Height pairings in the Iwasawa theory of abelian varieties

Schneider, Peter

First published in:
Séminaire de Théorie des Nombres, S. 309 – 316, Boston 1980-81, ISBN 3-7643-3066-X

Seminaire Delange-Pisot-Poitou
(Theorie des Nombres)
1980-81

HEIGHT PAIRINGS IN THE IWASAWA THEORY OF ABELIAN VARIETIES

Peter Schneider
University of Regensburg

Let $k|\mathbb{Q}$ be a finite algebraic number field. We fix an odd prime number p and denote by $\mu(p)$ resp. μ_{p^n} the group of all roots of unity of order a power of p resp. dividing p^n. The Galois group $G := \mathrm{Gal}(k_\infty|k)$ of $k_\infty := k(\mu(p))$ over k has the canonical decomposition $G = \Gamma \times \Delta$ with $\Gamma := \mathrm{Gal}(k_\infty|k(\mu_p))$ and $\Delta := \mathrm{Gal}(k(\mu_p)|k)$; furthermore the action of G on $\mu(p)$ defines a character $\kappa: G \to \mathbb{Z}_p^*$ into the p-adic units. We choose a topological generator γ of Γ in a canonical way by the requirement that $\kappa(\gamma)$ is of the form $1+p^e$ with $e \in \mathbb{N}$. The principle of Iwasawa theory is now the following: Given an algebraic object over k one tries to associate with it in a natural way certain modules over the completed group ring $\mathbb{Z}_p[[\Gamma]]$. If this is done in the right way, there should exist a deep connection between the "characteristic polynomials" of γ on these modules and the complex zeta functions of the object.

The Iwasawa theory of an abelian variety over k was initiated by Mazur in [3]. This talk will give a discussion of an analog of the conjecture of Birch/Swinnerton-Dyer/Tate in this setting.

1. The Iwasawa zeta function of an abelian variety.

Let A be an abelian variety over k and $\mathcal{A}$ its Néron-model over the ring of integers $\mathfrak{O}$ in k. Furthermore $\mathcal{A}(p) := \varinjlim \mathcal{A}_{p^j}$ denotes the ind-group scheme of kernels $\mathcal{A}_{p^j}$ of multiplication with p^j in $\mathcal{A}$. We then have the natural G-modules

$$H^i(\mathcal{O}_\infty, \mathcal{A}(p)),$$

where $\mathcal{O}_\infty$ is the ring of integers in k_∞ and the cohomology is (during the whole talk) understood to be taken with respect to the FPQF-topology. In order to get nice results about these cohomology groups we have to impose the following restriction on p, which from now on is assumed to be fulfilled:

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

Moreover we need some notation: Let $\tilde{A}$ be the dual abelian variety and $\tilde{\mathcal{A}}$ its Néron-model over $\mathcal{O}$; let $\tilde{\mathcal{A}}^0$ be the connected component of the $\mathcal{O}$-scheme $\tilde{\mathcal{A}}$ in the sense of SGA3 VI_B§3. For an abelian group M let M(p) be the p-primary torsion component; for a $\mathbb{Z}_p$-module N let $N^* := \mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontrjagin dual. Finally $\mathcal{O}_n$ denotes the ring of integers in $k_n := k(\mu_{p^n})$.

<u>Proposition 1</u> (Artin/Mazur). The cup-product induces a complete duality of finite groups

$$H^i(\mathcal{O}, \mathcal{A}_{p^j}) \times H^{3-i}(\mathcal{O}, \tilde{\mathcal{A}}_{p^j}) \to \mathbb{Q}/\mathbb{Z}\,.$$

<u>Proposition 2</u>.

i) $H^0(\mathcal{O}, \mathcal{A}(p))$ is finite;

ii) $H^i(\mathcal{O}, \mathcal{A}(p)) = 0$ for $i \geq 3$;

iii) $0 \to A(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathcal{O}, \mathcal{A}(p)) \to H^1(\mathcal{O}, \mathcal{A})(p) \to 0$ is exact;

iv) if $H^1(\mathcal{O}, \mathcal{A})(p)$ is finite, then $H^2(\mathcal{O}, \mathcal{A}(p)) = (\tilde{\mathcal{A}}^0(\mathcal{O}) \otimes \mathbb{Z}_p)^*$ and corank $H^1(\mathcal{O}, \mathcal{A}(p))$ = corank $H^2(\mathcal{O}, \mathcal{A}(p)) = \mathrm{rank}_{\mathbb{Z}} A(k)$.

<u>Proof</u>: This follows from Proposition 1 and a detailed study of the cohomology of the exact sequence $0 \to \mathcal{A}_{p^j} \to \mathcal{A} \xrightarrow{p^j} \mathcal{A}$.

<u>Proposition 3</u>.

i) $H^0(\mathcal{O}_\infty, \mathcal{A}(p))$ is finite;

ii) $H^1(\mathcal{O}_\infty, \mathcal{A}(p))^*$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$ -module;

iii) $H^i(\mathcal{O}_\infty, \mathcal{A}(p)) = 0$ for $i \geq 3$;

iv. if $H^1(\mathcal{O}_\infty,\mathcal{A}(p))^*$ is a $\mathbb{Z}_p[[\Gamma]]$-torsion module and $H^1(\mathcal{O}_n,\mathcal{A})(p)$ is finite for all $n \in \mathbb{N}$, then $H^2(\mathcal{O}_\infty,\mathcal{A}(p)) = 0$.

Proof: For i) see [1]. The other assertions follow from Proposition 2 and results in [3].

Remark: 1) In [3] it is shown that the p-primary component of the Tate-Šafarevič-group $Ш_k(A)$ of A is contained in $H^1(\mathcal{O},\mathcal{A})(p)$ with finite index. Therefore the conjectured finiteness of $Ш_k(A)$ would imply the finiteness of $H^1(\mathcal{O},\mathcal{A})(p)$.
2) Mazur conjectures in [3] that $H^2(\mathcal{O}_\infty,\mathcal{A}(p))^*$ is (under our condition on p - otherwise definitely not) always a $\mathbb{Z}_p[[\Gamma]]$-torsion module.

From now on we assume that

$$\mathcal{H} := H^1(\mathcal{O}_\infty,\mathcal{A}(p))^* \text{ is a } \mathbb{Z}_p[[\Gamma]]\text{-torsion module}$$

and

$$Ш_{k_n}(A)(p) \text{ is finite for all } n \in \mathbb{N}.$$

We think of $\mathcal{H}$ as the "right" module which is associated with A and p in a natural way. Since $d := \#\Delta$ is prime to p we have the natural decomposition

$$\mathcal{H} = \bigoplus_{j \bmod d} e_j\mathcal{H},$$

where $e_j\mathcal{H}$ is the maximal submodule on which $\delta \in \Delta$ acts as multiplication by $\kappa(\delta)^j$. If we identify $\mathbb{Z}_p[[\Gamma]]$ with the power series ring in one variable $\mathbb{Z}_p[[T]]$ by $\gamma \mapsto 1 + T$, then the general theory of $\mathbb{Z}_p[[T]]$-modules tells us the existence of quasi-isomorphisms (i.e. homomorphisms with finite kernel and cokernel)

$$e_j\mathcal{H} \to \bigoplus_{\alpha=1}^{\alpha_j} \mathbb{Z}_p[[T]]/\langle f^{(j)}(T)\rangle,$$

where $f_\alpha^{(j)}(T) \in \mathbb{Z}_p[T]$ is a distinguished polynomial or a power of p. Furthermore

$$F_j(T) := \prod_{\alpha=1}^{\alpha_j} f_\alpha^{(j)}(T)$$

depends only on $e_j\mathcal{H}$ and is called the characteristic polynomial of $e_j\mathcal{H}$ (see [2]).

<u>Definition</u>: The Iwasawa zeta function of A at p is

$$\zeta_p(A,s) := F_o((1 + p^e)^{1-s} - 1).$$

According to [3], $\zeta_p(A,s)$ has a functional equation with respect to $s \mapsto 2 - s$. Our aim is the study of this function at $s = 1$. This means we have to consider the numbers $\rho \geq 0$ and $c_p(A) \in \mathbb{Q}_p$ which are defined by

$$F_o(T)\cdot T^{-\rho}\Big|_{T=0} =: c_p(A) \neq 0.$$

For this purpose we have to connect the cohomology groups of $\mathfrak{A}(p)$ over $\mathcal{O}_\infty$ and over $\mathcal{O}$. But the morphism $\mathrm{Spec}(\mathcal{O}_\infty) \to \mathrm{Spec}(\mathcal{O})$ is not proetale; therefore, in this situation, a Hochschild-Serre spectral sequence does not exist!

2. <u>The descent diagram</u>.

Let $\pi : X := \mathrm{Spec}(\mathcal{O}_\infty) \to Y := \mathrm{Spec}(\mathcal{O})$ be the canonical morphism. If $\tilde{Y}$ denotes the category of sheaves on the fpqf-situs of Y, we then have the functors

$$\begin{aligned} \Gamma_X^G : \tilde{Y} &\rightsquigarrow \text{abelian groups} \\ \mathcal{F} &\mapsto (\pi^*\mathcal{F}(X))^G, \\ \pi_G : \tilde{Y} &\rightsquigarrow Y \\ \mathcal{F} &\mapsto \pi_G\,(V \to Y) := (\pi^*\mathcal{F})(V \times_Y X)^G, \end{aligned}$$

and the commutative diagrams of functors

$$\begin{array}{ccc} \tilde{Y} & \xrightarrow{\ \Gamma_X\ } & \text{discrete } G\text{-modules} \\ & {\scriptstyle \Gamma_X^G}\searrow \quad \swarrow{\scriptstyle H^o(G,.)} & \\ & \text{abelian groups} & \end{array}$$

$$\begin{array}{ccc} \tilde{Y} & \overset{\pi_G}{\rightsquigarrow} & \tilde{Y} \\ & {\scriptstyle \Gamma_X^G} \searrow \quad \swarrow {\scriptstyle \Gamma_Y} & \\ & \text{abelian groups} & \end{array}$$

where Γ_X and Γ_Y are the usual section functors. Now let

$$H^i(\mathcal{O}_\infty/\mathcal{O},.) := R^i\Gamma_X^G,$$

denote the right derived functions of Γ_X^G. Then it is not hard to show the existence of two spectral sequences

$$H^i(G,H^j(\mathcal{O}_\infty,\pi^*\mathcal{F})) \Rightarrow H^{i+j}(\mathcal{O}_\infty/\mathcal{O},\mathcal{F}) \tag{1}$$

and

$$H^i(\mathcal{O},R^j\pi_G\mathcal{F}) \Rightarrow H^{i+j}(\mathcal{O}_\infty/\mathcal{O},\mathcal{F}), \quad \mathcal{F} \in \tilde{Y}. \tag{2}$$

The following fact enables us to use these spectral sequences for our purposes.

Lemma 4. $\mathcal{G}(p) = \pi_G\mathcal{G}(p)$ as sheaves in $\tilde{Y}$ (not as ind-group schemes).

We are now ready to establish the exact "descent" diagram:

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & & & H^1(\mathcal{O},\mathcal{G}(p)) & \overset{\alpha}{\dashrightarrow} & & & \\
 & & & & \downarrow & & & & \\
0 & \to & H^1(G,A(k_\infty)(p)) & \to & H^1(\mathcal{O}_\infty/\mathcal{O},\mathcal{G}(p)) & \to & H^0(G,H^1(\mathcal{O}_\infty,\mathcal{G}(p))) & \to & 0 \\
 & & & & \downarrow & & & & \\
 & & & & H^0(\mathcal{O},R^1\pi_G\mathcal{G}(p)) & & & & \\
 & & & & \downarrow & & & & \\
 & & & & H^2(\mathcal{O},\mathcal{G}(p)) & \overset{\beta}{\dashrightarrow} & & & \\
 & & & & \downarrow & & & & \\
 & & & & H^2(\mathcal{O}_\infty/\mathcal{O},\mathcal{G}(p)) & = & H^1(G,H^1(\mathcal{O}_\infty,\mathcal{G}(p))) & . &
\end{array} \tag{3}$$

Here the vertical line is given by the exact sequence of lower terms of (2) after replacing $\mathcal{C}(p)$ by $\pi_G\mathcal{C}(p)$ according to lemma 4. The horizontal sequences are induced by (1) because of Proposition 3 and the fact that the cohomological p-dimension of G is ≤ 1. α and β denote simply the induced maps.

3. <u>The numbers</u> ρ <u>and</u> $c_p(A)$.

The key fact for the analysis of the descent diagram (3) is the following result.

<u>Proposition 5</u>. $H^0(\mathcal{O}, R^1\pi_G\mathcal{C}(p))$ is finite of order $(\prod_{\mathfrak{P}|p} \#\mathcal{C}(\kappa_{\mathfrak{P}})(p))^2$, where $\kappa_{\mathfrak{P}}$ denotes the residue class field of $\mathcal{O}$ at $\mathfrak{P}$.

<u>Idea of proof</u>: First we observe that the restriction of $R^1\pi_G\mathcal{C}(p)$ to $Y\setminus\{\mathfrak{P}|p\}$ is zero. Therefore $H^0(\mathcal{O}, R^1\pi_G\mathcal{C}(p))$ turns out to be a product of local cohomology groups at the primes above p. But the latter ones we can compute because of our assumption that A has not only good but ordinary reduction at all $\mathfrak{P}|p$.

<u>Corollary</u>: The maps α and β in (3) are quasi-isomorphisms.

<u>Proof</u>: Use Proposition 2 iv) and Proposition 5.

Now we consider the sequence of maps

$$\begin{array}{l} H^0(G,\mathcal{H}) \xrightarrow{f} H^1(G,\mathcal{H}) \xrightarrow{\alpha^*} H^1(\mathcal{O},\mathcal{C}(p))^* \to \operatorname{Hom}(A(k)\otimes\mathbb{Z}_p,\mathbb{Z}_p) \\ \quad\big\downarrow * \\ H^2(\mathcal{O},\mathcal{C}(p))^* \\ \quad\| \\ \tilde{\mathcal{C}}^0(\mathcal{O})\otimes\mathbb{Z}_p \\ \quad\cap\| \\ \tilde{A}(k)\otimes\mathbb{Z}_p\ , \end{array}$$

where f is induced by the identity on $\mathcal{H}$ (because of our chosen generator γ we can identify $H^1(G,\mathcal{H})$ with the coinvariants of G in $\mathcal{H}$), and the non-specified maps are given by Proposition 2.

Evidently this sequence of maps determines uniquely a pairing

$$< \, , \, > \; : \; A(k) \times \tilde{A}(k) \to \mathbb{Q}_p,$$

which is non-degenerate if and only if f is a quasi-isomorphism. Furthermore we can express $|\det < \, , \, >|_p$ in terms of the orders of the kernels and cokernels of the maps in the above sequence taken modulo torsion subgroups. Why is this pairing useful for our problem?

Lemma 6:

i) $\rho \geq \operatorname{rank}_{\mathbb{Z}_p} H^0(G,\mathcal{H})$;

ii) $\rho = \operatorname{rank}_{\mathbb{Z}_p} H^0(G,\mathcal{H}) \Leftrightarrow f$ is a quasi-isomorphism; in this case we have

$$|c_p(A)|_p^{-1} = (\# \operatorname{coker} f)/(\# \ker f) \; .$$

Proof: This is an easy generalization of Lemma z.4 in [4] if one takes the general structure theory of $\mathbb{Z}_p[[\Gamma]]$-modules into consideration.

Therefore we have a close relation between $\det< \, , \, >$ and $c_p(A)$ in the case that $< \, , \, >$ is non-degenerate. Using the descent diagram and Proposition 5 we can give this relation the following form.

Theorem:

i) $\rho \geq \operatorname{rank}_{\mathbb{Z}} A(k)$;

ii) $\rho = \operatorname{rank}_{\mathbb{Z}} A(k) \Leftrightarrow < \, , \, >$ is non-degenerate;

if this is fulfilled and if $e_0\mathcal{H}$ has no finite Γ-submodules $\neq 0$ (in addition to the assumptions already made), we then have

$$|c_p(A)|_p^{-1} = \left((Ш_k(A)(p) \cdot |\det< \, , \, >|_p^{-1}) / (\# A(k)(p) \cdot \# \widetilde{A(k)}(p)\right)$$

$$\cdot \prod_{\mathfrak{q}} \# \pi_{\mathfrak{q}}(A)(p) \cdot \Big(\prod_{\mathfrak{q} | p} \# \mathfrak{a}(\kappa_{\mathfrak{q}})(p) \Big)^2 ,$$

where $\pi_{\mathfrak{q}}(A)$ denotes the group of $\kappa_{\mathfrak{q}}$-rational connected components of the reduction of A at $\mathfrak{q}$.

REFERENCES

1. Imai, H. A remark on the rational points of abelian varieties with values in cyclotomiz $\mathbb{Z}_p$-extensions, Proc. Japan Acad. 51, 12-16 (1975).

2. Iwasawa, K. On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. Math. 98, 246-326 (1973).

3. Mazur, B. Rational points of abelian varieties with values in towers of number fields, Inventiones Math. 18, 183-266 (1972).

4. Tate, J. On the conjecture of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki, exp. 306 (1966).