University of Nottingham
UK | CHINA | MALAYSIA

Special Case of Bloch-Kato Conjecture

Daria Shchedrina

Thesis submitted to the University of Nottingham
for the degree of Master of Philosophy

November 2022

My thesis is dedicated to the Oak in Wollaton park, who provided me with quietness and peace during years in Nottingham.

Abstract

We prove that the conjecture of Birch and Swinnerton-Dyer for elliptic curves over the field of rational numbers follows from the Bloch and Kato Tamagawa number conjecture for motives in a direct way.

Acknowledgements

I am the most grateful to all my friends climbers and highliners who supported me in the most difficult time and who suggested not to throw away my PhD, but finish it instead and do something else afterwards.

I am especially grateful to one of my climbing partners, Vadim Vologodsky for helping me to understand p-adic Hodge theory and helping to find and correct many mistakes in the first version of the thesis. He also suggested possible generalization of results for abelian varieties.

I am very grateful to my boyfriend Alexey, my mom Olga, and my cats: Motya, Gavriusha, and Barty, who offered me the best mental support during time when I was writing this thesis, and who are to certain degree my co-authors.

Major part of this thesis has been written during COVID-19 lockdowns in 2020 and 2021. As a PhD student in Nottingham I had financial support provided by Vice-Chancellors Scholarship for research excellence during years 2016-2019.

Contents

Introduction

This thesis is focused on algebraic varieties called elliptic curves, which is probably the most well studied object after projective space. We will consider various conjectures about elliptic curves and try to relate these conjectures to each other. Throughout the thesis we assume that an elliptic curve E we are working with is defined over the field of rational numbers $\mathbb{Q}$.

Assumption 0.1. *Denote by N_E the conductor of E, it is the product of all primes of bad reduction of E with exponents given by Ogg's formula. By the theorem of Breuil-Conrad-Diamond-Taylor [Bre+01] and Wiles [Wil95] such an elliptic curve is modular, which means*

- *There exists a rational morphism $\iota_E : X_0(N_E) \to E$ which sends the ∞ cusp into the origin (identity element) $O \in E$.*
- *There exists a modular form f corresponding to the isogeny class of E. More precisely there exists a weight 2 newform $f \in S_2(\Gamma_0(N_E))$ such that the Fourier expansion $f = \sum_{n=1}^{\infty} a_n q^n$ has coefficients in $\mathbb{Z}$ and $L(E,s) = L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. We will define precisely what $L(E,s)$ is in the first couple of chapters.*

From the number-theoretic point of view the main object related to an elliptic curve is its Mordell-Weil group $E(K)$ for a number field K. It turns out to be more helpful to embed $E(K)$ into a subgroup of $H^1(K, E(\overline{K})_{tors})$ cut out by local conditions rather then just working directly with $E(K)$.
In the first chapter we introduce classical Selmer group and Tate-Shafarevich group as the cokernel in the short exact sequence 1.3. We will generally assume

the Tate-Shafarevich group $Ш(E/K)$ to be finite in all statements, except from the very last subsection where we prove under certain conditions that the p-primary part of $Ш(E/K)[p^\infty]$ is finite.

The second chapter is about Hasse-Weil L-functions. We only recall main definitions and statements following lecture notes of Kato [Kat93]. After recalling useful lemmas about determinants from [KM76] we define local $L-$factors and compute them for the case of an elliptic curve E over $\mathbb{Q}$.

After defining L-functions we are ready to formulate one of the major conjectures of the XX century, namely the Birch and Swinnerton-Dyer conjecture.

In the fourth chapter we consider the Mazur-Tate conjecture for elliptic curves. We closely follow [MT87], sometimes referring to [MT83] and [MTT86]. Now instead of the L-function we work with the modular element. The Theorem of Birch and Stevens 4.3 suggests a relation between modular elements and the L-function. The major aim of this section is to understand a different way to define Neron-Tate height pairing, see Theorem 4.12.

We end the chapter with the Conjecture 4.17 which gives a formula for the rank of the modular element in its first part. Note that under mild conditions the first part of the Mazur-Tate conjecture is the theorem of Ota [Ota18] (Theorem 1.2).

In the Chapter 5 we study Beilinson's conjectures; in this text we consider only the case of a motive $\mathcal{M} = H^i(X)(j)$ of weight $w = i - 2j = -1$ coming from an algebraic variety X. We define the local link pairing following the main reference for this chapter [Bei87], we then formulate conjectures of Beilinson 5.3 related to the local link pairing and the conjecture of Swinnerton-Dyer 5.5. A conjecture of this type was first stated by P. Deligne in [Del79] for motives of weight $w < -2$, then A. Beilinson added a different formulation for the case of weight -1.

The main result of this chapter is the Proposition 5.10 where we prove that the local link pairing defined by A. Beilinson in [Bei87] is the same as the intersection pairing appearing in the Mazur-Tate conjecture, and therefore by

the Theorem 4.12 and the Theorem of S. Bloch in [Blo80] it is the same as the Neron-Tate height pairing. We also mention in the Remark 5.8 the result of Deligne about computation of the determinant of the period matrix in the case of an elliptic curve.

The next chapter is about the first conjecture of Bloch and Kato about the order of vanishing. We define local Bloch-Kato Selmer groups for cases when $v|p$ and $v \nmid p$ and describe their structure for elliptic curves in Lemmas 6.7, 6.3. We describe the image of the Kummer map in terms of Bloch-Kato Selmer group in Lemmas 6.3 and 6.7. Afterwards we prove that the first part of BSD conjecture follows from the Bloch-Kato Conjecture 6.4, which was also done in [Bel09].

The seventh chapter is about the rings of periods as defined by Fontaine in [Fon94b]; they are needed for the formulation of comparison theorems in p-adic Hodge theory and for the forthcoming chapter on Dieudonne theory. We recall all the necessary definitions from classical articles [FF18], [Col19], [FO] and the Fundamental Exact Sequence 7.13 with its consequences 7.15, 7.16 which are crucial for establishing the relation between Bloch-Kato Selmer groups and L-functions. In the end of the chapter we prove an analogue of the Fundamental Exact Sequence for $\mathbf{B}_{st}$ instead of $\mathbf{B}_{cris}$ in the Lemma 7.16.

The chapter about Dieudonne modules is a collection of definitions of modules attached to a p-adic representation V corresponding to period rings from the previous chapter. We give a definition of an admissible representation and investigate in which situation the rational Tate module of an elliptic curve is crystalline, or semistable representation in the Lemma 8.2.

Afterwards we recall classical theorems on equivalence of categories between $\mathbf{B}_*$-admissible p-adic representations and the category $\mathcal{MF}^{ad}\varphi_K$ of filtered admissible φ-modules. We also write down formulas for the dimensions of all cohomology groups $H^1_*(K_v, V_p)$.

The last chapter is about the refined Bloch and Kato conjecture. This is the main part of the whole PhD thesis.

Implications of the Bloch-Kato conjecture have been studied before, in particular Guido Kings proved in [Kin03] that the Birch and Swinnerton-Dyer conjecture for elliptic curves follows from the Bloch-Kato Tamagawa number conjecture. The proof of Kings starts with the formulation of the Bloch-Kato conjecture in the way of Fontaine and Perrin-Riou via the fundamental line [FP94]. Note that the formulation of the Bloch-Kato conjecture using the fundamental line is valid for motives of all weights, while the original Tamagawa number conjecture as in [BK90] was formulated only for motives of weights ≤ -1.

An equivariant version of the Tamagawa number conjecture has been studied in [Ven07], where the formula for the leading coefficient of the L-function of an abelian variety is proven to show the Birch and Swinnerton-Dyer formula up to an element of $\mathbb{Z}_p^\times$.

Our approach is different from Kings' in the way of being direct extraction of the terms in the Birch and Swinnerton-Dyer conjecture from the Tamagawa number formula without usage of the fundamental line. Essentially we take the formula from the Tamagawa number conjecture 9.42 and plug into it a lattice related to a motive coming from an elliptic curve. We consider each local item in the Tamagawa number formula separately and prove equality with the corresponding values in the second part of the Birch and Swinnerton-Dyer conjecture.

Under the assumption of finiteness of the Tate-Shafarevich group and Beilinson's conjecture 5.7 we prove the following Theorem 9.46.

Theorem 0.2. *For the case of $\mathcal{M} = h^1(E)(1)$ with $V = V(E)$ and $D = H^1_{dR}(E/\mathbb{Q})$ the conjecture 3.5 follows from the Tamagawa number conjecture 9.42.*

While most of computations for the particular case of an elliptic curve are easy, some have been quite hard to deduce. The most interesting part was the computation of measures of the local Bloch-Kato Selmer groups $H^1_f(\mathbb{Q}_p, V_l E)$ for all possible cases of p and l in Lemmas 9.8, 9.12 and Corollaries 9.9, 9.14.

The BSD conjecture in its greatest generality was formulated for an abelian variety over a number field. The presented solution can also be generalised for an abelian variety over $\mathbb{Q}$ instead of elliptic curves. All the key statements in chapters 1 to 8 hold for the case of abelian variety with slightly more complicated proofs. The analogue of the Lemma 9.34 is proven in [Jor05], so for the motive $\mathcal{M} = h^1(A)$ assigned to an abelian variety A over $\mathbb{Q}$ the L-function $L(A, s)$ converges absolutely to a holomorphic function for $\mathrm{Re}(s) > \frac{3}{2}$.
However an obstruction occurs in the Lemma 9.16, more precisely in the proof of the Fact 9.18, where in the case of abelian variety one has to deal with Raynaud extensions instead of Tate uniformization and in that case there is no analogue of Kodaira-Neron theorem. I believe that results of section 9.2.1 can be proven for abelian varieties in a way similar to elliptic curves.

Chapter 1

Selmer groups

For the rest of the chapter we fix a prime p, we will set additional conditions on p from time to time.

This chapter is dedicated to the classical definition of the Selmer group and its main properties. Let E be an elliptic curve over a number field K. Denote as usual $G_K := \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group, which acts on $E[m]$, for any integer m and on $E(\overline{K})$. For a short exact sequence

$$0 \to E[m] \to E(\overline{K}) \stackrel{[m]}{\to} E(\overline{K}) \to 0$$

we consider corresponding long exact sequence by taking Galois cohomology

$$0 \to E(K)[m] \to E(K) \to E(K) \to H^1(G_K, E(\overline{K})[m]) \to$$
$$\to H^1(G_K, E(\overline{K})) \to H^1(G_K, E(\overline{K})) \to ...$$

and deduce from it the Kummer sequence:

$$0 \to E(K)/mE(K) \to H^1(G_K, E(\overline{K})[m]) \to H^1(G_K, E(\overline{K}))[m] \to 0$$

to extract the Kummer map $\kappa : E(K) \to H^1(G_K, E(\overline{K})[m])$. This map can be defined explicitly in the following way.

Construction 1.1. *We take a point $P \in E(K)$ and consider a point $Q \in$*

$E(\overline{K})$ such that $mQ = P$. We then send P into a cocycle ξ_P which works on $\sigma \in G_K$ as $\xi_P : \sigma \mapsto Q^\sigma - Q$.

We would like to look at $m = p^n$ for various n to get Kummer maps $\kappa : E(K)/p^nE(K) \to H^1(K, E(\overline{K})[p^n])$. After taking the direct limit over all n we obtain $\kappa : E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K, E[p^\infty])$.
In a similar way one can get a local map: namely for a prime η of K define K_η as the union of all η-adic completions of all finite extensions of K containing in K, then the local Kummer map is $\kappa_\eta : E(K_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_\eta, E[p^\infty])$.
In order to define a Selmer group of an elliptic curve over a number field K we look at the Kummer sequence for K and for a local field K_η and consider a commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K, E(\overline{K})[m]) & \longrightarrow & H^1(K, E(\overline{K}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_\eta)/mE(K_\eta) & \longrightarrow & H^1(K_\eta, E(\overline{K_\eta})[m]) & \longrightarrow & H^1(K_\eta, E(\overline{K_\eta}))[m] & \longrightarrow & 0. \end{array}$$

Take the direct limit over all m, bearing in mind $E(K)/mE(K) \simeq E(K) \otimes \mathbb{Z}/m\mathbb{Z}$ we get the following diagram combined from local and global Kummer exact sequences.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \longrightarrow & H^1(K, E(\overline{K})_{tors}) & \longrightarrow & H^1(K, E(\overline{K})) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_\eta) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} & \longrightarrow & H^1(K_\eta, E(\overline{K_\eta})_{tors}) & \longrightarrow & H^1(K_\eta, E(\overline{K_\eta})) & \longrightarrow & 0. \end{array}$$

We can see from these sequences how the yorsion-free part of the Mordell-Weil group embeds into the cohomology group $H^1(K, E(\overline{K})_{tors})$. It would have helped with studying $E(K)$ if this cohomology group was not so huge, so we cut it by local conditions by the diagram above.

Definition 1.2. *We define the Selmer group of E over K as the kernel of the map from global cohomology group into the product of local ones*

$$\mathrm{Sel}(E/K) := \ker(H^1(K, E(\overline{K})_{tors}) \to \prod_\eta H^1(K_\eta, E(\overline{K_\eta})_{tors})/\operatorname{Im}(\kappa_\eta)) \quad (1.1)$$

In case if we take only powers of p instead of all integer m following the same procedure leads to the

Definition 1.3. *The p-primary subgroup of the Selmer group for E over K. This one will be main object of our interest.*

$$\mathrm{Sel}(E[p^\infty]/K) = \ker(H^1(K, E[p^\infty]) \to \prod_\eta H^1(K_\eta, E[p^\infty])/E(K_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \tag{1.2}$$

Aside from the Selmer group we will also need the Tate-Shafarevich group for E/K. This mysterious group is participating in the BSD conjecture and it has generalized analogue for a motive instead of elliptic curve — the Bloch-Kato Shafarevich group which we will define in corresponding chapter.
One can think of elements of the Selmer group as principal homogeneous spaces that have K_η point for every η. On the other hand Tate-Shafarevich group encodes homogeneous spaces which have K_η point for every η, but do not have K-rational points.

Definition 1.4. *For an elliptic curve E over a number field K we define the Tate-Shafarevich group as*

$$Ш(E/K) := \ker(H^1(K, E(\overline{K})) \to \prod_\eta H^1(K_\eta, E(\overline{K_\eta})))$$

We define it in order to write down the fundamental exact sequence

$$0 \to E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}(E/K) \to Ш(E/K) \to 0 \tag{1.3}$$

Note that here tensoring with $(\mathbb{Q}/\mathbb{Z})$ just kills torsion. As well as everything else this short exact sequence has a p-primary part.

$$0 \to E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Sel}(E[p^\infty]/K) \to Ш(E/K)[p^\infty] \to 0 \tag{1.4}$$

The following theorem of Greenberg (theorem 2.4 in [Gre99]) provides a sim-

plification of the definition of the Selmer group above.

Theorem 1.5. *For K_η being either an algebraic extension of $\mathbb{Q}_l$, for $l \neq p$, or $\mathbb{C}$, or $\mathbb{R}$ the image of Kummer map $E(K_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ is trivial. For K_η being an algebraic extension of $\mathbb{Q}_p$ by theorem of Lutz* $\mathrm{Im}(\kappa_\eta) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_\eta:Q_p]}$.

From definition of the Selmer group and the Tate-Shafarevich group and especially from the fundamental exact sequence(1.4) one can see that they are needed for studying the Mordell-Weil group of elliptic curves. It is easier to understand Selmer groups, than Mordell-Weil groups directly, but the Tate-Shafarevich group is an obstruction to deducing properties of one from another. The conjecture by Tate and Shafarevich that $Ш(E/K)$ is finite is generally assumed in mathematical texts related to the subject, so we will as well assume $Ш(E/K)$ to be finite whenever needed.

Chapter 2

Hasse-Weil L-function

We begin with recollection about Hasse-Weil L-function. Later we will consider motivic L-function for more general conjectures and justify why the definition in this chapter is just a special case.
However in order to introduce L-factors properly we have to understand the concept of determinant so we recall definition and main properties of determinants in the next chapter, besides we will need them later on in discussion about sizes of groups and rational structures.

2.1 Determinants and integral structures

We follow [KM76] and [Kat93], a very good exposition of the theory is offered in [BB08]. Further on we denote by Λ a Noetherian, commutative, regular ring.

Definition 2.1. *Let P be a finitely generated projective module over Λ, we denote by $\mathcal{P}$ the corresponding quasi-coherent sheaf on* $\mathrm{Spec}(\Lambda)$*, which is locally free of finite rank. Let r be the rank of $\mathcal{P}$ then by* $\det_\Lambda P$ *we denote the Λ-module corresponding to rth exterior power of $\mathcal{P}$.*

An important example of determinant is when we start with $P = 0$, then $\det_\Lambda P = \Lambda$. The notion of determinant can be defined in greater generality when instead of a projective module over ring Λ one takes a perfect complex

over Λ.

Definition 2.2. *Let $P^\bullet$ be an object of the derived category of Λ-modules $\mathcal{D}\Lambda_{mod}$ represented by a perfect complex*

$$P^\bullet := ... \to P^q \to P^{q+1} \to ...$$

where P^qs are finite projective Λ-modules. Define

$$\det_\Lambda P^\bullet := \bigotimes_{q\in\mathbb{Z}} (\det_\Lambda P^q)^{(-1)^q}.$$

Immediately from definition we get for a complex of cohomology $H^\bullet(P^\bullet)$ the value of determinant:

$$\det_\Lambda H^\bullet(P^\bullet) = \det_\Lambda P^\bullet.$$

Moreover for a short exact sequence of (derived) modules

$$0 \to P_1^\bullet \to P^\bullet \to P_2^\bullet \to 0$$

we have an equality $\det P^\bullet = \det P_1^\bullet \otimes \det P_2^\bullet$. In the case we are working with usual finite projective modules over Λ we can view them as complexes centered at 0 degree.

Next step is to define the determinant with respect to a morphism.

Definition 2.3. *Let $f : P \to P$ be an automorphism of finite projective module P over Λ. Then one may view P as a perfect complex over Λ centered at degree 1, then $\det_\Lambda P$ is defined and it is a module of rank 1 over Λ. We denote by $\det_\Lambda(f; P)$ the element of Λ multiplication by which coincides with the map $\det_\Lambda P \to \det_\Lambda P$ induced by f.*

The above definition is the most important in case when we multiply by an element not invertible in Λ. The idea about integral structures is about presence of torsion in some cases. Here by integral structure we mean an $\mathcal{O}_K$-lattice in

a vector space over a complete discrete valuation field K. The definition above works only for modules that can not have torsion. However using projective resolutions 2.2 we can define the determinant for torsion modules as well.

Definition 2.4. *For Λ as above consider the fraction field $\mathrm{Frac}(\Lambda)$ and assume for P that $P \otimes \mathrm{Frac}(\Lambda) = 0$, then define the* ***characteristic ideal of*** *P $\mathrm{char}_\Lambda P$ to be the invertible ideal of Λ with the property: for any prime ideal $\mathfrak{p}$ of Λ the localization $\mathrm{char}_\Lambda P_\mathfrak{p}$ is the ideal $(\mathfrak{p}P_\mathfrak{p})^n$, where n is the length of $\Lambda_\mathfrak{p}$-module $P_\mathfrak{p}$.*

Then with the above definitions the theorem of Knudsen and Mumford holds

Theorem 2.5. *[KM76]*
The image of the composition

$$\det_\Lambda P \subset \det_\Lambda P \otimes_\Lambda \mathrm{Frac}(\Lambda) \simeq \det_\Lambda(P \otimes_\Lambda \mathrm{Frac}(\Lambda)) = \mathrm{Frac}(\Lambda)$$

coincides with the fractional ideal $(\mathrm{char}_\Lambda P)^{-1}$.

Example 2.6. *For a discrete valuation ring $\Lambda = \mathbb{Z}_p$ we have for an integer n a quasi-isomorphism $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq (p^n\mathbb{Z}_p \to \mathbb{Z}_p)$, thus $\det_{\mathbb{Z}_p}(\mathbb{Z}/p^n\mathbb{Z}) = p^{-n}\mathbb{Z}_p = |p^n|_p\mathbb{Z}_p$. This way for a general case of $\mathbb{Z}_p$-module P we get $\det_{\mathbb{Z}_p} P = |P_{tor}|_p \det_{\mathbb{Z}_p}(P/P_{tor})$, in future we will omit $\Lambda = \mathbb{Z}_p$ from notation.*

Lemma 2.7. *Let V be a finite dimensional vector space over $\mathbb{Q}_p$ and T be a $\mathbb{Z}_p$-lattice in V with an automorphism $f : V \to V$, such that $f(T) \subset T$. Then* $\det(\mathrm{coker} f) = |\det(f; T)|_p^{-1}\mathbb{Z}_p$.

Proof. Consider the complex $(V \xrightarrow{f} V)$ and a complex $(T \xrightarrow{f} T)$. Then the determinant of the first complex is isomorphic to the determinant of its cohomology complex, which is simply $\det 0 = \mathbb{Q}_p$. On the other hand the determinant of the second complex is $\det H^1(T \xrightarrow{f} T)^{-1} = (\det(\mathrm{coker} f|_T)^{-1})$ which equals to the determinant of the $\mathbb{Z}_p$-matrix representing morphism $f : T \to T$, namely $|\det(f; T)|_p^{-1}\mathbb{Z}_p$. □

2.2 Definition of L-function

We will be computing mainly the determinant of a map $1 - \mathrm{Fr}$, so for further we require construction of Frobenius as an element of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ corresponding to Frobenius morphism. The definition is classical, but we recall it here for future reference.

Construction 2.8. *We start with usual Frobenius map φ_p generating the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$ which is defined as $\varphi_p : x \mapsto x^p,\ x \in \overline{\mathbb{F}_p}$. The Frobenius map lifts to the ring of Witt vectors $\overline{\mathbb{Z}_p} := W(\overline{\mathbb{F}_p})$ and can be extended further to $W(\overline{\mathbb{F}_p})[\frac{1}{p}]$ which is nothing but $\mathbb{Q}_p^{nr}$ the maximal unramified extension of $\mathbb{Q}_p$. This way the Frobenius lifts to an element of $\mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p)$, we denote it by $\mathrm{Fr}_p = \varphi_p^{-1}$.*
Now consider the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We extend the p-adic valuation on $\mathbb{Q}$ to a valuation v on $\overline{\mathbb{Q}}$. Consider the decomposition group $\Gamma_v \subset G_{\mathbb{Q}}$ fixing v, it is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. We denote by $\mathrm{Fr}_p \in G_{\mathbb{Q}}$ a chosen lift of $\mathrm{Fr}_p \in \mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p)$ under this isomorphism.

From now on our main ring Λ is going to be of characteristic zero which can be represented as $\Lambda \simeq A \otimes \mathbb{Q}_l$ for some prime l and a ring A which is a finite product of finite extensions of $\mathbb{Q}$. We will also take into account a finite set of primes S which contains our fixed prime p.
In the rest of thesis we will work with V a finite dimensional $\mathbb{Q}_l$-vector space with a continuous action ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which is unramified outside finite set of prime numbers $S \ni p$.
Then for $l \notin S$ the local l-factor of the L-function of V with respect to A and S looks like

$$P_{\Lambda,p}(V,t) = \det_{\Lambda}(1 - \rho(\mathrm{Fr}_p^{-1})t; V^{I_p}) \in \Lambda[t] \tag{2.1}$$

Definition 2.9. • *We call the following **basic properties** for a quadruple (p, S, V, A): First, if for any prime number $l \notin S$ the polynomial $P_{\Lambda,p}(V,t)$ belongs to $A[t]$.*

Second property is when the product

$$L_{A,S}(V,s) = \prod_{l \notin S} P_{\Lambda,p}(V, l^{-s})^{-1}$$

for $s \in \mathbb{C}$ and l outside of S, converges absolutely in $A \otimes \mathbb{C}$ when $Re(s)$ is big enough.

- *We call the obtained function $L_{A,S}(V,s)$ the **L-function** of V with respect to A and S.*

We recall here here some general properties of this function:

1. Denote by $V(r) := V \otimes \mathbb{Q}_l(r)$ the rth Tate twist. If the quadruple (p, S, V, A) satisfies basic properties then $(p, S, V(r), A)$ does so as well. Moreover we have for L-function of the Tate twist $L_{A,S}(V(r), s) := L_{A,S}(V, s + r)$.

2. For a short exact sequence of $\mathbb{Q}_l$-vector spaces $0 \to V' \to V \to V'' \to 0$ with all $(p, S, V^?, A)$ satisfying basic properties we have $L_{A,S}(V, s) = L_{A,S}(V', s)L_{A,S}(V'', s)$.

Later we will be working with a vector spaces V equipped with a Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}_l}/\mathbb{Q}_l^{nr})$, so for this case we define $P_{\Lambda,p}(V,t) \in \Lambda[t]$ for $l \in S$ as:

Definition 2.10. *Local L-factor at primes where V is allowed ramification:*

$$\begin{cases} P_{\Lambda,p}(V,t) := \det_\Lambda(1 - \rho(\mathrm{Fr}_p^{-1})t);\ H^0(\mathrm{Gal}(\overline{\mathbb{Q}_l}/\mathbb{Q}_l^{nr}), V)) \text{ if } l \neq p, \\ P_{\Lambda,p}(V,t) := \det_\Lambda(1 - \phi_p^{-1}t; \mathbf{D}_{cris}(V)) \text{ if } l = p. \end{cases}$$

The next definition is of L-function as an Euler product of the above.

$$L_{A,\varnothing}(V,s) = L_A(V,s) := \prod_p P_{\Lambda,p}(V, p^{-s})^{-1}. \tag{2.2}$$

Remark 2.11. *We will see further that some l-adic representations better than others fit into this definition. The better ones are called crystalline, which*

means equality of dimensions $\dim \mathbf{D}_{cris}(V) = \dim V$. *However even if the representation is not crystalline and dimension of* $\mathbf{D}_{cris}(V)$ *is smaller, the definition stays the same.*

On definitions of $\mathbf{D}_{cris}$ and Frobenius operator ϕ_l see the chapter on Dieudonne modules. We omit A from notation if we are working with the field of rational numbers which would be our main case of concern. Let's have a look at an example of L-function. The main for us is to take instead of V the space of etale cohomology of a smooth elliptic curve E defined over $\mathbb{Q}$. We recall here a couple of classical results.

Fact 2.12. *For any prime* l *let* $V = H^1_{et}(E, \mathbb{Q}_l)$. *Then* V *is just the dual to the rational Tate module of* E *Tate-twisted by* -1.

Proof. First recall $H^1_{et}(E, \mathbb{Q}_l) := (\varprojlim_n H^1_{et}(E, \mathbb{Z}/l^n)) \otimes \mathbb{Q}_l$. It is a well known exercise on etale cohomology to compute $H^1_{et}(E, \mathbb{Z}/l^n)$. We have $E[l^n](\overline{\mathbb{Q}})$ the covering group for the etale covering map $l^n : E^* \to E$ which is cofinal among all etale covers $E' \to E$ of degree l^n, where E^* is the dual elliptic curve to E and they are isogenous. Therefore we get $H^1_{et}(E, \mathbb{Z}/l^n) \simeq \mathrm{Hom}(\pi_1^{et}(E), \mathbb{Z}/l^n) \simeq \mathrm{Hom}(E^*[l^n](\overline{\mathbb{Q}}), \mathbb{Z}/l^n)$. After taking inverse limits and using Weil pairing $E[l^n] \times E^*[l^n] \to \mu_{l^n}(\overline{\mathbb{Q}})$ we get

$$H^1_{et}(E, \mathbb{Z}_l) \simeq \mathrm{Hom}(\pi_1^{et}(E), \mathbb{Z}_l) \simeq \mathrm{Hom}(T_l E^*(-1), \mathbb{Z}_l)$$

Where the Tate twist is defined as $V(1) := V \otimes \mu_{p^\infty}(\overline{\mathbb{Q}})$. Plug this into the definition of the etale cohomology over $\mathbb{Q}_l$ to get $H^1_{et}(E, \mathbb{Q}_l) \simeq \mathrm{Hom}(V_l(E)(-1), \mathbb{Q}_l) = V_l(E)^\vee(-1)$. □

Now we would like to compute the L-function of E according to the above definition, i.e. compute $P_{\mathbb{Q}_l, p}(V_l(E)^{\vee I_p}, t)$ for all possible cases of l.

Lemma 2.13. *Right now we assume that* $l \neq p$. *The case of* $l = p$ *will be studied later after we define Dieudonne modules.*

1. *In the case of a prime p of good reduction for E we define*

$$P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p},t) = 1 - a_p t + pt^2;$$

2. *If E has split multiplicative reduction at p then*

$$P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p},t) = 1 - t$$

3. *If E has non-split multiplicative reduction at p then*

$$P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p},t) = 1 + t$$

4. *If E has additive reduction at p then*

$$P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p},t) = 1$$

Proof. The following is a recollection of [Har83], [Sil94], and [PRS11]. We start with primes $l \neq p$ of *good reduction* for E. Using Neron-Ogg-Shafarevich criterion we determine that $V_l(E) = H^1_{et}(E,\mathbb{Q}_l)$ is unramified at p if and only if E has good reduction at p. This means trivial action of inertia subgroup I_p of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on the rational Tate module $V_l(E)$. Denote by $\widetilde{E}$ the reduction of E over $\mathbb{F}_p$. As in the Construction 2.8 we denote by φ_p the Frobenius map which is a p-power on $\mathbb{F}_p$. Consider the morphism $\varphi_p : \widetilde{E} \to \widetilde{E}$ coming from the p-power on coordinates in $\overline{\mathbb{F}_p}(\widetilde{E})$ together with its lift $\varphi_{p,l} : V_l(\widetilde{E}) \to V_l(\widetilde{E})$. Since $V_l(\widetilde{E})$ is a 2-dimensional space over $\mathbb{Q}_l$ and $\varphi_{p,l}$ is a linear transform we can explicitly compute its characteristic polynomial

$$P_{\mathbb{Q}_l,p}(V_l(E),t) = \det(1 - \varphi_{p,l}^{-1}t) = 1 - \mathrm{Tr}\,\varphi_{p,l}t + \det\varphi_{p,l}t^2$$

A priori it has coefficients in $\mathbb{Z}_l[t]$, however by the theorem of Deligne [Har83] appendix C for smooth $\widetilde{E}$ we know that $P_{\mathbb{Q}_l,p}(V_l(E),t)$ is an element of $\mathbb{Z}[t]$.

By computations in [Sil09], chapter 5 we have $\operatorname{Tr}\varphi_{p,l} = 1 + p - |\widetilde{E}(\mathbb{F}_p)| = a_p$ and $\det\varphi_{p,l} = p$. Therefore we obtain the following explicit formula for the p-part of the L-function.

$$P_{\mathbb{Q}_l,p}(V_l(E),t) = 1 - a_p t + pt^2;$$

Moreover by the theorem of Deligne above we also know that both roots α_p, β_p of $P_{\mathbb{Q}_l,p}(V_l(E),t)$ satisfy $|\alpha_p| = |\beta_p| = \sqrt{p}$, then using Hasse inequality $a_p < 2\sqrt{p}$ we get the L-function as a product over all good reduction primes

$$L_{\mathbb{Q}_l,Good}(V_l(E),s) = \prod_{p\in\, Good} P_{\mathbb{Q}_l,p}(V_l(E),p^{-s})^{-1}.$$

This product converges absolutely for $\operatorname{Re}(s) > 3/2$ which means together with consequence of Deligne's theorem above that quadruple $(p, Good, V_l(E), \mathbb{Q}_l)$ satisfy basic properties from the definition of L-function.

We are left with cases of E having bad reduction at p. With the help of [Dar+13] chapter 3.3 we look at the action of inertia group I_p on $V_l(E)^\vee$ in various cases starting with *split multiplicative reduction* of E at p.

By Tate's uniformization we can write a Galois-equivariant short exact sequence:

$$1 \to q^{\mathbb{Z}} \to \overline{\mathbb{Q}_p}^{\times} \to E(\overline{\mathbb{Q}_p}) \to 0$$

. Denote by ζ_{l^n} the l^nth root of unity. Then it follows:

$$1 \to \mathbb{Z}/l^k\mathbb{Z}\zeta_{l^k} \to E(\overline{\mathbb{Q}_p})[l^k] \to \mathbb{Z}/l^k\mathbb{Z}\sqrt[l^k]{q} \to 0$$

Then the l^n-torsion subgroup $E[l^n]$ has a basis over $\mathbb{Q}_p$ represented by $\langle \zeta_{l^n}, q^{1/l^n}\rangle$ as a Galois module. We can write Galois action on $E[l^n]$ in this basis for $\sigma \in G_{\mathbb{Q}_p}$ as $\begin{pmatrix} \chi(\sigma) & * \\ 0 & 1 \end{pmatrix}$ where χ is the l-adic cyclotomic character. We obtain the following action of $G_{\mathbb{Q}_p}$ on the dual Tate module $V_l(E)^\vee$: an element

$\sigma \in G_{\mathbb{Q}_p}$ maps to a matrix $\begin{pmatrix} \chi^{-1}(\sigma) & 0 \\ * & 1 \end{pmatrix}$ but what we are really interested in is the action of inertia group I_p on the $V_l(E)^\vee$ which is given by $\begin{pmatrix} 1 & 0 \\ \phi(\sigma) & 1 \end{pmatrix}$ where $\phi : I_p \to \mathbb{Z}_l(1)$ is the l-adic tame character. This action has 1-dimensional invariant subspace, on which Frobenius acts trivially. Then we get

$$P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p}, t) = \det(1 - \varphi_{p,l}^{-1} t) = 1 - t$$

.

Next we go to the case of *non-split multiplicative reduction*. We look at the unramified quadratic extension $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ instead of $\mathbb{Q}_p$ together with associated character $\eta : G_{\mathbb{Q}_p} \to \mathrm{Gal}(\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p) \simeq \{\pm 1\}$. Consider the quadratic twist E_d of E, then we are reduced to the previous case of split mutliplicative reduction of E_d. We can find that $V_l(E) \simeq V_l(E_d) \otimes \eta$ as a Galois module. Then action of $G_{\mathbb{Q}_p}$ on $V_l(E)$ can be written as $\begin{pmatrix} \chi(\sigma)\eta(\sigma) & * \\ 0 & \eta(\sigma) \end{pmatrix}$ Again we are more interested in the action of I_p on $V_l(E)^\vee$ which looks like $\begin{pmatrix} -1 & 0 \\ \phi(\sigma) & -1 \end{pmatrix}$ this means that invariant subspace is 1-dimensional and $P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p}, t) = 1+t$. The last case is of *additive reduction*. This can be considered as two pieces of either potentially good, or potentially multiplicative reduction. In both cases we find the smallest possible finite field $K/\mathbb{Q}_p$ where E obtains either good or split multiplicative reduction. In both of them the assumption of inertia having a 1-dimensional fixed subspace leads to the trivial action of I_p on $V_l(E)^\vee$ which means $P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p}, t) = 1$. □

We can summarize properties above into a definition of the local L-factor of an elliptic curve E at prime p. Note that Lemma 2.13 can be generalised for the case of number field $K/\mathbb{Q}$ and prime $\mathfrak{p} \in \mathcal{O}_K$.

Definition 2.14. *The product over all primes l of local L-factors is called the global L-function of E, or Hasse-Weil L-function. If the curve is defined over the field of rational numbers it is denoted as*

$$L(E,s) := \prod_p P_{\mathbb{Q}_l,p}((V_l(E)^\vee)^{I_p}, p^{-s})^{-1}$$

Later in the chapter about conjectures of Bloch and Kato we will see why L-function defined in this way following Kato, is the same object as the motivic L-function for the motive $\mathcal{M} = h^1(E)(1)$.

The L-function of an elliptic curve is purely analytic object and our next aim would be to relate it to the arithmetic properties of a curve.

Chapter 3

Birch and Swinnerton-Dyer conjecture

The conjecture was formulated in 1960s by Bryan Birch and Peter Swinnerton-Dyer following numerical evidence of experimental observation, see [BS65]. By this time only some particular cases have been proven, the list is available on [Wik21]. We will state here the most common formulation and explore its relation to various other conjectures and theorems.

For the definition and description of the Tate-Shafarevich group $Ш(E/K)$ see the chapter on Selmer groups. In order to formulate the second part of conjecture we need some additional entries. We assume in this chapter that elliptic curve E is defined over $\mathbb{Q}$.

Consider the ***global minimal Weierstrass equation*** for

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

Then one defines ***the invariant differential*** (sometimes called the Neron differential) by the formula

$$\omega = \frac{\mathrm{d}\, x}{2y + a_1x + a_3}$$

From [Sil09] ch.3 we find that this differential is holomorphic, nonvanishing,

has neither zeroes nor poles, and is invariant under translation by a point. Moreover the pullback with respect to the map ι_E, defined in the very first assumption of this thesis, of the Neron differential satisfies $\iota_E^*\omega = c2\pi i f(\tau)d\tau$ for some constant c.

Definition 3.1. *We call $\Omega_E := \int_{E(\mathbb{R})} |\omega|$ **the real period**. Define c_∞ to be the number of connected components in $E(\mathbb{R})$, then $\Omega_E = c_\infty \int_{\gamma^+} |\omega| = c_\infty \Omega_+$. Where Ω_+ comes as the chosen generator of Neron lattice for E. The choice is defined by a closed path γ^+, which is the generator of the subgroup of $H_1(E(\mathbb{C}), \mathbb{Z})$ fixed by complex conjugation.*

For the complete definition of the ***canonical height*** which is sometimes called Neron-Tate height $\hat{h}_E$ on $E/\mathbb{Q}$ see chapter 9 of [Sil09]. We only shortly recall main properties of the canonical height here.

One first defines height function for a point in projective space $\mathbb{P}^1(\mathbb{Q})$ as maximal archimedean absolute value of its integer coprime coordinates $H(X) = \max\{|x_0|, |x_1|\}$, then one takes its logarithm $h(X) = \log H(X)$, then for a morphism $f : E \to \mathbb{P}^1(\mathbb{Q})$ sending $P \in E$ to $X \in \mathbb{P}^1(\mathbb{Q})$ define $h_f(P) = h(f(P))$. John Tate defined the canonical height as

$$\hat{h}_E(P) := \frac{1}{\deg f} \lim_{N\to\infty} 4^{-N} h_f([2^N]P),$$

which is proven to be independent of f.

We only recall here properties we need: if $\hat{h}_E(P) = 0$, then P is a torsion point, otherwise $\hat{h}_E(P) > 0$. The canonical height defines a positive definite quadratic form on a finite-dimensional vector space $E(\mathbb{Q}) \otimes \mathbb{R}$ of dimension $r = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

Definition 3.2. *Consider a lattice $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ from which the canonical height grows to all of $E(\mathbb{Q}) \otimes \mathbb{R}$. Then one can define canonical height pairing on $E/\mathbb{Q}$ as*

$$\langle P, Q\rangle = \frac{1}{2}(\hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q)).$$

It is important to note the following

Theorem 3.3. *The Neron-Tate height pairing is symmetric (obviously), bilinear, non-degenerate, and continuous since canonical height is continuous. Bilinearity and non-degeneratedness is the theorem of Neron and Tate, proven in the [Sil09] Theorem 9.3. It is also proven there that canonical height is the unique function satisfying properties above.*

An important invariant of E is the volume of the fundamental domain of the lattice $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ we call it the ***regulator*** $R(E/\mathbb{Q})$.

Definition 3.4. *The regulator is a positive real number. It can be computed as the determinant of the Neron-Tate pairing matrix. We choose points $P_1, ...P_r$ which generate $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ and define*

$$R(E/\mathbb{Q}) := \det(\langle P_i, P_j \rangle).$$

It remains to define ***Tamagawa numbers***. For any prime l where E has bad reduction consider the subgroup $E_0(\mathbb{Q}_l) \subset E(\mathbb{Q}_l)$ of local points which have nonsingular reduction at l. Then define Tamagawa number c_l as the size of the factor group $c_l := |E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l)|$, note that automatically by definition $c_l = 1$ in case of good reduction. Later in the discussion about Neron models we will link Tamagawa number to the group of connected components in the Neron model of an elliptic curve.
Now we are ready to formulate one of the most interesting conjectures up to nowadays, the conjecture of Birch and Swinnerton-Dyer [BS65].

Conjecture 3.5. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then:*

1. *The analytic rank of E equals to algebraic rank:*

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r;$$

2. *If Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite, then the leading coefficient*

$L(E,1)^* := \lim_{s\to 1} \frac{L(E,s)}{(s-1)^r}$ *is given by a formula*

$$\frac{L(E,1)^*}{\Omega_E R(E/\mathbb{Q})} = \frac{|Ш(E/\mathbb{Q})|}{(E(\mathbb{Q})_{tors})^2} \prod_l c_l;$$

The conjecture can also be stated for a number field $K/\mathbb{Q}$. All it takes is to define product of periods in a slightly different way, one has to take into account all the real and complex embeddings of the field K and divide the right hand side by a square root of discriminant $\Delta_{K/\mathbb{Q}}$. See conjecture 1 in [Ski18].

3.1 Conjectures

Because we cannot yet prove the Birch and Swinnerton-Dyer conjecture we decided to generalize it instead. Mathematicians came up with several conjectures that are similar to BSD and some imply it but none of those can be proven yet. Chapters to follow will be dedicated to formulations of these conjectures and for some of them proofs of how exactly BSD follows from a particular given one.

3.2 Twisted BSD conjecture

We want to make a fair attempt to formulate a twisted by character version of BSD. The first part about order of vanishing of an L-function is well known, however the formula for the leading coefficient of an L-function keeps its mysteries. In [DEW21] authors describe problems on the way to formulation of the refined conjecture. They have defined a substitution of the left-hand side of BSD $\frac{L(E,1)^*}{\Omega_+}$ but the right-hand side remains unknown.

Setup: We consider a Dirichlet character χ of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ for some n defining an irreducible representation $\chi : G_{\mathbb{Q}} \to \mathbb{C}_p^{\times}$ and an L-function $L(\chi, s) = \sum_{n\geq 1} \chi(n) n^{-s}$.

Consider a finite dimensional vector space V with the action of $G_{\mathbb{Q}}$. The character defines a 1-dimensional vector space V_χ where $G_{\mathbb{Q}}$ acts by χ, then we can define twisted L-function as $L((V_l(E) \otimes V_\chi)^{I_p}, s) =: L(E/\mathbb{Q}, \chi, s)$. If the L-function of elliptic curve is given by Fourier expansion $L(E, s) = \sum_{n\geq 1} a_n n^{-s}$, then we get a formula for

$$L((V_l(E) \otimes V_\chi)^{I_p}, s) = \sum_{n\geq 1} a_n \chi(n) n^{-s}.$$

For an abelian extension $K/\mathbb{Q}$ we look at all characters factoring through $\mathrm{Gal}(K/\mathbb{Q})$, then the following formula holds:

$$L(E/K, s) = \prod_{\chi} L(E/\mathbb{Q}, \chi, s)^{d_\chi}.$$

By the theorem of Rohrlich [Roh88] we know that $L(E/\mathbb{Q}, \chi, 1) = 0$ for all but finitely many Dirichlet characters χ, namely we discard all characters for which primes of bad reduction ramify in $\overline{\mathbb{Q}}^{\ker \chi}/\mathbb{Q}$. Thus we have the finiteness of multiplies in the product above. It follows from the formula above directly that:

$$\mathrm{ord}_{s=1} L(E/K, s) = \sum_{\chi} d_\chi \, \mathrm{ord}_{s=1} L(E/\mathbb{Q}, \chi, s).$$

Moreover we have additional information on the algebraic side of things about all the V_χ and d_χ. Namely there is an identity $\mathrm{rank}_{\mathbb{Z}}(E(K)) = \sum_\chi d_\chi m_\chi(E)$ for multiplicities $m_\chi(E)$ defined by the isomorphism

$$E(K) \otimes \mathbb{C} \simeq \bigoplus_\chi V_\chi^{m_\chi(E)}.$$

Then the twisted version of BSD can be formulated as:

Conjecture 3.6. *For an elliptic curve E defined over $\mathbb{Q}$ viewed as a curve over finite Galois extension $K/\mathbb{Q}$ with Galois group G let χ be an irreducible character of G. Then*

$$m_\chi(E) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, \chi, s).$$

As a special case of this conjecture in one direction Kato has proven in [Kat04] that in case when $K/\mathbb{Q}$ is abelian and when χ is one-dimensional from the fact $L(E/\mathbb{Q}, \chi, 1) \neq 0$ follows that $m_\chi(E) = 0$.
All of the above can be found in the first chapter of [Gre99].

Question 3.7. *Is it possible to derive twisted version of BSD conjecture from an appropriate formulation of the Bloch-Kato conjecture? For that one has to make sense of motivic L-function taking character into account as well as define the Bloch-Kato Selmer groups of a vector space $(V_l(E) \otimes V_\chi)^{I_p}$.*

Or maybe it is possible to formulate twisted BSD conjecture deriving it from some slightly less general than Bloch-Kato, but similar in nature. The next chapter is dedicated to one of possible candidates.

Chapter 4

Conjectures of Mazur and Tate

In 1987 in [MT87] Mazur and Tate have formulated several conjectures related to BSD conjecture 3.5 above and we would like to recall them here. For that purpose we define additional notions in a simplified way comparing to original articles. We would like to define family of numbers related to values of L-functions.

Setup: For now to give the basic definitions consider elliptic curve E to be over $\mathbb{Q}$ and the corresponding Riemann surface $E(\mathbb{C})$. To that surface corresponds a Neron lattice $\Lambda_E \subset \mathbb{C}$ which is a set of periods $\int_\gamma \omega$ for all $\gamma \in H^1(E(\mathbb{Q}), \mathbb{C})$. A real period defined above is one of the generators of Λ_E in the sense that it is one from a unique pair Ω_+, Ω_- for which:

$$\Lambda_E = \mathbb{Z}/2\Omega_+ + \mathbb{Z}/2\sqrt{-1}\Omega_-$$

Recall the modular form f corresponding to E as in 0.1. Then for a complex number $z \in \mathbb{C}$ we set

Definition 4.1. *For a rational number $r = \frac{a}{m}$ we define the modular symbol as the following:*

$$[r]^+ = \frac{1}{\Omega_+} \operatorname{Re}(2\pi i \int_{i\infty}^{r} f(z)\, \mathrm{d}\, z) \in \delta_E^{-1}\mathbb{Z}$$

for positive integer δ_E independent of r (see definition 1.1 in [MR20]).

There is one more modular symbol for r called $[r]^-$ which is given by the relation $2\pi \int_0^\infty f(r+iy)\,\mathrm{d}\,y = [r]^+\Omega_+ + [r]^-\sqrt{-1}\Omega_-$. These values are rational numbers due to theorem by Manin and Drinfeld. Put $[r] = [r]^+$.

Definition 4.2. *For any integer m we define the **modular element** as*

$$\theta_{E,m} = \frac{1}{2}\sum_{a \bmod m} \left[\frac{a}{m}\right]\sigma_a;$$

where σ_a is an element of $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ corresponding to a morphism $x \mapsto x^a$.

Such elements live in $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})]$ satisfy certain compatibility conditions which are formulas of $\theta_{E,ml}$ via $\theta_{E,m}$ for prime l, also they carry certain functional equation (see chapter 1 of [MTT86]). Note that in the most recent work of Mazur and Rubin [MR20] modular elements are defined in a slightly different way, namely they are multiplied by δ_E from above to move to $\mathbb{Z}[(\mathbb{Z}/m\mathbb{Z})^\times]$, therefore all statements are more refined.

Modular symbols keep information about values of L-function of elliptic curve $L(E,s)$ and its twists by a Dirichlet characters $L(E,\chi,s)$. For instance we have $\frac{L(E,1)}{\Omega_+} = [0]^+$ which we have seen in the Birch and Swinnerton-Dyer conjecture, or for the case of $L(E,\chi,s)$ for even χ we have that $\frac{L(E,\chi,1)}{\Omega_+}$ is an algebraic number by the theorem of Shimura. Further we assume $(m, N_E) = 1$ and for character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ we denote by χ as well its lift to a morphism of rings $\mathbb{Q}[(\mathbb{Z}/m\mathbb{Z})^\times] \to \mathbb{C}^\times$. Define $Ga(\chi) = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)e^{\frac{2\pi i a}{m}}$ is the Gauss sum for χ. Then the theorem of Birch and Stevens says

Theorem 4.3. *[MTT86] For χ a primitive even character of conductor m the following is true.*

$$\frac{L(E,\overline{\chi},1)^* Ga(\chi)}{2\Omega_+} = \chi(\theta_{E,m}) = \frac{1}{2}\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)[\frac{a}{m}].$$

To formulate weak vanishing conjecture we need some additional notions.

We denote by $R \subset \mathbb{Q}$ the ring generated over $\mathbb{Z}$ by coefficients of $\theta_{E,m}$. Also for $\mathbb{Q}(\mu_m)^+$ which is the real part of cyclotomic field we denote by $F_m(E/\mathbb{Q}(\mu_m)^+) \subset \mathbb{Z}[(\mathbb{Z}/m\mathbb{Z})^\times]$ the initial Fitting ideal of Pontryagin dual to the Selmer group viewed as $\mathbb{Z}[(\mathbb{Z}/m\mathbb{Z})^\times]$-module. Then the conjecture of Mazur and Tate formulated in [MT87] is the following

Conjecture 4.4.

$$\theta_{E,m} \in F_m(E/\mathbb{Q}(\mu_m)^+) \otimes R \subset R[(\mathbb{Z}/m\mathbb{Z})^\times]$$

However they do not expect this to be a generator of the ideal $F_m(E/\mathbb{Q}(\mu_m)^+) \otimes R$.

Additionally to a couple of conjectures regarding orders of vanishing of modular symbols formulated using degrees of augmentation ideals, there is a conjectural statement about the leading coefficient (e.g. image in the highest degree of such ideal). We would like to recall them here.
We denote by $R[\chi]$ an R-algebra generated by values of χ. We are interested in the ring homomorphism $\tilde{\chi} : R[\chi][(\mathbb{Z}/m\mathbb{Z})^\times] \to R[\chi]$ or more precisely in its kernel I_χ.

Definition 4.5. *For an element* $y \in R[\chi][(\mathbb{Z}/m\mathbb{Z})^\times]$ *we define*

- *the* ***order of vanishing*** *as biggest power of* I_χ *in which* y *is contained. We denote the order of vanishing as* r.
- *the* ***leading coefficient*** *as the image of* y *in* I_χ^r/I_χ^{r+1}.

We can view the element $\theta_{E,m} \in \mathbb{Q}[(\mathbb{Z}/m\mathbb{Z})^\times]$ as an element of $R[\chi][(\mathbb{Z}/m\mathbb{Z})^\times]$ and consider its order of vanishing according to given definition.
We consider the space $E(\mathbb{Q}(\mu_m)^+) \otimes_{\mathbb{Q}} \mathbb{C}$ and take a complex vector subspace inside it which is a kernel of $\chi(a)v - \sigma_a v$. We call this subspace ***the χ-part of Mordell-Weil group*** and denote it by $V_{E,\chi}$. Mazur and Tate have proven the following

Theorem 4.6. *Assume that Conjecture 4.4 holds. Then the order of vanishing of $\theta_{E,m}$ is greater or equal to the dimension of the χ-part of the Mordell-Weil group of $E(\mathbb{Q})$.*

Note that there are also examples in [MT87] when the order of vanishing of $\theta_{E,m}$ is strictly greater the dimension of the χ-part of $E(\mathbb{Q})$.
Now we come to a statement about the leading coefficient of $\theta_{E,m}$. In the same article in the conjecture 4 they have suggested not only a conjectural formula for the order of vanishing, but also a description of leading coefficient of $\theta_{E,m}$ looking a lot like the second part of BSD conjecture 3.5.
For an elliptic curve E denote by S the set of primes in $\mathbb{Q}$ of bad reduction, we consider $S_{mu} \subset S$ the set of primes with split multiplicative reduction. As earlier we consider minimal Weierstrass equation for E and for a prime $p \in \mathbb{Z}$ we look at what E does over $\mathbb{Q}_p$. In this chapter as well as later in chapters about Bloch-Kato conjectures we will need Neron models of elliptic curves, so we recall here main definitions.

Definition 4.7. *Following [Sil94] (chapter 9) we define $\mathcal{C}/\mathbb{Z}_p$ a minimal proper regular model of E over $\mathbb{Z}_p$ and $\mathcal{E}$ to be the largest smooth subscheme of $\mathcal{C}/\mathbb{Z}_p$, it is usually called a* ***Neron model*** *for $E/\mathbb{Q}_p$ and it has a universal property.*

From the Neron mapping property we deduce an isomorphism $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$. We denote by $\mathcal{E}^0/\mathbb{Z}_p$ the identity component of the special fiber of $\tilde{\mathcal{E}}/\mathbb{F}_p$, which is an open subgroup scheme.

Remark 4.8. *The corollary from Tate's algorithm says that the identity component is isomorphic to the largest smooth subscheme of the closed scheme defined by minimal Weierstrass equation for $E/\mathbb{Q}_p$. So essentially we know that the group of points of non-singular reduction and the identity component of Neron model are the same things.*

We denote by $E^0(\mathbb{Q}_p)$ the set of points of non-singular reduction and the

notation for reduction of Weierstrass equation is similar. We define

$$\varphi_{S_{mu}} := \operatorname{coker}(E(\mathbb{Q}) \to \prod_{p \in S_{mu}} \tilde{\mathcal{E}}(\mathbb{F}_p)/\tilde{\mathcal{E}}^0(\mathbb{F}_p))$$

This value plays the role of Tamagawa number from Birch and Swinnerton-Dyer conjecture.

4.1 Biextensions and trivializations

We would like to have an entity behaving like regulator to formulate Mazur-Tate conjecture. It is as usually the hardest bit. In general (see chapter on Beilinson's conjectures) a sensible non-degenerate pairing is hard to obtain. For this purpose biextensions provide a convenient enviroment to define global pairing. So we need to understand biextensions for a pair of abelian varieties A, B. They are best described in book [Pol03] we will transfer the needed material into the situation of elliptic curves.

Definition 4.9. *In general for two group schemes A, B over a field F a **biextension** of A, B by G is a G-torsor $\mathcal{B}$ on $A \times B$ with natural isomorphisms $\mathcal{B}_{a+a',b} \simeq \mathcal{B}_{a,b} + \mathcal{B}_{a',b}$ and $\mathcal{B}_{a,b+b'} \simeq \mathcal{B}_{a,b} + \mathcal{B}_{a,b'}$ satisfying compatibility conditions. In our case group schemes A and B will represent an abelian variety and its dual, or an elliptic curve E for both.*

In the case when we have $G = \mathbb{G}_m$ there is an equivalence between categories of line bundles and $\mathbb{G}_m$-torsors on $A \times B$ we may view biextension on $A \times B$ as a line bundle $\mathcal{B}$ with bilinearity structure $\mathcal{B}_{a+a',b} \simeq \mathcal{B}_{a,b} \otimes \mathcal{B}_{a',b}$ and $\mathcal{B}_{a,b+b'} \simeq \mathcal{B}_{a,b} \otimes \mathcal{B}_{a,b'}$ satisfying compatibility conditions. Namely that three isomorphisms $\mathcal{B}_{a+a'+a'',b} \simeq \mathcal{B}_{a,b} \otimes \mathcal{B}_{a',b} \otimes \mathcal{B}_{a'',b}$ all coincide and two other isomorphisms $\mathcal{B}_{a+a',b+b'} \simeq \mathcal{B}_{a,b} \otimes \mathcal{B}_{a',b} \otimes \mathcal{B}_{a,b'} \otimes \mathcal{B}_{a',b'}$ coincide.

We then know from [Pol03] that biextensions correspond to morphisms $A \to \widehat{B}$, where $\widehat{B}$ is the dual abelian variety to B. By the definition of Cartier dual we have a canonical isomorphism $A \xrightarrow{\sim} \widehat{\widehat{A}}$ and correspondent to it ***canonical***

biextension $\mathcal{E}$ on $A \times \widehat{A}$ by $\mathbb{G}_m$.

We will be interested in the following particular case of a biextension on A, A by $\mathbb{G}_m$ coming from a line bundle $\mathcal{L}$ on A in the following way

$$\Lambda(\mathcal{L}) := m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$$

Where $p_{1,2} : A \times A \to A$ are natural projections and $m : A \times A \to A$ is the group law. This structure is called ***Mumford bundle***.

For an elliptic curve E denote by $\mathcal{O}_E$ the structure sheaf on E, note that $\widehat{E} \simeq E$ in this case. Then line bundles of degree 0 are just $\mathcal{O}_E(P - O)$ for a point P on E, here we write $P - O$ as a Weil divisor on E. Then from the formula above one deduces that biextensions on E, E are of the form

$$\Lambda(\mathcal{O}_E(P - O)) := \mathcal{O}_{E\times E}(m^{-1}(P - O) \otimes p_1^{-1}(P - O) \otimes p_2^{-1}(P - O))$$

In articles by Mazur and Tate for a biextension $\mathcal{B}$ of A, B they defined notions of local modification and trivialization. We recall them here for consistency of the document.

Definition 4.10. *For a biextension $\mathcal{B}$ of abelian varieties A, B by $\mathbb{G}_m$ over a local field F with valuation v and ring of integers $\mathcal{O}$ we denote by $\mathcal{B}(F)$ a set-theoretic biextension of $A(F), B(F)$ by $F^\times$.*

- *By a **modification** of a biextension $\mathcal{B}$ we mean a quadruple $(\mathcal{B}', \alpha, \beta, \rho)$. Where $\alpha : A' \to A(F)$, $\beta : B' \to B(F)$, and $\rho : \mathbb{G}_m \to G$ are group homomorphisms, and $\mathcal{B}'$ is a pullback of $\mathcal{B}(F)$ by α, β and further pushout by ρ.*

- *A splitting ψ of $\mathcal{B}'$ is a map $\psi : (\alpha^*, \beta^*)(\mathcal{B}(F)) \to G$ such that for $g \in \mathbb{G}_m$ and $x \in \mathcal{B}(K)$ we have $\psi(x + g) = \psi(x) + \rho(g)$ and for any $a \in A(F)$, $b \in B(F)$ the restriction of ψ to layers of $\mathcal{B}$ above $\{a\} \times B$ and $A \times \{b\}$ are group homomorphisms.*

- *By a* ***trivialization*** *of $\mathcal{B}(F)$ we call a modification together with a splitting ψ of $\mathcal{B}$.*

For decent examples of trivializations one should consult [MT87], we start with the **Neron unramified trivialization** for a modification

$$(E(F), E^0(F) \hookrightarrow E(F), F^\times/\mathcal{O}^\times \simeq \mathbb{Z}).$$

It is characterized by properties that v is discrete and ρ is unramified, i.e. $\rho(\mathcal{O}^\times) = 0$. Then Mazur and Tate have proven that there exists a unique splitting ψ of $\mathcal{B}'(F)$ such that $\psi(\mathcal{B}'(\mathcal{O})) = 0$. Additionally to this one we will need only Archimedean Neron unramified and split multiplicative trivializations.

Definition 4.11. *In general for n divisors $D_1, ..., D_n$ and a point $x \in E(F)$ common for all of them we define* ***intersection multiplicity*** *as* $\mathrm{mult}(x) = \dim \mathcal{O}_x/(f_1, ..., f_n)$ *for f_is to be local equations of D_is. Then the* ***intersection index*** *is defined as*

$$D_1 \cdot D_2 \cdot ... \cdot D_n := \sum_{x \in D_1 \cap ... \cap D_n} \mathrm{mult}(x)$$

It is known to define symmetric and n-linear map $\mathrm{Pic}(X)^n \to \mathbb{Z}$. It turns out (see [MT83]) that the splitting for the unramified case is given by the intersection index formula for two divisors $D_1, D_2 \in \mathrm{Div}^0(E(F))$ with disjoint supports $\psi(D_1, D_2) = -(D_1 \cdot D_2) \log |f_v|$ where f_v is the residue field. We additionally require for D_2 to intersect every component of special fiber $E_{\mathbb{F}_p}$ with $\deg(D_2 \cdot X_i) = 0$ to ensure it to be in $E^0(F)$.

Theorem 4.12. *Points on a curve E define Weil divisors which we denote as (P) and $(P) - (O)$ for a point $P \in E(F)$. We know that pairing above to be symmetric and bilinear, moreover if we take $\log |\psi((D_1, D_2))|$ it is continuous and therefore for $D_1 = (P) - (O)$ and $D_2 = (Q) - (O)$ it is nothing but the Neron-Tate height pairing as uniquely determined by its properties: to be*

bilinear, symmetric, and continuous as mentioned in 3.3. See chapter 2 of [Blo80] for a substantial proof.

Roughly speaking **tamely ramified trivialization** is defined for a triple $E(F), E^1(F), F^\times/U^1$. A divisor D corresponds to a point of $E^1(F)$ therefore goes to 0 via reduction to the residue field $\mathbb{F}_p$. Then D is principal and we can take a function f_D corresponding to D and define a pairing $\psi(D_1, D_2) = \log|f_{D_2}(D_1)|$.

There is no simple description of **split multiplicative trivialization** and very roughly one should consider abelian varieties as rigid analytic varieties and work with a meromorphic theta function instead of divisor as above. Then formula for $\psi(D, \theta, a) = \log|a\theta(D)|$ where $a \in F^\times$.

4.2 Global pairing

So far we have been working with purely local objects but we are aiming to define a global pairing $E(K) \times E(K) \to \mathbb{R}$ where K is a number field. From now until the end of chapter we take $F = K_v$ for an archimedean or discrete v. We look at all such places v and consider all corresponding local trivializations $(\mathcal{B}'_v, \alpha_v, \beta_v, \rho_v, \psi_v)$ such that for all but finitely many v they are just Neron unramified trivializations defined above.

One of the main aims of this section is to explain why the global pairing defined by trivializations is the same as Neron-Tate height pairing. This would give another point of view on the regulator of an elliptic curve. Later in the chapter about Beilinson's conjectures we will make good use of the Theorem 4.12 when we want to relate the link pairing to the intersection pairing and the Neron-Tate height.

Recall the group of ideles $I_K = \prod'_v K_v^\times$ of K to be defined as restricted product. To define global pairing we will consider all maps ρ_v for all v at once. Previously we have been working with $\rho_v : K_v^\times \to G_v$ for some group G_v which is generally just $\mathbb{Z}$ except some finite number of cases. Now a morphism $\rho = \sum_v \rho_v$ maps

I into $\bigoplus_v G_v$ later we will send it further into a product of $\mathbb{F}_p^\times \times \mathbb{Z}_l^\times$ for certain p and ls.

We know that for all but finitely many $\alpha_v = \mathrm{id}$ as well as β_v. So if we look at all α_v we get that $\prod_v \ker\alpha_v \subset I_K$ as well as $\prod_v \mathrm{coker}\alpha_v \subset I_K$.

Definition 4.13. *We define the global group E' as a term in short exact sequence*

$$0 \to \prod_v \ker\alpha_v \to E' \to E(K) \to \prod_v \mathrm{coker}\alpha_v \to 0 \tag{4.1}$$

The pairing we are looking for is defined globally as a bilinear non-degenerate map $E' \times \widehat{E}' \to \mathbb{R}$. Lets have a look at what are these E' and $\widehat{E}'$ precisely for a given elliptic curve E.

For an elliptic curve E over a number field K we denoted above by S the set of all places of K of bad reduction for E. Inside S there is a set of all places of split multiplicative reduction S_{mu}. Now we want to understand what all the notions above happen to be in this case. We take for an archimedean v the corresponding final $G_v = 0$. Further we assume v to be discrete and $v \notin S$ for all but finitely many v. We take

1. ψ_v coming from Neron unramified trivialization if v is of good reduction;
2. tamely ramified trivialization in case $v \in S \setminus S_{mu}$;
3. split multiplicative trivialization for the case of $v \in S_{mu}$;

Definition 4.14. *For all the cases we define a subgroup $U_v \in K_v^\times$ in the following way:*

- *for archimedean v say $U_v = K_v^\times$,*
- *for non-archimedean $v \notin S$ take $U_v = \mathcal{O}_v^\times$,*
- *for $v \in S \setminus S_{mu}$, take $U_v = 1 + \mathfrak{m}_v$,*
- *and for $v \in S_{mu}$ define $U_v = (1)$.*

For each G_v take it to be $K_v^\times/U_v$, then the final group for image of the global version of ψ is $G_S = I_K/(K^\times \prod_v U_v)$. So now we have $G_v \simeq \mathbb{Z}$ for all good places of K.

We define a global pairing ψ_S for our case as following: by Mordell-Weil theorem we take a basis of points of $E(K)$ and the dual to it in $\widehat{E}(K)$. The canonical embedding of fields $K \hookrightarrow K_v$ defines a morphism of groups $E(K) \to E(K_v)$, in an analogous way one gets $\widehat{E}(K) \to \widehat{E}(K_v)$, we look at images of all basis points P_i in $E(K_v)$ and in $\widehat{E}(K_v)$ denote them as P_is again and further work with with them locally.

In case of each v we consider a biextension $\mathcal{B}(K_v)$ defined by a triple of groups $E(K_v), \widehat{E}(K_v), K_v^\times$ as described above, its modification $\mathcal{B}'(K_v)$ corresponding to the situation with v (depending on whether v is unramified, tame, or split) and lift all points P_i to elements of $\mathcal{B}'(K_v)$. Then

Definition 4.15. *The **Mazur-Tate pairing** is*

$$\langle\ ,\ \rangle_S : E(K) \times \widehat{E}(K) \to G_S$$

$$\langle P_i, P_j \rangle_S \mapsto \prod_v \psi_v(P_i, P_j).$$

One can find basic properties like restriction to smaller set $S_{mu} \subset T \subset S$ proven in article [MT87], we would like to mention here that obtained pairing is bilinear and non-degenerate because each ψ_v is.

4.3 Formulation of the conjecture

The final notion of discriminant is related to determinant of the pairing matrix above. We look at the short exact sequence 4.1 for E' and $\widehat{E}'$. Despite the isomorphism $E \simeq \widehat{E}$, in general it is NOT true that $E' \simeq \widehat{E}'$ and short exact sequences are different. Namely

$$0 \to \prod_v \ker \alpha_v \to E' \to E(K) \to 0;$$

$$0 \to \prod_v \ker \beta_v \to \widehat{E}' \to \widehat{E}(K) \to \prod_{v \in S \setminus S_{mu}} \widehat{E}(k_v) \prod_{v \notin S} \widehat{E}/\widehat{E}^0(k_v) \to 0$$

For the map $\langle\ ,\ \rangle_S$ to land in $\mathbb{R}$ we tensor both sequences with $\mathbb{R}$ to get

$$0 \to \prod_v \ker \alpha_v \otimes \mathbb{R} \to E' \otimes \mathbb{R} \to E(K) \otimes \mathbb{R} \to 0;$$

and the same sequence for $\widehat{E}$ since $\prod_{v \in S \setminus S_{mu}} \widehat{E}(k_v) \prod_{v \notin S} \widehat{E}/\widehat{E}^0(k_v)$ is finite group. Moreover we get a duality between $\mathbb{R}$-vector spaces $\ker \alpha_v \otimes \mathbb{R}$ and $\ker \beta_v \otimes \mathbb{R}$.

Definition 4.16. *With all of the above Mazur and Tate defined discriminant as*

$$\mathrm{D}_S(E) = \frac{\prod_{v \in S \setminus S_{mu}} (q_v - 1 - n_v)}{[\widehat{E}(K)_{S_{mu}} : \widehat{E}']} (1 \otimes \det(\langle\ ,\ \rangle_S))$$

an element of $K \otimes \mathrm{Sym}_{\mathbb{Z}}(\prod_v G_v)$. *Here* $q_v = |k_v|$ *and* $n_v = |\widehat{E}^0(k_v)|$, *by* $\widehat{E}(K)_{S_{mu}}$ *we denote the toric part of reduction of* $\widehat{E}(K)$ *at* v.

Currently we got an element $\mathrm{D}_S(E) \in K \otimes \mathrm{Sym}_{\mathbb{Z}}(\prod_v G_v)$ or more precisely in $R \otimes \mathrm{Sym}_{\mathbb{Z}}(\prod_v G_v)$ where R is a ring over $\mathcal{O}_K$ in which index $[\widehat{E}(K)_{S_{mu}} : \widehat{E}']$ becomes invertible. It is not evident why is it in needed degree of an ideal.
For the conjecture we consider the case of $K = \mathbb{Q}$, then there is an explicit way to write down $\prod_v G_v = \prod_{p \in S \setminus S_{mu}} \mathbb{F}_p^\times \times \prod_{p \in S_{mu}} \mathbb{Z}_p^\times$ and a morphism

$$\prod_v G_v \to (\mathbb{Z}/(\prod_{p \in S \setminus S_{mu}} p \prod_{p \in S_{mu}} p^2)\mathbb{Z}).$$

If we take a group algebra of the latter with coefficients in R and consider its augmentation ideal I we get a map $R \otimes \mathrm{Sym}_r(\prod_v G_v) \to I^r/I^{r+1}$ induced by the above morphism of groups, here r will be defined soon. We take as $\mathrm{Disc}_S(E)$ the image of $\mathrm{D}_S(E)$ under this map.

Conjecture 4.17. *[MT87]*

1. *The order of vanishing of the modular element $\theta_{E,m}$ equals*

$$r := \operatorname{rank} E(\mathbb{Q}) + |S_m|;$$

2. *Denote by $\tilde{\theta}_{E,m} \in I^r/I^{r+1}$ the leading coefficient of $\theta_{E,m}$, then*

$$\tilde{\theta}_{E,m} = |Ш(E/\mathbb{Q})| \cdot \varphi_{S_{mu}} \cdot \operatorname{Disc}_S(E)$$

One can notice the similarity between the Mazur-Tate Conjecture and the BSD Conjecture 3.5 above: both start with statement about order of vanishing of a function, both have rational part and transcendental part in second statement. We have mentioned above a relationship between modular symbols and L-functions of an elliptic curve, however it would be good question on whether it is possible to derive one conjecture from the other one.

Question 4.18. *It also seems to be possible to formulate a twisted BSD conjecture deriving it from the statement above and using theorem of Birch and Stevens 4.3.*

Chapter 5

Beilinson's conjectures

We are slowly approaching vast generalizations of the BSD conjecture. For instance there exist statements generalizing BSD from elliptic curves to smooth algebraic varieties of any dimension given by A. Beilinson [Bei87], P. Deligne [Del79], and P. Swinnerton-Dyer.

The topic has been quite popular and is well studied in a number of surveys from various viewpoints: one of the main resources [Bei85], [Nek94] about the motivic intuition, a collection of works [RSS88] with [Sch88] among them, [Sch94] on the way from motives to algebraic varieties.

Setup: We assume that K is a number field and X is a smooth projective variety of dimension n over K. Then one can define an L-function in the same way as in the Definition 2.9 for $V = H^{2n-1}_{et}(X, \mathbb{Q}_l)$ and we want to know its properties.

One of the hardest tasks in formulating conjectures of BSD-type is to define a sensible regulator, we have seen already in the chapter about Mazur-Tate conjecture one of the ways that works for abelian varieties and can be generalized further for smooth algebraic varieties. In his article [Bei87] A. Beilinson has defined a local height pairing for algebraic varieties of higher dimensions and proven equivalence of all the definitions given (Lemma 2.1.1).

As in the case of the Mazur and Tate pairing the intersection pairing defined locally for each prime and then combined into a global pairing. We will de-

scribe the notion of local link pairing in general case of an algebraic variety of dimension n as in [Bei87] and later consider it for elliptic curves. Denote by cl the cycle class map which extends to a localization:

$$cl : CH^*(X) \to H^{2*}(X, \mathbb{Q}_l(n));$$

Construction 5.1. *For a non-archimedean place $v \in K$ consider the corresponding valuation field K_v. Define $X_v = X \times \mathrm{Spec}(K_v^{ur})$. To define the local height pairing take two cycles a_1, a_2 on X_v with disjoint supports Y_1, Y_2 and of dimensions d_1, d_2 correspondingly so that $d_1 + d_2 = n + 1$ and $cl(a_i) = 0 \in H^{2d_i}(X_v, \mathbb{Q}_l(d_i))$. Then two open subsets of X_v given as $U_i = X_v \setminus Y_i$ form an etale cover of X_v and one may consider the Mayer-Vietoris sequence. Consider the boundary map $H^{2d_i-1}(U_i, \mathbb{Q}_l(d_i)) \to H^{2d_i}_{Y_i}(X_v, \mathbb{Q}_l(d_i))$ then for each $a_i \in CH^{d_i}(X_v)$ there exists corresponding cohomology class $cl(a_i) \in H^{2d_i}_{Y_i}(X_v, \mathbb{Q}_l(d_i))$, we denote its preimage by α_i. The cup product maps*

$$H^{2d_1-1}(U_1, \mathbb{Q}_l(n+1)) \times H^{2d_2-1}(U_2, \mathbb{Q}_l(n+1)) \to H^{2n}(U_1 \cap U_2, \mathbb{Q}_l(n+1))$$

$$(\alpha_1, \alpha_2) \mapsto \alpha_1 \cup \alpha_2$$

Definition 5.2. *In the situation described above we have the following: $\langle a_1, a_2 \rangle_v$ is the image of $\alpha_1 \cup \alpha_2$ under the map $H^{2n}(U_1 \cap U_2, \mathbb{Q}_l(n+1)) \to H^{2n+1}(X_v, \mathbb{Q}_l(n+1))$ coming from the Mayer-Vietoris sequence. We then send it further $H^{2n+1}(X_v, \mathbb{Q}_l(n+1)) \to \mathbb{Q}_l$ via the trace map.*

A. Beilinson has given in his article [Bei87] two more definitions of the local link pairing and proven their equivalence. We preferred the one above for its simplicity.One of conjectures of Beilinson says

Conjecture 5.3. *[Bei87] The local link pairing between algebraic cycles is $\mathbb{Q}$-valued and independent on the choice of prime number l different from characteristic of residue field at which local situation was studied.*

The situation however changes over archimedean places v, as the value of pairing becomes real instead of rational. Later in chapter 4 of the same article he defined global height pairing in the following situation.

Let K be as before a number field, X is a smooth projective variety of dimension n over K. Assume that for all non-archimedean primes $v \in \mathcal{O}_K$ the scheme $X_v = X \times \mathrm{Spec}(K_v^{ur})$ satisfies local Beilinson conjectures. Then define

$$\mathrm{CH}^i(X)^\circ := \ker(\mathrm{CH}^i(X) \to \mathrm{H}^{2i}_{et}(X \times_K \mathrm{Spec}(\overline{K}), \mathbb{Q}_l(i)))$$

We assume this does not depend on l as it can be defined in a different way. As it was defined in the article for each place v of K we take $r(v) = \log |k_v|$ for all archimedean places v, $r(v) = 1$ for $K_v = \mathbb{R}$, and $r(v) = 2$ for $K_v = \mathbb{C}$.

Definition 5.4. *For X as above define the global height pairing as*

$$\begin{aligned} \langle\ ,\ \rangle : \mathrm{CH}^i(X)^\circ \times \mathrm{CH}^{n+1-i}(X)^\circ &\to \mathbb{R} \\ \langle cl\, a, cl\, b\rangle &= \sum_v r(v)\langle a, b\rangle_v \end{aligned} \tag{5.1}$$

for a, b cycles on X with empty intersection of supports. Note that for given a, b and almost all v the value $\langle a, b\rangle_v = 0$.

The second conjecture of Beilinson [Bei87] says that the height pairing defined above is non-degenerate.

We have seen that Hasse-Weil L-function can be defined for an l-adic representation V. Then comparing to the rank part of the statement of Birch and Swinnerton-Dyer conjecture there has been given a more general conjecture due to Swinnerton-Dyer:

Conjecture 5.5. *[Bei87] Let X be a smooth projective n-dimensional scheme over $\mathbb{Q}$. Assume that the $L-$function of X analytically continues to $\mathbb{C}$ and satisfies functional equation. Then groups $\mathrm{CH}^i(X)^\circ$ are finitely generated and*

$$\mathrm{ord}_i L(H^{2i-1}_{et}(X), s) = \mathrm{rank}\, \mathrm{CH}^i(X)^\circ$$

A. Beilinson decided to go further and formulate a refined version. We have stated above that the obtained height pairing is bilinear and non-degenarate, due to classes equivalence it is defined up to an element of $\mathbb{Q}^\times$. Then one gets a regulator as the determinant of its Gram matrix.
Define Ω_X to be the period matrix for $H^{2i-1}(X,\mathbb{Q})$. It is obtained from the classical de Rham theorem:

Theorem 5.6. *Let X be a proper and smooth scheme over $\mathbb{Q}$. Then there exist a functorial isomorphism*

$$\alpha_{dR} : H^n_{dR}(X) \otimes \mathbb{C} \simeq H^n_{sing}(X,\mathbb{Q}) \otimes \mathbb{C}$$

It induces a non-degenerate pairing

$$H^n_{dR}(X) \times H_n(X,\mathbb{C}) \to \mathbb{C}$$

by sending a differential form and a cycle (ω,γ) to $\int_\gamma \omega$.

Since both $H^n_{dR}(X)$ and $H^n(X,\mathbb{Q})$ are finite dimensional vector spaces over $\mathbb{Q}$ and by the above of the same dimension, after choosing bases ω_i and γ_j in them one may write down a Gram matrix $\delta_{i,j} = \int_{\gamma_j} \omega_i$ and compute its determinant which is denoted as $\det \Omega_X$. More on this see Deligne's article [Del79].
We have now a pairing that takes values in $\mathbb{C}$ however we would like it to go to $\mathbb{R}$ instead, for this we take a filtered piece of the de Rham cohomology and a subspace of singular cohomology fixed by the complex conjugation. These subspaces are dual to each other under the de Rham isomorphism. The determinant of the corresponding Gram matrix is denoted as $\det \Omega^+_X$.
Then the following conjecture [Bei87] should be thought of as generalization of the second part of the BSD conjecture.

Conjecture 5.7. *Assume that the L-function of X has an analytic continuation to all $\mathbb{C}$ and satisfy the functional equation. Denote by $L^*(H^{2i-1}_{et}(X),s)$*

the leading coefficient of the L-function, i. e. the value of

$$\lim_{s\to i}\frac{L(H_{et}^{2i-1}(X),s)}{(s-i)^{\mathrm{ord}_i L(H_{et}^{2i-1}(X),s)}}$$

then

$$L^*(H_{et}^{2i-1}(X),s)=\det_i\langle\ ,\ \rangle\cdot\det(\Omega_X^+)\cdot u$$

for some $u\in\overline{\mathbb{Q}}^*$*, where* $\det(\Omega_X^+)$ *is defined in chapter 4 of [Del79].*

In fact this latest conjecture is formulated for a motive of weight -1 corresponding to an algebraic variety with all the entities defined accordingly. Now we would like to understand why the above statement is really a generalisation of BSD conjecture, namely what do all the ingredients on the right hand side mean in the case of elliptic curve. For that we will compute values of $\det_i\langle\ ,\ \rangle$ and $\det(\Omega_X^+)$ when X is a smooth projective curve of genus 1 over $\mathbb{C}$.

Remark 5.8. *We start with proving that* $\det\Omega_X^+$ *equals to* Ω_E *for the case* $X=E(\mathbb{C})$ *an elliptic curve considered as a Riemann surface.*
From topology course we know that $\dim H^1_{sing}(E(\mathbb{C}),\mathbb{Q})=2$*. We know as well that* $\dim H^1_{dR}(E(\mathbb{C}))=2$ *and* $H^0(E(\mathbb{C}),\Omega^1)=Fil^0H^1_{dR}(E(\mathbb{C}))=\mathbb{Q}\omega$ *so we extend* ω *to a basis of* $H^1_{dR}(E(\mathbb{C}))=\omega\mathbb{Q}\oplus\omega_1\mathbb{Q}$*. By the duality set in the Theorem 5.6 we may choose a basis* (γ^+,γ^-) *of* $H_{1,sing}(E(\mathbb{C}),\mathbb{Q})$ *dual to* (ω,ω_1)*.*
Then by chapter 4 in [Del79] we have the computation of

$$\det\Omega_E^+=\langle\omega,\gamma^+\rangle=[E(\mathbb{R}):E(\mathbb{R})^\circ]\Big|\int_{\gamma^+}\omega\Big|.$$

Where $E(\mathbb{R})^\circ$ *is a connected component of* $E(\mathbb{R})$*, so* $[E(\mathbb{R}):E(\mathbb{R})^\circ]=c_\infty$ *in the notation of BSD conjecture.*

Next we would like to understand why in the case of elliptic curve the pairing introduced by Beilinson as described above becomes Neron-Tate height pairing. For that we will work locally for good places of E in $\mathbb{Q}$.

Remark 5.9. *In the chapter about the Mazur-Tate conjecture we have explained why the Mazur-Tate pairing which locally on places of good reduction is just an intersection index coincides with the canonical Neron-Tate height pairing, see the Remark 4.12 and we refer to [Blo80] for the proof. So it is left to explain why the pairing defined via cup product of cohomology classes coincides with intersection pairing.*

Proposition 5.10. *For $X = E(\mathbb{C})$ being smooth projective curve of genus 1 over the field $\mathbb{Q}$ the pairing defined in the Conjecture 5.4 is the Neron-Tate height pairing defined in 3.2.*

We will check this locally on all places of good reduction v in K. By Neron's theory the Neron-Tate height pairing can be broken into local pieces. A. Beilinson gives a good intuitive description of this statement in general for an algebraic X over $\mathbb{Q}_p$ of dimension n. Then a point of X is a map $\operatorname{Spec}\mathbb{Q}_p \to X$ and when we choose a regular proper model of X over $\mathbb{Z}_p$ we mean the following

$$\begin{array}{ccccc} X_s & \xrightarrow{i_X} & X_{\mathcal{O}} & \xleftarrow{f_X} & X \\ {\scriptstyle s}\uparrow & & \uparrow & & \uparrow{\scriptstyle \eta} \\ \operatorname{Spec}\mathbb{F}_p & \xrightarrow{i} & \operatorname{Spec}\mathbb{Z}_p & \xleftarrow{f} & \operatorname{Spec}\mathbb{Q}_p \end{array}$$

We understand a scheme X as a manifold fibered over $\operatorname{Spec}\mathbb{Q}_p$ and we want to have X of good reduction over p. Denote by X_s the special fiber and X the generic fiber of X. For any subset $S \subset X$ we denote in the same way its image under f_X. Then the situation we have is the following: there are two cycles on X homologous to 0 of dimensions d_1 and d_2 such that $d_1 + d_2 = n + 1$.
We look at cycles a_1 and a_2 and their images in $X_{\mathcal{O}}$ which are now sections of $X_{\mathcal{O}}$ over $\mathbb{Z}_p$ and we define the local link pairing $\langle a_1, a_2 \rangle_p$ as the intersection index of those sections. It is non-zero only if they intersect non-trivially modulo p.

In the case of an elliptic curve $E(\mathbb{C})$ we look at its Neron model over $\mathbb{Z}_p$, as for cycles a_1 and a_2 they are just points on E and can be seen as two maps $\operatorname{Spec}\mathbb{Q}_p \to E$, we continue them to maps $\operatorname{Spec}\mathbb{Z}_p \to \mathcal{E}$ and take intersection

index of images. It is non-zero if and only if points a_1, a_2 coincide modulo p.

Proof. of the Proposition 5.10 In general for cycles $cl(a_i) \in H^{2d_i}_{Y_i}(X_{\mathcal{O}}, \mathbb{Q}_l(d_i))$ their intersection index is defined as the image under sequence

$$H^{2d_1}_{Y_1}(X_{\mathcal{O}}, \mathbb{Q}_l(d_1)) \times H^{2d_2}_{Y_2}(X_{\mathcal{O}}, \mathbb{Q}_l(d_2)) \to H^{2d_1}(X_{\mathcal{O}}, \mathbb{Q}_l(d_1)) \times H^{2d_2}(X_{\mathcal{O}}, \mathbb{Q}_l(d_2))$$
$$\xrightarrow{\cup} H^{2n+2}_{|X_s|}(X_{\mathcal{O}}, \mathbb{Q}_l(n+1)) \xrightarrow{Tr} H^2_{|s|}(\mathrm{Spec}(\mathbb{Z}_p), \mathbb{Q}_l(1)) \simeq \mathbb{Q}_l \tag{5.2}$$

Then for an elliptic curve with good reduction over p we consider divisors $a_1 = \sum \alpha_i P_i$ and $a_2 = \sum \beta_j Q_j$ to find out their local pairing $\langle a_1, a_2 \rangle_p$ following the path above. As previously we denote by Y_i the support of a_i. Here α_i, β_j are some l-adic numbers and P_i, Q_j are points on $E(\mathbb{Q}_p)$, then $d_1 = d_2 = 1$. Therefore both local link pairing and intersection index can be represented by a commutative diagram using Definition 5.2 and intersection index as defined above 5.2

$$\begin{array}{ccc}
H^1(U_1, \mathbb{Q}_l(1)) \times H^1(U_2, \mathbb{Q}_l(1)) & \xrightarrow{\cup} & H^1(U_1 \cap U_2, \mathbb{Q}_l(1)) \\
\uparrow & & \\
H^1(E_{\mathbb{Z}_p} \setminus Y_1, \mathbb{Q}_l(1)) \times H^1(E_{\mathbb{Z}_p} \setminus Y_2, \mathbb{Q}_l(1)) & & \\
\downarrow & & \\
H^2(E_{\mathbb{Z}_p}, \mathbb{Q}_l(1)) \times H^2(E_{\mathbb{Z}_p}, \mathbb{Q}_l(1)) & \xrightarrow{\cup} & H^4_{E_{\mathbb{F}_p}}(E_{\mathbb{Z}_p}) \\
\xrightarrow{MV} & H^3(E, \mathbb{Q}_l(2)) & \xrightarrow{\mathrm{Tr}} H^1(\mathrm{Spec}\, \mathbb{Q}_p, \mathbb{Q}_l(1)) \simeq \mathbb{Q}_l \\
\xrightarrow{\mathrm{Tr}} H^2_{|s|}(\mathrm{Spec}(\mathbb{Z}_p), \mathbb{Q}_l(1)) \simeq \mathbb{Q}_l & &
\end{array}$$

together with a boundary map $H^1(\mathrm{Spec}\, \mathbb{Q}_p, \mathbb{Q}_l(1)) \to H^2_{|s|}(\mathrm{Spec}(\mathbb{Z}_p), \mathbb{Q}_l(1))$. We start with two cycles $a_1 \in H^1(E_{\mathbb{Z}_p} \setminus Y_1, \mathbb{Q}_l(1))$ and $a_2 \in H^1(E_{\mathbb{Z}_p} \setminus Y_2, \mathbb{Q}_l(1))$ and going up follows the definition of linking number but going down gives the definition of intersection index and therefore height pairing via Mazur and Tate. Which in turn is known to be the Neron-Tate height pairing. □

Chapter 6

The first Bloch-Kato conjecture

6.1 Main prerequisites

It is widely known that one of the Bloch-Kato conjectures is in some way the generalisation of the BSD Conjecture 3.5. It is less widely known though in what way exactly.

The Bloch-Kato conjecture consists of two parts. One easy about the order of vanishing of motivic L-function defined in 9.30, one harder about the description of leading coefficient which is called the Tamagawa number conjecture. In this chapter we will explain why the first part is generalisation of the first statement of the BSD conjecture and later we will prove that the second part of the Tamagawa number conjecture is generalisation of the refined BSD conjecture.

Setup: Denote until the end of chapter by K a number field. In the BSD conjecture one should work with the Mordell-Weil group $E(K)$. Assuming the conjecture on finiteness of the Tate-Shafarevich group $Ш(E/K)$ one has the rank of $E(K)$ to be the same as rank of $\mathrm{Sel}(E/K)$ by the Fundamental Exact Sequence 1.4. Then one may work with Selmer group instead of Mordell-Weil group.

Here for the case of a general algebraic scheme X we can not work with $X(K)$ as we have no idea about its structure, it is not a group anymore. We will introduce a so-called Bloch-Kato Selmer group which is a subgroup

of $H^1(G_K, V(X))$ for a certain p-adic representation $V(X)$. We want to work with good enough representation, called *coming from geometry*.

Definition 6.1.

- *A **p-adic representation** V of the group G_K is a finite dimensional $\mathbb{Q}_p$-vector space equipped with a continuous action of G_K.*
- *We say that a p-adic representation V is **coming from geometry** if there exists a smooth proper variety X/K such that V is a subspace of a quotient of $H^n_{et}(X_{\overline{K}}, \mathbb{Q}_p)$ for some n.*

We will assume all p-adic representations in this chapter to satisfy this property. Similarly to the usual Selmer group the Bloch-Kato Selmer group is cut out by local conditions for every place v of K, now we need to determine what are those conditions exactly. Since we are working with etale cohomology with coefficients in $\mathbb{Q}_p$ for some fixed prime p, we need to consider two separate cases of v being above p and away from it. The second case involves study of p-adic Hodge theory so we start with first.

6.2 Case away from p

Setup: K_v is a finite extension of $\mathbb{Q}_l$ for $v \nmid p$, V a p-adic representation coming from geometry. In this given case to say that a representation $V = H^n_{et}(X, \mathbb{Q}_p)$ is unramified means that X has good reduction at v so this would be our geometric condition.

Definition 6.2. *The unramified cohomology:*

$$H^1_{ur}(K_v, V) := \ker(H^1(K_v, V) \to H^1(I_{K_v}, V))$$

Where $I_{K_v} \subset G_{K_v}$ is the inertia subgroup. Then define local Bloch-Kato Selmer group as

$$H^1_f(K_v, V) := H^1_{ur}(K_v, V).$$

The next lemma provides justification for the words "Selmer group" in the name.

Lemma 6.3. *Let E be an elliptic curve over a number field K with non-archimedean place $v|p$ away from l. Then the subspace of unramified cohomology $H^1_{ur}(K_v, V_l E(\overline{K_v})) \subset H^1(K_v, V_l E)$ contains the image of the composition of the Kummer map and localization map*

$$E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l \xrightarrow{\kappa} H^1(K, V_l E(\overline{K})^{I_v}) \to H^1(K_v, V_l E(\overline{K_v})^{I_v}). \tag{6.1}$$

In the following paragraphs we explain the essential meaning of this lemma: recall the definition of the Selmer group 1.2. It can be summarized in the following way: Define a subgroup $S_{p^n,v} \subset H^1(K, E(\overline{K})[p^n])$ by the exact diagram

$$\begin{array}{ccccc} & S_{p^n,v} & \searrow & & \\ E(K)/p^nE(K) & \xrightarrow{\kappa_p} & H^1(K, E(\overline{K})[p^n]) & & \\ \downarrow & & \downarrow f & \searrow & \\ E(K_v)/p^nE(K_v) & \xrightarrow{\kappa_{v,p}} & H^1(K_v, E(\overline{K_v})[p^n]) & \longrightarrow & H^1(K_v, E(\overline{K_v})[p^n])/\operatorname{Im}\kappa_{v,p} \end{array} \tag{6.2}$$

Where $\kappa_{v,p}$ is the local Kummer map, see chapter on Selmer groups. We also define a group $S_{p,v} = \varinjlim_n S_{p^n,v}$ this is the p-primary Selmer group over v, namely $\operatorname{Im}\kappa_{v,p}$, then the p-primary subgroup of the Selmer group satisfies $\mathrm{Sel}(E[p^\infty]/K) = \bigcap_v S_{p,v}$.

On the other hand by analogy one can define $S_{m,v}$ for any m instead of p^n in the very same way with a diagram and take an injective limit over all m. This way one would obtain a group S_v that lives inside $H^1(K, E(\overline{K})_{tors})$. Then by definition the Selmer group is just $\mathrm{Sel}(E/K) = \bigcap_v S_v$, so we may call our S_v a ***local Selmer group*** and correspondingly groups $S_{p,v}$ to be called ***local p-Selmer groups***.

Let's see how they relate to the unramified cohomology. From the definition of $S_{p^n,v}$ we get the image of $S_{p^n,v}$ under vertical map f which lives in $H^1(K_v, E(\overline{K_v})[p^n])$ to be contained in the image of the Kummer map $\operatorname{Im}\kappa_{v,p} \subset H^1(K_v, E(\overline{K_v})[p^n])$.

We take the exact diagram 6.2 above for all n and take the inverse limit of all such diagrams over all n tensoring with $\mathbb{Q}_p$ afterwards to get a new group $S'_{p,v}$.

$$S'_{p,v} := \varprojlim_n S_{p^n,v} \otimes \mathbb{Q}_p$$

$$\begin{array}{ccccc} & & & \searrow & \\ E(K)\otimes\mathbb{Q}_p & \xrightarrow{\kappa_p} & H^1(K, V_pE(\overline{K})) & & \\ \downarrow & & \downarrow f & \searrow & \\ E(K_v)\otimes\mathbb{Q}_p & \xrightarrow{\kappa_{v,p}} & H^1(K_v, V_pE(\overline{K_v})) & \longrightarrow & H^1(K_v, V_pE(\overline{K_v}))/\operatorname{Im}\kappa_{v,p} \end{array}$$

Then the obtained $S'_{p,v}$ maps via the vertical arrow f into a subgroup of $H^1(K_v, V_pE(\overline{K_v}))$ contained in the image of the Kummer map. Then by the lemma 6.3

$$S'_{p,v} \subseteq H^1_{ur}(K_v, V_pE(\overline{K_v})) \subset H^1(K_v, V_p(E)).$$

Fact 6.4. *In the setting of the Lemma 6.3 denote by $\mathcal{E}$ the Neron model of elliptic curve E over $\operatorname{Spec}\mathcal{O}_{K_v}$ and by $\mathcal{E}^0$ the identity component of the special fiber of the Neron model. Then there is an isomorphism of $\operatorname{Gal}(\overline{K}_v/K_v)$-modules*

$$T_l\mathcal{E}^0 \simeq (T_lE)^{I_v}.$$

It follows immediately that $V_l\mathcal{E}^0 \simeq (V_lE)^{I_v}$.

Proof. Take a finite unramified extension L_w/K_v, then $\operatorname{Spec}\mathcal{O}_{L_w}$ is smooth over $\operatorname{Spec}\mathcal{O}_{K_v}$ and by Neron mapping property we get $\mathcal{E}(\mathcal{O}_{L_w}) \simeq E(L_w)$. Passing to the limit we get $\mathcal{E}(\mathcal{O}^{nr}) \simeq E(K_v^{nr})$, where $\mathcal{O}^{nr}$ is the ring of integers of K_v^{nr} – maximal unramified extension of K_v.

On the other hand we know $E(\overline{K})^{I_v} \simeq E(K_v^{nr})$, then it follows $(T_lE)^{I_v} \simeq \varprojlim E(K_v^{nr})[l^n]$. By the above this shows $T_l\mathcal{E} \simeq (T_lE)^{I_v}$. Consider the exact

sequence defining the component group of the special fiber

$$1 \to \widetilde{\mathcal{E}}^0(k_v) \to \widetilde{\mathcal{E}}(k_v) \to \Phi_v \to 1,$$

then corresponding sequence of Tate modules is left-exact. Moreover since Φ_v is a finite group we get $T_l\Phi_v = 0$, therefore $T_l\mathcal{E} \simeq T_l\mathcal{E}^0$. □

Remark 6.5. *In view of this fact we may restate lemma 6.3 in the following way: The subspace of unramified cohomology $H^1_f(K_v, V_lE(\overline{K}_v))$ contains the image of the Kummer map and localization map*

$$E(K)\widehat{\otimes}\mathbb{Q}_l/\mathbb{Z}_l \to H^1(K_v, V_l\mathcal{E}^0(\mathcal{O}_{K_v^{nr}})).$$

Proof. of the Lemma 6.3. Recall that the Kummer map is the boundary map in the long exact cohomology sequence $E(K_v)/l^n \to H^1(K_v, E[l^n])$ so it sends a point $P \in E(K_v)$ into an $E[l^n]$-torsor of points Q such that $[l^n]Q = P$. In the case when elliptic curve E has good reduction over p the Neron model $\mathcal{E}$ over $\mathcal{O}_{K_v}$ is smooth and proper and a point $P \in E$ maps into a point P' of $\mathcal{E}$ via the diagram

$$\begin{array}{ccc} \mathcal{E} & \longleftarrow & E \\ \uparrow & & \uparrow \\ \operatorname{Spec}\mathcal{O}_{K_v} & \longleftarrow & \operatorname{Spec}K_v \end{array}$$

In all other cases the same holds for the identity component $\mathcal{E}^0(\mathbb{F}_p)$ of the special fiber of the Neron model instead of $\mathcal{E}(\mathbb{F}_p)$. Therefore all points Q from the $E[l^n]$-torsor corresponding to P map into points $Q' \in \mathcal{E}$ such that $[l^n]Q' = P'$ which means that all such Q' form an $\mathcal{E}^0[l^n]$-torsor.

In the case when E has good reduction over v we have $\mathcal{E}$ being finite etale over $\mathcal{O}_{K_v}$ (or in the case of bad reduction $\mathcal{E}^0$ finite etale) and since $v \nmid l$ all the $[l^n] : \mathcal{E}^0 \to \mathcal{E}^0$ are finite etale as well. In the case of good reduction everything is unramified so we have $V_lE^{I_{K_v}} = V_lE$ and thus image of the Kummer map lives in $H^1(G_{K_v}/I_{K_v}, E[l^n])$, in the case of bad reduction all

moves to $H^1(G_{K_v}/I_{K_v}, E[l^n]^{I_v})$.

As we have already mentioned above since the place v is away from p, the morphism $[p] : E(K) \to E(K)$ is a finite etale map. Now note that by inflation-restriction sequence it follows from definition of Bloch-Kato Selmer group, that $H^1_{ur}(K_v, V) = H^1(G_{K_v}/I_{K_v}, V^{I_{K_v}})$ for any V, so all we need is for image of composition 6.1 to land in $H^1(G_{K_v}/I_{K_v}, V_l E^{I_{K_v}}) = H^1(G_{K_v}/I_{K_v}, V_l\mathcal{E}^0)$.

Note that this lemma (and proof) still hold for more general situation when instead of elliptic curve one works with abelian variety. □

6.3 The case $v \mid p$

Now we want to define local Bloch-Kato Selmer group for the case when v is above p, that would require some knowledge of basic p-adic Hodge theory from the corresponding chapter. By analogy to the definition of unramified cohomology we define local Bloch-Kato Selmer group as kernel of some map from local cohomology $H^1(K_v, V)$ but now we are working with a p-adic representation V over a p-adic field K_v. Therefore we don't speak of inertia subgroup.

Definition 6.6. *The local Bloch-Kato Selmer group is defined as*

$$H^1_f(K_v, V) = \ker(H^1(K_v, V) \to H^1(K_v, V \otimes \mathbf{B}_{cris}(\mathbb{Z}_p))) \tag{6.3}$$

We want to have an analog of lemma 6.3 for the case when our representation is the rational Tate module $V = V_pE$ for an elliptic curve E.

Lemma 6.7. *Let E be an elliptic curve over a number field K, let v be a place of K above p, no assumption on reduction required. For the p-adic representation V_pE the image of Kummer map*

$$E(K_v)\widehat{\otimes}\mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa} H^1(K_v, V_pE(\overline{K_v})). \tag{6.4}$$

coincides with $H^1_f(K_v, V_pE(\overline{K_v}))$.

In the proof of lemma in this case we will be using results from later chapter on Dieudonne theory, namely Lemma 8.2 and Theorem 8.17.

Proof. First note that the Kummer map above is injective. Consider the group of points of an elliptic curve E over K_v as a compact $p-$adic Lie group. The group of points on the Neron model $\mathcal{E}(\mathcal{O}_{K_v})$ contains a connected component $\mathcal{E}^0(\mathcal{O}_{K_v})$ which is a finite free $\mathbb{Z}_p$-module. Then the p-adic completion $E(K_v)\widehat{\otimes}\mathbb{Q}_p$ of the group of points on E over K_v is isomorphic to an open subgroup of $E(K_v)$. Therefore there is no open subgroup of $E(K)$ which maps to 0 under Kummer map.

In order to prove the claim we need to check that Kummer map goes into $H^1_f(K_v, V_pE(\overline{K_v}))$ and to prove that $E(K_v)\widehat{\otimes}\mathbb{Q}_p$ and $H^1_f(K_v, V_pE(\overline{K_v}))$ have the same dimension as $\mathbb{Q}_p$-vector spaces.

In order to see that the image of κ belongs to $H^1_f(K_v, V_pE(\overline{K_v}))$ we use an isomorphism $H^1(K_v, V_pE(\overline{K_v})) \simeq \mathrm{Ext}^1_{G_{K_v}}(\mathbb{Q}_p, V_pE(\overline{K_v}))$ which brings out description of $H^1(K_v, V_pE(\overline{K_v}))$ in terms of extensions

$$0 \to V_pE \to V \to \mathbb{Q}_p \to 0.$$

Such an extension corresponds to an element in $H^1_f(K_v, V_pE(\overline{K_v}))$ if and only if the corresponding extension

$$0 \to \mathbf{D}_{cris}(V_pE) \to \mathbf{D}_{cris}(V) \to \mathbf{D}_{cris}(\mathbb{Q}_p) = \mathbf{B}_{cris} \to 0$$

is a short exact sequence. This happens when a p-adic representation V has the same property as V_pE, i.e. it is crystalline or semi-stable together with V_pE. More on this see chapter 3 of [BK90]. Recall from lemma 8.2 that V_pE is crystalline if E has good reduction at p and it is semi-stable if E has multiplicative reduction, assume for now that reduction is good and V_pE is crystalline. Then all we need is to prove that V is crystalline.

Denote as usual $\mathcal{E}$ the Neron model of E over $\mathcal{O}_{K_v}$, then we are working with

a class $\xi \in E(K_v) = \mathcal{E}(\mathcal{O}_{K_v})$. We take a pullback of the short exact sequence

$$0 \to \mathcal{E}[p^n] \to \mathcal{E} \xrightarrow{p^n} \mathcal{E} \to 0$$

along ξ and view it as an $\mathcal{E}[p^n]$-torsor over $\mathcal{O}_{K_v}$. It canonically corresponds to a short exact sequence

$$0 \to \mathcal{E}[p^n] \to X \to \mathbb{Z}/p^n \to 0,$$

where X is a p-divisible group over $\mathcal{O}_{K_v}$. Since all these sequences are compatible for all n we can take an inverse limit to end up with an extension of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mathcal{E}[p^\infty]$ with a p-divisible group X_∞ over $\mathcal{O}_{K_v}$.

$$0 \to \mathcal{E}[p^\infty] \to X_\infty \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

We then use the following theorem to get what we wanted.

Theorem 6.8. ***Fontaine*** *Let $\mathcal{O}_{K_v}$ be the ring of integers in a p-adic field K_v, let G be a p-divisible group over $\mathcal{O}_{K_v}$, then the p-adic representation $V_p(G)$ is crystalline.*

In more general case of multiplicative reduction instead of complete Neron model one has to think about the connected component of 0 with proof similar to above.

Consider the logarithmic map $\log : E(K_v) \to t_{E(K_v)}$, it has the set of torsion points of $E(K_v)$ as its kernel, however it is locally injective near $O \in E(K_v)$. Moreover it is an isomorphism on the connected component of 0, which is a finite index subgroup of $E(K_v)$ to an open subgroup of Lie$E(K_v)$. Then we get $\dim \kappa(E(K_v) \otimes \mathbb{Q}_p) = [K_v : \mathbb{Q}_p]$.

On the other hand by theorem 8.17 we have

$$\dim H^1_f(K_v, V_pE(\overline{K_v})) = \dim_{\mathbb{Q}_p} \mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE) = [K_v : \mathbb{Q}_p].$$

Where the first equality holds as V_pE is de Rham in any reduction case. □

6.4 Conjecture about order of vanishing

After defining Bloch-Kato Selmer group for all local cases the definition of global Bloch-Kato Selmer group naturally comes to mind as:

Definition 6.9. *For a p-adic representation V of $G_K = \mathrm{Gal}(\overline{K}/K)$ the global Bloch-Kato Selmer group $H^1_f(K,V)$ is the subspace of $H^1(K,V)$ defined by the following commutative diagram:*

$$\begin{array}{ccc} H^1_f(K,V) & \longrightarrow & H^1(K,V) \\ \downarrow & & \downarrow{\scriptstyle res_v} \\ \prod_v H^1_f(K_v,V) & \longrightarrow & \prod_v H^1(K_v,V) \end{array}$$

Namely all the elements in $H^1(K,V)$ that land in groups $H^1_f(K_v,V)$ for all valuations v on K.

In their article Bloch and Kato call this object finite cohomology by analogy with finite adeles. One can not help but notice a vast similarity with definition of usual Selmer group.
We now have enough tools to formulate the main conjecture of this section.

Conjecture 6.10. ***Bloch-Kato*** *For a p-adic representation V coming from geometry the order of vanishing of L-function equals the difference between dimension of global Bloch-Kato Selmer group and Galois fixed points of V.*

$$\dim_{\mathbb{Q}_p} H^1_f(K,V^\vee(1)) - \dim_{\mathbb{Q}_p} H^0(K,V^\vee(1)) = \mathrm{ord}_{s=0}\, L(V,s).$$

Let's see what it means for our favourite case of $V = V_pE$ where E is an elliptic curve. If we take a number field K, then we have $\dim_{\mathbb{Q}_p} H^0(K,V) = 0$ since $E(K)$ is finitely generated by Mordell-Weil theorem, so starting from some n

we would not find any points of order p^n. Then conjectural formula becomes

$$\dim_{\mathbb{Q}_p} H^1_f(K, V_pE^\vee(1)) = \operatorname{ord}_{s=0} L(V_pE^\vee(1), s) = \operatorname{ord}_{s=1} L(V_pE, s).$$

Which in turn by Lemmas 6.3, 6.7 implies the first part of BSD conjecture.

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank} E(K)$$

Note that for motivic L-function we consider order of vanishing at 0 and for the L-function of elliptic curve we look at order of vanishing at 1. This happens because of twist in our motive $\mathcal{M} = h^1(E)(1)$ by one.

The next two chapters recall classical but not widely studied subjects from p-adic Hodge theory. Most of definitions and statements will be needed for computation of measure of Bloch-Kato Selmer group in the equicharacteristic case.

Chapter 7

Fontaine's rings of period

The rings we will study in this chapter play central role in the p-adic analogue of Hodge theory, they are needed for the formulation of Bloch-Kato conjecture, and as preface to [FF18] suggests they provide an enviroment for studying the Fargues-Fontaine curve. This theory was originally introduced by Jean Marc Fontaine in his 1994 Asterisque article [Fon94b] and deeply studied and much needed afterwards.

We would like to recall here definitions of all Fontaines rings $\mathbf{A}_{inf}$, $\mathbf{B}_{dR}$, $\mathbf{B}_{cris}$, $\mathbf{B}_e$, $\mathbf{B}_{st}$ to build all fundamental exact sequences that we will need later in chapters. All of the below is well-known theory written in many documents thus we recall only important statements and constructions referring for proofs to [Fon94b], [FF18], [BMS18].

First we would like to introduce the ring $\mathbf{A}_{inf}$ as "the one to rule them all" in the collection of works dedicated memory of Fontaine and Wintenberger [Col19]. Fix a prime p and a commutative ring R separated and complete with respect to the p-adic topology. Consider the absolute Frobenius map $\mathrm{Fr} : R/pR \to R/pR$. We define ***the tilt*** of R as:

Definition 7.1.

$$R^\flat := \varprojlim_{\mathrm{Fr}} R/pR;$$

Then the infinitesimal period ring $\mathbf{A}_{inf}(R)$ *is defined as the Witt vectors ring*

of the tilt of R.

$$\mathbf{A}_{inf}(R) := W(R^\flat).$$

To an element $x \in R$ correspond an element $x^\flat \in R^\flat$ defined as an infinite sequence of p-th roots of x, i. e. $x^\flat := (x^{(0)} = x, x^{(1)}, \dots, x^{(n)}, \dots)$ such that $(x^{(n+1)})^p = x^{(n)}$ for all n. With such interpretation $R^\flat$ contains unit $\epsilon = (1, \zeta_p, \zeta_{p^2}, \dots)$ where each ζ_{p^n} is a primitive root of degree p^n of 1.
This currently "set" $R^\flat$ can be given a structure of ring, namely it easily becomes multiplicative monoid with " $\cdot$ " defined on elements as $x^\flat \cdot y^\flat = (x^{(0)}, x^{(1)}, \dots, x^{(n)}, \dots) \cdot (y^{(0)}, y^{(1)}, \dots, y^{(n)}, \dots) = (x^{(0)}y^{(0)}, x^{(1)}y^{(1)}, \dots, x^{(n)}y^{(n)}, \dots)$.
The following lemma is proven in the thesis of P. Scholze:

Lemma 7.2. *The tilt $R^\flat$ and $\varprojlim_{x \mapsto x^p} R$ are isomorphic when viewed as multiplicative monoids.*

The addition in $R^\flat$ is slightly more complicated. In order to add two elements $x^\flat = (x^{(0)}, x^{(1)}, \dots, x^{(n)}, \dots)$ and $y^\flat = (y^{(0)}, y^{(1)}, \dots, y^{(n)}, \dots)$ we take corresponding

$$(x+y)^{(n)} := \lim_{k \to \infty} (x^{(n+k)} + y^{(n+k)}).$$

So far we have defined the map $R \to R^\flat$ on elements above, but there is one more called $\# : R^\flat \to R$ defined as following:

Definition 7.3. *We take an element $\overline{a} = (\overline{a}_0, \dots \overline{a}_n, \dots) \in R^\flat = \varprojlim_{\mathrm{Fr}} R/pR$, lift all $\overline{a}_i$ to elements $a_i \in R$ in any way we wish and define*

$$\overline{a}^\# := \lim_{n \to \infty} a_n^{p^n} \in R$$

An alternative definition would be to view $R^\flat$ as $\varprojlim_{x \mapsto x^p} R$ as above and for an element $x = (x^{(0)}, x^{(1)}, \dots, x^{(n)}) \in R^\flat$ define $x^\# = x^{(0)}$. This map $\#$ gives correspondence between the valuations on rings R and $R^\flat$.

Now that we understood what the tilt really is we can look at its ring of Witt

vectors

$$\mathbf{A}_{inf}(R) := W(R^\flat).$$

For an element $x \in R^\flat$ denote by $[x]$ the Teichmuller lift of x to $W(R^\flat)$. Then any element of $W(R^\flat)$ can be represented in unique way as a series $\sum_k p^k[x_k]$. There exists a Frobenius lift from R/p to $R^\flat$ and therefore to the whole $\mathbf{A}_{inf}(R)$ as the Witt vector Frobenius. The map itself can be described as $\mathrm{Fr}(\sum_k p^k[x_k]) = \sum_k p^k[x_k^p]$.

Definition 7.4. *We define the Fontaine's map* $\theta : \mathbf{A}_{inf}(R) \to R^\flat \xrightarrow{\#} R$ *by*

$$\theta(\sum_k p^k[x_k]) := \sum_k p^k x_k^\#.$$

It is a hard but greatly important theorem that this map θ *is surjective and the ideal of its kernel is principal, generated by a distinguished element* $d = p - [p^\flat]$*, then* $(d) \subset \mathbf{A}_{inf}(R)$*.*

This ideal is what defines all the further rings of Fontaine.

Definition 7.5. *The ring* $\mathbf{A}_{cris}(R)$ *is defined as a formal p-adic PD-thickening of* $\mathbf{A}_{inf}$ *with respect to the ideal* $J = (d) \subset \mathbf{A}_{inf}(R)$ *completed in p-adic topology, namely*

$$\mathbf{A}_{cris}(R) := \widehat{\mathbf{A}_{inf}\Big[\frac{(d)^k}{k!}\Big]}, \text{for all } k \in \mathbb{N};\ \mathbf{B}^+_{cris} := \mathbb{Q}_p \otimes \mathbf{A}_{cris}.$$

Next we define the de Rham period ring.

Definition 7.6. *The ring* $\mathbf{B}^+_{dR}$ *is the completion of* $\mathbf{A}_{inf}(R)[\frac{1}{p}]$ *with respect to* (d)*, namely*

$$\mathbf{B}^+_{dR} := \varprojlim_k (\mathbf{A}_{inf}(R)\Big[\frac{1}{p}\Big]/(d)^k).$$

This ring has a number of valuable properties: it is a discrete valuation ring with residue field $R[\frac{1}{p}] = \mathrm{Frac}(R)$, it also contains $\mathbf{A}_{cris}$ as a subring, in case of $R = \mathbb{Z}_p$ it is non-canonically isomorphic to $\mathbb{C}_p[[t]] \simeq \mathbf{B}^+_{dR}$ and if one wishes, one can consider this case whenever $\mathbf{B}^+_{dR}$ appears on horizon.

To define higher rings $\mathbf{B}_{dR}$ and $\mathbf{B}_{cris}$ we need the logarithm of p-th roots of unity $t = \log([\epsilon])$ defined as usual by formal Taylor series of $\sum_k \frac{(1-[\epsilon])^k}{k}$ as variable.

Definition 7.7. *The cristalline period ring and the de Rham period field are defined as:*

$$\mathbf{B}_{cris} := \mathbf{B}^+_{cris}\Big[\frac{1}{t}\Big], \text{ and } \mathbf{B}_{dR} := \mathbf{B}^+_{dR}\Big[\frac{1}{t}\Big].$$

The de Rham period ring $\mathbf{B}_{dR}$ is a field and carries a decreasing filtration defined by degrees of t as $\mathrm{Fil}^i\mathbf{B}_{dR} = t^i\mathbf{B}^+_{dR}$.
By definition the element t belongs to $\mathbf{A}_{cris}$, therefore to all the other rings $\mathbf{B}^+_{cris}$ and $\mathbf{B}_{cris}$. Then Frobenius morphism extends from $\mathbf{A}_{inf}$ to $\mathbf{A}_{cris}$ as $\mathrm{Fr}\, t = pt$, and further to $\mathbf{B}^+_{dR}$ and $\mathbf{B}^+_{cris}$, moreover the Frobenius agrees with filtration on $\mathbf{B}_{dR}$.

Example 7.8. *The important case of the above recollection is when we start with the ring of integers $R = \mathcal{O}_{\mathbb{C}_p}$, where $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ it fits all the requirements. One may keep this example in their head whenever we address this section. Then the tilt of R is $R^\flat \simeq \mathcal{O}_{\mathbb{C}_p^\flat} \simeq \mathcal{O}_{\widehat{\overline{\mathbb{F}_p((u))}}}$, the ring $\mathbf{A}_{inf}(R) = W(\mathcal{O}_{\mathbb{C}_p^\flat})$, an element d can be represented as $d = p - [u] \in \mathbf{A}_{inf}(R)$.*

Proof. This can be proven starting from an isomorphism $\varprojlim_{x\mapsto x^p} \mathbb{Z}_p \simeq \mathbb{F}_p[[u]]$ given by $u := p^\flat = (p, p^{1/p}, p^{1/p^2}, ...)$. Then taking fraction fields we get $\varprojlim_{x\mapsto x^p} \mathbb{Q}_p \simeq \mathbb{F}_p((u))$, which after algebraic closure and completion becomes

$$\mathbb{C}_p^\flat = \varprojlim_{x\mapsto x^p} \widehat{\overline{\mathbb{Q}_p}} \simeq \widehat{\overline{\mathbb{F}_p((u))}}.$$

□

For the case of the semi-stable reduction we need the ring $\mathbf{B}^+_{st}$. To define it we use the $\log[p^\flat] =: s$.

Definition 7.9. *The semi-stable period ring is defined as:*

$$\mathbf{B}_{st}^{+} := \mathbf{B}_{cris}^{+}[s] \text{ and } \mathbf{B}_{st} := \mathbf{B}_{cris}[s] = \mathbf{B}_{st}^{+}[\frac{1}{t}].$$

Additionally to the Frobenius morphism defined by $\mathrm{Fr}(s) := ps$ *this rings carry the monodromy operator* $N : \mathbf{B}_{st} \to \mathbf{B}_{st}$ *defined as the unique derivation such that* $N(s) := 1$*, which commutes with* $G_{\mathbb{Q}_p}$*-action and has the property* $N \circ \mathrm{Fr} = p\,\mathrm{Fr} \circ N$*.*

By definition the monodromy operator fits into a short exact sequence:

$$0 \to \mathbf{B}_{cris} \to \mathbf{B}_{st} \xrightarrow{N} \mathbf{B}_{st} \to 0.$$

Lemma 7.10. *The morphism from the above sequence* $\mathbf{B}_{st} \to \mathbf{B}_{dR}$ *extending an inclusion* $\mathbf{B}_{cris} \hookrightarrow \mathbf{B}_{dR}$ *is* $G_{\mathbb{Q}_p}$*-equivariant. It allows us to define a decreasing filtration on* $\mathbf{B}_{st}$ *that agrees with the Frobenius morphism.*

Consider a finite totally ramified extension K of $\mathbb{Q}_p$. There is an action of $\mathrm{Gal}(\mathbb{C}_p/K)$ on $\mathbf{A}_{inf}$ commuting with Frobenius automorphism that lifts all the way to $\mathbf{A}_{cris}$ and to $\mathbf{B}_{dR}$ respecting the filtration. We will assume from now this to be our case of concern.

Definition 7.11. *There is an ideal* J *in the ring* $\mathbf{B}_{cris}^{+}$ *defined by the following sequence:*

$$0 \to J \to \mathbf{B}_{cris}^{+} \to \mathbb{C}_p \to 0;$$

A close look at it gives out J *to be the kernel of the map induced from* $\theta : \mathbf{A}_{inf} \to \mathcal{O}_{\mathbb{C}_p}$*, therefore* J *is the ideal of* $\mathbf{B}_{cris}^{+}$ *generated by all the divided powers of* d*, namely:* $J = \langle \gamma_n(d) \rangle$*. There is a descending filtration of* J *by ideals* $J^{[r]}$ *defined as* $J^{[r]} := \langle \gamma_n(d), \text{ for } n \geq r \rangle$*.*

Fontaine has proven in his original Asterisque article [Fon94b] the exactness

of the sequences below and defined filtration on $\mathbf{B}^+_{cris}$ by $J^{[r]}$:

$$\begin{aligned} 0 \to \mathbb{Q}_p(r) \to J^{[r]} \xrightarrow{1-p^{-r}\,\mathrm{Fr}} \mathbf{B}^+_{cris} \to 0 \\ 0 \to \mathbb{Q}_p(r) \to J^{[r]} \xrightarrow{1-p^{-r}\,\mathrm{Fr}} \mathbf{B}_{cris} \to 0 \end{aligned} \tag{7.1}$$

One more piece of magic of ideals $J^{[r]}$ gives an alternative definition of de Rham period ring as in the following lemma. We would like to prove here that the definition of $\mathbf{B}^+_{dR}$ by Bloch and Kato in [BK90] is equivalent to the classical one.

Lemma 7.12.

$$\mathbf{B}^+_{dR} \simeq \varprojlim_r \mathbf{B}^+_{cris}/J^{[r]}$$

Proof. We need to construct a map from $\mathbf{B}^+_{dR}$ to every $\mathbf{B}^+_{cris}/J^{[r]}$ so that all this maps for all r agree and prove that the object $\mathbf{B}^+_{dR}$ is universal with respect to this property. Observe by the definition of $\mathbf{B}^+_{cris}$ above that

$$\mathbf{B}^+_{cris}/J^{[r]} = (\mathbf{A}_{inf}\widehat{\Big[\Big\langle \frac{(d)^k}{k!} \Big\rangle\Big]} \otimes \mathbb{Q}_p)/J^{[r]},$$

It is enough to build a morphism

$$\mathbf{A}_{inf}\Big[\frac{1}{p}\Big]/(d)^k \to \mathbf{A}_{inf}\Big[\Big\langle \frac{(d)^k}{k!} \Big\rangle\Big] \otimes \mathbb{Q}_p)/J^{[r]}$$

then construction of the map into the completion $\mathbf{A}_{inf}\widehat{[\langle \frac{(d)^k}{k!} \rangle]}$ will follow as well as the morphism from the inverse limit of all right hand sides for all k into $\mathbf{B}^+_{dR}$. By definition of $J^{[r]}$ we may rewrite the latest factor as $\mathbf{A}_{inf}[\langle \frac{(d)^k}{k!} \rangle][\frac{1}{p}]/\frac{d^r}{r!}$ since A_{inf} is a $\mathbb{Z}_p$-module. Then we use natural maps for all r

$$\mathbf{A}_{inf}\Big[\frac{1}{p}\Big]/(d)^r \to \mathbf{A}_{inf}\Big[\Big\langle \frac{(d)^k}{k!} \Big\rangle\Big]\Big[\frac{1}{p}\Big]/\Big(\frac{d^r}{r!}\Big).$$

The constructed maps $\mathbf{B}^+_{dR} = \varprojlim_r \mathbf{B}^+_{cris}/J^{[r]}$ all agree.

We are left to prove the universal property and in order to get it assume there is

a module P with a morphism $P \to \varprojlim_r \mathbf{B}^+_{cris}/J^{[r]}$. Then P must be d-adically complete since the limit above is by the definition of $J^{[r]}$ containing raising powers of d. Also P maps to $\mathbf{A}_{inf}[\frac{1}{p}]$ if we take $k = r = 0$, therefore there is a morphism $P \to \mathbf{B}^+_{dR}$. □

In the preface to [FF18] P. Colmez calls the ring $\mathbf{B}_e$ "main", it was proven by J. M. Fontaine that it belongs to the class of Bezout rings, currently common notion for $\mathbf{B}_e$ is "exponential". The ring has multiple mysterious properties unlike other period rings, some of those properties remain unknown and they are listed in the same text. The ring is defined quite easily $\mathbf{B}_e := \mathbf{B}^{\mathrm{Fr}=1}_{cris}$, where the Frobenius action comes from $\mathbf{A}_{cris}$ and $\mathrm{Fr}(t) = pt$. But that's where the easy things about it come to end, we do not even know how its residue ring looks like. This ring $\mathbf{B}_e$ plays central role in formulation of Bloch-Kato conjecture by sitting in the middle of the fundamental exact sequence, recall from [FO] Theorem 6.26:

Theorem 7.13. *The following sequence is exact*

$$0 \to \mathbb{Q}_p \to \mathbf{B}_e \to \mathbf{B}_{dR}/\mathbf{B}^+_{dR} \to 0; \tag{7.2}$$

It is equivalent to the following two facts: first is that $\mathbf{B}_e \cap \mathbf{B}^+_{dR} = \mathbb{Q}_p$, and second is $\mathbf{B}_e + \mathbf{B}^+_{dR} = \mathbf{B}_{dR}$. Then $\mathbf{B}_{dR}/\mathbf{B}^+_{dR} \simeq \mathbf{B}_e/\mathbf{B}_e \cap \mathbf{B}^+_{dR}$ from where follows everything we need.

As a direct consequence we obtain

Corollary 7.14.

$$0 \to \mathbb{Q}_p \xrightarrow{a} \mathbf{B}_e \oplus \mathbf{B}^+_{dR} \xrightarrow{b} \mathbf{B}_{dR} \to 0. \tag{7.3}$$

with maps defined by $a(x) = (x, x)$, *and* $b(x, y) = x - y$.

As a consequence we obtain the following exact sequence [BK90]:

Corollary 7.15.

$$0 \to \mathbb{Q}_p \xrightarrow{a} \mathbf{B}_{cris} \oplus \mathbf{B}^+_{dR} \xrightarrow{b} \mathbf{B}_{cris} \oplus \mathbf{B}_{dR} \to 0. \tag{7.4}$$

With maps defined by $a(x) = (x, x)$ *and* $b(x, y) = (x - \mathrm{Fr}(x), x - y)$.

Proof. The surjectivity of of the map b in the second variable follows from the corollary 7.14, the exactness in other terms is obvious, we need only surjectivity on $\mathbf{B}_{cris}$.

The surjectivity of $1 - \mathrm{Fr}$ follows from Theorem 5.3.7 (iii) in [Fon94b]. □

We would like to have an analogue of this corollary for the ring $\mathbf{B}_{st}$ instead of $\mathbf{B}_{cris}$ for one of the lemmas about bad semi-stable reduction. The short exact sequence is similar, however the kernel is a bit different.

Lemma 7.16. *Define the ring* $\mathbf{B}_{est} := \mathbf{B}_{st}^{\mathrm{Fr}=1}$. *We have* $\mathbf{B}_{est} \cap \mathbf{B}_{dR}^{+} = \mathbb{Q}_p$ *and* $\mathbf{B}_{est} + \mathbf{B}_{dR}^{+} = \mathbf{B}_{dR}$. *We have the following short exact sequence:*

$$0 \to \mathbb{Q}_p \xrightarrow{a} \mathbf{B}_{st} \oplus \mathbf{B}_{dR}^{+} \xrightarrow{b} \mathbf{B}_{st} \oplus \mathbf{B}_{dR} \to 0. \tag{7.5}$$

With maps defined by $a(x) = (x, x)$ *and* $b(x, y) = (x - \mathrm{Fr}(x), x - y)$.

Proof. The equality $\mathbf{B}_{est} + \mathbf{B}_{dR}^{+} = \mathbf{B}_{dR}$ follows immediately from $\mathbf{B}_{e} + \mathbf{B}_{dR}^{+} = \mathbf{B}_{dR}$, to prove $\mathbf{B}_{est} \cap \mathbf{B}_{dR}^{+} = \mathbb{Q}_p$ consider the intersection $\mathbf{B}_{cris}^{Fr=p^{-1}} \cap \mathbf{B}_{dR}^{+} =?$.
We prove this intersection is null. If there is a nonzero element $x \in \mathbf{B}_{cris}^{Fr=p^{-1}} \cap \mathbf{B}_{dR}^{+}$, then $tx \in \mathbf{B}_{e} \cap \mathbf{B}_{dR}^{+} = \mathbb{Q}_p$, so $t^{-1}x^{-1} \in \mathbb{Q}_p$, so $t^{-1} \in \mathbf{B}_{dR}^{+}$.
Now we have exactness of the sequence 7.5 everywhere except from the last member. To prove surjectivity of b we need to prove surjectivity of $1 - \mathrm{Fr}$ on $\mathbf{B}_{st}$. Consider the exact sequence of Fontaine for any $r \in \mathbb{Z}$:

$$0 \to \mathbb{Q}_p \to Fil^{r}\mathbf{B}_{cris} \xrightarrow{1-p^{-r}\,\mathrm{Fr}} \mathbf{B}_{cris} \to 0.$$

Due to this sequence and by definition of $\mathbf{B}_{st} = \mathbf{B}_{cris}[s]$ we only need to find an element $x \in \mathbf{B}_{st}$ such that $x - \mathrm{Fr}(x) = s$. Since in the case of $\mathbf{B}_{cris}$ the sequence above holds for any $r \in \mathbb{Z}$ there exists $y \in \mathbf{B}_{cris}$ such that $y - p\,\mathrm{Fr}(y) = -1$.
On the other hand by the short exact sequence

$$0 \to \mathbf{B}_{cris} \to \mathbf{B}_{st} \xrightarrow{N} \mathbf{B}_{st} \to 0$$

we get an element $x_0 \in \mathbf{B}_{st}$ such that $N(x_0) = y$. Plug it into the equality above to get $N(x_0) - p\,\mathrm{Fr} \circ N(x_0) = -1$. Recall that $N \circ \mathrm{Fr} = p\,\mathrm{Fr} \circ N$, so we get $N(x_0) - N(\mathrm{Fr}(x_0)) = N(s)$, therefore $s + \alpha = x_0 - \mathrm{Fr}(x_0)$ for some $\alpha \in \mathbf{B}_{cris}$. However we have by Theorem of Fontaine $\alpha = \beta - \mathrm{Fr}(\beta)$, so we just take $x := x_0 - \beta$.

□

Remark 7.17. *Note how one can immediately get the corollary 7.15 by applying invariants of monodromy on the 7.5 using the fact* $H^1(\langle N \rangle, \mathbb{Q}_p[s]) = 0$. *This happens because* $\mathbf{B}_{st} = \mathbf{B}_{cris}[s]$ *and* $N(s) = -1$ *by definition, so when we apply invariants of* N *to a subring* $B \subset \mathbf{B}_{st}$ *we are left with* $B \cap \mathbf{B}_{cris}$.

The exact sequences 7.14 and 7.15 are both needed for formulation of the refined Bloch-Kato conjecture, we will talk about it in later chapters.

Chapter 8

Dieudonne modules

8.1 Definition and main examples

There are different ways to define Bloch-Kato Selmer groups depending on the property of cohomology theory one wants to emphasize. One way would use the $\mathbf{B}_{dR}$ period ring and another uses $\mathbf{B}_e$. These different ways to define local Bloch-Kato Selmer groups are needed for construction of Bloch-Kato exponential and computation of dimensions of cohomology spaces.
Before working with them we would like to give a description of what can be done to a p-adic representation V. Throughout this section we will assume that V is a p-adic representation over a local field K_v with $v \mid p$ unless specified otherwise, i.e. the theory is developed for $l = p$ situation. We only recall necessary theorems and definitions, for proofs we refer to [Fon94a], [BB08], [BK90], [CF00], [Fon82]. The following definition is classical and can be found in the original article by Fontaine [Fon94a].

Definition 8.1. *Let V a be vector space over $\mathbb{Q}_p$ with a continuous action of a Galois group G_{K_v}. Then we define $\mathbb{Z}_p$-modules:*

- *The crystalline module $\mathbf{D}_{cris}(V) := H^0(K_v, \mathbf{B}_{cris} \otimes V) = (\mathbf{B}_{cris} \otimes V)^{G_{K_v}}$ is a vector space over K_v. It is equipped with action of Frobenius coming from Frobenius on $\mathbf{B}_{cris}$ and a filtration induced by ideals $J^{[r]}$ composing into filtration on $\mathbf{B}^+_{cris}$.*

- *The de Rham module* $\mathbf{D}_{dR}(V) := H^0(K_v, \mathbf{B}_{dR} \otimes V)$ *is a vector space over* K_v*, it inherits a decreasing separated and exhaustive filtration coming from the one on* $\mathbf{B}_{dR}$ *in the following way:* $\mathrm{Fil}^i \mathbf{D}_{dR}(V) = (\mathrm{Fil}^i \mathbf{B}_{dR} \otimes V)^{G_{K_v}}$.

- *The exponential module* $\mathbf{D}_e(V) := H^0(K_v, (\mathbf{B}_{cris} \otimes V)^{\mathrm{Fr}=1}) = H^0(K_v, \mathbf{B}_e \otimes V) = (\mathbf{B}_e \otimes V)^{G_{K_v}}$*. A submodule of* $\mathbf{D}_{cris}(V)$*, it inherits all the properties.*

- *The semi-stable module* $\mathbf{D}_{st}(V) := H^0(K_v, \mathbf{B}_{st} \otimes V) = (\mathbf{B}_{st} \otimes V)^{G_{K_v}}$ *a vector space over* K_v*. It has the action of Frobenius operator coming from* $\mathbf{B}_{st}$*, a monodromy operator* N*, and a decreasing filtration coming from* $\mathbf{B}_{dR}$*.*

Immediately by definition from inclusions $\mathbf{B}_e \subset \mathbf{B}_{cris} \subset \mathbf{B}_{st} \subset \mathbf{B}_{dR}$ we get the comparison of their dimensions:

$$\dim \mathbf{D}_e(V) \leq \dim \mathbf{D}_{cris}(V) \leq \dim \mathbf{D}_{st}(V) \leq \dim \mathbf{D}_{dR}(V) \leq \dim_{\mathbb{Q}_p} V \quad (8.1)$$

We call a p-adic representation $\mathbf{B}_*$-admissible if $\mathbf{D}_*(V) = \dim_{\mathbb{Q}_p} V$. We will often assume that representation V we are working with is $\mathbf{B}_{cris}$-admissible, or as we also call it *crystalline*. We would like to check this property for our main case of concern with $V = V_pE$.

Lemma 8.2. *Let* E *be an elliptic curve defined over the field of rational numbers* $\mathbb{Q}$*, let* p *be a prime of good reduction for* E*, then* V_pE *is crystalline and hence it is de Rham. When* p *is prime of multiplicative reduction the representation is not crystalline, however it is semistable. In case if* p *is of additive reduction* V_pE *is only a de Rham representation.*

Proof. The statement for the case of good reduction is the theorem of Fontaine. In case of any reduction type we have the dimension of V_pE over $\mathbb{Q}_p$ equal to 2. Now we need to compute dimension of the vector space $(\mathbf{B}_{cris} \otimes V_pE)^{G_{\mathbb{Q}_p}}$.

In the case of bad reduction $\dim V_pE(\overline{\mathbb{Q}_p})^{I_p} = 0$. This can be seen via applying an isomorphism $V_pE(\overline{\mathbb{Q}_p})^{I_p} \simeq V_p\widetilde{E}_{ns}(\overline{\mathbb{F}_p})$ that follows from the Fact 6.4 and knowledge of $\widetilde{E}_{ns}(\overline{\mathbb{F}_p}) = \overline{\mathbb{F}_p}^{\times}$ in case of multiplicative reduction and $\widetilde{E}_{ns}(\overline{\mathbb{F}_p}) = \overline{\mathbb{F}_p}^{+}$ in case of additive. Then considering Tate module we have $V_pE(\overline{\mathbb{Q}_p})^{I_p} = 0$. In the case of multiplicative reduction we can apply Tate uniformization after a finite unramified extension, then

$$0 \to \mathbb{Q}_p(1) \to V_pE \to \mathbb{Q}_p \to 0$$

by proof of the Lemma 2.13. We choose basis of V_pE over $\mathbb{Q}_p$ as above $\langle \varprojlim \zeta_{p^n}, \varprojlim q^{1/p^n} \rangle$ and recall the action of inertia group as $\begin{pmatrix} \chi(\sigma) & c(\sigma) \\ 0 & 1 \end{pmatrix}$ where $c(\sigma)$ is a p-adic integer. It remains to see how I_p acts on $\mathbf{B}_{cris}$ where we consider $\mathbf{A}_{inf} := \mathbf{A}_{inf}(\mathbb{Z}_p)$, then by definition $\mathbf{A}_{inf} = W(\mathbb{F}_p[[(p-[p^\flat])]])$. Then for the tilt of q in $\mathcal{O}^\flat_{\mathbb{C}_p} \ni q^\flat$ we have the action of σ described as $\sigma(q^\flat) = q\epsilon^{c(\sigma)}$, where $\epsilon = (1, \zeta_p, \zeta_{p^2}, ...)$ as defined in 7. Which means that Galois action on $\log[q^\flat]$ is $\sigma(\log[q^\flat]) = \log[q^\flat] + c(\sigma)\log[\epsilon]$. By definition of $\mathbf{B}_{cris}$ it contains $t = \log[\epsilon]$.

Moreover we have $\frac{q}{p^{v_p(q)}} \in \mathbb{Z}_p^\times$ and therefore $\log[(\frac{q}{p^{v_p(q)}})^\flat]$ exists in $\mathbf{B}^+_{cris}$. One may write by properties of logarithm $\log[q^\flat] = v_p(q)\log([p^\flat]) + \log[(\frac{q}{p^{v_p(q)}})^\flat]$. Then by definition of $\mathbf{B}_{st} := \mathbf{B}_{cris}[(\log[p^\flat])]$ we obtain $\log[q^\flat] \in \mathbf{B}_{st}$. Therefore $(\mathbf{B}_{st} \otimes V_pE)^{G_{\mathbb{Q}_p}}$ contains linearly independent elements $\log[q^\flat]$ and t which means semi-stability for V_pE.

On the other hand by the Lemma 6.11 in [FO] the element $\log[p^\flat]$ is transcendental over $\mathbf{B}_{cris}$ and so is $\log[q^\flat]$. So for p of multiplicative reduction the representation V_pE is not crystalline.

We need to prove that in case of additive reduction we still work with a de Rham representation. Recall that over large enough finite extension K of $\mathbb{Q}$ the curve E has either multiplicative or good reduction. Consider E over K, then $(\mathbf{B}_{dR} \otimes V_pE)^{\mathrm{Gal}(\overline{\mathbb{Q}_p}/K)}$ has dimension two and thus over K the representation

V_pE is de Rham. But taking invariants under $G_{\mathbb{Q}_p}/(\operatorname{Gal}\overline{\mathbb{Q}_p}/K) \simeq \operatorname{Gal} K/\mathbb{Q}_p$ doesn't change the dimension.

To put it all together we get the following: For $\mathbf{D}_*$ defined from $\mathbf{A}_{inf}(\mathbb{Z}_p)$:

$$\dim_{\mathbb{Q}_p} V_pE = \begin{cases} \dim \mathbf{D}_{cris}(V_pE) \text{ if } E \text{ has good reduction at } p; \\ \dim \mathbf{D}_{st}(V_pE) \text{ if } E \text{ has multiplicative reduction at } p; \\ \dim \mathbf{D}_{dR}(V_pE) \text{ in case of additive reduction.} \end{cases}$$

□

Example 8.3. *[Fal88], [BC09] Let K_v be a complete extension of $\mathbb{Q}_p$ with perfect residue field and let X be a smooth and proper algebraic variety over K_v. Define V to be ith etale cohomology of X, namely $V := H^i_{et}(X_{\overline{K_v}}, \mathbb{Q}_p)$. Then by comparison theorems of p-adic Hodge theory we obtain:*

- $\mathbf{D}_{dR}(V) = (\mathbf{B}_{dR} \otimes V)^{G_{K_v}} \simeq H^i_{dR}(X_{K_v})$.
- *If additionally to the above X has good reduction at v, then $\mathbf{D}_{cris}(V) = (\mathbf{B}_{cris} \otimes V)^{G_{K_v}} \simeq H^i_{cris}(\mathcal{X}_k/W(k))$, where k is the residue field of K_v, and $\mathcal{X}_k$ the reduction of proper regular model $\mathcal{X}$ of X over $\mathcal{O}_{K_v}$.*
- *If X has semi-stable reduction at v, namely the special fiber is represented by strictly normal crossing divisor, then $\mathbf{D}_{st}(V) = (\mathbf{B}_{st} \otimes V)^{G_{K_v}} \simeq H^i_{HK}(X)$. Here H^*_{HK} denote the Hyodo-Kato cohomology, or log-crystalline cohomology it is defined as*

$$H^*_{HK}(X) := H^*_{cris}(\mathcal{X}_k/Spec(W(k))_0) \otimes_{W(k)} \operatorname{Frac}(W(k)).$$

Where $Spec(W(k))_0$ is the log-scheme $Spec(W(k))$ with log-structure defined by $\mathbb{N} \to W(k)$ via $1 \mapsto 0$.

We see from this example how functors $\mathbf{D}_*$ compute various cohomology groups of X from its etale cohomology.

In order to complete the computation of L-function for elliptic curve E we need to write down explicit formula for $P_{\mathbb{Q}_p,p}(H^1_{et}(E,\mathbb{Q}_p)(1),t)$.

Lemma 8.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ with good reduction at p. Then $P_{\mathbb{Q}_p,p}(H^1_{et}(E,\mathbb{Q}_p)(1),t) = \det(1-\mathrm{Fr}_p^{-1}\,t|\mathbf{D}_{cris}(H^1_{et}(E,\mathbb{Q}_p)(1)))$.*

Proof. Note that by the example above in case when E has good reduction at p we have $\mathbf{D}_{cris}(H^1_{et}(E,\mathbb{Q}_p)) = H^1_{cris}(\mathcal{E}_{\mathbb{F}_p}/\mathbb{Z}_p)$. In this case one can compute $H^1_{cris}(\mathcal{E}_{\mathbb{F}_p}/\mathbb{Z}_p) \simeq \mathbb{Z}_p^2$.
Then by the Lefschetz trace formula for etale cohomology:

$$1 + p - \mathrm{Tr}_{\mathrm{Fr}_p}(H^1_{cris}(\mathcal{E}_{\mathbb{F}_p}/\mathbb{Z}_p)) = |\widetilde{E}(\mathbb{F}_p)|,$$

while the determinant of Fr_p equals p. Then the characteristic polynomial for Fr_p looks like $1 - a_p t + pt^2$.

□

8.2 Equivalence of categories

The modules in the Definition 8.1 are given by functors $\mathbf{D}_*$ which go from the category of p-adic representations of G_K to certain subcategories of the category of modules over $\mathbb{Z}_p$. In order to state precise theorems we need to define Hodge and Newton numbers to make sense of admissibility condition.

Definition 8.5. *We say that a module D over a p-adic field K is φ-module if D is equipped with a Frobenius action and a filtration that agree.*

- *For a φ-module D of rank 1 over K we choose a basis $v \in D$ and take λ such that $\varphi(v) = \lambda v$. Define the Newton number $t_N(D) := v_p(\lambda)$. In case of module D of higher rank than 1 we define $t_N(D) = t_N(\det D)$.*

- *For a filtered module D of rank 1 we choose a basis $v \in D$ and define the Hodge number t_H to be the unique $i \in \mathbb{Z}$ such that $v \in \mathrm{Fil}^i D \setminus \mathrm{Fil}^{i+1} D$. Again for module D of higher rank than 1 we define $t_H(D) = t_H(\det D)$.*

We call a filtered φ-module D over K ***admissible*** *if $t_N = t_H$.*

The following theorems additionally to their general beauty provide a construction of a p-adic representation starting from a filtered φ-module with continuous action of G_K. We will need to modify constructions of functors $\mathbf{V}_{cris}$ and $\mathbf{V}_{st}$ for the case of a $\mathbb{Z}_p$-lattice T in filtered φ-module.

Theorem 8.6. *[CF00]*
Let K be a p-adic field, we denote by G_K its absolute Galois group. Denote by $\mathcal{R}ep^{cris}_{\mathbb{Q}_p}(G_K)$ the category of $\mathbf{B}_{cris}$-admissible p-adic representations of G_K and by $\mathcal{MF}^{ad}\varphi_K$ the category of filtered admissible φ-modules over K. Then the functor

$$\mathbf{D}_{cris} : \mathcal{R}ep^{cris}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathcal{MF}^{ad}\varphi_K$$

is fully faithful, exact, tensor functor with the inverse functor given by $\mathbf{V}_{cris} : D \mapsto \mathrm{Fil}^0(\mathbf{B}_{cris} \otimes_K D)^{\varphi=1}$, together they give equivalence of categories:

$$\mathbf{D}_{cris} : \mathcal{R}ep^{cris}_{\mathbb{Q}_p}(G_K) \longleftrightarrow \mathcal{MF}^{ad}\varphi_K : \mathbf{V}_{cris}.$$

In particular for a crystalline representation V we have $\mathbf{V}_{cris}(\mathbf{D}_{cris}(V)) \simeq V$.

The Theorem of Fontaine has a semistable analogue proven by Hyodo and Kato, see [HK94] and [CF00].

Theorem 8.7. *Denote by $\mathcal{R}ep^{st}_{\mathbb{Q}_p}(G_K)$ the category of $\mathbf{B}_{st}$-admissible p-adic representations of G_K and by $\mathcal{MF}^{ad}(\varphi, N)_K$ the category of filtered admissible φ, N-modules over K. Then the functor*

$$\mathbf{D}_{st} : \mathcal{R}ep^{st}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathcal{MF}^{ad}(\varphi, N)_K$$

is fully faithful, exact, tensor functor with the inverse functor given by $\mathbf{V}_{st} : D \mapsto \mathrm{Fil}^0(\mathbf{B}_{st} \otimes_K D)^{N=0,\varphi=1}$, together they give equivalence of categories:

$$\mathbf{D}_{st} : \mathcal{R}ep^{st}_{\mathbb{Q}_p}(G_K) \longleftrightarrow \mathcal{MF}^{ad}(\varphi, N)_K : \mathbf{V}_{st}.$$

In particular $\mathbf{V}_{st}(\mathbf{D}_{st}(V)) \simeq V$.

The main focus of these theorems is about both categories $\mathcal{MF}^{ad}\varphi_K$ and $\mathcal{MF}^{ad}(\varphi, N)_K$ being abelian, while analogous categories without admissibility condition are additive, but not abelian.
Further on around measure computations we will be interested in valuating the functor $\mathbf{V}_{st}$ in the subcategory of $\mathbb{Z}_p$-modules inside $\mathcal{R}ep^{st}_{\mathbb{Q}_p}(G_K)$. For this we recall from [FL82] and [BM02] the definition of Dieudonne module:

Definition 8.8. *For a p-adic field K a filtered Dieudonne module D over is a module over $\mathcal{O}_K$ of finite type equipped with:*

(1) A decreasing, exhaustive, and separated filtration by $\mathbb{Z}_p$-submodules $D^{i+1} \subset D^i \subset D$ such that $D^i = D$ for $i << 0$ and $D^i = 0$ for $i >> 0$;

(2) A family of Frobenius operators $\varphi_i : D^i \to D$ such that $\varphi_i|_{D^{i+1}} = p\varphi_{i+1}$, and $D = \sum \varphi_i(D^i)$.

Such modules form a category denoted by $\mathcal{MF}\varphi_K$ with morphisms that respect filtrations and commute with Frobenius maps. Moreover by theorem of Fontaine and Laffaille it is a full subcategory in $\mathcal{MF}^{ad}\varphi_K$ and therefore abelian.

We then define for a filtered Dieudonne module D a functor $T_{cris}(D)$ as

$$T_{cris}(D) := \mathrm{Fil}^r(\mathbf{B}^+_{cris} \otimes_{\mathcal{O}_K} D)^{\varphi_r=1}(-r).$$

Where the filtration on the tensor product is represented by $\mathrm{Fil}^r(\mathbf{B}^+_{cris} \otimes_{\mathcal{O}_K} D) := \sum J^{[i]} \otimes D^{r-i}$. The following theorem is due to Fontaine and Laffaille.

Theorem 8.9. *[FL82]*
The functor $T_{cris}(D)$ goes from $\mathcal{MF}\varphi_K$ to the category of crystalline representations of $G_{\mathbb{Q}_p}$. It is exact and fully faithful.

It would have been enough just to consider filtered Dieudonne modules to compute measures of local groups if not for bad reduction primes which will

inevitably appear in the nearest future. To deal with those we will have to write down an analogue of Fontaine-Laffaille theory for semistable reduction.

Definition 8.10. *A filtered Dieudonne module with connection is a filtered Dieudonne module as above 8.8 with additional monodromy operator N defined as a $\mathbb{Z}_p$-linear endomorphism $N : D \to D$ such that $N\varphi = p\varphi N$. Namely N cooperates with filtration in the following way $N(\mathrm{Fil}^i D) \subset \mathrm{Fil}^{i-1} D$ and with Frobenius as $N\varphi_i = \varphi_{i-1} N$.*

We will need to replace $\mathbf{B}^+_{cris}$ with the ring $\mathbf{B}^+_{st}$, where monodromy operator is defined and to a module D we associate a filtered Dieudonne $\mathbf{B}^+_{st}$-module with connection $\mathbf{B}^+_{st} \otimes_{\mathbb{Z}_p} D$. But all of that must be done carefully for preservation of important properties.

The notion of connection comes from the way the monodromy operator N is defined on variables: $N(ax) = N(a)x + aN(x)$ for any $a \in \mathbf{B}^+_{st}$, $x \in D$.

Remark 8.11. *Filtered Dieudonne modules with connection form a category denoted by $\mathcal{MF}\varphi_K, N$. Morphisms in this category respect filtrations, commute with Frobenius maps, and with monodromy operators. The category $\mathcal{MF}\varphi_K, N$ is a full subcategory in $\mathcal{MF}^{ad}(\varphi, N)_K$ and the category of filtered Dieudonne modules $\mathcal{MF}\varphi_K$ embeds fully faithfully into $\mathcal{MF}\varphi_K, N$ as modules where the action of monodromy is trivial $N = 0$.*

Theorem 8.12. *[Bre02] For a filtered Dieudonne module with connection D we define a functor $T_{st}(D)$ as*

$$T_{st}(D) := \mathrm{Fil}^r(\mathbf{B}^+_{st} \otimes_{\mathcal{O}_K} D)^{\varphi_r=1}_{N=0}(-r).$$

The functor goes from $\mathcal{MF}\varphi_K, N$ to the category of semistable representations of $G_{\mathbb{Q}_p}$, it is exact and fully faithful.

We would like to give a definition and handy description of Bloch-Kato exponential map and for that by analogy with finite Bloch-Kato Selmer group $H^1_f(K_v, V)$ we define Bloch-Kato Selmer groups related to rings $\mathbf{B}_e$ and $\mathbf{B}_{dR}$.

Definition 8.13. *[BK90]*

- *The subspace of exponential cohomology* $H^1_e(K_v, V) = 0$ *if* $v \nmid p$, *and* $H^1_e(K_v, V) := \ker(H^1(K_v, V) \to H^1(K_v, \mathbf{B}_e \otimes V))$ *otherwise.*
- *The subspace of Bloch-Kato de Rham cohomology* $H^1_g(K_v, V) = H^1(K_v, V)$ *if* $v \nmid p$, *and* $H^1_g(K_v, V) := \ker(H^1(K_v, V) \to H^1(K_v, \mathbf{B}_{dR} \otimes V))$ *otherwise.*

By analogy with the above we take $\mathbf{B}_{st}$ *instead of* $\mathbf{B}_{cris}$ *and* $\mathbf{B}_{st}^{\mathrm{Fr}=1} = \mathbf{B}_e[s]$ *instead of* $\mathbf{B}_{cris}^{\mathrm{Fr}=1} = \mathbf{B}_e$ *to define the groups:*

- *The subspace of semi-stable cohomology* $H^1_{st}(K_v, V) := H^1_{cris}(K_v, V) = H^1_{ur}(K_v, V)$ *if* $v \nmid p$, *and* $H^1_{st}(K_v, V) := \ker(H^1(K_v, V) \to H^1(K_v, \mathbf{B}_{st} \otimes V))$ *otherwise;*
- *The subspace of semi-stable exponential cohomology* $H^1_{est}(K_v, V) := 0$ *if* $v \nmid p$, *and* $H^1_{est}(K_v, V) := \ker(H^1(K_v, V) \to H^1(K_v, \mathbf{B}_{st}^{\mathrm{Fr}=1} \otimes V))$ *otherwise;*

Then by definition we obtain $H^1_e(K_v, V) \subset H^1_{est}(K_v, V)$ and:

$$H^1_e(K_v, V) \subset H^1_f(K_v, V) \subset H^1_{st}(K_v, V) \subset H^1_g(K_v, V) \subset H^1(K_v, V)$$

8.3 The exponential map

Consider the fundamental exact sequence of p-adic period rings 7.1.

$$0 \to \mathbb{Q}_p \to \mathbf{B}_e \to \mathbf{B}_{dR}/\mathbf{B}_{dR}^+ \to 0$$

Tensoring it with our vector space V over $\mathbb{Q}_p$ and taking cohomology

$$0 \to V^{G_{K_v}} \to \mathbf{D}_e(V) \to (\mathbf{B}_{dR}/\mathbf{B}_{dR}^+ \otimes_{\mathbb{Q}_p} V)^{G_{K_v}} \to H^1(K_v, V) \to H^1(K_v, \mathbf{B}_e \otimes_{\mathbb{Q}_p} V)$$

Then in case when V is de Rham by definition of $H^1_e(K_v, V)$ we obtain the boundary map

$$\mathbf{D}_{dR}(V)/\mathbf{D}^+_{dR}(V) \to H^1_e(K_v, V). \tag{8.2}$$

It is surjective and has $\mathbf{D}_e(V)/V^{G_{K_v}}$ as kernel. This map is called the Bloch-Kato exponential, the reason for it is the following lemma proven in the article by Bloch and Kato in [BK90].

Lemma 8.14. *Let E be an elliptic curve over p-adic field K_v, where $v \mid p$. Then for the rational Tate module $V_p(E)$ the following diagram commutes:*

$$\begin{array}{ccc} t_E & \xrightarrow{exp} & E(K_v) \otimes \mathbb{Q} \\ \| & & \downarrow \delta \\ \mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE) & \xrightarrow{BK-exp} & H^1_e(K_v, V_pE) \end{array} \tag{8.3}$$

where t_E is the tangent space to E at the origin O and δ is an isomorphism coming from Kummer sequence. Here the upper horizontal map is the usual exponent of Lie algebra and the lower one is Bloch-Kato exponent.

Bloch and Kato prove in 4.1 in their article [BK90] the following:

Theorem 8.15. *Let V is $\mathbf{B}_{dR}$-admissible, or as often they are called, a de Rham representation, by definition 8.1 this means $\dim_K \mathbf{D}_{dR}(V) = \dim_{\mathbb{Q}_p} V$. Then the Bloch-Kato exponential map is an isomorphism and moreover*

$$H^1_e(K_v, V_pE) = H^1_f(K_v, V_pE).$$

There is an interesting conjecture about de Rham representations:

Conjecture 8.16. ***Fontaine-Mazur*** *If a $p-$adic representation V is de Rham at all places dividing p and unramified in all but finitely many primes, then V comes from geometry in the sense of the Definition 6.1.*

So far in [Vol05] there have been described conditions for a p-adic representation to come from abelian variety.

Now we have written this section specifically to compute dimensions of the spaces $H^1_*(K_v, V_l)$ and later we will compute measures of Bloch-Kato Selmer groups. Consider short exact sequences from the chapter about Fontaines rings 7.14 and 7.15. We take each of them, tensor with V_l and take long exact cohomology sequences. From those we may derive dimension formulas as:

Theorem 8.17. *[BK90] For a p-adic representation V_p over a local field K_v with $v \mid p$ the following hold:*

$$\dim H^1_f(K_v, V_p) = \dim(\mathbf{D}_{dR}(V_p)/\mathbf{D}^+_{dR}(V_p)) + \dim H^0(K_v, V_p); \tag{8.4}$$

$$\dim H^1_e(K_v, V_p) = \dim(\mathbf{D}_{dR}(V_p)/\mathbf{D}^+_{dR}(V_p)) - \dim \mathbf{D}_e(V_p) + \dim H^0(K_v, V_p)$$

additionally to the above by using the fact that under the perfect pairing $\cup : H^1(G_{K_v}, V_p) \times H^1(G_{K_v}, V_p^*(1)) \to H^2(G_{K_v}, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$ spaces $H^1_e(K_v, V_p)$ and $H^1_g(K_v, V_p^*(1))$ are orthogonal with respect to each other we can compute dimension of $H^1_g(K_v, V_p)$

$$\dim H^1_g(K_v, V_p) = \dim(\mathbf{D}_{dR}(V_p)/\mathbf{D}^+_{dR}(V_p)) + \dim \mathbf{D}_e(V_p^*(1)) + \dim H^0(K_v, V_p).$$

Where all dimensions are taken as dimensions of $\mathbb{Q}_p$-vector spaces.

We would like to pass to the global Tate module and for that we introduce the ring of adeles. We denote by $\mathbb{A}_\mathbb{Q}$ the ring of finite adeles for $\mathbb{Q}$. By definition

$$\mathbb{A}_\mathbb{Q} := \prod_p{}' \mathbb{Q}_p = \left\{(a_p) \in \prod_p \mathbb{Q}_p : \, a_p \in \mathbb{Z}_p \textit{ for all but finitely many } p\right\}$$

However we will mostly work with the completed ring of adeles is $\mathbb{A}_\mathbb{Q} \oplus \mathbb{R}$ defined in the same way but with possibility of $p = \infty$. We get an inclusion $\mathbb{Q} \hookrightarrow \mathbb{A}_\mathbb{Q}$ from $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for all p.

Lemma 8.18. *One can define the product norm on the ring of adeles for $\mathbb{Q}$ by $|(a_p)| := \prod_p |a_p|_p \in \mathbb{R}_{\geq 0}$. It is well defined since we know that $|a_p|_p \leq 1$ for*

almost all p. Then the topology generated by the adelic norm makes $\mathbb{A}_{\mathbb{Q}}$ *locally compact and Hausdorff.*

Definition 8.19. *For an elliptic curve E over a number field K define a* $\widehat{\mathbb{Z}}$*-module* $T(E) := \prod_l T_l(E)$ *the total Tate module. The total rational Tate module is the adelic product* $V(E) := \prod' V_l$ *with respect to all* T_l*s.*
In order to define local Bloch-Kato Selmer groups for total $V(E)$ *for all* $* = e$*,* f*,* g *we define* $H^1_*(K_v, V(E)) := \prod_l H^1_*(K_v, V_l)$*.*

We have defined all sorts of local Bloch-Kato Selmer groups for case of local field K_v. In case of a number field K definitions analogous to 6.9 will work as well.

Chapter 9

The refined conjecture of Bloch and Kato

The aim of this chapter is to explain how to get from the Bloch-Kato Tamagawa number conjecture to the BSD conjecture in the case of elliptic curves. The main reference for this part is the original article by Bloch and Kato [BK90], there is also a number of excellent surveys on this subject dedicated to the Fontaine and Perrin-Riou conjecture which is known to be equivalent to Bloch-Kato conjecture: [Fla04], [Kin11], [Ven07] and lecture notes useful for understanding the whole picture [Gro16]. In [Kin11] it is proven that the Fontaine-Perrin-Riou conjecture implies BSD. We take a different more direct approach of proving equivalence of BSD and the Tamagawa number conjecture for the motive $\mathcal{M} = h^1(E)(1)$.

From now we assume the base field to be the field of rational numbers $K = \mathbb{Q}$. Bloch and Kato introduced a **motivic pair** (V, D) of finite dimensional $\mathbb{Q}$-vector spaces and formulated their conjecture for certain groups $A(\mathbb{Q}_p)$ defined for a motivic pair. We will check the conditions for the pair for $V = H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i)),\ D = \mathbf{D}_{dR}(V) \simeq H^1_{dR}(E/\mathbb{Q})$ to be motivic. But before that we study these vector spaces locally. Recall the Theorem of Artin, [Art68]

Theorem 9.1. *For an algebraic scheme $X/\mathbb{C}$ denote by X^{an} the space $X(\mathbb{C})$*

with complex-analytic topology. Then for any prime p we have an isomorphism:

$$H^*_{et}(X, \mathbb{Z}_p) \simeq H^*(X^{an}, \mathbb{Z}_p).$$

Then we have $V \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}} \simeq H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i)) \otimes \mathbb{A}_{\mathbb{Q}} \simeq H^1_{et}(E_{\overline{\mathbb{Q}}}, \mathbb{A}_{\mathbb{Q}}) \simeq V(E)$ where $V(E)$ is defined above in 8.19 and adelic cohomology considered in [Del79].

The modules $(V_l E, D_l)$ can be recovered from each other as in the theory of Fontaine and Laffaille about Dieudonne modules, namely for $\mathbf{A}_{inf} := \mathbf{A}_{inf}(\mathbb{Z}_l)$ we define

$$D_l := \mathbf{D}_{dR}(V_l E) \quad and \quad V_l E := \mathbf{V}_{cris}(D_l).$$

In case when we start with a crystalline representation V (defined $\mathbf{B}_{cris}$-admissible) we have the property of $\mathbf{D}_{dR}(V) = \mathbf{D}_{cris}(V)$ immediately by comparison of dimensions 8.1. Therefore when we start with rational Tate module $V_l E$ of an elliptic curve E with good reduction at l and apply first functor $\mathbf{D}_{cris}$ to get a filtered admissible φ-module $\mathbf{D}_{cris}(V)$ to which afterwards we can apply the inverse functor $\mathbf{V}_{cris}$ we get again $V_l E$ by the theorem of Fontaine 8.6.

Proposition 9.2. *For an elliptic curve E over $\mathbb{Q}$ the pair*

$$(V = H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i)),\ D = H^1_{dR}(E/\mathbb{Q}))$$

is motivic in the sense of Bloch and Kato, see definition 5.5 [BK90].

Proof. First we check the structure: the action of $G_{\mathbb{Q}}$ on $V \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}$ is continuous, $\mathbb{A}_{\mathbb{Q}}$-linear, and $V \otimes 1$ is stable under complex conjugation. The space $\mathbf{D}_{dR}(V) = (\mathbf{B}_{dR} \otimes V)^{G_{\mathbb{Q}}}$ carries a decreasing filtration coming from one on $\mathbf{B}_{dR}$ and which stabilizes away from finite set of indexes. We evidently get an isomorphism $D_l \simeq \mathbf{D}_{dR}(V_l E)$ directly, we also define $D_\infty := (V \otimes \mathbb{C})^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}$.

It remains to check all axioms (P1-P4): We take the set $U = \mathrm{Spec}(\mathbb{Z}) \setminus S$ of all primes of good reduction. Then by Neron-Ogg-Shafarevich criterion $V_l(E) = H^1_{et}(E, \mathbb{Q}_l)$ is unramified at $p \in U$. On the other hand it is the Theorem of

Fontaine and Laffaille (Theorem 4.3 in [BK90]) that V_pE is crystalline, i.e. $\dim_{\mathbb{Q}_p} \mathbf{D}_{cris}(V) = \dim_{\mathbb{Q}_p} V$.

For the $\mathbb{Z}$-lattice in second property we take the cohomology with integer coefficients $T := H^1(E(\mathbb{C}), \mathbb{Z}(2\pi i))$ in V, then by analogy with the proof of the Fact 2.12 we get $T \otimes \mathbb{Z}_p \simeq T_pE$. Locally the lattice in D_l comes from T_lE by definition, then the property (P2) on lattices holds. For the finite set of primes S we use all bad reduction primes of E and ∞. Then for $p \notin S$ we get V_pE to be crystalline by above. We also have for the de Rham filtration existence of $i, j \in \mathbb{Z}$ such that $Fil^i D_l = D$, $Fil^j D_l = 0$, and $j - i < p$ again as a part of theorem of Fontaine and Laffaille.

We have seen before in the proof of the Lemma 2.13 that polynomial $P_{\mathbb{Q}_l,p}(V_l(E), t)$ is an element of $\mathbb{Z}[t]$ and therefore it is independent of p which gives the third property. As for the lattice T in fourth property we take the integral Tate module $T(E)$, it is $G_{\mathbb{Q}_p}$-stable and $T(E) \otimes \mathbb{Q}_l/\mathbb{Z}_l = T_lE \otimes \mathbb{Q}_l/\mathbb{Z}_l$. We only need to know that $H^0(\mathbb{Q}_p^{ur}, T_lE \otimes \mathbb{Q}_l/\mathbb{Z}_l)$ is divisible for all unramified l. We know that $\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \simeq \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ from Witt vectors formalism and that action of inertia group I_p is trivial by definition so we are looking at $(T_lE \otimes \mathbb{Q}_l/\mathbb{Z}_l)^{G_{\mathbb{Q}_p}}$ note that T_lE is divisible by all primes as $\mathbb{Z}_l$-module, except from l and $\mathbb{Q}_l/\mathbb{Z}_l$ is divisible by l. □

A motivic pair can be defined for any motive over $\mathbb{Q}$, however we are mostly interested in case of $\mathcal{M} = h^m(X)(r)$ for a smooth proper scheme X over $\mathbb{Q}$. This type of motive would give a motivic pair in the following way: we take $V := H^m(X(\mathbb{C}), \mathbb{Q}((2\pi i)^r))$ and $D := H^m_{dR}(X/\mathbb{Q})$ then by Faltings' comparison theorems structure axioms (P1-P4) hold and we have $D_p \simeq \mathbf{D}_{dR}(V_p)$. For all $p < \infty$ there is a filtration on D_p coming from the filtration on $\mathbf{B}_{dR}$. The zero filtered factor of D_p is denoted by $D_p^0 := F^0 D_p$ and by definition it coincides with $\mathbf{D}^+_{dR}(V_p)$. The filtration on D is just the Hodge filtration, also we get a Galois action on V coming from theorem of Artin $V \otimes \mathbb{A}_{\mathbb{Q}} \simeq H^m_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{A}_{\mathbb{Q}})(r)$. In the next section we define groups $A(\mathbb{Q}_p)$ and $A(\mathbb{R})$ of local points associated

to a motive $\mathcal{M}$ with groups of global points $A(\mathbb{Q})$ to be described afterwards. We will see for the case of 1-motive of elliptic curve that these groups are isomorphic to the usual Mordell-Weil groups of a curve over a field.
Afterwards we will discuss measures defined on these groups. We closely follow exposition of Bloch and Kato [BK90] in discussion here recalling measures for case of good reduction and define them in reasonable way for bad. When all prerequisites are filled we will turn our attention to L-functions for motives.

9.1 Groups of points

Our case of concern is $X = E$ and the associated motive $\mathcal{M} = h^1(E)(1)$. In this case we define the groups $A(\mathbb{Q}_p)$ following [BK90] chapter 5.6.
Recall that for an elliptic curve E over the field of complex numbers $\mathbb{C}$ the Hodge-de Rham filtration is represented by a short exact sequence

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

Note that in our case $D_\infty = H^1_{dR}(E/\mathbb{Q})$, then by definition $D^0_\infty \otimes \mathbb{C} := \mathrm{Fil}^1 D_\infty = \mathrm{Fil}^1 H^1(E, \mathbb{C}) = H^{1,0} = H^0(E, \Omega^1_E)$.

Definition 9.3. *For a $\mathbb{Z}$-lattice T we pick as above $H^1(E(\mathbb{C}), \mathbb{Z}(2\pi i))$, then $T \otimes \widehat{\mathbb{Z}} \simeq T(E)$ is $G_\mathbb{Q}$-stable in $V \otimes \mathbb{A}_\mathbb{Q} \simeq V(E)$. Define local groups*

$$\begin{cases} A(\mathbb{Q}_p) := H^1_f(\mathbb{Q}_p, T(E)), \ \textit{if } p < \infty; \\ A(\mathbb{R}) := (H^1_{dR}(E/\mathbb{C})/(H^0(E, \Omega^1_E) + T))^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} \ \textit{if } p = \infty. \end{cases} \tag{9.1}$$

The rest of this chapter is dedicated to the computation of measures of these groups which is vital for the formulation of the Tamagawa number conjecture.

Remark 9.4. *We will see later why it does not matter which $\mathbb{Z}$-lattice in V we take as long as it is Galois stable, the formulation of conjecture is not going to change.*

As we have mentioned above following the Lemma-Definition 8.14 Bloch and Kato proved the isomorphism $exp_{BK} : D_p/D_p^0 \to H_f^1(\mathbb{Q}_p, V_p)$ so for $p < \infty$ the composition

$$D_p/D_p^0 \xrightarrow{exp} H_f^1(\mathbb{Q}_p, V_p) \to A(\mathbb{Q}_p)$$

is a local isomorphism on a neighborhood of 0 in D_p/D_p^0.

Construction 9.5. *By definition one may view D_p/D_p^0 as a finite dimensional vector space over $\mathbb{Q}_p$ and over $\mathbb{R}$ when $p = \infty$. Then we can consider its determinant as the highest exterior power just like in the chapter on determinants. The space obtained in such a way is one dimensional over $\mathbb{Q}_p$ or over $\mathbb{R}$. So we choose an isomorphism for $p \leq \infty$:*

$$\det_p : D_p/D_p^0 \to \mathbb{Q}_p.$$

Using this isomorphism Bloch and Kato define Haar measure on the space D_p/D_p^0. Afterwards the measure can be extended to $A(\mathbb{Q}_p)$ via the exponential map, we call the measure μ_p.
For the case of $p = \infty$ the measure μ_∞ on $A(\mathbb{R})$ comes from $\mathbb{C}$. We have $D_\infty/D_\infty^0 = H^{0,1} = H^1(E, \mathcal{O}_E)$ and the exponent map is the canonical one $H^1(E, \mathcal{O}_E) \simeq \mathrm{Lie}(E) \to \mathbb{C}$.

We would like to describe a way of defining this Haar measure μ_p on an example. We start with the usual p-adic Haar measure on $\mathbb{Q}_p$, then we have $\mu_p = |\cdot|_p$, so $\mu_p(\mathbb{Z}_p) = 1$ and $\mu_p(p\mathbb{Z}_p) = p^{-1}$. It grows to a measure μ_p^d on the affine space $\mathbb{Q}_p^d$, where the resulting measure respects change of variable and one the Implicit Function Theorem holds for this case.

Example 9.6. *Let X be a smooth scheme over $\mathbb{Q}_p$ of dimension d. Consider the top degree module of differential forms $\Omega^d_{X/\mathbb{Q}_p}$, it is a one-dimensional vector space over $\mathbb{Q}_p$, so we pick a generator $\omega \in \Omega^d_{X/\mathbb{Q}_p}$. This allows us to define a measure $|\omega|\mu_p^d$ on $X(\mathbb{Q}_p)$.*
Now we want to define a canonical measure for $X = E$. For that we look at

the Neron model $\mathcal{E}$ and a $\mathbb{Z}_p$-module $\Omega^d_{\mathcal{E}/\mathbb{Z}_p}$ of rank 1. We then choose such an element $\omega \in \Omega^d_{E/\mathbb{Q}_p}$ that is a generator of $\Omega^d_{\mathcal{E}/\mathbb{Z}_p}$, this choice is up to $\mathbb{Q}_p^\times$, but when we multiply $|\omega|$ by an element λ of $\mathbb{Q}_p^\times$ the measure itself scales by $|\lambda|_p$. Note that the same can be done for a finite extension $K_v/\mathbb{Q}_p$.

Remark 9.7. *One can repeat the construction in the example above where instead of $\Omega_{X/\mathbb{Q}_p}$ we take the module of Kahler differentials $\Omega_{(D_p/D_p^0)/\mathbb{Q}_p}$ to define measure on D_p/D_p^0. Then by the commutative diagram in lemma 8.14 we have that measures on $E(K_v)$ and $D_p/D_p^0 = \mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE)$ agree.*

For the formulation of the Tamagawa number conjecture we need to compute values of measure $\mu_l(A(\mathbb{Q}_p))$ for all possible cases of l and p including ∞. We will do that in a few steps.

Bloch and Kato discuss the case of abelian variety with good reduction over p to define μ_p, however all bad reduction cases remain unsolved. We will recall results on good reduction for completeness and compute measure in bad reduction.

9.1.1 Measures in the case $l \neq p$

Instead of cohomology groups $H^1_*(\mathbb{Q}_p, V)$ for $* \in \{e, f, g\}$ Bloch and Kato consider cohomology with coefficients in $G_{\mathbb{Q}_p}$-stable $\mathbb{Z}_l$-sublattice T in V and in case when $l \neq p$ they state the following (Theorem 4.1 in [BK90])

Lemma 9.8. *Let V_l be an $l-$adic representation unramified at $p \neq l$ and $T_l \subset V_l$ be a $G_{\mathbb{Q}_p}$-stable sublattice.*

Then the number of elements in $H^1_f(\mathbb{Q}_p, T_l)$ equals the value of $|P_{\mathbb{Q}_p}(V_l, 1)|_l^{-1}$, where $P_{\mathbb{Q}_p}(V_l, 1) = P_{\mathbb{Q}_l,p}(V_l, 1)$ is defined in 2.1. Therefore we have

$$|H^1_f(\mathbb{Q}_p, T_l)| = \mu_l(A(\mathbb{Q}_p)) = |P_{\mathbb{Q}_p}(V_l, 1)|_l^{-1}.$$

Corollary 9.9. *The lemma above holds for ramified representation if instead of T_l we consider invariants of inertia $T_l^{I_p}$ and we will prove the statement*

in this setting. For the case of elliptic curve E we allow bad reduction at p and the lemma implies that $\mu_l(H^1_f(\mathbb{Q}_p, T_l)) = |c_p|_l^{-1}|P(V_l, 1)|_l^{-1}$ where c_p is the number of connected components in the Neron model of E over $\mathbb{Q}_p$ viewed as an l-adic number.

Before proving Lemma 9.8 we consider a couple of helpful statements that must be proven before we start counting elements in a group $H^1_f(\mathbb{Q}_p, T_l)$. We just want to know it is finite.

Lemma 9.10. *For $V = V_lE$ and K_v a finite extension of $\mathbb{Q}_p$ we have the following:*

- $\dim H^0(K_v, V_lE) = 0$*;*
- $$\dim H^1(K_v, V_lE) = \begin{cases} 0, & \text{if } l \neq p \\ 2[K_v : \mathbb{Q}_p], & l = p. \end{cases}$$
- *for $l \neq p$ we have* $\dim H^1_f(K_v, V_lE) = \dim H^0(K_v, V_lE) = 0$*;*

Note that we do not put any requirements on the action of inertia on V_lE, i.e. V_lE is allowed to be ramified at p.

Proof. The first assertion is easy, since $E(K_v)$ has finite torsion bit. Namely because by Proposition VII.6.3 in [Sil09] $E(K_v)$ contains a subgroup of finite index isomorphic to $\mathcal{O}^+_{K_v}$ which is free over $\mathbb{Z}^+_p$.
The second follows from the first by duality on cohomology groups

$$H^i(K_v, V_l) \times H^{2-i}(K_v, V_l^*(1)) \to H^2(K_v, \mathbb{Q}_l(1)) \simeq \mathbb{Q}_l.$$

Then we get $\dim H^2(K_v, V_l^*(1)) = \dim H^0(K_v, V_l) = 0$ by above, where for an elliptic curve $V_lE^*(1) = V_lE$. Then the formula follows from Euler characteristic for group cohomology (a corollary of Lefschetz trace formula for identity

map).

$$\dim H^0(K_v, V_l) - \dim H^1(K_v, V_l) + \dim H^2(K_v, V_l) = \begin{cases} 0, & \text{if } l \neq p \\ -[K_v : \mathbb{Q}_p] \dim V_l E, & l = p. \end{cases}$$

Recall the Definition 6.2 of unramified cohomology for the case $l \neq p$

$$H^1_f(K_v, V_l E) = H^1_{ur}(K_v, V_l E) := \ker(H^1(K_v, V_l E) \to H^1(I_v, V_l E)).$$

By inflation-restriction sequence we can write

$$H^1_{ur}(K_v, V_l E) = H^1(G_{K_v}/I_v, V_l^{I_v}).$$

On the other hand we have $G_{K_v}/I_v \simeq \widehat{\mathbb{Z}}$ a group with cohomological dimension 1 and a property of $\dim H^0(\widehat{\mathbb{Z}}, V) = \dim H^1(\widehat{\mathbb{Z}}, V)$ for any p-adic representation V, see [Ser79]. Then

$$\dim H^1(G_{K_v}/I_v, V_l^{I_v}) = \dim H^0(G_{K_v}/I_v, V_l^{I_v})$$

which is in turn $\dim H^0(G_{K_v}, V_l) = 0$ by the first property. □

Note a similarity of the second point with the Greenberg's theorem 1.5.

Proof. of the Lemma 9.8 By previous lemma we see that $\dim H^0(\langle \mathrm{Fr} \rangle, V_l^{I_v}) = 0 = \dim H^1(\langle \mathrm{Fr} \rangle, V_l^{I_v})$ so we may try to compute a number of elements in the torsion subgroup of $H^1(\langle \mathrm{Fr} \rangle, T_l^{I_v})$ for a lattice $T_l \subset V_l$. By definition $P(V_l, 1) = \det(1 - \mathrm{Fr}\,|V_l^{I_v})$ then by the Lemma 2.7

$$|\det(1 - \mathrm{Fr}\,|V_l^{I_v})|_l^{-1} \mathbb{Z}_l = \det \operatorname{coker}(T_l^{I_v} \xrightarrow{1-\mathrm{Fr}} T_l^{I_v}) = H^1(\langle \mathrm{Fr} \rangle, T_l^{I_v}).$$

Here by $\langle a \rangle$ we denote a cyclic group, generated by a. On the other hand by

definition of unramified cohomology we have as above

$$H^1_f(K_v, T_l^{I_v}) = H^1_{ur}(K_v, T_l^{I_v}) = \ker(H^1(G_{K_v}, T_l^{I_v}) \to H^1(I_v, T_l^{I_v}))$$

while inflation-restriction sequence implies

$$H^1(G_{K_v}/I_v, T_l^{I_v}) = \ker(H^1(G_{K_v}, T_l^{I_v}) \to H^1(I_v, T_l^{I_v})^{G_{K_v}/I_v}).$$

It is crucial at this point that the inertia group acts trivially on T_l in case of good reduction, otherwise we take $T_l^{I_v}$ for a ramified representation, which means $H^1(I_v, T_l^{I_v}) = 0$ which implies

$$H^1_f(K_v, T_l^{I_v}) \simeq H^1(G_{K_v}/I_v, T_l^{I_v}) \simeq H^1(\langle \mathrm{Fr} \rangle, T_l^{I_v}).$$

We have used here isomorphisms $\mathrm{Gal}(\overline{K}/K_{ur}) \simeq G_{K_v}/I_v \simeq \widehat{\mathbb{Z}} = \langle \mathrm{Fr} \rangle$ where the last one is topologically generated by the Frobenius map.
Then by results from section about determinants Lemma 2.7 and Example 2.6 we obtain the size of the torsion subgroup in $H^1(\langle \mathrm{Fr} \rangle, T_l^{I_v})$ as:

$$|H^1(\langle \mathrm{Fr} \rangle, T_l^{I_v})_{tor}| = |\det(1 - \mathrm{Fr}\,|V_l^{I_v})|_l^{-1}.$$

In case of $K_v = \mathbb{Q}_p$ we get precisely $|H^1_f(\mathbb{Q}_p, T_l)| = |P(V_l, 1)|_l^{-1}$. □

Proof. of the Corollary 9.9 The proof of lemma above written for $V_l = V_l E$ holds until the ramified representation comes into picture. From now assume that E has bad reduction at p and we want to compute $\mu_l(H^1_f(\mathbb{Q}_p, T_l))$. Then there is a piece of inflation-restriction sequence that looks like

$$0 \to H^1(G_{\mathbb{Q}_p}/I_p, T_l^{I_p}) \to H^1(\mathbb{Q}_p, T_l) \to H^1(I_p, T_l)^{G_{\mathbb{Q}_p}/I_p} \to 0.$$

Now we would like to know a bit more about $H^1(I_p, T_l)$ and especially a part

of it $H^1(I_p, T_l)^{G_{\mathbb{Q}_p}/I_p}$. Lets have a look at the short exact sequence

$$0 \to T_l \to V_l \to V_l/T_l \to 0$$

and the corresponding long exact cohomology sequence of the inertia I_p with coefficients in this sequence. Then

$$H^1(I_p, T_l) \simeq \operatorname{coker}(V_l^{I_p} \to (V_l/T_l)^{I_p}); \tag{9.2}$$

since $H^1(I_p, V_l) = 0$ and $H^1(G_{\mathbb{Q}_p}/I_p, V_l^{I_p}) = H^1_f(G_{\mathbb{Q}_p}, V_l) = 0$ we obtain from the long exact sequence of cohomology groups of $G_{\mathbb{Q}_p}/I_p \simeq \operatorname{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p)$ that $H^1(I_p, T_l^{G_{\mathbb{Q}_p}/I_p}) = 0$. When we are working with finite abelian groups

$$0 \to H \hookrightarrow G \to G/H \to 0$$

we get for the number of elements: $|G| = |H| \cdot |G/H|$. Applying this to our short exact sequences together with the definition of H^1_f and the short exact sequence for $H^1(G_{\mathbb{Q}_p}/I_p, T_l^{I_p})$ above we see that

$$\frac{|H^1_f(\mathbb{Q}_p, T_l)|}{|H^1(G_{\mathbb{Q}_p}/I_p, T_l^{I_p})|} = \frac{|H^1(I_p, T_l^{G_{\mathbb{Q}_p}/I_p})|}{|H^1(I_p, T_l)|}. \tag{9.3}$$

By previous lemma we have $\mu(H^1(G_{\mathbb{Q}_p}/I_p, T_l^{I_p})) = |\det(1 - \operatorname{Fr}|V_l^{I_v})|_l^{-1}$.
We will prove that $\operatorname{coker}(V_l^{I_p} \xrightarrow{f} (V_l/T_l)^{I_p}) \simeq \Phi(\mathbb{F}_p)$ the group of connected components in the Neron model of E over $\mathbb{Z}_p$ and it will solve the problem. To see that the map f is not surjective consider an element from I_p looking like $\begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix}$ we have seen before in the proof of the Lemma 2.13 that the inertia group consists of elements of this sort. Then this matrix fixes elements in $V_l^{I_p}$ killed by l, but since V_l is a free $\mathbb{Q}_l$-module, then there is only 0 among such elements. On the other hand in $(V_l/T_l)^{I_p}$ there is whole $E[l](\mathbb{Q}_p^{nr})$ fixed by the matrix above.

Now by the Fact 6.4 we have $V_l^{I_p} \simeq V_l(\mathcal{E}^0) = V_l(\mathcal{E}(\mathcal{O}_{\mathbb{Q}_p^{nr}}))$ so we are dealing with connected components in the Neron model here. If we take an element from $V_l(\mathcal{E}^0)$ and apply f to it, then this point will go to some connected component, all of which are isomorphic to $V_l/T_l(\mathcal{E}^0)$, thus cokernel of map f is exactly the group of connected components.

By definition the Tamagawa number $c_p = |\Phi(\mathbb{F}_p)|$, so by formula 9.3 above the reasoning implies that $|H^1_f(\mathbb{Q}_p, T_l)| = |H^1(I_p, T_l)|^{-1}|H^1(G_{\mathbb{Q}_p}/I_p, T_l^{I_p})|$ so the l-adic measure is $\mu_l(H^1_f(\mathbb{Q}_p, T_l)) = |c_p|_l^{-1}|\det(1 - \mathrm{Fr}\,|V_l^{I_v})|_l^{-1}$. □

9.1.2 Measures in the case $l = p$

The case of $l = p$ is more subtle. When we work in the situation of crystalline representation V_p there is a way due to Fontaine and Laffaille to construct a Galois stable sublattice T_p of V_p and introduce a Haar measure on $H^1_f(\mathbb{Q}_p, T_p)$ coming from filtration and measure on $\mathbf{D}_{dR}(V_p)$. Then Bloch and Kato prove in theorem 4.1 of [BK90] the following

Theorem 9.11. *Assume $p = l$, let V be a finite dimensional representation of $G_{\mathbb{Q}_p}$ and assume V is a de Rham representation, then*

- *There is an isomorphism of groups $H^1_e(\mathbb{Q}_p, V) \simeq H^1_f(\mathbb{Q}_p, V)$.*
- *The exponential map $exp_{BK} : \mathbf{D}_{dR}(V)/Fil^0\mathbf{D}_{dR}(V) \to H^1_e(\mathbb{Q}_p, V)$ is an isomorphism. We define a Haar measure on $H^1_f(\mathbb{Q}_p, V)$ coming from Haar measure on $\mathbf{D}_{dR}(V)/Fil^0\mathbf{D}_{dR}(V)$ via an isomorphism (1).*
- *If V is crystalline and $\mathbf{D}_{dR}(V)$ is a Dieudonne module, we can take a strongly divisible lattice $D \in \mathbf{D}_{dR}(V)$ and a Galois stable lattice $T = T_{cris}(D) \subset V$. Then $\mu_p(H^1_f(\mathbb{Q}_p, T)) = |P(V, 1)|_p^{-1}$ for a normalized valuation defined by p.*

For our case this means by definition of $A(\mathbb{Q}_p)$ that $\mu_p(A(\mathbb{Q}_p)) = P_p(V_p, 1)$ in the case of good reduction prime. The -1 degree is gone since the valuation is

normalized as $|p|_p = p^{-1}$ and the value of $P_p(V,1)$ is the power of p and thus its p-adic norm $|P_p(V,1)|_p$ is nothing but itself inverted.

The next task is to define measure μ_p on $A(\mathbb{Q}_p)$ for primes $l = p$ at which our elliptic curve E has bad reduction which means that representation V_pE is not crystalline. The rest of the chapter is dedicated to the proof of the following lemma and its highly important consequence. Assume we are in the situation with a semi-stable p-adic representation V.

Lemma 9.12. *Let V be a semi-stable p-adic representation. For a finitely generated $\mathbb{Z}_p$-submodule D in the Dieudonne module $\mathbf{D}_{st}(V)$ which inherits a filtration from $\mathbf{D}_{dR}(V)$ with a property of $D = \sum p^{-i} \operatorname{Fr}(Fil^i D)$ the following is true: consider a Galois stable lattice $T \subset V$ defined as $T := T_{st}(D)$. Then*

$$\mu_p(H^1_f(\mathbb{Q}_p, T)) = |P(V,1)|_p^{-1} = |\det(1 - \operatorname{Fr} |\mathbf{D}_{st}(V)^{N=0})|_p^{-1}.$$

Note that the same statement holds as well in the case of crystalline representation V_p, since in that case $\mathbf{D}_{st}(V) = \mathbf{D}_{cris}(V)$ and we come to the statement of the Lemma 4.1 (iii) in [BK90].

Remark 9.13. *We should explain why we changed the common notation in the lemma. The reason is we have $\mathbf{D}_{st}(V)^{N=0} = \mathbf{D}_{cris}(V)$ whenever V is a finite-dimensional vector space over $\mathbb{Q}_p$. Namely we take the short exact sequence:*

$$0 \to \mathbf{B}_{cris} \to \mathbf{B}_{st} \xrightarrow{N} \mathbf{B}_{st} \to 0$$

and tensor it with V. Since V is a free $\mathbb{Q}_p$-module it is flat as $\mathbb{Q}_p$-algebra so tensoring with V is left-exact. After that we take cohomology of $\operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ with coefficients in the obtained short exact sequence to find out that

$$0 \to \mathbf{D}_{cris}(V) \to \mathbf{D}_{st}(V) \xrightarrow{N} \mathbf{D}_{st}(V) \to ...$$

Therefore $\mathbf{D}_{cris}(V)$ is the kernel of the monodromy operator acting on $\mathbf{D}_{st}(V)$.

Corollary 9.14. *Let E be an elliptic curve over $\mathbb{Q}_p$ with semi-stable reduction at p. Then the Lemma 9.12 implies that the measure of finite cohomology with coefficients in the integral Tate module T_pE equals $\mu(H^1_f(\mathbb{Q}_p, T_pE)) = |c_p|_p^{-1}|P(V_pE,1)|_p^{-1}$ and in case of good reduction the measure is $\mu(H^1_f(\mathbb{Q}_p, T_pE)) = |P(V_pE,1)|_p^{-1}$. Where c_p is the number of elements in the group of connected components of the special fiber of the Neron model of E.*

We immediately notice the similarity with the Corollary 9.9, indeed this is just the $l = p$ version of the above.

Note that for the case of $V_p = V_pE$ with E of good reduction at p the special fiber of the Neron model is a connected group, so $c_p = 1$ so the statement of the second assertion of the Corollary 9.14 is just partial case of the first.

The following useful statement is completely analogous to the Lemma 4.3 in [BK90], but for modules with monodromy action.

Lemma 9.15. *The category of filtered Dieudonne modules with connection $\mathcal{MF}\varphi_K, N$ over $\mathbb{Z}_p$ has the initial object $\mathcal{O}$ with filtration defined by*

$$Fil^i\mathcal{O} = \begin{cases} \mathbb{Z}_p, & \text{if } i \leq 0; \\ 0 \text{ otherwise.} \end{cases}$$

Frobenius operator on filtered pieces is given by $\mathrm{Fr}_i(Fil^i\mathcal{O}) \subset p^{-i}\,\mathrm{Fr}_p$, where Fr_p is the Witt vector Frobenius acting on $\mathbb{Z}_p$, and the action of the monodromy operator is trivial $N(x) = 0$ for $x \in Fil^i\mathcal{O}$.

For an object $D_p \in \mathcal{MF}\varphi_K, N$ consider the short exact sequence

$$0 \to h^0(D_p) \to D_p^0 \xrightarrow{1-\mathrm{Fr}} D_p \to h^1(D_p) \to 0$$

Define the objects $h^0(D_p)$ and $h^1(D_p)$ as corresponding kernel and cokernel in the sequence. Then $h^i(D_p) = \mathrm{Ext}^i_{\mathbb{Z}_p}(\mathcal{O}, D_p)$.

To prove Lemma 9.12 we need another useful statement analogous to the Lemma 4.5 in [BK90].

Lemma 9.16. *Assume that a filtered Dieudonne module D_p with connection has bounded by p filtration, i.e. there are integers $i \leq 0$, $j \geq 1$ such that $j - i < p$ and $D_p^i = D_p$ with $D_p^j = 0$. Denote by $T = T_{st}(D_p)$ with $V = T \otimes \mathbb{Q}$. Recall that for usual* Ext *we have* $\mathrm{Ext}^i_{\mathbb{Z}_p[G_{\mathbb{Q}_p}]}(\mathbb{Z}_p, T) = H^i(\mathbb{Q}_p, T)$.
Denote by $\theta_i : h^i = \mathrm{Ext}^i_{\mathbb{Z}_p}(\mathbb{Z}_p, D_p) \to \mathrm{Ext}^i_{\mathbb{Z}_p[G_{\mathbb{Q}_p}]}(\mathbb{Z}_p, T_{st}(D_p))$ for h^i defined in the previous lemma. Then

- *θ_0 is an isomorphism, and θ_1 is an injection.*

- *There is a commutative diagram with exact rows:*

$$\begin{array}{ccccccc} h^0(D_p)\otimes\mathbb{Q} & \longrightarrow & D_p^0\otimes\mathbb{Q} & \xrightarrow{1-\mathrm{Fr}} & D_p\otimes\mathbb{Q} & \longrightarrow & h^1(D_p)\otimes\mathbb{Q} \\ \downarrow{\scriptstyle\theta_0} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\theta_1} \\ H^0(\mathbb{Q}_p,V) & \longrightarrow & \mathbf{D}_{st}(V)\oplus\mathbf{D}^+_{dR}(V) & \longrightarrow & \mathbf{D}_{st}(V)\oplus\mathbf{D}_{dR}(V) & \longrightarrow & H^1(\mathbb{Q}_p,V) \end{array} \tag{9.4}$$

where the middle vertical arrows send $x \mapsto (x, x)$ and $x \mapsto (x, 0)$.
Since V is semi-stable we get $D_p \otimes \mathbb{Q} \simeq \mathbf{D}_{st}(V) \simeq \mathbf{D}_{dR}(V)$. Then it follows from diagram that $h^1(D_p) \otimes \mathbb{Q} \simeq H^1_{est}(\mathbb{Q}_p, V)$ and we get the following explicit description of the exponential map:

$$\begin{array}{ccc} D_p/D_p^0\otimes\mathbb{Q} & \xrightarrow{exp} & H^1(\mathbb{Q}_p,V) \\ \downarrow{\scriptstyle 1-\mathrm{Fr}} & & {\scriptstyle\theta_1}\uparrow \\ D_p/(1-\mathrm{Fr}_0)D_p^0\otimes\mathbb{Q} & = & h^1(D_p)\otimes\mathbb{Q} \end{array}$$

On the integral side the following is true: If D_p is torsion-free then there is an injection $h^1(D_p) \overset{\theta_1}{\hookrightarrow} H^1(\mathbb{Q}_p, T)$ which induces an isomorphism

$$h^1(D_p) \simeq H^1_{st}(\mathbb{Q}_p, T) := \ker(H^1(\mathbb{Q}_p, T) \to H^1(\mathbb{Q}_p, V)/H^1_{st}(\mathbb{Q}_p, V));$$

so we can drop tensoring with $\mathbb{Q}$ from the diagram above

$$\begin{array}{ccc} D_p/D_p^0 & \xrightarrow{exp} & H^1(\mathbb{Q}_p, T) \\ \downarrow{\scriptstyle 1-\mathrm{Fr}} & & \uparrow{\scriptstyle \theta_1} \\ D_p/(1-\mathrm{Fr}_0)D_p^0 & = & h^1(D_p) \end{array}$$

Proof. The injectivity of θ_1 and the assertion about θ_0 being an isomorphism follows from fully-faithfulness of the functor T_{st} by the Theorem 8.12. Namely by the definition of T_{st} we have for the initial Dieudonne module with connection $T_{st}(\mathcal{O}) = \mathbb{Z}_p$. Since group cohomology compute right derived to the functor Hom, then θ_0 is immediately an isomorphism and injectivity of θ_1 is the question about injectivity of $\mathrm{Ext}^i_{\mathbb{Z}_p}(\mathbb{Z}_p, T) \hookrightarrow H^1(\mathbb{Q}_p, V)$.
The exactness of the lower row of the diagram comes from tensoring the exact sequence in the Lemma 7.16 with V to get

$$0 \to V \xrightarrow{a} (\mathbf{B}_{st} \oplus \mathbf{B}^+_{dR}) \otimes V \xrightarrow{b} (\mathbf{B}_{st} \oplus \mathbf{B}_{dR}) \otimes V \to 0.$$

Where $b(x, y) := ((1 - \mathrm{Fr})x, x - y)$. Afterwards we take the long exact cohomology sequence of the absolute Galois group of $\mathbb{Q}_p$ with coefficients in this sequence to obtain precisely

$$0 \to H^0(\mathbb{Q}_p, V) \to \mathbf{D}_{st}(V) \oplus \mathbf{D}^+_{dR}(V) \to \mathbf{D}_{st}(V) \oplus \mathbf{D}_{dR}(V) \to H^1(\mathbb{Q}_p, V) \to 0$$

The exactness of the upper row follows from the Lemma 9.15. In order to prove the commutativity it helps to look at filtered pieces.
Define the Tate twist of a Dieudonne module with connection D in the following way: the ith filtration piece is $D^i_{(r)} := D^{i+r}$ with Frobenius acting as $\mathrm{Fr}_i\,|D_{(r)} := \mathrm{Fr}_{i+r}\,|D$ and monodromy acting via $N|D^i_{(r)} := N|D^{i+r}$ which means that $N : D_{(r)} \to D_{(r+1)}$. Note that this definition agrees with $N\,\mathrm{Fr} = p\,\mathrm{Fr}\,N$. Then if we define for $M(r) := M \otimes \mathbb{Q}_p(r)$ following theorem

8.12

$$T_{st}(D) \ = T_{st}(D_{(r)})(-r)$$

the result will be independent on r. Then for r such that $D^1_{(r)} = 0$ and $D^{2-p}_{(r)} = D_{(r)}$ we have a commutative diagram with middle vertical arrows sending $x \mapsto (x, x)$, and $x \mapsto (x, 0)$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & Fil^0(\mathbf{B}^+_{st} \otimes D_{(r)})(-r) & \xrightarrow{(1-\mathrm{Fr})} & (\mathbf{B}^+_{st} \otimes D_{(r)})(-r) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V & \longrightarrow & (\mathbf{B}_{st} \otimes V) \oplus (\mathbf{B}^+_{dR} \otimes V) & \longrightarrow & (\mathbf{B}_{st} \otimes V) \oplus (\mathbf{B}_{dR} \otimes V) & \longrightarrow & 0 \end{array} \tag{9.5}$$

Where $1-\mathrm{Fr}$ in the upper row is surjective by Lemma 7.16. The commutativity follows from the Lemma 3.8.1 in [BK90] which means that the map $\mathbf{B}^+_{dR} \otimes V \to \mathbf{B}_{dR} \otimes V$ is surjective.

By applying long exact cohomology sequence for $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ with coefficients in the Diagram above 9.5 we get the statement of lemma, not yet involving integrality as one has to be careful with it.

It follows from the exactness of the Diagram 9.4 that

$$H^1_{st}(\mathbb{Q}_p, V) \simeq \mathrm{coker}(\mathbf{D}_{dR}(V) \xrightarrow{1-\mathrm{Fr}} \mathbf{D}_{dR}(V))$$

with $D_p = \mathbf{D}_{dR}(V)$. Thus in the case of semi-stable representation V we are working with $\mathrm{coker}(\mathbf{D}_{st}(V) \xrightarrow{1-\mathrm{Fr}} \mathbf{D}_{st}(V))$

We come to the integral part. For $* \in \{e, f, g, st, est\}$ the group $H^1_*(K, T)$ is defined so there is a natural arrow $H^1_*(K, T) \to H^1_*(K, V)$ fitting into the commutative diagram:

$$\begin{array}{ccc} H^1_*(K,T) & \longrightarrow & H^1_*(K,V) \\ \downarrow & & \downarrow \\ H^1(K,T) & \longrightarrow & H^1(K,V) \\ & \searrow & \downarrow \\ & & H^1(K,V)/H^1_*(K,V) \end{array}$$

We know already that $h^1(D_p) \otimes \mathbb{Q} \widetilde{\to} H^1_e(\mathbb{Q}_p, V) \hookrightarrow H^1(\mathbb{Q}_p, V)$, then the injection $h^1(D_p) \hookrightarrow H^1(\mathbb{Q}_p, T)$ factors through $h^1(D_p) \to H^1_e(\mathbb{Q}_p, T)$. As the cokernel of the map $H^1_e(\mathbb{Q}_p, T) \hookrightarrow H^1(\mathbb{Q}_p, T)$ is a finite free $\mathbb{Z}_p$-module in order to understand the claim, it is enough to prove that the map $h^1(D_p) \hookrightarrow H^1(\mathbb{Q}_p, T)$ has torsion-free cokernel. As it can only have p-torsion it is enough to prove that in diagram of two exact columns cokernels are isomorphic

$$\begin{array}{ccc} h^1(D_p) & \xrightarrow{\ p\ } & h^1(D_p) \\ \downarrow & & \downarrow \\ H^1(\mathbb{Q}_p, T) & \longrightarrow & H^1(\mathbb{Q}_p, T) \\ \downarrow & & \downarrow \\ Cokernel1 & = & Cokernel2 \end{array}$$

But this follows from $h^i(D_p/pD_p) \to H^i(\mathbb{Q}_p, T/pT)$ having zero cokernels for $i = 0, 1$. □

Remark 9.17. *Note that by definition of T_{st} and the Dieudonne-Tate twist the following diagram is also commutative:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & Fil^0(\mathbf{B}^+_{st} \otimes D_{(r)})^{N=0}(-r) & \xrightarrow{(1-\mathrm{Fr})} & (\mathbf{B}^+_{st} \otimes D_{(r)})^{N=0}(-r) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V & \longrightarrow & (\mathbf{B}_{st} \otimes V)^{N=0} \oplus (\mathbf{B}^+_{dR} \otimes V) & \longrightarrow & (\mathbf{B}_{st} \otimes V)^{N=0} \oplus (\mathbf{B}_{dR} \otimes V) & \longrightarrow & ... \end{array}$$

Where in place of ... we have the continuation of the long exact cohomology sequence for N.

$$\to H^1(\langle N \rangle, V) \to H^1(\langle N \rangle, \mathbf{D}_{st}(V)) \to ...$$

It follows from lemma that we also have the isomorphism between $h^1(D_p)$ and a part of $H^1_{est}(\mathbb{Q}_p, V)$ fixed by monodromy which can be defined as $\ker(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, (\mathbf{B}_{est} \otimes V)^{N=0}))$. By definition of $\mathbf{B}_e$ and $\mathbf{B}_{est}$ we get $(\mathbf{B}_{est} \otimes V)^{N=0} \simeq (\mathbf{B}_e \otimes V)$ so the monodromy fixed part of $H^1_{est}(\mathbb{Q}_p, V)$ is just the exponential cohomology group $H^1_e(\mathbb{Q}_p, V)$ which is isomorphic to $H^1_f(\mathbb{Q}_p, V)$ by the Theorem 9.11.

In the case of crystalline representation the action of monodromy on $\mathbf{D}_{st}(V) = \mathbf{D}_{cris}(V)$ *is trivial, so all the first cohomology groups* $H^1(\langle N\rangle, \mathbf{D}_{st}(V))$ *are trivial.*

Proof. of Lemma 9.12 By properties of the determinant in order to prove the lemma we should represent $H^1_f(\mathbb{Q}_p, T)$ as a cokernel of $1 - \mathrm{Fr}$ acting on $\mathbf{D}_{st}(V)^{N=0}$.

We have seen already that whenever a p-adic representation is semi-stable, it is de Rham, so by Theorem 9.11 we need to do the same for $H^1_e(\mathbb{Q}_p, T) \simeq H^1_f(\mathbb{Q}_p, T)$.

Then lemma follows from a general statement of the Lemma 9.16 as shown in the Remark 9.17. The integral part of Lemma states that $\mu(H^1_f(\mathbb{Q}_p, T)) = \mu(h^1(D_p))$ while by Lemma 9.15 and by definition of determinant we have the measure $\mu(H^1_{st}(\mathbb{Q}_p, T)) = |\det(1 - \mathrm{Fr})|\mathbf{D}_{st}(V)|_p^{-1}$. On top of that we get by the Remark above the following measurement

$$\mu(h^1(\mathbf{D}_{st}(V)^{N=0})) = |h^1(\mathbf{D}_{st}(V)^{N=0})_{tors}| = |\det(1 - \mathrm{Fr})|\mathbf{D}_{st}(V)^{N=0}|.$$

Moreover in the case of a crystalline representation we have found out that $\mu(H^1_f(\mathbb{Q}_p, T)) = |\det(1 - \mathrm{Fr})|\mathbf{D}_{cris}(V)|_p^{-1}$ which is precisely part of the statement of the Lemma 4.1 in [BK90].

Again since we work with $\mathbb{Z}_p$-module the number of elements in the torsion part of a module equals to inverse of its $p-$adic norm. □

Proof. of the Corollary 9.14 We start with computation of $\dim H^1_f(\mathbb{Q}_p, V_pE)$. We have seen already in the Lemma 9.10 that $\dim H^1(\mathbb{Q}_p, V_pE) = 2$ and by the Theorem 8.17 and by the Lemma 9.10 we see that

$$\dim H^1_f(\mathbb{Q}_p, V_pE) = \dim(\mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE)) = 1.$$

Then $H^1_f(\mathbb{Q}_p, T_pE)$ is a $\mathbb{Z}_p$-module of rank 1 and we are interested in the size of its torsion bit.

First we deal with the case of good reduction for its simplicity since it follows from the Lemma 9.12. Recall that in our case the representation $V = V_pE$ is crystalline, so $\mathbf{D}_{cris}(V_pE) = \mathbf{D}_{st}(V_pE) = \mathbf{D}_{dR}(V_pE)$ then the statement of Lemma 9.12 is just the Lemma 4.5 in [BK90].

We substitute $D_p = \mathbf{D}_{st}(V_pE) \simeq \mathbf{D}_{cris}(V_pE)$ into the statement of the integral part of the Lemma 9.16 then we get $T = T_{st}(V_pE) = T_pE$ which then implies $h^1(\mathbf{D}_{st}(V_pE)) \simeq H^1_f(\mathbb{Q}_p, T_pE)$ and the exponential map is the composition

$$exp_{BK} = \theta_1 \circ (1 - \mathrm{Fr}) : \mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE) \to H^1_f(\mathbb{Q}_p, T_pE).$$

On the other hand the Lemma 9.15 allows to compute the measure of $h^1(\mathbf{D}_{dR}(V_pE))$ as determinant of $1-\mathrm{Fr}$. Which gives the desired measure of Bloch-Kato Selmer group $\mu(H^1_f(\mathbb{Q}_p, T_pE)) = |P(V_p, 1)|_p^{-1}$.

Also we know that in case of good reduction of E at p the Neron model $\mathcal{E}$ consists from only one component so $c_p = 1$ and the good reduction case is only a special case of a more general bad reduction statement.

In the case of bad reduction everything is far more tricky. Naturally proving the statement we want to proceed in a way similar to the proof of Corollary 9.9. The proof of Lemma 9.12 together with discussion on the good reduction (crystalline) case almost work well.

The item changing everything in this case is the sequence continuing the lower row of the Diagram 9.5 after taking monodromy invariants as in the Remark 9.17 since it is no longer trivial. So we want to see what is the group $H^1(\langle N \rangle, \mathbf{D}_{st}(V))$.

Consider the short exact sequence

$$0 \to T_pE \to V_pE \to V_pE/T_pE \to 0.$$

As $\mathbf{B}_{st}$ is a free $\mathbb{Z}_p$-module it is flat and tensoring with it is left-exact, so we

get

$$0 \to T_pE \otimes \mathbf{B}_{st} \to V_pE \otimes \mathbf{B}_{st} \to V_pE/T_pE \otimes \mathbf{B}_{st} \to 0.$$

Now we take long exact sequence of cohomology of the group $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ with coefficients in the short sequence above.

$$0 \to \mathbf{D}_{st}(T_pE) \to \mathbf{D}_{st}(V_pE) \to \mathbf{D}_{st}(V_pE/T_pE) \to H^1(\mathbb{Q}_p, T_pE \otimes \mathbf{B}_{st}) \to ...$$

On the other hand we have $T_pE \otimes \mathbf{B}_{st} \simeq V_pE \otimes \mathbf{B}_{st}$, so the sequence above is short exact

$$0 \to \mathbf{D}_{st}(T_pE) \to \mathbf{D}_{st}(V_pE) \to \mathbf{D}_{st}(V_pE/T_pE) \to 0$$

If we apply now invariants of monodromy to the sequence above we will get

$$\mathrm{coker}(\mathbf{D}_{st}(V_pE)^{N=0} \to \mathbf{D}_{st}(V_pE/T_pE)^{N=0}) \simeq H^1(\langle N=0\rangle, \mathbf{D}_{st}(T_pE)).$$

The corollary now follows from the fact 9.18 which is an analogue of the isomorphism $\mathrm{coker}(V_l^{I_p} \xrightarrow{f} (V_l/T_l)^{I_p}) \simeq \Phi(\mathbb{F}_p)$ from the case of $l \neq p$. We will prove it here.

Fact 9.18. *Let E be an elliptic curve over $\mathbb{Q}_p$ with semi-stable reduction at p. Then*

$$\mathrm{coker}(\mathbf{D}_{st}(V_pE)^{N=0} \to \mathbf{D}_{st}(V_pE/T_pE)^{N=0}) \simeq \Phi(\mathbb{F}_p)$$

for $\Phi(\mathbb{F}_p)$ – the cyclic group of connected components in the special fiber of the Neron model $\mathcal{E}(\mathbb{Z}_p)$.

It means that together with an isomorphism $h^1(D_p) \simeq H^1_e(\mathbb{Q}_p, V_pE)$ we have the following diagram

$$\begin{array}{ccccc} & & & & h^1(D_p) \\ & & & & \downarrow \\ \mathrm{coker}(\mathbf{D}_{st}(V_pE) \xrightarrow{1-\mathrm{Fr}} \mathbf{D}_{st}(V_pE)) & \longrightarrow & H^1(\mathbb{Q}_p, V_pE) & \longrightarrow & H^1(\langle N\rangle, \mathbf{D}_{st}(V)) \end{array}$$

So the desired value of measure of $H^1_e(\mathbb{Q}_p, V_pE)$ follows from diagram. □

Proof. of the Fact 9.18 By the Theorem of Tate [MP05] an elliptic curve with semi-stable reduction over a p-adic field is isomorphic to a Tate curve $\overline{\mathbb{Q}_p}^{\times}/q^{\mathbb{Z}}$ up to a twist which does not influence the group of connected components. By the same result the j-invariant of this curve is represented by a power series with q^{-1} as the leading term, therefore $v_p(j(E)) = -v_p(q)$.
By the theorem of Kodaira and Neron VII.6.1 in [Sil09] the last value is exactly additive reverse to the order of the cyclic group of connected components $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. On the other hand we know how Tate module looks like in the case of Tate curve

$$0 \to \mathbb{Q}_p(1) \to V_pE \to \mathbb{Q}_p \to 0$$

The monodromy operator is acting on 2-dimensional space $\mathbf{D}_{st}(V_pE)$ is represented by a matrix $\begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix}$. We see that the cokernel in the Formula 9.18 consists of elements in T_pE annihilated by monodromy. Since T_pE is a $\mathbb{Z}_p$-module of rank 2 the kernel of monodromy is a cyclic group of order $v_p(q)$. □

Remark 9.19. *To prove the Corollary 9.14 an alternative intuitively easy argument can be used for elliptic curves and abelian varieties only by the Example 3.11 in [BK90]. In that case we have an isomorphism $H^1_f(\mathbb{Q}_p, T_p\mathcal{E}) \simeq E(\mathbb{Q}_p)$, so we are only looking for a measure of Mordell-Weil group. By Neron mapping property we have $E(\mathbb{Q}_p) \simeq \mathcal{E}(\mathbb{Z}_p)$, denote by $\mathcal{E}^0(\mathbb{F}_p)$ the connected component of O in the special fiber of the Neron model $\mathcal{E}$, then*

$$0 \to \mathcal{E}^0(\mathbb{F}_p) \to \mathcal{E}(\mathbb{F}_p) \to \Phi(\mathbb{F}_p) \to 0.$$

From this sequence we deduce the following: Since $\mathcal{E}^0$ is smooth over $\mathbb{Z}_p$ and

an open subgroup of $\mathcal{E}$ we have a fiber square

$$\begin{array}{ccc} \mathcal{E}^0(\mathbb{Z}_p) & \longrightarrow & \mathcal{E}^0(\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathcal{E}(\mathbb{Z}_p) & \longrightarrow & \mathcal{E}(\mathbb{F}_p) \end{array}$$

From the isomorphism $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$ we get an open subgroup of $E(\mathbb{Q}_p)$ corresponding to $\mathcal{E}^0(\mathbb{Z}_p)$, denote it by $E^0(\mathbb{Q}_p)$, then we obtain $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p) \simeq \Phi(\mathbb{F}_p)$. Bearing in mind that $T_p(\Phi(\mathbb{F}_p)) = \Phi(\mathbb{F}_p)$ since $\Phi(\mathbb{F}_p)$ is cyclic of order p^n for some n we get

$$\mu(H^1_f(\mathbb{Q}_p, T_p\mathcal{E})) = |\Phi(\mathbb{F}_p)| \cdot \mu(H^1_f(\mathbb{Q}_p, T_p\mathcal{E}^0)).$$

The measure of $\mu(H^1_f(\mathbb{Q}_p, T_p\mathcal{E}^0))$ is computed by the Lemma 9.12.

9.1.3 Primes at ∞

At last it remains to investigate primes of the only other type left by now, namely archimedean, i.e. we are left with computing $\mu_\infty(A(\mathbb{R}))$.

Lemma 9.20. *For the case of an elliptic curve the value of $\mu_\infty(E(\mathbb{R}))$ equals to $\det \Omega_E$ from the Beilinson Conjecture 5.8.*

Proof. Lets have a look at what is $\det \Omega_E$. In the Remark 5.8 $\det \Omega_E$ is proven to be $c_\infty \int_{\gamma^+} \omega$, where c_∞ is the number of connected components in $E(\mathbb{R})$, ω is the Neron differential, and γ is the corresponding generator of $H_{1,sing}(E(\mathbb{C}), \mathbb{Q})$.

Recall the de Rham Theorem 5.6 which induces an isomorphism

$$\alpha_{dR} : H^1_{dR}(E) \otimes \mathbb{C} \to H^1_{sing}(E, \mathbb{Q}) \otimes \mathbb{C}$$

which descends to $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ invariant subgroups

$$\alpha^+_{dR} : H^1_{sing}(E, \mathbb{Q}) \otimes \mathbb{R} \to H^1_{dR}(E)/Fil^0 H^1_{dR}(E) \otimes \mathbb{R}.$$

Then by definitions of determinant, the pairing from de Rham theorem, and generators of both $H^{1+}_{sing}(E,\mathbb{Q})$ and $H^1_{dR}(E)/Fil^0H^1_{dR}(E)$ we have $\det\Omega_E = \det\alpha^+_{dR}$. On the other hand the integral $\int_{\gamma^+}\omega$ can be defined as an integration of ω over the real part of $H_{1,sing}(E,\mathbb{C})$, denoted by $H^+_{1,sing}(E,\mathbb{R})$ which is one-dimensional vector space over $\mathbb{R}$. Consider the lattice $\Gamma\subset\mathbb{C}$ defining $j: E(\mathbb{C})\simeq\mathbb{C}/\Gamma$. Then volume $vol(E(\mathbb{C})) = \int_{E(\mathbb{C})}\mathrm{d}\,\omega\wedge\omega_1$, which is by Stokes theorem equal to integral $\int_\Gamma\omega\wedge\omega_1$.

Generators γ^+,γ^- of $H_{1,sing}(E,\mathbb{C})$ together form the boundary of the fundamental domain of Γ so we integrate along cycles γ^+,γ^-. But we are interested in volume of a connected component of $E(\mathbb{R})$, and to get it we integrate along the generator of $H^+_{1,sing}(E,\mathbb{R})$. So we consider only the real part of the integral above, namely $\int_{\gamma^+}\omega$ which is $\frac{\det\Omega_E}{c_\infty}$ by above.

We have computed measure $\mu(E(\mathbb{R}))$, but we were interested in $A(\mathbb{R})$ from the Definition 9.3. They are the same in our case by the Remark 9.27. □

The next step is to define in a natural way global groups $A(\mathbb{Q})$ together with natural homomorphisms $A(\mathbb{Q})\to A(\mathbb{Q}_p)$ for all p. For that Bloch and Kato define the group $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q},M\otimes\widehat{\mathbb{Z}})$.

Definition 9.21. *The group $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q},M\otimes\widehat{\mathbb{Z}})$ is the subgroup of all cohomology classes in $H^1(\mathbb{Q},M\otimes\widehat{\mathbb{Z}})$ which under all localization maps $H^1(\mathbb{Q},M\otimes\widehat{\mathbb{Z}})\to H^1(\mathbb{Q}_p,M\otimes\widehat{\mathbb{Z}})$ land in $H^1_f(\mathbb{Q}_p,M\otimes\widehat{\mathbb{Z}})$ for all rational primes $p\leq\infty$.*

Conjecture 9.22. ***Beilinson, Jannsen***

Let $\mathcal{M} := h^m(X)(r)$ for a smooth proper scheme X with proper regular model $\mathcal{X}$ over $\mathbb{Z}$. Consider a finite dimensional $\mathbb{Q}$-vector space

$$\begin{cases}\Phi := \mathrm{Im}(gr^1(K_{2r-m-1}(\mathcal{X})\otimes\mathbb{Q})\to gr^1(K_{2r-m-1}(X)\otimes\mathbb{Q}))\\ \text{for case of } m\neq 2r-1;\\ \Phi^m := CH^r(X)^0\otimes\mathbb{Q} \text{ if } m=2r-1;\end{cases}$$

sometimes it is called the zeroes motivic cohomology of X. Here $CH^r(X)^0_{\mathbb{Q}}$ are

cycles homologically equivalent to 0.

Then there is an isomorphism induced by Chern class map:

$$\Phi \otimes \mathbb{A}_{\mathbb{Q}} \simeq H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, V \otimes \mathbb{A}_{\mathbb{Q}}) \subset H^1(\mathbb{Q}, V \otimes \mathbb{A}_{\mathbb{Q}}).$$

Definition 9.23. *Assuming the conjecture holds Bloch and Kato define a subgroup* $A(\mathbb{Q}) \subset H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, V \otimes \mathbb{A}_{\mathbb{Q}})$ *as the preimage of* $\Phi \otimes 1$ *under the above Isomorphism 9.22. It is well defined since the lattice* $M \otimes \widehat{\mathbb{Z}}$ *is Galois stable.*

Remark 9.24. *For a motivic pair* (V, D) *the groups* $A(\mathbb{Q}_p)$ *are defined as finite Bloch-Kato Selmer groups. We have mentioned already that in our case they are isomorphic to the p-primary Selmer groups and due to the Fundamental Exact Sequence 1.4 in the chapter on Selmer groups and Proposition 9.47 this is up to torsion isomorphic to Mordell-Weil group. This explains notation* $A(\mathbb{Q}_p)$.

Lemma 9.25. *For our main case of* $\mathcal{M} = h^1(E)(1)$ *the conjecture holds as we have only two motivic cohomology groups* $\Phi = 0$ *and* $\Phi^1 \simeq E(\mathbb{Q}) \otimes \mathbb{Q}$. *Moreover in this case* $A(\mathbb{Q})$ *is just the Mordell-Weil group* $E(\mathbb{Q})$.

Proof. First we compute Φ^1. By definition

$$\Phi^1 = CH^1(E)^0 \otimes \mathbb{Q} \simeq \mathrm{Pic}^0(E(\mathbb{Q})) \otimes \mathbb{Q} \simeq E(\mathbb{Q}) \otimes \mathbb{Q}.$$

For the second part we need to compute the image of $E(\mathbb{Q}) \otimes 1$ in the group $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, V \otimes \mathbb{A}_{\mathbb{Q}})$ under the above Isomorphism 9.22. Since the group $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, V(E))$ contains $E(\mathbb{Q})$ and the map 9.22 is injective, we get the $E(\mathbb{Q})$ itself. □

Conjecture 9.26. ***Beilinson***

For X *and* Φ *as in the Conjecture 9.22 in case if* $m \neq 2r-1, 2r-2$ *the*

regulator map induces an isomorphism:

$$Reg : \Phi \otimes \mathbb{R} \simeq H^m_{dR}(X)/(Fil^r H^m_{dR}(X) + H^m(X(\mathbb{C}), \mathbb{R}(2\pi i)^r))^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}.$$

Remark 9.27. *It is easy to see that in case of $\mathcal{M} = h^1(E)(1)$ this conjecture means $E(\mathbb{Q}) \otimes \mathbb{R} \simeq (H^1_{dR}(E/\mathbb{C})/(H^0(E, \Omega^1_E) + H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i))))^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}$ which is true by the Definition 9.3.*
We can find natural homomorphisms $A(\mathbb{Q}) \to A(\mathbb{Q}_p)$ induced by

$$H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, M \otimes \widehat{\mathbb{Z}}) \to H^1_f(\mathbb{Q}, M \otimes \widehat{\mathbb{Z}}),$$

and we will prove later in the Lemma 9.44 that all torsion elements in $A(\mathbb{Q})$ are coming from Galois fixed part of $H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i)) \otimes \mathbb{Q}/\mathbb{Z}$.

9.2 Motives and L-functions

We have already mentioned motives in this thesis a couple of times, but now we want to give some notion of pure motives and their weights. This is again classical theory but we recall it here briefly for completeness. For reasons and motivations see [Mil13].

Definition 9.28. *We define the category $\mathcal{MOT}(\mathbb{Q})$ of Grothendieck motives over $\mathbb{Q}$ in the following way:*

- *For every smooth projective variety $X/\mathbb{Q}$ and an integer number $n \in \mathbb{Z}$ we have an object $(X, e, n) \in \mathcal{MOT}(\mathbb{Q})$, where $e \in \mathrm{End}(X, X)$ is an idempotent which is often omitted from notation.*
- *Morphisms in $\mathcal{MOT}(\mathbb{Q})$ are $Hom((X, e, n), (Y, f, m)) := f \circ C^{\dim X}(X \times Y) \circ e$, where $C^{\dim X + m - n}(X \times Y)$ is the group of correspondences from X to Y of degree $m - n$ defining algebraic cycles up to numerical equivalence of degree $\dim X + m - n$ in $X \times Y$.*

This category has a number of interesting properties:

- *The category $\mathcal{MOT}(\mathbb{Q})$ is semi-simple and abelian;*
- *The Hom sets are finite-dimensional $\mathbb{Q}$-vector spaces;*
- *There is a notion of direct sum of motives: $(X, e, n) \oplus (Y, f, n) := (X \sqcup Y, e \oplus f, n)$;*
- *There is a notion of tensor product of motives: $(X, e, n) \otimes (Y, f, m) := (X \times Y, e \times f, n + m)$;*
- *There is a notion of a dual motive $(X, e, n)^\vee$ together with the universal evaluation map $ev : (X, e, n) \otimes (X, e, n)^\vee \to (\mathbb{P}^1, 0, 0)$.*

We generally deal with a motive via its realizations, naturally we want realizations of a motive defined by a variety X to represent various cohomology theories of X. We will show the true nature of realizations of a motive (X, e, n). Consider a cohomology theory $\mathcal{H}$ over some field K, then there is a functor $F : \mathcal{MOT}(\mathbb{Q}) \to \mathrm{Vect}(K)$ such that:

$$F(X, e, 0) = \mathcal{H}^*(X) = \bigoplus_{i=0}^{2\dim X} H^i(X).$$

Conjecturally $(X, e, 0)$ itself can be decomposed into a direct sum $\bigoplus_0^{2\dim X}(X, e_i, 0)$ mapping into the above summandwise. Further on we will denote motive (X, e_i, n) by $h^i(X)(n)$.

Example 9.29. *Consider a motive $\mathcal{M} = (X, e_i, n)$, then the realizations*

- ***The l-adic realization*** *$\mathcal{M}_l$ is a finite dimensional $\mathbb{Q}_l$-linear representation of $G_\mathbb{Q}$. In our case it is the space of etale cohomology of X. We have $\mathcal{M}_l = H^i_{et}(X, \mathbb{Q}_l)(n)$.*
- ***The Betti realization*** *$\mathcal{M}_B$ is a finite dimensional $\mathbb{Q}$-vector space with an action of complex conjugation and a Hodge structure*

$$\mathcal{M}_B \otimes \mathbb{C} \simeq H^{i,j}$$

where $H^{i,j}$ are $\mathbb{C}$-vector spaces and complex conjugation acts as $\iota H^{i,j} := H^{j,i}$.

In our case it is the Betti cohomology of X, namely $\mathcal{M}_B = H^i((X \times \mathbb{C})(\mathbb{C}), \mathbb{Q}(n))$.

- ***The de Rham realization*** *$\mathcal{M}_{dR}$ is a finite-dimensional $\mathbb{Q}$-vector space equipped with a decreasing exhaustive filtration $Fil^k \mathcal{M}_{dR}$. In our case it is the de Rham cohomology of X, we have $\mathcal{M}_{dR} = H^i(X_{Zar}, \Omega^\bullet_{X/\mathbb{Q}})(n)$ with filtration defined by $Fil^k \mathcal{M}_{dR} = H^i(X_{Zar}, \Omega^{\geq k+n}_{X/\mathbb{Q}})$.*

These realizations satisfy classical and p-adic Hodge theory comparison theorems. And we define the rank of a motive as

$$\operatorname{rank} \mathcal{M} := \dim_{\mathbb{Q}} \mathcal{M}_B = \dim_{\mathbb{Q}} \mathcal{M}_{dR} = \dim_{\mathbb{Q}_l} \mathcal{M}_l.$$

We recall here the common definition of the motivic L-function $L(\mathcal{M}, s)$, see also [Nek94].

Definition 9.30. *For a pure motive $\mathcal{M}$ over the field $\mathbb{Q}$ we define the local L-factor at prime $p \neq l$ as*

$$P_p(\mathcal{M}, s) := \det(1 - \operatorname{Fr}_p^{-1} l^{-s}; \mathcal{M}_l^{I_p}).$$

For a prime $l = p$ the local L-factor looks like

$$P_p(\mathcal{M}, s) := \det(1 - \operatorname{Fr}_p^{-1} l^{-s}; \mathbf{D}_{cris}(\mathcal{M}_p)).$$

For archimedean primes we define the L-function for two motives and in the rest of cases it is uniquely determined by properties of motivic L-function below. If $\mathcal{M}$ is of rank 1 and has de Rham realization of Hodge type $(0, 0)$, then

$$P_\infty(\mathcal{M}, s) := \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2);$$

If $\mathcal{M}$ is of rank 2 and has de Rham realization of Hodge type $(k,0)+(0,k)$ for $k>0$, then

$$P_\infty(\mathcal{M},s) := \Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1).$$

The global motivic L-function for a finite set of places $S \ni \infty$ is defined as the product

$$L_S(\mathcal{M},s) := \prod_p P_p(\mathcal{M},s)^{-1}.$$

Remark 9.31. *Local L-factors satisfy the following properties:*

$$\begin{aligned} P_p(\mathcal{M}(n),s) &:= P_p(\mathcal{M},s+n); \\ P_p(\mathcal{M}_1 \oplus \mathcal{M}_2,s) &:= P_p(\mathcal{M}_1,s)P_p(\mathcal{M}_2,s); \end{aligned} \tag{9.6}$$

Remark 9.32. *Consider a motive $\mathcal{M} = h^1(E)(1)$ for an elliptic curve E. Note that the motivic L-function used by Bloch and Kato needs to be twisted in this case by 1, because $L(\mathcal{M}(1),s) = L(\mathcal{M},s+1)$ so further instead of the value of L-function at 0 we will always consider its value at 1.*
It follows directly from definitions that for the motive $\mathcal{M} = h^1(E)(1)$ the L-function coincides with the L-function for elliptic curve E defined in 2.2, since in this case all the corresponding local L-factors coincide.

Remark 9.33. ***A conjecture on weights*** *According to definition in [Nek94] the motive $\mathcal{M} = h^i(X)(n)$ has weights $w := i-2n$.*
An alternative definition of weight by Bloch and Kato says that a motive $\mathcal{M}$ has weight w if for all non-archimedean primes p the polynomial $P_p(\mathcal{M},s)$ is of the form $\prod(1-\alpha_i s)$ such that $|\alpha_i| \leq p^{w/2}$. In this case the L-function converges absolutely for $\mathrm{Re}(s) > w/2+1$.
It is not known however why two different definitions give the same result of motivic weight.

Lemma 9.34. *For the case of $\mathcal{M} = h^1(E)(1)$ the Euler product of motivic L-function defined above converges absolutely for all $s > \frac{1}{2}$.*

Proof. First note that by the Example above 9.29 for a motive coming from

an elliptic curve $\mathcal{M} = h^1(E)(1)$ the etale realization is the dual to the rational Tate module $\mathcal{M}_l = H^1_{et}(E, \mathbb{Q}_l) = V_l(E)^\vee$ by the Fact 2.12.

For an elliptic curve we know how local Euler factors look like in the Lemma 2.13. In case of quadratic polynomial, namely for primes of good reduction we can write it down as $(1 - \alpha l^{-s})(1 - \beta^{-s})$, where α, β are eigenvalues of Frobenius map. Then their absolute values $|\alpha_p| = |\beta_p| = p^{-1/2}$.

For the product $\prod_{p \notin S} \det(1 - \mathrm{Fr}_p^{-1}\, p^{-s}; \mathcal{M}_l^{I_p})^{-1}$ to converge we need the series $\sum_p (\alpha_p + \beta_p) p^{-s}$ to converge, which absolute value is less than $2 \sum p^{-1/2} p^{-s}$ and converges for $-\operatorname{Re} s - \frac{1}{2} < -1$. □

9.2.1 Formulation of the conjecture

A motive $\mathcal{M} = h^i(X)$ corresponds to a motivic pair by defining $V := \mathcal{M}_B$, then $\mathcal{M}_B \otimes \mathbb{A}_\mathbb{Q} \simeq \prod_l' \mathcal{M}_l$, where the product of all the $H^i_{et}(X, \mathbb{Q}_l)$ is taken with respect to $H^i_{et}(X, \mathbb{Z}_l)$. Since $\mathbf{D}_{dR}(V_l)$ are defined locally for each l the corresponding $D := \mathcal{M}_{dR}$ is defined.

Before we define measure on the product of all $A(\mathbb{Q}_p)$ we should recall the following fact about the L-function of an elliptic curve.

Theorem 9.35. *[Wil95] From now until the end of this section we will be working with an elliptic curve E with finite set S of rational primes of bad reduction containing ∞. Consider the corresponding L-function $L(E, s)$ which can be analytically continued to $\mathrm{Re}(s) > 1 - \varepsilon$ for $\varepsilon = \frac{1}{2}$ as we have seen above. In our case of $\mathcal{M} = h^1(E)(1)$ the L-function of elliptic curve corresponds to an L-function of a cusp form by the Theorem of Taylor and Wiles.*

Therefore just like in the Definition 5.9 [BK90] we can define a measure on the adelic product $\prod_{p \leq \infty} A(\mathbb{Q}_p)$ as

$$\mu := |\lim_{s \to 0} (s-1)^k L(E, s)^{-1}| \mu_\infty \prod_{p \in \mathbb{Z}} (P_p(V, 1)^{-1} \mu_p). \tag{9.7}$$

Here k is the order of vanishing of $L(E, s)$ at 1. Moreover by Lemmas 9.8,

and 9.14 the adelic measure above is well-defined since it contains only finite amount of multiples not equal to 1.

Definition 9.36. *In case of a motive $\mathcal{M}$ of pure weight -1 we consider corresponding motivic pair (V, D) and a lattice $T \subset V$ as defined in the previous section. Then in [BK90] the Tamagawa number is defined as*

$$\mathrm{Tam}(M) = \mathrm{Tam}(V, D) := \frac{\mu(\prod_p A(\mathbb{Q}_p)) \cdot \mathrm{R}}{|A(\mathbb{Q})_{tor}|}.$$

Where R *is the determinant of the height pairing defined in 5.4.*

Remark 9.37. *Note that it doesn't quite correspond to the usual Tamagawa number in BSD conjecture, but instead it cares about regulator as well. But even more it can also be seen why Tamagawa number in Bloch-Kato conjecture is called so. In fact in the BSD conjecture items about regulator and Tamagawa number encode some "volume" of certain archimedean groups, so they can be understood as measures of certain groups.*
Originally in the most general case of motives of weight ≤ -3 the Tamagawa number was defined in a bit different way. Namely

Definition 9.38.

$$\mathrm{Tam}(V, D) := \mu\Big(\prod_p \frac{A(\mathbb{Q}_p)}{A(\mathbb{Q})}\Big)$$

However in our case the definition containing regulator is more viable. Moreover both definitions are equivalent. For an elliptic curve E we characterized regulator as the volume of the fundamental domain of the lattice $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ inside $E(\mathbb{R})$. We have also proven in the Proposition 5.10 that the usual Neron-Tate height pairing coincides with Beilinson height pairing defined in 5.4. Then by the original definition of Tamagawa number we have:

$$\frac{\mu(\prod_p E(\mathbb{Q}_p))}{\mu(E(\mathbb{Q}))} = \frac{\mu(\prod_{p<\infty} E(\mathbb{Q}_p))\mu(E(\mathbb{R}))}{\mu(E(\mathbb{Q}))} = \frac{\mu(\prod_{p<\infty} E(\mathbb{Q}_p))\mu(E(\mathbb{R}))}{\mu(E(\mathbb{Q})/E(\mathbb{Q})_{tor}) \cdot |E(\mathbb{Q})_{tor}|} =$$

$$= \frac{\mu(\prod_{p<\infty} E(\mathbb{Q}_p))\mathrm{Reg}}{|E(\mathbb{Q})_{tor}|}.$$

Definition 9.39. *For a motivic pair (V, D) with lattice M Bloch and Kato define the analogue of Tate-Shafarevich group as:*

$$Ш(T)_{BK} := \ker\Big(\frac{H^1(\mathbb{Q}, T\otimes\mathbb{Q}/\mathbb{Z})}{A(\mathbb{Q})\otimes\mathbb{Q}/\mathbb{Z}} \xrightarrow{\alpha_T} \bigoplus_{p\le\infty} \frac{H^1(\mathbb{Q}_p, T\otimes\mathbb{Q}/\mathbb{Z})}{A(\mathbb{Q}_p)\otimes\mathbb{Q}/\mathbb{Z}}\Big) \tag{9.8}$$

We will prove in the Lemma 9.43 that in our case this is usual Tate-Shafarevich group of elliptic curve. One may view the map in the Definition 9.39 as a short exact sequence with $\ker\alpha_M$ and $\mathrm{coker}\alpha_M$ on its sides then it is proven in [BK90] that $\mathrm{coker}\alpha_M$ is finite. We can not quite talk about Euler characteristic of this sequence as some items participating in it are infinite. However we can encode their relation in the Tamagawa number and make one useful classic assumption:

Conjecture 9.40. *As defined in 9.39 the Tate-Shafarevich group $Ш_{BK}$ is of finite order.*

In such case we may consider Euler characteristic of this sequence.

Lemma 9.41. *Define $\chi(T) := \mathrm{Tam}(T)\cdot|Ш_{BK}(T)|\cdot|\mathrm{coker}\alpha_T|^{-1}$ the inverse to the Euler characteristic of the exact sequence defining $Ш_{BK}$. Then for any lattice $T'\subset V$ with $T'\otimes\widehat{\mathbb{Z}}$ Galois stable in $V\otimes\mathbb{A}_{\mathbb{Q}}$ we have $Ш(T')$ finite as well and moreover $\chi(T) = \chi(T')$.*

This lemma is proven in the Chapter 5 of [BK90] and it is the promised earlier reason not to care much about lattice T, we will further denote everything as depending on the motivic pair (V, D) only, which is equivalent data to a motive. Altogether this comes to the formulation of Tamagawa number conjecture by Bloch and Kato.

Conjecture 9.42. ***Tamagawa number conjecture***

For a motivic pair (V, D) consider a Galois stable $\mathbb{Z}$-lattice T in V. Then the value of the corresponding Euler characteristic $\chi(T) = 1$.

Our main result of this chapter is to see what does it mean for the L-function of an elliptic curve E when $(V, D) = (V := H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i)), \mathbf{D}_{dR}(V))$. The answer is that the Birch and Swinnerton-Dyer conjecture can be deduced from the Tamagawa number conjecture. We will do it in a few steps each of which is taking part of the formula in the Lemma 9.41 above and viewing it in the case of elliptic curve. The first step is to look at the Tate-Shafarevich group.

Lemma 9.43. *In the case when* $\mathcal{M} = h^1(E)(1)$ *with* $V = H^1(E(\mathbb{C}), \mathbb{Q}(2\pi i))$ *and* $D = H^1_{dR}(E/\mathbb{Q})$ *for the lattice* $T = H^1(E(\mathbb{C}), \mathbb{Z}(2\pi i))$ *we have* $Ш(T)_{BK} = Ш(E/\mathbb{Q})$.

Proof. To prove it we remember the short exact sequence from Selmer groups chapter for any integer m:

$$0 \to E(\overline{\mathbb{Q}})[m] \to E(\overline{\mathbb{Q}}) \stackrel{[m]}{\to} E(\overline{\mathbb{Q}}) \to 0$$

and take cohomology of $G_{\mathbb{Q}}$ with coefficients in this sequence. Then

$$0 \to E(\mathbb{Q})[m] \to E(\mathbb{Q}) \stackrel{[m]}{\to} E(\mathbb{Q}) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})[m]) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \to 0$$

The first term is zero for big enough m and the last arrow is clearly surjective. Then we can rewrite this sequence as:

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})[m]) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \to 0 \tag{9.9}$$

Note that for $m = p^n$ we have $E(\overline{\mathbb{Q}})[p^n] \simeq T_pE/p^n$ for any prime p. Then taking the direct limit over all n which is left-exact in our case:

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathbb{Q}, T_pE \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \to 0$$

From this sequence we obtain an isomorphism:

$$H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \simeq \frac{H^1(\mathbb{Q}, T_pE \otimes \mathbb{Q}_p/\mathbb{Z}_p)}{E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

Since it's valid for all primes p we can replace T_pE with $T(E)$. The above construction works well for all $\mathbb{Q}_p$ instead of $\mathbb{Q}$ so we have isomorphisms:

$$H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}_p})) \simeq \frac{H^1(\mathbb{Q}_p, T(E) \otimes \mathbb{Q}/\mathbb{Z})}{E(\mathbb{Q}_p) \otimes \mathbb{Q}/\mathbb{Z}}$$

which means that the Definition 9.39 recovers the original Definition 1.4 of Tate-Shafarevich group from the chapter on Selmer groups. □

Next we would like to understand what is $\mathrm{coker}\alpha_T$.

Lemma 9.44.

- *In general for a motivic pair associated to an algebraic variety a $\mathbb{Z}$-lattice $T = H^m(X, \mathbb{Z}(2\pi i)^r)$ in space $V = H^m(X, \mathbb{Q}(2\pi i)^r)$ the $\mathrm{coker}\alpha_T$ is finite and there is an isomorphism between $H^0(\mathbb{Q}, T^* \otimes \mathbb{Q}/\mathbb{Z}(2\pi i))^*$ and $\mathrm{coker}\alpha_T$.*
- *For a $\mathbb{Z}$-lattice T in a space V there is an isomorphism $A(\mathbb{Q})_{tor} \simeq H^0(\mathbb{Q}, T \otimes \mathbb{Q}/\mathbb{Z})$.*

Here we denote by $T^* := \mathrm{Hom}(T, \mathbb{Z})$ the dual lattice to T. For the case of elliptic curve we have $T = H^1(E(\mathbb{C}), \mathbb{Z}(2\pi i))$, so $T^* \otimes \mathbb{Q}/\mathbb{Z}(2\pi i) \simeq H^1(E(\mathbb{C}), \mathbb{Q}/\mathbb{Z})$. Then for an elliptic curve the second part means $H^0(\mathbb{Q}, T^* \otimes \mathbb{Q}/\mathbb{Z}(2\pi i)) \simeq E^\vee(\mathbb{Q})_{tor}$. By the Tate duality we get then

$$E(\mathbb{Q})_{tor} \simeq E^\vee(\mathbb{Q})_{tor} \simeq H^0(\mathbb{Q}, T^* \otimes \mathbb{Q}/\mathbb{Z}(2\pi i))^* \simeq \mathrm{coker}\alpha_T.$$

This would mean that number of elements in $\mathrm{coker}\alpha_T$ equals number of elements in $A(\mathbb{Q})_{tor}$.

Proof. The first part is the Lemma 5.14 in [BK90] which is proven in the article. The second part is the Lemma 5.10 (i) which was not proven there. By the Definition 9.23 the group $A(\mathbb{Q})$ in general is the finitely generated abelian group such that

$$A(\mathbb{Q}) \otimes \widehat{\mathbb{Z}} \simeq H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, T \otimes \widehat{\mathbb{Z}}).$$

which means that torsion in $A(\mathbb{Q})$ is isomorphic to torsion in $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, T \otimes \widehat{\mathbb{Z}})$. From now we will consider $T = H^1(E(\mathbb{C}), \mathbb{Z}(2\pi i))$, then $T \otimes \widehat{\mathbb{Z}} \simeq T(E)$. First we want to prove that

Fact 9.45. $H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, T(E))_{tor} \simeq H^1(\mathbb{Q}, T(E))_{tor}$.

Proof. By definition of $H^1_{f,\mathrm{Spec}(\mathbb{Z})}$ we have for any p a commutative diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1_{f,\mathrm{Spec}(\mathbb{Z})}(\mathbb{Q}, T(E))_{tor} & \longrightarrow & H^1(\mathbb{Q}, T(E))_{tor} \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1_f(\mathbb{Q}_p, T(E))_{tor} & \longrightarrow & H^1(\mathbb{Q}_p, T(E))_{tor} \longrightarrow H^1(I_{\mathbb{Q}_p}, T(E))_{tor} \end{array}$$

where the last arrow comes from the Definition of $H^1_f(\mathbb{Q}_p, T(E))$ as an unramified cohomology 6.2. To prove the Fact above we need only that $H^1(I_{\mathbb{Q}_p}, T(E))$ has no torsion for any prime p. That means $H^1_f(\mathbb{Q}_p, T(E))_{tor} \simeq H^1(\mathbb{Q}_p, T(E))_{tor}$ and the fact follows from diagram. □

We have mentioned in the Lemma 2.13 that in the case of primes of good reduction the inertia acts trivially on Tate module. Then we are left with semistable reduction which can be achieved over finite extension. In this case we know how exactly inertia acts on T_pE, namely $\begin{pmatrix} 1 & 0 \\ \phi(\sigma) & 1 \end{pmatrix}$. Then $H^1(I_{\mathbb{Q}_p}, T_pE)$ by definition is the group of cocycles f such that $f(\sigma\gamma) = f(\sigma) + \sigma f(\gamma)$ modulo all principal cocycles $f(\sigma) = \sigma(x, y) - (x, y) = (0, \phi(\sigma)x)$.
On the other hand $f(\sigma\gamma)(x, y) = f(\sigma) + f(\gamma) + (0, \phi(\sigma)x')$ then after factoring by principal cocycles we get $f(\sigma\gamma) = f(\sigma) + f(\gamma)$ instead of cocycle condition. Which means that $H^1(I_{\mathbb{Q}_p}, T_pE) = \mathrm{Hom}(I_{\mathbb{Q}_p}, T_pE)$ and since T_pE is free over $\mathbb{Z}_p$ we find out there is no torsion in $H^1(I_{\mathbb{Q}_p}, T_pE)$.
It remains to understand torsion in $H^1(\mathbb{Q}, T(E))_{tor}$. We will again work with the situation locally for every prime p. Lets have a look at a short exact sequence:

$$0 \to p^n T_pE \to T_pE \to T_pE/p^n \to 0$$

The corresponding long exact cohomology sequence:

$$0 \to H^0(\mathbb{Q}, p^n T_p E) \to H^0(\mathbb{Q}, T_p E) \to H^0(\mathbb{Q}, T_p E/p^n T_p E) \to$$
$$H^1(\mathbb{Q}, p^n T_p E) \to H^1(\mathbb{Q}, T_p E) \to H^1(\mathbb{Q}, T_p E/p^n T_p E) \to H^2(\mathbb{Q}, p^n T_p E) \tag{9.10}$$

In terms of group cohomology we have isomorphisms $H^*(\mathbb{Q}, p^n T_p E) \simeq H^*(\mathbb{Q}, T_p E)$, so the long exact sequence implies

$$0 \to H^0(\mathbb{Q}, T_p E/p^n T_p E) \to H^1(\mathbb{Q}, T_p E) \to ...$$

which means that the torsion as the finite piece of the abelian group $H^1(\mathbb{Q}, T_p E)_{tor} = H^0(\mathbb{Q}, T_p E/p^n T_p E)$ for any p, n. Taking colimits and considering situation over all p we get

$$H^1(\mathbb{Q}, T(E))_{tor} \simeq H^0(\mathbb{Q}, T(E) \otimes \mathbb{Q}/\mathbb{Z}).$$

□

Now from results on measures in Lemmas 9.8, 9.12 and Corollaries 9.9 and 9.14 above we see that for primes of bad reduction $p \in S \setminus \infty$ we get $\mu_p(A(\mathbb{Q}_p)) = c_p$ and the measure of the group of points in archimedean case $\mu_\infty(A(\mathbb{R})) = \Omega_+$ which is proven in the Lemma 9.20. Combining it with Lemmas 9.43 and 9.44 we obtain the following

Theorem 9.46. *For the case of $\mathcal{M} = h^1(E)(1)$ with $V = H^1(E, \mathbb{Q}(2\pi i))$ and $D = H^1_{dR}(E/\mathbb{Q})$ the Birch and Swinnerton-Dyer Conjecture 3.5 follows from the Tamagawa number Conjecture 9.42.*

Proof. By the Definition of the adelic measure 9.7 we write:

$$\mu(\prod_{p \leq \infty} A(\mathbb{Q}_p)) = \Big| \lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} \Big|^{-1} \mu_\infty(A(\mathbb{R})) \prod_{p \in \mathbb{Z}} \frac{\mu_p(A(\mathbb{Q}_p))}{P_p(V, 1)}.$$

Denote the leading coefficient $\frac{L(E,s)}{(s-1)^r} =: L(E,1)^*$, so the formula looks like:

$$\mu(\prod_{p\leq\infty} A(\mathbb{Q}_p)) = |L(E,1)^*|^{-1}\mu_\infty(A(\mathbb{R}))\prod_p \frac{\mu_p(A(\mathbb{Q}_p))}{P_p(V,1)}.$$

By the Lemma 9.8 we know that for good reduction primes the bit

$$\prod_{p\notin S} \frac{\mu_p(A(\mathbb{Q}_p))}{P_p(V,1)} = 1$$

while by the Lemma 9.12 primes of bad reduction give Tamagawa numbers:

$$\prod_{p\in S\setminus\infty} \frac{\mu_p(A(\mathbb{Q}_p))}{P_p(V,1)} = \prod_{p\in S\setminus\infty} c_p.$$

On the other hand from the Tamagawa number Conjecture 9.42 it follows:

$$|\mathrm{coker}\alpha_T|^{-1}\cdot \mathrm{Tam}(T)\cdot |Ш_{BK}(T)| = 1.$$

By the definition of the Tamagawa number for motives of weight -1:

$$\mathrm{Tam}(T) = \frac{\mu(A(\mathbb{A}_\mathbb{Q}))\cdot \mathrm{Reg}}{|A(\mathbb{Q})_{tor}|} = \frac{\mu(\prod_{p\leq\infty} A(\mathbb{Q}_p))\cdot \mathrm{Reg}}{|A(\mathbb{Q})_{tor}|}.$$

Rewrite the above formula according to this and get:

$$\frac{\mu(\prod_{p\leq\infty} A(\mathbb{Q}_p))\cdot \mathrm{Reg}\cdot |Ш_{BK}(T)|}{|A(\mathbb{Q})_{tor}|\cdot|\mathrm{coker}\alpha_T|} = 1.$$

Then by the formula for adelic measure we can write down a formula for the leading coefficient of L-function of an elliptic curve:

$$|L(E,1)^*| = \frac{\prod_{p\in S\setminus\infty}\frac{\mu_p(A(\mathbb{Q}_p))}{P_p(V,1)}\cdot\mu_\infty(A(\mathbb{R}))\cdot \mathrm{Reg}(E)\cdot|Ш_{BK}(T)|}{|A(\mathbb{Q})_{tor}|\cdot|\mathrm{coker}\alpha_T|} \qquad (9.11)$$

Then by the Lemma 9.44 $|L(E,1)^*| = \frac{\prod_{p\in S} c_p\cdot\Omega_E\cdot\mathrm{Reg}(E)\cdot|Ш_{BK}(T)|}{|E(\mathbb{Q})_{tor}|^2}$. Which is nothing but the second part of the Birch and Swinnerton-Dyer Conjecture 3.5 after applying Lemmas 9.43, and Proposition 5.10. □

9.3 Finiteness of Ш

We will prove the Proposition 5.4 from article of Bloch and Kato [BK90].

Proposition 9.47. *Let K be a number field, E be an elliptic curve. Then there is an injection $E(K)\otimes\widehat{\mathbb{Z}} \hookrightarrow H^1_g(K, T(E))$. If it is an isomorphism, then the l-primary part of Tate-Shafarevich group $Ш(E/K)[l^\infty]$ is finite for all l.*

Proof. We will work out the statement locally for all primes $v \in K$. We must deal with possibilities for l separately first discussing $l \neq p$ and then $l = p$ where v is a prime over p. Recall that $T(E) = \prod_l T_l E$ and so the isomorphism above is equivalent to $E(K) \otimes \mathbb{Z}_l \simeq H^1_g(K, T_l E)$ for all l.
We start with the easier case $l \neq p$, which means by definition that $H^1_g(K_v, V_l E) = H^1(K_v, V_l E)$. Then since $H^1_g(K, T(E))$ is the pre-image of $H^1_g(K_v, V(E))$ under the inclusion $\iota : H^1(K, T(E)) \hookrightarrow H^1(K_v, T(E) \otimes \mathbb{Q})$ we find that $H^1_g(K, T_l E) = H^1(K, T_l E)$.
From the isomorphism above we see that $E(K)\otimes\mathbb{Z}/l^n\mathbb{Z} \simeq H^1_g(K, T_l E)\otimes\mathbb{Z}/l^n\mathbb{Z}$, so $E(K)/(l^n) \simeq H^1(K, E[l^n])$, taking the direct limit over all n we get $E(K)\otimes \mathbb{Q}_l/\mathbb{Z}_l \simeq H^1(K, E[l^\infty])$. Due to the short exact sequence 1.4 to prove finiteness of the Tate-Shafarevich group is the same as to prove equality of ranks of the Selmer group and the Mordell-Weil group. Now by definition of Selmer group and by above we get

$$\mathrm{Sel}(E[p^\infty]/K) = \ker(E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l \to \prod_\eta H^1(K_v, E[p^\infty])/E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

which then coincides with $E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l$ and therefore has the same rank.
As usually case of $l = p$ is more complicated but more interesting as well. We will follow the same strategy of proving ranks equality but first we would like to understand some more information about $H^1_g(K, V_l E)$. The Tate representation is de Rham by the Theorem of Fontaine so we can apply the dimension

formula 8.17 to find that

$$\dim H^1_g(K_v, V_pE) = \dim(\mathbf{D}_{dR}(V_pE)/\mathbf{D}^+_{dR}(V_pE)) + \dim \mathbf{D}_e(V_pE^*(1)) + \dim H^0(K_v, V_pE).$$

we used here the fact that under duality between $H^1(K, V)$ and $H^1(K, V^*(1))$ the spaces $H^1_e(K, V)$ and $H^1_g(K, V^*(1))$ are exact orthogonals to each other, it is proven in the Proposition 3.8 in [BK90].

Now we use the fact that $\dim_{\mathbb{Q}_p} H^1_g(K_v, V_pE) = \operatorname{rank}_{\mathbb{Z}_p} H^1_g(K_v, T_pE)$ and so by the condition $H^1_g(K_v, T_pE) \simeq E(K) \otimes \mathbb{Z}_p$ all we need is $\operatorname{rank}_{\mathbb{Z}_p} H^1_g(K_v, T_pE)$ to be equal to $\operatorname{rank}_{\mathbb{Z}_p} H^1_e(K_v, T_pE)$ which is the rank of Selmer group by Lemma 6.7. Note that this would imply $H^1_e(K_v, T_pE) = H^1_f(K_v, T_pE) = H^1_g(K_v, T_pE)$. This needed equality follows from the Theorem of Bloch and Kato 4.1 in [BK90] that exponential map 8.2 is an isomorphism and the fact of $H^1_e(K_v, V_pE) = H^1_f(K_v, V_pE)$. Note that this is true also for $V_pE^*(1)$ instead of V_pE. So we get

$$H^1_f(K_v, V_pE) \perp H^1_f(K_v, V_pE^*(1)) = H^1_e(K_v, V_pE^*(1)) \perp H^1_g(K_v, V_pE)$$

and since all are exact orthogonals we get $H^1_f(K_v, V_pE) = H^1_g(K_v, V_pE)$. □

9.4 Conclusion

The Birch and Swinnerton-Dyer conjecture was formulated as a result of numerical experiment, but it is not easy to understand why the result happens to be the exact conjectural formula.

However the viewpoint of Bloch-Kato conjecture provides an environment for careful reasoning on the origins of BSD conjecture. It is no longer a computational experiment, but a rigorous statement about an exactness of a certain sequence.

In order to formulate the Bloch-Kato conjecture one has to study theory of motives, motivic L-function, and motivic cohomology. By today motives is

the only well-working version of a unified cohomology theory, it is thought of as cohomology of an algebraic variety with coefficients in $\mathbb{Q}$. We need them because of the way Bloch and Kato conjecture is formulated, namely we apply similar operations to cohomology groups with coefficients in all completions of the field of rational numbers.

Bibliography

[Art68] M. Artin. *The etale topology of schemes*. English. Tr. Mezhdunarod. Kongr. Mat., Moskva 1966, 44-56. 1968.

[BB08] Denis Benois and Laurent Berger. "Théorie d'Iwasawa des représentations cristallines. II." French. In: *Comment. Math. Helv.* 83.3 (2008), pp. 603–677. ISSN: 0010-2571.

[BC09] Oliver Brinon and Brian Conrad. *CMI SUMMER SCHOOL NOTES ON p-ADIC HODGE THEORY*. 2009. URL: https://math.stanford.edu/~conrad/papers/notes.pdf.

[Bei85] A. A. Beilinson. "Higher regulators and values of L-functions". In: *J. Sov. Math.* 30 (1985), pp. 2036–2070. ISSN: 0090-4104.

[Bei87] A. A. Beilinson. *Height pairing between algebraic cycles*. English. K-theory, arithmetic and geometry, Semin., Moscow Univ. 1984-86, Lect. Notes Math. 1289, 1-26 (1987). 1987.

[Bel09] Joel Bellaiche. *An introduction to Bloch and Kato's conjecture*. 2009. URL: https://www.claymath.org/sites/default/files/bellaiche.pdf.

[BK90] Spencer Bloch and Kazuya Kato. "L-functions and Tamagawa numbers of motives". English. In: *The presentation functor and the compactified Jacobian*. 1990, pp. 333–400.

[Blo80] S. Bloch. "A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture". English. In: *Invent. Math.* 58 (1980), pp. 65–76. ISSN: 0020-9910.

[BM02] Christophe Breuil and William Messing. *Torsion étale and crystalline cohomologies.* Paris: Société Mathématique de France, 2002, pp. 81–124. ISBN: 2-85629-117-1.

[BMS18] Bhargav Bhatt, Matthew Morrow, and Peter Scholze. "Integral p-adic Hodge theory". In: *Publ. Math., Inst. Hautes Étud. Sci.* 128 (2018), pp. 219–397. ISSN: 0073-8301.

[Bre+01] Christophe Breuil et al. "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises". English. In: *J. Am. Math. Soc.* 14.4 (2001), pp. 843–939. ISSN: 0894-0347.

[Bre02] Christophe Breuil. "Integral p-adic Hodge theory." English. In: *Algebraic geometry 2000, Azumino. Proceedings of the symposium, Nagano, Japan, July 20–30, 2000*. Tokyo: Mathematical Society of Japan, 2002, pp. 51–80. ISBN: 4-931469-20-5.

[BS65] B. J. Birch and H. P. F. Swinnerton-Dyer. "Notes on elliptic curves. II". In: *J. Reine Angew. Math.* 218 (1965), pp. 79–108. ISSN: 0075-4102.

[CF00] Pierre Colmez and Jean-Marc Fontaine. "Construction des représentations p-adiques semi-stables". French. In: *Invent. Math.* 140.1 (2000), pp. 1–43. ISSN: 0020-9910. DOI: 10.1007/s002220000042.

[Col19] Collective. *Jean-Marc Fontaine and Jean-Pierre Wintenberger*. 2019. URL: https://webusers.imj-prg.fr/~pierre.colmez/FW.html?fbclid=IwAR1seGn2OPmXMm1ru5egg8DW-yFPJaNOBjcLENc1otFg8F12HXklj

[Dar+13] Henri Darmon et al., eds. *Elliptic curves, Hilbert modular forms and Galois deformations*. English. Basel: Birkhäuser/Springer, 2013, pp. xii + 249. ISBN: 978-3-0348-0617-6; 978-3-0348-0618-3.

[Del79] Pierre Deligne. *Valeurs de fonctions L et périodes d'intégrales*. French. Automorphic forms, representations and L-functions, Proc. Symp. Pure Math. Am. Math. Soc., Corvallis/Oregon 1977, Proc. Symp. Pure Math. 33, No. 2, 313-346. 1979.

[DEW21] Vladimir Dokchitser, Robert Evans, and Hanneke Wiersema. *On a BSD-type formula for L-values of Artin twists of elliptic curves*. 2021.

[Fal88] Gerd Faltings. "p-adic Hodge theory". English. In: *J. Am. Math. Soc.* 1.1 (1988), pp. 255–299. ISSN: 0894-0347. DOI: 10.2307/1990970.

[FF18] Laurent Fargues and Jean-Marc Fontaine. *Courbes et fibrés vectoriels en théorie de Hodge p-adique*. Vol. 406. Paris: Société Mathématique de France (SMF), 2018, pp. xiii + 382. ISBN: 978-2-85629-896-1.

[FL82] Jean-Marc Fontaine and Guy Laffaille. "Construction de représentations p-adiques." In: *Ann. Sci. Éc. Norm. Supér. (4)* 15 (1982), pp. 547–608. ISSN: 0012-9593.

[Fla04] Matthias Flach. *The equivariant Tamagawa number conjecture: a survey*. Providence, RI: American Mathematical Society (AMS), 2004, pp. 79–125. ISBN: 0-8218-3480-0.

[FO] Jean-Marc Fontaine and Yi Ouyang. *Theory of p-adic Galois Representations*. URL: https://www.imo.universite-paris-saclay.fr/~fontaine/galoisrep.pdf.

[Fon82] Jean-Marc Fontaine. "Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate." French. In: *Ann. Math. (2)* 115 (1982), pp. 529–577. ISSN: 0003-486X. DOI: 10.2307/2007012.

[Fon94a] Jean-Marc Fontaine. "Exposé III : Représentations p-adiques semi-stables". fr. In: *Périodes ¡span class="mathjax-formula"¿p¡/span¿-adiques - Séminaire de Bures, 1988*. Ed. by Jean-Marc Fontaine. Astérisque 223. talk:3. Société mathématique de France, 1994. URL: http://www.numdam.org/item/AST_1994__223__113_0/.

[Fon94b] Jean-Marc Fontaine, ed. *Périodes p-adiques. Séminaire du Bures-sur-Yvette, France, 1988*. French. Vol. 223. Paris: Société Mathématique de France, 1994, p. 397.

[FP94] Jean-Marc Fontaine and Bernadette Perrin-Riou. *Autour des conjectures de Bloch et Kato: Cohomologie galoisienne et valeurs de fonctions L*. Providence, RI: American Mathematical Society, 1994, pp. 599–706. ISBN: 0-8218-1636-5; 0-8218-1635-7.

[Gre99] Ralph Greenberg. "Iwasawa theory for elliptic curves". In: *Arithmetic theory of elliptic curves. Lectures given at the 3rd session of the Centro Internazionale Matematico Estivo (CIME), Cetraro, Italy, July 12–19, 1997*. Berlin: Springer, 1999, pp. 51–144. ISBN: 3-540-66546-3.

[Gro16] Study Group. *Number theory learning seminar 2015-2016*. 2015-2016. URL: http://virtualmath1.stanford.edu/~conrad/BSDseminar/.

[Har83] Robin Hartshorne. *Algebraic geometry. Corr. 3rd printing*. English. Vol. 52. Springer, Cham, 1983, pp. xvi + 496.

[HK94] Osamu Hyodo and Kazuya Kato. "Exposé V: Semi-stable reduction and crystalline cohomology with logarithmic poles". English. In: (1994), pp. 221–268.

[Jor05] Andrei Jorza. *The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields*. 2005. URL: https://www3.nd.edu/~ajorza/notes/bsd.pdf.

[Kat04] Kazuya Kato. *p-adic Hodge theory and values of zeta functions of modular forms*. Paris: Société Mathématique de France, 2004, pp. 117–290. ISBN: 2-85629-118-9.

[Kat93] Kazuya Kato. *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}*. Berlin: Springer-Verlag, 1993, pp. 50–163. ISBN: 3-540-57110-8.

[Kin03] Guido Kings. "The Bloch-Kato conjecture on special values of L-functions. A survey of known results." In: *J. Théor. Nombres Bordx.* 15.1 (2003), pp. 179–198. ISSN: 1246-7405.

[Kin11] Guido Kings. *The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture*. Providence, RI: American Mathematical Society (AMS); Princeton, NJ: Institute for Advanced Study., 2011, pp. 315–349. ISBN: 978-0-8218-5320-7.

[KM76] Finn Knudsen and David Mumford. "The projectivity of the moduli space of stable curves. I: Preliminaries on "det" and "Div"". In: *Math. Scand.* 39 (1976), pp. 19–55. ISSN: 0025-5521.

[Mil13] James S. Milne. *Motives – Grothendieck's dream*. Somerville, MA: International Press; Beijing: Higher Education Press, 2013, pp. 325–342. ISBN: 978-1-57146-278-7.

[MP05] Yu. I. Manin and A. A. Panchishkin. *Introduction to modern number theory. Fundamental problems, ideas and theories. Transl. from the Russian*. English. Vol. 49. Berlin: Springer, 2005, pp. xv + 514. ISBN: 3-540-20364-8.

[MR20] Barry Mazur and Karl Rubin. *Arithmetic conjectures suggested by the statistical behaviour of modular symbols*. 2020. URL: https://arxiv.org/pdf/1910.12798.pdf.

[MT83] B. Mazur and J. Tate. *Canonical height pairings via biextensions*. English. Arithmetic and geometry, Pap. dedic. I. R. Shafarevich, Vol. I: Arithmetic, Prog. Math. 35, 195-237. 1983.

[MT87] B. Mazur and J. Tate. "Refined conjectures of the "Birch and Swinnerton-Dyer type"". In: *Duke Math. J.* 54 (1987), pp. 711–750. ISSN: 0012-7094.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer". In: *Invent. Math.* 84 (1986), pp. 1–48. ISSN: 0020-9910.

[Nek94] Jan Nekovář. *Beilinson's conjectures*. Providence, RI: American Mathematical Society, 1994, pp. 537–570. ISBN: 0-8218-1636-5; 0-8218-1635-7.

[Ota18] Kazuto Ota. "Kato's Euler system and the Mazur-Tate refined conjecture of BSD type". In: *Am. J. Math.* 140.2 (2018), pp. 495–542. ISSN: 0002-9327.

[Pol03] Alexander Polishchuk. *Abelian varieties, theta functions, and the Fourier transform*. English. Vol. 153. Cambridge: Cambridge University Press, 2003, pp. xvi + 292. ISBN: 0-521-80804-9.

[PRS11] Cristian Popescu, Karl Rubin, and Alice Silverberg, eds. *Arithmetic of L-functions. Lecture notes from the IAS/Park City Mathematics Institute (PCMI) graduate summer school, Park City, UT, USA, 2009*. English. Vol. 18. Providence, RI: American Mathematical Society (AMS); Princeton, NJ: Institute for Advanced Study., 2011, pp. xiv + 499. ISBN: 978-0-8218-5320-7.

[Roh88] David E. Rohrlich. "L-functions and division towers". In: *Math. Ann.* 281.4 (1988), pp. 611–632. ISSN: 0025-5831.

[RSS88] M. Rapoport, Norbert Schappacher, and P. Schneider, eds. *Beilinson's conjectures on special values of L-functions (based on the meeting of the Arbeitsgemeinschaft Geyer-Harder held in Oberwolfach, FRG in April 1986)*. English. Boston, MA etc.: Academic Press, Inc., 1988, pp. xxiii + 373. ISBN: 0-12-581120-9.

[Sch88] Peter Schneider. *Introduction to the Beilinson conjectures*. English. Beilinson's conjectures on special values of L-functions, Meet. Oberwolfach/FRG 1986, Perspect. Math. 4, 1-35. 1988.

[Sch94] A. J. Scholl. *Height pairings and special values of L-functions*. English. Providence, RI: American Mathematical Society, 1994, pp. 571–598. ISBN: 0-8218-1636-5; 0-8218-1635-7.

[Ser79] Jean-Pierre Serre. *Local fields. Translated from the French by Marvin Jay Greenberg*. English. Vol. 67. Springer, Cham, 1979.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. English. Vol. 106. New York, NY: Springer, 2009, pp. xx + 513. ISBN: 978-0-387-09493-9; 978-0-387-09494-6.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. English. Vol. 151. New York, NY: Springer-Verlag, 1994, pp. xiii + 525. ISBN: 0-387-94325-0.

[Ski18] Cristopher Skinner. *Lectures on the Iwasawa theory of elliptic curves*. 2018. URL: https://www.math.arizona.edu/~swc/aws/2018/2018SkinnerNotes.pdf.

[Ven07] Otmar Venjakob. *From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture – a survey*. 2007.

[Vol05] Maja Volkov. "A class of p-adic Galois representations arising from abelian varieties over $\mathbb{Q}_p$". In: *Math. Ann.* 331.4 (2005), pp. 889–923. ISSN: 0025-5831.

[Wik21] Wikipedia. *Birch and Swinnerton-Dyer conjecture*. 2021. URL: https://en.wikipedia.org/wiki/Birch_and_Swinnerton-Dyer_conjecture.

[Wil95] Andrew Wiles. "Modular forms, elliptic curves, and Fermat's Last Theorem". English. In: *Proceedings of the international congress of mathematicians, ICM '94, August 3-11, 1994, Zürich, Switzerland. Vol. I*. Basel: Birkhäuser, 1995, pp. 243–245. ISBN: 3-7643-5153-5.