Universität Regensburg
Mathematik

An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture

Guido Kings

Preprint Nr. 26/2009

Contents

An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture

Guido Kings

IAS/Park City Mathematics Series
Volume XX, XXXX

An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture

Guido Kings

Introduction

The equivariant Tamagawa number conjecture (ETNC) can be seen as a vast generalization of the analytic class number formula for number fields or of the Birch-Swinnerton-Dyer conjecture (BSD) to all motives. 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 [**BK**].

In this sense, it might be a useful approach for a general introduction to the ETNC to treat the BSD conjecture as a special example. It is very instructive (and a kind of small wonder) to see how all the different factors occurring in the BSD conjecture have a cohomological interpretation.

To treat just the equivalence of ETNC with the BSD conjecture, one could confine oneself with a very modest formulation of the ETNC, in fact, as no coefficients are needed, one could do with just formulating the TNC. The idea of the current lecture at the PCMI 2009 Graduate Summer School was, however, also to show how the ETNC unifies different conjectures about special values of L-functions, most notably the Stark conjecture and its equivariant refinements.

To achieve this impossible goal, of being very concrete and extremely general at the same time, the author of the current lectures had to compromise. Instead of dealing with arbitrary non-commutative coefficients with the effect of explaining a lot of technicalities, we work here with commutative coefficients and the theory of determinants in the sense of Knudsen and Mumford (which is already intimidating enough for beginners).

As a consequence our approach does not add very much to the existing literature, especially to the excellent paper [**Fo**], except that we work with (Chow) motives instead of "motivic structures". We feel that, even if most of the ETNC has to do with the realizations of a motive, it is important not to forget that the source of all regulator maps is of a purely algebraic origin.

On the positive side we treat the case of the motive $h_1(E)(1)$ associated to an elliptic curve $E/\mathbb{Q}$ with all details, only assuming elementary facts as explained in Silverman's basic book [**Si**]. In fact to be more selfcontained, in Lecture 3, Section 5 we review the facts from the reduction theory, which we need.

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

It was surprising for the author of these lectures that, although well-known to the experts, the equivalence of the ETNC and the BSD conjecture seems to be not well-documented in the literature. A notable exception is [**Ve**], which treats the general case of abelian varieties, but omits many details and does not treat $p = 2$. We therefore hope that these notes are of some values also for the expert in this field.

For a complete account of the conjecture it is indispensable to consult [**BF**], although in the case of commutative coefficients very good introductions are [**Fo**] or [**Ka**]. The later one especially explains the connection with Iwasawa theory, which is necessary for proofs of the ETNC, but unfortunately could not be treated here do to lack of space and time.

Finally, it is a great pleasure to thank all the participants of the PCMI 2009 Graduate Summer School for their interest, their questions and their comments.

LECTURE 1

Motives, cohomology and determinants

In the first lecture we introduce some background about motives, their realizations and motivic cohomology. We introduce the L-function of a motive and finally, we give a short review of the theory of determinants for commutative rings.

1. Motives

We consider here only a very elementary theory 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**] §4, where *homological* motives are considered. A very good introduction is [**Sc1**], but there *cohomological* motives are used. The reader only interested in the case of elliptic curves, should just take notice of the existence of $h_1(E)$ in Example 1 and proceed to its realizations in Example 4.

Let $\mathcal{V}_{\mathbb{Q}}$ be the category of smooth and projective schemes over $\mathbb{Q}$. If $X, Y \in \mathcal{V}_{\mathbb{Q}}$ and $Y = \coprod Y_i$ with Y_i connected, let for $r \in \mathbb{Z}$

$$A^r(X \times Y) := \bigoplus_i CH^{\dim Y_i + r}(X \times_{\mathbb{Q}} Y_i)_{\mathbb{Q}},$$

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

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

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. Note that $A^0(X \times X)$ is a ring with the diagonal Δ as unit element.

Definition 1. The category of *Chow motives* $\mathcal{M}_{\mathbb{Q}}$ over $\mathbb{Q}$ has objects

$$M = (X, q, r),$$

where $X \in \mathcal{V}_{\mathbb{Q}}$, $q \circ q = q$ an idempotent in $A^0(X \times X)$ and $r \in \mathbb{Z}$. Here the morphisms are

$$\mathrm{Hom}_{\mathcal{M}_{\mathbb{Q}}}(M, N) := q' \circ A^{r-r'}(X \times X') \circ q,$$

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

We use the following notation (here Δ denotes the diagonal):

$$h(X) := (X, \Delta, 0), \quad \text{the } \textit{motive} \text{ of } X$$
$$\mathbb{Q}(n) := (\mathrm{Spec}\mathbb{Q}, \Delta, n), \quad \text{the } \textit{Tate motive}$$
$$M(n) := (X, p, r + n), \quad \text{the } \textit{n-fold Tate twist}.$$

The functor $\mathcal{V}_{\mathbb{Q}} \to \mathcal{M}_{\mathbb{Q}}$, which sends X to $h(X)$ and $f : X \to Y$ to its graph $\Gamma_f \subset X \times_{\mathbb{Q}} Y$ 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

$$\Gamma_f : h(X) \to h(Y)$$
$$\Gamma_f^t : h(Y) \to h(X)(\dim X - \dim Y).$$

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

$$M \otimes_{\mathbb{Q}} N := (X \times_{\mathbb{Q}} X', q \times_{\mathbb{Q}} q', r + r') \quad \text{the } \textit{product}$$
$$M^\vee := (X, q^t, \dim X - r) \quad \text{the } \textit{dual},$$

where q^t is the image of q under the map, which interchanges the two factors in $X \times_{\mathbb{Q}} X$. If $r = r'$, we define the direct sum by

$$M \oplus N := (X \coprod X', q \oplus q', r).$$

For arbitrary direct sums we refer to [**Sc1**] 1.14 but remember that there cohomological motives are used.

Remark 1. The product $M \otimes_{\mathbb{Q}} N$ of motives 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 a $\mathbb{Q}$-algebra, then M has *coefficients in* A, if $\mathrm{End}_{\mathcal{M}_{\mathbb{Q}}}(M)$ admits a ring homomorphism

$$\phi : A^{\mathrm{opp}} \to \mathrm{End}_{\mathcal{M}_{\mathbb{Q}}}(M).$$

This strange looking definition is necessary, if one wants that A (and not A^{opp}) acts on the realizations of M. This is a consequence of using homological motives. How this action comes up naturally, see Example 2 below. Note that the dual motive $M^\vee$ has coefficients in A^{opp}, where $a \in A$ acts via $\phi(a)^t$.

Example 1. Consider an elliptic curve $E/\mathbb{Q}$ with unit section $e : \mathrm{Spec}\mathbb{Q} \to E$ and the idempotents $q_0 := E \times e$ and $q_2 := e \times E$ and let $q_1 := \Delta - q_0 - q_2$. Then

$$h(E) = h_0(E) \oplus h_1(E) \oplus h_2(E),$$

where $h_i(E) := (E, q_i, 0)$. One has $h_2(E) \cong \mathbb{Q}(-1)$ and

$$(h_1(E)(1))^\vee(1) = h_1(E)(1).$$

It is shown in [**Sc1**] Proposition 4.5. that the natural map

$$\mathrm{End}_{\mathbb{Q}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{End}_{\mathcal{M}_{\mathbb{Q}}}(h_1(E)),$$

which sends $\phi \mapsto \Gamma_\phi$ is an isomorphism.

Example 2. Let $K/\mathbb{Q}$ be a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q})$ and $X := \mathrm{Spec}K$. Then G acts from the right on X and one gets a ring homomorphism

$$\mathbb{Q}[G]^{\mathrm{opp}} \to \mathrm{End}(h(\mathrm{Spec}K)) = A^0(X \times X),$$

where $\mathbb{Q}[G]$ is the group ring of G with coefficients in $\mathbb{Q}$. It is not too difficult to see that this is in fact a ring-isomorphism. One has

$$h(\mathrm{Spec}K)^\vee = h(\mathrm{Spec}K).$$

Remark 2. If K is any field, one has also the notion of motives over K, replacing $\mathcal{V}_{\mathbb{Q}}$ by $\mathcal{V}_K$ If $K/\mathbb{Q}$ is a finite field extension, one has two functors

$$\mathrm{Res}_{K/\mathbb{Q}} : \mathcal{M}_K \to \mathcal{M}_{\mathbb{Q}} \qquad \text{resp.} \qquad \times_{\mathbb{Q}} K : \mathcal{M}_{\mathbb{Q}} \to \mathcal{M}_K,$$

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

Example 3. With the notion of restriction and extension of scalars, the above Example 2 can be generalized to arbitrary motives $M \in \mathcal{M}_{\mathbb{Q}}$ in the following way. Let $K/\mathbb{Q}$ be as above a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q})$ and consider

$$M[G] := \mathrm{Res}_{K/\mathbb{Q}}(M \times_{\mathbb{Q}} K) \cong \mathrm{Res}_{K/\mathbb{Q}}(M \otimes h(\mathrm{Spec} K)).$$

It is straightforward to check that $M[G]$ has coefficients in $\mathbb{Q}[G]$. Example 2 is the special case $M = \mathbb{Q}(0)$.

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.

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

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

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

by $q^*(\xi) := \mathrm{pr}_{2,*}(\mathrm{cl}(q) \cup \mathrm{pr}_1^* \xi)$, where $\mathrm{cl}(q) \in H^{2\dim X}(X \times X, \dim X)$ is the cycle class of q.

The general rule for the i-th realization of M in the twisted cohomology theory $H^{\cdot}$ is

$$H^i(M, j) := q^* H^i(X, j + r)$$

the image under q^* of $H^i(X, j + r)$. We now make the realizations needed to formulate the ETNC explicit.

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

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

the subspace, which is fixed by F_∞.

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

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

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 by definition

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

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 $\mathbb{Q}_p(r)$ is the one dimensional $\mathbb{Q}_p$ 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 3. 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 4. 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

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

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). Indeed, the reader should check that q_1^* is zero on $H^i_?$ for $i \neq 1$ and the identity on $H^1_?$ for $? = B, \mathrm{dR}, p$. We identify

$$M_B = H^1(E(\mathbb{C}), \mathbb{Q}(1)) = \mathrm{Hom}(\Gamma, \mathbb{Z}(1)) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$$

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

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

The de Rham realization has a filtration

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

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

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

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

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then we let

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

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

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

via the Weil pairing $V_pE \times V_pE \to \mathbb{Q}_p(1)$. Note that $T_pE \subset V_pE$ is a $G_\mathbb{Q}$-stable $\mathbb{Z}_p$-lattice and that one has a natural isomorphism of $\mathbb{Z}_p$-modules $\Gamma \otimes_\mathbb{Z} \mathbb{Z}_p \cong T_pE$.

Example 5. Let $K/\mathbb{Q}$ be a finite field extension and consider $M = h(\mathrm{Spec}K)$. Then the realizations of $M(n)$ are

$$M(n)_B = \bigoplus_{\tau:K\to\mathbb{C}} \mathbb{Q}(n) \qquad M(n)_{\mathrm{dR}} = K \qquad M(n)_p = \bigoplus_{\tau:K\to\overline{\mathbb{Q}}} \mathbb{Q}_p(n).$$

Here the Hodge filtration on $M(n)_{\mathrm{dR}}$ is $\mathrm{Fil}^i M(n) = M(n)$ for $i \leq -n$ and $\mathrm{Fil}^i M(n) = 0$ for $i > -n$.

The period map for M generalizes the periods for Riemann surfaces. The embedding of $\mathbb{C}$ into the de Rham complex $\Omega^\cdot$ and a GAGA result give a comparison isomorphism $H^i_B(X(\mathbb{C}), \mathbb{Q}(j)) \otimes_\mathbb{Q} \mathbb{C} \cong H^i_{\mathrm{dR}}(X/\mathbb{Q}) \otimes_\mathbb{Q} \mathbb{C}$. In particular, there is a comparison isomorphism $M_B \otimes_\mathbb{Q} \mathbb{C} \cong M_{\mathrm{dR}} \otimes_\mathbb{Q} \mathbb{C}$ between the Betti and the de Rham realization, which is equivariant for the action of $F_\infty \otimes c$ on the left and $1 \otimes c$ on the right. Here c denotes complex conjugation. This gives

$$(M_B \otimes_\mathbb{Q} \mathbb{C})^{F_\infty \otimes c = 1} \cong M_{\mathrm{dR}} \otimes_\mathbb{Q} \mathbb{R}.$$

Definition 8. The *period map* is the composition of the inclusion of $M^+_{B,\mathbb{R}}$ into $(M_B \otimes_\mathbb{Q} \mathbb{C})^{F_\infty \otimes c=1}$ and the projection $M_{\mathrm{dR}} \otimes_\mathbb{Q} \mathbb{R} \to t(M) \otimes_\mathbb{Q} \mathbb{R}$:

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

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

Example 6. 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 4. Then the *period* Ω_∞ of E is the real number defined by

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

One has $\Omega_\infty = \int_{E(\mathbb{R})^0} \omega$.

Remark 4. The period map α_M behaves well under duality. One has a perfect pairing

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

which induces isomorphisms

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

3. Motivic cohomology

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

Definition 9. 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 (unramified) *motivic cohomology* $H^i_{\mathrm{mot}}(\mathbb{Z}, M)$ is defined as

$$H^0_{\mathrm{mot}}(\mathbb{Z}, M) := \begin{cases} 0 & \text{if } i \neq 2r \\ q^* CH^r(X)_\mathbb{Q}/CH^r(X)^0_\mathbb{Q} & \text{if } i = 2r. \end{cases}$$

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

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.

This is independent of the choice of $\mathcal{X}$ (see [**Sch**] page 13). Note that for weight $w = i - 2r > -1$ one has

$$H^1_{\mathrm{mot}}(\mathbb{Z}, M) = 0.$$

Remark 5. If one does not want to assume the existence of a proper, flat, regular model one can use also use a definition given by Scholl [**Sc2**], which uses alterations.

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

Example 7. Let $E/\mathbb{Q}$ be an elliptic curve, $M = h_1(E)(1)$ and $i = 1$, then Conjecture 1 is true. More precisely,

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

Another case where Conjecture 1 is known are the motives of number fields.

Example 8. Let $K/\mathbb{Q}$ be a finite field extension with ring of integers $\mathcal{O}_K$. Then $\mathrm{Spec}\mathcal{O}_K$ is a proper, flat, regular model of $\mathrm{Spec}K$ and for $M = h(\mathrm{Spec}K)$ (only $i = 0$ is interesting) one gets

$$H^0_{\mathrm{mot}}(\mathbb{Z}, M) = \mathbb{Q} \qquad\qquad H^0(\mathbb{Z}, M(n)) = 0 \text{ for } n \neq 0$$

and

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

By a result of Borel [**Bo**] one knows moreover:

$$\dim_{\mathbb{Q}} H^1_{\mathrm{mot}}(\mathbb{Z}, M(n)) = \begin{cases} r_2 & n \text{ even } n \geq 1 \\ r_1 + r_2 & n \text{ odd } n \geq 1, \end{cases}$$

where r_1 and r_2 are the number of real (resp. complex) embeddings of K.

4. L-functions

Starting from this section, we let $M = (X, q, r) \in \mathcal{M}_{\mathbb{Q}}$ be a motive over $\mathbb{Q}$ with coefficients in a finite dimensional, semi-simple and commutative algebra $A/\mathbb{Q}$ and we *fix* $i \in \mathbb{Z}_{\geq 0}$. Note that A is a product of fields.

We need Fontaine's $D_{\mathrm{cris}}(M_p) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} M_p)^{G_{\mathbb{Q}_p}}$, which is a finite dimensional $\mathbb{Q}_p$-vector space with a Frobenius endomorphism ϕ.

Definition 10. For each finite place v of $\mathbb{Q}$ let

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

be the local Euler factor at v. This is a polynomial in $A_{\mathbb{Q}_p}[T]$. Here I_v is the inertia group and Frob_v is the Frobenius endomorphism.

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

Definition 11. The *L-function* of M is the formal Euler product for $s \in \mathbb{C}$

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

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

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

(see [**BF**] Lemma 8). Note that

$$L(M(n),s) = L(M,s+n).$$

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

Conjecture 3 (Meromorphic continuation)**.** *Assuming Conjecture 2, the function $s \mapsto L(M,s)$ has a meromorphic continuation to $s=0$.*

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 (Order of vanishing)**.** *Assume Conjecture 1 and Conjecture 3, then*

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

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

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

Definition 12. Assume Conjectures 2 and 3. Let $r_M := \mathrm{ord}_{s=0} L(M,s)$ and define the *leading coefficient* at $s=0$ by

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

Example 9. Let $E/\mathbb{Q}$ be an elliptic curve and consider $M = h_1(E)(1)$ and $i=1$. We know from Example 4 that $M_p \cong V_pE$ and it is shown in Lecture 3, Section 5 in Lemma 5 that $V_pE^{I_v} = V_p\widetilde{E}_v^{\mathrm{ns}}$ for $v \neq p$. Here $\widetilde{E}_v^{\mathrm{ns}}$ are the non-singular points in the reduction at v of a global minimal Weierstraß equation of E. Let

$$S := \{v \mid I_v \text{ acts non-trivially on } V_pE\}$$

the set of places of $\mathbb{Q}$, where V_pE is ramified (equals the set of places of bad reduction by the criterion of Neron-Ogg-Shafarevich). The computations in [**Si**] V§2 imply that for $v \neq p$ and $v \notin S$

$$L_v(M_p,T) = 1 - \mathrm{tr}(\mathrm{Frob}_v)v^{-1}T + v^{-1}T^2.$$

It also follows from loc. cit. that $\mathrm{tr}(\mathrm{Frob}_v) = v + 1 - \#\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)$. For $v \neq p$ and $v \in S$ we have to distinguish additive and multiplicative reduction. In the case of additive reduction $E_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) = \overline{\mathbb{F}}_v$ (see [**Si**] VII Proposition 5.1. (c)) and hence $V_pE^{I_v} = 0$, which gives $L_v(M_p,T) = 1$. In the multiplicative case we have by loc. cit. $E_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) = \overline{\mathbb{F}}_v^*$ and $V_pE^{I_v}$ is a one-dimensional $\mathbb{Q}_p$ vector space. As Frob_v needs to have integral eigenvalues, we see that Frob_v acts by $+1$ or -1 in this case. This gives $L_v(M_p,T)=1\pm T$. In the case where Frob_v acts by -1 one has $E_v^{\mathrm{ns}}(\mathbb{F}_{v^2})=\mathbb{F}_{v^2}^*$ and one sees $\#E_v^{\mathrm{ns}}(\mathbb{F}_v)=v+1$. Thus we have in all cases

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

and the L-function of M agrees up to a shift with the usual L-function of E, i.e.,

$$L(M,s)=L(E,s+1).$$

By the work of Wiles et al. it is known that E is modular. In particular, the L-function has a meromorphic continuation to $\mathbb{C}$ and Conjecture 3 holds. Conjecture 2 is known for $v\neq p$ by the remarks above (essentially the Weil conjectures) and for $v=p$ by the work of Saito [**Sa**], who again proves this result for the L-function of a modular form.

5. Determinants

We review the theory of determinants for commutative rings following [**KM**], for which we refer for more details and proofs.

For any ring A let $P_{\mathrm{fg}}(A)$ be the category of finitely generated, projective A-modules.

Definition 13. Let A be a commutative ring. The category of isomorphisms of graded invertible A-modules $\mathcal{L}\,\mathrm{is}_A$ has objects pairs (L,r), where L is an invertible A-module and $r:\mathrm{Spec}A\to\mathbb{Z}$ is a locally constant function. The morphisms are

$$\mathrm{Mor}_{\mathcal{P}_A}((L,r),(M,s)):=\begin{cases}\mathrm{Isom}(L,M) & \text{if } r=s\\ \emptyset & \text{if } r\neq s.\end{cases}$$

The (tensor) product is defined by

$$(L,r)\cdot(M,s):=(L\otimes_A M,r+s)$$

with commutativity constraint

$$\psi_{(L,r),(M,s)}:(L,r)\cdot(M,s)\cong(M,s)\cdot(L,r)$$

defined by $\psi_{(L,r),(M,s)}(l\otimes m):=(-1)^{r(\mathfrak{p})s(\mathfrak{p})}m\otimes l$, if $l\in L_{\mathfrak{p}}$, $m\in M_{\mathfrak{p}}$, where $\mathfrak{p}\subset A$ is a prime ideal.

Note that we follow the convention in [**BF**] in the commutativity constraint. The unit object for the product is $(A,0)$. For each (L,r) let $L^{-1}:=\mathrm{Hom}_A(L,A)$, then $(L,r)^{-1}:=(L^{-1},-r)$ is an inverse of (L,r) and one has an isomorphism

$$\mathrm{ev}:(L,r)\cdot(L^{-1},-r)\cong(A,0),$$

induced by the usual evaluation morphism $\mathrm{ev}:L\otimes_A\mathrm{Hom}_A(L,A)\to A$. There exists also a base change functor for ring homomorphisms.

Definition 14. Let $f:A\to B$ be a ring homomorphism, then the functor

$$\otimes_A B:\mathcal{L}\,\mathrm{is}_A\to\mathcal{L}\,\mathrm{is}_B$$

is defined by $(L,r)\otimes_A B:=(L\otimes_A B,r\circ f^*)$ on objects and in the obvious way on morphisms. Here $f^*:\mathrm{Spec}B\to\mathrm{Spec}A$ is the induced map.

For each $P \in P_{\rm fg}(A)$ define

$$\mathrm{Det}_A(P) := (\bigwedge_A^{\mathrm{rk}_A(P)} P, \mathrm{rk}_A(P)),$$

where $\mathrm{rk}_A : P_{\rm fg}(A) \to \mathbb{Z}$ is the A-rank of P and $\bigwedge_A^{\mathrm{rk}_A(P)} P$ the exterior power over A. Note that $\mathrm{Det}_A(0) = (A, 0)$ is the unit object and that one has for a short exact sequence $0 \to P' \to P \to P'' \to 0$ of objects in $P_{\rm fg}(A)$ an isomorphism

$$\mathrm{Det}_A(P') \cdot \mathrm{Det}_A(P'') \cong \mathrm{Det}_A(P).$$

It is important to note that the base change functor $\otimes_A B$ commutes with determinants, i.e.,

$$\mathrm{Det}_A(C^\cdot) \otimes_A B \cong \mathrm{Det}_B(C^\cdot \otimes_A B).$$

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

$$\mathrm{Det}_A(C^\cdot) := \prod_{i \in \mathbb{Z}} \mathrm{Det}_A(C^i)^{-1}.$$

This construction extends to a functor Det_A from the category of bounded complexes $C^\cdot$ of modules in $P_{\rm fg}(A)$ with quasi-isomorphisms as morphisms to the category $\mathcal{L}\mathrm{is}_A$. In particular, one has for acyclic complexes $C^\cdot$ a canonical isomorphism

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

In fact one can define determinants for more general complexes. Denote by Perf_A the category of complexes of A-modules, which are quasi-isomorphic to a bounded complex of modules in $P_{\rm fg}(A)$.

Definition 15. For each complex $C^\cdot \in \mathrm{Perf}_A$ fix a quasi-isomorphism $\widetilde{C}^\cdot \to C^\cdot$, where $\widetilde{C}^\cdot$ is a bounded complex of modules in $P_{\rm fg}(A)$. Then we define

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

If $C^\cdot \in \mathrm{Perf}_A$ has the property that $H^j(C^\cdot) \in P_{\rm fg}(A)$ for all $j \in \mathbb{Z}$, one has

$$\mathrm{Det}_A(C^\cdot) \cong \prod_j \mathrm{Det}_A(H^j(C^\cdot))^{(-1)^j}.$$

Example 10. Let $\phi : P \cong Q$ be an isomorphism of modules in $\mathcal{L}\mathrm{is}_A$. Considered as an acyclic complex (in degree $0, 1$) one has a canonical isomorphism

$$\rho : \mathrm{Det}_A([P \to Q]) = \mathrm{Det}_A(P) \cdot \mathrm{Det}_A(Q)^{-1} \cong \mathrm{Det}_A(0),$$

which is induced by the isomorphism $\mathrm{Det}_A(\phi) : \mathrm{Det}_A(P) \cong \mathrm{Det}_A(Q)$ and the evaluation $\mathrm{Det}_A(Q) \cdot \mathrm{Det}_A(Q)^{-1} \cong \mathrm{Det}_A(0)$. If it happens that $P = Q$, then the evaluation gives directly $\mathrm{ev} : \mathrm{Det}_A([P \to P]) \cong \mathrm{Det}_A(0)$, but this differs from the above by $\det(\phi)$, one has

$$\rho = \det(\phi)\mathrm{ev}.$$

Example 11. Let $A = \mathbb{Z}_p$, then all modules in $P_{\rm fg}(\mathbb{Z}_p)$ are free. Let H be a finite abelian group, which is a $\mathbb{Z}_p$-module. Then we claim that

$$\mathrm{Det}_{\mathbb{Z}_p}(H) \subset \mathrm{Det}_{\mathbb{Q}_p}(H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \mathrm{Det}_{\mathbb{Q}_p}(0)$$

is the $\mathbb{Z}_p$-sublattice $(\#H)^{-1}\mathbb{Z}_p$. To show this let

$$0 \to P \xrightarrow{\phi} Q \to H \to 0$$

be a resolution with $P, Q \in P_{\mathrm{fg}}(\mathbb{Z}_p)$. Choose bases $p_1, \ldots, p_r$ and $q_1, \ldots, q_r$ of P and Q respectively, then $\mathrm{Det}_{\mathbb{Z}_p}(H) \subset \mathrm{Det}_{\mathbb{Q}_p}(H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is generated by

$$(q_1 \wedge \ldots \wedge q_r)(p_1 \wedge \ldots \wedge p_r)^{-1} \in \mathrm{Det}_{\mathbb{Z}_p}(Q) \cdot \mathrm{Det}_{\mathbb{Z}_p}(P)^{-1} \cong \mathrm{Det}_{\mathbb{Z}_p}(H).$$

The identification

$$\mathrm{Det}_{\mathbb{Z}_p}(0) = \mathrm{Det}_{\mathbb{Q}_p}(H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cong \mathrm{Det}_{\mathbb{Q}_p}(Q \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cdot \mathrm{Det}_{\mathbb{Q}_p}(P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{-1}$$

is as in Example 10 and maps $(q_1 \wedge \ldots \wedge q_r)(p_1 \wedge \ldots \wedge p_r)^{-1}$ to $\det(\phi)^{-1}$. It is well-known and not difficult to show that $\det(\phi) = \#H$, which proves the claim.

LECTURE 2

The equivariant Tamagawa number conjecture

In this lecture we formulate the Rationality Conjecture of Beilinson and Deligne and the equivariant Tamagawa number conjecture of Bloch-Kato, Fontaine-Perrin-Riou and Burns-Flach. As explained in the introduction, we restrict here to the case of commutative coefficients. For the general case we refer to [**BF**] (and to [**HK1**], [**Ve**] for a formulation with non-commutative determinants, more in the spirit of this lecture).

We let $M = (X, q, r) \in \mathcal{M}_{\mathbb{Q}}$ with coefficients in a finite-dimensional, semi-simple and commutative $A/\mathbb{Q}$ (i.e., A is a product of fields). Fix $i \in \mathbb{Z}_{\geq 0}$. We will 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.

1. Rationality conjecture

In this section we formulate the Rationality Conjecture of Beilinson and Deligne, which states essentially that $L(M, 0)^*$ divided by a certain period is "rational".

Recall from Definition 8 the period map

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

The following conjecture formulates a very deep relation between the kernel and the cokernel of the period map and the motivic cohomology.

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

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

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

Note that the conjecture implies also that the motivic cohomology groups have finite dimension.

Remark 6. Assume that the weight $w = i - 2r$ of M is not -1. Then by the remark after Definition 9 either $H^1_{\mathrm{mot}}(\mathbb{Z}, M)$ or $H^1_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1))$ is zero. If furthermore, $w \neq 0$, then the above conjecture says that there is either an isomorphism

$$\ker\alpha_M \xrightarrow{r_\infty^\vee} H^1_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1))_{\mathbb{R}}^\vee$$

or an isomorphism

$$H^1_{\mathrm{mot}}(\mathbb{Z}, M)_{\mathbb{R}} \xrightarrow{r_\infty} \mathrm{coker}\alpha_M.$$

Example 12. Let $M = h_1(E)(1)$ and $i = 1$, then Conjecture 5 holds for M. Indeed, α_M is an isomorphism, so that $\ker\alpha_M = 0 = \operatorname{coker}\alpha_M$. By definition $H^0_{\mathrm{mot}}(\mathbb{Z}, M) = 0 = H^0_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1))$. 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

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

Example 13. Let $K/\mathbb{Q}$ be a number field, then it follows from the results by Borel [**Bo**] (and the comparison of the Borel and Beilinson regulator by Beilinson) that Conjecture 5 holds for $h(\operatorname{Spec}K)(n)$.

Definition 16. The *fundamental line* is defined by

$$\begin{aligned}\Delta(M) :=& \operatorname{Det}_A(H^0_{\mathrm{mot}}(\mathbb{Z}, M)) \cdot \operatorname{Det}_A^{-1}(H^1_{\mathrm{mot}}(\mathbb{Z}, M)) \cdot \operatorname{Det}_A(t(M)) \\ & \operatorname{Det}_A^{-1}(H^0_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1))^\vee) \cdot \operatorname{Det}_A(H^1_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1))^\vee) \cdot \operatorname{Det}_A^{-1}(M_B^+).\end{aligned}$$

Example 14. Let $M = h_1(E)(1)$ and $i = 1$, then with Examples 4 and 7 we get

$$\Delta(M) = \operatorname{Det}_{\mathbb{Q}}(E(\mathbb{Q})_{\mathbb{Q}})^{-1} \cdot \operatorname{Det}_{\mathbb{Q}}(E(\mathbb{Q})^\vee_{\mathbb{Q}}) \cdot \operatorname{Det}_{\mathbb{Q}}(\operatorname{Lie}E) \cdot \operatorname{Det}_{\mathbb{Q}}(\Gamma^+_{\mathbb{Q}})^{-1}.$$

Example 15. Let $M = h(\operatorname{Spec}K)$ and $K/\mathbb{Q}$ a Galois extension with $G = \operatorname{Gal}(K/\mathbb{Q})$ abelian, then the fundamental line $\Delta(M(n))$ is given by

$$\operatorname{Det}_{\mathbb{Q}[G]}(H^0_{\mathrm{mot}}(\mathbb{Z}, M(n)))\operatorname{Det}_{\mathbb{Q}[G]}(H^1_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1-n))^\vee)\operatorname{Det}^{-1}_{\mathbb{Q}[G]}(M(n)^+_B)$$

if $n \leq 0$ and by

$$\operatorname{Det}_{\mathbb{Q}[G]}(H^0_{\mathrm{mot}}(\mathbb{Z}, M^\vee(1-n))^\vee)\operatorname{Det}^{-1}_{\mathbb{Q}[G]}(H^1_{\mathrm{mot}}(\mathbb{Z}, M(n)))\operatorname{Det}^{-1}_{\mathbb{Q}[G]}(M(n)^+_B)\operatorname{Det}_{\mathbb{Q}[G]}(M(n)_{\mathrm{dR}})$$

if $n \geq 1$.

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

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

induces a canonical isomorphism

$$\theta_\infty : \Delta(M)_{\mathbb{R}} \cong \operatorname{Det}_{A_{\mathbb{R}}}(0).$$

The first part of the ETNC (the Rationality Conjecture, due to Deligne and Beilinson) can now be formulated.

Conjecture 6 (Rationality Conjecture)**.** *Assume Conjectures 2, 3 and 5. Let M be as above with coefficients in A. Consider $L(M,0)^* \in A^\times_{\mathbb{R}}$, then there exist a* zeta element

$$\zeta_A(M) \in \Delta(M)$$

such that

$$\theta_\infty(\zeta_A(M)) = (L(M,0)^*)^{-1} \in A^\times_{\mathbb{R}}.$$

2. Local unramified cohomology

We review here the definition of local unramified cohomology, for more details one should consult [**Fo**] and [**BF**]. In fact, to work properly with determinants one has to use "true triangles", instead of just triangles in the derived category, so that for precise definitions we refer to [**BF**] 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

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

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

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

Note that the comparison isomorphism (due to Faltings) between M_p and M_{dR} over $\mathbb{Q}_p$ induces an isomorphism

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

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

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

Here $I_v \subset G_{\mathbb{Q}_v}$ is the inertia subgroup and the complexes for $v \neq \infty$ are placed in degree $0, 1$. We denote the cohomology of $R\Gamma_f(\mathbb{Q}_v, M_p)$ by $H^i_f(\mathbb{Q}_v, M_p)$.

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

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

Definition 19. The *Bloch-Kato exponential map*

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

is the composition of the inclusion $t(M_p) \to D_{\mathrm{cris}}(M_p) \oplus t(M_p)$, which maps $t \mapsto (0, t)$, and the surjection $D_{\mathrm{cris}}(M_p) \oplus t(M_p) \to H^1_f(\mathbb{Q}_p, M_p)$.

For computations 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. Let

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

For $H^i_{/f}$ let

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

Note that the torsion subgroups of $H^1_f(\mathbb{Q}_v,T_p)$ and $H^1(\mathbb{Q}_v,T_p)$ coincide by definition. If T_p is unramified at v, one can give a different description of $H^1_f(\mathbb{Q}_v,T_p)$.

Lemma 1. *Let T_p be unramified at $v\neq p$ (i.e., the inertia I_v acts trivially on T_p). Then*

$$H^1_f(\mathbb{Q}_v,T_p)=\ker\left(H^1(\mathbb{Q}_v,T_p)\to H^1(I_v,T_p)\right).$$

Note that under the conditions of the lemma $H^1(I_v,T_p)=\mathrm{Hom}_{\mathrm{ct}}(I_v,T_p)$ (continuous homomorphisms).

PROOF. By definition of $H^1_f(\mathbb{Q}_v,M_p)$ and because M_p is unramified, we have

$$H^1_f(\mathbb{Q}_v,M_p)=H^1(G_{\mathbb{Q}_v}/I_v,M_p)=\ker\left(H^1(\mathbb{Q}_v,M_p)\to H^1(I_v,M_p)\right).$$

This implies that $H^1_f(\mathbb{Q}_v,T_p)$ is the kernel of the composition

$$H^1(\mathbb{Q}_v,T_p)\to H^1(\mathbb{Q}_v,M_p)\to H^1(I_v,M_p).$$

As the canonical map $H^1(I_v,T_p)=\mathrm{Hom}_{\mathrm{ct}}(I_v,T_p)\to H^1(I_v,M_p)=\mathrm{Hom}_{\mathrm{ct}}(I_v,M_p)$ is injective, the commutative diagram

$$\begin{array}{ccc} H^1(\mathbb{Q}_v,T_p) & \longrightarrow & H^1(I_v,T_p)\\ \downarrow & & \downarrow\\ H^1(\mathbb{Q}_v,M_p) & \longrightarrow & H^1(I_v,M_p)\end{array}$$

shows that $H^1_f(\mathbb{Q}_v,T_p)$ is also the kernel of $H^1(\mathbb{Q}_v,T_p)\to H^1(I_v,T_p)$. □

3. Global unramified cohomology

Fix a prime number p. Denote by S a finite set of places of $\mathbb{Q}$, which contains p,∞ and the places v, for which M_p is ramified (i.e., where I_v acts non-trivially). 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

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

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

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

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

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

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

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 important triangle (which can be made a true triangle, see [**BF**] 3.2)

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

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

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

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

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

For later use, we introduce an integral structure on $H^1_f(\mathbb{Q}, M_p)$. Note that by definition

$$H^1_f(\mathbb{Q}, M_p) = \{\xi \in H^1(\mathbb{Z}_S, M_p) \mid \xi_v \in H^1_f(\mathbb{Q}_v, M_p) \text{ for all } v \in S\},$$

where ξ_v is the image of ξ in $H^1(\mathbb{Q}_v, M_p)$.

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

$$\begin{aligned} H^1_f(\mathbb{Q}, T_p) &:= \{\xi \in H^1(\mathbb{Z}_S, T_p) \mid \xi_v \in H^1_f(\mathbb{Q}_v, T_p) \text{ for all } v \in S\} \\ &= \ker\left(H^1(\mathbb{Z}_S, T_p) \to \bigoplus_{v\in S} H^1_{/f}(\mathbb{Q}_v, T_p)\right), \end{aligned}$$

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

For later use, we note:

Lemma 2. *Let $T_p \subset M_p$ be a $G_\mathbb{Q}$-stable $\mathbb{Z}_p$-lattice, then*

$$H^1_f(\mathbb{Q}, T_p) = \ker\left(H^1(\mathbb{Q}, T_p) \to \prod_v H^1_{/f}(\mathbb{Q}_v, T_p)\right).$$

Proof. We claim that

$$H^1(\mathbb{Z}_S, T_p) = \ker\left(H^1(\mathbb{Q}, T_p) \to \prod_{v\notin S} H^1_{/f}(\mathbb{Q}_v, T_p)\right).$$

Accepting the claim, the statement of the lemma follows immediately: each $\xi \in H^1(\mathbb{Q}, T_p)$, which maps to zero in $\prod_{v\notin S} H^1_{/f}(\mathbb{Q}_v, T_p)$ comes from an element in $H^1(\mathbb{Z}_S, T_p)$. If it also maps to zero in $\bigoplus_{v\in S} H^1_{/f}(\mathbb{Q}_v, T_p)$ it is in $H^1_f(\mathbb{Q}, T_p)$. To prove the claim, let $\mathbb{Q}^S$ be the maximal extension of $\mathbb{Q}$, which is unramified outside of S and $G_{\mathbb{Q}^S} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^S)$. The inflation-restriction sequence gives

$$0 \to H^1(\mathbb{Z}_S, T_p) \to H^1(\mathbb{Q}, T_p) \to H^1(\mathbb{Q}^S, T_p).$$

The last group is $\mathrm{Hom}_{\mathrm{ct}}(G_{\mathbb{Q}^S}, T_p)$ because $G_{\mathbb{Q}^S}$ acts trivially on T_p. As $G_{\mathbb{Q}^S}$ is the smallest closed normal subgroup of $G_\mathbb{Q}$, which contains I_v for all $v \notin S$, we have an injection

$$H^1(\mathbb{Q}^S, T_p) = \mathrm{Hom}_{\mathrm{ct}}(G_{\mathbb{Q}^S}, T_p) \hookrightarrow \prod_{v\notin S} \mathrm{Hom}_{\mathrm{ct}}(I_v, T_p),$$

so that the sequence

$$0 \to H^1(\mathbb{Z}_S, T_p) \to H^1(\mathbb{Q}, T_p) \to \prod_{v\notin S} \mathrm{Hom}_{\mathrm{ct}}(I_v, T_p) \tag{1}$$

is still exact. By Lemma 1 we see that $\mathrm{Hom}_{\mathrm{ct}}(I_v, T_p) = H^1_{/f}(\mathbb{Q}_v, T_p)$, which implies the claim. □

4. The equivariant Tamagawa number conjecture

The following conjecture relates the motivic cohomology to the global unramified cohomology. It contains deep conjectures of Tate and Jannsen as special cases and the finiteness of the p-torsion of the Tate-Shafarevich group.

Conjecture 7 (Regulators)**.** *The p-adic regulators*

$$r_p : H^0_{\mathrm{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \to H^0_f(\mathbb{Q}, M_p)$$
$$r_p : H^1_{\mathrm{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}, M_p)$$

are isomorphisms for all p.

Example 16. Let $E/\mathbb{Q}$ be an elliptic curve and $M = h_1(E)(1)$, then Conjecture 7 for p is true if and only if $Ш(\mathbb{Q}, E)[p^\infty]$ is a finite group. This follows from Theorem 2 below as the regulator $E(\mathbb{Q})_{\mathbb{Q}_p} = H^1_{\mathrm{mot}}(\mathbb{Z}, M)_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}, M_p)$ is given by the Kummer map and $H^0_{\mathrm{mot}}(\mathbb{Z}, M) = 0 = H^0_f(\mathbb{Q}, M_p)$.

Remark 7. Let $K/\mathbb{Q}$ be a number field $K/\mathbb{Q}$ and $M = h(\mathrm{Spec}K)$. One can show that $r_p : H^i_{\mathrm{mot}}(\mathbb{Z}, M(n))_{\mathbb{Q}_p} \to H^i_f(\mathbb{Q}, M(n)_p)$ for $i = 0, 1$ are isomorphisms for all n.

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

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

The triangle for $R\Gamma_c(\mathbb{Z}_S, M_p)$ in (3) gives

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

Together with the isomorphism ι_v in (4) one gets

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

With Conjecture 7 and Proposition 1 the right hand side is canonically isomorphic to $\Delta(M)_{\mathbb{Q}_p}$.

Definition 23. For any p let

$$\theta_{p,S} : \Delta(M)_{\mathbb{Q}_p} \cong \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p))$$

be the isomorphism defined above.

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

Definition 24. Let $A/\mathbb{Q}$ be finite dimensional, commutative and semi-simple $\mathbb{Q}$-algebra. 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

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

is a Galois stable lattice in M_p.

Example 17. For an elliptic curve $E/\mathbb{Q}$, the subgroup $H^1(E(\mathbb{C}), \mathbb{Z}(1)) \subset h(E)(1)_B$ is a projective $\mathbb{Z}$-structure. For the motive $h(\mathrm{Spec}K)(n)$, where $K/\mathbb{Q}$ is an (abelian) Galois extension with $G = \mathrm{Gal}(K/\mathbb{Q})$, the $\mathbb{Z}[G]$-module $\bigoplus_{\tau:K\to\mathbb{C}} \mathbb{Z} \subset h(\mathrm{Spec}K)_B$ is a projective $\mathbb{Z}[G]$-structure for the order $\mathbb{Z}[G] \subset \mathbb{Q}[G]$.

We can now formulate the equivariant Tamagawa number conjecture due to Bloch-Kato, Fontaine-Perrin-Riou and Burns-Flach.

Conjecture 8 (Equivariant Tamagawa number conjecture (ETNC))**.** *Let $M \in \mathcal{M}_{\mathbb{Q}}$ be a motive with coefficients in A and assume Conjectures 2, 3, 5, the Rationality Conjecture 6 and Conjecture 7. Let T_B be a projective $\mathcal{A}$-structure in M and let $\zeta_A(M) \in \Delta(M)$ be the zeta element defined in Conjecture 6. Let S be a finite set of places of $\mathbb{Q}$, such that M_p is unramified outside of S and $p, \infty \in S$. Then the $\mathcal{A}_{\mathbb{Z}_p}$-submodule*

$$\theta_{p,S}(\zeta_A(M))\mathcal{A}_{\mathbb{Z}_p} \subset \mathrm{Det}_{A_{\mathbb{Q}_p}}(R\Gamma_c(\mathbb{Z}_S, M_p))$$

coincides with $\mathrm{Det}_{\mathcal{A}_{\mathbb{Z}_p}}(R\Gamma_c(\mathbb{Z}_S, T_p))$*, where* $T_p := T_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$*.*

Remark 8. 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

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

where T'_p/T_p is finite. By Example 11 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 [**Mi**] I 2.8 and 5.1).

Remark 9. 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

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

The complex $R\Gamma(\mathbb{F}_v, T_p^{I_v})$ can be represented by $[T_p^{I_v} \xrightarrow{1-\mathrm{Frob}_v^{-1}} T_p^{I_v}]$, which is mapped under ι_v to $\mathcal{A}_{\mathbb{Z}_p}$. This implies $\theta_{p,S}(\zeta_A(M))\mathcal{A}_{\mathbb{Z}_p} = \theta_{p,S'}(\zeta_A(M))\mathcal{A}_{\mathbb{Z}_p}$.

Remark 10. The independence of S and the compatibility of zeta elements in towers of number fields also shows that the zeta elements give rise to Euler systems, see [**Ka**] Remark 4.14 for more details.

5. Unramified cohomology for elliptic curves

In this section we compute the local and global unramified cohomology for elliptic curves.

Consider an elliptic curve $E/\mathbb{Q}$ and let T_pE and V_pE be as defined in Example 4. Fix a finite set of places S of $\mathbb{Q}$, such that T_pE is unramified outside of S and $p, \infty \in S$.

The Kummer sequence induces for any place v of $\mathbb{Q}$ an exact sequence

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

where $E(\mathbb{Q}_v)^{\wedge p} := \varprojlim_n E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v)$ is the p-adic completion and $T_p(\dots) := \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \dots)$. Note that T_p of a finite group is zero.

We need the following fact on the exponential map $\exp_{\mathrm{BK}} : \mathrm{Lie}E_{\mathbb{Q}_p} \to H^1_f(\mathbb{Q}_p, V_pE)$ and $H^0_f(\mathbb{Q}_p, V_pE)$.

Proposition 2 ([**BK**] Example 3.10.1 and 3.11)**.** *One has $H^0_f(\mathbb{Q}_p, V_pE) = 0$ and the diagram*

$$\begin{CD} E_1(\mathbb{Q}_p)_{\mathbb{Q}_p} @>{Kummer}>> H^1(\mathbb{Q}_p, V_pE) \\ @A{\exp}A{\cong}A @AAA \\ \mathrm{Lie}(E)_{\mathbb{Q}_p} @>{\exp_{\mathrm{BK}}}>{\cong}> H^1_f(\mathbb{Q}_p, V_pE) \end{CD}$$

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

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

Remark 11. The same result of Bloch and Kato also shows that for finite field extension $K/\mathbb{Q}_p$ and $M = h(\mathrm{Spec}K)$ the Kummer map induces an isomorphism

$$(\mathcal{O}^*_{K_p})^{\wedge p}_{\mathbb{Q}_p} \cong H^1_f(\mathbb{Q}_p, M(1)_p),$$

where we have written $K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\mathcal{O}_{K_p} \cong \prod_{w|p} \mathcal{O}_{K_w}$.

The next theorem gives the complete describtion of the local unramified cohomology of T_pE.

Theorem 1. *The Kummer sequence induces for all v*

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

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

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

Remark 12. Continuing Remark 11 let $T_p := \bigoplus_{\tau: K \to \overline{\mathbb{Q}}} \mathbb{Z}_p$ be a Galois stable $\mathbb{Z}_p$ lattice in M_p. Then, one can show that the Kummer sequence induces an isomorphism

$$(\mathcal{O}^*_{K_p})^{\wedge p} \cong H^1_f(\mathbb{Q}_p, T_p(1))$$

(cf. [**HK2**] Lemma A.1).

We first prove a lemma.

Lemma 3. *For $v \neq p, \infty$ the map $1 - \mathrm{Frob}_v^{-1}$ induces an isomorphism*

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

so that

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

For $v = p$ we have

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

Proof. As $\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)$ is finite, this follows from Lecture 3, Section 5 Lemma 5 and Proposition 2. □

Proof of Theorem 1. By Lemma 3, we have $H^0_f(\mathbb{Q}_v, T_pE) = 0$ for all $v \neq \infty$. We claim that for all places $v \neq \infty$

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

For $v = p$ this is contained in Proposition 2. For $v \neq p, \infty$ both sides are zero: indeed, the left hand side is zero by the structure of $E(\mathbb{Q}_v)$ recalled in Theorem 6 because the p-adic completion of $E_1(\mathbb{Q}_v)$ is zero, so that $E(\mathbb{Q}_v)^{\wedge p}$ is a finite group. The right hand side is zero by Lemma 3. Consider the commutative diagram:

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

As $T_pH^1(\mathbb{Q}_v, E)$ is torsion free, the right vertical arrow is injective. 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 $E(\mathbb{Q}_v)^{\wedge p} \cong H^1_f(\mathbb{Q}_v, T_pE)$ for $v \neq \infty$. For $v = \infty$, the group $H^1(\mathbb{R}, E)$ is 2-torsion, which implies that $H^1(\mathbb{R}, E[2]) \to H^1(\mathbb{R}, E)$ is surjective. Hence, $H^1(\mathbb{R}, E)$ is finite, so that $T_pH^1(\mathbb{R}, E) = 0$. This gives

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

The statement about $T_pH^1(\mathbb{Q}_v, E)$ follows from the definition of $H^1_{/f}((\mathbb{Q}_v, T_pE)$. □

To compute the global unramified cohomology $H^1_f(\mathbb{Q}, T_pE)$, we recall the definition of the Shafarevich-Tate group.

Definition 25. Let $E/\mathbb{Q}$ be an elliptic curve, then

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

is called the *Shafarevich-Tate group*.

Theorem 2. *The Kummer sequence identifies*

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

inside $H^1(\mathbb{Q}, T_pE)$ if and only if $Ш(\mathbb{Q}, E)[p^\infty]$ is a finite group.

PROOF. Consider the commutative diagram

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

Consider the kernel-cokernel sequence (cf. [**Mi**] I Proposition 0.24) of the composition

$$H^1(\mathbb{Q}, T_pE) \to T_pH^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, T_pE).$$

As the functor $T_p(\dots) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \dots)$ is left exact, $H^1_{/f}(\mathbb{Q}_v, T_pE) = T_pH^1(\mathbb{Q}_v, E)$ by Theorem 1 and using Lemma 2, this kernel-cokernel sequence gives an exact sequence

$$0 \to E(\mathbb{Q})^{\wedge p} \to H^1_f(\mathbb{Q}, T_pE) \to T_p Ш(\mathbb{Q}, E) \to 0.$$

If $Ш(\mathbb{Q}, E)[p^\infty]$ is finite, we get that $T_pШ(\mathbb{Q}, E) = T_pШ(\mathbb{Q}, E)[p^\infty] = 0$. If $E(\mathbb{Q})^{\wedge p} \to H^1_f(\mathbb{Q}, T_pE)$ is an isomorphism we have $T_pШ(\mathbb{Q}, E)[p^\infty] = 0$. But it is well-known that $Ш(\mathbb{Q}, E)[p^N]$ is a finite group for every N (see [**Mi**] Remark 6.7), which implies that $Ш(\mathbb{Q}, E)[p^\infty]$ is an extension of a finite group by divisible groups of the form $\mathbb{Q}_p/\mathbb{Z}_p$. If $T_pШ(\mathbb{Q}, E)[p^\infty] = 0$ then the divisible part of $Ш(\mathbb{Q}, E)[p^\infty]$ must be zero. □

LECTURE 3

The relation to the Birch-Swinnerton-Dyer conjecture

In this last lecture we show that the equivariant Tamagawa number conjecture for the motive $M = h_1(E)(1)$ is equivalent to the Birch-Swinnerton-Dyer conjecture. At the end we review some results on elliptic curves, which were needed for the computation of the unramified cohomology.

1. The Tamagawa number and the Birch-Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $M = h_1(E)(1)$ (as always $i = 1$). 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 12.

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

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

Definition 27. Let

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

where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ defined in Theorem 6 and $E(\mathbb{R})^0$ is the connected component of $E(\mathbb{R})$. Note that $c_v = 1$ for almost all v.

Remark 13. 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*

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

where Ω_∞ is the period of E from Example 6.

We can now formulate the main theorem of these lectures:

Theorem 3 (Main theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, $M = h_1(E)(1)$ and $A = \mathbb{Q}$.*

(1) *Conjectures 1, 2, 3 and 5 hold for M.*

(2) *Conjecture 4 on the order of vanishing of $L(E, s)$ at $s = 1$ is equivalent to part a) of the BSD conjecture.*

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

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

(4) *Conjecture 7 holds for p if and only if $Ш(E/\mathbb{Q})[p^\infty]$ is finite.*

(5) *The ETNC (Conjecture 8) for M and all p is equivalent to part b) of the BSD conjecture.*

We prove here (1)-(4). Part (5) is proven in Section 4.

Proof of (1)-(4). The statement in (1) just repeats Examples 7, 9 and 12. For (2) using Example 7, Conjecture 4 says for $M = h_1(E)(1)$ that

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

if we observe that $L(M,s) = L(E, s+1)$. This proves (2).

We show (3). The fundamental line of M is

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

Let $\underline{x}^\vee := (x_1^\vee, \dots, x_r^\vee)$ be the basis of $(E(\mathbb{Q})^{\mathrm{free}})^\vee$ dual to $\underline{x} := (x_1, \dots, x_r)$ 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 4. We define $\beta \in \Delta(M)$ to be the element

$$\beta := (x_1 \wedge \dots \wedge x_r)^{-1}(x_1^\vee \wedge \dots \wedge x_r^\vee)(\mathrm{cl}_{E(\mathbb{R})^0})^{-1}(\omega^\vee) \in \Delta(M).$$

A possible zeta element $\zeta_\mathbb{Q}(M)$ is necessarily a rational multiple of β, i.e., of the form $\zeta_\mathbb{Q}(M) = q\beta$, with $q \in \mathbb{Q}^\times$, Conjecture 6 is now equivalent to the fact that

$$q\theta_\infty(\beta) = (L(M,0)^*)^{-1} \in \mathbb{R}^\times.$$

By definition of θ_∞ we get that

$$\theta_\infty(\beta) = (\Omega_\infty R(E/\mathbb{Q}))^{-1} \in \mathbb{R}^\times.$$

Thus

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

Finally, (4) is the content of Example 16. □

2. The 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. Fix a prime number p. We denote by S the union of the finite set of places where E has bad reduction and of p, ∞.

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

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

Note that one has an exact sequence

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

Definition 29. For any topologically abelian group H, we let

$$H^* := \mathrm{Hom}_{\mathrm{ct}}(H, \mathbb{Q}_p/\mathbb{Z}_p),$$

where $\mathbb{Q}_p/\mathbb{Z}_p$ has the discrete topology.

Now we can describe the determinant of the complex $R\Gamma_c(\mathbb{Z}_S, T_pE)$ more explicitly. First note that by (3) and Lemma 3, we can write

$$\text{(2)} \quad \mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_c(\mathbb{Z}_S, V_pE)) \cong \mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_f(\mathbb{Q}, V_pE)) \cdot \mathrm{Det}_{\mathbb{Q}_p}(H^1_f(\mathbb{Q}_p, V_pE)) \cdot \mathrm{Det}^{-1}_{\mathbb{Q}_p} V_pE^+.$$

Theorem 4. *There is a canonical isomorphism*

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

which induces after $\mathbb{Q}_p \otimes_{\mathbb{Z}_p}$ the isomorphism in (2).

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

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

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

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

Taking the inverse limit of the Tate duality pairing in Theorem 7 one gets $E(\mathbb{Q}_v)^{\wedge p} \cong H^1(\mathbb{Q}_v, E)[p^\infty]^*$ and a commutative diagram

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

where the right row is exact by Lemma 4 below. 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

$$
\begin{aligned}
0 \to & H^1_f(\mathbb{Q}, T_pE) \to H^1(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} T_pH^1(\mathbb{Q}_v, E) \to \\
\to & \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^* \to H^2(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, T_pE) \to \\
\to & H^0(\mathbb{Z}_S, E[p^\infty])^* \to 0.
\end{aligned} \tag{3}
$$

Here by Definition 22 and Theorem 1, the kernel of the map from $H^1(\mathbb{Z}_S, T_pE)$ to $\bigoplus_{v\in S} T_pH^1(\mathbb{Q}_v, E)$ is $H^1_f(\mathbb{Q}, T_pE)$. 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)

$$
\begin{aligned}
0 \to H^0(\mathbb{R}, T_pE) \to & H^1_c(\mathbb{Z}_S, T_pE) \to H^1(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, T_pE) \to \\
\to & H^2_c(\mathbb{Z}_S, T_pE) \to H^2(\mathbb{Z}_S, T_pE) \to \bigoplus_{v\in S} H^2(\mathbb{Q}_v, T_pE) \to \\
\to & H^3_c(\mathbb{Z}_S, T_pE) \to 0.
\end{aligned} \tag{4}
$$

Taking $\mathrm{Det}_{\mathbb{Z}_p}$ of the exact sequences in Equations (3) and (4) gives the desired result. $\square$

Finally, we give prove that the Selmer group can be described also as a subgroup of $H^1(\mathbb{Z}_S, E[p^\infty])$ as was needed in the proof of Theorem 4

Lemma 4. *The inclusion* $H^1(\mathbb{Z}_S, E[p^\infty]) \subset H^1(\mathbb{Q}, E[p^\infty])$ *induces an isomorphism*

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Z}_S, E[p^\infty]) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, E)[p^\infty]) \right).$$

PROOF. We claim that

$$H^1(\mathbb{Z}_S, E[p^\infty]) = \ker\left(H^1(\mathbb{Q}, E[p^\infty]) \to \prod_{v\notin S} H^1(\mathbb{Q}_v, E)[p^\infty]) \right).$$

Accepting the claim, consider the kernel-cokernel sequence (cf. [**Mi**] Proposition 0.24) of the composition

$$H^1(\mathbb{Q}, E[p^\infty]) \to \prod_v H^1(\mathbb{Q}_v, E)[p^\infty]) \to \prod_{v\notin S} H^1(\mathbb{Q}_v, E)[p^\infty]),$$

which gives with the claim an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to H^1(\mathbb{Z}_S, E[p^\infty]) \to \bigoplus_{v\in S} H^1(\mathbb{Q}_v, E)[p^\infty]).$$

This is the statement of the lemma. To prove the claim, note that by the same argument as in the proof of 2 we have an exact sequence

$$0 \to H^1(\mathbb{Z}_S, E[p^\infty]) \to H^1(\mathbb{Q}, E[p^\infty]) \to \prod_{v\notin S} H^1(I_v, E[p^\infty])$$

(recall that I_v acts trivially on $E[p^\infty]$ as $v \notin S$ and that E has good reduction outside of S). It follows from Theorem 6 that $E(\overline{\mathbb{Q}}_v)^{I_v} = E(\mathbb{Q}_v^{\mathrm{unr}})$ is p-divisible, so that $H^1(I_v, E[p^N]) \to H^1(I_v, E)$ is injective for every N (consider the long exact cohomology sequence of the Kummer sequence). We get a commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(\mathbb{Z}_S, E[p^\infty]) & \longrightarrow & H^1(\mathbb{Q}, E[p^\infty]) & \longrightarrow & \prod_{v\notin S} H^1(I_v, E[p^\infty]) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{v\notin S} H^1(\mathbb{F}_v, E^{I_v})[p^\infty] & \longrightarrow & \prod_{v\notin S} H^1(\mathbb{Q}_v, E)[p^\infty] & \longrightarrow & \prod_{v\notin S} H^1(I_v, E)[p^\infty]. \end{array}$$

As the right vertical arrow is injective, the claim follows if we can show that $H^1(\mathbb{F}_v, E(\mathbb{Q}_v^{\mathrm{unr}}))[p^\infty] = 0$. As $E_1(\mathbb{Q}_v^{\mathrm{unr}})$ is uniquely p-divisible by Theorem 6 the long exact cohomology sequence of

$$0 \to E_1(\mathbb{Q}_v^{\mathrm{unr}}) \to E(\mathbb{Q}_v^{\mathrm{unr}}) \to \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) \to 0$$

shows that $H^1(\mathbb{F}_v, E(\mathbb{Q}_v^{\mathrm{unr}}))[p^\infty] \cong H^1(\mathbb{F}_v, \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v))[p^\infty]$. Now we use the interpretation of $H^1(\mathbb{F}_v, \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v))$ by principal homogeneous spaces (see [**Si**] X §3). We have to show that each principal homogeneous spaces C of E has an $\mathbb{F}_v$-rational point. This follows by Lang's trick: let $x \in C(\overline{\mathbb{F}}_v)$, then there exists $p \in E(\overline{\mathbb{F}}_v)$ such that $p+x = Fx$, where F is the Frobenius. As $\mathrm{id}-F$ is an isogeny of E, there exist $q \in E(\overline{\mathbb{F}}_v)$ with $p = q - Fq$. This implies $q + x = Fq + Fx = F(q + x)$, where the last equality holds because the action $E \times C \to C$ is Frobenius equivariant. Thus, $q + x \in C(\mathbb{F}_v)$. □

3. Local Tamagawa numbers

In this section we study how the integral structure $E(\mathbb{Q}_v)^{\wedge p}$ behaves under the identification (4):

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

Recall that by Theorem 1

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

Theorem 5. *With the above notations one has*

$$\iota_v(\mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p})) = \begin{cases} c_v^{-1}\mathbb{Z}_p & \text{if } v \neq p, \infty \\ c_p^{-1}\omega^\vee\mathbb{Z}_p & \text{if } v = p. \end{cases}$$

Proof. We treat first the case $v \neq p$. Recall from Lemma 5 in Section 5 the exact sequence

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

As $E_1(\mathbb{Q}_v)^{\wedge p} = 0$ for $v \neq p$, 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

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

As $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pE^{I_v} = V_pE^{I_v}$ it follows from the definition of ι_v that

$$\iota_v(\mathrm{Det}^{-1}_{\mathbb{Z}_p}(T_pE^{I_v}) \cdot \mathrm{Det}_{\mathbb{Z}_p}(T_pE^{I_v})) = \mathbb{Z}_p.$$

The determinant computation for finite $\mathbb{Z}_p$-modules in Example 11 shows that $\iota_v(\mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p})) = c_v^{-1}\mathbb{Z}_p$ because

$$c_v^{-1}\mathbb{Z}_p = \#(E(\mathbb{Q}_v)^{\wedge p}/E_0(\mathbb{Q}_v)^{\wedge p})^{-1}\mathbb{Z}_p.$$

This settles the case $v \neq p$. Consider $v = p$ 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

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

we have

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

where ϕ is the Frobenius on $D_{\mathrm{cris}}(V_pE)$. Indeed, consider the complex

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

We get

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

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

(5) $$\mathrm{triv} : \mathrm{Det}^{-1}_{\mathbb{Q}_p}[D_{\mathrm{cris}}(V_pE) \xrightarrow{(1-\phi)} D_{\mathrm{cris}}(V_pE)] = \\ = \mathrm{Det}^{-1}_{\mathbb{Q}_p}(D_{\mathrm{cris}}(V_pE)) \cdot \mathrm{Det}_{\mathbb{Q}_p}(D_{\mathrm{cris}}(V_pE)) = \mathrm{Det}_{\mathbb{Q}_p}(0)$$

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

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

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

Using Proposition 2 in Section 5, the map $\exp_{\mathrm{BK}}$ is given by the exponential map $\exp : \mathrm{Lie}E_{\mathbb{Q}_p} \to E_1(\mathbb{Q}_p) = \widehat{E}(p\mathbb{Z}_p)$. Let $q = p$ if $p \neq 2$ and $q = 4$ if $p = 2$. Then by our choice of basis $\omega^\vee \in \mathrm{Lie}E$ one gets an isomorphism $\exp : q\omega^\vee\mathbb{Z}_p \cong \widehat{E}(q\mathbb{Z}_p)$ by Theorem 6. This gives

$$\exp_{\mathrm{BK}}^{-1}(\mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p})) = \#(E(\mathbb{Q}_p)^{\wedge p}/\widehat{E}(q\mathbb{Z}_p))^{-1}q\omega^\vee\mathbb{Z}_p = \\ = \#(E(\mathbb{Q}_p)^{\wedge p}/E_0(\mathbb{Q}_p)^{\wedge p})^{-1}c_p^{-1}\#\widetilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)^{-1}p\omega^\vee\mathbb{Z}_p.$$

Here the last equality holds, because $\widehat{E}(q\mathbb{Z}_p) = E_1(\mathbb{Q}_p)^{\wedge p}$ for $p \neq 2$ and has index 2 if $p = 2$. As Conjecture 2 holds in our case for all v, we have $\det(1-\phi) = \frac{\#\widetilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)}{p}$. This gives

$$\iota_p(\mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_p)^{\wedge p})) = c_p^{-1}\omega^\vee\mathbb{Z}_p.$$

□

4. Proof of the Main Theorem

Here we finish the proof of the Main Theorem 3.

Proof of (5) of Theorem 3. Recall from the proof of Theorem 3 (3) that $\zeta_{\mathbb{Q}}(M) = q\beta$, with

$$\beta := (x_1 \wedge \ldots \wedge x_r)^{-1}(x_1^\vee \wedge \ldots \wedge x_r^\vee)(\mathrm{cl}_{E(\mathbb{R})^0})^{-1}(\omega^\vee) \in \Delta(M)$$

and that

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

Let us identify the lattice

$$\begin{aligned}(6)\quad \mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)) \cong \mathrm{Det}^{-1}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}, T_pE)) \cdot \mathrm{Det}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})^*)\cdot \\ \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(H^0(\mathbb{Z}_S, E[p^\infty])^*) \cdot \prod_{v\in S} \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p}) \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(T_pE^+),\end{aligned}$$

of $\mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_c(\mathbb{Z}_S, V_pE))$. By Theorem 2 and because $E(\mathbb{Q})$ is finitely generated, 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

$$\mathrm{Det}^{-1}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}, T_pE)) \cong \mathrm{Det}^{-1}_{\mathbb{Z}_p}(E(\mathbb{Q})^{\mathrm{free}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cdot \mathrm{Det}^{-1}_{\mathbb{Z}_p}(E(\mathbb{Q})[p^\infty])$$

and $\#E(\mathbb{Q})[p^\infty](x_1 \wedge \ldots \wedge x_r)^{-1}$ is a generator of this lattice. Taking the dual of the sequence in (2), one gets

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

This gives

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

and $(\#Ш(E/\mathbb{Q})[p^\infty])^{-1}(x_1 \vee \wedge \ldots \wedge x_r^\vee)$ generates this lattice. Putting these results together and using that $H^0(\mathbb{Z}_S, E[p^\infty]) = E(\mathbb{Q})[p^\infty]$, we get

$$\begin{aligned}(7)\quad &\mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)) \cong \\ &\frac{(\#E(\mathbb{Q})[p^\infty])^2}{\#Ш(E/\mathbb{Q})[p^\infty]}(x_1 \wedge \ldots \wedge x_r)^{-1}(x_1^\vee \wedge \ldots \wedge x_r^\vee)(\mathrm{cl}_{E(\mathbb{R})^0})^{-1} \prod_{v\in S} \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p})\end{aligned}$$

inside $\mathrm{Det}_{\mathbb{Q}_p}(R\Gamma_c(\mathbb{Z}_S, V_pE))$. With Theorem 5, we see that $\theta_{p,S}$ maps $\prod_{v\in S} c_v^{-1}\omega^\vee \mathbb{Z}_p$ to $\prod_{v\in S} \mathrm{Det}_{\mathbb{Z}_p}(E(\mathbb{Q}_v)^{\wedge p})$. Taking everything together, this implies that

$$\frac{(\#E(\mathbb{Q})[p^\infty])^2}{\#Ш(E/\mathbb{Q})[p^\infty]} \prod_{v\in S} c_v^{-1}\theta_{p,S}(\beta)\mathbb{Z}_p = \mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)).$$

Thus, $\theta_{p,S}(\zeta_{\mathbb{Q}}(M))\mathbb{Z}_p = q\theta_{p,S}(\beta)\mathbb{Z}_p$ equals $\mathrm{Det}_{\mathbb{Z}_p}(R\Gamma_c(\mathbb{Z}_S, T_pE)$ if and only if

$$\frac{L(M,0)^*}{\Omega_\infty R(E/\mathbb{Q})} = q^{-1} = \frac{\#Ш(E/\mathbb{Q})[p^\infty]}{(\#E(\mathbb{Q})[p^\infty])^2} \prod_{v\in S} c_v.$$

This holds for all p if and only if the BSD conjecture holds. □

5. Appendix: Review of some results on elliptic curves

Here we collect some results on elliptic curves $E/\mathbb{Q}$, which we will need in these lectures. This section is independent from the rest of the text.

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 6 ([**Si**] 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*

$$E_1(K) \subset E_0(K) \subset E(K)$$

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

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

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* $E_1(K) = \widehat{E}(\mathfrak{m})$ *are the points of the formal group associated to* E*, where* $\mathfrak{m}$ *is the maximal ideal of* K. *The structure of* $\widehat{E}(\mathfrak{m})$ *is as follows: If the valuation* w *of* K *is normalized (i.e.,* $w(K^*) = \mathbb{Z}$*), then the logarithm induces an isomorphism* $\widehat{E}(\mathfrak{m}^r) \cong \mathfrak{m}^r$ *for all* $r > w(p)/(p-1)$ *and for all* $r \geq 1$ *one has an isomorphism* $\widehat{E}(\mathfrak{m}^r)/\widehat{E}(\mathfrak{m}^{r+1}) \cong \mathfrak{m}^r/\mathfrak{m}^{r+1}$.

Lemma 5. *For* $v \neq p$ *one has*

$$T_p E^{I_v} \cong T_p \widetilde{E}_v^{\mathrm{ns}}$$

and an exact sequence

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

Proof. The sequence in Theorem 6 for $K = \mathbb{Q}_v^{\mathrm{unr}}$ gives

$$0 \to E_1(\mathbb{Q}_v^{\mathrm{unr}}) \to E_0(\mathbb{Q}_v^{\mathrm{unr}}) \to \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) \to 0.$$

As $v \neq p$, the group $E_1(\mathbb{Q}_v^{\mathrm{unr}})$ is uniquely p-divisible so that one has for all n an isomorphism $E_0(\mathbb{Q}_v^{\mathrm{unr}})[p^n] \cong \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v)[p^n]$. This implies

$$T_p E_0(\mathbb{Q}_v^{\mathrm{unr}}) \cong T_p \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) = T_p \widetilde{E}_v^{\mathrm{ns}}.$$

As $E(\mathbb{Q}_v^{\mathrm{unr}})/E_0(\mathbb{Q}_v^{\mathrm{unr}})$ is finite, one has $T_p E_0(\mathbb{Q}_v^{\mathrm{unr}}) = T_p E(\mathbb{Q}_v^{\mathrm{unr}})$ and one gets

$$T_p E^{I_v} = T_p E(\mathbb{Q}_v^{\mathrm{unr}}) = T_p E_0(\mathbb{Q}_v^{\mathrm{unr}}) \cong T_p \widetilde{E}_v^{\mathrm{ns}}.$$

This proves the first claim. For the exact sequence, consider the p^n-multiplication on the exact sequence

$$0 \to \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v) \to \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) \xrightarrow{1-\mathrm{Frob}_v^{-1}} \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v) \to 0.$$

Then the snake lemma gives

$$0 \to \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)[p^n] \to \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v)[p^n] \xrightarrow{1-\mathrm{Frob}_v^{-1}} \widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v)[p^n] \to \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)/p^n \widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v) \to 0,$$

as $\widetilde{E}_v^{\mathrm{ns}}(\overline{\mathbb{F}}_v)$ is p-divisible. Taking $\varprojlim_n$ gives the desired sequence as T_p applied to the finite group $\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)$ is 0. □

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

Theorem 7 (see [**Mi**] I 3.4 and I 3.7)**.** *For any place* v *of* $\mathbb{Q}$ *one has a perfect pairing*

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

Proof. For finite v this is [**Mi**] I 3.4. For $v = \infty$, the result in [**Mi**] I 3.7 gives a perfect pairing

$$\pi_0(E(\mathbb{R})) \times H^1(\mathbb{R}, E) \to \mathbb{Q}_2/\mathbb{Z}_2,$$

where $\pi_0(E(\mathbb{R})) = E(\mathbb{R})/E(\mathbb{R})^0$. Note that both groups in this pairing are 2-torsion. This is clear for $H^1(\mathbb{R}, E)$ and for $\pi_0(E(\mathbb{R}))$ it follows from the fact that the trace map $E(\mathbb{C}) \to E(\mathbb{R})$ is a continuous map of Lie groups, whose image is a closed connected subgroup of $E(\mathbb{R})$, which contains $2E(\mathbb{R})$ because this is the image of $E(\mathbb{R})$ under the trace map. Thus, the image of the trace map is also open in $E(\mathbb{R})$ and hence equal to $E(\mathbb{R})^0$ and $2E(\mathbb{R}) \subset E(\mathbb{R})^0$. As a connected, compact and commutative Lie group, we have $E(\mathbb{R})^0 \cong \mathbb{R}/\mathbb{Z}$, which is divisible. It follows that for each prime p, we have $\pi_0(E(\mathbb{R}))/p^n\pi_0(E(\mathbb{R})) \cong E(\mathbb{R})/p^nE(\mathbb{R})$, which proves the statement in the theorem. $\square$

Bibliography

[BK] 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.

[Bo] A. Borel, Stable real cohomology of arithmetic groups, Ann. Sci. ENS 7 (1974) 235-272.

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

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

[FP] 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

[FK] 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.

[HK1] 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.

[HK2] A. Huber and G. Kings, Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters, Duke Math. J., 119 (2003) 393-464.

[Ja] U. Jannsen, Deligne homology, Hodge-$\mathcal{D}$-conjecture and motives, in: Beilinson's conjectures on special values of L-functions, Academic Press (1988).

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

[KM] F. Knudsen, D. Mumford, The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'div', Math. Scand. (1976), 39:19– 55.

[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)

[Sa] T. Saito, Modular forms and p-adic Hodge theory, Invent. Math. 129 (1979) 607-620.

[Sc1] A. J. Scholl, Classical motives, In: Motives, PSPM vol. 55 I (1994) 163-187.

[Sc2] 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

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

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

[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.