lemma we simply have to observe that $\mathbb{Z}_p[\![\Gamma_{\mathfrak{p}}]\!]_{\Gamma_{\mathfrak{p}}}=\mathbb{Z}_p$.

Proposition 8. *Suppose that $H^2(\mathfrak{o}_n,\mathscr{A}(p))\to H^2(\mathfrak{o}_\infty/\mathfrak{o}_n,\mathscr{A}(p))$ is surjective for all $n\in\mathbb{N}$ (for example, if A is ordinary for k_∞). We then have an exact sequence of $\mathbb{Z}_p[\![\Gamma]\!]$-modules*

$$0\to\varprojlim\tilde{A}(k_n)(p)\to H^2(\mathfrak{o}_\infty,\mathscr{A}(p))^*\to X\to 0$$

where X is a submodule of finite index in a finitely generated free $\mathbb{Z}_p[\![\Gamma]\!]$-module.

Proof. In a first step we want to show that

$$H^2_{\cdot}(\mathfrak{o}_\infty,\mathscr{A}(p))_{\Gamma_n}=0 \quad\text{for } n\geq 0. \tag{1}$$

By change of the base field it is sufficient to consider the case $\Gamma=\Gamma_n$. From the first descent spectral sequence and the vanishing of $H^3(\mathfrak{o}_\infty,\mathscr{A}(p))$ we derive

$$H^2(\mathfrak{o}_\infty,\mathscr{A}(p))_\Gamma=H^3(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p)).$$

The relative cohomology sequence then gives the exact sequence

$$\bigoplus_{\substack{\mathfrak{p}/p\\ \mathfrak{p}\notin\Sigma}}H^3_{\cdot}(\mathfrak{o}_{\mathfrak{p}},\mathscr{A}(p))\oplus H^3_\Sigma(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))\to H^3(\mathfrak{o}_\infty/\mathfrak{o},\mathscr{A}(p))\to H^3(\mathfrak{o}',\mathscr{A}(p)).$$

But the outer terms vanish because of Lemma 5, Lemma 7i and

$$H^3_{\cdot}(\mathfrak{o}_{\mathfrak{p}},\mathscr{A}(p))=(\varprojlim\tilde{\mathscr{A}}(\mathfrak{o}_{\mathfrak{p}})_{p^\nu})^*=0 \quad\text{for } \mathfrak{p}/p.$$

Now, from Lemma 4 and the global flat duality theorem we get the exact sequences

$$0\to\tilde{\mathscr{A}}^0(\mathfrak{o}_n)(p)\to H^2(\mathfrak{o}_n,\mathscr{A}(p))^*\to H^1(\mathfrak{o}_n,T_p(\tilde{\mathscr{A}}))_{\mathrm{Tor}}\to 0$$

and passing to the projective limit the exact sequence

$$0\to N\to H^2(\mathfrak{o}_\infty,\mathscr{A}(p))^*\to X\to 0$$

with

$$N:=\varprojlim\tilde{\mathscr{A}}^0(\mathfrak{o}_n)(p)=\varprojlim\tilde{A}(k_n)(p) \quad\text{and}\quad X:=\varprojlim H^1(\mathfrak{o}_n,T_p(\tilde{\mathscr{A}}))_{\mathrm{Tor}}.$$

The finiteness of N_{Γ_n} together with (1) means that X^{Γ_n} also is finite and even

$$X^{\Gamma_n}=0 \tag{2}$$

since X is $\mathbb{Z}_p$-torsion free. We thus have the exact commutative diagram

$$\begin{array}{ccccccccc}0 & \to & N_{\Gamma_n} & \to & (H^2(\mathfrak{o}_\infty,\mathscr{A}(p))^*)_{\Gamma_n} & \to & X_{\Gamma_n} & \to & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \tilde{\mathscr{A}}^0(\mathfrak{o}_n)(p) & \to & H^2(\mathfrak{o}_n,\mathscr{A}(p))^* & \to & H^1(\mathfrak{o}_n,T_p(\tilde{\mathscr{A}}))_{\mathrm{Tor}} & \to & 0.\end{array}$$

By our assumption the middle vertical map is injective. On the other hand, the order of the cokernel of the map $N_{\Gamma_n}\to\tilde{\mathscr{A}}^0(\mathfrak{o}_n)(p)$ is bounded independently of n. Therefore

$$\#\operatorname{Tor}(X_{\Gamma_n}) \text{ is bounded independently of } n. \tag{3}$$

By the general structure theory, (2) and (3) imply the property of X asserted in the proposition. q.e.d.

We now come back to the proof of Theorem 1. The assumptions imply that the maps f and γ are quasi-isomorphisms and thus in particular

$$\operatorname{corank} H^1(o_\infty, \mathscr{A}(p))^\Gamma = \operatorname{corank} H^1(o_\infty, \mathscr{A}(p))_\Gamma$$

and

$$\# H^2(o_\infty, \mathscr{A}(p))^\Gamma < \infty.$$

It follows that $H^1(o_\infty, \mathscr{A}(p))^*$ and $H^2(o_\infty, \mathscr{A}(p))^*$ are finitely generated $\mathbb{Z}_p[[\Gamma]]$-torsion modules. Taking Proposition 8 into consideration this establishes the first and second part of the theorem. In order to prove the third part we will show that $H^1(\Gamma, H^1(o_\infty, \mathscr{A}(p)))$ is divisible; our assertion namely is a consequence of that fact by a general property of pro-p-groups ([21] I-32). Since $H^2(o_\infty, \mathscr{A}(p))^\Gamma$ is finite, it suffices to prove divisibility for $H^2(o_\infty/o, \mathscr{A}(p))$ (look at the descent diagram). We use the relative cohomology sequence

$$H^2_\Sigma(o_\infty/o, \mathscr{A}(p)) \to H^2(o_\infty/o, \mathscr{A}(p)) \to H^2(o', \mathscr{A}(p)) \to H^3_\Sigma(o_\infty/o, \mathscr{A}(p)).$$

According to Lemma 7 the first term is divisible and the last one vanishes. But $H^2(o', \mathscr{A}(p)) = H^2_{\text{et}}(o', \mathscr{A}(p))$ is divisible, too. Namely, since the cokernel of $\mathscr{A}^0(p)_{/o'_{\text{et}}} \to \mathscr{A}(p)_{/o'_{\text{et}}}$ is a skyscraper sheaf that follows from the divisibility of $H^2_{\text{et}}(o', \mathscr{A}^0(p))$ which itself is derived from Lemma 5 using the exact sequence

$$H^2_{\text{et}}(o', \mathscr{A}^0(p)) \xrightarrow{p} H^2_{\text{et}}(o', \mathscr{A}^0(p)) \longrightarrow H^3_{\text{et}}(o', \mathscr{A}^0_p). \quad \text{q.e.d.}$$

We certainly should remark that Theorem 1 is a really conditional statement in the sense that there exist examples where A is ordinary for k_∞ but $H^1(o_\infty, \mathscr{A}(p))^*$ is not a $\mathbb{Z}_p[[\Gamma]]$-torsion module. One may hope that $\langle\langle\, , \rangle\rangle_\phi$ always is nondegenerate if k_∞/k is the cyclotomic $\mathbb{Z}_p$-extension. An "unconditional" but not very precise statement is the following one.

Proposition 9. *If A is ordinary for k_∞ then*

$$\operatorname{Defect}(\langle\langle\, , \rangle\rangle_\phi) \geqq \operatorname{rank}_{\mathbb{Z}_p[[\Gamma]]} H^2(o_\infty, \mathscr{A}(p))^* = \operatorname{rank}_{\mathbb{Z}_p[[\Gamma]]} H^1(o_\infty, \mathscr{A}(p))^*.$$

Proof. (The defect of a pairing, by definition, is the rank of its nullspaces.) It is easy to see that

$$\operatorname{Defect}(\langle\langle\, , \rangle\rangle_\phi) \geqq \operatorname{rank}_{\mathbb{Z}_p}(\ker \gamma^*) = \operatorname{corank} H^0(\Gamma, H^2(o_\infty, \mathscr{A}(p))).$$

But Proposition 8 implies that the right hand side is nothing else than the $\mathbb{Z}_p[[\Gamma]]$-rank of $H^2(o_\infty, \mathscr{A}(p))^*$. The equality in the statement can be derived from the descent diagram; instead of doing that we will give a more conceptual proof of it in Paragraph 3.

The equality sign would hold in the above proposition if and only if the action of Γ upon $H^1(o_\infty, \mathscr{A}(p))$ fulfills a certain partial semi-simplicity property. But G. Brattström has computed examples where strict inequality occurs.

§ 2. Birch and Swinnerton-Dyer formulas

We now are ready to improve Theorem 5 of [20]. Fixing a nontrivial continuous character $\kappa\colon \Gamma \to \mathbb{Z}_p^\times$ we always assume that the following conditions are fulfilled.

Hypotheses (H): A is ordinary for k_∞ and $\langle\langle\, , \rangle\rangle_\kappa$ is nondegenerate.

Because of Theorem 1 the characteristic polynomials

$$F_i(t) := p^{\mu(H_i)} \cdot \det(t - (\phi - 1); H_i \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$$

of the $\mathbb{Z}_p[[\Gamma]]$-modules $H_i := H^i(o_\infty, \mathscr{A}(p))^*$ then are defined; here, $\mu(H_i)$ denotes the μ-invariant of H_i which can be nonzero only for $i = 1$. We call

$$L_p(A, \kappa, s) := \prod_{i \geqq 0} F_i(\kappa(\phi)^{1-s} - 1)^{(-1)^{i+1}} \qquad (s \in \mathbb{Z}_p)$$

the *Iwasawa L-function* of A with respect to κ.

Remark. In the case of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k and the cyclotomic character κ the L-function $L_p(A, \kappa, s)$ is the same as the L-function $L_p^{(1)}(A, s)$ considered in [20].

We want to determine the integer

$$m := \text{multiplicity of the zero of } L_p(A, \kappa, s) \text{ at } s = 1$$

and up to a p-adic unit (indicated by $\sim$) also the leading coefficient

$$c := [L_p(A, \kappa, s) \cdot (s-1)^{-m}]_{s=1}.$$

Proposition 1. *Assuming (H), we have $m = \operatorname{rank}_{\mathbb{Z}_p} H^1(o, T_p(\mathscr{A}))$ and*

$$c \sim \frac{\det \langle\langle\, , \rangle\rangle_\kappa}{I} \cdot \prod_{i \geqq 0} \# H^i(o, \mathscr{A}(p))_{\text{Div}}^{(-1)^{i+1}} \cdot \Big(\prod_{p \in \Sigma} \# \mathscr{A}(\kappa_p)\Big)^2.$$

Proof. Reformulate the proof of [20] (8.2) in the present context (using, of course, Theorem 1 i) and ii)).

We recall that by definition

$$I = \# \ker(\operatorname{Div} H^1(o, \mathscr{A}^0(p)) \to \operatorname{Div} H^1(o, \mathscr{A}(p)));$$

let $\tilde{I}$ be the order of the corresponding kernel for the dual abelian variety $\tilde{A}$.

Lemma 2.

$$\prod_{i \geqq 0} \# H^i(o, \mathscr{A}(p))_{\text{Div}}^{(-1)^{i+1}} = \tilde{I}^{-1} \cdot \frac{\# Ш_k(A)(p)_{\text{Div}}}{\# A(k)(p) \cdot \# \tilde{A}(k)(p)} \cdot \prod_{p} \# \pi_p(A)(p)$$

where $\pi_p(A)$ denotes the group of connected components of $\mathscr{A} \times_o \kappa_p$.

Proof. We have $H^0(o, \mathscr{A}(p))_{\text{Div}} = A(k)(p)$ and, according to the global flat duality theorem and Lemma (1.4),

$$(H^2(o, \mathscr{A}(p))_{\text{Div}})^* = \operatorname{Tor} H^1(o, T_p(\tilde{\mathscr{A}})) = \tilde{\mathscr{A}}^0(o)(p).$$

In order to compute $\# H^1(\mathcal{o},\mathscr{A}(p))_{\mathrm{Div}}$ we start from the exact sequence

$$0\to(\tilde{A}(k)/\tilde{\mathscr{A}}^0(\mathcal{o}))(p)\to\bigoplus_{\mathfrak{p}}\pi_{\mathfrak{p}}(\tilde{A})(p)\to H^1(\mathcal{o},\tilde{\mathscr{A}}^0)(p)\to Ш_k(\tilde{A})(p)\to 0$$

which is established in [13] (appendix). It gives

$$\# H^1(\mathcal{o},\tilde{\mathscr{A}}^0)(p)_{\mathrm{Div}}=\tilde{\mathscr{I}}^{-1}\cdot|[\tilde{A}(k):\tilde{\mathscr{A}}^0(\mathcal{o})]|_p\cdot\# Ш_k(\tilde{A})(p)_{\mathrm{Div}}\cdot\prod_{\mathfrak{p}}\#\pi_{\mathfrak{p}}(\tilde{A})(p)$$

with

$$\begin{aligned}\tilde{\mathscr{I}}:&=\#\ker(\mathrm{Div}\,H^1(\mathcal{o},\tilde{\mathscr{A}}^0)(p)\to\mathrm{Div}\,Ш_k(\tilde{A})(p))\\&=\#\ker(\mathrm{Div}\,H^1(\mathcal{o},\tilde{\mathscr{A}}^0)(p)\to\mathrm{Div}\,H^1(\mathcal{o},\tilde{\mathscr{A}})(p)).\end{aligned}$$

But we have $\# Ш_k(\tilde{A})(p)_{\mathrm{Div}}=\# Ш_k(A)(p)_{\mathrm{Div}}$ and $\#\pi_{\mathfrak{p}}(\tilde{A})(p)=\#\pi_{\mathfrak{p}}(A)(p)$. According to [20] (8.3) the group $H^1(\mathcal{o},\tilde{\mathscr{A}}^0)(p)_{\mathrm{Div}}$ is dual to $H^1(\mathcal{o},\mathscr{A}(p))_{\mathrm{Div}}$. Finally, using [20] (6.6) we see that

$$\tilde{\mathscr{I}}=\tilde{I}\cdot|[\tilde{A}(k)_{\mathrm{Tor}}:\tilde{\mathscr{A}}^0(\mathcal{o})_{\mathrm{Tor}}]|_p$$

holds true. We thus get

$$\# H^1(\mathcal{o},\mathscr{A}(p))_{\mathrm{Div}}=\tilde{I}^{-1}\cdot\# Ш_k(A)(p)_{\mathrm{Div}}\cdot\prod_{\mathfrak{p}}\#\pi_{\mathfrak{p}}(A)(p)\cdot\frac{\#\tilde{\mathscr{A}}^0(\mathcal{o})(p)}{\#\tilde{A}(k)(p)}.\qquad\text{q.e.d.}$$

Combining the above two statements leads to the main result.

Theorem 2. *Assuming (H), we have* $m=\mathrm{rank}_{\mathbb{Z}_p}H^1(\mathcal{o},T_p(\mathscr{A}))$ *and*

$$c\sim\frac{\det\langle\!\langle\,,\,\rangle\!\rangle_\kappa\cdot\# Ш_k(A)(p)_{\mathrm{Div}}}{I\cdot\tilde{I}\cdot\#\mathrm{Tor}\,A(k)\cdot\#\mathrm{Tor}\,\tilde{A}(k)}\cdot\prod_{\mathfrak{p}}\#\pi_{\mathfrak{p}}(A)\cdot\big(\prod_{\mathfrak{p}\in\Sigma}\#\mathscr{A}(\kappa_{\mathfrak{p}})\big)^2.$$

Using Lemma (1.4) and [20] (6.6) we can formulate this result in a different way which shows an astonishing analogy to the complex Birch and Swinnerton-Dyer conjecture.

Theorem 2′. *Let A be ordinary for k_∞, and suppose that $Ш_k(A)(p)$ is finite and that $\langle\,,\,\rangle_\kappa$ is nondegenerate. We then have $m=\mathrm{rank}_{\mathbb{Z}}A(k)$ and*

$$c\sim\frac{\det\langle\,,\,\rangle_\kappa\cdot\# Ш_k(A)(p)}{\#\mathrm{Tor}\,A(k)\cdot\#\mathrm{Tor}\,\tilde{A}(k)}\cdot\prod_{\mathfrak{p}}\#\pi_{\mathfrak{p}}(A)\cdot\big(\prod_{\mathfrak{p}\in\Sigma}\#\mathscr{A}(\kappa_{\mathfrak{p}})\big)^2.$$

We mention that in the context of elliptic curves with complex multiplication similar theorems are contained in [2] and [17]. In Sect. B we shall prove that the pairing $\langle\,,\,\rangle_\kappa$ is equal to the corresponding analytic p-adic height pairing as defined in [19]. It seems that such an identification is fundamental for any future proof of the nondegeneracy of $\langle\,,\,\rangle_\kappa$ in the cyclotomic case. On the other hand, it might be an interesting problem to decide whether the nondegeneracy of $\langle\!\langle\,,\,\rangle\!\rangle_\kappa$ already implies the finiteness of $Ш_k(A)(p)$.

We conclude this paragraph by making the remark that $L_p(A,\kappa,s)$ has a functional equation with respect to $s\mapsto 2-s$. For the polynomial $F_1(t)$ this is proved in [13]. So, we only have to observe that

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}_p}(H_2,\mathbb{Z}_p)&=\mathrm{Hom}_{\mathbb{Z}_p}(\varprojlim\tilde{A}(k_n)(p),\mathbb{Z}_p)=\mathrm{Hom}_{\mathbb{Z}_p}(\varprojlim\tilde{A}(k_\infty)_{p^\nu},\mathbb{Z}_p)\\&=(\tilde{A}(k_\infty)(p)^*)_{\mathrm{Tor}}=(H^0(\mathcal{o}_\infty,\tilde{\mathscr{A}}(p))^*)_{\mathrm{Tor}}\end{aligned}$$

and therefore by using a k-polarization of A

$$\mathrm{Hom}_{\mathbb{Q}_p}(H_2\otimes_{\mathbb{Z}_p}\mathbb{Q}_p,\mathbb{Q}_p)\cong H_0\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$$

holds true.

§ 3. The nonordinary case

We also want to discuss what the ranks of the various $\mathbb{Z}_p[\![\Gamma]\!]$-modules might be if A is not assumed to be ordinary for k_∞. Define

$$\rho:=\mathrm{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}H^1(\mathcal{o}_\infty,\mathscr{A}(p))^*,$$

$$\rho':=\mathrm{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}H^2(\mathcal{o}_\infty,\mathscr{A}(p))^*,$$

and

$$\rho_{\mathfrak{p}}:=\mathrm{rank}_{\mathbb{Z}_p[\![\Gamma_{\mathfrak{p}}]\!]}H^1(k_{\mathfrak{p},\infty},A)(p)^*\quad\text{for }\mathfrak{p}\in\Sigma.$$

We first compute some Euler characteristics.

Lemma 1. i) $\sum_{i\geq 0}(-1)^i\,\mathrm{corank}\,H^i(\mathcal{o},\mathscr{A}(p))=0;$

ii) $\sum_{i\geq 0}(-1)^i\,\mathrm{corank}\,H^i(\mathcal{o}_\infty/\mathcal{o},\mathscr{A}(p))=\rho'-\rho;$

iii) $\sum_{i\geq 0}(-1)^i\,\mathrm{corank}\,H^i_\Sigma(\mathcal{o},\mathscr{A}(p))=\dim A\cdot\big(\sum_{\mathfrak{p}\in\Sigma}[k_{\mathfrak{p}}:\mathbb{Q}_p]\big);$

iv) $\sum_{i\geq 0}(-1)^i\,\mathrm{corank}\,H^i_\Sigma(\mathcal{o}_\infty/\mathcal{o},\mathscr{A}(p))=\sum_{\mathfrak{p}\in\Sigma}\rho_{\mathfrak{p}}.$

Proof. i) We have to show that

$$\mathrm{corank}\,H^1(\mathcal{o},\mathscr{A}(p))=\mathrm{corank}\,H^2(\mathcal{o},\mathscr{A}(p))$$

holds true (compare [20] (6.4)). According to loc. cit. (6.6) and [13] (appendix) we have

$$\begin{aligned}\mathrm{corank}\,H^1(\mathcal{o},\mathscr{A}(p))&=\mathrm{rank}_{\mathbb{Z}}A(k)+\mathrm{corank}\,H^1(\mathcal{o},\mathscr{A})(p)\\&=\mathrm{rank}_{\mathbb{Z}}A(k)+\mathrm{rank}_{\mathbb{Z}_p}T_p(Ш_k(A)).\end{aligned}$$

On the other hand using the fact that A and $\tilde{A}$ are k-isogenous, the global flat duality theorem, and Lemma (1.4) we get

$$\begin{aligned}\mathrm{corank}\,H^2(\mathcal{o},\mathscr{A}(p))&=\mathrm{corank}\,H^2(\mathcal{o},\tilde{\mathscr{A}}(p))=\mathrm{rank}_{\mathbb{Z}_p}H^1(\mathcal{o},T_p(\mathscr{A}))\\&=\mathrm{rank}_{\mathbb{Z}}A(k)+\mathrm{rank}_{\mathbb{Z}_p}T_p(Ш_k(A)).\end{aligned}$$

ii) This comes out of the first descent spectral sequence taking $H^i(\mathcal{o}_\infty,\mathscr{A}(p))=0$ for $i\geq 3$ into respect.

iii) Using [20] (3.4) we get

$$\sum_{i\geq 0}(-1)^i \operatorname{corank} H^i_\Sigma(\mathscr{o},\mathscr{A}(p)) = \sum_{\mathfrak{p}\in\Sigma}(\operatorname{corank} H^2(\mathscr{o}_\mathfrak{p},\mathscr{A}(p)) - \operatorname{corank} H^3(\mathscr{o}_\mathfrak{p},\mathscr{A}(p))).$$

But applying the local flat duality theorem we easily see that

$$\operatorname{corank} H^3(\mathscr{o}_\mathfrak{p},\mathscr{A}(p)) = \operatorname{rank}_{\mathbb{Z}_p} \varprojlim \tilde{A}(k_\mathfrak{p})_{p^\nu} = 0.$$

Finally, in [13] (5.3) the equality

$$\operatorname{corank} H^2(\mathscr{o}_\mathfrak{p},\mathscr{A}(p)) = \dim A\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$$

is proved.

iv) Compare the proof of Lemma (1.7).

Lemma 2.

$$\rho = \rho' + \sum_{\mathfrak{p}\in\Sigma}(\dim A\cdot[k_\mathfrak{p}:\mathbb{Q}_p] - \rho_\mathfrak{p}).$$

Proof. This is a consequence of Lemma 1 and Lemma (1.3).

From Lemma (1.6) we know that $\rho_\mathfrak{p} = \dim A\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$ if A has ordinary good reduction at $\mathfrak{p}$. This proves the following result.

Proposition 3. *If A is ordinary for k_∞ then $\rho=\rho'$.*

We guess that $\rho_\mathfrak{p}$ is equal to $r_\mathfrak{p}\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$ where

$$r_\mathfrak{p} := p\text{-rank of the reduction } \mathscr{A}_{/\kappa_\mathfrak{p}}$$

(i.e., $p^{r_\mathfrak{p}} = \#\mathscr{A}(\bar\kappa_\mathfrak{p})_p$). As we shall see the computation of $\rho_\mathfrak{p}$ can be reduced to a problem about universal norm subgroups of formal Lie groups, which is not solved in general.* We therefore can prove the above equality only if $r_\mathfrak{p}\geq\dim A-1$. Nevertheless the main argument should be presented in its general setting.

Let $\mathscr{G}$ be a p-divisible group over $\mathscr{o}_\mathfrak{p}$ and denote by $\tilde{\mathscr{G}}$ the dual p-divisible group. We have the canonical exact sequences

$$0\to\mathscr{G}^0\to\mathscr{G}\to\mathscr{G}^{\mathrm{et}}\to 0$$

and

$$0\to\mathscr{G}^{\mathrm{mult}}\to\mathscr{G}^0\to\mathscr{G}^{00}\to 0$$

of p-divisible groups over $\mathscr{o}_\mathfrak{p}$ where $\mathscr{G}^{\mathrm{et}}$, resp. $\mathscr{G}^0$, is the etale, resp. connected, part of $\mathscr{G}$ and $(\mathscr{G}^{\mathrm{mult}})\tilde{}$, resp. $(\mathscr{G}^{00})\tilde{}$, is the etale, resp. connected, part of $(\mathscr{G}^0)\tilde{}$. Because of

$$H^3(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G}^0) = H^3(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G}^{\mathrm{mult}}) = H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G}^{\mathrm{mult}}) = 0$$

([20] (3.5)), where $\mathscr{o}_{\mathfrak{p},\infty}$ denotes the ring of integers in $k_{\mathfrak{p},\infty}$, we get the exact sequence

$$H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G}^{00})\to H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G})\to H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G}^{\mathrm{et}})\to 0.$$

* In a forthcoming paper we will establish the required property of formal Lie groups in complete generality. In particular, the formula $\rho_\mathfrak{p} = r_\mathfrak{p}\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$ always holds true.

The dual groups of $\mathscr{G}^{00}$ and $\mathscr{G}^{\mathrm{et}}$ are connected. But if $\tilde{\mathscr{G}}$ is connected we can use a description of $H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G})^*$ as projective limit of certain universal norm groups associated with $\tilde{\mathscr{G}}$. Namely, let $k_{\mathfrak{p},n}$ be the unique subfield of $k_{\mathfrak{p},\infty}$ of degree p^n over $k_\mathfrak{p}$, and denote by $\mathscr{o}_{\mathfrak{p},n}$ the ring of integers in $k_{\mathfrak{p},n}$. We put

$$N\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n}) := \bigcap_{m\geq n}\operatorname{Norm}(\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},m})).$$

From the local flat duality theorem and the assumption that $\tilde{\mathscr{G}}$ is connected we derive (compare the reasoning on p. 357 in [12])

$$H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G})^* = \varprojlim \tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n}) = \varprojlim N\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n})$$

where the projective limits are taken with respect to the norm maps.

In a first step we now assume that $\mathscr{G}$ is etale of height h. $\tilde{\mathscr{G}}$ then is a formal Lie group of dimension h of multiplicative type over $\mathscr{o}_\mathfrak{p}$. We certainly have the exact sequences

$$\begin{tikzcd}
0 \arrow[d] & \\
\varprojlim_{m\geq n} H^{-1}(G_{m,n},\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},m})) \arrow[d] & \\
(\varprojlim_{m\geq n}\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},m}))_{\Gamma_{\mathfrak{p},n}} \arrow[d] \arrow[r, equal] & (H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G})^*)_{\Gamma_{\mathfrak{p},n}} \arrow[d] \\
\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n}) \arrow[d] \arrow[r, equal] & H^2(\mathscr{o}_{\mathfrak{p},n},\mathscr{G})^* \\
\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n})/N\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n}) \arrow[d] & \\
0 &
\end{tikzcd}$$

with $\Gamma_{\mathfrak{p},n} := \operatorname{Gal}(k_{\mathfrak{p},\infty}/k_{\mathfrak{p},n})$ and $G_{m,n} := \operatorname{Gal}(k_{\mathfrak{p},m}/k_{\mathfrak{p},n})$. On the other hand, from [11] (which is a simplified version of [13] § 4) follows (combine the Lemmata 2 and 3 and the second diagram on p. 239) that we also have exact sequences

$$0\longrightarrow\varprojlim_{m\geq n} H^{-1}(G_{m,n},\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},m}))\longrightarrow(\Gamma_{\mathfrak{p},n})^h\xrightarrow{\mathrm{Id}-u}(\Gamma_{\mathfrak{p},n})^h$$
$$\longrightarrow\varprojlim_{m\geq n}\hat{H}^0(G_{m,n},\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},m})) = \tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n})/N\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n})\longrightarrow 0$$

for n big enough (such that $k_{\mathfrak{p},\infty}/k_{\mathfrak{p},n}$ is totally ramified) where u is the twist matrix of $\mathscr{G}$ over $\mathscr{o}_{\mathfrak{p},n}$. Both together imply

$$\operatorname{corank} H^2(\mathscr{o}_{\mathfrak{p},\infty},\mathscr{G})^{\Gamma_{\mathfrak{p},n}} = \operatorname{rank}_{\mathbb{Z}_p}\tilde{\mathscr{G}}(\mathscr{o}_{\mathfrak{p},n}) = h\cdot[k_{\mathfrak{p},n}:\mathbb{Q}_p]$$

for n big enough. By the general structure theory of $\mathbb{Z}_p[[\Gamma_\mathfrak{p}]]$-modules we thus have proved that $H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{G}^{et})^*$ is a finitely generated $\mathbb{Z}_p[[\Gamma_\mathfrak{p}]]$-module of rank height $(\mathcal{G}^{et})\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$.

It remains to consider the case where $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are connected. Here, there is the following result of Konovalov ([9]; see also Hazewinkel [25]).

Proposition (Konovalov). *Let $F(X, Y)$ be a commutative finite dimensional formal group law over the ring of integers R in a finite extension K of $\mathbb{Q}_p$. Assume the power series which represent the multiplication by p on the reduction of $F(X, Y)$ are power series in X^{p^2}. Then the subgroup of universal norms in $F(R)$ with respect to any totally ramified $\mathbb{Z}_p$-extension of K is trivial.*

Altogether the above considerations give a result which should be true in full generality, namely:

Proposition 4. *If $(\mathcal{G}^{00}_{/\kappa_\mathfrak{p}})^\sim$ is zero or isomorphic to a product of one-dimensional p-divisible groups, then $H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{G})^*$ is a finitely generated $\mathbb{Z}_p[[\Gamma_\mathfrak{p}]]$-module of rank* height $(\mathcal{G}^{et})\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$.

Proof. We have $H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{G}^{00})=0$ since $(\mathcal{G}^{00})^\sim$ fulfills the assumption made in the above proposition. Namely, all the one-dimensional factors of $(\mathcal{G}^{00}_{/\kappa_\mathfrak{p}})^\sim$ obviously must be of height at least 2.

Theorem 3. *If $r_\mathfrak{p} \geqq \dim A-1$ (for some $\mathfrak{p}\in\Sigma$) then $\rho_\mathfrak{p}=r_\mathfrak{p}\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$.*

Proof. We already have discussed the ordinary case. Assume therefore that $r_\mathfrak{p} =\dim A-1$. According to [13] (5.2) we have

$$H^1(k_{\mathfrak{p},\infty}, A)(p)=H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p))$$

where $\mathcal{A}(p)$ is the p-divisible group associated with $\mathcal{A}$ over $o_\mathfrak{p}$. $(\mathcal{A}(p)^{00}_{/\kappa_\mathfrak{p}})^\sim$ is the connected one-dimensional p-divisible group of height two, and height $(\mathcal{A}(p)^{et}) =$ height $(\mathcal{A}(p)^{et}_{/\kappa_\mathfrak{p}})=r_\mathfrak{p}$.

Corollary 5. *Let A be an elliptic curve. For $\mathfrak{p}\in\Sigma$ we have*

$$\rho_\mathfrak{p}=\begin{cases}[k_\mathfrak{p}:\mathbb{Q}_p] & \text{if } A \text{ is ordinary at } \mathfrak{p},\\ 0 & \text{if } A \text{ is supersingular at } \mathfrak{p},\end{cases}$$

and therefore

$$\rho=\rho'+\sum_{\substack{\mathfrak{p}\in\Sigma\\ A \text{ supersingular}\\ \text{at } \mathfrak{p}}} [k_\mathfrak{p}:\mathbb{Q}_p].$$

Remark. To prove the equality $\rho_\mathfrak{p}=r_\mathfrak{p}\cdot[k_\mathfrak{p}:\mathbb{Q}_p]$ in any case means to generalize the result of Konovalov to any connected p-divisible group with connected dual.

Next we have to discuss the rank ρ'. As already was indicated at the end of §1 the behavior of ρ' if k_∞ varies through the different $\mathbb{Z}_p$-extensions of k may be rather complicated. In order to get a general statement we have to impose a strong condition on the abelian variety A.

Lemma 6. *Assume that*

a) *$A(k)$ and $\text{Ш}_k(A)(p)$ are finite, and*

b) *$H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p)^{00})=0$ for $\mathfrak{p}\in\Sigma$.*

We then have $H^2(o_\infty, \mathcal{A}(p))^*=\varprojlim \tilde{A}(k_n)(p)$.

Proof. We first prove that

$$H^2(o_n, \mathcal{A}(p))\to H^2(o_\infty/o_n, \mathcal{A}(p))$$

is surjective for n big enough. As we have seen in the proof of Proposition (1.2) this is a local problem; it namely suffices to show the surjectivity of

$$H^2_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p))\to H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p))^{\Gamma_{\mathfrak{p},n}}$$

for n big enough and $\mathfrak{p}\in\Sigma$. Since the twist matrix of $\mathcal{A}(p)^{et}$ over $o_{\mathfrak{p},n}$ has no roots of unity as eigenvalues (otherwise $\mathcal{A}$ would have infinitely many rational points in some finite extension of $\kappa_\mathfrak{p}$ which is not possible) the considerations before Proposition 4 together with assumption b) imply that

$$H^2_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p)^{et})\to H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p)^{et})^{\Gamma_{\mathfrak{p},n}}=H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p))^{\Gamma_{\mathfrak{p},n}}$$

is surjective for n big enough. We claim that

$$H^2_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p))\to H^2_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p)^{et})$$

is surjective, too. From local flat duality and the fact that a formal Lie group has only finitely many torsion points over $o_{\mathfrak{p},n}$, resp. the above mentioned property of the twist matrix, we derive $H^3_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p)^{00})=0$, resp. $H^3_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p)^{mult})=0$, and thus $H^3_\cdot(o_{\mathfrak{p},n}, \mathcal{A}(p)^0)=0$. The first step therefore is established. The same reasoning proves that for arbitrary $n\geqq 0$ the map

$$H^2(o_n, \mathcal{A}(p))\to H^2(o_\infty/o_n, \mathcal{A}(p))$$

at least has a finite cokernel. On the other hand, it is a consequence of assumption a) that $H^2(o, \mathcal{A}(p))$ is finite (compare the proof of Lemma 1). A look at the descent diagram then shows the finiteness of $H^0(\Gamma, H^2(o_\infty, \mathcal{A}(p)))$. Combining these facts with Proposition (1.8) now gives the lemma.

Theorem 4. *Assume that $r_\mathfrak{p} \geqq \dim A-1$ for all $\mathfrak{p}\in\Sigma$ (for example, if A is an elliptic curve). If $A(k)$ and $\text{Ш}_k(A)(p)$ are finite, then we have*

$$H^2(o_\infty, \mathcal{A}(p))^*=\varprojlim \tilde{A}(k_n)(p)$$

and in particular $\rho'=0$ and

$$\rho=\sum_{\mathfrak{p}\in\Sigma}(\dim A-r_\mathfrak{p})\cdot[k_\mathfrak{p}:\mathbb{Q}_p].$$

Proof. If $r_\mathfrak{p}=\dim A$, resp. $=\dim A-1$, we have $\mathcal{A}(p)^{00}_{/o_\mathfrak{p}}=0$, resp. $H^2_\cdot(o_{\mathfrak{p},\infty}, \mathcal{A}(p)^{00})=0$ by Konovalov's result. Therefore, the assertion is a consequence of the above lemma and Theorem 3.

On the other hand we have a rather clear picture of what to expect if k_∞ is the cyclotomic $\mathbb{Z}_p$-extension. In that situation Mazur conjectures that $\rho=0$ (and therefore $\rho'=0$) holds true for any A which is ordinary for k_∞. Motivated by the analogous function field case we propose the following more general conjecture.

Conjecture. $H^2(\mathcal{o}_\infty, \mathcal{A}(p))=0$ if k_∞/k is the cyclotomic $\mathbb{Z}_p$-extension.

This vanishing statement certainly is correct under the assumptions of Theorem 4. Theorem 1 shows that for A which is ordinary for k_∞ the conjecture would be a consequence of the expected nondegeneracy of the p-adic height pairing $\langle\langle\ ,\ \rangle\rangle_\kappa$ associated with A and the cyclotomic character κ. But there is another case which we can attack. Let us call an elliptic curve A supersingular at p if it has supersingular good reduction at all primes of k above p.

Lemma 7. *Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension and denote by $\mathcal{o}'_\infty$ the ring of p-integers in k_∞. If A is an elliptic curve which is supersingular at p we have*

$$H^i(\mathcal{o}_\infty, \mathcal{A}(p))=H^i_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}(p)) \quad \textit{for } i\geqq 0.$$

Proof. From Konovalov's result we know that $H^i(\mathcal{o}_{\mathfrak{p},\infty}, \mathcal{A}(p))=0$ for $\mathfrak{p}/p$. The further proof is an argument with the relative cohomology sequence and proceeds along the same lines as the proof of (3.3) in [20].

This result connects our conjecture with a second one which turns out to be well known.

Conjecture. $\mathrm{cd}_p(\mathcal{o}'_\infty)_{\mathrm{et}}\leqq 1$ (where $\mathcal{o}'_\infty$ is the ring of p-integers in the cyclotomic $\mathbb{Z}_p$-extension).

Let us slightly modify our notation for a moment writing $\mathcal{o}'_\infty(k)$ instead of $\mathcal{o}'_\infty$.

Lemma 8. *The following assertions are equivalent:*

a) $\mathrm{cd}_p(\mathcal{o}'_\infty(k))_{\mathrm{et}}\leqq 1$ *for all finite extensions $k/\mathbb{Q}$;*

b) $H^2_{\mathrm{et}}(\mathcal{o}'_\infty(k), \mu_p)=0$ *for all finite extensions $k/\mathbb{Q}$;*

c) $\mathrm{Pic}(\mathcal{o}'_\infty(k))$ *is p-divisible for all finite extensions $k/\mathbb{Q}$;*

d) $\mathrm{Pic}(\mathcal{o}'_\infty(k))(p)^*$ *is a finitely generated $\mathbb{Z}_p$-module for all finite extensions $k/\mathbb{Q}$.*

Proof. We know that $\mathrm{cd}_p(\mathcal{o}'_\infty(k))_{\mathrm{et}}\leqq 2$ (compare [20] (3.7)). The equivalence of a) and b) then follows from SGA 4 IX § 5. The exact sequence

$$0\to\mu_p\to\mathbb{G}_m\xrightarrow{p}\mathbb{G}_m\to 0$$

of sheaves on $(\mathcal{o}'_\infty(k))_{\mathrm{et}}$ leads to the exact cohomology sequence

$$0\to\mathrm{Pic}(\mathcal{o}'_\infty(k))\otimes\mathbb{Z}/p\mathbb{Z}\to H^2_{\mathrm{et}}(\mathcal{o}'_\infty(k),\mu_p)\to H^2_{\mathrm{et}}(\mathcal{o}'_\infty(k),\mathbb{G}_m)_p\to 0.$$

But we have $H^2_{\mathrm{et}}(\mathcal{o}'_\infty(k), \mathbb{G}_m)_p\subseteq H^2_{\mathrm{et}}(k_\infty, \mathbb{G}_m)_p=0$ since $\mathrm{cd}_p(k_\infty)_{\mathrm{et}}\leqq 1$. Thus b) and c) are equivalent. Iwasawa ([7] Theorem 16) has shown that $\mathrm{Pic}(\mathcal{o}'_\infty(k))(p)^*$ is a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-torsion module which has no nonzero finite Γ-submodules. The general structure theory of $\mathbb{Z}_p[\![\Gamma]\!]$-modules now implies the equivalence of c) and d). q.e.d.

Iwasawa's conjecture about "$\mu=0$" states that the assertion d) above always holds true. It was proved by Ferrero/Washington ([3]) for abelian extensions $k/\mathbb{Q}$. Therefore, I think that the Lemmata 7 and 8 provide considerable evidence for our original conjecture. But they also lead to a concrete result.

Theorem 5. *Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension, and let A be an elliptic curve which is supersingular at p; assume that $k/\mathbb{Q}$ is abelian and that $A(k)$ contains a nonzero point of order p. We then have $H^2(\mathcal{o}_\infty, \mathcal{A}(p))=0$ and $\rho=[k:\mathbb{Q}]$.*

Proof. Because of the existence of the Weil pairing we have an exact sequence

$$0\to\mathbb{Z}/p\mathbb{Z}\to A_p\to\mu_p\to 0$$

over k_{et}. Using the universal property of the Néron model we derive from that an exact sequence

$$0\to\mathbb{Z}/p\mathbb{Z}\to\mathcal{A}_p\to\mu_p\to\mathcal{F}\to 0$$

over $(\mathcal{o}'_\infty)_{\mathrm{et}}$ where $\mathcal{F}$ is a skyscraper sheaf. Since the residue class fields of $\mathcal{o}'_\infty$ are p-closed we get $H^i_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{F})=0$ for $i>0$. On the other hand, we have seen that the Ferrero-Washington theorem implies

$$H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathbb{Z}/p\mathbb{Z})=H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mu_p)=0.$$

It thus follows $H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}_p)=0$. Finally the exact sequence

$$0\to\mathcal{A}_p\to\mathcal{A}(p)\xrightarrow{p}\mathcal{A}(p)\to\mathcal{F}'\to 0$$

over $(\mathcal{o}'_\infty)_{\mathrm{et}}$ where $\mathcal{F}'$ again is a skyscraper sheaf leads to the exact sequence

$$H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}_p)\to H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}(p))\xrightarrow{p} H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}(p))$$

which shows that $H^2_{\mathrm{et}}(\mathcal{o}'_\infty, \mathcal{A}(p))$ vanishes, too. We now just apply Lemma 7 and Corollary 5.

B. The comparison theorem for algebraic and analytic p-adic heights

We retain the notations introduced in the previous paragraphs. In particular, k_∞/k is a fixed (but arbitrary) $\mathbb{Z}_p$-extension with Galois group Γ and $\kappa: \Gamma\to\mathbb{Z}_p^\times$ is a nontrivial continuous character. In this section we will show that the pairing $\langle\ ,\ \rangle_\kappa$ defined in §1 is the same as the analytic p-adic height pairing associated with κ. Since the proof is rather long and complicated we first want to say a few words about the idea behind it. Using Bloch's description of the

Néron-Tate height it is an easy matter in the global function field case to derive the still simpler and direct description

$$\tilde{A}(k)=\mathrm{Ext}^1_S(\mathscr{A}^0,\mathbb{G}_m)\times\mathscr{A}^0(S)\to H^1(S,\mathbb{G}_m)=\mathrm{Pic}\,S\xrightarrow{\deg}\mathbb{Z}$$

as a Yoneda pairing followed by the usual degree map on divisor classes (S here is the curve which replaces $\mathrm{Spec}(\mathscr{o})$). To compare it with some other cohomologically defined pairing then is a question of handling the cohomological formalism in the right way. (All this was carried out in [18].) If we try to imitate this procedure in the number field case we immediately run into the problem that $\mathrm{Pic}(\mathscr{o})$ is finite. We have to take into consideration that the analytic p-adic height somewhat is of a transcendental nature at the primes in Σ. This should be reflected by the degree map we are looking for. Our first task therefore is to develop a cohomological formalism which is closely related to the flat cohomology but allows to modify sheaves like $\mathbb{G}_m$ or $\mathscr{A}^0$ at the primes in Σ in such a way that they contain the "transcendental" information we want to conserve. This is done in §4. In §5, we then are able to define a trace or degree map from a modified divisor class group of $\mathscr{o}$, resp. $\mathscr{o}_\infty$, into $\mathbb{Z}_p$. The key step of our proof is contained in §6 where we show that $\langle\ ,\ \rangle_\kappa$ can be described as a Yoneda pairing in our modified cohomology theory followed by the degree map. This step is not purely formal insofar as we have to use a nontrivial result of Serre ([22]) about congruence subgroups of abelian varieties. This result will enable us to check the commutativity of a certain diagram locally and away from the primes in Σ. Finally, in §7 we compare that Yoneda pairing with the analytic p-adic height which, of course, will be easy since we now have the correct cohomology theory at our disposal.

§4. Modified cohomology theories

For any scheme S, resp. affine scheme $S=\mathrm{Spec}(R)$, let us denote by $\mathscr{S}(S)$, resp. $\mathscr{S}(R)$, the category of abelian sheaves on the *fppf*-site on S. Put $Y:=\mathrm{Spec}(\mathscr{o})\setminus\Sigma$. For $\mathfrak{p}\in\Sigma$, we consider the left exact functor

$$H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\cdot):\mathscr{S}(Y)\to\mathscr{S}(k_{\mathfrak{p}})\to(\Gamma_{\mathfrak{p}}\text{-modules})$$

into the category of discrete $\Gamma_{\mathfrak{p}}$-modules where

$$\alpha_{\mathfrak{p}}:\mathrm{Spec}(k_{\mathfrak{p},\infty})\to Y$$

is the canonical morphism. We define $\mathscr{X}(\mathscr{o})=\mathscr{X}(\mathscr{o};\Sigma)$ to be the mapping cylinder of these functors: The objects of $\mathscr{X}(\mathscr{o})$ are tuples

$$(\mathscr{F};(M_{\mathfrak{q}})_{\mathfrak{q}\in\Sigma};(\mu_{\mathfrak{q}})_{\mathfrak{q}\in\Sigma})$$

with $\mathscr{F}\in\mathscr{S}(Y)$, $M_{\mathfrak{q}}\in(\Gamma_{\mathfrak{q}}\text{-modules})$, and $\mu_{\mathfrak{q}}:M_{\mathfrak{q}}\to H^0(k_{\mathfrak{q},\infty},\alpha_{\mathfrak{q}}^*\mathscr{F})$ a homomorphism of $\Gamma_{\mathfrak{q}}$-modules; the morphisms between these tuples are defined in the evident manner. $\mathscr{X}(\mathscr{o})$ again is an abelian category with enough injective

objects, and we have the functors

$$\begin{tikzcd} \mathscr{S}(Y) \arrow[r, shift left=2, "\mathscr{J}_!"] \arrow[r, shift right=2, "\mathscr{J}_*"'] & \mathscr{X}(\mathscr{o}) \arrow[l, "\mathscr{J}^*"'] \arrow[r, shift left=2, "I_{\mathfrak{q}}^*"] \arrow[r, shift right=2, "I_{\mathfrak{q}}^!"'] & (\Gamma_{\mathfrak{q}}\text{-modules}) \arrow[l, "I_{\mathfrak{q}*}"'] \end{tikzcd}$$

given by

$$\mathscr{J}_!:\mathscr{F}\mapsto(\mathscr{F};0;0)\qquad I_{\mathfrak{q}}^*:(\mathscr{F};M_{\mathfrak{p}};\mu_{\mathfrak{p}})\mapsto M_{\mathfrak{q}}$$

$$\mathscr{J}^*:(\mathscr{F};M_{\mathfrak{p}};\mu_{\mathfrak{p}})\mapsto\mathscr{F}\qquad I_{\mathfrak{q}*}:M\mapsto(0;0\ldots \underset{\substack{\uparrow\\ \text{q-th place}}}{M}\ldots 0;0)$$

$$\mathscr{J}_*:\mathscr{F}\mapsto(\mathscr{F};H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F});\mathrm{id})\qquad I_{\mathfrak{q}}^!:(\mathscr{F};M_{\mathfrak{p}};\mu_{\mathfrak{p}})\mapsto\ker\mu_{\mathfrak{q}}.$$

They have the following properties:

i) Each functor is left adjoint to the one listed below it;

ii) $\mathscr{J}^*$, $\mathscr{J}_!$, $I_{\mathfrak{p}}^*$, $I_{\mathfrak{p}*}$ are exact; $\mathscr{J}_*$, $I_{\mathfrak{p}}^!$ are left exact;

iii) $\mathscr{J}_*$, $\mathscr{J}^*$, $I_{\mathfrak{p}}^!$, $I_{\mathfrak{p}*}$ map injective objects to injective ones;

iv) $H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\cdot)=I_{\mathfrak{p}}^*\mathscr{J}_*$.

Proposition 1. *For $\mathscr{G}=(\mathscr{F};M_{\mathfrak{p}};\mu_{\mathfrak{p}})\in\mathscr{X}(\mathscr{o})$ we have*

$$R^iI_{\mathfrak{p}}^!(\mathscr{G})=\begin{cases}\ker\mu_{\mathfrak{p}} & \text{for } i=0,\\ \operatorname{coker}\mu_{\mathfrak{p}} & \text{for } i=1,\\ H^{i-1}(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F}) & \text{for } i\geqq 2\end{cases}$$

with the evident $\Gamma_{\mathfrak{p}}$-module structure.

Proof. If $0\to\mathscr{G}^1\to\mathscr{G}\to\mathscr{G}^2\to 0$ with $\mathscr{G}^v=(\mathscr{F}^v;M_{\mathfrak{p}}^v;\mu_{\mathfrak{p}}^v)$ is an exact sequence, then the diagram

$$\begin{tikzcd} 0 \arrow[r] & M_{\mathfrak{p}}^1 \arrow[r] \arrow[d, "\mu_{\mathfrak{p}}^1"] & M_{\mathfrak{p}} \arrow[r] \arrow[d, "\mu_{\mathfrak{p}}"] & M_{\mathfrak{p}}^2 \arrow[r] \arrow[d, "\mu_{\mathfrak{p}}^2"] & 0 \\ 0 \arrow[r] & H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F}^1) \arrow[r] & H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F}) \arrow[r] & H^0(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F}^2) \arrow[r] & H^1(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F}^1) \arrow[r] & \ldots \end{tikzcd}$$

is commutative and exact. Passing to the ker-coker sequence shows that the right hand terms in our assertion form an exact δ-functor. It therefore remains to prove that this δ-functor is universal, i.e., that

$$\operatorname{coker}\mu_{\mathfrak{p}}=H^{i-1}(k_{\mathfrak{p},\infty},\alpha_{\mathfrak{p}}^*\mathscr{F})=0\quad\text{for } i\geqq 2$$

if $\mathscr{G}$ and thus $\mathscr{F}$ are injective. But for injective $\mathscr{G}$ the map

$$\mathscr{G}\to\mathscr{J}_*\mathscr{J}^*\mathscr{G}=\mathscr{J}_*\mathscr{F}$$

induced by the $\mu_{\mathfrak{p}}$ is an epimorphism (SGA4 V 4.7) which in particular implies $\operatorname{coker}\mu_{\mathfrak{p}}=0$. On the other hand, since $k_{\mathfrak{p},\infty}$ is the filtered direct limit of finitely generated Y-algebras, it follows from a limit argument that α_p^* maps injective sheaves to acyclic ones.

Definition.

$$\hat{H}^i(o,.):=\operatorname{Ext}^i_{\mathscr{X}(o)}(\mathscr{J}_*\mathbf{Z},.), \quad \text{and} \quad \hat{H}^i_p(o,.):=\operatorname{Ext}^i_{\mathscr{X}(o)}(I_{p*}\mathbf{Z},.) \quad \text{for } p\in\Sigma.$$

Proposition 2. *For $\mathscr{G}=(\mathscr{F};M_p;\mu_p)\in\mathscr{X}(o)$ we have*

i) *the exact relative cohomology sequence*

$$\to\bigoplus_{p\in\Sigma}\hat{H}^i_p(o,\mathscr{G})\to\hat{H}^i(o,\mathscr{G})\to H^i(Y,\mathscr{F})\to\bigoplus_{p\in\Sigma}\hat{H}^{i+1}_p(o,\mathscr{G})\to$$

and

ii) *the spectral sequences*

$$H^i(\Gamma_p,R^jI^!_p(\mathscr{G}))\Rightarrow\hat{H}^{i+j}_p(o,\mathscr{G}).$$

Proof. i) Apply the functor $\operatorname{Ext}^i_{\mathscr{X}(o)}(.,\mathscr{G})$ to the exact sequence

$$0\to\mathscr{J}_!\mathbf{Z}\to\mathscr{J}_*\mathbf{Z}\to\bigoplus_{p\in\Sigma}I_{p*}\mathbf{Z}\to 0.$$

ii) We have $\operatorname{Hom}_{\mathscr{X}(o)}(I_{p*}\mathbf{Z},\mathscr{G})=\operatorname{Hom}_{\Gamma_p}(\mathbf{Z},I^!_p\mathscr{G})=H^0(\Gamma_p,I^!_p\mathscr{G})$.

Proposition 3. $R^i\mathscr{J}_*\mathscr{F}=\bigoplus_{p\in\Sigma}I_{p*}H^i(k_{p,\infty},\alpha_p^*\mathscr{F})$ *for $i>0$ and $\mathscr{F}\in\mathscr{S}(Y)$.*

Proof. Similar to the proof of Proposition 1.

Of course there is a relationship between our modified cohomology theory $\hat{H}^*$ and the usual flat cohomology of $\operatorname{Spec}(o)$. Let $o_{p,\infty}$ be the ring of integers in $k_{p,\infty}$ and denote by $\alpha_p:\operatorname{Spec}(o_{p,\infty})\to\operatorname{Spec}(o)$ the canonical morphism. We then have the left exact functor

$$M:\mathscr{S}(o)\to\mathscr{X}(o)$$
$$\mathscr{F}\to(\mathscr{F}_{/Y};H^0(o_{p,\infty},\alpha_p^*\mathscr{F});\text{canonical})$$

where $H^i(o_{p,\infty},\alpha_p^*\mathscr{F})$ is equipped with the evident Γ_p-module structure.

Lemma 4. i) $R^iM(\mathscr{F})=\bigoplus_{p\in\Sigma}I_{p*}H^i(o_{p,\infty},\alpha_p^*\mathscr{F})$ *for $i>0$ and $\mathscr{F}\in\mathscr{S}(o)$;*

ii) *M maps injective sheaves to $\hat{H}^0(o,\cdot)$-acyclic objects;*

iii) $\hat{H}^0(o,M\mathscr{F})=H^0(o_\infty/o,\mathscr{F})$.

Proof. i) This is shown in a similar way as Proposition 1.

ii) Let $\mathscr{F}\in\mathscr{S}(o)$ be injective. By a limit argument we get

$$H^i(o_{p,\infty},\alpha_p^*\mathscr{F})=H^i(k_{p,\infty},\alpha_p^*\mathscr{F})=0 \quad \text{for } i>0.$$

In particular, the maps $H^0(o_{p,\infty},\alpha_p^*\mathscr{F})\to H^0(k_{p,\infty},\alpha_p^*\mathscr{F})$ are surjective (we have $\alpha_p^*\mathscr{F}/k_{p,\infty}=\alpha_p^*\mathscr{F}$). An appropriate modification of Lemma 3 in the Appendix of [20] shows that the kernels of these maps are acyclic Γ_p-modules. Together with Proposition 1 and Proposition 2 ii) these facts imply

$$\hat{H}^i_p(o,M\mathscr{F})=0 \quad \text{for } i>0.$$

Of course, $\mathscr{J}^*\mathscr{F}$ is injective in $\mathscr{S}(Y)$. Our assertion thus follows from Proposition 2 i).

iii) If $\pi:\operatorname{Spec}(o_\infty)\to\operatorname{Spec}(o)$ denotes the canonical morphism and $Y_\infty:=Y\underset{o}{\times}o_\infty$ is the base extension we have $H^0(o_\infty/o,\mathscr{F})=\pi^*\mathscr{F}(o_\infty)^\Gamma$ and

$$\begin{aligned}\hat{H}^0(o,M\mathscr{F})&=\operatorname{Hom}_{\mathscr{X}(o)}(\mathscr{J}_*\mathbf{Z},M\mathscr{F})\\&=\{(x;x_p)\in\mathscr{F}(Y)\times\prod_{p\in\Sigma}H^0(o_{p,\infty},\alpha_p^*\mathscr{F})^{\Gamma_p}:x=x_p\text{ in }H^0(k_{p,\infty},\alpha_p^*\mathscr{F})\}\\&=\{(x;x_p)\in\pi^*\mathscr{F}(Y_\infty)\times\prod_{p\in\Sigma}H^0(o_\infty\underset{o}{\otimes}o_p,\alpha_p^*\mathscr{F}):x=x_p\text{ in }H^0(o_\infty\underset{o}{\otimes}k_p,\alpha_p^*\mathscr{F})\}^\Gamma.\end{aligned}$$

It therefore remains to prove that

$$\mathscr{F}(o_\infty)=\{(x,x_p)\in\mathscr{F}(Y_\infty)\times\prod_{p\in\Sigma}H^0(o_\infty\underset{o}{\otimes}o_p,\mathscr{F}):x=x_p\text{ in }H^0(o_\infty\underset{o}{\otimes}k_p,\mathscr{F})\}$$

holds true for any sheaf $\mathscr{F}\in\mathscr{S}(o_\infty)$. Obviously there is a map

$$\mathscr{F}(o_\infty)\to\text{right hand side.}$$

We now fix an element $(x;x_p)$ in the right hand group. Let $A_p^{(\beta)}$ be a filtered direct system of flat o_∞-algebras of finite type with $\operatorname{Spec}(o_\infty\underset{o}{\otimes}o_p)=\varprojlim\operatorname{Spec}(A_p^{(\beta)})$. We then have $\operatorname{Spec}(o_\infty\underset{o}{\otimes}k_p)=\varprojlim\operatorname{Spec}(Y_\infty\underset{o_\infty}{\times}A_p^{(\beta)})$ and

$$H^0(o_\infty\underset{o}{\otimes}o_p,\mathscr{F})=\varinjlim\mathscr{F}(A_p^{(\beta)}),\quad H^0(o_\infty\underset{o}{\otimes}k_p,\mathscr{F})=\varinjlim\mathscr{F}(Y_\infty\underset{o_\infty}{\times}A_p^{(\beta)}).$$

There are indices $\beta(p)$ such that x_p lifts to $\mathscr{F}(B_p)$, $B_p:=A_p^{(\beta(p))}$, with $x=x_p$ in $\mathscr{F}(Y_\infty\underset{o_\infty}{\times}B_p)$. But $\{Y_\infty,\operatorname{Spec}(B_p)\}$ is an $fppf$-covering of $\operatorname{Spec}(o_\infty)$. We can assume that $\operatorname{Spec}(B_p)\underset{o_\infty}{\times}\operatorname{Spec}(B_q)$ for $p\neq q$ already projects to Y_∞. The sheaf property of $\mathscr{F}$ for this covering then implies that the x and x_p come from a uniquely determined $y\in\mathscr{F}(o_\infty)$. q.e.d.

As a consequence of the above lemma we have the spectral sequence

$$\hat{H}^i(o,R^jM(\mathscr{F}))\Rightarrow H^{i+j}(o_\infty/o,\mathscr{F}) \quad \text{for } \mathscr{F}\in\mathscr{S}(o).$$

Proposition 5. *If $\mathscr{F}\in\mathscr{S}(o)$ is represented by a smooth connected commutative o-group scheme, then we have $R^iM(\mathscr{F})=0$ for $i>0$ and therefore $\hat{H}^i(o,M\mathscr{F})=H^i(o_\infty/o,\mathscr{F})$ for $i\geqq 0$.*

Proof. First note that $\mathscr{F}$ is of finite type over o by SGA 3 VI_B 5.5. According to [13] (5.1 iii) we have $H^i(o_{p,\infty},\alpha_p^*\mathscr{F})=0$ for $i>0$. The assertion now follows from Lemma 4 i and the above spectral sequence.

In a completely analogous way we get a modified cohomology theory over $\mathcal{o}_\infty$. Let $k_\mathfrak{P}$ be the "completion" (i.e., the union of the completions of the finite intermediate layers) of k_∞ with respect to a prime $\mathfrak{P}$ of k_∞ above Σ, let $\mathcal{o}_\mathfrak{P}$ be the ring of integers in $k_\mathfrak{P}$, and denote by $a_\mathfrak{P}$: $\operatorname{Spec}(k_\mathfrak{P}) \to Y_\infty := Y \times \mathcal{o}_\infty$, resp. $\alpha_\mathfrak{P}$: $\operatorname{Spec}(\mathcal{o}_\mathfrak{P}) \to \operatorname{Spec}(\mathcal{o}_\infty)$, the canonical morphisms. Let $\mathscr{Z}(\mathcal{o}_\infty)$ be the mapping cylinder of the functors

$$H^0(k_\mathfrak{P}, a_\mathfrak{P}^*.)\colon \mathscr{S}(Y_\infty) \to \mathscr{S}(k_\mathfrak{P}) \to (\text{abelian groups})$$

and define $\hat{H}^i(\mathcal{o}_\infty, .)$ to be the corresponding cohomology theory. Concerning the previous results there are the following simplifications in this context ("$k_{\mathfrak{P},\infty} = k_\mathfrak{P}$ and $\Gamma_\mathfrak{P} = 1$").

Proposition 2′. *For $\mathscr{G} = (\mathscr{F}; M_\mathfrak{P}; \mu_\mathfrak{P}) \in \mathscr{Z}(\mathcal{o}_\infty)$ we have the exact relative cohomology sequence*

$$\begin{aligned} 0 \to \bigoplus_{\mathfrak{P}/\Sigma} \ker \mu_\mathfrak{P} \quad &\to \hat{H}^0(\mathcal{o}_\infty, \mathscr{G}) \to H^0(Y_\infty, \mathscr{F}) \to \\ \to \bigoplus_{\mathfrak{P}/\Sigma} \operatorname{coker} \mu_\mathfrak{P} \quad &\to \hat{H}^1(\mathcal{o}_\infty, \mathscr{G}) \to H^1(Y_\infty, \mathscr{F}) \to \\ \to \bigoplus_{\mathfrak{P}/\Sigma} H^1(k_\mathfrak{P}, a_\mathfrak{P}^* \mathscr{F}) &\to \hat{H}^2(\mathcal{o}_\infty, \mathscr{G}) \to H^2(Y_\infty, \mathscr{F}) \to \\ \to \bigoplus_{\mathfrak{P}/\Sigma} H^2(k_\mathfrak{P}, a_\mathfrak{P}^* \mathscr{F}) &\to \dots \end{aligned}$$

If $M_\infty\colon \mathscr{S}(\mathcal{o}_\infty) \to \mathscr{Z}(\mathcal{o}_\infty)$ denotes the functor analogous to M we have the exact sequence

$$0 \to \hat{H}^1(\mathcal{o}_\infty, M_\infty \mathscr{F}) \to H^1(\mathcal{o}_\infty, \mathscr{F}) \to \bigoplus_{\mathfrak{P}/\Sigma} H^1(\mathcal{o}_\mathfrak{P}, \alpha_\mathfrak{P}^* \mathscr{F}) \to \dots$$

$$\dots \to \hat{H}^i(\mathcal{o}_\infty, M_\infty \mathscr{F}) \to H^i(\mathcal{o}_\infty, \mathscr{F}) \to \bigoplus_{\mathfrak{P}/\Sigma} H^i(\mathcal{o}_\mathfrak{P}, \alpha_\mathfrak{P}^* \mathscr{F}) \to \dots$$

for $\mathscr{F} \in \mathscr{S}(\mathcal{o}_\infty)$.

Proposition 5′. *If $\mathscr{F} \in \mathscr{S}(\mathcal{o}_\infty)$ is represented by a smooth connected commutative $\mathcal{o}_\infty$-group scheme, then we have $R^i M_\infty(\mathscr{F}) = 0$ for $i > 0$ and therefore $\hat{H}^i(\mathcal{o}_\infty, M_\infty \mathscr{F}) = H^i(\mathcal{o}_\infty, \mathscr{F})$ for $i \geqq 0$.*

Let π: $\operatorname{Spec}(\mathcal{o}_\infty) \to \operatorname{Spec}(\mathcal{o})$ again denote the canonical morphism. We finally consider the exact functor

$$\pi^*\colon \mathscr{Z}(\mathcal{o}) \to \mathscr{Z}(\mathcal{o}_\infty)$$

$$\mathscr{G} = (\mathscr{F}; M_p; \mu_p) \to \pi^* \mathscr{G} := (\pi^* \mathscr{F}; M_\mathfrak{P}; \mu_\mathfrak{P})$$

with $M_\mathfrak{P} := M_p$ and $\mu_\mathfrak{P} := \mu_p$: $M_p \to H^0(k_{p,\infty}, a_p^* \mathscr{F}) = H^0(k_\mathfrak{P}, a_\mathfrak{P}^* \pi^* \mathscr{F})$ for $\mathfrak{P}/p$.

Remark 6. i) $H^0(\Gamma, \hat{H}^0(\mathcal{o}_\infty, \pi^* \mathscr{G})) = \hat{H}^0(\mathcal{o}, \mathscr{G})$ for any $\mathscr{G} \in \mathscr{Z}(\mathcal{o})$;

ii) the Γ-module $\hat{H}^0(\mathcal{o}_\infty, \pi^* \mathscr{G})$ is acyclic for injective $\mathscr{G} \in \mathscr{Z}(\mathcal{o})$.

Proof. i) Easy. ii) For injective $\mathscr{G} \in \mathscr{Z}(\mathcal{o})$ we have:

a) $\mathscr{J}^* \mathscr{G} \in \mathscr{S}(Y)$ is injective;

b) $\ker \mu_p$ is an injective Γ_p-module;

c) the maps μ_p and $\mu_\mathfrak{P}$ are surjective (SGA 4 V 4.7).

From c) and Proposition 2′ we derive the exact sequence

$$0 \to \bigoplus_{\mathfrak{P}/\Sigma} \ker \mu_\mathfrak{P} \to \hat{H}^0(\mathcal{o}_\infty, \pi^* \mathscr{G}) \to H^0(Y_\infty, \pi^* \mathscr{J}^* \mathscr{G}) \to 0.$$

Because of a) and the proof of III 2.20 in [16], resp. b) and Shapiro's lemma, the right term, resp. the left term, is acyclic as Γ-module, and therefore the middle term is, too. q.e.d.

With the help of the relative cohomology sequence it is easy to see that the δ-functor $\hat{H}^*(\mathcal{o}_\infty, \pi^*.)$ is universal, i.e., $R^i \hat{H}^0(\mathcal{o}_\infty, \pi^*.) = \hat{H}^i(\mathcal{o}_\infty, \pi^*.)$. We thus get the spectral sequence

$$H^i(\Gamma, \hat{H}^j(\mathcal{o}_\infty, \pi^* \mathscr{G})) \Rightarrow \hat{H}^{i+j}(\mathcal{o}, \mathscr{G})$$

for $\mathscr{G} \in \mathscr{Z}(\mathcal{o})$.

Lemma 7. *For $\mathscr{F} \in \mathscr{S}(\mathcal{o})$ we have $M_\infty \pi^* \mathscr{F} = \pi^* M \mathscr{F}$ and the morphism of spectral sequences*

$$\begin{array}{ccc} H^i(\Gamma, \hat{H}^j(\mathcal{o}_\infty, M_\infty \pi^* \mathscr{F})) & \Rightarrow & \hat{H}^{i+j}(\mathcal{o}, M \mathscr{F}) \\ \downarrow & & \downarrow \\ H^i(\Gamma, H^j(\mathcal{o}_\infty, \pi^* \mathscr{F})) & \Rightarrow & H^{i+j}(\mathcal{o}_\infty/\mathcal{o}, \mathscr{F}). \end{array}$$

Proof. Left to the reader as an exercise.

For the convenience of the reader we now give some comments on our notations concerning homological algebra:

1) If it is possible from the context we often skip the symbols M and M_∞; for example, we write $\hat{H}^i(\mathcal{o}, \mathscr{F})$ instead of $\hat{H}^i(\mathcal{o}, M\mathscr{F})$ for $\mathscr{F} \in \mathscr{S}(\mathcal{o})$.

2) We do not distinguish in the notation between cohomology and hypercohomology; for example, if $\mathscr{G}^\cdot$ is an object in the derived category $D^+(\mathscr{Z}(\mathcal{o}))$ its hypercohomology groups are simply denoted by $\hat{H}^i(\mathcal{o}, \mathscr{G}^\cdot)$. The same for the Ext-functors.

3) Let $\mathfrak{A}$ be an abelian category, A an object in $\mathfrak{A}$, and $n \in \mathbb{N}$ a natural number. We denote by $A[n]$ the complex

$$A \xrightarrow{n} A \quad (\text{in degree 0 and 1})$$

viewed as an element in the derived category $D^+(\mathfrak{A})$. In $D^+(\mathfrak{A})$ we then have the distinguished triangle

$$\begin{tikzcd}
A \arrow[r, "\mathrm{id}"] & A \arrow[r, "\mathrm{id}"] & A \arrow[rr] & & 0 \\
 & & & 0 \arrow[ul, "\cong"'] \arrow[ur] & \\
0 \arrow[r] \arrow[uu] & A \arrow[r, "0 \oplus \mathrm{id}"] \arrow[uu, "n"] & A \oplus A \arrow[rr, "-\mathrm{id}+0"] \arrow[uu, "\mathrm{id}+n"] & & A \arrow[uu] \\
 & & & A \arrow[ul, "-n \oplus \mathrm{id}", "\cong"'] \arrow[ur, "n"'] \arrow[uu] &
\end{tikzcd}$$

$$T^{-1}(A) \to A[n] \to A \xrightarrow{n} A$$

(the indicated isomorphism takes place in $D^+(\mathfrak{A})$, it is even an isotopy) and therefore an exact sequence

$$\dots \longrightarrow F^i(A[n]) \longrightarrow F^i(A) \xrightarrow{n} F^i(A) \longrightarrow F^{i+1}(A[n]) \longrightarrow \dots$$

for any covariant cohomological functor F on $D^+(\mathfrak{A})$. If $A \xrightarrow{n} A$ is an epimorphism, then $A[n]$ and $A_n := \ker(A \xrightarrow{n} A)$ are canonically isomorphic in $D^+(\mathfrak{A})$ and we get $F^i(A[n]) = F^i(A_n)$. More generally, for any complex $A^\cdot$ in $\mathfrak{A}$ which is bounded below and any $n \in \mathbb{Z}$, let $A^\cdot[n]$ denote the simple complex which is functorially associated with the double complex

$$A^\cdot \xrightarrow{n} A^\cdot \quad \text{(in first degree 0 and 1).}$$

Using the second double complex spectral sequence one easily sees that $A^\cdot \to A^\cdot[n]$ induces a functor on $D^+(\mathfrak{A})$. Furthermore there is the canonical isomorphism

$$T(A^\cdot)[n] = T(A^\cdot[-n]) \xrightarrow{\cong} T(A^\cdot[n])$$

which is induced by the isomorphism of double complexes

$$\begin{tikzcd} A^\cdot \arrow[r, "-n"] \arrow[d, "="'] & A^\cdot \arrow[d, "-1"] \\ A^\cdot \arrow[r, "n"] & A^\cdot. \end{tikzcd}$$

4) Yoneda product, resp. cup-product, is denoted by $\vee$, resp. $\cup$. We refer the reader to SGA $4\frac{1}{2}$[C.D.] for the definition.

§ 5. Trace maps

Let G be a commutative Y-group scheme locally of finite type. For $\mathfrak{p} \in \Sigma$ and any finite intermediate layer E of $k_{\mathfrak{p},\infty}/k_{\mathfrak{p}}$ we denote by $NG(E) \subseteq G/(E)$ the subgroup of universal norms with respect to the extension $k_{\mathfrak{p},\infty}/E$. We put

$$NG(k_{\mathfrak{p},\infty}) := \bigcup_{E \subset k_{\mathfrak{p},\infty}} NG(E)$$

Of course, $NG(k_{\mathfrak{p},\infty})$ is a $\Gamma_{\mathfrak{p}}$-submodule of $G(k_{\mathfrak{p},\infty})$.

Definition.

$$NG := (G; NG(k_{\mathfrak{p},\infty}); \text{inclusion}) \in \mathscr{X}(o).$$

In this paragraph we study the cohomology of the "modified multiplicative group" $N\mathbb{G}_m \in \mathscr{X}(o)$. For simplicity, we write $N. := N\mathbb{G}_m(.)$.

Remark 1.

$$k^x_{\mathfrak{p},\infty}/Nk_{\mathfrak{p},\infty} = k^x_{\mathfrak{p}}/Nk_{\mathfrak{p}} \quad \text{for } \mathfrak{p} \in \Sigma.$$

Let $\mathscr{G}_m$ be the Néron model of $\mathbb{G}_{m/k}$ over Y, and define the sheaf $\mathscr{D} \in \mathscr{S}(Y)$ by the exact sequence

$$0 \to \mathbb{G}_{m/Y} \to \mathscr{G}_m \to \mathscr{D} \to 0. \tag{1}$$

We then have the exact sequence

$$0 \to N\mathbb{G}_m \to \mathscr{I}_* \mathscr{G}_m \to \hat{\mathscr{D}} := (\mathscr{D}; k^x_{\mathfrak{p},\infty}/Nk_{\mathfrak{p},\infty}; 0) \to 0 \tag{2}$$

in $\mathscr{X}(o)$.

Remark 2. i) $\hat{H}^0(o, \mathscr{I}_* \mathscr{G}_m) = k^x$;

ii) $\hat{H}^1(o, \mathscr{I}_* \mathscr{G}_m) = 0$;

iii) $\hat{H}^0(o, \hat{\mathscr{D}}) = (\bigoplus_{\mathfrak{p} \notin \Sigma} k^x_{\mathfrak{p}}/o^x_{\mathfrak{p}}) \oplus (\bigoplus_{\mathfrak{p} \in \Sigma} k^x_{\mathfrak{p}}/Nk_{\mathfrak{p}})$.

Proof. i) Clear. ii) We have the injective homomorphisms

$$\hat{H}^1(o, \mathscr{I}_* \mathscr{G}_m) \to H^1(Y, \mathscr{G}_m) = H^1_{\text{et}}(Y, g_* \mathbb{G}_m) \to H^1_{\text{et}}(k, \mathbb{G}_m) = 0$$

where g: Spec$(k) \to Y$ denotes the canonical morphism.

iii) Since $\mathbb{G}_{m/Y}$ is smooth, the sequence (1) remains exact after restriction to Y_{et}. We therefore have $H^0(Y, \mathscr{D}) = \bigoplus_{\mathfrak{p} \notin \Sigma} k^x_{\mathfrak{p}}/o^x_{\mathfrak{p}}$ (compare [16] p. 73). q.e.d.

Using the above remark we derive from the cohomology sequence belonging to (2) the exact sequence

$$\begin{tikzcd} k^x \arrow[r] & (\bigoplus_{\mathfrak{p} \notin \Sigma} k^x_{\mathfrak{p}}/o^x_{\mathfrak{p}}) \oplus (\bigoplus_{\mathfrak{p} \in \Sigma} k^x_{\mathfrak{p}}/Nk_{\mathfrak{p}}) \arrow[r] \arrow[d, "-v_{k,\kappa}"'] & \hat{H}^1(o, N\mathbb{G}_m) \arrow[r] \arrow[dl, dashed, "\deg"] & 0 \\ & \mathbb{Z}_p & & \end{tikzcd}$$

Here $v_{k,\kappa}$ denotes the map induced by $\log_p \circ \kappa$ via global class field theory. Since it vanishes on the image of k^x the map $-v_{k,\kappa}$ induces a homomorphism

$$\deg\colon \hat{H}^1(o, N\mathbb{G}_m) \longrightarrow \mathbb{Z}_p$$

which we call the *trace map*. We also need the following modified version

$$\deg_\phi := (-\log_p \circ \kappa(\phi))^{-1} \cdot \deg$$

which depends on the topological generator ϕ of Γ but is surjective. In the same way $-v_\kappa := -\varinjlim [k_n : k]^{-1} \cdot v_{k_n,\kappa}$ induces a Γ-equivariant homomorphism

$$\deg\colon \hat{H}^1(o_\infty, N\mathbb{G}_m) \to \mathbb{Z}_p \quad (\text{resp. } \deg_\phi := (-\log_p \kappa(\phi))^{-1} \cdot \deg)$$

such that we have the commutative diagram

$$\begin{tikzcd} \hat{H}^1(o, N\mathbb{G}_m) \arrow[rr] \arrow[dr, "\deg"'] & & \hat{H}^1(o_\infty, N\mathbb{G}_m) \arrow[dl, "\deg"] \\ & \mathbb{Z}_p & \end{tikzcd}$$

Lemma 3. *For $i \geqq 2$, $\hat{H}^i(\mathfrak{o}_\infty, N\mathbb{G}_m)$ is a torsion group with trivial p-primary component.*

Proof. The assertion follows from the relative cohomology sequence since the groups $H^i(Y_\infty, \mathbb{G}_m)$, resp. $H^i(k_\mathfrak{P}, \mathbb{G}_m)$ for $\mathfrak{P}/\Sigma$, have the required property for $i \geqq 2$, resp. $i \geqq 1$. The map

$$H^2(Y_\infty, \mathbb{G}_m)(p) \longrightarrow \bigoplus_{\mathfrak{P}/\Sigma} H^2(k_\mathfrak{P}, \mathbb{G}_m) = 0$$

namely is injective (compare [16], p. 109).

Lemma 4.

i) $\hat{H}^i(\mathfrak{o}_\infty, N\mathbb{G}_m[p^v]) = \begin{cases} \hat{H}^1(\mathfrak{o}_\infty, N\mathbb{G}_m) \otimes \mathbb{Z}/p^v\mathbb{Z} & \text{for } i=2, \\ 0 & \text{for } i \geqq 3; \end{cases}$

ii) $\hat{H}^i(\mathfrak{o}, N\mathbb{G}_m[p^v]) \cong \begin{cases} \hat{H}^2(\mathfrak{o}_\infty, N\mathbb{G}_m[p^v])_\Gamma & \text{for } i=3, \\ 0 & \text{for } i \geqq 4 \end{cases}$

(the isomorphism depends on the choice of ϕ).

Proof. Part i) follows from Lemma 3 and the exact sequences

$$0 \to \hat{H}^{i-1}(\mathfrak{o}_\infty, N\mathbb{G}_m) \otimes \mathbb{Z}/p^v\mathbb{Z} \to \hat{H}^i(\mathfrak{o}_\infty, N\mathbb{G}_m[p^v]) \to \hat{H}^i(\mathfrak{o}_\infty, N\mathbb{G}_m)_{p^v} \to 0.$$

The assertion ii) then is a consequence of i), the spectral sequence before Lemma (4.7), and the fact that $\mathrm{cd}_p \Gamma = 1$. q.e.d.

Because of the above lemma the map deg, resp. $\deg_\phi$, in a natural way induces a homomorphism

$$d': \hat{H}^2(\mathfrak{o}_\infty, N\mathbb{G}_m[p^v]) \to \mathbb{Z}/p^v\mathbb{Z},$$

resp. a surjective homomorphism

$$d: \hat{H}^3(\mathfrak{o}, N\mathbb{G}_m[p^v]) \to \mathbb{Z}/p^v\mathbb{Z}$$

which does not depend on the special choice of ϕ.

What can be said about the kernel of the trace map? It seems most likely that $\ker(\hat{H}(\mathfrak{o}_\infty, N\mathbb{G}_m) \xrightarrow{\deg} \mathbb{Z}_p)$ is p-divisible if k_∞ is the cyclotomic $\mathbb{Z}_p$-extension, which in particular would imply that d is an isomorphism in that case. Let us consider the extension $k_\infty = \mathbb{Q}(\mu(p))/k = \mathbb{Q}(\mu_p)$: There we have the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & 1+p\mathbb{Z}_p \arrow[r] \arrow[d, "\log_p"'] & \hat{H}^1(\mathfrak{o}_\infty, N\mathbb{G}_m) \arrow[r] \arrow[dl, "(1-p)\cdot\deg"] & \mathrm{Pic}(\mathfrak{o}'_\infty) \arrow[r] & 0 \\ & \mathbb{Z}_p & & & \end{tikzcd}$$

and thus $\mathrm{Pic}(\mathfrak{o}'_\infty) = \ker(\hat{H}^1(\mathfrak{o}_\infty, N\mathbb{G}_m) \xrightarrow{\deg} \mathbb{Z}_p)$. But according to the Ferrero-Washington theorem $\mathrm{Pic}(\mathfrak{o}'_\infty)$ is p-divisible. In the general case not only Iwasawa's "$\mu=0$"-conjecture is involved but also the nonvanishing of certain p-adic regulators which describe the behavior of the group of p-units in k_∞ under v_κ. Using results of Greenberg ([4]) one can prove the above divisibility property if $k/\mathbb{Q}$ is abelian and k_∞/k is the cyclotomic $\mathbb{Z}_p$-extension. We do not go into this since it is not needed in the following.

We finally have to provide a compatibility between the map d and certain "local trace maps". For any finite prime $\mathfrak{p}$, there is the canonical identification (compare [12])

$$H^3_\cdot(\mathfrak{o}_\mathfrak{p}, \mu_{p^v}) = H^2_{\text{et}}(k_\mathfrak{p}, \mu_{p^v}) = \mathbb{Z}/p^v\mathbb{Z}.$$

Using the relative cohomology sequence we then may consider the diagram

$$\begin{tikzcd} \bigoplus\limits_{\mathfrak{p}\notin S} H^3_\cdot(\mathfrak{o}_\mathfrak{p}, \mu_{p^v}) \arrow[r] \arrow[d, "\cong"] & \hat{H}^3(\mathfrak{o}, N\mathbb{G}_m[p^v]) \arrow[d, "d"] \\ \bigoplus\limits_{\mathfrak{p}\notin S} \mathbb{Z}/p^v\mathbb{Z} \arrow[r, "\Sigma"] & \mathbb{Z}/p^v\mathbb{Z} \end{tikzcd}$$

where $S = S(k_\infty/k)$ denotes the set of primes of k which lie above p or which split completely in k_∞.

Lemma 5. *The above diagram is commutative.*

Proof. The primes not in S split finitely in k_∞. The local component of $(\log_p \cdot \kappa(\phi))^{-1} \cdot v_\kappa$ corresponding to $\mathfrak{P}/\mathfrak{p} \notin S$ therefore is given by the normalized discrete valuation on $k_\mathfrak{P}^\times$. The further details are left to the reader.

§ 6. Algebraic heights

We now come back to the situation of § 1. In particular, the abelian variety A always is assumed to be ordinary for k_∞/k! The fundamental tool for the comparison of algebraic and analytic p-adic height is the pairing

$$\mathrm{Ext}^1_{\mathfrak{X}(\mathfrak{o})}(N\mathscr{A}^0, N\mathbb{G}_m) \times \hat{H}^0(\mathfrak{o}, N\mathscr{A}^0) \xrightarrow{\vee} \hat{H}^1(\mathfrak{o}, N\mathbb{G}_m) \xrightarrow{\deg} \mathbb{Z}_p. \qquad (*)$$

Lemma 1. *For $\mathfrak{p} \in \Sigma$ we have $H^0(\Gamma_\mathfrak{p}, NA(k_{\mathfrak{p},\infty})) = NA(k_\mathfrak{p})$.*

Proof. We have to show that the canonical map

$$A(k_\mathfrak{p})/NA(k_\mathfrak{p}) \to A(E)/NA(E)$$

is injective for any finite intermediate layer E of $k_{\mathfrak{p},\infty}/k_\mathfrak{p}$. Put $g := \mathrm{Gal}(k_{\mathfrak{p},\infty}/E)$. By Tate's local duality theorem the required injectivity is equivalent to the surjectivity of the corestriction map

$$H^1(g, \tilde{A}(k_{\mathfrak{p},\infty})) \xrightarrow{\text{cores}} H^1(\Gamma_\mathfrak{p}, \tilde{A}(k_{\mathfrak{p},\infty})).$$

We now make use of the computations on p. 283/284 in [20]. Let L denote the completion of the maximal unramified extension of $k_\mathfrak{p}$, and put $L_\infty := k_{\mathfrak{p},\infty} \cdot L$, $\Gamma_\mathfrak{p}^0 := \mathrm{Gal}(L_\infty/L)$, and $g^0 := \mathrm{Gal}(L_\infty/EL)$

$$\begin{tikzcd}[column sep=small]
 & L_\infty \arrow[dl, dash] \arrow[d, dash, "g^0"] \\
k_{\mathfrak{p},\infty} \arrow[d, dash, "g"'] & EL \arrow[dl, dash] \arrow[d, dash] \\
E \arrow[d, dash] & L \arrow[dl, dash] \\
k_{\mathfrak{p}} &
\end{tikzcd}$$

The general case follows by a successive application of the following two special cases.

1. Case. Let $E/k_{\mathfrak{p}}$ be unramified, i.e., $g^0=\Gamma_{\mathfrak{p}}^0$. We then have the commutative diagram

$$\begin{tikzcd}
H^1(g,\tilde{A}(k_{\mathfrak{p},\infty})) \arrow[r, "\cong"] \arrow[d, "\mathrm{cores}"'] & H^0(\mathrm{Gal}(L/E), H^1(\Gamma_{\mathfrak{p}}^0,\tilde{A}(L_\infty))) \arrow[d, "\mathrm{cores}"] \\
H^1(\Gamma_{\mathfrak{p}},\tilde{A}(k_{\mathfrak{p},\infty})) \arrow[r, "\cong"] & H^0(\mathrm{Gal}(L/k_{\mathfrak{p}}), H^1(\Gamma_{\mathfrak{p}}^0,\tilde{A}(L_\infty)))
\end{tikzcd}$$

with isomorphisms in the rows (see loc. cit., p. 283). But the right hand corestriction map is surjective since according to loc. cit., p. 284, the discrete $\mathrm{Gal}(L/E)$-module $H^1(\Gamma_{\mathfrak{p}}^0,\tilde{A}(L_\infty))$ has no non-zero coinvariants (compare the argument in the proof of [6] Th. 3.1).

2. Case. Let $E/k_{\mathfrak{p}}$ be totally ramified, i.e., $\Gamma_{\mathfrak{p}}=\Gamma_{\mathfrak{p}}^0$ and $g=g^0$. In this situation we have commutative exact diagrams

$$\begin{tikzcd}
H^1(g,\tilde{A}(k_{\mathfrak{p},\infty})) \arrow[r, "\cong"] \arrow[d, "\mathrm{cores}"'] & H^0(\mathrm{Gal}(L/k_{\mathfrak{p}}), H^1(g,\tilde{A}(L_\infty))) \arrow[d, "H^0(\mathrm{Gal}(L/k_{\mathfrak{p}}),\mathrm{cores})"] \\
H^1(\Gamma_{\mathfrak{p}},\tilde{A}(k_{\mathfrak{p},\infty})) \arrow[r, "\cong"] & H^0(\mathrm{Gal}(L/k_{\mathfrak{p}}), H^1(\Gamma_{\mathfrak{p}},\tilde{A}(L_\infty)))
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & H^1(g,\tilde{A}(L_\infty)) \arrow[r] \arrow[d, "\mathrm{cores}"] & H^1(g,\tilde{\mathscr{A}}(\bar{\kappa}_{\mathfrak{p}})(p)) \arrow[r] \arrow[d, "\cong"', "\mathrm{cores}"] & 0 \\
0 \arrow[r] & N \arrow[r] & H^1(\Gamma_{\mathfrak{p}},\tilde{A}(L_\infty)) \arrow[r] & H^1(\Gamma_{\mathfrak{p}},\tilde{\mathscr{A}}(\bar{\kappa}_{\mathfrak{p}})(p)) \arrow[r] & 0
\end{tikzcd}$$

(see loc. cit.) which obviously imply the required surjectivity (even bijectivity). q.e.d.

Since $NA(k_{\mathfrak{p}})$ is of finite index in $A(k_{\mathfrak{p}})$ for $\mathfrak{p}\in\Sigma$ (by our assumption about A) we see that

$$N\mathscr{A}^0(o):=\hat{H}^0(o,N\mathscr{A}^0)=\{a\in\mathscr{A}^0(Y)\colon a\in NA(k_{\mathfrak{p}}) \text{ for } \mathfrak{p}\in\Sigma\}$$

is a subgroup of finite index in $A(k)$. Furthermore, Lemma 3 in [19] implies that the map

$$\mathrm{Ext}^1_o(\mathscr{A}^0,\mathbb{G}_m)\to\mathrm{Ext}^1_{\mathscr{X}(o)}(N\mathscr{A}^0,N\mathbb{G}_m)$$
$$(0\to\mathbb{G}_m\to\mathscr{X}\to\mathscr{A}^0\to 0)\mapsto(0\to N\mathbb{G}_m\to N\mathscr{X}\to N\mathscr{A}^0\to 0)$$

is well defined. On the other hand, we derive from [15] (5.1) (compare Lemma 9 in [18]) the canonical identification

$$\tilde{A}(k)=\mathrm{Ext}^1_o(\mathscr{A}^0,\mathbb{G}_m).$$

Hence, by restriction, (*) induces a pairing

$$(\ ,\ )\colon \tilde{A}(k)\times N\mathscr{A}^0(o)\to\mathbb{Z}_p.$$

The aim of this paragraph is to prove the following result.

Proposition 2.

$$\langle\ ,\ \rangle_\kappa=-(\ ,\ ).$$

Our algebraic pairing

$$(\log_p\kappa(\phi))^{-1}\cdot\langle\ ,\ \rangle_\kappa\colon \tilde{\mathscr{A}}^0(o)\times\mathscr{A}^0(o)\to\mathbb{Q}_p$$

was defined by the diagram

$$\begin{tikzcd}[row sep=small]
\tilde{\mathscr{A}}^0(o)\otimes\mathbb{Z}_p \arrow[dddddddd] & \mathscr{A}^0(o)\otimes\mathbb{Q}_p/\mathbb{Z}_p \arrow[d] & \\
 & H^1(o,\mathscr{A}^0(p)) \arrow[d] & \\
 & H^1(o,\mathscr{A}(p)) \arrow[d] & \\
 & H^1(o_\infty/o,\mathscr{A}(p)) \arrow[d] & \\
 & H^1(o_\infty,\mathscr{A}(p))^\Gamma \arrow[d] & \\
 & H^1(o_\infty,\mathscr{A}(p))_\Gamma \arrow[d] & \\
 & H^2(o_\infty/o,\mathscr{A}(p)) & \\
 & & \\
\varprojlim H^1(o,\tilde{\mathscr{A}}^0_{p^\nu}) \quad\times & H^2(o,\mathscr{A}(p)) \arrow[uu] \arrow[r, "\cup"] & \mathrm{H}^3(o,\mu(p))=\mathbb{Q}_p/\mathbb{Z}_p
\end{tikzcd} \tag{1}$$

using the identification

$$\mathrm{Hom}(\mathscr{A}^0(o)\otimes\mathbb{Q}_p/\mathbb{Z}_p,\mathbb{Q}_p/\mathbb{Z}_p)=\mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{A}^0(o)\otimes\mathbb{Z}_p,\mathbb{Z}_p).$$

In several steps we now replace the diagram by another one which only contains modified cohomology (resp. Ext-) groups.

First we observe that there is the following commutative diagram (2):

$$\begin{tikzcd}[column sep=small]
\mathscr{A}^0(o)/p^v \arrow[d, "\delta"] \arrow[r, equal] & H^0(o_\infty/o, \mathscr{A}^0)/p^v \arrow[ddd, "\delta"] \arrow[r, equal] & \hat{H}^0(o, \mathscr{A}^0)/p^v \arrow[ddd, "\delta"] & N\mathscr{A}^0(o)/p^v \arrow[l] \arrow[ddd, "\delta"] \\
H^1(o, \mathscr{A}^0_{p^v}) \arrow[d] & & & \\
H^1(o, \mathscr{A}_{p^v}) \arrow[d] & & & \\
H^1(o_\infty/o, \mathscr{A}_{p^v}) \arrow[d] & H^1(o_\infty/o, \mathscr{A}^0[p^v]) \arrow[l] \arrow[d] \arrow[r, equal] & \hat{H}^1(o, \mathscr{A}^0[p^v]) \arrow[d] & \hat{H}^1(o, N\mathscr{A}^0[p^v]) \arrow[l] \arrow[d] \\
H^1(o_\infty, \mathscr{A}_{p^v})^\Gamma \arrow[d] & H^1(o_\infty, \mathscr{A}^0[p^v])^\Gamma \arrow[l] \arrow[d] \arrow[r, equal] & \hat{H}^1(o_\infty, \mathscr{A}^0[p^v])^\Gamma \arrow[d] & \hat{H}^1(o_\infty, N\mathscr{A}^0[p^v])^\Gamma \arrow[l] \arrow[d] \\
H^1(o_\infty, \mathscr{A}_{p^v})_\Gamma \arrow[d] & H^1(o_\infty, \mathscr{A}^0[p^v])_\Gamma \arrow[l] \arrow[d] \arrow[r, equal] & \hat{H}^1(o_\infty, \mathscr{A}^0[p^v])_\Gamma \arrow[d] & \hat{H}^1(o_\infty, N\mathscr{A}^0[p^v])_\Gamma \arrow[l] \arrow[d] \\
H^2(o_\infty/o, \mathscr{A}_{p^v}) & H^2(o_\infty/o, \mathscr{A}^0[p^v]) \arrow[l] \arrow[r, equal] & \hat{H}^2(o, \mathscr{A}^0[p^v]) & \hat{H}^2(o, N\mathscr{A}^0[p^v]) \arrow[l]
\end{tikzcd}$$

Explanations. (i) For the identification $\mathscr{A}^0(o) = H^0(o_\infty/o, \mathscr{A}^0)$ compare the proof of § 7 Lemma 1 in [20]. The existence of the other maps between the first and second column is obvious from the fact that the o-morphism $\mathscr{A}^0 \xrightarrow{p^v} \mathscr{A}^0$ is faithfully flat.

(ii) The identifications between the second and third column are a consequence of the fact that $R^iM(\mathscr{A}^0) = R^iM_\infty(\mathscr{A}^0) = 0$ for $i > 0$ (see Propositions (4.5) and (4.5')).

(iii) There is a canonical inclusion $N\mathscr{A}^0 \subseteq M\mathscr{A}^0$ since A has good reduction at the primes $\mathfrak{p} \in \Sigma$.

(iv) The maps δ arise from the distinguished triangles in $D^+(\mathscr{S}(o))$, resp. $D^+(\mathscr{Z}(o))$, which correspond to multiplication by p^v on $\mathscr{A}^0$, resp. $M\mathscr{A}^0$, resp. $N\mathscr{A}^0$.

(v) The maps between the second and third, resp. fourth and fifth, row are given by the first descent spectral sequence and by the spectral sequence after Remark (4.6) (the respective cohomology groups are p-torsion groups, and $\mathrm{cd}_p\Gamma \leq 1$). According to Lemma (4.7) the two spectral sequences are compatible.

(vi) The maps between the third and fourth row are induced by the identity maps. Recall that we always fix our generator ϕ of Γ.

One possibility to define cup-product is to require the commutativity of the diagram

$$\begin{tikzcd}
H^1(o, \tilde{\mathscr{A}}^0_{p^v}) \arrow[d] & \times & H^2(o, \mathscr{A}^0_{p^v}) \arrow[r, "\cup"] \arrow[dd, equal] & H^3(o, \mu_{p^v}) = \mathbb{Z}/p^v\mathbb{Z} \arrow[dd, equal] \\
H^1(o, \underline{\mathrm{Hom}}_o(\mathscr{A}^0_{p^v}, \mu_{p^v})) \arrow[d, "\varepsilon_1"] & & & \\
\mathrm{Ext}^1_o(\mathscr{A}^0_{p^v}, \mu_{p^v}) & \times & H^2(o, \mathscr{A}^0_{p^v}) \arrow[r, "\vee"] & H^3(o, \mu_{p^v}) = \mathbb{Z}/p^v\mathbb{Z}
\end{tikzcd} \quad (3)$$

where the homomorphism of sheaves $\tilde{\mathscr{A}}^0_{p^v} \to \underline{\mathrm{Hom}}_o(\mathscr{A}^0_{p^v}, \mu_{p^v})$ is induced by the pairing $\tilde{\mathscr{A}}^0 \otimes \mathscr{A}^0 \to \mu$ which defines the cup-product in the upper row, and

where ε_1 is the first edge morphism in the local-global spectral sequence for Ext's. Using (2) and (3) we can replace (1) by the diagram

$$\begin{tikzcd}
\tilde{\mathscr{A}}^0(o) \otimes \mathbb{Z}_p \arrow[d, "\delta"] & N\mathscr{A}^0(o) \otimes \mathbb{Q}_p/\mathbb{Z}_p \arrow[d, "\delta"] \\
\varprojlim H^1(o, \tilde{\mathscr{A}}^0_{p^v}) \arrow[dd] & \varinjlim \hat{H}^1(o, N\mathscr{A}^0[p^v]) \arrow[d] \\
& \varinjlim \hat{H}^1(o_\infty, N\mathscr{A}^0[p^v])^\Gamma \arrow[d] \\
\varprojlim H^1(o, \underline{\mathrm{Hom}}_o(\mathscr{A}^0_{p^v}, \mu_{p^v})) \arrow[dd, "\varepsilon_1"] & \varinjlim \hat{H}^1(o_\infty, N\mathscr{A}^0[p^v])_\Gamma \arrow[d] \\
& \varinjlim \hat{H}^2(o, N\mathscr{A}^0[p^v]) \arrow[d] \\
& H^2(o_\infty/o, \mathscr{A}^0(p)) \\
\varprojlim \mathrm{Ext}^1_o(\mathscr{A}^0_{p^v}, \mu_{p^v}) \quad \times & H^2(o, \mathscr{A}^0(p)) \arrow[u] \xrightarrow{\vee} H^3(o, \mu(p)) = \mathbb{Q}_p/\mathbb{Z}_p.
\end{tikzcd} \quad (4)$$

In the next step we transform the left column of (4) into a sequence of Ext-groups. We consider the diagram

$$\begin{tikzcd}
H^1(o, \tilde{\mathscr{A}}^0_{p^v}) \arrow[d] & H^0(o, \tilde{\mathscr{A}}^0) \arrow[l, "-\delta"'] \arrow[d] \\
H^1(o, \underline{\mathrm{Hom}}_o(\mathscr{A}^0_{p^v}, \mu_{p^v})) \arrow[d, "\varepsilon_1"] & H^0(o, \underline{\mathrm{Ext}}^1_o(\mathscr{A}^0, \mathbb{G}_m)) \\
\mathrm{Ext}^1_o(\mathscr{A}^0_{p^v}, \mu_{p^v}) & \mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m). \arrow[l, "r"'] \arrow[u, "\cong", "\varepsilon_2"']
\end{tikzcd} \quad (5)$$

Here ε_2 is the second edge morphism in the local-global spectral sequence for Ext's; because of $\underline{\mathrm{Hom}}_o(\mathscr{A}^0, \mathbb{G}_m) = 0$ (see SGA 7 VII 1.3.8) it is an isomorphism. The canonical biextension of $(A, \tilde{A})$ by $\mathbb{G}_m$ given by the Poincaré divisor defines a canonical homomorphism of sheaves

$$\tilde{\mathscr{A}}^0 \to \underline{\mathrm{Ext}}^1_o(\mathscr{A}^0, \mathbb{G}_m)$$

such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & \underline{\mathrm{Hom}}_o(\mathscr{A}^0_{p^v}, \mu_{p^v}) \arrow[r] & \underline{\mathrm{Ext}}^1_o(\mathscr{A}^0, \mathbb{G}_m) \arrow[r, "p^v"] & \underline{\mathrm{Ext}}^1_o(\mathscr{A}^0, \mathbb{G}_m) & \\
0 \arrow[r] & \tilde{\mathscr{A}}^0_{p^v} \arrow[u] \arrow[r] & \tilde{\mathscr{A}}^0 \arrow[u] \arrow[r, "p^v"] & \tilde{\mathscr{A}}^0 \arrow[u] \arrow[r] & 0
\end{tikzcd}$$

is commutative (see SGA 7 VIII). Of course, the composite map in the right column of (5) is the same as the "inclusion"

$$\tilde{\mathscr{A}}^0(o) \subseteq \tilde{A}(k) = \mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m).$$

The map r is induced by the obvious map of complexes

$$r^{\cdot}\colon \underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0, I^{\cdot}) \to \underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, I^{\cdot}_{p^\nu}) \to \underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, J^{\cdot})$$

where $\mathbb{G}_m \xrightarrow{\sim} I^{\cdot}$, resp. $I^{\cdot}_{p^\nu} \xrightarrow{\sim} J^{\cdot}$, is an injective resolution of $\mathbb{G}_m$, resp. the complex of sheaves $I^{\cdot}_{p^\nu}$.

Lemma 3. *The diagram* (5) *is commutative.*

Proof. In the language of derived categories the edge morphisms ε_1 and ε_2 have the following descriptions:

$$\varepsilon_1\colon\ \begin{array}{c} H^1(\wp, \underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu})), \\ \downarrow \\ H^1(\wp, \tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu})) \\ \| \\ H^1(\wp, \mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu})) \\ \| \\ \mathrm{Ext}^1_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \end{array} \qquad \text{and} \qquad \varepsilon_2\colon\ \begin{array}{c} \mathrm{Ext}^1_{\wp}(\mathscr{A}^0, \mathbb{G}_m) \\ \| \\ H^1(\wp, \mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0, \mathbb{G}_m)) \\ \| \\ H^1(\wp, \tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0, \mathbb{G}_m)) \\ \downarrow \cong \\ H^1(\wp, T^{-1}(\underline{\mathrm{Ext}}^1_{\wp}(\mathscr{A}^0, \mathbb{G}_m))) \\ \| \\ H^0(\wp, \underline{\mathrm{Ext}}^1_{\wp}(\mathscr{A}^0, \mathbb{G}_m)) \end{array}$$

where $\tau_{\leqq 1}$ denotes the truncation functor in dimension 1 (see SGA 4 XVII 1.1.13). We therefore have to prove that the outer part of the following diagram is commutative in the derived category $D^+(\mathscr{S}(\wp))$:

$$\begin{tikzcd}
\tilde{\mathscr{A}}^0_{p^\nu} \arrow[rr, "\cong"] \arrow[ddd] & & \tilde{\mathscr{A}}^0[p^\nu] & & T^{-1}(\tilde{\mathscr{A}}^0) \arrow[ll, "-1"'] \arrow[ddd] \\
& & (a) & & \\
& {[\tilde{\mathscr{A}}^0_{p^\nu} \to \tilde{\mathscr{A}}^0]} \arrow[uul, "{(\mathrm{id},0)}"] \arrow[uurrr, "{(0,p^\nu)}", "\cong"'] \arrow[d] & (b) & (b) & \\
& {[\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \xrightarrow{\delta} \underline{\mathrm{Ext}}^1_{\wp}(\mathscr{A}^0, \mathbb{G}_m)]} \arrow[dl, "{(\mathrm{id},0)}"'] \arrow[drrr, "{(0,p^\nu)}"] & & & \\
\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \arrow[d] & & (c) & & T^{-1}(\underline{\mathrm{Ext}}^1_{\wp}(\mathscr{A}^0, \mathbb{G}_m)) \\
\tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) & & & & \tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0, \mathbb{G}_m) \arrow[llll, "r"'] \arrow[u, "\cong"']
\end{tikzcd}$$

(the indicated isomorphisms take place in $D^+(\mathscr{S}(\wp))$). It is easy to check that the part (a) of the above diagram is commutative up to homotopy; the

commutativity of the parts (b) is trivial. It remains to consider the part (c). Let

$$\mathbb{G}_m \xrightarrow{\sim} I^{\cdot}, \quad I^{\cdot}_{p^\nu} \xrightarrow{\sim} J^{\cdot}, \quad \text{and} \quad s^{\cdot}\colon \underline{\mathrm{Hom}}_{\wp}(\mathscr{A}^0_{p^\nu}, J^{\cdot}) \xrightarrow{\sim} K^{\cdot}$$

be injective resolutions. We shall extract all the necessary information from the exact diagram of complexes

$$\begin{tikzcd}
0 \arrow[r] & \underline{\mathrm{Hom}}(\mathscr{A}^0, I^{\cdot}) \arrow[r, "p^\nu"] & \underline{\mathrm{Hom}}(\mathscr{A}^0, I^{\cdot}) \arrow[r] \arrow[dr, "r^{\cdot}"'] & \underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, I^{\cdot}_{p^\nu}) \arrow[r] \arrow[d] & 0 \\
& & & \underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, J^{\cdot}) \arrow[d, "s^{\cdot}"] & \\
& & & K^{\cdot} &
\end{tikzcd}$$

(in order to simplify the notation we skip the subscript "$\wp$" in the following). Because of $\underline{\mathrm{Hom}}(\mathscr{A}^0, \mathbb{G}_m) = 0$ we find a map h which makes the diagram

$$\begin{tikzcd}
0 \arrow[d] & & \\
\underline{\mathrm{Hom}}(\mathscr{A}^0, I^0) \arrow[r, "r^0"] \arrow[d] & \underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, J^0) \arrow[r, "s^0"] & K^0 \\
\underline{\mathrm{Hom}}(\mathscr{A}^0, I^1)_\partial \arrow[urr, dashed, "h"'] & &
\end{tikzcd}$$

commutative (the subscript "∂" indicates the kernel of the differential in the respective complex). One easily checks that

$$\begin{aligned} &(K^0 \to K^1_\partial) \circ h - (s^1 \circ r^1) | \underline{\mathrm{Hom}}(\mathscr{A}^0, I^1)_\partial \\ &\quad = (\underline{\mathrm{Hom}}(\mathscr{A}^0, I^1)_\partial \to \underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m) \xrightarrow{f} K^1_\partial) \end{aligned}$$

for an appropriate map f. This means that the diagram

$$\text{(d)} \qquad \begin{tikzcd}
\tau_{\leqq 1}K^{\cdot}(\mathrm{d}) & T^{-1}(\underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m)) \arrow[l, "{(0,-f)}"'] \\
\tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \arrow[u, "\tau_{\leqq 1}s^{\cdot}"] & \tau_{\leqq 1}\mathbf{R}^+\underline{\mathrm{Hom}}(\mathscr{A}^0, \mathbb{G}_m) \arrow[l, "r"'] \arrow[u]
\end{tikzcd}$$

is commutative up to homotopy. Furthermore $\tau_{\leqq 1}s^{\cdot}$ induces an isomorphism in $D^+(\mathscr{S}(\wp))$.

On the other hand we find a map g such that

$$\begin{tikzcd}
\underline{\mathrm{Hom}}(\mathscr{A}^0, I^1)_\partial \arrow[r, "h\circ p^\nu"] \arrow[d] & K^0 \\
\underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m) \arrow[ur, dashed, "g"'] \arrow[d] & \\
0 &
\end{tikzcd}$$

is commutative. It is not hard to see that g fits into the commutative diagram

$$\begin{tikzcd}
\underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \arrow[rr] \arrow[d, "\delta"'] & & K^0 \arrow[d] \\
\underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m) \arrow[r, "p^\nu"] \arrow[urr, "g"] & \underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m) \arrow[r, "f"] & K^1_\partial .
\end{tikzcd}$$

But this means that the diagram

$$\text{(e)}\qquad \begin{tikzcd}
 & {[\underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \xrightarrow{\delta} \underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m)]} \arrow[dl, "(\mathrm{id},0)"'] \arrow[dr, "(0,p^\nu)"] & \\
\underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \arrow[d] & & T^{-1}(\underline{\mathrm{Ext}}^1(\mathscr{A}^0, \mathbb{G}_m)) \arrow[d, "(0,-f)"'] \\
\tau_{\leq 1} \mathbf{R}^+ \underline{\mathrm{Hom}}(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) \arrow[rr, "\tau_{\leq 1} s^\cdot"] & & \tau_{\leq 1} K^\cdot
\end{tikzcd}$$

is commutative up to homotopy. Now, (d) and (e) together imply the commutativity of (c) in the derived category. q.e.d.

Using (5) we can replace (4) by the diagram

$$\begin{tikzcd}
\tilde{\mathscr{A}}^0(o) \otimes \mathbf{Z}_p \arrow[ddd, "\subseteq"'] & & N\mathscr{A}^0(o) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[d, "\delta"'] & \\
 & & \varinjlim \hat{H}^1(o, N\mathscr{A}^0[p^\nu]) \arrow[d] & \\
 & & & \\
\mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m) \otimes \mathbf{Z}_p \arrow[ddd, "-r"'] & & \varinjlim \hat{H}^1(o_\infty, N\mathscr{A}^0[p^\nu])^\Gamma \arrow[d] & \\
 & & \varinjlim \hat{H}^1(o_\infty, N\mathscr{A}^0[p^\nu])_\Gamma \arrow[d] & \\
 & & \varinjlim \hat{H}^2(o, N\mathscr{A}^0[p^\nu]) \arrow[d] & \\
 & & H^2(o_\infty/o, \mathscr{A}^0(p)) & \\
\varprojlim \mathrm{Ext}^1_o(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) & \times & H^2(o, \mathscr{A}^0(p)) \arrow[u] \arrow[r, "\vee"] & H^3(o, \mu(p)) = \mathbf{Q}_p/\mathbf{Z}_p .
\end{tikzcd} \tag{6}$$

The essential step will be the next in which we transform the Yoneda pairing in the bottom row into one between modified cohomology groups. We first define a map similar to r. If

$$\begin{aligned}
&\mathrm{Ext}^1_{\mathscr{Z}(o)}(N\mathscr{A}^0, N\mathbb{G}_m) = \mathrm{Hom}_{D^+(\mathscr{Z}(o))}(N\mathscr{A}^0, T(N\mathbb{G}_m)) \\
&\quad \to \mathrm{Hom}_{D^+(\mathscr{Z}(o))}(N\mathscr{A}^0[p^\nu], T(N\mathbb{G}_m[p^\nu])) = \mathrm{Ext}^1_{\mathscr{Z}(o)}(N\mathscr{A}^0[p^\nu], N\mathbb{G}_m[p^\nu])
\end{aligned}$$

is the canonical map given by the functoriality of the $[p^\nu]$-construction then we denote by $\hat{r}$ the composite map

$$\hat{r}\colon \mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m) \to \mathrm{Ext}^1_{\mathscr{Z}(o)}(N\mathscr{A}^0, N\mathbb{G}_m) \to \varprojlim \mathrm{Ext}^1_{\mathscr{Z}(o)}(N\mathscr{A}^0[p^\nu], N\mathbb{G}_m[p^\nu]).$$

We want to prove that the diagram

$$\begin{tikzcd}
\varprojlim \mathrm{Ext}^1_{\mathscr{Z}(o)}(N\mathscr{A}^0[p^\nu], N\mathbb{G}_m[p^\nu]) & \times & \varinjlim \hat{H}^2(o, N\mathscr{A}^0[p^\nu]) \arrow[r, "\vee'"] \arrow[d] & \varinjlim \hat{H}^3(o, N\mathbb{G}_m[p^\nu]) \arrow[d, "d"] \\
\mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m) \arrow[u, "\hat{r}"] \arrow[d, "r"'] & & H^2(o_\infty/o, \mathscr{A}^0(p)) & \mathbf{Q}_p/\mathbf{Z}_p \arrow[d, equal] \\
\varprojlim \mathrm{Ext}^1_o(\mathscr{A}^0_{p^\nu}, \mu_{p^\nu}) & \times & H^2(o, \mathscr{A}^0(p)) \arrow[u] \arrow[r, "\vee"] & H^3(o, \mu(p))
\end{tikzcd}$$

is almost commutative in the following sense.

Lemma 4. *There is a $C \in \mathbb{N}$ such that, for any $e \in \mathrm{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m)$ and for any*

$$y \in \varinjlim \hat{H}^2(o, N\mathscr{A}^0[p^\nu]) \quad \text{and} \quad x \in H^2(o, \mathscr{A}^0(p))$$

which map to the same element in $H^2(o_\infty/o, \mathscr{A}^0(p))$, we have

$$C \cdot (r(e) \vee x - d(\hat{r}(e) \vee y)) = 0.$$

Proof. Because of $H^3(o_\infty/o, \mu(p)) = 0$ this cannot be proved directly. Instead of that we use a local method based on an important result of Serre. Namely, let S be the set of primes of k which lie above ∞ or p or which split completely in k_∞ or at which A has bad reduction. Because of [13] (5.1(v)) the vertical maps in the commutative diagram

$$\begin{tikzcd}
H^1(o, \tilde{\mathscr{A}}_{p^\nu}) \arrow[r, "\rho'_\nu"] \arrow[d] & \prod_{\mathfrak{p} \notin S} H^1(o_{\mathfrak{p}}, \tilde{\mathscr{A}}_{p^\nu}) \arrow[d] \\
H^1(k, \tilde{A}_{p^\nu}) \arrow[r, "\rho_\nu"] & \prod_{\mathfrak{p} \notin S} H^1(k_{\mathfrak{p}}, \tilde{A}_{p^\nu})
\end{tikzcd}$$

are injective. Since S is a set of density zero we have, according to [22], that the groups $\ker \rho_\nu$ are finite and that $\varprojlim(\ker \rho_\nu) = 0$ (the result is stated there only for finite sets S, but the proof literally extends to our situation by using the Čebotarev density theorem) and consequently

$$\varprojlim (\ker \rho'_\nu) = 0.$$

Using the local and global flat duality theorems this implies the surjectivity of the map

$$\bigoplus_{\mathfrak p\notin S} H^2_\cdot(\mathfrak o_{\mathfrak p},\mathscr A(p))\to H^2(\mathfrak o,\mathscr A(p)).$$

The cokernel of the map

$$\bigoplus_{\mathfrak p\notin S} H^2_\cdot(\mathfrak o_{\mathfrak p},\mathscr A(p))\to H^2(\mathfrak o,\mathscr A^0(p))$$

therefore is finite of order C_1, say. Now let $(x_{\mathfrak p})_{\mathfrak p\notin S}\in\bigoplus_{\mathfrak p\notin S} H^2_\cdot(\mathfrak o_{\mathfrak p},\mathscr A(p))$ be a preimage of $C_1 x$ and denote by y' the image of $(x_{\mathfrak p})$ under the natural map

$$\bigoplus_{\mathfrak p\notin S} H^2_\cdot(\mathfrak o_{\mathfrak p},\mathscr A(p))\to \varinjlim \hat H^2(\mathfrak o, N\mathscr A^0[p^v]).$$

The compatibility assertion of Lemma (5.5) then implies

$$C_1\cdot(r(e)\vee x)=\sum_{\mathfrak p\notin S} r(e)\vee x_{\mathfrak p}=\sum_{\mathfrak p\notin S}\hat r(e)\vee x_{\mathfrak p}=d(\hat r(e)\vee y').$$

But from our assumption follows $C_2\cdot y'=C_2C_1\cdot y$ where C_2 denotes the order of the kernel of the map

$$\varinjlim \hat H^2(\mathfrak o, N\mathscr A^0[p^v])\to H^2(\mathfrak o_\infty/\mathfrak o,\mathscr A^0(p))$$

which is finite since A has ordinary good reduction at the primes in Σ. With $C:=C_2C_1$ we finally get

$$C\cdot(r(e)\vee x)=C\cdot d(\hat r(e)\vee y).\quad \text{q.e.d.}$$

From (6) and Lemma 4 we easily derive that our algebraic pairing $(\log_p\kappa(\phi))^{-1}\cdot\langle\ ,\ \rangle_\kappa$ also is defined by the diagram

$$\begin{tikzcd}
\tilde{\mathscr A}^0(\mathfrak o)\otimes\mathbb Z_p \arrow[dd,"\subseteq"'] & N\mathscr A^0(\mathfrak o)\otimes\mathbb Q_p/\mathbb Z_p \arrow[d,"\delta"] & \\
 & \varinjlim \hat H^1(\mathfrak o, N\mathscr A^0[p^v]) \arrow[d] & \\
\mathrm{Ext}^1_{\mathfrak o}(\mathscr A^0,\mathbf G_m)\otimes\mathbb Z_p \arrow[dd,"-\hat r"'] & \varinjlim \hat H^1(\mathfrak o_\infty, N\mathscr A^0[p^v])^\Gamma \arrow[d] & \\
 & \varinjlim \hat H^1(\mathfrak o_\infty, N\mathscr A^0[p^v])_\Gamma \arrow[d] & \\
\varprojlim \mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0[p^v],N\mathbf G_m[p^v])\times & \varinjlim \hat H^2(\mathfrak o, N\mathscr A^0[p^v]) \arrow[r,"\vee"] & \varinjlim \hat H^3(\mathfrak o, N\mathbf G_m[p^v]) \arrow[d,"d"] \\
 & & \mathbb Q_p/\mathbb Z_p.
\end{tikzcd}$$

But for functorial reasons the above diagram can further be simplified to the following one:

$$\begin{tikzcd}
\tilde A^0(\mathfrak o)\otimes\mathbb Z_p \arrow[d,"\subseteq"'] & N\mathscr A^0(\mathfrak o)\otimes\mathbb Q_p/\mathbb Z_p \arrow[ddd,"-\delta"] & \\
\mathrm{Ext}^1_{\mathfrak o}(\mathscr A^0,\mathbf G_m)\otimes\mathbb Z_p \arrow[d] & & \\
\mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0,N\mathbf G_m)\otimes\mathbb Z_p \arrow[d] & & \\
\varprojlim \mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0[p^v],N\mathbf G_m[p^v])\times & \varinjlim \hat H^1(\mathfrak o, N\mathscr A^0[p^v]) \arrow[r,"\vee"] & \varinjlim \hat H^2(\mathfrak o, N\mathbf G_m[p^v]) \arrow[d] \\
 & & \varinjlim \hat H^2(\mathfrak o_\infty, N\mathbf G_m[p^v]) \arrow[d,"\deg_\phi"] \\
 & & \mathbb Q_p/\mathbb Z_p.
\end{tikzcd}$$

The anticommutativity of the connecting homomorphism implies the commutativity of

$$\begin{tikzcd}
\mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0,N\mathbf G_m) \arrow[d] & \times & N\mathscr A^0(\mathfrak o) \arrow[r] \arrow[d,"-\delta"] & \hat H^1(\mathfrak o, N\mathbf G_m) \arrow[r,"\deg_\phi"] \arrow[d,"\delta"] & \mathbb Z_p \arrow[dd] \\
\mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0[p^v],N\mathbf G_m[p^v]) & \times & \hat H^1(\mathfrak o, N\mathscr A^0[p^v]) \arrow[r] & \hat H^2(\mathfrak o, N\mathbf G_m[p^v]) \arrow[d] & \\
 & & & \hat H^2(\mathfrak o_\infty, N\mathbf G_m[p^v]) \arrow[r,"\deg_\phi"] & \mathbb Z/p^v\mathbb Z.
\end{tikzcd}$$

The combination of the last two diagrams shows that the pairing $\langle\ ,\ \rangle_\kappa$ is given by

$$\begin{tikzcd}
\tilde{\mathscr A}^0(\mathfrak o) \arrow[d,"\subseteq"'] & N\mathscr A^0(\mathfrak o) \arrow[dd, equal] & & \\
\mathrm{Ext}^1_{\mathfrak o}(\mathscr A^0,\mathbf G_m) \arrow[d] & & & \\
\mathrm{Ext}^1_{\mathscr X(\mathfrak o)}(N\mathscr A^0,N\mathbf G_m)\times & N\mathscr A^0(\mathfrak o) \arrow[r,"\vee"] & \hat H^1(\mathfrak o, N\mathbf G_m) \arrow[r,"-\deg"] & \mathbb Z_p
\end{tikzcd}$$

which precisely is the assertion we wanted to prove.

§ 7. Analytic heights

We begin by recalling the definition given in [19] (but see also [24]) of the analytic p-adic height pairing associated with κ. For any

$$\tilde{a}=(0\to\mathbb{G}_m\to\mathscr{X}\to\mathscr{A}^0\to 0)\in\operatorname{Ext}^1_{\mathscr{o}}(\mathscr{A}^0,\mathbb{G}_m)=\tilde{A}(k)$$

we have the exact sequence of points in the finite adeles $\mathbb{A}$ of k

$$0\to\mathbb{G}_m(\mathbb{A})\to\mathscr{X}(\mathbb{A})\to\mathscr{A}^0(\mathbb{A})\to 0.$$

The homomorphism $v_{k,\kappa}\colon \mathbb{G}_m(\mathbb{A})\to\mathbb{Z}_p$ extends in a unique way to a homomorphism $v_{\tilde{a}}\colon \mathscr{X}(\mathbb{A})\to\mathbb{Q}_p$ which vanishes on $\prod_{\mathfrak{p}\notin\Sigma}\mathscr{X}(\mathscr{o}_\mathfrak{p})\times\prod_{\mathfrak{p}\in\Sigma}N\mathscr{X}(k_\mathfrak{p})$. By restriction to global points $v_{\tilde{a}}$ induces a map $v_{\tilde{a}}\colon A(k)\to\mathbb{Q}_p$ and we put

$$(\ ,\ )_\kappa\colon \tilde{A}(k)\times A(k)\to\mathbb{Q}_p$$
$$(\tilde{a},a)\mapsto v_{\tilde{a}}(a).$$

Proposition 1.

$$(\ ,\ )_\kappa=(\ ,\ ).$$

Proof. If $N\tilde{a}=(0\to N\mathbb{G}_m\to N\mathscr{X}\to N\mathscr{A}^0\to 0)$ denotes the image of $\tilde{a}$ in $\operatorname{Ext}^1_{\mathscr{Z}(\mathscr{o})}(N\mathscr{A}^0,N\mathbb{G}_m)$ then, for $a\in N\mathscr{A}^0(\mathscr{o})=\operatorname{Hom}_{\mathscr{Z}(\mathscr{o})}(\mathscr{J}_*\mathbb{Z},N\mathscr{A}^0)$, the Yoneda product $N\tilde{a}\vee a\in\hat{H}^1(\mathscr{o},N\mathbb{G}_m)=\operatorname{Ext}^1_{\mathscr{Z}(\mathscr{o})}(\mathscr{J}_*\mathbb{Z},N\mathbb{G}_m)$ is given by the commutative exact diagram

$$\begin{array}{lccccccccc}
N\tilde{a}\vee a\colon & 0 & \longrightarrow & N\mathbb{G}_m & \longrightarrow & \mathscr{Y} & \longrightarrow & \mathscr{J}_*\mathbb{Z} & \longrightarrow & 0\\
 & & & & & \downarrow & & \downarrow{\scriptstyle a} & & \\
\tilde{a}\colon & 0 & \longrightarrow & N\mathbb{G}_m & \longrightarrow & N\mathscr{X} & \longrightarrow & N\mathscr{A}^0 & \longrightarrow & 0.
\end{array}$$

By composition we get an extension

$$v_{N\tilde{a}\vee a}\colon \mathscr{Y}(\mathbb{A})\longrightarrow\mathscr{X}(\mathbb{A})\xrightarrow{v_{\tilde{a}}}\mathbb{Q}_p$$

of $v_{k,\kappa}$ which vanishes on $\prod_{\mathfrak{p}\notin\Sigma}\mathscr{Y}(\mathscr{o}_\mathfrak{p})\times\prod_{\mathfrak{p}\in\Sigma}H^0(\Gamma_\mathfrak{p},I_\mathfrak{p}^*\mathscr{Y})$ (observe that because of Lemma (6.1) and [19] Lemma 3 we have $H^0(\Gamma_\mathfrak{p},I_\mathfrak{p}^*N\mathscr{X})=N\mathscr{X}(k_\mathfrak{p})$). It induces a map

$$v_{N\tilde{a}\vee a}\colon \mathbb{Z}\xrightarrow{a}N\mathscr{A}^0(\mathscr{o})\xrightarrow{v_{\tilde{a}}}\mathbb{Q}_p$$

with the property

$$(\tilde{a},a)_\kappa=v_{N\tilde{a}\vee a}(1).$$

Our assertion now is a consequence of the following lemma.

Lemma 2. *For*

$$e=(0\to N\mathbb{G}_m\to\mathscr{Y}\to\mathscr{J}_*\mathbb{Z}\to 0)\in\operatorname{Ext}^1_{\mathscr{Z}(\mathscr{o})}(\mathscr{J}_*\mathbb{Z},N\mathbb{G}_m)=\hat{H}^1(\mathscr{o},N\mathbb{G}_m)$$

and an extension $v_e\colon \mathscr{Y}(\mathbb{A})\to\mathbb{Q}_p$ of $v_{k,\kappa}$ which vanishes on

$$\prod_{\mathfrak{p}\notin\Sigma}\mathscr{Y}(\mathscr{o}_\mathfrak{p})\times\prod_{\mathfrak{p}\in\Sigma}H^0(\Gamma_\mathfrak{p},I_\mathfrak{p}^*\mathscr{Y})$$

let $v_e\colon \mathbb{Z}\to\mathbb{Q}_p$ be the map induced by restriction to global sections. We then have

$$v_e(1)=\deg e.$$

Proof. We choose $f\in\hat{H}^0(\mathscr{o},\hat{\mathscr{D}})=\operatorname{Hom}_{\mathscr{Z}(\mathscr{o})}(\mathscr{J}_*\mathbb{Z},\hat{\mathscr{D}})$ such that $\delta f=e$ where δ is the connecting homomorphism corresponding to (2) in § 5. This amounts to the existence of a commutative exact diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N\mathbb{G}_m & \longrightarrow & \mathscr{Y} & \longrightarrow & \mathscr{J}_*\mathbb{Z} & \longrightarrow & 0\\
 & & \| & & \downarrow & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & N\mathbb{G}_m & \longrightarrow & \mathscr{J}_*\mathscr{G}_m & \longrightarrow & \hat{\mathscr{D}} & \longrightarrow & 0.
\end{array}$$

If $(f_\mathfrak{p})_\mathfrak{p}\in\hat{H}^0(\mathscr{o},\hat{\mathscr{D}})=(\bigoplus_{\mathfrak{p}\notin\Sigma}k_\mathfrak{p}^\times/\mathscr{o}_\mathfrak{p}^\times)\oplus(\bigoplus_{\mathfrak{p}\in\Sigma}k_\mathfrak{p}^\times/Nk_\mathfrak{p})$ denotes the image of $1\in\hat{H}^0(\mathscr{o},\mathscr{J}_*\mathbb{Z})$ under f we obviously have

$$\deg e=-v_{k,\kappa}((f_\mathfrak{p})_\mathfrak{p}).$$

Let now $s_\mathfrak{p}\in\mathscr{Y}(\mathscr{o}_\mathfrak{p})$ for $\mathfrak{p}\notin\Sigma$, resp. $\in H^0(\Gamma_\mathfrak{p},I_\mathfrak{p}^*\mathscr{Y})$ for $\mathfrak{p}\in\Sigma$, be a preimage of $1\in\mathbb{Z}$ (we observe that because of Remark (5.1) and Hilbert 90 we have $H^1(\Gamma_\mathfrak{p},Nk_{\mathfrak{p},\infty})=0$ and therefore the exact sequence

$$0\to Nk_\mathfrak{p}\to H^0(\Gamma_\mathfrak{p},I_\mathfrak{p}^*\mathscr{Y})\to\mathbb{Z}\to 0).$$

Also let $s\in\mathscr{Y}(k)$ be a preimage of $1\in\mathbb{Z}$, and denote by $s'_\mathfrak{p}\in k_\mathfrak{p}^\times$, resp. $s'\in k^\times$, the image of $s_\mathfrak{p}$, resp. s, under the map f'. We then compute

$$\begin{aligned}
v_e(1)=v_e(s)&=v_e((s_\mathfrak{p}^{-1}\cdot s)_\mathfrak{p})=v_{k,\kappa}((s_\mathfrak{p}^{-1}\cdot s)_\mathfrak{p})\\
&=v_{k,\kappa}((s_\mathfrak{p}'^{-1}\cdot s')_\mathfrak{p})=-v_{k,\kappa}((s'_\mathfrak{p})_\mathfrak{p})=-v_{k,\kappa}((f_\mathfrak{p})_\mathfrak{p})\\
&=\deg e. \quad \text{q.e.d.}
\end{aligned}$$

The above proposition and Proposition (6.2) together give the main result of this Sect. B.

Theorem 6. *Let A be ordinary for k_∞. We have $\langle\ ,\ \rangle_\kappa=-(\ ,\ )_\kappa$.*

As a consequence, Theorem 2′ can be transformed into the following statement which should be considered as an analog for $L_p(A,\kappa,s)$ of the conjecture of Birch and Swinnerton-Dyer.

Theorem 7. *Let A be ordinary for k_∞, and suppose that $Ш_k(A)(p)$ is finite and that $(\ ,\ )_\kappa$ is nondegenerate. We then have $m=\operatorname{rank}_\mathbb{Z}A(k)$ and*

$$c\sim\frac{\det(\ ,\ )_\kappa\cdot\#Ш_k(A)(p)}{\#\operatorname{Tor}A(k)\cdot\#\operatorname{Tor}\tilde{A}(k)}\cdot\prod_\mathfrak{p}\#\pi_\mathfrak{p}(A)\cdot\Big(\prod_{\mathfrak{p}\in\Sigma}\#\mathscr{A}(\kappa_\mathfrak{p})\Big)^2.$$

We also get a criterion for the finite generation of $A(k_\infty)$ which is independent of any assumption about the Tate-Šafarevič group.

Theorem 8. *Let A be ordinary for k_∞, and suppose that $(\ ,\ )_\kappa\colon \tilde{A}(k_n)\times A(k_n)\to \mathbb{Q}_p$ is nondegenerate for all $n\in\mathbb{N}$. Then $A(k_\infty)$ is finitely generated as an abelian group if $\operatorname{Tor} A(k_\infty)$ is finite (which is the case, for example, for the cyclotomic $\mathbb{Z}_p$-extension k_∞; see* [5]).

Proof. According to the argument in the proof of [13] (6.11) we have to show that $\operatorname{rank}_{\mathbb{Z}} A(k_n)$ is bounded independently of n. But

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}} A(k_n) &= \operatorname{rank}((\ ,\ )_\kappa \text{ for } A_{/k_n})\\ &= \operatorname{rank}(\langle\ ,\ \rangle_\kappa \text{ for } A_{/k_n})\\ &\leqq \operatorname{rank}_{\mathbb{Z}_p} H^0(\Gamma_n, H^1(o_\infty, \mathscr{A}(p))^*)\end{aligned}$$

is bounded by the $\mathbb{Z}_p$-rank of the $\mathbb{Z}_p[\![\Gamma]\!]$-torsion submodule of $H^1(o_\infty, \mathscr{A}(p))^*$.

Appendix: A cohomological interpretation of the Néron-Tate height

There is also an interesting modification of the usual $fppf$-cohomology of $\operatorname{Spec}(o)$ at infinity. For simplicity and in order to emphasize the parallelism we use in the following the same notations as in § 4. Let $\mathscr{X}(o)$ be the mapping cylinder of the left exact functors

$$H^0(k_p, \alpha_p^*\cdot)\colon \mathscr{S}(o)\to\mathscr{S}(k_p)\to(\text{abelian groups})$$

for p/∞ where k_p denotes the completion of k at p and $\alpha_p\colon \operatorname{Spec}(k_p)\to\operatorname{Spec}(o)$ is the canonical morphism. We define

$$\hat{H}^i(o,.) := \operatorname{Ext}^i_{\mathscr{X}(o)}(\mathscr{J}_*\mathbb{Z},.)$$

as new cohomology theory which takes the archimedean primes into respect. One obviously can develop for $\hat{H}^i(o,.)$ a similar formalism as in § 4. And again one has a trace map: For p/∞ let $Nk_p \leqq k_p^\times$ denote the maximal compact subgroup of $k_p^\times$; we have

$$Nk_p = \ker(\log\circ|\ |_p)$$

where, for any prime p, $|\ |_p\colon k_p^\times\to\mathbb{R}_+^\times$ denotes the normalized absolute value. The "multiplicative group" in $\mathscr{X}(o)$ now is

$$N\mathbb{G}_m := (\mathbb{G}_{m/o}; (Nk_p)_{p/\infty}; \text{inclusion}).$$

There is a canonical exact sequence

$$\begin{array}{ccccccc} k^\times & \longrightarrow & \Big(\bigoplus\limits_{p\nmid\infty} k_p^\times/o_p^\times\Big)\oplus\Big(\bigoplus\limits_{p/\infty} k_p^\times/Nk_p\Big) & \longrightarrow & \hat{H}^1(o, N\mathbb{G}_m) & \longrightarrow & 0\\ & & \Big\downarrow{\scriptstyle -\Sigma_p \log\cdot|\,|_p\ =:\ v_k} & \swarrow{\scriptstyle \deg} & & & \\ & & \mathbb{R} & & & & \end{array}$$

which shows that v_k induces a homomorphism

$$\deg\colon \hat{H}^1(o, N\mathbb{G}_m)\to\mathbb{R}$$

called the (real) trace map.

Let now $A_{/k}$ be an arbitrary abelian variety over k. We have the pairing

$$\operatorname{Ext}^1_{\mathscr{X}(o)}(\mathscr{J}_*\mathscr{A}^0, N\mathbb{G}_m)\times\hat{H}^0(o, \mathscr{J}_*\mathscr{A}^0) = \mathscr{A}^0(o) \xrightarrow{\ \vee\ } \hat{H}^1(o, N\mathbb{G}_m)\xrightarrow{\ \deg\ }\mathbb{R}.$$

Via the natural map

$$\tilde{A}(k) = \operatorname{Ext}^1_o(\mathscr{A}^0, \mathbb{G}_m)\to\operatorname{Ext}^1_{\mathscr{X}(o)}(\mathscr{J}_*\mathscr{A}^0, N\mathbb{G}_m)$$

$$(0\to\mathbb{G}_m\to\mathscr{X}\to\mathscr{A}^0\to 0)\to(0\to N\mathbb{G}_m\to N\mathscr{X}\to\mathscr{J}_*\mathscr{A}^0\to 0)$$

with $N\mathscr{X} := (\mathscr{X};\ (\text{max. compact subgroup of } \mathscr{X}(k_p))_{p/\infty};\ \text{inclusion})$ it induces a pairing

$$(\ ,\ )\colon \tilde{A}(k)\times A(k)\to\mathbb{R}.$$

Proposition. $(\ ,\ )$ *is the Néron-Tate height pairing.*

The proof is completely analogous to the proof of Proposition (7.1) and is based on Bloch's description of the Néron-Tate height in [1].

In this context we also should mention the pairing

$$\operatorname{Hom}_{\mathscr{X}(o)}(\mathscr{J}_!\mathbb{Z}, N\mathbb{G}_m) = o^\times\times\hat{H}^1(o, \mathscr{J}_!\mathbb{Z})\xrightarrow{\ \vee\ }\hat{H}^1(o, N\mathbb{G}_m)\longrightarrow\mathbb{R} \qquad (*)$$

between finitely generated abelian groups of the same rank.

Proposition. *The determinant of* (*) *is equal (up to sign) to the unit regulator of k.*

See [10] for a very similar result.

References

1. Bloch, S.: A note on height pairings, Tamagawa numbers and the Birch and Swinnerton-Dyer conjecture. Invent. math. **58**, 65–76 (1980)
2. Coates, J.: Infinite Descent on Elliptic Curves with Complex Multiplication. In: Arithmetic and Geometry, Papers Dedicated to I.R. Shafarevich, vol. I. Progress in Math. vol. 35, pp. 107–137. Boston-Basel-Stuttgart: Birkhauser 1983
3. Ferrero, B., Washington, L.: The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. Math. **109**, 377–395 (1979)
4. Greenberg, R.: On a Certain l-Adic Representation. Invent. math. **21**, 117–124 (1973)
5. Imai, H.: A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions. Proc. Japan Acad. **51**, 12–16 (1975)
6. Iwasawa, K.: On some properties of Γ-finite modules. Ann. Math. **70**, 291–312 (1959)
7. Iwasawa, K.: On $\mathbb{Z}_\ell$-extensions of algebraic number fields. Ann. Math. **98**, 246–326 (1973)
8. Jannsen, U.: Über Galoisgruppen lokaler Körper. Invent. math. **70**, 53–69 (1982)
9. Konovalov, G.: The universal Γ-norms of formal groups over a local field. Ukrain. Mat. Z. **28**, 396–398 (1976)
10. Lichtenbaum, S.: Values of zeta and L-functions at zero. Astérisque **24-25**, 133–138 (1975)
11. Lubin, J., Rosen, M.: The Norm Map for Ordinary Abelian Varieties. J. Algebra **52**, 236–240 (1978)
12. Mazur, B.: Local flat duality. Amer. J. Math. **92**, 343–361 (1970)
13. Mazur, B.: Rational Points of Abelian Varieties with Values in Towers of Number Fields. Invent. math. **18**, 183–266 (1972)
14. Mazur, B.: Notes on étale cohomology of number fields. Ann. sci. ENS **6**, 521–556 (1973)
15. Mazur, B., Messing, W.: Universal extensions and one-dimensional crystalline cohomology. Lecture Notes in Math., vol. 370. Berlin-Heidelberg-New York: Springer 1974
16. Milne, J.S.: Etale cohomology. Princeton: Princeton Univ. Press 1980
17. Perrin-Riou, B.: Arithmétique des courbes elliptiques et théorie d'Iwasawa. Thése 1983
18. Schneider, P.: Zur Vermutung von Birch and Swinnerton-Dyer über globalen Funktionenkörpern. Math. Ann. **260**, 495–510 (1982)
19. Schneider, P.: p-adic height pairings I. Invent. math. **69**, 401–409 (1982)
20. Schneider, P.: Iwasawa L-functions of varieties over algebraic number fields. A first approach. Invent. math. **71**, 251–293 (1983)

21. Serre, J-P.: Cohomologie Galoisienne. Lecture Notes in Math., vol. 5. Berlin-Heidelberg-New York: Springer 1964
22. Serre, J-P.: Sur les groupes de congruence des variétés abéliennes I, II. Izv. Akad. Nauk SSSR **28**, 3-20 (1964) and **35**, 731-737 (1971)
23. Serre, J-P.: Letter to Mazur, 1974
24. Mazur, B., Tate, J.: Canonical Height Pairings via Biextensions. In Arithmetic and Geometry, Papers Dedicated to I.R. Shafarevich, vol. I. Progress in Math. vol. 35, pp. 195-237. Boston-Basel-Stuttgart: Birkhauser 1983
25. Hazewinkel, M.: Norm maps for formal groups I: J. Algebra **32**, 89-108 (1974). II: J. reine angew. Math. **268/69**, 222-250 (1974). III: Duke Math. J. **44**, 305-314 (1977). IV: Michigan Math. J. **25**, 245-255 (1978)
SGA Grothendieck, A., Artin, M., Deligne, P., Demazure, M., Verdier, J.L.: Séminaire de Géométrie Algébrique du Bois Marie. 3I: Lecture Notes in Math. vol. 151. Berlin-Heidelberg-New York: Springer 1970. 4: Ibidem **269**, **270**, **305** (1972-73). $4\frac{1}{2}$: Ibidem **569** (1977). 7I: Ibidem **288** (1972)

Oblatum 1-II & 31-VII-1984