Contents

The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture for elliptic curves

Guido Kings

IAS/Park City Mathematics Series
Volume XX, XXXX

The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture for elliptic curves

Guido Kings

Introduction

This series of lectures has the modest goal to introduce the novice to the equivariant Tamagawa number conjecture (ETNC) by explicitly working out the example of the L-value of an elliptic curve at $s = 1$. It turns out (which is of course well-known to all experts) that the ETNC here is equivalent to the Birch-Swinnerton-Dyer (BSD) conjecture. In fact, the BSD conjecture was one of the guiding principles in the original formulation of the Tamagawa number conjecture by Bloch and Kato in [**BlKa**].

Although the extra generality of working equivariantly is completely superfluous for this result, it adds in fact not too much technicalities. It was the aim to show how BSD is part of much more general conjecture.

For a complete account of the conjecture it is indispensable to consult [**BuFl**], although more genteel introductions are [**Ka**] or [**Fo**], which both consider only commutative coefficients.

The beginner will find the working with determinant functors difficult and confusing. It should be very helpful to go through the exercises and to consider first only commutative rings to get a better feeling for this technical notion.

It was surprising for the author of these lectures that, although well-known, this equivalence between the ETNC and the BSD conjecture seems to never have been worked out explicitly in the literature. A notable exception is [**Ve**], which treats the general case of abelian varieties, but omits many details and $p = 2$. We therefore hope that these notes can provide a ready reference also for the expert in this field.

Universität Regensburg, NWF I-Mathematik, 93040 Regensburg, Germany
E-mail address: guido.kings@mathematik.uni-regensburg.de

LECTURE 1

Motives, cohomology and determinants

1. Motives

In this lecture we consider only a primitive version of motives. The whole ETNC can (and should) be set up for much more advanced theories of (mixed) motives. We follow here the exposition in [Ja] except that we use homological motives and use only equi-dimensional varieties for simplicity.

Let K be a field. Our main interest is $K = \mathbb{Q}$. Let $\mathcal{V}_K$ be the category of smooth, projective, equi-dimensional schemes over K. If $X, Y \in \mathcal{V}_K$, let for $r \in \mathbb{Z}$

$$A^{\dim X+r}(X \times Y) := CH^{\dim X+r}(X \times_K Y)_{\mathbb{Q}}, \tag{1}$$

the Chow group of $\mathbb{Q}$-linear codimension $\dim X + r$ cycles. Define a composition

$$\circ : A^{\dim X_1+r}(X_1 \times X_2) \times A^{\dim X_2+s}(X_2 \times X_3) \to A^{\dim X_1+r+s}(X_1 \times X_3) \tag{2}$$

by $f \times g \mapsto g \circ f := \mathrm{pr}_{13*}(\mathrm{pr}_{12}^*(f) \cdot \mathrm{pr}_{23}^*(g))$, where $\cdot$ is the intersection product and pr_{ij} is the projection onto the i, j component.

Definition 1. The category of *Chow motives* $\mathcal{M}_K$ over K has objects

$$M = (X, q, r), \tag{3}$$

where X/K is a smooth, projective and equi-dimensional variety, $q \circ q = q$ an idempotent in $A^{\dim X}(X \times X)$ and $r \in \mathbb{Z}$. Here the morphisms are

$$\mathrm{Hom}_{\mathcal{M}_K}(M, N) := q' \circ A^{\dim X'+r-r'}(X \times X') \circ q, \tag{4}$$

where $N = (X', q', r')$.

We use the following notation:

$$\begin{aligned} h(X) &:= (X, \Delta, 0), \quad \Delta \text{ the diagonal} \\ \mathbb{Q}(n) &:= (\mathrm{Spec} K, \Delta, n), \quad \text{the } \textit{Tate motive} \\ M(n) &:= (X, p, r+n), \quad \text{the } \textit{n-fold Tate twist.} \end{aligned} \tag{5}$$

Note that the functor, which sends X to $h(X)$ and f to its graph Γ_f is *covariant* (this means that our motives are homological, other conventions are possible). In particular, for a morphism $f : X \to Y$ one gets maps

$$\begin{aligned} \Gamma_f &: h(X) \to h(Y) \\ \Gamma_f^t &: h(Y) \to h(X)(\dim Y - \dim X). \end{aligned} \tag{6}$$

Definition 2. For $M = (X, p, r), N = (X', q', r') \in \mathcal{M}_K$ let

$$\begin{aligned} M \otimes_K N &:= (X \times_K X', q \times_K q', r + r') \quad \text{the } \textit{product} \\ M^\vee &:= (X, q^t, \dim X - r) \quad \text{the } \textit{dual}, \end{aligned} \tag{7}$$

where q^t is the image of q under the map, which interchanges the two factors in $X \times_K X$.

Remark 1. Note that the product is not the good one as it is not compatible with the product of the realizations of M and N. The problem is that the cup-product in cohomology is graded commutative, whereas the above product is commutative.

Definition 3. Let $A/\mathbb{Q}$ be finite dimensional and semi-simple. If $\mathrm{End}_{\mathcal{M}_K}(M)$ admits a ring homomorphism

$$\phi : A \to \mathrm{End}_{\mathcal{M}_K}(M) \tag{8}$$

we say that M has *coefficients in A*.

Example 1. Let L/K be a Galois extension, $G := \mathrm{Gal}(L/K)$ and $\mathbb{Q}[G]$ the group ring of G, then letting G act on Spec$L$ from the left, we have

$$\mathbb{Q}[G] \to \mathrm{End}(h(\mathrm{Spec}L)(n)). \tag{9}$$

One has

$$h(\mathrm{Spec}L)^\vee = h(\mathrm{Spec}L). \tag{10}$$

Example 2. Consider an elliptic curve E/K with unit section $e : \mathrm{Spec}K \to E$ and the idempotents $q_0 := E \times e$ and $q_2 := e \times E$ and let $q_1 := \Delta - p_0 - p_2$. Then

$$h(E) = h_0(E) \oplus h_1(E) \oplus h_2(E), \tag{11}$$

where $h_i(E) := (E, q_i, 0)$. Note that

$$(h_1(E)(1))^\vee(1) = h_1(E)(1). \tag{12}$$

Remark 2. If L/K is a finite field extension, one can define two functors

$$\mathrm{Res}_{L/K} : \mathcal{M}_L \to \mathcal{M}_K \qquad \text{resp.} \qquad \times_K L : \mathcal{M}_K \to \mathcal{M}_L, \tag{13}$$

which are called *restriction* and *extension* of scalars, respectively. Here $\mathrm{Res}_{L/K}M = (X, q, r)$ now considered over K and $M \times_k L = (X \times_K L, q \times_K L, r)$.

2. Realizations

Let $M = (X, q, r) \in \mathcal{M}_\mathbb{Q}$ and *fix* $i \in \mathbb{Z}_{\geq 0}$. We are going to define the i-th realizations of M but we *suppress* i from the notations.

Remark 3. The ETNC can be formulated for motives over number fields $K/\mathbb{Q}$ but it is compatible with restriction of scalars as defined in Remark 2, so that it is enough to consider motives in $\mathcal{M}_\mathbb{Q}$.

We need to define an action of correspondences $q \in A^{\dim X}(X \times X)$ on a cohomology theory.

Definition 4. Let $H^\cdot$ be a cohomology theory for $\mathcal{V}_K$, which admits cycle classes and has a product $\cup$ compatible with cycle classes. Let $X \in \mathcal{V}_K$ and $q \in A^{\dim X}(X \times X)$, then define

$$q^* : H^\cdot(X) \to H^\cdot(X) \tag{14}$$

by $q^*(\xi) := \mathrm{pr}_{2,*}(\xi \cup \mathrm{cl}(q))$, where $\mathrm{cl}(q) \in H^{2\dim X}(X \times X)$ is the cycle class.

Definition 5. The (i-th)*Betti realization* of M is

$$M_B := q^* H^i_{\mathrm{sing}}(X(\mathbb{C}), \mathbb{Q}(r)),$$

with its (pure) $\mathbb{Q}$-Hodge structure of weight $w = i - 2r$ and $F_\infty \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$-action induced from the one on $X(\mathbb{C})$ and on $\mathbb{Q}(r) := (2\pi i)^r \mathbb{Q} \subset \mathbb{C}$.

We denote by

$$M_B^+ = M_B^{F_\infty = 1} \tag{15}$$

the subspace, which is fixed by F_∞.

Definition 6. The (i-th) *de Rham realization* of M is

$$M_{\mathrm{dR}} := q^* H^i_{\mathrm{dR}}(X/\mathbb{Q}) = qH^i(\Omega^\cdot_{X/\mathbb{Q}})$$

together with the shifted Hodge filtration, i.e.,

$$\mathrm{Fil}^n M_{\mathrm{dR}} := q^* \mathrm{Fil}^{n+r} H^i_{\mathrm{dR}}(X/\mathbb{Q}) = q^* \mathrm{Im}(H^i(\Omega^{\geq n+r}_{X/\mathbb{Q}}) \to H^i(\Omega^\cdot_{X/\mathbb{Q}})).$$

The *tangent space* of M is

$$t(M) := M_{\mathrm{dR}} / \mathrm{Fil}^0 M_{\mathrm{dR}}.$$

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$.

Definition 7. Let p be a prime number. The (i-th) *p-adic realization* of M is

$$M_p := q^* H^i_{\text{ét}}(X \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p(r))$$

with its continuous $G_{\mathbb{Q}}$-action. Here $\mathbb{Q}(r)$ is the one dimensional $\mathbb{Q}$ vector space on which $G_{\mathbb{Q}}$ acts via the r-th power of the cyclotomic character.

Note that if M has coefficients in A, the realizations $M_B, M_{\mathrm{dR}}, M_p$ and $t(M)$ are A-modules.

Remark 4. For the dual motive $M^\vee$ we use the following convention. If we consider the i-th realization of M, then we consider the $(2\dim X - i)$-th realization of $M^\vee$. Note that if M has coefficients in A, then $M^\vee$ has coefficients in A^{opp}.

The following example is crucial for this lecture:

Example 3. We will use the following notations throughout these lectures. Let $E/\mathbb{Q}$ be an elliptic curve and fix $E(\mathbb{C}) \cong \mathbb{C}/\Gamma$. Denote by

$$T_pE := \varprojlim_n E[p^n](\overline{\mathbb{Q}}) \qquad \text{resp.} \qquad V_pE := T_E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \tag{16}$$

its Tate-module and its Tate-module tensor $\mathbb{Q}_p$. Consider $M = h_1(E)(1)$ and $i = 1$ (all other realizations are trivial). Then we identify

$$M_B = \mathrm{Hom}(\Gamma, \mathbb{Z}(1))_{\mathbb{Q}} \cong \Gamma_{\mathbb{Q}} \tag{17}$$

via the intersection pairing $\Gamma \times \Gamma \to \mathbb{Z}(1)$. Note that the connected component $E(\mathbb{R})^0$ of the Lie group $E(\mathbb{R})$ defines a generator

$$\mathrm{cl}_{E(\mathbb{R})^0} \in H_1(E(\mathbb{C}), \mathbb{Z})^+ \cong \Gamma^+. \tag{18}$$

The de Rham realization has a filtration

$$0 \to H^0(E, \Omega^1_{E/\mathbb{Q}}) \to H^1_{\mathrm{dR}}(E/\mathbb{Q}) \to H^1(E, \mathcal{O}_E) \to 0, \tag{19}$$

with $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(E/\mathbb{Q}) = H^0(E, \Omega^1_{E/\mathbb{Q}})$. We identify

$$t(M) = H^1(E, \mathcal{O}_E) \cong \mathrm{Lie}E. \tag{20}$$

For later use, we fix a basis $\omega \in H^0(E, \Omega^1_{E/\mathbb{Q}})$ and the dual $\omega^\vee$ in $\mathrm{Lie}E$ as follows: Suppose that $E/\mathbb{Q}$ is written in global minimal Weierstraß equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{21}$$

then we let

$$\omega := \frac{dx}{2y + a_1x + a_3} \tag{22}$$

and let $\omega^\vee \in \mathrm{Lie}E$ be its dual. The p-adic realization of M we identify

$$M_p = \mathrm{Hom}(V_pE, \mathbb{Q}_p) \cong V_pE \tag{23}$$

via the Weil pairing $T_pE \times T_pE \to \mathbb{Z}_p(1)$. Note that $T_pE \subset V_pE$ is a $G_\mathbb{Q}$-stable $\mathbb{Z}_p$-lattice.

The period map for M generalizes the periods for Riemann surfaces.

Definition 8. The comparison isomorphism $(M_B \otimes_\mathbb{Q} \mathbb{C})^+ \cong (M_{\mathrm{dR}} \otimes_\mathbb{Q} \mathbb{C})^+ = M_{\mathrm{dR},\mathbb{R}}$ induces via the inclusion $M^+_{B,\mathbb{R}} \subset (M_B \otimes_\mathbb{Q} \mathbb{C})^+$ and the projection $M_{\mathrm{dR},\mathbb{R}} \to t(M)_\mathbb{R}$ the *period map*

$$\alpha_M : M^+_{B,\mathbb{R}} \to t(M)_\mathbb{R}. \tag{24}$$

Here we have written $M_{\mathrm{dR},\mathbb{R}} := M_{\mathrm{dR}} \otimes_\mathbb{Q} \mathbb{R}$ etc.

Example 4. Let $M = h_1(E)(1)$ and $\mathrm{cl}_{E(\mathbb{R})^0} \in M^+_B$, $\omega^\vee \in \mathrm{Lie}E$ be the elements fixed in Example 3. Then the *period* Ω_∞ of E is the real number defined by

$$\alpha_M(\mathrm{cl}_{E(\mathbb{R})^0}) = \Omega_\infty \omega^\vee. \tag{25}$$

Remark 5. Note that α_M behaves well under duality. One has a perfect pairing

$$\mathrm{coker}\alpha_M \times \ker\alpha_{M^\vee(1)} \to \mathbb{R}, \tag{26}$$

which induces isomorphisms

$$\mathrm{coker}\alpha_M^\vee \cong \ker\alpha_{M^\vee(1)} \quad \text{and} \quad \ker\alpha_M^\vee \cong \mathrm{coker}\alpha_{M^\vee(1)}. \tag{27}$$

3. Motivic cohomology

Let $M = (X, q, r) \in \mathcal{M}_\mathbb{Q}$ and *fix* $i \in \mathbb{Z}_{\geq 0}$.

Definition 9. The motivic cohomology $H^j_{\mathrm{mot}}(\mathbb{Q}, M)$ of the pair (M, i) is defined for $j = 0, 1$ by

$$\begin{aligned} H^0_{\mathrm{mot}}(\mathbb{Q}, M) &:= \begin{cases} 0 & \text{if } i \neq 2r \\ CH^r(X)_\mathbb{Q}/CH^r(X)^0_\mathbb{Q} & \text{if } i = 2r. \end{cases} \\ H^1_{\mathrm{mot}}(\mathbb{Q}, M) &:= \begin{cases} K_{2r-i-1}(X)^{(r)}_\mathbb{Q} & \text{if } i \neq 2r-1 \\ CH^r(X)^0_\mathbb{Q} & \text{if } i = 2r-1. \end{cases} \end{aligned} \tag{28}$$

Here $CH^r(X)^0_\mathbb{Q} \subset CH^r(X)_\mathbb{Q}$ are the cycles homologically equivalent to zero. and $K_{2r-i-1}(X)^{(r)}_\mathbb{Q}$ is the r-th Adams eigenspace of the algebraic K-theory of X.

Simple examples show that $H^1_{\text{mot}}(\mathbb{Q}, M)$ has not the right dimension in general: For $M = h(\text{Spec}L)(1)$ one gets $H^1_{\text{mot}}(\mathbb{Q}, M) = L^\times \otimes_{\mathbb{Z}} \mathbb{Q}$, which is infinite dimensional. To remedy this defect, one possibility is to use the integral motivic cohomology:

Definition 10. Suppose that X has a proper, flat, regular model $\mathcal{X}/\mathbb{Z}$ (i.e. $\mathcal{X} \times_{\mathbb{Z}} \mathbb{Q} = X$). Then the *integral motivic cohomology* $H^i_{\text{mot}}(\mathbb{Z}, M)$ is defined as

$$H^0_{\text{mot}}(\mathbb{Z}, M) := H^0_{\text{mot}}(\mathbb{Q}, M)$$

(29)
$$H^1_{\text{mot}}(\mathbb{Z}, M) := \begin{cases} \text{Im}(K_{2r-i-1}(\mathcal{X})^{(r)}_{\mathbb{Q}} \to K_{2r-i-1}(X)^{(r)}_{\mathbb{Q}}) & \text{if } i \neq 2r-1 \\ CH^r(X)^0_{\mathbb{Q}} & \text{if } i = 2r-1. \end{cases}$$

This is independent of the choice of $\mathcal{X}$ (see [**Schn**] page 13).

Conjecture 1. *Suppose that M has coefficients in A. Then the groups $H^i_{\text{mot}}(\mathbb{Z}, M)$ for $i = 0, 1$ are A-modules of finite rank.*

Remark 6. If one does not want to assume the existence of a proper, flat, regular model one can use also use the construction using alterations by Scholl [**Scho2**].

Example 5. Let $L/\mathbb{Q}$ be a finite extension with ring of integers $\mathcal{O}_L$. Then $\text{Spec}\mathcal{O}_L$ is a proper, flat, regular model and for $M = h(\text{Spec}L)(1)$ one gets

(30)
$$H^1_{\text{mot}}(\mathbb{Z}, M) = \mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Example 6. Let $E/\mathbb{Q}$ be an elliptic curve, $M = h_1(E)(1)$ and $i = 1$, then

(31)
$$H^0_{\text{mot}}(\mathbb{Q}, M) = 0$$
$$H^1_{\text{mot}}(\mathbb{Q}, M) = CH^1(E)^0_{\mathbb{Q}} \cong \text{Pic}^0(E/\mathbb{Q})_{\mathbb{Q}} \cong E(\mathbb{Q})_{\mathbb{Q}}.$$

By definition, we have

(32)
$$H^i_{\text{mot}}(\mathbb{Z}, M) = H^i_{\text{mot}}(\mathbb{Q}, M) \quad \text{for } i = 0, 1.$$

Note: ① The motivic cohomology does not see torsion. ② These examples are essentially the only cases where conj. 1 is known.

4. L-functions

Let $M = (X, q, r) \in \mathcal{M}_{\mathbb{Q}}$ with coefficients in A and *fix* $i \in \mathbb{Z}_{\geq 0}$. From now on, A will always denote a finite dimensional, semi-simple $\mathbb{Q}$-algebra.

For simplicity of the exposition, we define the equivariant L-function in the case where $A/\mathbb{Q}$ is finite dimensional, semi-simple and commutative (i.e. a product of field extensions of $\mathbb{Q}$). This covers the case of $\mathbb{Q}[G]$ for G abelian, but not more general group rings. In Remark 7 we explain how to proceed in the general case.

Recall that $D_{\text{cris}}(M_p) := (B_{\text{cris}} \otimes_{\mathbb{Q}_p} M_p)^{G_{\mathbb{Q}_p}}$ is a finite dimensional $\mathbb{Q}_p$-vector space with a Frobenius endomorphism ϕ.

Definition 11. Let A be commutative. For each finite place v of $\mathbb{Q}$ let

(33)
$$L_v(M_p, T) := \begin{cases} \det_{A_{\mathbb{Q}_p}}(1 - \text{Frob}_v^{-1}T, M_p^{I_v}) & \text{if } v \neq p \\ \det_{A_{\mathbb{Q}_p}}(1 - \phi T, D_{\text{cris}}(M_p)) & \text{if } v = p. \end{cases}$$

be the local Euler factor at v. Here I_v is the inertia group and Frob_v is the Frobenius endomorphism.

Note that $L_v(M_p, T) \in A_{\mathbb{Q}_p}[T]$.

Conjecture 2. *The polynomial $L_v(M_p, T)$ lies in $A[T]$ and is independent of p.*

Definition 12. The *L-function* of M is the formal Euler product for $s \in \mathbb{C}$

$$L(M,s) := \prod_v L_v(M_p, v^{-s})^{-1}. \tag{34}$$

If we assume Conjecture 2, then $L(M,s)$ actually converges for $Res \gg 0$ (by the Weil conjectures) and defines an element in $A \otimes_{\mathbb{Q}} \mathbb{C}$. Conjecture 2 also implies that for real s

$$L(M,s) \in A \otimes_{\mathbb{Q}} \mathbb{R} \tag{35}$$

(see **[BuFl]** Lemma 8).

Remark 7. If $A/\mathbb{Q}$ is a finite dimensional, semi-simple algebra one can give the same definition of local Euler factors but with $\det_{A_{\mathbb{Q}_p}}$ replaced by the reduced determinant $\mathrm{detred}_{A_{\mathbb{Q}_p}}$ (see Example 13 for a definition). The resulting polynomials are in $Z(A_{\mathbb{Q}_p})[T]$, where $Z(A_{\mathbb{Q}_p})$ is the center of $A_{\mathbb{Q}_p}$. Conjecture 2 should then be formulated as $L_v(M_p,T)$ lies in $Z(A)[T]$ and is independent of p. The L-function $L(M,s)$ has then values in $Z(A) \otimes_{\mathbb{Q}} \mathbb{C}$. Note that $Z(A)$ is a product of field extensions of $\mathbb{Q}$.

Note that

$$L(M(n),s) = L(M,s+n). \tag{36}$$

We are interested in a conjecture concerning the special value of $L(M,s)$ at $s=0$. For this we need:

Conjecture 3. *The function $s \mapsto L(M,s)$ has a meromorphic continuation to (a neighborhood of) $s=0$.*

Conjecturally the order of vanishing of $L(M,s)$ at $s=0$ should be determined by the rank of the motivic cohomology. More precisely:

Conjecture 4. *Let A be commutative and assume Conjecture 1, then*

$$r_M := \mathrm{ord}_{s=0} L(M,s) = \mathrm{rk}_A H^1_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1)) - \mathrm{rk}_A H^0_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1)) \tag{37}$$

(equality of locally constant functions on $\mathrm{Spec}A$*).*

Remark 8. If A is not commutative, one has to replace the rank by the reduced rank $\mathrm{rkred}_A : K_0(A) \to \mathbb{Z}^{\#\mathrm{Spec}Z(A)}$, defined in Example 13.

The ETNC addresses the leading coefficient of Laurent series of $L(M,s)$ at $s=0$:

Definition 13. Assume Conjectures 2, 3 and 4. Let $r_M := \mathrm{ord}_{s=0}L(M,s)$ and define the *leading coefficient* at $s=0$ by

$$L(M,0)^* := \lim_{s\to 0} s^{-r_M} L(M,s) \in (A \otimes_{\mathbb{Q}} \mathbb{R})^\times. \tag{38}$$

Example 7. Let $E/\mathbb{Q}$ be an elliptic curve and consider $M = h_1(E)(1)$ and $i=1$. Then Conjecture 2 is known for $v \neq p$. Conjecture 3 follows from the work of Wiles et al., which identifies $L(M,s)$ with the L-function of a cusp form. Note that for$v \neq p$

$$L_v(M_p, v^{-1}) = \frac{\#\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)}{v}, \tag{39}$$

where $\widetilde{E}_v^{\mathrm{ns}}$ are the non-singular points in the reduction at v of a global minimal Weiertraß equation of E.

5. Determinants

We review the theory of determinants for arbitrary rings following the excellent exposition in [**FuKa**] to which we also refer for further details.

Let A be a ring and $P_{\mathrm{fg}}(A)$ the category of finitely generated, projective A-modules. We will use $K_0(A)$ and $K_1(A)$ (whose definition is recalled in Remark 9).

Definition 14. The category of *virtual objects* $V(A)$ has as objects pairs (P,Q), where $P,Q \in P_{\mathrm{fg}}(A)$. Let

(40)
$$\mathrm{Mor}_{V(A)}((P,Q),(P',Q')) := \begin{cases} \emptyset & \text{if } [P]-[Q] \neq [P']-[Q'] \in K_0(A) \\ K_1(A)-\text{torsor} & \text{if } [P]-[Q] = [P']-[Q'] \in K_0(A) \end{cases}$$

More precisely, choose $R \in P_{\mathrm{fg}}(A)$ such that $P \oplus Q' \oplus R \cong P' \oplus Q \oplus R$ and let $I_R := \mathrm{Isom}(P \oplus Q' \oplus R, P' \oplus Q \oplus R)$ be the $G_R := \mathrm{Aut}_A(P' \oplus Q \oplus R)$-torsor of isomorphisms. Then define

$$\mathrm{Mor}_{V(A)}((P,Q),(P',Q')) := K_1(A) \times^{G_R} I_R \tag{41}$$

as the push-out of the torsor I_R under the canonical map $G_R \to K_1(A)$. If R' is a different module with this property, let $R'' := R \oplus R'$. Then the canonical maps $G_R \to G_{R''}$ and $G_{R'} \to G_{R''}$ define isomorphisms

$$K_1(A) \times^{G_R} I_R \cong K_1(A) \times^{G_{R''}} I_{R''} \cong K_1(A) \times^{G_{R'}} I_{R'}, \tag{42}$$

which we use to identify the corresponding torsors.

One introduces the following notation

$$\begin{aligned} (P,Q)\cdot(P',Q') &:= (P \oplus Q, P' \oplus Q'), \quad \text{the } \textit{product} \\ (P,Q)^{-1} &:= (Q,P), \quad \text{the } \textit{inverse} \\ \mathrm{Det}_A(P) &:= (P,0), \quad \text{the } \textit{determinant}. \end{aligned} \tag{43}$$

One has

$$(P,Q) = \mathrm{Det}_A(P)\cdot \mathrm{Det}_A(Q)^{-1}. \tag{44}$$

Note that $\mathrm{Det}_A(0) = (0,0)$ is the unit object for the above product and that

$$\mathrm{Mor}_{V(A)}(\mathrm{Det}_A(0), \mathrm{Det}_A(0)) = K_1(A). \tag{45}$$

For a bounded complex $C^\cdot$ of modules in $P_{\mathrm{fg}}(A)$, define $\mathrm{Det}_A(C^\cdot) \in V(A)$ by

$$\mathrm{Det}_A(C^\cdot) := (C^{\mathrm{even}}, C^{\mathrm{odd}}), \tag{46}$$

where $C^{\mathrm{even}} := \bigoplus_j C^{2j}$ and $C^{\mathrm{odd}} := \bigoplus_j C^{2j+1}$.

One checks that for acyclic complexes $C^\cdot$ one has a canonical isomorphism

$$\mathrm{Det}_A(0) \cong \mathrm{Det}_A(C^\cdot). \tag{47}$$

Let $f: A \to B$ be a ring homomorphism. Then we have a functor

$$B\otimes_A : V(A) \to V(B) \tag{48}$$

defined by $B \otimes_A (P,Q) := (B \otimes_A P, B \otimes_A Q)$. For each isomorphism $\psi \in V(A)$ we denote by ψ_B the corresponding isomorphism in $V(B)$.

Example 8. Let $A/\mathbb{Q}$ be finite dimensional, commutative and semi-simple (i.e. a product of field extensions). Then $K_0(A) \cong \mathbb{Z}^{\#\mathrm{Spec}A}$ and the determinant induces an isomorphism $K_1(A) \cong A^\times$.

Example 9. Let $C^\cdot$ be an acyclic complex of modules in $P_{\mathrm{fg}}(A)$, then there is a canonical isomorphism $\mathrm{Det}_A(0) \cong \mathrm{Det}_A(C^\cdot)$. This implies that any quasi-isomorphism $C^\cdot \cong \widetilde{C}^\cdot$ induces $\mathrm{Det}_A(C^\cdot) \cong \mathrm{Det}_A(\widetilde{C}^\cdot)$ (as the cone is acyclic). Similarly, if $f,g : C^\cdot \to \widetilde{C}^\cdot$ are homotopic quasi-isomorphisms, the induced maps on determinants agree. This shows that the functor $C^\cdot \mapsto \mathrm{Det}_A(C^\cdot)$ factors though the image of $C^\cdot$ in the derived category.

This last example allows to define determinants for more general complexes.

Definition 15. For each complex $C^\cdot$, which is quasi-isomorphic to a bounded complex $\widetilde{C}^\cdot$ of modules in $P_{\mathrm{fg}}(A)$, we define

$$\mathrm{Det}_A(C^\cdot) := \mathrm{Det}_A(\widetilde{C}^\cdot). \tag{49}$$

Example 10. One can check that for a bounded complex $C^\cdot$ of modules in $P_{\mathrm{fg}}(A)$ with $H^j(C^\cdot) \in P_{\mathrm{fg}}(A)$ for all $i \in \mathbb{Z}$, one has

$$\mathrm{Det}_A(C^\cdot) \cong \prod_j \mathrm{Det}_A(H^j(C^\cdot)). \tag{50}$$

Example 11. Let A be commutative. Suppose that $B := (b_1, \dots, b_r)$ is a basis of P, then B induces an isomorphism

$$B : \mathrm{Det}_A(A^r) \cong \mathrm{Det}_A(P). \tag{51}$$

Let $B' = \phi B$ be a different choice of basis with $\phi \in \mathrm{End}(A^r)$, then the isomorphism $B' : \mathrm{Det}_A(A^r) \cong \mathrm{Det}_A(P)$ equals $B' = \det(\phi)B$.

Example 12. Let us consider the case $A = \mathbb{Z}_p$ in more detail. In this case all modules in $P_{\mathrm{fg}}(\mathbb{Z}_p)$ are free. As $\mathrm{rk}_{\mathbb{Z}_p} : K_0(\mathbb{Z}_p) \cong \mathbb{Z}$, two modules in $P_{\mathrm{fg}}(\mathbb{Z}_p)$ have isomorphic determinants, if and only if they have the same rank. In particular, let H be a finite group and a $\mathbb{Z}_p$-module. Then there is a resolution

$$0 \to P \xrightarrow{\psi} Q \to H \to 0, \tag{52}$$

with $P, Q \in P_{\mathrm{fg}}(\mathbb{Z}_p)$. As P and Q have the same rank, say r, one can choose bases $p_1, \dots, p_r$ and $q_1, \dots, q_r$ of P and Q respectively, and an isomorphism $\rho : P \cong Q$, which maps $\rho(p_i) = q_i$ for $i = 1, \dots, r$. Thus, one gets a map (again called ρ by abuse of notation)

$$\rho : \mathrm{Det}_{\mathbb{Z}_p}(0) \cong \mathrm{Det}_{\mathbb{Z}_p}(Q) \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(P) \tag{53}$$

induced by $\mathrm{Det}_{\mathbb{Z}_p}(P) \cong \mathrm{Det}_{\mathbb{Z}_p}(Q)$. On the other hand, the map $\mathrm{id}_{\mathbb{Q}_p} \otimes \psi$ is an isomorphism, so that one has a canonical isomorphism

$$\mathrm{id}_{\mathbb{Q}_p} \otimes \psi : \mathrm{Det}_{\mathbb{Q}_p}(0) \cong \mathrm{Det}_{\mathbb{Q}_p}(Q_{\mathbb{Q}_p}) \cdot \mathrm{Det}^{-1}_{\mathbb{Q}_p}(P_{\mathbb{Q}_p}). \tag{54}$$

Then one has $\rho_{\mathbb{Q}_p} = (\#H)^{-1}\mathrm{id}_{\mathbb{Q}_p} \otimes \psi$, where $\#H$ is considered as an element in $K_1(\mathbb{Q}_p) = \mathbb{Q}_p^\times$.

Example 13. We recall here some results about finite dimensional, central simple algebras A/F over a field F. Choose a splitting field F'/F such that $A \otimes_F F' \cong$

$\mathrm{Mat}_n(F')$ and an indecomposable idempotent $e \in A \otimes_F F'$. For each $V \in P_{\mathrm{fg}}(A)$ define the *reduced rank* of V to be

(55) $$\mathrm{rkred}_A(V) := \dim_{F'}(e(V \otimes_F F')).$$

This induces a map

(56) $$\mathrm{rkred}_A : K_0(A) \to \mathbb{Z}.$$

For an endomorphism $\phi \in \mathrm{End}_A(V)$ define the *reduced determinant* by

(57) $$\mathrm{detred}_A(\phi) := \det_{F'}(\phi \otimes \mathrm{id} \mid e(V \otimes_F F')).$$

Both notions are independent of the splitting field chosen. The reduced determinant induces the *reduced norm*

(58) $$\mathrm{normred}_A : K_1(A) \to Z(A)^\times = F^\times,$$

where $Z(A)$ denoted the center of A. It is shown in **[CuRe]** §45 A, that in the case where F is either a local or a global field, the map $\mathrm{normred}_A$ is injective. If F is a local field different from $\mathbb{R}$, $\mathrm{normred}_A$ is even an isomorphism. For $F = \mathbb{Q}$ one has

(59) $$\mathrm{Im}(\mathrm{normred}_A) = \{f \in \mathbb{Q}^\times \mid f_\infty > 0, \text{ if } A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{Mat}_n(H)\},$$

where H is the division algebra of real quaternions.

Remark 9. We recall the definition of $K_0(A)$ and $K_1(A)$. The abelian group $K_0(A)$ is generated by $[P]$, where P is a finitely generated projective A-module. The relations are 1) $[P] = [Q]$ if $P \cong Q$ and 2) $[P \oplus Q] = [P] + [Q]$. The abelian group $K_1(A)$ is generated by $[P, \alpha]$, where P is a finitely generated projective A-module and $\alpha \in \mathrm{Aut}_A(P)$. The relations are 1) $[P, \alpha] = [Q, \beta]$ if there is a $\gamma : P \cong Q$ such that $\beta = \gamma \circ \alpha \circ \gamma^{-1}$, 2) $[P, \alpha][P, \beta] = [P, \alpha \circ \beta]$ and 3) $[P \oplus Q, \alpha \oplus \beta] = [P, \alpha][Q, \beta]$. Note that one has a map $\mathrm{Aut}_A(P) \to K_1(A)$, which maps $\alpha \mapsto [P, \alpha]$. In particular, one has $\mathrm{Gl}_n(A) \to K_1(A)$, which are compatible for different n, and induce in the limit an isomorphism

(60) $$\mathrm{Gl}(A)/[\mathrm{Gl}(A), \mathrm{Gl}(A)] \cong K_1(A),$$

where $[\mathrm{Gl}(A), \mathrm{Gl}(A)]$ is the commutator subgroup.

6. Exercises

Exercise 1.1 (Motives). Let $E/\mathbb{Q}$ be an elliptic curve and $h_0(E), h_1(E)$ and $h_2(E)$ as in Example 2.

(1) Show that the q_0, q_1 and q_2 in Example 2 are idempotents and that $h(E) = h_0(E) \oplus h_1(E) \oplus h_2(E)$.
(2) Show that $h_0(E) \cong \mathbb{Q}(0)$ and $h_2(E) \cong \mathbb{Q}(1)$.
(3) Show that for $M = h_1(E)$ the i-th realizations M_B, M_{dR} and M_p are zero for $i \neq 1$.
(4) Consider $\mathbb{P}^1/\mathbb{Q}$. Show that $h(\mathbb{P}^1) = \mathbb{Q}(0) \oplus \mathbb{Q}(1)$.

Exercise 1.2 (Determinants). Let A be a ring, $C^\cdot, \widetilde{C}^\cdot$ bounded complexes of modules in $P_{\mathrm{fg}}(A)$.

(1) Show that if $C^\cdot$ is acyclic, then there exists a canonical isomorphism $\mathrm{Det}_A(0) \cong \mathrm{Det}_A(C^\cdot)$.
(2) Use (1) to show that if $\psi : C^\cdot \to \widetilde{C}^\cdot$ is a quasi-isomorphism, then one has a canonical isomorphism $\psi : \mathrm{Det}_A(C^\cdot) \cong \mathrm{Det}_A(\widetilde{C}^\cdot)$ (consider the cone).

(3) Suppose that the cohomology groups of $C^{\cdot}$ are all in $P_{\mathrm{fg}}(A)$. Show that $\mathrm{Det}_A(C^{\cdot}) \cong \prod_{i\in\mathbb{Z}} \mathrm{Det}_A(H^i(C^{\cdot}))$.
(4) Let $A = \mathbb{Z}_p$ and consider the category $L_{\mathrm{gr}}(A)$ of graded line bundles. Its objects are pairs (L, r), where L is a free $\mathbb{Z}_p$-module of rank 1 and $r \in \mathbb{Z}$. Let

$$\mathrm{Mor}((L,r),(L',r')) = \begin{cases} \emptyset & \text{if } r \neq r' \\ \mathrm{Isom}(L,L') & \text{if } r = r'. \end{cases}$$

Show that $V(\mathbb{Z}_p)$ is equivalent to this category.
(5) Consider the inclusion $\mathbb{Z}_p \subset \mathbb{Q}_p$ and define a functor $\mathbb{Q}_p\otimes_{\mathbb{Z}_p} : L_{\mathrm{gr}}(\mathbb{Z}_p) \to L_{\mathrm{gr}}(\mathbb{Q}_p)$ by $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} (L,r) := (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L, r)$. Show that this is compatible with $\mathbb{Q}_p\otimes_{\mathbb{Z}_p} : V(\mathbb{Z}_p) \to V(\mathbb{Q}_p)$ under the above equivalence of categories.
(6) Let $A = \mathbb{Z}_p$ and H be a $\mathbb{Z}_p$-module, which is also a finite group. Show that there exists $\rho : \mathrm{Det}_{\mathbb{Z}_p}(0) \cong \mathrm{Det}_{\mathbb{Z}_p}(H)$, such that $\rho_{\mathbb{Q}_p} : \mathrm{Det}_{\mathbb{Q}_p}(0) \cong \mathrm{Det}_{\mathbb{Q}_p}(H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \mathrm{Det}_{\mathbb{Q}_p}(0)$ equals $(\#H)^{-1} \in \mathbb{Q}_p^{\times}$.

LECTURE 2

Formulation of the ETNC

1. Rationality conjecture

For the rest of these lectures we let $M = (X, q, r) \in \mathcal{M}_{\mathbb{Q}}$ with coefficients in $A/\mathbb{Q}$ finite dimensional and semi-simple. Fix $i \in \mathbb{Z}_{\geq 0}$. We will from now on use systematically notations like $V_{\mathbb{R}} := V \otimes_{\mathbb{Q}} \mathbb{R}$ for $\mathbb{Q}$-vector spaces V, if no confusion is possible. Similarly, we use $V_{\mathbb{Q}_p} := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\mathcal{V}_{\mathbb{Q}_p} := \mathcal{V} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, if $\mathcal{V}$ is a $\mathbb{Z}_p$-module.

In this section we formulate the rationality conjecture, which states essentially that $L(M, 0)^*$ divided by a certain period is "rational".

Recall from Definition 8 the period map

$$\alpha_M : M^+_{B,\mathbb{R}} \to t(M)_{\mathbb{R}}. \tag{61}$$

Conjecture 5. *There exists an exact sequence (the* fundamental exact sequence*) of $A_{\mathbb{R}}$-modules (of finite rank)*

$$\begin{aligned} 0 \to & H^0_{\text{mot}}(\mathbb{Z}, M)_{\mathbb{R}} \xrightarrow{c} \ker\alpha_M \xrightarrow{r^\vee_\infty} H^1_{\text{mot}}(\mathbb{Z}, M^\vee(1))^\vee_{\mathbb{R}} \to \\ \xrightarrow{<,>} & H^1_{\text{mot}}(\mathbb{Z}, M)_{\mathbb{R}} \xrightarrow{r_\infty} \text{coker}\alpha_M \xrightarrow{c^\vee} H^0_{\text{mot}}(\mathbb{Z}, M^\vee(1))^\vee_{\mathbb{R}} \to 0, \end{aligned} \tag{62}$$

where r_∞ is the Beilinson-Deligne regulator, c is the Chern-class map and $<,>$ the height pairing, $(\ )^\vee$ denotes the dual vector space.

Example 14. Let $M = h_1(E)(1)$ and $i = 1$, then Conjecture 5 holds for M. Indeed, α_M is an isomorphism, so that $\ker\alpha_M = 0 = \text{coker}\alpha_M$. By definition $H^0_{\text{mot}}(\mathbb{Z}, M) = 0 = H^0_{\text{mot}}(\mathbb{Z}, M^\vee(1))$. Finally, the Neron-Tate height h defines a pairing $< P, Q >:= \frac{1}{2}(h(P+Q) - h(P) - h(Q))$, which induces an isomorphism

$$<,>: H^1_{\text{mot}}(\mathbb{Z}, M^\vee(1))^\vee_{\mathbb{R}} = E(\mathbb{Q})^\vee_{\mathbb{R}} \cong H^1_{\text{mot}}(\mathbb{Z}, M)_{\mathbb{R}} = E(\mathbb{Q})_{\mathbb{R}}. \tag{63}$$

Definition 16. The *fundamental line* is the object in $V(A)$ defined by

$$\begin{aligned} \triangle(M) := & \text{Det}_A(H^0_{\text{mot}}(\mathbb{Z}, M)) \cdot \text{Det}^{-1}_A(H^1_{\text{mot}}(\mathbb{Z}, M)) \cdot \text{Det}_A(t(M)) \\ & \text{Det}^{-1}_A(H^0_{\text{mot}}(\mathbb{Z}, M^\vee(1))^\vee) \cdot \text{Det}_A(H^1_{\text{mot}}(\mathbb{Z}, M^\vee(1))^\vee) \cdot \text{Det}^{-1}_A(M^+_B). \end{aligned} \tag{64}$$

Taking $\text{Det}_{A_{\mathbb{R}}}$ of the fundamental exact sequence in Conjecture 5 and of the tautological exact sequence

$$0 \to \ker\alpha_M \to M^+_{B,\mathbb{R}} \to t(M)_{\mathbb{R}} \to \text{coker}\alpha_M \to 0 \tag{65}$$

induces a canonical isomorphism

$$\vartheta_\infty : \triangle(M)_{\mathbb{R}} \cong \text{Det}_{A_{\mathbb{R}}}(0). \tag{66}$$

The first part of the ETNC (the rationality conjecture) can now be formulated. We stick here to the case where A is finite dimensional, semi-simple and commutative and explain the general case in Remark 10.

Conjecture 6 (Rationality conjecture). *Let M be as above with coefficients in A and assume that A is commutative. Then $K_1(A) \cong A^\times$ and we can consider $L(M,0)^* \in K_1(A_\mathbb{R}) \cong A_\mathbb{R}^\times$. There exist a* zeta isomorphism

$$\zeta_A(M) : \mathrm{Det}_A(0) \cong \Delta(M) \tag{67}$$

such that

$$\theta_\infty \circ \zeta_A(M)_\mathbb{R} = (L(M,0)^*)^{-1} \in K_1(A_\mathbb{R}) = A_\mathbb{R}^\times. \tag{68}$$

Remark 10. Here we explain the formulation of Conjecture 6 for arbitrary $A/\mathbb{Q}$ finite dimensional and semi-simple. The problem with this case is that $L(M,0)^* \in Z(A_\mathbb{R})^\times$ and that the map $K_1(A_\mathbb{R}) \to Z(A_\mathbb{R})^\times$ induced by the reduced determinant is injective but not surjective in general. It is shown in [**BuFl**] Lemma 9 that there exists a $\lambda \in Z(A)^\times$ such that $(\lambda L(M,0)^*)^{-1} \in K_1(A_\mathbb{R})$. The conjecture now reads as follows: There exists a *zeta isomorphism*

$$\zeta_A(M, \lambda^{-1}) : \mathrm{Det}_A(0) \cong \Delta(M) \tag{69}$$

(depending on λ) such that $\theta_\infty \circ \mathbb{R} \otimes_\mathbb{Q} \zeta_A(M, \lambda^{-1}) = (\lambda L(M,0)^*)^{-1} \in K_1(A_\mathbb{R})$. If one chooses a different $\lambda' \in Z(A)^\times$, then $\lambda'\lambda^{-1} \in K_1(A)$ as follows from the description of the image of the reduced norm in Example 13.

2. Review of some results on elliptic curves

Here we collect some results on elliptic curves $E/\mathbb{Q}$, which we will need in the rest of the lectures.

We assume that E is given by a global minimal Weierstraß equation. We denote by $\widetilde{E}_v$ the reduction of E at a finite place v and by $\widetilde{E}_v^{\mathrm{ns}}$ the set of non-singular points in $\widetilde{E}_v$. Note that this a group scheme over $\mathbb{F}_v$.

Theorem 1 ([**Sil**] VII 2.1, 2.2, 6.1 and IV 6.4). *Let $K = \mathbb{Q}_v$ or $K = \mathbb{Q}_v^{\mathrm{unr}}$), then there are subgroups*

$$E_1(K) \subset E_0(K) \subset E(K) \tag{70}$$

such that $E(K)/E_0(K)$ is finite and one has an exact sequence

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_v^{\mathrm{ns}}(k) \to 0, \tag{71}$$

where $k = \mathbb{F}_v$ or $k = \overline{\mathbb{F}}_v$ is the residue field of K. Moreover, $E_0(K) = E(K)$ if E has good reduction and $E_1(K)$ are the points of the formal group associated to E. In particular, if the valuation w of K is normalized (i.e., $w(K^*) = \mathbb{Z}$), then the logarithm induces an isomorphism $E_1(\mathfrak{m}^r) \cong \mathfrak{m}^r$ for all $r > w(p)/(p-1)$, where $\mathfrak{m}$ is the maximal ideal of K.

Lemma 1. *For $v \neq p$ one has*

$$T_pE^{I_v} \cong T_pE_v^{\mathrm{ns}} \tag{72}$$

and an exact sequence

$$0 \to T_pE^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} T_pE^{I_v} \to \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v) \otimes_\mathbb{Z} \mathbb{Z}_p \to 0. \tag{73}$$

PROOF. Exercise! ☐

Finally, we need to recall Tate's local duality theorem:

Theorem 2 (see [**Mi**] I 3.4). *For any place v of $\mathbb{Q}$ one has a perfect pairing*

$$E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v) \times H^1(\mathbb{Q}_v, E)[p^n] \to \mathbb{Q}_p/\mathbb{Z}_p. \tag{74}$$

3. Local unramified cohomology

We review here the definition of local unramified cohomology, for more details one should consult [**BuFl**] 3.2.

Fix for each place v of $\mathbb{Q}$ an algebraic closure $\overline{\mathbb{Q}}_v$ of $\mathbb{Q}_v$ and and an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_v$. Denote by $G_{\mathbb{Q}_v} := \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$ the absolute Galois group of $\mathbb{Q}_v$. For each continuous $G_{\mathbb{Q}_v}$-module V we let

$$R\Gamma(\mathbb{Q}_v, V) := C^{\cdot}(G_{\mathbb{Q}_v}, V) \tag{75}$$

the complex of continuous cochaines of $G_{\mathbb{Q}_p}$ with values in V. Recall that $D_{\mathrm{cris}}(M_p) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} M_p)^{G_{\mathbb{Q}_p}}$ is equipped with a Frobenius morphism ϕ and that $D_{\mathrm{dR}}(M_p) := (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} M_p)^{G_{\mathbb{Q}_p}}$ has a filtration inherited from B_{dR}.

Definition 17. The p-adic *tangent space* is

$$t(M_p) := D_{\mathrm{dR}}(M_p)/\mathrm{Fil}^0 D_{\mathrm{dR}}(M_p). \tag{76}$$

The comparison isomorphism between M_p and M_{dR} over $\mathbb{Q}_p$ induces an isomorphism

$$t(M_p) \cong t(M)_{\mathbb{Q}_p}. \tag{77}$$

Definition 18. The complex of *local unramified cohomology* is defined as

$$R\Gamma_f(\mathbb{Q}_v, M_p) := \begin{cases} R\Gamma(\mathbb{R}, M_p) & \text{if } v = \infty \\ (M_p^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} M_p^{I_v}) & \text{if } v \neq p, \infty \\ (D_{\mathrm{cris}}(M_p) \xrightarrow{(1-\phi,\mathrm{pr})} D_{\mathrm{cris}}(M_p) \oplus t(M_p)) & \text{if } v = p. \end{cases} \tag{78}$$

Here $I_v \subset G_{\mathbb{Q}_v}$ is the inertia subgroup and the complexes are placed in degree $0, 1$.

The complex $R\Gamma_f(\mathbb{Q}_v, M_p)$ is quasi-isomorphic to a sub-complex $R\Gamma_f(\mathbb{Q}_v, M_p) \subset R\Gamma(\mathbb{Q}_v, M_p)$ (see [**BuFl**] 3.2) and one defines $R\Gamma_{/f}(\mathbb{Q}_v, M_p)$ to be the cokernel, so that one has

$$0 \to R\Gamma_f(\mathbb{Q}_v, M_p) \to R\Gamma(\mathbb{Q}_v, M_p) \to R\Gamma_{/f}(\mathbb{Q}_v, M_p) \to 0. \tag{79}$$

Definition 19. The map induced by the inclusion $t(M_p) \to D_{\mathrm{cris}}(M_p) \oplus t(M_p)$ together with the isomorphism $t(M_p) \cong t(M)_{\mathbb{Q}_p}$

$$\exp_{\mathrm{BK}} : t(M)_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}_p, M_p) \tag{80}$$

is called the *Bloch-Kato exponential map.*

We need the following fact on the exponential map $\exp_{\mathrm{BK}} : t(M)_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}_p, V_pE)$

Theorem 3 ([**BlKa**] Example 3.10.1 and 3.11). *One has* $H^0_f(\mathbb{Q}_p, V_pE) = 0$ *and the diagram*

$$\begin{array}{ccc} E_1(\mathbb{Q}_p)_{\mathbb{Q}_p} & \xrightarrow{\text{Kummer}} & H^1(\mathbb{Q}_p, V_pE) \\ \uparrow{\scriptstyle\exp} & & \uparrow \\ \mathrm{Lie}(E)_{\mathbb{Q}_p} & \xrightarrow{\exp_{\mathrm{BK}}} & H^1_f(\mathbb{Q}_p, V_pE) \end{array} \tag{81}$$

where exp *is the exponential of the formal group* E_1 *commutes. In particular, the Kummer map induces an isomorphism*

$$E(\mathbb{Q}_p)^{\wedge p}_{\mathbb{Q}_p} \cong H^1_f(\mathbb{Q}_p, V_pE). \tag{82}$$

For computation it is decisive to have a version of unramified cohomology with integral coefficients.

Definition 20. Let $T_p \subset M_p$ be a $G_{\mathbb{Q}_v}$-stable $\mathbb{Z}_p$-lattice and let $u : H^1(\mathbb{Q}_v, T_p) \to H^1(\mathbb{Q}_v, M_p)$ be the natural map. Then define

$$\begin{aligned} H^0_f(\mathbb{Q}_v, T_p) &:= H^0(\mathbb{Q}_v, T_p) \\ H^1_f(\mathbb{Q}_v, T_p) &:= \{\xi \in H^1(\mathbb{Q}_v, T_p) \mid u(\xi) \in H^1_f(\mathbb{Q}_v, M_p)\} \\ H^2_f(\mathbb{Q}_v, T_p) &:= 0. \end{aligned} \tag{83}$$

For $H^i_{/f}$ let

$$H^i_{/f}(\mathbb{Q}_v, T_p) := H^i(\mathbb{Q}_v, T_p)/H^i_f(\mathbb{Q}_v, T_p). \tag{84}$$

Note that the torsion subgroups of $H^1_f(\mathbb{Q}_v, T_p)$ and $H^1(\mathbb{Q}_v, T_p)$ coincide.

Theorem 4. *Consider an elliptic curve $E/\mathbb{Q}$ and T_pE and V_pE as defined in Example 3. The Kummer sequence induces for any place v of $\mathbb{Q}$*

$$0 \to E(\mathbb{Q}_v)^{\wedge p} \to H^1(\mathbb{Q}_v, T_pE) \to T_pH^1(\mathbb{Q}_v, E) \to 0, \tag{85}$$

where $E(\mathbb{Q}_v)^{\wedge p} := \varprojlim_n E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v)$ is the p-adic completion and $T_p(\ \ ) :=$ $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p,\ \ )$. Then for all v

$$E(\mathbb{Q}_v)^{\wedge p} \cong H^1_f(\mathbb{Q}_v, T_pE) \tag{86}$$

and $T_pH^1(\mathbb{Q}_v, E) \cong H^1_{/f}(\mathbb{Q}_v, T_pE)$. For all $v \neq \infty$ one has

$$H^0_f(\mathbb{Q}_v, T_pE) = 0. \tag{87}$$

We first prove a lemma.

Lemma 2. *For $v \neq p, \infty$ the map $1 - \mathrm{Frob}_v^{-1}$ induces an isomorphism*

$$V_pE^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} V_pE^{I_v}, \tag{88}$$

so that

$$\begin{aligned} H^0_f(\mathbb{Q}_v, V_pE) &= H^0(\mathbb{Q}_v, V_pE) = 0 \\ H^1_f(\mathbb{Q}_v, V_pE) &= 0. \end{aligned} \tag{89}$$

For $v = p$ we have

$$H^0_f(\mathbb{Q}_v, V_pE) = 0. \tag{90}$$

PROOF. This follows from Lemma 1 and Theorem 3. □

PROOF OF THEOREM 4. We claim that for all places $v \neq \infty$

$$E(\mathbb{Q}_v)^{\wedge p}_{\mathbb{Q}_p} \cong H^1_f(\mathbb{Q}_v, V_pE). \tag{91}$$

For $v = p$ this is contained in Theorem 3. For $v \neq p, \infty$ both sides are zero: the left hand side by the structure of $E(\mathbb{Q}_v)$ recalled in Theorem 1 and the right hand side by Lemma 2. Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q}_v)^{\wedge p} & \longrightarrow & H^1(\mathbb{Q}_v, T_pE) & \longrightarrow & T_pH^1(\mathbb{Q}_v, E) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_v)^{\wedge p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p & \longrightarrow & H^1(\mathbb{Q}_v, V_pE) & \longrightarrow & T_pH^1(\mathbb{Q}_v, E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p & \longrightarrow & 0. \end{array}$$

Here the lower sequence is exact, as $T_pH^1(\mathbb{Q}_v, E)$ is torsion free and hence flat. This also implies that the right vertical arrow is injective. Using our claim, a diagram chase shows that $E(\mathbb{Q}_v)^{\wedge p}$ is identified with the elements in $H^1(\mathbb{Q}_v, T_pE)$, which map to $E(\mathbb{Q}_v)^{\wedge p}_{\mathbb{Q}_p} \cong H^1_f(\mathbb{Q}_v, V_pE)$. This proves the statement of the theorem for $v \neq \infty$. For $v = \infty$ Exercise! □

4. Global unramified cohomology

We need more notation: Fix a prime number p. Denote by S a finite set of places of $\mathbb{Q}$, which contains p, ∞ and the places, for which M_p is ramified. Let G_S be the Galois group of the maximal extension of $\mathbb{Q}$, which is unramified outside of S. For any continuous G_S-module V we let

$$R\Gamma(\mathbb{Z}_S, V) := C^\cdot(G_S, V) \tag{92}$$

be the complex of continuous cochaines of G_S with values in V.

Definition 21. The complex of *cohomology with compact support* is

$$R\Gamma_c(\mathbb{Z}_S, V) := \operatorname{Cone}\left(R\Gamma(\mathbb{Z}_S, V) \to \bigoplus_{v\in S} R\Gamma(\mathbb{Q}_v, V)\right)[-1], \tag{93}$$

where V is any continuous G_S-module. The complex of *global unramified cohomology* is

$$R\Gamma_f(\mathbb{Q}, M_p) := \operatorname{Cone}\left(R\Gamma(\mathbb{Z}_S, M_p) \to \bigoplus_{v\in S} R\Gamma_{/f}(\mathbb{Q}_v, M_p)\right)[-1]. \tag{94}$$

The cohomology groups of $R\Gamma_c(\mathbb{Z}_S, V)$ and $R\Gamma_f(\mathbb{Q}, M_p)$ are denoted by $H^i_c(\mathbb{Z}_S, V)$ and $H^i_f(\mathbb{Q}, M_p)$ respectively.

Putting the resulting exact triangles together one obtains the very important exact triangle

$$R\Gamma_c(\mathbb{Z}_S, M_p) \to R\Gamma_f(\mathbb{Q}, M_p) \to \bigoplus_{v\in S} R\Gamma_f(\mathbb{Q}_v, M_p). \tag{95}$$

The global unramified cohomology $H^i_f(\mathbb{Q}, M_p)$ is self-dual in the following sense:

Theorem 5 ([**BuFl**] Lemma 19). *One has* $H^i_f(\mathbb{Q}, M_p) = 0$ *for* $i \neq 0, 1, 2, 3$ *and*

$$H^i_f(\mathbb{Q}, M_p) \cong H^{3-i}_f(\mathbb{Q}, M_p^\vee(1))^\vee, \tag{96}$$

where $(\quad)^\vee$ *denotes the* $\mathbb{Q}_p$ *dual.*

We introduce an integral structure on $H^1_f(\mathbb{Q}, T_p)$:

Definition 22. Let $T_p \subset M_p$ be a $G_\mathbb{Q}$-stable $\mathbb{Z}_p$-lattice, then define

$$H^1_f(\mathbb{Q}, T_p) := \ker\left(H^1(\mathbb{Q}, T_p) \to \prod_{v\neq\infty} H^1_{/f}(\mathbb{Q}_v, T_p)\right), \tag{97}$$

where $H^1_{/f}(\mathbb{Q}_v, T_p)$ is as in Definition 20.

To compute $H^1_f(\mathbb{Q}, T_pE)$ we need:

Definition 23. Let $E/\mathbb{Q}$ be an elliptic curve, then

$$\text{Ш}(E/\mathbb{Q}) := \ker(H^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, E)) \tag{98}$$

is called the *Shafarevich-Tate group.*

Theorem 6. *Suppose that* $\text{Ш}(\mathbb{Q}, E)$ *is finite, then the Kummer sequence identifies*

$$E(\mathbb{Q})^{\wedge p} \cong H^1_f(\mathbb{Q}, T_pE)$$

inside $H^1(\mathbb{Q}, T_pE)$.

PROOF. Exercise! □

5. Formulation of the ETNC

The following conjecture relates the motivic cohomology to the global unramified cohomology.

Conjecture 7. *The p-adic regulators*

$$\begin{aligned} r_p &: H^0_{\text{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \to H^0_f(\mathbb{Q}, M_p) \\ r_p &: H^1_{\text{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}, M_p) \end{aligned} \tag{99}$$

are isomorphisms for all p.

We are going to define an isomorphism $\theta_p : \Delta(M)_{\mathbb{Q}_p} \cong \text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p))$. By definition of $R\Gamma_f(\mathbb{Q}_v, M_p)$ (see Definition 18), we can identify

$$\iota_v : \text{Det}^{-1}_{A_{\mathbb{Q}_p}} R\Gamma_f(\mathbb{Q}_v, M_p) := \begin{cases} \text{Det}^{-1}_{A_{\mathbb{Q}_p}} M_p^+ & \text{if } v = \infty \\ \text{Det}_{A_{\mathbb{Q}_p}}(0) = & \text{if } v \neq p, \infty \\ \text{Det}_{A_{\mathbb{Q}_p}} t(M)_{\mathbb{Q}_p} & \text{if } v = p. \end{cases} \tag{100}$$

The triangle for $R\Gamma_c(\mathbb{Z}_S, M_p)$ in (95) gives

$$\text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p)) \cong \text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_f(\mathbb{Q}, M_p)) \cdot \prod_{v \in S} \text{Det}^{-1}_{A_{\mathbb{Q}_p}}(R\Gamma_f(\mathbb{Q}_v, M_p)). \tag{101}$$

Together with the isomorphism ι_v in (100) one gets

$$\text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p)) \cong \text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_f(\mathbb{Q}, M_p)) \cdot \text{Det}^{-1}_{A_{\mathbb{Q}_p}}(M_p^+) \cdot \text{Det}_{A_{\mathbb{Q}_p}}(t(M)_{\mathbb{Q}_p}). \tag{102}$$

With Conjecture 7 and Theorem 5 the right hand side is canonically isomorphic to $\Delta(M)_{\mathbb{Q}_p}$.

Definition 24. For any p let

$$\theta_p : \Delta(M)_{\mathbb{Q}_p} \cong \text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p)) \tag{103}$$

be the isomorphism defined above.

The ETNC states roughly that the zeta element $\zeta_A(M)$ from Definition 6 generates an integral structure in $\text{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p))$. To formulate this, we need:

Definition 25. Let $A/\mathbb{Q}$ be finite dimensional, semi-simple. An *order* $\mathcal{A}$ in A is a sub-algebra, which is a finitely generated $\mathbb{Z}$-module, such that $\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q} = A$. A *projective* $\mathcal{A}$*-structure* in M, is a projective $\mathcal{A}$-module $T_B \subset M_B$ such that for all p the image of $T_p := T_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ under the comparison isomorphism

$$M_B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_p \tag{104}$$

is a Galois stable lattice in M_p.

Very important examples of orders are $\mathbb{Z}[G] \subset \mathbb{Q}[G]$, where G is a finite group.

Conjecture 8 (ETNC equivariant Tamagawa number conjecture). *Let $M \in \mathcal{M}_{\mathbb{Q}}$ be a motive with coefficients in A and suppose that A is commutative (see Remark 13 below for the general case). Let T_B be a projective $\mathcal{A}$-structure in M and let $\zeta_A(M) : \mathrm{Det}_A(0) \cong \triangle(M)$ be the zeta element defined in Conjecture 6. Then there is an isomorphism $\zeta_{\mathcal{A}_{\mathbb{Z}_p}} : \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(0) \cong \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(R\Gamma_c(\mathbb{Z}_S, T_p))$ such that*

$$\theta_p \circ \zeta_A(M)_{\mathbb{Q}_p} : \mathrm{Det}_{A_{\mathbb{Q}_p}}(0) \cong \triangle(M)_{\mathbb{Q}_p} \cong \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p)) \tag{105}$$

coincides with $(\zeta_{\mathcal{A}_{\mathbb{Z}_p}})_{\mathbb{Q}_p}$.

Remark 11. The ETNC is independent of the choice of the projective $\mathcal{A}$-structure T_B. Indeed, for a different $\mathcal{A}$-structure T'_B we can consider $p^n T_p \subset T_p \cap T'_p$ and so reduce to the case of $T_p \subset T'_p$. We get an exact triangle

$$R\Gamma_c(\mathbb{Z}_S, T_p) \to R\Gamma_c(\mathbb{Z}_S, T'_p) \to R\Gamma_c(\mathbb{Z}_S, T'_p/T_p), \tag{106}$$

where T'_p/T_p is finite. By Example 12 the isomorphisms $\zeta_{\mathcal{A}_{\mathbb{Z}_p}}$ for $R\Gamma_c(\mathbb{Z}_S, T_p)$ and $R\Gamma_c(\mathbb{Z}_S, T'_p)$ differ by $\prod_{i=0,1,2,3}(\#H^i_c(\mathbb{Z}_S, T'_p/T_p))^{(-1)^i} = 1$, (see **[Fl]** Theorem 5.1).

Remark 12. The ETNC is also independent of the choice of S in the sense that if it holds for S, then it also holds for a different set of places S'. We may assume $S \subset S'$. Then there is an exact triangle

$$R\Gamma_c(\mathbb{Z}_S, T_p) \to R\Gamma_c(\mathbb{Z}_{S'}, T_p) \to \bigoplus_{v \in S' \setminus S} R\Gamma(\mathbb{F}_v, T_p^{I_v}). \tag{107}$$

The complex $R\Gamma(\mathbb{F}_v, T_p^{I_v})$ can be represented by $[T_p^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} T_p^{I_v}]$ and one gets $\mathrm{triv} : \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(0) \cong \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(R\Gamma(\mathbb{F}_v, T_p^{I_v}))$. This means that for $\theta_{p,S} : \triangle(M)_{\mathbb{Q}_p} \cong \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p))$ and $\theta_{p,S'} : \triangle(M)_{\mathbb{Q}_p} \cong \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_{S'}, M_p))$ one has $\theta_{p,S} \cdot \mathrm{triv}_{\mathbb{Q}_p} = \theta_{p,S'}$. With a similar notation $\zeta_{\mathcal{A}_{\mathbb{Z}_p},S} \cdot \mathrm{triv} = \zeta_{\mathcal{A}_{\mathbb{Z}_p},S'}$. Putting this together, gives the result.

Remark 13. To formulate the ETNC for a general finite dimensional, semi-simple A recall the zeta isomorphism $\zeta_A(M, \lambda^{-1}) : \mathrm{Det}_A(0) \cong \triangle(M)$ from Remark 10. As the reduced norm induces an isomorphism $\mathrm{normred}_{A_{\mathbb{Q}_p}} : K_1(A_{\mathbb{Q}_p}) \cong (Z(A_{\mathbb{Q}_p}))^\times$ we can consider

$$\lambda\zeta_A(M, \lambda^{-1})_{\mathbb{Q}_p} : \mathrm{Det}_{A_{\mathbb{Q}_p}}(0) \cong \triangle(M)_{\mathbb{Q}_p}, \tag{108}$$

which is independent of λ. The ETNC says in this case, that there is an isomorphism $\zeta_{\mathcal{A}_{\mathbb{Z}_p}} : \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(0) \cong \mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(R\Gamma_c(\mathbb{Z}_S, T_p))$ such that

$$\theta_p \circ \lambda\zeta_A(M, \lambda^{-1})_{\mathbb{Q}_p} : \mathrm{Det}_{A_{\mathbb{Q}_p}}(0) \cong \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p)) \tag{109}$$

coincides with $(\zeta_{\mathcal{A}_{\mathbb{Z}_p}})_{\mathbb{Q}_p}$.

6. Exercises

Exercise 2.3. Show that for any abelian group H, the group $T_pH := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p, H)$ is torsion free and that $T_pH = 0$ for finite H.

Exercise 2.4. Show Lemma 1.

Exercise 2.5. Show Theorem 4 for $v = \infty$, i.e., that $E(\mathbb{R})^{\wedge p} \cong H^1(\mathbb{R}, T_pE)$.

Exercise 2.6. Show Theorem 6.

LECTURE 3

The ETNC and the Birch-Swinnerton-Dyer conjecture

1. Relation to the Birch-Swinnerton-Dyer conjecture

In the last lecture we want to show that the ETNC for the motive $h_1(E)(1)$ is essentially equivalent to the Birch and Swinnerton-Dyer conjecture.

In this section, we consider again an elliptic curve $E/\mathbb{Q}$ and let $M = h_1(E)(1)$. We denote by $r := \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q})$. Choose a basis $\underline{x} := (x_1, \ldots, x_r)$ of the free part $E(\mathbb{Q})^{\mathrm{free}}$ of $E(\mathbb{Q})$ and let $<,>$ be the Neron-Tate height pairing as defined in Example 14.

Definition 26. The *regulator* of E is the real number

$$R(E/\mathbb{Q}) := \det(< x_i, x_j >)_{i,j=1,\ldots,r}. \tag{110}$$

Definition 27. Let

$$c_v := \begin{cases} \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)) & \text{if } v \neq \infty \\ \#(E(\mathbb{R})/E(\mathbb{R})^0) & \text{if } v = \infty, \end{cases} \tag{111}$$

where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ defined in Theorem 1 and $E(\mathbb{R})^0$ is the connected component of $E(\mathbb{R})$.

Note that $c_v = 1$ for almost all v. One can show that for finite v one has $c_v = \#(\mathcal{E}(\mathbb{F}_v)/\mathcal{E}^0(\mathbb{F}_v))$ where $\mathcal{E}$ is the Neron model of E and $\mathcal{E}^0 \subset \mathcal{E}$ is the connected component of the identity.

Conjecture 9 (Birch-Swinnerton-Dyer conjecture (BSD)). *Let $E/\mathbb{Q}$ be an elliptic curve, $r := \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q})$, then:*

a) $\mathrm{ord}_{s=1} L(E, s) = r$

b) *If $Ш(E/\mathbb{Q})$ is finite, then*

$$\frac{L(E,1)^*}{\Omega_\infty R(E/\mathbb{Q})} = \frac{\#Ш(E/\mathbb{Q})}{(E(\mathbb{Q})_{\mathrm{tors}})^2} \prod_v c_v, \tag{112}$$

where Ω_∞ is the period of E from Example 4.

We can now formulate the main theorem of these lectures:

Theorem 7 (Main theorem). *Let $E/\mathbb{Q}$ be an elliptic curve, $M = h_1(E)(1)$ $(i = 1)$ and $A = \mathbb{Q}$.*

(1) *The conjecture of the order of vanishing of $L(E, s)$ at $s = 1$ is equivalent to part a) of the BSD conjecture.*

(2) *If 1) holds, Conjecture 6 is equivalent to*

$$\frac{L(E,1)^*}{\Omega_\infty R(E/\mathbb{Q})} \in \mathbb{Q}^\times.$$

(3) *If* $Ш(E/\mathbb{Q})$ *is finite and Conjecture 2 on local L-factors holds even for* $v = p$*, then the ETNC for* M *and all* p *is equivalent to part b) of the BSD conjecture.*

We prove here (1) and (2). Part (3) will be proven in Section 4.

PROOF OF (1) AND (2). Obviously, using Example 6, Conjecture 4 says for $M = h_1(E)(1)$ that

$$r = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=0} L(M, s), \tag{113}$$

if we observe that $L(M, s) = L(E, s+1)$. This proves (1).

We show that Conjecture 6 is equivalent to

$$\frac{L(M,0)^*}{\Omega_\infty R(E/\mathbb{Q})} \in \mathbb{Q}^\times. \tag{114}$$

Indeed, the fundamental line of M is

$$\triangle(M) = \mathrm{Det}_{\mathbb{Q}}^{-1}(E(\mathbb{Q})_{\mathbb{Q}}) \cdot \mathrm{Det}_{\mathbb{Q}}(E(\mathbb{Q})_{\mathbb{Q}})^\vee \cdot \mathrm{Det}_{\mathbb{Q}}^{-1} M_B^+ \cdot \mathrm{Det}_{\mathbb{Q}}(\mathrm{Lie} E). \tag{115}$$

Let $\underline{x}^\vee := (x_1^\vee, \ldots, x_r^\vee)$ be the basis of $(E(\mathbb{Q})^{\mathrm{free}})^\vee$ dual to $\underline{x} := (x_1, \ldots, x_r)$ and let $\mathrm{cl}_{E(\mathbb{R})^0}$ and $\omega^\vee$ be the basis elements of M_B^+ and $\mathrm{Lie}E$ respectively, defined in Example 3. We have isomorphisms $\underline{x} : \mathrm{Det}_{\mathbb{Q}}(\mathbb{Q}^r) \cong \mathrm{Det}_{\mathbb{Q}}(E(\mathbb{Q})^{\mathrm{free}})$ etc. induced by these bases and we define β to be the composite isomorphism

$$\beta : \mathrm{Det}_{\mathbb{Q}}(0) \cong Det_{\mathbb{Q}}^{-1}(\mathbb{Q}^r) \cdot \mathrm{Det}_{\mathbb{Q}}(\mathbb{Q}^r) \cdot \mathrm{Det}_{\mathbb{Q}}^{-1}(\mathbb{Q}) \cdot \mathrm{Det}_{\mathbb{Q}}(\mathbb{Q}) \cong \triangle(M) \tag{116}$$

induced by these bases. As a possible zeta isomorphism $\zeta_{\mathbb{Q}}(M)$ is of the form $\zeta_{\mathbb{Q}}(M) = q\beta$, with $q \in \mathbb{Q}^\times$, Conjecture 6 is now equivalent to the fact that

$$q\theta_\infty \circ \beta_{\mathbb{R}} = (L(M,0)^*)^{-1} \in K_1(\mathbb{R}) = \mathbb{R}^\times. \tag{117}$$

By definition of θ_∞ we get that

$$\theta_\infty \circ \beta_{\mathbb{R}} = (\Omega_\infty R(E/\mathbb{Q}))^{-1} \in K_1(\mathbb{R}) = \mathbb{R}^\times. \tag{118}$$

Thus

$$\frac{L(M,0)^*}{\Omega_\infty R(E/\mathbb{Q})} = q^{-1} \in \mathbb{Q}^\times. \tag{119}$$

□

2. Selmer group and $R\Gamma_c(\mathbb{Z}_S, T_pE)$

In this section, $E/\mathbb{Q}$ is an elliptic curve and T_pE is the Tate-module of E.

Definition 28. Fix a prime number p. The *Selmer group* of $E/\mathbb{Q}$ is defined as

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E[p^\infty]) \to \prod_v H^1(\mathbb{Q}_v, E)[p^\infty]) \right). \tag{120}$$

Note that one has an exact sequence

$$0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0. \tag{121}$$

Definition 29. For any topologically abelian H, we let $H^* := \mathrm{Hom}_{\mathrm{cont}}(H, \mathbb{Q}_p/\mathbb{Z}_p)$, where $\mathbb{Q}_p/\mathbb{Z}_p$ has the discrete topology.

Note that by (95) and Lemma 2, we can write

(122)

$$\mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_c(\mathbb{Z}_S, V_pE)) \cong \mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_f(\mathbb{Q}, V_pE)) \cdot \mathrm{Det}_{\mathbb{Q}_p}(H^1_f(\mathbb{Q}_p, V_pE)) \cdot \mathrm{Det}^{-1}_{\mathbb{Q}_p} V_pE^+.$$

Theorem 8. *There is a canonical isomorphism*

$$\begin{aligned}(123)\quad \mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)) \cong \mathrm{Det}^{-1}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}, T_pE)) \cdot \mathrm{Det}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^*)\cdot \\ \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(H^0(\mathbb{Z}_S, E[p^\infty])^*) \cdot \prod_{v\in S} \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}) \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(T_pE^+),\end{aligned}$$

which induces after $\mathbb{Q}_p \otimes_{\mathbb{Z}_p}$ *the isomorphism in* (122).

Proof. The Poitou-Tate sequence (see **[NSW]** (8.6.10)) gives for each integer $n \geq 1$ a long exact sequence of finite groups

$$\begin{aligned} H^1(\mathbb{Z}_S, E[p^n]) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, E[p^n]) \to H^1(\mathbb{Z}_S, E[p^n])^* \to \\ H^2(\mathbb{Z}_S, E[p^n]) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, E[p^n]) \to H^0(\mathbb{Z}_S, E[p^n])^* \to 0.\end{aligned}$$

Here we have identified $E[p^n] \cong \mathrm{Hom}(E[p^n], \mu_{p^n})$ via the Weil pairing. As the groups in this sequence are finite, taking $\varprojlim_n$ is exact. We get

$$\begin{aligned} H^1(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, T_pE) \to H^1(\mathbb{Z}_S, E[p^\infty])^* \to \\ H^2(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, T_pE) \to H^0(\mathbb{Z}_S, E[p^\infty])^* \to 0.\end{aligned}$$

By Definition 22, the kernel of the first map is $H^1_f(\mathbb{Q}, T_pE)$. Taking the inverse limit of the Tate duality pairing in Theorem 2 one gets $E(\mathbb{Q}_v)^{\wedge p} \cong H^1(\mathbb{Q}_v, E)[p^\infty]^*$ and a commutative diagram

(124)

$$\begin{array}{ccc} \bigoplus_{v\in S} E(\mathbb{Q}_v)^{\wedge p} & \xrightarrow{\cong} & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, E)[p^\infty]^* \\ \downarrow & & \downarrow \\ \bigoplus_{v\in S} H^1(\mathbb{Q}_v, T_pE) & \longrightarrow & H^1(\mathbb{Z}_S, E[p^\infty])^* \\ \downarrow & & \downarrow \\ \bigoplus_{v\in S} T_pH^1(\mathbb{Q}_v, E) & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^* \\ \downarrow & & \downarrow \\ 0 & & 0. \end{array}$$

Thus, if we factor out the isomorphism $E(\mathbb{Q}_v)^{\wedge p} \cong H^1(\mathbb{Q}_v, E)[p^\infty]^*$ we get a long exact sequence

(125)

$$\begin{aligned} 0 \to & H^1_f(\mathbb{Q}, T_pE) \to H^1(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} T_pH^1(\mathbb{Q}_v, E) \to \\ \to & \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^* \to H^2(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, T_pE) \to \\ \to & H^0(\mathbb{Z}_S, E[p^\infty])^* \to 0.\end{aligned}$$

On the other hand we have by Definition 21 a long exact sequence for $R\Gamma_c(\mathbb{Z}_S, T_pE)$ (note that $H^0_c(\mathbb{Z}_S, T_pE) = H^0(\mathbb{Z}_S, T_pE) = 0$ and $H^0(\mathbb{Q}_v, T_pE) = 0$ for v finite)

$$\begin{aligned} 0 \to H^0(\mathbb{R}, T_pE) \to & H^1_c(\mathbb{Z}_S, T_pE) \to H^1(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, T_pE) \to \\ & \to H^2_c(\mathbb{Z}_S, T_pE) \to H^2(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, T_pE) \to \\ & \to H^3_c(\mathbb{Z}_S, T_pE) \to 0. \end{aligned} \tag{126}$$

Taking $\mathrm{Det}_{\mathbb{Z}_p}$ of these two exact sequences gives the desired result. □

3. Local Tamagawa numbers

In this section we study how the integral structure $E(\mathbb{Q}_v)^{\wedge p}$ behaves under the identification 100

$$\iota_v : \mathrm{Det}^{-1}_{\mathbb{Q}_p} R\Gamma_f(\mathbb{Q}_v, V_pE) \cong \begin{cases} \mathrm{Det}_{\mathbb{Q}_p}(0) & \text{if } v \neq p, \infty \\ \mathrm{Det}_{\mathbb{Q}_p} \mathrm{Lie}(E)_{\mathbb{Q}_p} & \text{if } v = p. \end{cases} \tag{127}$$

Recall that by Theorem 4

$$\mathrm{Det}^{-1}_{\mathbb{Z}_p}(R\Gamma_f(\mathbb{Q}_v, T_pE)) \cong \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}). \tag{128}$$

Let

$$\rho_v : \mathrm{Det}_{\mathbb{Z}_p}(0) \cong \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}) \tag{129}$$

for $v \neq p$ the isomorphism defined in Example 12. For the group $E(\mathbb{Q}_p)^{\wedge p}$ we get

$$\mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p}) \cong \mathrm{Det}_{\mathbb{Z}_p}(E_1(\mathbb{Q}_p)^{\wedge p}) \cdot \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p}/E_1(\mathbb{Q}_p)^{\wedge p}). \tag{130}$$

The isomorphism $\exp : p\omega^\vee \mathbb{Z}_p \cong E_1(\mathbb{Q}_p)^{\wedge p}$ gives a basis $\exp(p\omega^\vee)$ for $E_1(\mathbb{Q}_p)^{\wedge p}$ and together with Example 12 we get

$$\widetilde{\rho}_p : \mathrm{Det}_{\mathbb{Z}_p}(\mathbb{Z}_p) \cong \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p}). \tag{131}$$

We define

$$\rho_p = \frac{\#\widetilde{E}^{\mathrm{ns}}_p(\mathbb{F}_p) \otimes_{\mathbb{Z}} \mathbb{Z}_p}{\#\widetilde{E}^{\mathrm{ns}}_p(\mathbb{F}_p)} \widetilde{\rho}_p : \mathrm{Det}_{\mathbb{Z}_p}(\mathbb{Z}_p) \cong \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p}). \tag{132}$$

Denote for each number $q \in \mathbb{Q}_p^\times$ by

$$[q]_p := p^{w(q)} \text{ the } p\text{-part of } q. \tag{133}$$

Here w is the p-adic valuation.

Theorem 9. *Let for $v = p$*

$$\omega^\vee_{\mathbb{Q}_p} : \mathrm{Det}_{\mathbb{Q}_p}(\mathbb{Q}_p) \cong \mathrm{Det}_{\mathbb{Q}_p}(\mathrm{Lie}E_{\mathbb{Q}_p}) \tag{134}$$

induced by the basis element $\omega^\vee$. Then

$$\iota_v \circ (\rho_v)_{\mathbb{Q}_p} = \begin{cases} [c_v]_p^{-1} \in \mathbb{Q}_p^\times & \text{if } v \neq p, \infty \\ [c_p]_p^{-1} \omega^\vee_{\mathbb{Q}_p} & \text{if } v = p. \end{cases} \tag{135}$$

PROOF. We treat first the case $v \neq p$. Recall from Lemma 1 the exact sequence

$$0 \to T_pE^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} T_pE^{I_v} \to \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to 0. \tag{136}$$

As $E_1(\mathbb{Q}_v)^{\wedge p} = 0$, we have $E_0(\mathbb{Q}_v)^{\wedge p} \cong \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. This gives

(137)

$$\rho_v : \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}) \cong \mathrm{Det}_{\mathbb{Z}_p}^{-1}(T_pE^{I_v}) \cdot \mathrm{Det}_{\mathbb{Z}_p}(T_pE^{I_v}) \cdot \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}/E_0(\mathbb{Q}_v)^{\wedge p}).$$

As $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pE^{I_v} = V_pE^{I_v}$ it follows from the definition of ι_v and Example 12 that $\iota_v \circ (\rho_v)_{\mathbb{Q}_p} = [c_v]_p^{-1}$ because $[c_v]_p = \#(E(\mathbb{Q}_v)^{\wedge p}/E_0(\mathbb{Q}_v)^{\wedge p})$.

Consider now $v = p$ and recall the exponential map $\exp_{\mathrm{BK}} : \mathrm{Lie}E_{\mathbb{Q}_p} \cong H^1_f(\mathbb{Q}_p, V_pE)$ from Definition 19. We claim that for the induced isomorphism

$$\exp_{\mathrm{BK}}^{-1} : \mathrm{Det}_{\mathbb{Q}_p} H^1_f(\mathbb{Q}_p, V_pE) \cong \mathrm{Det}_{\mathbb{Q}_p} \mathrm{Lie}E_{\mathbb{Q}_p} \tag{138}$$

we have

$$\iota_p = \det(1-\phi)\exp_{\mathrm{BK}}^{-1}. \tag{139}$$

Indeed, consider the complex

$$R\Gamma_f(\mathbb{Q}_p, V_pE) = [D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi,\mathrm{pr})} D_{\mathrm{cris}}(V_pE) \oplus \mathrm{Lie}E_{\mathbb{Q}_p}]. \tag{140}$$

We get

(141)

$$\mathrm{Det}_{\mathbb{Q}_p}(\mathrm{Lie}E_{\mathbb{Q}_p}) \cdot \mathrm{Det}_{\mathbb{Q}_p}^{-1}[D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi)} D_{\mathrm{cris}}(V_pE)] \cong \mathrm{Det}_{\mathbb{Q}_p}^{-1}(R\Gamma_f(\mathbb{Q}_p, V_pE)).$$

The quasi-isomorphism $\exp_{\mathrm{BK}} : \mathrm{Lie}E_{\mathbb{Q}_p}[-1] \cong R\Gamma_f(\mathbb{Q}_p, V_pE)$ is induced by the embedding of the sub-complex $[0 \to \mathrm{Lie}E_{\mathbb{Q}_p}]$. The quotient is the acyclic complex $[D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi)} D_{\mathrm{cris}}(V_pE)]$. The isomorphism ι_p is obtained by using

$$\begin{aligned}\mathrm{triv} : \mathrm{Det}_{\mathbb{Q}_p}^{-1}[D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi)} D_{\mathrm{cris}}(V_pE)] &= \\ = \mathrm{Det}_{\mathbb{Q}_p}^{-1}(D_{\mathrm{cris}}(V_pE)) \cdot \mathrm{Det}_{\mathbb{Q}_p}(D_{\mathrm{cris}}(V_pE)) &= \mathrm{Det}_{\mathbb{Q}_p}(0)\end{aligned} \tag{142}$$

and the isomorphism $\exp_{\mathrm{BK}}^{-1}$ by using that

$$\mathrm{acyclic} : \mathrm{Det}_{\mathbb{Q}_p}^{-1}[D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi)} D_{\mathrm{cris}}(V_pE)] \cong \mathrm{Det}_{\mathbb{Q}_p}(0) \tag{143}$$

is an acyclic complex. As $\mathrm{triv} \circ \mathrm{acyclic}^{-1} = \det(1-\phi)$ the claim follows.

Now by using Theorem 3, the map $\exp_{\mathrm{BK}}$ is given by the exponential map from $\exp : \mathrm{Lie}E_{\mathbb{Q}_p} \to E_1(\mathbb{Q}_p)$ and by our choice of basis $\omega^\vee \in \mathrm{Lie}E$ one gets an isomorphism $\exp : p\omega^\vee\mathbb{Z}_p \cong E_1(\mathbb{Q}_p)$. By definition of $\widetilde{\rho}_p$ in (131) the isomorphism

$$\exp_{\mathrm{BK}}^{-1} \circ (\widetilde{\rho}_p)_{\mathbb{Q}_p} : \mathrm{Det}_{\mathbb{Q}_p}(\mathbb{Q}_p) \cong \mathrm{Det}_{\mathbb{Q}_p}(\mathrm{Lie}E_{\mathbb{Q}_p}) \tag{144}$$

equals

$$\#(E(\mathbb{Q}_p)^{\wedge p}/E_1(\mathbb{Q}_p)^{\wedge p})^{-1} p\omega_{\mathbb{Q}_p}^\vee = [c_p]_p^{-1}\#(\widetilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p) \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{-1} p\omega_{\mathbb{Q}_p}^\vee. \tag{145}$$

As $\det(1-\phi) = \frac{\#\widetilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)}{p}$ we have

$$\iota_p \circ (\widetilde{\rho}_p)_{\mathbb{Q}_p} = \frac{\#\widetilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)}{p} \exp_{\mathrm{BK}}^{-1} \circ (\widetilde{\rho}_p)_{\mathbb{Q}_p} \tag{146}$$

and by definition of ρ_p in (132) we get $\iota_p \circ (\rho_p)_{\mathbb{Q}_p} = [c_p]_p^{-1}\omega_{\mathbb{Q}_p}^\vee$. □

4. Proof of the Main Theorem

Here we prove part (3) of the Main Theorem 7.

PROOF OF (3) OF THEOREM 7. Using Theorem 8, we are going to define an isomorphism

$$\zeta_{\mathbb{Z}_p} : \mathrm{Det}_{\mathbb{Z}_p}(0) \cong \mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)). \tag{147}$$

By Theorem 6 we have $H^1_f(\mathbb{Q}, T_pE) \cong E(\mathbb{Q})^{\wedge p} \cong E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. This gives

$$\mathrm{Det}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}, T_pE)) \cong \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q})^{\mathrm{free}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cdot \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q})_{\mathrm{tors}} \otimes_{\mathbb{Z}} \mathbb{Z}_p). \tag{148}$$

The basis $x_1, \ldots, x_r$ and Example 12 induce an isomorphism

$$\mathrm{Det}_{\mathbb{Z}_p}(\mathbb{Z}_p^r) \cong \mathrm{Det}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}, T_pE)). \tag{149}$$

Taking the dual of the sequence in (121), one gets

$$0 \to Ш(E/\mathbb{Q})[p^\infty]^* \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^* \to (E(\mathbb{Q})^{\mathrm{free}})^\vee \otimes_{\mathbb{Z}} \mathbb{Z}_p \to 0. \tag{150}$$

This gives

$$\mathrm{Det}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^*) \cong \mathrm{Det}_{\mathbb{Z}_p}(Ш(E/\mathbb{Q})[p^\infty]^*) \cdot \mathrm{Det}_{\mathbb{Z}_p}((E(\mathbb{Q})^{\mathrm{free}})^\vee \otimes_{\mathbb{Z}} \mathbb{Z}_p) \tag{151}$$

and assuming that $Ш(E/\mathbb{Q})$ is finite, the basis $x_1^\vee, \ldots, x_r^\vee$ and Example 12 give

$$\mathrm{Det}_{\mathbb{Z}_p}(\mathbb{Z}_p^r) \cong \mathrm{Det}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^*). \tag{152}$$

For T_pE^+ we use the basis $\mathrm{cl}_{E(\mathbb{R})^0}$ of $H_1(E(\mathbb{C}), \mathbb{Z})^+$ and the comparison isomorphism $H_1(E(\mathbb{C}), \mathbb{Z})^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong T_pE^+$ to define

$$\mathrm{Det}^{-1}_{\mathbb{Z}_p}(\mathbb{Z}_p) \cong \mathrm{Det}_{\mathbb{Z}_p}(T_pE^+). \tag{153}$$

Finally, $H^0(\mathbb{Z}_S, E[p^\infty])^*$ is finite and for $\prod_{v\in S, v\neq p} E(\mathbb{Q}_v)^{\wedge p}$ we use the ρ_v defined in (129) and (132). Combining these isomorphisms we get

$$\zeta_{\mathbb{Z}_p} : \mathrm{Det}_{\mathbb{Z}_p}(0) \cong \mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)). \tag{154}$$

Recall from (116) the definition of the zeta isomorphism

$$\zeta_{\mathbb{Q}}(M) = q\beta : \mathrm{Det}_{\mathbb{Q}}(0) \cong \Delta(M). \tag{155}$$

The definition of $\theta_p : \Delta(M)_{\mathbb{Q}_p} \cong \mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_c(\mathbb{Z}_S, V_pE))$ involves the maps r_p : $H^1_{\mathrm{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \cong E(\mathbb{Q})_{\mathbb{Q}_p}$, ι_v and the comparison isomorphism $M_B^+ \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong V_pE^+$. By definition of $\zeta_{\mathbb{Z}_p}$ and using Theorem 9 one gets that $\theta_p \circ \zeta_{\mathbb{Q}}(M)_{\mathbb{Q}_p}$ equals

$$\left(q^{-1} \frac{(\#E(\mathbb{Q})^{\wedge p}_{\mathrm{tors}}))^2}{\#(Ш(E/\mathbb{Q})[p^\infty])} \prod_v [c_v]_p^{-1} \right) \zeta_{\mathbb{Q}_p}. \tag{156}$$

This implies that the ETNC for $M = h_1(E)(1)$ holds if and only if

$$[q^{-1}]_p = \frac{\#(Ш(E/\mathbb{Q})[p^\infty])}{(\#E(\mathbb{Q})^{\wedge p}_{\mathrm{tors}}))^2} \prod_v [c_v]_p \tag{157}$$

for all p, that is if and only if the BSD conjecture holds. □

5. exercise

Exercise 3.7. Fill in the details in the poof of Theorem 7 (3).

Bibliography

[BlKa] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives. The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math., 86, Birkhuser Boston, Boston, MA, 1990.

[BuFl] D. Burns and M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients. Documenta Math. 6 (2001) 501-570.

[CuRe] C. W. Curtis and I. Reiner, Methods of representation theory. Vol. II. With applications to finite groups and orders. Pure and Applied Mathematics (New York). A Wiley-Interscience Publication, 1987

[Fl] M. Flach, Euler characteristics in relative K-groups, Bull. London Math. Soc. 32 (2000) 272-284.

[Fo] J-M. Fontaine, Valeurs spéciales des fonctions L de motifs, Séminaire Bourbaki, Exposé 751, Asterisque 206 (1992)

[FoPe] J-M. Fontaine and B. Perrin-Riou, Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L, In: Motives, PSPM vol. 55 I (1994) 599-706

[FuKa] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory. Proceedings of the St. Petersburg Mathematical Society. Vol. XII, 1–85, Amer. Math. Soc. Transl. Ser. 2, 219, Amer. Math. Soc., Providence, RI, 2006.

[HuKi] A. Huber and G. Kings, Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture. Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 149–162.

[Ja] U. Jannsen, Motives, numerical equivalence and semi-simplicity, Invent. math. 107 (1992) 447-452.

[Ka] K. Kato, Iwasawa theory and p-adic Hodge-theory, Kodai Math. J. 16 (1993), 1-31.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields. 2nd Edition, Springer 2008.

[Mi] J. S. Milne, Arithmetic duality theorems, Academic Press (1986)

[Scho1] A. J. Scholl, Classical motives, In: Motives, PSPM vol. 55 I (1994) 163-187.

[Scho2] A. J. Scholl, Integral elements in K-theory and products of modular curves. The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), 467–489

[Schn] P. Schneider, Introduction to the Beilinson conjectures, In: Beilinson's conjectures on special values of L-functions, Academic Press (1988).

[Si1] J. H. Silverman, The arithmetic of elliptic curves, Springer (1986)

[Si2] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer (1994)

[Ve] O. Venjakob,From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture—a survey. L-functions and Galois representations, 333–380, London Math. Soc. Lecture Note Ser., 320, Cambridge Univ. Press, Cambridge, 2007.