An introduction to the conjecture of Bloch and Kato

Two lectures at the Clay Mathematical Institute Summer School,
Honolulu, Hawaii, 2009

Prerequisites: The prerequisites for these lectures are elementary:

(i) Algebraic number theory, including class field theory, and structure of the Galois group of number fields (decomposition groups, Frobenius elements, etc);

(ii) Basic theory of finite-dimensional representations of groups;

(iii) Group cohomology.

Some knowledge of Galois cohomology (the duality theorems and the Euler-Poincaré characteristic formula) can be useful, but I shall recall what I need. Similarly, I shall recall and use some hard results in étale cohomology, and it is not necessary to know them beforehand, nor their proof, but a familiarity with algebraic geometry is necessary to understand their formulation.

Exercises: There are exercises in the text. I shall try to separate them in the notes for other lectures, but here it would be artificial. Some exercises have the label **(easy)**, which means that you should be able to solve them at sight, if you have read and understood what is just above. So if you try and can't solve an easy exercise, reread what is above and try again. If you still can't solve it, then I have made a mistake. Most exercises have no label, meaning that they are of intermediate difficulty and that you should be able to solve them with a paper and a pencil in a few minutes. Some have the label **(difficult)**, and they are difficult exercises that need either some real new ideas, or the knowledge of some other theory, or both.

Terminology and convention: In all those lectures, a p-adic representation V of G will be a *finite-dimensional* vector space over $\mathbb{Q}_p$, with a continuous linear action of a topological group G (in general a Galois group). We could also consider representations over finite extensions of $\mathbb{Q}_p$, but those representations can be seen as p-adic representations in our sense, so this greater generality would only be apparent. If V is a p-adic representation, $V(n)$ is V tensor the cyclotomic character to the power n. The symbol dim means the dimension over $\mathbb{Q}_p$, when not otherwise specified.

Depending on the context, K will be either a characteristic 0 local field, or a number field. In the latter case, v will denote a place of K, and G_v will denote G_{K_v}. There is a natural morphism $G_v \to G_K$ well defined up to conjugacy that allows us to define the restriction $V_{|G_v}$ to G_v of a representation of G_K, without ambiguity up to equivalence.

Frobeniuses are arithmetic Frobeniuses, denoted Frob_v. *Predictions* are corollary of conjectures. Errors are mine.

CONTENTS

The aim of those lectures is to introduce the conjecture of Bloch-Kato and to explain its number-theoretical significance. This conjecture appeared in print ([BK])

in 1990 in The Grothendieck Festschrift[1] related to a collection of papers in honor of Grothendieck's 60th birthday. It generalizes at least some important part of the Birch and Swinnerton-Dyer conjecture, which is one of the seven Clay's millennium problem.

This conjecture has a particularity: it is a "second-order conjecture" (or call it a meta-conjecture if you are fond of Hofstadter). That is to say, it talks about objects whose basic properties, and which is worse sometimes definitions, depend on unproved conjectures. A consequence is that there are several formulations of the Bloch-Kato conjecture, that should be equivalent, but for which a proof of their equivalence requires using more basic, or level-1, but yet unproved and certainly very hard, conjectures.

In this lecture, I shall present a panorama of those level-1 conjectures needed to get a full grasp of the Bloch-Kato conjecture, that I shall try to motivate by showing how many classical (solved or still conjectural) questions of number theory can be reformulated to become a special part of it.

In doing so, I will restrain myself to only a part of the conjecture of Bloch-Kato, the part concerned with characteristic 0 phenomena. That is to say, I will consider only Galois representations over finite extensions of $\mathbb{Q}_p$, instead of $\mathbb{Z}_p$ or $\mathbb{Z}/p^n\mathbb{Z}$, (or "iso-motives" instead of "motives", see below §1.3) and order of zero and poles of L-functions, instead of their principal values. I have to warn the reader that this is only the tip of the iceberg. There is a world of interesting phenomena in characteristic p, and even if we are only concerned with characteristic 0 questions, some motivations, and the proofs of many results unavoidably require a détour in characteristic p. Yet I believe that it may be easier to get a global picture of this huge set of conjectures, and of what is proved (very little) by restraining ourselves to characteristic 0.

In characteristic 0, the Bloch-Kato conjecture relates two objects attached to a geometric Galois representation. A *geometric Galois representation V* is a semi-simple continuous representation of the absolute Galois group G_K of a number field K on a finite dimensional vector space V over $\mathbb{Q}_p$ (or some finite extension) which satisfies certain properties satisfied by the Galois representations that appears in the étale cohomology $H^i(X, \mathbb{Q}_p)$ (see below §1.1.1) of proper and smooth variety X over K. It is conjectured (the Fontaine-Mazur conjecture) that every geometric

---

[1]Actually, this paper contains two important and related but quite different conjectures, and both have been known as "the Bloch-Kato conjecture", which has been a frequent source of confusion during the past twenty years. The conjecture that will be studied in those notes, arguably the most fundamental of the two, is the one that is also known as "the Tamagawa number conjecture", though as we restrict ourselves here to characteristic 0 phenomena, there will be no Tamagawa number whatsoever. The **other** Bloch-Kato conjecture, which generalizes the Milnor conjecture and a proof of which has been announced in 2009, relates the Bloch-Kato Selmer group (an object we shall study in these notes) to K-theory (that shall not be used here) – see 2.3.4 for a few more details and [W] for an introduction to **that** conjecture.

representation appears this way. The first section will include a quick discussion of those geometric Galois representations and their fundamental properties (be they proved or conjectural).

To a geometric representation V of G_K, one can attach two objects, one analytic, and one algebraic, and the Bloch-Kato's conjecture is a mysterious relation between those objects. The analytic object is an analytic function of a complex variable s, with possibly some poles, the L-function $L(V, s)$. Its definition and properties are studied in section 3. The algebraic object is called the Bloch-Kato Selmer groups and denoted by $H^1_f(G_K, V)$. It is a $\mathbb{Q}_p$-vector space, and it is an attempt to generalize for any geometric representation V the Mordell-Weil group of an elliptic curve (in the sense that if $V_p(E)$ is the Tate module of an elliptic curve E over K, we have a canonical injective linear map $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \hookrightarrow H^1_f(G_K, V_p(E))$ which is conjecturally an isomorphism, so the rank of the Mordell-Weil group of E should be the same as the dimension of the Bloch-Kato Selmer group of $V_p(E)$). The definition of the Bloch-Kato Selmer group as well as many of its properties are studied in §2. The connection between those two objects predicted by (the characteristic 0 part of) the Bloch-Kato conjecture is that the dimension of $H^1_f(K, V)$ is equal to the order of the 0 of $L(V^*(1), s)$ at $s = 0$ (where V^* is the dual representation of V). Motivation, examples, and stability properties of that conjecture are discussed in §4.

1. Geometric Galois representations

For an alternative exposition of much of this material, see [Tay2].

1.1. **Representations coming from geometry.**

1.1.1. *Very brief reminder on étale cohomology.* Let K be a number field. For X a proper and smooth variety over K of dimension n, i an integer and p a prime number, one sets

$$H^i(X, \mathbb{Q}_p) = \left(\varprojlim H^i_{\text{ét}}(X \times \bar{K}, \mathbb{Z}/p^n\mathbb{Z}) \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

By transport of structure, the $\mathbb{Q}_p$-space $H^i(X, \mathbb{Q}_p)$ has a natural $\mathbb{Q}_p$-linear action of the Galois group G_K. The following properties are well known in étale cohomology. They are the only ones we shall use, so a reader who ignores everything of étale cohomology and takes them as axioms should have no serious problem reading the sequel.

E1.– The space $H^i(X, \mathbb{Q}_p)$ is finite-dimensional and of dimension independent of p. The action of G_K is continuous.

Actually, there is more: If one uses any embedding ι of K into $\mathbb{C}$ to associate to X an algebraic variety $X \times_{K,\iota} \mathbb{C}$ over $\mathbb{C}$, and then its analytic variety X_{an} over $\mathbb{C}$, then $H^i(X, \mathbb{Q}_p)$ is naturally isomorphic as a $\mathbb{Q}_p$-vector space to $H^i_{\text{betty}}(X_{\text{an}}, \mathbb{Q}_p)$,

where the H^i_{betty} is the singular cohomology (or any usual cohomology theory of manifolds).

E2.– $X \mapsto H^i(X, \mathbb{Q}_p)$ is a contravariant functor from the category of proper and smooth varieties over K to the category of p-adic representations of G_K.

E3.– We have $H^i(X, \mathbb{Q}_p) = 0$ for $i < 0$ and $i > 2n = 2 \dim X$. If X is geometrically connected, $H^0(X, \mathbb{Q}_p) = \mathbb{Q}_p$ (with trivial action) and $H^{2n}(X)(\mathbb{Q}_p) = \mathbb{Q}_p(-n)$.

E4.– There is a functorial cup-product map of G_K-representations $H^i(X, \mathbb{Q}_p) \otimes H^j(X, \mathbb{Q}_p) \to H^{i+j}(X, \mathbb{Q}_p)$. When $i + j = 2n$, it is a perfect pairing.

In particular, $H^i(X, \mathbb{Q}_p)^* \simeq H^{2n-i}(X, \mathbb{Q}_p)(-n)$.

Also, if X and Y are two proper and smooth varieties, and k an integer, the natural map

$$\bigoplus_{i+j=k} H^i(X) \otimes H^j(Y) \overset{\text{pr}_1^* \otimes \text{pr}_2^*}{\longrightarrow} \bigoplus_{i+j=k} H^i(X \times Y) \otimes H^j(X \times Y) \overset{\text{cup-product}}{\longrightarrow} H^k(X \times Y)$$

is an isomorphism (this is known as *Kunneth formula*).

Let v be a finite place of K, and $\mathcal{O}_{(v)}$ the localization of the ring of integer $\mathcal{O}_K$ of K at v. We call k_v the residue field of that local ring. We say that X has *good reduction* at v if there is a proper and smooth scheme $\mathcal{X}$ over $\text{Spec} \, \mathcal{O}_{(v)}$ such that $\mathcal{X} \times \text{Spec} \, K \simeq X$. Such an $\mathcal{X}$ is called a *model* of X over $\mathcal{O}_{(v)}$.

E5.– Let v be a finite place of K prime to p. If X has good reduction at v, then the representation $H^i(X, \mathbb{Q}_p)$ is unramified at v. The characteristic polynomial of Frob_v acting on $H^i(X, \mathbb{Q}_p)$ has its coefficients in $\mathbb{Z}$, and is independent of p (as long as p stays prime to v). We call it $P_v(X) \in \mathbb{Z}[X]$. Its roots all have complex absolute value equal to $q_v^{-i/2}$, where q_v is the cardinality of the residue field k_v.

This is part of the cohomological interpretation of the Weil's conjecture due to Grothendieck, the assertion about the absolute value of the roots being the last Weil's conjecture proved by Deligne in 1973. Even if we shall not need it, let us mention the Lefschetz's fixed point formula (aka Lefschetz Trace formula) of Grothendieck: If $\mathcal{X}$ is a model of X over $\mathcal{O}_{(v)}$, and $\mathcal{X}_v$ is its special fiber over k_v, then $|\mathcal{X}_v(k_v)| = \sum_{i=0}^{2n}(-1)^i \text{tr}(\text{Frob}_v|H^i(X, \mathbb{Q}_p))$.

A proper and smooth variety over K has good reduction for almost all v, so $H^i(X, \mathbb{Q}_p)$ is, as a p-adic representation of G_K, unramified at almost all places.

Exercise 1.1. Prove this when X is projective and smooth.

E6.– Let v be a place of K dividing p. Then as a representation of G_v, $H^i(X, \mathbb{Q}_p)$ is de Rham. If X has good reduction at v, $H^i(X, \mathbb{Q}_p)$ is even crystalline.

This is a hard result of Faltings, which will be discussed in Andreatta's lectures ([A]).

E7.– If Z is a subvariety of codimension q, then there is associated to Z a cohomology class $\eta(Z) \in H^{2q}(X, \mathbb{Q}_l)(q)$ that is invariant by G_K. The map η extends

by linearity to cycles and rationally equivalent cycles have the same cohomology class. Intersection of cycles become cup-product of cohomology classes. If P is closed point, then $\eta(P) \in H^{2n}(X, \mathbb{Q}_p)(n) = \mathbb{Q}_p$ is non-zero

Besides those proved (with great difficulties) results, there are still some open conjectures.

EC1.– If X has good reduction at v and v is prime to p, then the operator Frob_v of $H^i(X, \mathbb{Q}_p)$ is semi-simple (that is diagonalizable over $\bar{\mathbb{Q}}_p$.) If v divides p, then if $\varphi = \phi^{f_v}$, where ϕ is the crystalline Frobenius acting on $D_{\mathrm{crys}}(V_{|G_v})$ and f_v is the degree of the residual extension at v of $K/\mathbb{Q}$, the linear operator φ acts semi-simply on $D_{\mathrm{crys}}(V_{|G_v})$.

This is called the *semi-simplicity of Frobenius*. There are also variants for places v with bad reduction. Conjecture EC1 is known for abelian varieties by a theorem of Tate.

EC2.– The representation $H^i(X, \mathbb{Q}_p)$ of G_K is semi-simple.

This is sometimes called "conjecture of Grothendieck-Serre". This is known for abelian varieties, by a theorem that Faltings proved at the same times he proved the Mordell's conjecture, and in a few other cases (some Shimura varieties, for example).

EC3.– The subspace $(H^{2q}(X, \mathbb{Q}_p)(q))^{G_K}$ is generated over $\mathbb{Q}_p$ by the classes $\eta(Z)$ of sub-varieties Z of codimension q.

This is Tate's conjecture, still open.

1.1.2. *Representations coming from geometry.*

Definition 1.1. Let V be an irreducible p-adic representation of G_K. We say that V *comes from geometry* if there is an integer i, an integer n, and a proper and smooth variety X over K such that V is isomorphic to a subquotient of $H^i(X, \mathbb{Q}_p)(n)$. (If EC2 holds, one can replace "sub-quotient" by "sub-representation").

If V is a semi-simple representation of G_K we shall say that V *comes from geometry* if every irreducible component of V comes from geometry.

We shall refrain from talking about non-semi-simple representations coming from geometry. All representations coming from geometry shall be by definition semi-simple.

Exercise 1.2. Show that the category of p-adic representations coming from geometry of G_K (morphisms are morphisms of representations) is stable by dual and by tensor product.

1.2. **Geometric representations.**

1.2.1. *The Fontaine-Mazur conjecture.*

Definition 1.2. Let V be a p-adic semi-simple representation of G_K. We say that V is *geometric* if it is unramified at almost all places and de Rham at all places dividing p.

A p-adic representation V coming from geometry is geometric by properties E5 and E6 above.

Conjecture 1.1 (Fontaine-Mazur)**.** *If V is geometric, then V comes from geometry.*

This fundamental conjecture is still widely open, but impressive progresses have been made in the past fifteen years. Before giving a very quick review of these progresses, we not that the conjecture was known before it was even formulated for abelian representation (this is not trivial however: this uses a combination of global class field theory, Weil's theory of algebraic Hecke characters, and Deuring's theory of complex multiplication for elliptic curves and its generalization to abelian varieties). Most of the recent progresses arose from a work by Taylor who was able to prove ([Tay1]), building on the proof by Wiles and Taylor-Wiles of Fermat's last theorem, on many beautiful new ideas) that a geometric representation V of dimension 2 of $G_{\mathbb{Q}}$ that is odd and with distinct Hodge-Tate weights comes from geometry *after restriction to G_F, where F is a suitable totally real number field.* Such a result is known as a *potential modularity* result. This result has now been reinforced in dimension 2, where Kisin was able to prove that a geometric odd representation V which regular Hodge-Tate weight does come from geometry. More recently, Emerton has given a different proof of the same result. In other word, a great part of Fontaine-Mazur's conjecture in dimension 2 is now known. In higher dimensions, potential modularity results are known (work of Clozel-Harris-Taylor, and others) for many representations V of G_F where F is a totally real field that satisfy a polarization hypothesis, that is that are equivalent, up to a twist, to their dual, and that have distinct weights. Back to dimension 2, it has been observed by Calegari [C], that under some technical restrictions, those higher-dimensional results can be used to remove the oddness condition in Kisin's result. In all those results, the fact that V comes from geometry is actually obtained as a consequence of the fact that V is automorphic (see §1.2.4 below), which is the hard result actually proven.

The Fontaine-Mazur conjecture is widely believed to be true, though a general proof would probably require many completely new ideas.

1.2.2. *Algebraicity and purity. The notion of motivic weight.* Let V be a representation of G_K that is unramified outside a finite set of places Σ.

Definitions 1.3. We shall say that a representation is *algebraic* if there is a finite set of places Σ' containing Σ such that the characteristic polynomial of Frob_v on

V has coefficients in $\bar{\mathbb{Q}}$ when $v \notin \Sigma'$. When one wants to precise the set Σ', we say Σ'-*algebraic*.

For $w \in \mathbb{Z}$, we shall say that a representation is *pure of weight w* if there is a finite set of places Σ' containing Σ such that V is Σ'-algebraic and all the roots of the characteristic polynomial of Frob_v have complex absolute values (for all embeddings of $\bar{\mathbb{Q}}$ to $\mathbb{C}$) $q_v^{-w/2}$. (Here q_v is as above the cardinality of the residue field k_v of K at v). When one wants to specify the set Σ', one says Σ'-*pure*.

When V is pure of weight w, we call w the *motivic weight* of V, or simply its *weight*.

Exercise 1.3. (easy) Show that the cyclotomic character $\mathbb{Q}_p(1)$ is algebraic and pure of weight -2.

Proposition 1.1. *A representation coming from geometry is algebraic. An irreducible representation coming from geometry is pure.*

Proof —   We can assume that V is irreducible, and appears as a sub-quotient of $H^i(X, \mathbb{Q}_p)(n)$ for some X, i, n. Then by E5, V is Σ'-algebraic where Σ' is the set of primes where X has bad reduction or that divides p. Moreover, by E5 as well, V is pure of weight $i - 2n$. $\square$

Remember that $H^i(X, \mathbb{Q}_p)$ is pure of weight i.

If we believe that the Fontaine-Mazur conjecture is true, then

Prediction 1.1. *Any geometric representation is algebraic, and if irreducible, pure of some weight $w \in \mathbb{Z}$.*

This statement does not seem simpler to prove than the Fontaine-Mazur conjecture itself.

1.2.3. *Motivic weight and Hodge-Tate weights.* The notion of *motivic weight* should not be confused with the notion of Hodge-Tate weight. A geometric representation V of dimension d of G_K (K a number field) which is pure has exactly one motivic weight. But each of its restrictions to G_v for v dividing p has d Hodge-Tate weights, so V carries a big package of Hodge-Tate weights.

Yet there is a relation between the Hodge-Tate weights of V and its motivic weight, when both are defined. To state it, let us introduce the following notation:

Definition 1.4. For V a geometric representation of G_K, and for each $k \in \mathbb{Z}$, we denote by $m_k = m_k(V)$ the sum

$$m_k(V) = \sum_{v \mid p} [K_v : \mathbb{Q}_p] m_k(V_{|G_v})$$

where $m_k(V_{|G_v})$ is the multiplicity of the Hodge-Tate weight k for the representation $V_{|G_v}$ of G_v. We call $m_k(V)$ the *total multiplicity of k as an Hodge-Tate weight of V*.

Obviously, the $m_k(V)$ are almost all 0, and we have

$$\sum_{k \in \mathbb{Z}} m_k = [K : \mathbb{Q}] \dim V.$$

Lemma 1.1. *If K_0 is a subfield of K, and $W = \mathrm{Ind}_{G_K}^{G_{K_0}} V$, them $m_k(V) = m_k(W)$.*

The proof is an exercise.

Proposition 1.2. *Let V be a p-adic representation of G_K that is Hodge-Tate at all places dividing p, and pure of weight w.*

(1)
$$w[K : \mathbb{Q}] \dim V = 2 \sum_{k \in \mathbb{Z}} m_k k$$

In other words, the weighted average of the Hodge-Tate weights k of V (weighted by their total multiplicity m_k) is $w/2$.

Proof — We prove this proposition by successive reduction.

First we can assume that $K = \mathbb{Q}$. Indeed, replacing V by $W := \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} V$, the right hand side is unchanged because of Lemma 1.1, and so is the left hand side because $w(V) = w(W)$, and $[K : \mathbb{Q}] \dim V = \dim W$.

Second, we can assume that $\dim V = 1$ (and still $K = \mathbb{Q}$). Indeed, if V is pure of weight w, then $\det V = \Lambda^{\dim V} V$ is of dimension 1 and pure of weight $w \dim V$. Therefore the RHS of (1) for $\det V$ is the same as for V. The same is true concerning the LHS, as the unique Hodge-Tate weight of $(\det V)_{|G_p}$ is the sum of the Hodge-Tate weights of $V_{|G_p}$. So proving the case of $\det V$ implies the case of V.

Third we can assume that $\dim V = 1$, $K = \mathbb{Q}$, and the Hodge-Tate weight of $V_{|G_p}$ is 0. For if this weight is k, then the one of $V(k)$ is 0, and $-2k$ is added to both the LHS and the RHS of (1) when we change V to $V(k)$.

Finally, assume that $\dim V = 1$, $K = \mathbb{Q}$, and that the Hodge-Tate weight of $V_{|G_p}$ is 0. We need to prove that V has motivic weight 0. By Sen's theorem, the inertia I_p of G_p acts through a finite quotient of V. Let χ be the character of $\mathbb{A}_{\mathbb{Q}}^*$ attached to V by global class field theory. By local class field theory and its compatibility with global class field theory, $\ker \chi$ contains an open subgroup U_p of $\mathbb{Z}_p^*$. By continuity, $\ker \chi$ contains also an open subgroup U^p of $\prod_{l \neq p} \mathbb{Z}_l^*$, and by definition it contains $\mathbb{R}_+^*$. Therefore, χ factors through $\mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* U_p U^p \mathbb{R}_*^+$, which is finite. Thus χ has finite image, and this implies immediately that V has motivic weight 0. $\square$

Exercise 1.4. Assume that $V = H^i(X, \mathbb{Q}_p)$ for some proper and smooth variety over K. Give another proof of (1) for V using Faltings's theorem relating the Hodge-Tate decomposition of V with the Hodge decomposition on $H^i(X)$ (see [Co]).

There should actually be stronger relations among the Hodge-Tate weights, but we need to assume conjectures EC2 and EC3 to prove them. Let us just mention

them without proof (but see Exercise 1.7 and Theorem 4.1). The first one is a simple symmetry among Hodge-Tate weights, which is an indirect consequence of Tate's conjecture (EC3).

Prediction 1.2. *Let V be a p-adic representation of G_K coming from geometry. Let w be the motivic weight of V. We have for all $k \in \mathbb{Z}$*

$$m_k = m_{w-k}.$$

As a consequence, if we define

(2) $$m_{<w/2} = \sum_{k<w/2} m_k,$$

then we have

$$[K : \mathbb{Q}] \dim V \ = \ 2m_{<w/2} \text{ if } w \text{ is odd}$$

$$[K : \mathbb{Q}] \dim V \ = \ 2m_{<w/2} + m_{w/2} \text{ if } w \text{ is even.}$$

We can say something more precise. Let

(3) $$a^{\pm}(V) = \sum_{v|\infty} a_v^{\pm},$$

where $a_v^{\pm} = \dim V$ is v is complex, and $a_v^{\pm}$ is the dimension of the ± 1-eigenspace of the action of the complex conjugation at v on V if v is real. In other words,

$$a^+ = \sum_{v|\infty} \dim H^0(G_v, V)$$

We have by simple counting that

$$a^+(V) + a^-(V) = [K : \mathbb{Q}] \dim V,$$

and

$$a^{\pm}(V) = a^{\pm}(\mathrm{Ind}_{G_K}^{G_{K_0}} V).$$

Prediction 1.3. *Let V be a p-adic representation of G_K coming from geometry. Let w be the motivic weight of V. Then $a^{\pm} \geq m_{<w/2}$.*

Of course, if we assume in addition the Fontaine-Mazur conjecture, then Predictions 1.2 and 1.3 should hold for all geometric V. Note that for such a representation, Prediction 1.2 is stronger than Prop. 1.2.

Exercise 1.5. (easy) Keep the hypotheses of Prediction 1.2 and Prediction 1.3 (and suppose they are correct), and assume either that w is odd, or that K is totally complex. Show that $a^+ = a^-$.

Exercise 1.6. Keep the hypotheses of Prediction 1.2 and Prediction 1.3 (and suppose they are correct), and prove that for a representation of $G_{\mathbb{Q}}$ of even dimension and distinct Hodge-Tate weights, we have $\mathrm{tr}(c) = 0$ where c is the non-trivial element of $G_{\mathbb{R}}$ acting on V.

Exercise 1.7. (difficult)

Let X be a proper and smooth variety over $\mathbb{Q}$ and $V = H^i(X, \mathbb{Q}_p)$. Show Predictions 1.2 and 1.3 for V using Faltings' theorem comparing Hodge and Hodge-Tate weight. (Hint: you don't need any conjecture for this case. For Prediction 1.3 use the fact that $H^p(X, \Omega^q)$ and $H^q(X, \Omega^p)$ for $p + q = i$ are conjugate for the relevant complex structure.)

1.2.4. *Automorphic Galois representations.* We can not seriously discuss here the fundamental subject of automorphic forms and their Galois representations, even as a survey, because it would take hundreds of pages and I have to go to the beach. But to complete our picture of the conjectural landscape, and also to prepare the discussion about L-functions of geometric Galois representations, let us just say the following:

We assume that the reader knows (or is ready to pretend he knows) what is a cuspidal automorphic representation $\pi = \otimes'_v \pi_v$ of $\mathrm{GL}_n(\mathbb{A}_K)$ (K a number field) and what it means for such an automorphic representation to be algebraic (this is a condition on the local factors π_v for v archimedean). A p-adic semi-simple Galois representation ρ is *attached to* π if it is unramified almost everywhere, and for almost all places v of K, the characteristic polynomial of Frob_v on V is equal to the Satake polynomial of the local factor π_v, up to a suitable normalization (we have chosen once and for all a embedding of $\mathbb{Q}_p$ into $\mathbb{C}$ to be able to compare the characteristic polynomial of Frob_v who lives in $\mathbb{Q}_p[X]$ and the Satake polynomial who lives in $\mathbb{C}[X]$. But actually, both polynomial should have algebraic coefficients.) By Cebotarev density theorem, if ρ is attached to π it is the only one that is.

It is expected (as a part of the global *Langlands program*) that to every automorphic cuspidal algebraic representation π of GL_n/K as above there exists one (and only one) semi-simple representation $\rho_\pi : G_K \to \mathrm{GL}_n(L)$ attached to π(where L is a finite extension of $\mathbb{Q}_p$ in general, but if π is $\mathbb{Q}$-rational, that is if its Satake polynomials at almost every place have coefficients in $\mathbb{Q}$, we should be able to take $L = \mathbb{Q}_p$.)

A p-adic representation which is ρ_π for some π as above is called *automorphic*.

So far, the main result in that direction is that we know the existence of ρ_π when K is a totally real field (resp. a CM field), when π satisfies a self-duality (resp. conjugate self-duality) condition, and the local factors π_v when v is infinite are not only algebraic, but also *regular* (this condition corresponds to ρ_π having distinct Hodge-Tate weights at places dividing p). This result is an important part of the global Langlands program, and it has required an incredible amount of work along a sketch by Langlands, including the stabilization of the trace formula by Arthur, the proof of the Fundamental Lemma by Laumon and Ngo, and hard final pushes by Shin, Morel, Harris and other. See [Sh], [M], the book project on the web page of Michael Harris, and Shin's lecture for more details.

The representations ρ_π for all cuspidal algebraic π should moreover be irreducible and geometric. In the cases described above, it is known that ρ_π is geometric. (In most of those cases, the representation ρ_π is, by construction, coming from geometry, but there are some cases where ρ_π is constructed by a limiting process, and we only know that it is geometric.) The irreducibility assertion is not known, except in low dimension ($n \leq 3$ by results of Ribet, Wiles, Blasius-Rogawski and $n = 4$, $K = \mathbb{Q}$ by a result of D. Ramakrishna)

Conversely, we have the following folklore conjecture, sometimes called Langlands-Fontaine-Mazur (as it is a combination of the Langlands philosophy and of the Fontaine-Mazur conjecture)

Conjecture 1.2. *Every geometric irreducible p-adic representation of G_K is automorphic.*

So far, mainly cases of dimension 2 and $K = \mathbb{Q}$ (and also all the cases $n = 1$, any K by Class Field Theory) are known.

1.3. **Appendix: Motives.** It is important to be aware that p-adic geometric Galois representations are only a proxy for a more fundamental notion discovered by Grothendieck, the notion of pure iso-motive (many people say "pure motive" or simply "motive" instead of "pure iso-motive", and we shall do the same from now, but the right term should be pure iso-motive as we work with coefficients in characteristic 0, and proper and smooth varieties over K).

Let $\mathcal{VPS}_K$ be the categories of proper and smooth varieties over a field K. Grothendieck and others have constructed many cohomology theories for objects in $\mathcal{VPS}_K$. All are contravariant functors from $\mathcal{VPS}_K$ to some abelian (or at least additive) categories, that satisfy some standard properties. For example, for i an integer, and p a prime, one has the functor $X \mapsto H^i(X, \mathbb{Q}_p)$ defined using étale cohomology as above, from the category $\mathcal{VPS}_K$ to the category of p-adic representations of G_K. We also have the de Rham cohomology $X \mapsto H^i_{\mathrm{dR}}(X)$ from $\mathcal{VPS}_K$ to the category of K-vector spaces with a filtration (the Hodge filtration). As explained in Conrad's lecture [Co] there is no canonical splitting of this filtration in general, but there is one if $K = \mathbb{C}$. If $\iota : K \to \mathbb{C}$ is a field embedding, we also have the functor $X \mapsto H^i_\iota(X, \mathbb{Z}) = H^i_{\mathrm{betty}}((X \times_{K,\iota} \mathbb{C})(\mathbb{C}), \mathbb{Z})$ from $\mathcal{VPS}_K$ to the category of finite $\mathbb{Z}$-modules, where H^i_{betty} is the usual cohomology of topological spaces.

There are some comparison results between those cohomology theories. For example, all our $H^i(X)$ have same dimension or rank. Also, if ι is as above, there is a natural and functorial isomorphism of complex space $u : H^i_\iota(X, \mathbb{Z}) \otimes_\mathbb{Z} \mathbb{C} \simeq H^i_{\mathrm{dR}}(X) \otimes_{K,\iota} \mathbb{C}$. Combining the $H^i_\iota(X, \mathbb{Z})$ and the $H^i_{\mathrm{dR}}(X)$ one can attach functorially on X a rich structure called, according to the following definition a *K-Hodge-deRham structure of weight i* (see the definition below) ; $(H^i_\iota(X, \mathbb{Z}) \otimes_\mathbb{Z} \mathbb{Q}, H^i_{\mathrm{dR}}(X), u, (H^p(X \times \mathrm{Spec}\,\mathbb{C}, \Omega^q))_{p,q \in \mathbb{N}, p+q=i})$.

Definition 1.5. A K-Hodge-deRham structure (where K is a subfield or $\mathbb{C}$, or when an embedding $\iota : K \to \mathbb{C}$ is given) is a 4-uple $(V_{\mathbb{Q}}, V_K, u, (V_{p,q})_{p,q \in \mathbb{Z}^2})$ where V_Q is a finite $\mathbb{Q}$-vector space, V_K a finite K-vector space, u is an isomorphism $V_K \otimes_{K,\iota} \mathbb{C} \to V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$, $(V_{p,q})$ is a finite family of subspaces of $V_K \otimes \mathbb{C}$ such that one has $V_K \otimes \mathbb{C} = \oplus_{p,q} V_{p,q}$, $V_{p,q} = \overline{V}_{q,p}$ for the conjugation on $V_K \otimes \mathbb{C}$ attached to the real structure given by $u^{-1}(V_{\mathbb{Q}} \otimes \mathbb{R})$, and where for each (i, p_0) the subspaces $\oplus_{p \geq p_0} V_{p,i-p}$ of $V_K \otimes \mathbb{C}$ descend to V_K.

If for some $i \in \mathbb{Z}$ we have $V_{p,q} = 0$ whenever $p + q \neq i$, we say that V is pure of weight i.

Grothendieck has conjectured for every field K the existence of a universal abelian category (the category of motives over K) through which all cohomology functors from $\mathcal{VPS}_K$ to various additive categories should factor. More precisely, he has conjectured the existence of a universal $\mathbb{Q}$-linear, abelian, graded, semi-simple category $\mathcal{M}_K$ of (pure iso-) motives over K with contravariant functors $H^i : \mathcal{VPS}_K \to \mathcal{M}_K$ (with image in objects whose only non trivial graded part is gr_i - we call those objects "pure of weight i") and realizations $\mathbb{Q}$-linear functors Real_p, Real_ι, $\mathrm{Real}_{\mathrm{dR}}$ from $\mathcal{M}_K$ to the categories of respectively of p-adic representations of G_K, $\mathbb{Z}$-modules, filtered K-vector spaces, with natural isomorphism of functors $H^i(-, \mathbb{Q}_p) = \mathrm{Real}_p \circ H^i$, $H^i_\iota(-, \mathbb{Z}) = \mathrm{Real}_\iota \circ H^i$, $H^i_{\mathrm{dR}}(-) = \mathrm{Real}_{\mathrm{dR}} \circ H^i$, with functorial isomorphisms $\mathrm{Real}_{\mathrm{dR}} \otimes_{K,\iota} \mathbb{C} \simeq \mathrm{Real}_\iota \otimes_{\mathbb{Z}} \mathbb{C}$ making $\mathrm{Real}_\iota(M) \otimes \mathbb{C}$ a K-Hodge structure $\mathrm{Hodge}(M)$. There should be plenty of other properties (comparison for various K, existence of classes attached to subvarieties, existence of tensor products and dual objects in $\mathcal{M}_K$, etc.) that I shall not state.

Grothendieck has also proposed a construction of this category, but verifying that the resulting category has the required properties needs the so-called *standard conjectures of type Hodge and of type Lefschetz*, that are still open. The standard conjecture of type Hodge is a generalization of Hodge index theorem, and should not be confused with the very famous Hodge conjecture, which also plays a role in the theory of motives. There has been many propositions to define the category of motives assuming different conjectures, or even no conjecture at all, which are important, but none cane provide an unconjectural category of motives unconjecturally satisfying all basic expected properties.

If we admit the standard conjectures, then the category $\mathcal{M}_K$ is constructed, and two of the most important conjectures in algebraic geometry can be reinterpreted as saying that some realization functor from $\mathcal{M}_k$ are fully faithful. First (for $K = \mathbb{C}$, or even K any subfield of $\mathbb{C}$) the functor $M \mapsto \mathrm{Hodge}(M)$ would be fully faithful if and only if the Hodge conjecture held (cf. [H, Prop. 1.2]). Analogously, for K a number field, the Tate conjecture EC3 (combined with the Grothendieck-Serre conjecture EC2) would be equivalent to the full faithfulness, for any prime p, of the functor Real_p from $\mathcal{M}_K$ to the category of p-adic representations of G_K. Therefore,

if those conjecture held, Real_p would be an equivalence from the category of motives $\mathcal{M}_K$ to the categories of representations coming from geometry. This functor sends a motive that is graded only in weight i to a representation that is pure of weight i.

Alternatively, if we are not willing to assume the standard conjectures, but only the Tate and Grothendieck-Serre conjectures, we could choose a prime p and define the category $\mathcal{M}_K$ as the category of p-adic representations coming from geometry of G_K, and the result would be an independent on p semi-simple $\mathbb{Q}$-linear abelian category satisfying all properties stated above (but maybe not all the properties one wants for $\mathcal{M}_K$).

To summarize, in an ideal world in which all what we expect is true, a p-adic representation V of G_K coming from geometry should be not the primary object of interest, but a tangible realization $\mathrm{Real}_p(M)$, or as one says, an *avatar*, of a more fundamental if less accessible object M in the category of motives $\mathcal{M}_K$. The motive M should be determined by V up to isomorphism, and thus in particular to we should be able to attach to V a K-Hodge structure $\mathrm{Hodge}(V) = \mathrm{Hodge}(M)$.

(For more about motives, cf. [**?**] or [An])

2. BLOCH-KATO SELMER GROUPS

For a more advanced presentation of most of this material, see [BK] or [FPR].

2.1. **Reminder of Galois cohomology.**

2.1.1. *Continuous and discrete coefficients.* Let G be a profinite group and p be a prime. We shall consider the following condition, for $i \geq 0$ an integer

(Fin(p,i)) For every open subgroup U of G, the set $H^i(U, \mathbb{Z}/p\mathbb{Z})$ is finite.

(Fin(p)) G satisfies Fin(p,i) for all $i \geq 0$.

Remark 2.1. Fin stands of course for "finiteness". Note that Fin$(p,1)$ is the p-finiteness condition used in Galois deformation theory. (See Kisin's lectures [Ki].)

Exercise 2.1. a.– Let F be the p-Frattini subgroup of U, that is the closure of the subgroup of U generated by all commutators and all p-powers. Show that F is normal in U. Show that $H^1(U, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(U, \mathbb{Z}/p\mathbb{Z})$ is finite if and only if U/F is finite.

b.– **(difficult)** Let L/K be an algebraic Galois extension of fields, and assume that $G = \mathrm{Gal}(L/K)$ satisfies Fin$(p,1)$. Show that G satisfies Fin$(p,2)$ if and only if for all open normal subgroup U of G the group $H^2(G/U, (L^U)^*)[p]$ is finite.

c.– Show that if K is a finite extension of $\mathbb{Q}_l$, then G_K and I_K (the inertia subgroup of G_K) satisfies Fin(p) (use a.– and local class field theory for Fin$(p,1)$; use b.– and the theory of the Brauer group for Fin$(p,2)$. There is nothing to prove (e.g. [S2, Chapter II, §4.3]) for the other cases Fin(p,i), with $i > 2$).

d.– Show that if K is a number field, then G_K **does not** satisfy $\mathrm{Fin}(p,1)$ nor $\mathrm{Fin}(p,2)$. However, show that if Σ is a finite set of places, $G_{K,\Sigma}$ satisfies $\mathrm{Fin}(p)$. (use a.– and global class field theory for $\mathrm{Fin}(p,1)$; use b.– and the theory of the Brauer group for $\mathrm{Fin}(p,2)$. There is almost nothing to prove (e.g. [S2, Chapter II, §4.4]) for the other cases $\mathrm{Fin}(p,i)$, with $i > 2$.

We shall be concerned with continuous group cohomology $H^i(G,V)$ of profinite groups G satisfying $\mathrm{Fin}(p)$ (actually only among the Galois groups considered in the above exercise) with values in finite dimensional $\mathbb{Q}_p$-vector spaces V with a continuous action of G (V being provided with its p-adic topology, given by any p-adic norm).

Let us first note that the usual tools of group cohomology (Shapiro's lemma, inflation-restriction, long exact sequence attached to a short exact sequence) work without problem for continuous cohomology with values in finite dimensional vector space over $\mathbb{Q}_p$ with continuous G-action (that is, p-adic representation). The only technical point to check, for the existence of a long exact sequence, is that a short exact sequence of p-adic representation is always split as a short exact sequence of $\mathbb{Q}_p$-vector spaces, which is obvious.

Since all basic results in Galois cohomology are proved with discrete coefficients, we need a way to pass from discrete coefficients to p-adic coefficients. Such a way is provided by the following result of Tate.

Proposition 2.1 (Tate). *Let G be a profinite group satisfying $\mathrm{Fin}(p)$ and V be a continuous representation of G. Let Λ be a $\mathbb{Z}_p$-lattice in V stable by G.*

  (a) *The continuous cohomology group $H^i(G,\Lambda)$ (with Λ given its p-adic topology) is a finite $\mathbb{Z}_p$-module and we have a canonical isomorphism*

$$H^i(G,V) \simeq H^i(G,\Lambda) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

  (b) *We have a canonical isomorphism $H^i(G,\Lambda) = \varprojlim H^i(G,\Lambda/p^n\Lambda)$ (where $\Lambda/p^n\Lambda$ is a finite group provided with its discrete topology).*

The end of this § is devoted to the proof of (a), which is copied form [T] for the commodity of the reader. For (b), which is simpler, see [T].

Lemma 2.1. *If G is a profinite group satisfying $\mathrm{Fin}(p)$, and A be any finite (discrete) p-primary abelian group with continuous G-action, then the groups $H^i(G,A)$ are finite.*

Proof — There exists an open normal subgroup U such that U acts trivially on A. That is, as an U-module, A is a successive extension of $\mathbb{Z}/p\mathbb{Z}$ (with trivial U-action). By $\mathrm{Fin}(p)$ and the long exact sequences, the groups $H^i(U,A)$ are finite. By the Hochschild-Serre spectral sequence $H^i(G/U,H^j(U,A)) \Rightarrow H^{i+j}(G,A)$, and since G/U is finite, the groups $H^i(G,A)$ are finite. $\square$

Let Λ be any finite-type $\mathbb{Z}_p$-module with a continuous G-action.

Lemma 2.2. *Let Y be a finitely generated $\mathbb{Z}_p$-submodule of $H^i(G, \Lambda)$, and set $Z = H^i(G, \Lambda)/Y$. If $Z = pZ$ then $Z = 0$.*

Proof —   Let $g_1, \ldots, g_k$ be cocycles that represent a generating family of Y. Suppose $x_n \in H^i(G, \Lambda)$, $n = 0, 1, 2, \ldots$, are such that $x_n \equiv px_{n+1} \pmod{Y}$. We need to prove that $x_0 \in Y$. Choosing cocycles f_n representing x_n we have $f_n = pf_{n+1} + \sum_{m=1}^k a_{nm}g_m + dh_n$ with h_n an $(i-1)$-cochain. We thus get by induction and p-adic limit $f_0 = \sum_{m=1}^k (\sum_{n \geq 1} p^n a_{nm})g_m + d(\sum_{n \geq 1} p^n h_n)$, so $x_0 \in Y$. This proves the lemma. $\qquad\square$

Lemma 2.3. *Assume G satisfies Fin(p). Then $H^i(G, \Lambda)$ is finitely generated for all i.*

Proof —   By the long exact sequence, $H^i(G, \Lambda)/pH^i(G, \Lambda)$ is a sub-module of $H^i(G, \Lambda/p\Lambda)$, which is finite by Lemma 2.1. Lifting to $H^i(G, \Lambda)$ all elements of $H^i(G, \Lambda)/pH^i(G, \Lambda)$ we get a family $g_1, \ldots, g_m$ in $H^i(G, \Lambda)$ which generates a $\mathbb{Z}_p$-submodule Y such that $Z := H^i(G, \Lambda)/Y$ satisfies $Z = pZ$. Therefore $Z = 0$, and $H^i(G, \Lambda) = Y$ is finitely generated. $\qquad\square$

Now assume that Λ is free as a $\mathbb{Z}_p$-module, and set $V = \Lambda \otimes \mathbb{Q}_p$, and let $W = V/\Lambda$. We have a long exact sequence attached to the short exact sequence $0 \to \Lambda \to V \to W \to 0$:

$$H^{i-1}(G, V) \to H^{i-1}(G, W) \xrightarrow{\delta} H^i(G, \Lambda) \to H^i(G, V) \to H^i(G, W)$$

Lemma 2.4. *Assume that G satisfies Fin(p). Then $\ker \delta$ is the maximal divisible subgroup of $H^{i-1}(G, W)$ and $\operatorname{Im} \delta$ is the torsion of $H^i(G, \Lambda)$. Moreover $H^{i-1}(G, W)$ is torsion.*

Proof —   The Kernel $\ker \delta$ is the image of the $\mathbb{Q}_p$-vector space $H^{i-1}(G, V)$ and is therefore divisible. By Lemma 2.3, each divisible subgroup of $H^{i-1}(G, V)$ must be in $\ker \delta$. This proves the assertion about $\ker \delta$.

Since G is compact and W is discrete, a cochain $f : G^{i-1} \to W$ takes only a finite number of values, and since W is torsion, so is $H^{i-1}(G, W)$. Therefore the image of δ is torsion. Moreover, the image of δ is the kernel of $H^i(G, \Lambda) \to H^i(G, V)$ and since $H^i(G, V)$ is torsion free, $\operatorname{Im} \delta$ contains all torsion in $H^i(G, \Lambda)$. $\qquad\square$

Using the Lemma (assuming that G satisfies Fin(p)), we see that the natural map $H^i(G, \Lambda) \otimes \mathbb{Q}_p \to H^i(G, V)$ is injective, and that its cokernel is a torsion group tensor $\mathbb{Q}_p$, that is 0. This completes the proof of (a).

2.1.2. *The Kummer morphism.* An important way to construct interesting elements of H^1 is the Kummer construction.

Let K be a field, and A be a commutative group scheme over K, such that the map "multiplication by p", $[p] : A \to A$ is finite and surjective. Let n be an integer. The kernel of the map $[p^n] : A \to A$, that is the multiplication by p^n in A, denoted $A[p^n]$ is a finite abelian group scheme over K, and $A[p^n](\bar{K})$ is a finite abelian group with a continuous action of G_K. The multiplication by p induces surjective homomorphisms $A[p^{n+1}] \to A[p^n]$ of group schemes over K, hence surjective morphisms $A[p^{n+1}](\bar{K}) \to A[p^n](\bar{K})$ compatible with the action of G_K.

We set $T_p(A) = \varprojlim A[p^n](\bar{K})$ and $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. The space $V_p(A)$ is a p-adic representation of G_K.

Examples 2.1. If $A = \mathbb{G}_m$, then $V = \mathbb{Q}_p(1)$. If A is an abelian variety (e.g. an elliptic curve), then $V_p(A)$ is the usual Tate module of A. It satisfies $V_p(A)^*(1) \simeq V_p(A)$ (Weil's pairing).

The Kummer map κ will be a $\mathbb{Q}_p$-linear homomorphism $A(K) \to H^1(G, V_p(A))$ for G some suitable quotient of G_K through which $V_p(A)$ factors. To construct it, we shall take the projective limit of "finite-level Kummer maps" κ_n that we now describe.

We construct a Kummer map

$$\kappa_n : A(K)/p^n A(K) \to H^1(G_K, A[p^n](\bar{K}))$$

as follows. There is a short exact sequence of abelian groups with action of G_K:

$$0 \to A[p^n](\bar{K}) \to A(\bar{K}) \overset{[p^n]}{\to} A(\bar{K}) \to 0.$$

Taking the long exact sequence, we get

(4) $$A(K) \overset{[p^n]}{\to} A(K) \overset{\delta}{\to} H^1(G_K, A[p^n](\bar{K})) \to H^1(G_K, A(\bar{K}))$$

The connecting morphism δ defines an injective morphism $\kappa_n : A(K)/p^n A(K) \to H^1(G_K, A[p^n](\bar{K}))$.

Exercise 2.2. When $A = \mathbb{G}_m$, show that κ_n is surjective.

This quick and easy construction of κ_n is not very explicit. Let us give a **second**, more down-to-earth, **construction** of that morphism. Let x be in $A(K)$. Since $p^n : A(\bar{K}) \to A(\bar{K})$ is surjective, there exists $y \in A(\bar{K})$ such that $p^n y = x$. Let us choose such a y, and define $c_y(g) := g(y) - y$ for all $g \in G_K$. We have $p^n c_y(g) = p^n(g(y) - y) = g(p^n y) - p^n y = g(x) - x = 0$, so $c_y(g) \in A[p^n](\bar{K})$. It is readily seen that the map $g \mapsto c_y(g)$ is a 1-cocycle from G_K to $A[p^n](\bar{K})$. This map therefore has a class $\bar{c}_y$ in $H^1(G_K, A[p^n](\bar{K}))$. We claim that this class does not depend on the choice of y, but depends only on x. For if y_0 is another

element of $A(\bar{K})$ such that $p^n y_0 = x$, we have $z = y - y_0 \in A[p^n](\bar{K})$, and $c_y(g) = c_{y_0} + g(z) - z$ which shows that c_y and c_{y_0} only differs by a coboundary, hence have the same class in $H^1(G_K, A[p^n](\bar{K}))$. We thus have defined a map $x \mapsto \bar{c}_y$, $A(K) \to H^1(G_K, A[p^n](\bar{K}))$. This map is a morphism of groups, for if x and x' are in $A(K)$ and y and y' are any elements in $A(\bar{K})$ such that $p^n y = x$ and $p^n y' = x'$, our map sends $x - x'$ to $\bar{c}_{y-y'}$ which is the same as $\bar{c}_y - \bar{c}_{y'}$ since $c_{y-y'}(g) = g(y - y') - (y - y') = g(y) - y - (g(y') - y') = c_y(g) - c_{y'}(g)$. And finally, our map sends $p^n A(K)$ to 0, since for $x \in p^n A(K)$ one can take $y \in A(K)$ and $c_y = g(y) - y$ is already 0 for all g. Therefore, we have a map $A(K)/p^n A(K) \to H^1(G_K, A[p^n](\bar{K}))$. This map is the same map as the map κ_n constructed above.

Exercise 2.3. Look up in some text on group cohomology (e.g. Serre, local fields) an explicit construction of the connecting homomorphism δ to check the last assertion.

We shall now give a **third construction of** κ_n, which is actually a more conceptual but still very concrete formulation of the second one. It will be fundamental in certain proofs below. Assume for simplicity that K is perfect. Let again $x \in A(K)$. Instead of choosing a y such that $p^n y = x$, we consider the set of all such y, or more precisely, we consider the fiber $T_{n,x}$ at x of the map $[p^n]$. This is a finite subscheme of A; obviously this is not a group scheme, but there is an algebraic action of the commutative group scheme $A[p^n]$ on $T_{n,x}$ (that is a morphism of K-schemes $A[p^n] \times T_{n,x} \to T_{n,x}$ which on R-points is a group action of the group $A[p^n](R)$ on the set $T_{n,x}(R)$ for all K-algebras R): the map that sends (z, y) to $z + y$. Over $\bar{K}$, this action (of $A[p^n](\bar{K})$ on $T_{n,x}(\bar{K})$) is obviously simply transitive, or in other words, $T_{n,x}$ is isomorphic (over $\bar{K}$, as a scheme with $A[p^n]$-action) to $A[p^n]$ itself with its right translation action. This implies (technically since $\mathrm{Spec}\, \bar{K}$ is an étale cover of $\mathrm{Spec}\, K$) that $T_{n,x}$ is what we call *a K-torsor under $A[p^n]$*, locally trivial for the étale (or Galois) topology. As part of the general principle that objects that are locally (for some Grothendieck topology) isomorphic to some trivial object are classified by the H^1 (on the same topology) of the automorphism group sheaf of the corresponding trivial object, such torsors are classified by the $H^1_{\text{ét}}(\mathrm{Spec}\, K, A[p^n]) = H^1(G_K, A[p^n](\bar{K}))$. In particular, our torsor $T_{n,x}$ defines an element of $H^1(G_K, A[p^n](\bar{K}))$ – this is $\kappa_n(x)$.

Finally, we construct a map κ form the κ_n's. There is a small technical difficulty due to the fact that G_K might not satisfy $\mathrm{Fin}(p)$.

Let G be a quotient of G_K through which the action on $V_p(A)$ factors, and such that the image of κ_n lies in $H^1(G, A[p^n](\bar{K})) \subset H^1(G_K, A[p^n](\bar{K}))$. Assume that G satisfies $\mathrm{Fin}(p)$. (If K is a characteristic 0 local field, one can simply take $G = G_K$. If K is a number field, it will be possible in practice to take $G = G_{K,\Sigma}$ for a suitable finite set of places Σ).

It is clear that the injective maps

$$\kappa_n : A(K)/p^n A(K) = A(K) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \to H^1(G_K, A[p^n]) \to H^1(G, A[p^n](\bar{K}))$$

for various n are compatible, so they define a map

$$\varprojlim A(K) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \to \varprojlim H^1(G, A[p^n](K)).$$

The LHS is the p-adic completion of $A(K)$, that we shall denote $\widehat{A(K)}$. There is a natural map from $A(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ to $\widehat{A(K)}$ which is an isomorphism if $A(K)$ is finitely generated. The RHS is by Prop. 2.1 $H^1(G, T_p(A))$. Tensorizing by $\mathbb{Q}_p$, we finally get an injective map

$$\kappa : \widehat{A(K)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G, V_p(A)).$$

Exercise 2.4. Let K be a finite extension of $\mathbb{Q}_l$ (with l a prime number equal or different from p), $G = G_K$, $A = \mathbb{G}_m$. Show that the above map $\kappa : \widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G_K, \mathbb{Q}_p(1))$ is an isomorphism.

2.1.3. *Results in local Galois cohomology.* Let K be a finite extension of $\mathbb{Q}_l$, and V be a p-adic representation of G_K. From the standard results of Tate for Galois cohomology with finite coefficients, we deduce using Prop. 2.1

Proposition 2.2.
(Cohomological Dimension) $H^i(G_K, V) = 0$ *if* $i > 2$.
(Duality) *We have a canonical isomorphism* $H^2(G_K, \mathbb{Q}_p(1)) = \mathbb{Q}_p$ *and the pairing* $H^i(G_K, V) \times H^{2-i}(G_K, V^*(1)) \to H^2(G_K, \mathbb{Q}_p(1)) = \mathbb{Q}_p$ *given by the cup-product is a perfect pairing for* $i = 0, 1, 2$
(Euler-Poincaré) $\dim H^0(G_K, V) - \dim H^1(G_K, V) + \dim H^2(G_K, V)$ *is* 0 *if* $l \neq p$ *and* $[K : \mathbb{Q}_p] \dim V$ *if* $l = p$.

Exercise 2.5. Prove those results using Prop. 2.1 and the results in any book of Galois cohomology.

The importance of this theorem is that in practice one can very easily compute the dimension of any $H^i(G_K, V)$. For $\dim H^0(G_K, V) = \dim V^{G_K}$ is simply the multiplicity of the trivial representation $\mathbb{Q}_p$ as a sub-representation of V; $\dim H^2(G_K, V) = \dim H^0(G_K, V^*(1))$ (by duality) is simply the multiplicity of the cyclotomic character $\mathbb{Q}_p(1)$ as a quotient of V. And $\dim H^1(G_K, V)$ can then be computed using the Euler-Poincaré formula. Actually, the result for $\dim H^1(G_K, V)$ is easy to remember, and worth remembering : it is 0 or $[K : \mathbb{Q}] \dim V$, plus the number of times $\mathbb{Q}_p$ appears as a sub-representation and $\mathbb{Q}_p(1)$ appears as a quotient in V, so most of the time, it is simply 0 or $[K : \mathbb{Q}] \dim V$ (according to whether $l \neq p$ or $l = p$).

Exercise 2.6. (easy) Let V be an absolutely irreducible representation of $G_{\mathbb{Q}_p}$ of dimension d. What is the dimension of $H^1(G_{\mathbb{Q}_p}, \mathrm{ad}V)$?

Exercise 2.7. What is the dimension of $H^1(G_K, \mathbb{Q}_p(1))$? of $\widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$? (Recall that $\widehat{A}$ is the p-adic completion of the abelian group A.) Compare with Exercise 2.4.

2.1.4. *The unramified H^1.* Same notations as in the preceding §.

Definition 2.1. The *unramified H^1* is $H^1_{ur}(G_K, V) = \ker(H^1(G_K, V) \to H^1(I_K, V))$

Proposition 2.3.   (a) *We have* $\dim H^1_{ur}(G_K, V) = \dim H^0(G_K, V)$.
   (b) *An element of $H^1(G_K, V)$ that corresponds to an extension $0 \to V \to W \to \mathbb{Q}_p \to 0$ is in $H^1_{ur}(G_K, V)$ if and only if the sequence $0 \to V^{I_K} \to W^{I_K} \to \mathbb{Q}_p \to 0$ is still exact.*
   (c) *Assume $l \neq p$. Then for the duality betwen $H^1(G_K, V)$ and $H^1(G_K, V^*(1))$, the orthogonal of $H^1_{ur}(G_K, V)$ is $H^1_{ur}(G_K, V^*(1))$.*

Proof —   By the inflation-restriction exact sequence, the inflation map

$$H^1(G_K/I_K, V^{I_K}) \to H^1_{ur}(G_K, V)$$

is an isomorphism. But $G_K/I_K \simeq \hat{\mathbb{Z}}$, and for any p-adic representation W of $\hat{\mathbb{Z}}$, we have $\dim H^0(\hat{\mathbb{Z}}, W) = \dim H^1(\hat{\mathbb{Z}}, W)$ (and $\dim H^i(\hat{\mathbb{Z}}, W) = 0$ if $i > 1$): this is well-known is W is finite and the case of p-adic representations W follows using Prop. 2.1 . Therefore, $\dim H^1_{ur}(G_K, V) = \dim H^0(G_K/I_K, V^{I_K}) = \dim H^0(G_K, V)$. This proves (a).

For a short exact sequence of representation of I_K: $0 \to V \to W \to \mathbb{Q}_p \to 0$ we have a long exact sequence $0 \to V^{I_K} \to W^{I_K} \to \mathbb{Q}_p \xrightarrow{\delta} H^1(I_K, V)$ and by the construction of the connecting morphism δ, the image of δ is the line generated by the element of $H^1(I_K, V)$ corresponding to that extension. The assertion (b) follows immediately.

For (c) we note that the image of $H^1_{ur}(G_K, V) \otimes H^1_{ur}(G_K, V^*(1))$ in $H^2(G_K, \mathbb{Q}_p(1))$ is 0 since it lies (using the fact that inflation maps are isomorphisms as in the proof of (a)) in $H^2(G_K/I_K, \mathbb{Q}_p(1)) = 0$ (as seen in (a)). Assume $l \neq p$. We only have to show that $\dim H^1_{ur}(G_K, V) + \dim H^1_{ur}(G_K, V^*(1)) = \dim H^1(G_K, V)$. But by (a), the LHS is $\dim H^0(G_K, V) + \dim H^0(G_K, V^*(1)) = \dim H^0(G_K, V) + \dim H^2(G_K, V)$ using the duality. But this is exactly the dimension of the RHS, by the Euler-Poincaré characteristic formula since $l \neq p$.   □

Exercise 2.8. (easy) Assume $l \neq p$. Show that the only irreducible representation of G_K such that $H^1_{ur}(G_K, V) \neq H^1(G_K, V)$ is $V = \mathbb{Q}_p(1)$. Show that in this case $H^1_{ur}(G_K, V) = 0$,

As suggested by the above exercise, the case of the representation $\mathbb{Q}_p(1)$ is quite special, and we study it in details. Remember (see §2.1.2 and exercise 2.4) that the Kummer map is an isomorphism $\kappa : \widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G_K, \mathbb{Q}_p(1))$.

Proposition 2.4. *Assume $p \neq l$. The isomorphism κ identifies the subspace $\widehat{\mathcal{O}_K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of $\widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with the subspace $H_{ur}^1(G_K, \mathbb{Q}_p(1))$ of $H^1(G_K, \mathbb{Q}_p(1))$*

Proof — Indeed, both subspaces have dimension 0.   □

Remark 2.2. This trivial result is the shadow in characteristic 0 of a non-trivial (and important) result with torsion coefficients, that we know describe. Define

$$H_{\mathrm{ur}}^1(G_K, \mu_{p^n}(\bar{K})) = \ker(H^1(G_K, \mu_{p^n}(\bar{K})) \to H^1(I_K, \mu_{p^n}(\bar{K}))).$$

Here $\mu_{p^n} = \mathbb{G}_m[p^n]$ denotes as usual the group scheme of p^n-root of 1). We have an isomorphism $\mu_{p^n} = \mathbb{Z}/p^n\mathbb{Z}(1)$ of G_K-modules. The afore-mentionned result is that κ_n maps $\mathcal{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}$ into $H_{\mathrm{ur}}^1(G_K, \mu_{p^n}(\bar{K}))$.

For pedagogical reasons, as we shall need later to do a more complicated proof along the same lines, we make an exception to our rule of limiting ourselves to characteristic 0 result and we prove this fact.

Let x in $\mathcal{O}_K^*$, and $y \in \bar{K}^*$ such that $y^{p^n} = x$. The extension $K(y)/K$ is unramified, since the polynomial $Y^{p^n} - x$ has no multiple roots in the residue field k of K (since its derivative is $p^n Y^{p^n-1}$ has only the root 0 of k (remember that $p \neq l$) and 0 is not a root of $Y^{p^n} - \bar{x}$ since $x \in \mathcal{O}_K^*$). Therefore, for all $g \in I_K$, $g(y)/y = 1$, and the cocycle $\kappa_n(x)$ is trivial on I_K.

In the proof above, we have used the second construction of κ_n given in §2.1.2. We could also have used the third. The end of the proof would have been: Let $x \in \mathcal{O}_K^*$. The μ_{p^n}-torsor $T_{n,x}$ over K is the generic fiber of a μ_{p^n}-torsor $\mathcal{T}_{n,x}$ over $\mathcal{O}_K$ (defined by the equation $Y^{p^n} = x$.). This torsor is étale over $\mathrm{Spec}\,\mathcal{O}_K$, hence locally trivial for the étale topology of $\mathrm{Spec}\,\mathcal{O}_K$, therefore the class $\kappa_n(x)$ of $T_{n,x}$ in $H_{\text{ét}}^1(\mathrm{Spec}\,K, \mu_{p^n}) = H^1(G_K, \mu_{p^n})$ lies in $H_{\text{ét}}^1(\mathcal{O}_K, \mu_{p^n}) = H^1(G_K/I_K, \mu_{p^n})$. QED.

Exercise 2.9. Assume $l \neq p$, and let E be an elliptic curve over K. Define

$$H_{\mathrm{ur}}^1(G_K, E[p^n](\bar{K})) = \ker(H^1(G_K, E[p^n](\bar{K})) \to H^1(I_K, E[p^n](\bar{K}))).$$

a.– Assuming that E has good reduction, show by mimicking the proof in the above remark that κ_n maps $E(K)/p^n E(K)$ into $H_{\mathrm{ur}}^1(G_K, E[p^n](\bar{K}))$.

b.– **(difficult)** Prove the same result in the case of bad reduction.

Exercise 2.10. Assume $l \neq p$. Let E be an elliptic curve over K, and $V_p(E)$ be its Tate module. Show that $H^1(G_K, V_p(E)) = 0$. (Here is one possible method: show first that $H_{\mathrm{ur}}^1(G_K, V_p(E)) = 0$ using (a) of Prop. 2.3. Then use (c) of that proposition to conclude, using that $V_p(E) \simeq V_p(E)^*(1)$.)

2.1.5. *Results in Global Galois cohomology, and Selmer groups.* Let K be a number field and p be a prime number. In what follows, Σ will always denote a finite set of primes of K containing all primes above p and ∞. For v a place of K, we recall that we denote by G_v the absolute Galois group of the completion K_v of K at v. Let V be a p-adic representation of $G_{K,\Sigma}$, that is a representation of G_K that is unramified at all prime not in Σ.

For global Galois cohomology we still have a simple Euler-Poincaré formula:

Proposition 2.5.

$$\dim H^0(G_{K,\Sigma}, V) - \dim H^1(G_{K,\Sigma}, V) + \dim H^2(G_{K,\Sigma}, V) =$$
$$\sum_{v|\infty} H^0(G_v, V) - [K : \mathbb{Q}] \dim V.$$

Exercise 2.11. (easy) Let V be an irreducible representation of dimension 2 of $G_{\mathbb{Q},\Sigma}$. Show that $\dim H^1(\mathbb{G}_{\mathbb{Q},\Sigma}, \mathrm{ad}V)$ is at least 3 if V is odd (that is, the complex conjugation acts with trace 0 on V), and at least 1 if V is even.

We also have an analog of local duality, but instead of one clear theorem it is a web of inter-related results known as Poitou-Tate (e.g. Poitou-Tate duality, the nine-term Poitou-Tate exact sequence, etc.). Those results do not relate the dimension of $H^1(G_{K,\Sigma}, V)$ with the dimension of $H^1(G_{K,\Sigma}, V^*(1))$ but rather with the dimension of a space of more general type (a *Selmer group*), which is the subspace of $H^1(G_{K,\Sigma}, V)$ of elements whose local restrictions at places $v \in \Sigma$ are 0. Moreover, those results do not give us any easy way to compute $H^2(G_{K,\Sigma}, V)$ as in the local case – and indeed, even determining the dimension of $H^2(G_{K,\Sigma}, \mathbb{Q}_p)$ is still an open problem for most number fields K (see §5 below). The bottom line is that in general the Euler-Poincaré formula gives us a lower bound for H^1 but that in general we do not know if this lower bound is an equality. In exercise 2.11 for example, if V is geometric, it is conjectured that the lower bounds 3 and 1 are equality, but this is not known in general.

We shall not expose here all the results belonging to the Poitou-Tate world. We refer the reader to the literature for that (see e.g. [Mi] or [CNF].) We shall content ourselves with two results. The first one is easily stated.

Proposition 2.6. *Let $i = 0, 1, 2$. In the duality between $\prod_{v \in \Sigma} H^i(G_v, V)$ and $\prod_{v \in \Sigma} H^i(G_v, V^*(1))$, the images of $H^1(G_{K,\Sigma}, V)$ and the image of $H^1(G_{K,\Sigma}, V^*(1))$ are orthogonal of each other.*

To explain the second one, we need to introduce the general notion of Selmer groups.

Definition 2.2. Let V be a p-adic representation of G_K unramified almost everywhere. A *Selmer structure* $\mathcal{L} = (L_v)$ for V is the data of a family of subspaces L_v of $H^1(G_v, V)$ for all finite places v of K such that for almost all v, $L_v = H^1_{\mathrm{ur}}(G_v, V)$.

Definition 2.3. The *Selmer group* attached to $\mathcal{L}$ is the subspace $H^1_{\mathcal{L}}(G_K, V)$ of elements $x \in H^1(G_K, V)$ such that for all finite places v, the restriction x_v if x to $H^1(G_v, V)$ is in L_v. In other words,

$$H^1_{\mathcal{L}}(G_K, V) = \ker \left(H^1(G_K, V) \to \prod_{v \text{ finite place of } K} H^1(G_v, V)/L_v. \right)$$

Exercise 2.12. If $\mathcal{L}$ is a Selmer structure, there is a finite set Σ of primes of K containing the places above p, and such that for all finite place $v \notin \Sigma$, $\mathcal{L}_v = H^1_{\mathrm{ur}}(G_v, V)$. Show that $H^1_{\mathcal{L}}(G_K, V) = \ker \left(H^1(G_{K,\Sigma}, V) \to \prod_{v \in \Sigma} H^1(G_v, V)/L_v \right)$. In particular, $H^1_{\mathcal{L}}(G_K, V)$ is finite dimensional.

When v is finite, the most obvious choices for a component L_v of a Selmer structure are (0), $H^1(G_v, V)$ and of course $H^1_{\mathrm{ur}}(G_v, V)$. When v is prime to p, those are the only L_v than one meets in practice. For v dividing p, Bloch and Kato have introduced other very important L_v: see next §. When v is infinite, $H^1(G_v, V) = 0$ so the only possibility is $L_v = 0$.

Definition 2.4. If $\mathcal{L}$ is a Selmer structure for V, we define a Selmer structure $\mathcal{L}^{\perp}$ for $V^*(1)$ by taking for $L_v^{\perp}$ the orthogonal of L_v in $H^1(G_v, V^*(1))$.

Exercise 2.13. (easy) Why is $\mathcal{L}^{\perp}$ a Selmer structure?

We can now state the second duality result:

Proposition 2.7.

$$\begin{aligned}
\dim H^1_{\mathcal{L}}(G_K, V) = \ & \dim H^1_{\mathcal{L}^{\perp}}(G_K, V^*(1)) \\
& + \dim H^0(G_K, V) - \dim H^0(G_K, V^*(1)) \\
& + \sum_{v \text{ place of } K \text{ (finite or not)}} \dim L_v - \dim H^0(G_v, V)
\end{aligned}$$

This formula, or rather its analog for finite coefficients, a consequence of the Poitou-Tate machinery, appeared first (for finite coefficients) in the work of Greenberg, and gained immediate notoriety when it was used in Wiles' work on the Taniyama-Shimura-Weil conjecture.

Exercise 2.14. Applying the Prop. 2.7 for $V^*(1)$ instead of V, we get another formula. Show that it is equivalent to the first one.

Exercise 2.15. Using Prop. 2.7, find a lower bound for the dimension of $H^1(G_{K,\Sigma}, V)$. Compare it with the lower bound you can get using the Euler-Poincaré characteristic formula.

2.2. **The local Bloch-Kato Selmer groups at places dividing p.** In all this §, K is a finite extension of $\mathbb{Q}_p$.

2.2.1. *The local Bloch and Kato's H_f^1.* If V a p-adic representation of G_K, we are looking for a subspace L of $H^1(G_K, V)$ which is the analog of the subspace $H^1_{\mathrm{ur}}(G_{K'}, V)$ of $H^1(G_{K'}, V)$ where K' is a finite extension of $\mathbb{Q}_l$ and V a p-adic representation, $p \neq l$.

The naive answer ($L = H^1_{\mathrm{ur}}(G_K, V)$) is not satisfying. For one thing, we know that the p-adic analog of the l-adic notion of being *unramified* is not *unramified* but *crystalline*. Moreover, the subspace $H^1_{\mathrm{ur}}(G_K, V)$ is not the orthogonal of the subspace $H^1_{\mathrm{ur}}(G_K, V^*(1))$ when the residual characteristic of K is p: their dimensions do not add up to $\dim H^1(G_K, V) = \dim H^1(G_K, V^*(1))$ but is smaller (by (a) of Prop. 2.3 and the local Euler-Poincaré characteristic formula).

The right answer has been found by Bloch and Kato ([BK])

Definition 2.5. We set $H_f^1(G_K, V) = \ker(H^1(G_K, V) \to H^1(G_K, V \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}))$.

We have a very concrete alternative description of the H_f^1.

Lemma 2.5. *An element of $H^1(G_K, V)$ that corresponds to an extension $0 \to V \to W \to \mathbb{Q}_p \to 0$ is in $H_f^1(G_K, V)$ if and only if the sequence $0 \to D_{crys}(V) \to D_{crys}(W) \to D_{crys}(\mathbb{Q}_p) \to 0$ is still exact. In particular, if V is crystalline, then the extension W is in $H_f^1(G_K, V)$ if and only if it is crystalline.*

Proof — The proof is exactly the same as the one of (b) of Prop. 2.3. $\qquad\square$

When V is de Rham (which is the only case of interest), it is easy to compute the dimension of the (local) H_f^1.

Proposition 2.8. *Assume that V is de Rham. Let $D_{dR}^+(V) = (V \otimes B_{dR}^+)^{G_K} \subset D_{dR}(V) = (V \otimes B_{dR})^{G_K}$. Then we have*

$$\dim_{\mathbb{Q}_p} H_f^1(G_K, V) = \dim_{\mathbb{Q}_p}(D_{dR}(V)/D_{dR}^+(V)) + \dim_{\mathbb{Q}_p} H^0(G_K, V).$$

Note that $D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}^+(V)$ is a K-vector space. We insist that the formula involves its dimension over $\mathbb{Q}_p$, that is $[K : \mathbb{Q}_p]$ times its dimension over K.

Proof — We use the exact sequence (see [Co])

$$0 \to \mathbb{Q}_p \xrightarrow{\alpha} B_{\mathrm{crys}} \oplus B_{\mathrm{dR}}^+ \xrightarrow{\beta} B_{\mathrm{crys}} \oplus B_{\mathrm{dR}} \to 0$$

with $\alpha(x) = (x, x)$ and $\beta(y, z) = (y - \phi(y), y - z)$ where ϕ is the Frobenius on B_{crys}. Tensorizing it by V and taking the long exact sequence, we get

$$0 \to H^0(G_K, V) \xrightarrow{\alpha} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}^+(V) \xrightarrow{\beta} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}(V)$$

(5)
$$\to H^1(G_K, V) \xrightarrow{\alpha_1} H^1(G_K, V \otimes B_{\mathrm{crys}}) \oplus H^1(G_K, V \otimes B_{\mathrm{dR}}^+)$$

$$\xrightarrow{\beta_1} H^1(G_K, V \otimes B_{\mathrm{crys}}) \oplus H^1(G_K, V \otimes B_{\mathrm{dR}}),$$

with $\alpha_1(x) = (x_c, x_d)$ where x_c (resp. x_d) is the image of x by the map $H^1(G_K, V) \to H^1(G_K, V \otimes B_{\mathrm{crys}})$ (resp. $H^1(G_K, V) \to H^1(G_K, V \otimes B_{\mathrm{dR}}^+)$), and $\beta_1(y, z) =$

$(y - \phi(y), y' - z'')$ where y' is the image of y by the map induced by the inclusion $B_{\mathrm{crys}} \subset B_{\mathrm{dR}}$ and z'' is the image of z by the map induced by the inclusion $B_{\mathrm{dR}}^+ \subset B_{\mathrm{dR}}$.

We claim that $\ker \alpha_1 = \ker(H^1(G_K, V) \overset{x \mapsto x_c}{\to} H^1(G_K, V \otimes B_{\mathrm{crys}}))$. The inclusion $\subset$ is clear, so let us prove the other, and consider an $x \in H^1(G_K, V)$ such that $x_c = 0$. Since $(x_c, x_d) \in \operatorname{Im} \alpha_1 = \ker \beta_1$, we have $(x_c)' - (x_d)'' = 0$ so $(x_d)'' = 0$, but the map $z \mapsto z''$ is injective by the Lemma below, so we have $x_d = 0$, so $\alpha_1(x) = (0,0)$ which proves the claim.

Now we observe that the claim exactly says that $\ker \alpha_1 = H_f^1(G_K, V)$. The exact sequence (5) thus becomes

(6)
$$0 \to H^0(G_K, V) \overset{\alpha}{\to} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}^+(V)$$
$$\overset{\beta}{\to} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}(V) \to H_f^1(G_K, V) \to 0.$$

Since the alternate sum of the dimension of the spaces in an exact sequence is 0, we get the result. $\qquad\square$

Lemma 2.6. *The natural map* $z \mapsto z''$, $H^1(G_K, V \otimes B_{dR}^+) \to H^1(V \otimes B_{dR})$ *is injective.*

Proof —   By the long exact sequence attached to the short exact sequence $0 \to B_{\mathrm{dR}}^+ \to B_{\mathrm{dR}} \to B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0$ tensor V, we only have to prove that the sequence

$$0 \to D_{\mathrm{dR}}^+(V) \to D_{\mathrm{dR}}(V) \to (V \otimes B_{\mathrm{dR}}/B_{\mathrm{dR}}^+)^{G_K} \to 0,$$

which is exact at $D_{\mathrm{dR}}^+(V)$ and $D_{\mathrm{dR}}(V)$, is exact. It suffices to show that

$$\dim_K D_{\mathrm{dR}}(V) \geq \dim_K D_{\mathrm{dR}}^+(V) + \dim_K(V \otimes B_{\mathrm{dR}}/B_{\mathrm{dR}}^+)^{G_K}.$$

But using that $t^i B_{\mathrm{dR}}/t^{i+1} B_{\mathrm{dR}} \simeq \mathbb{C}_p(i)$, we get that $\dim_K D_{\mathrm{dR}}^+(V) \leq \sum_{i \geq 0} \dim(V \otimes \mathbb{C}_p(i))$, and $\dim_K(V \otimes B_{\mathrm{dR}}/B_{\mathrm{dR}}^+)^{G_K} \leq \sum_{i < 0} \dim(V \otimes \mathbb{C}_p(i))$, so $\dim_K D_{\mathrm{dR}}^+(V) + \dim_K(V \otimes B_{\mathrm{dR}}/B_{\mathrm{dR}}^+)^{G_K} \leq \sum_{i \in \mathbb{Z}} \dim(V \otimes \mathbb{C}_p(i))^{G_K}$ which is known by a result of Tate to be less that $\dim V = \dim_K D_{\mathrm{dR}}(V)$. $\qquad\square$

Exercise 2.16. With the same kind of ideas as in the Lemma, one can prove that for any de Rham representation V, $\dim_K D_{\mathrm{dR}}^+(V) + \dim_K D_{\mathrm{dR}}^+(V^*(1)) = \dim_{\mathbb{Q}_p} V$. Do it.

As for the local cohomology group, the formula for the dimension of the H_f^1 is simple and worth remembering. If $H^0(G_K, V) = 0$, then $\dim H_f^1(G_K, V)$ is $[K : \mathbb{Q}_p]$ times the number of negative Hodge-Tate weights of V.

Exercise 2.17. (easy) Show that if V is de Rham with all its Hodge-Tate weights positive, then $H_f^1(G_K, V)$ is 0. Show that V is de Rham with all its Hodge-Tate weights ≤ -2, then $H_f^1(G_K, V) = H^1(G_K, V)$.

Exercise 2.18. Compute $H^1_f(G_K, \mathbb{Q}_p(n))$ for all n. In particular, show that $H^1_f(G_K, \mathbb{Q}_p)$ is a line in $H^1(G_K, \mathbb{Q}_p) = \mathrm{Hom}_{\mathrm{cont}}(K^*, \mathbb{Q}_p)$ which has dimension $[K : \mathbb{Q}] + 1$. Show that this line is generated by the map $x \mapsto v_p(x)$, where v_p is the p-adic valuation on K.

Exercise 2.19. Show that $H^1_{\mathrm{ur}}(G_K, V) \subset H^1_f(G_K, V)$. When do we have equality?

The first strong indication that $H^1_f(G_K, V)$ is a good analog in the p-adic case of $H^1_{\mathrm{ur}}(G_K, V)$ in the l-adic case is the following theorem of Bloch and Kato.

Theorem 2.1. *Assume that V is de Rham. Then for the duality between $H^1(G_K, V)$ and $H^1(G_K, V^*(1))$, the orthogonal of $H^1_f(G_K, V)$ is $H^1_f(G_K, V^*(1))$.*

Proof — We first notice that by Prop. 2.8, the dimension of $H^1_f(G_K, V)$ and $H^1_f(G_K, V^*(1))$ add up to

$$\dim H^0(G_K, V) + \dim H^0(G_K, V^*(1))$$

$$+ \dim D_{\mathrm{dR}}(V)/D^+_{\mathrm{dR}}(V) + \dim D_{\mathrm{dR}}(V^*(1))/D_{\mathrm{dR}}(V^*(1)),$$

that is using exercise 2.16 to

$$\dim H^0(G_K, V) + \dim H^0(G_K, V^*(1)) + [K : \mathbb{Q}_p] \dim V,$$

which is $\dim H^1(G_K, V)$ by the Euler characteristic formula.

Therefore, we only have to prove that the restriction of the cup product

$$H^1(G_K, V) \otimes H^1(G_K, V^*(1)) \to H^2(G_K, \mathbb{Q}_p(1)) = \mathbb{Q}_p$$

to $H^1_f(G_K, V) \otimes H^1_f(G_K, V^*(1)$ is 0. Let x be an element in $H^1_f(G_K, V^*)$, and let us denote by $\cup x$ the cup-products by x (from $H^i(G_K, W)$ to $H^{i+1}(G_K, W \otimes V^*(1))$ where i is any integer and W any space with a continuous G_K-action.) The crucial fact we shall use (a well-known fact of group cohomology) is the compatibility of $\cup x$ with the connecting homomorphisms in a long exact sequence of cohomology attached to a short exact sequence. This fact is used to guarantee the commutativity of the diagram below:

$$
\begin{array}{ccc}
D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}(V) = H^0(G_K, V \otimes B_{\mathrm{crys}} \oplus V \otimes B_{\mathrm{dR}}) & \longrightarrow & H^1(G_K, V) \\
\downarrow {\scriptstyle \cup x} & & \downarrow {\scriptstyle \cup x} \\
H^1(G_K, V \otimes V^*(1) \otimes B_{\mathrm{crys}} \oplus V \otimes V^*(1) \otimes B_{\mathrm{dR}}) & \longrightarrow & H^2(G_K, V \otimes V^*(1))
\end{array}
$$

where the first line is a part of the long exact sequence (5) and the second line is another part of the same exact sequence but with V replaced by $V \otimes V^*(1)$. The first vertical map $\cup x$ obviously depends only on the image of x in $H^1(G_K, V^*(1) \otimes B_{\mathrm{crys}})$, so it is 0 when $x \in H^1_f(G_K, V^*(1))$. Therefore, the second vertical map $\cup x$ is 0 on the image of the first horizontal map when $x \in H^1_f(G_K, V^*(1))$. But by (6), this image is precisely $H^1_f(G_K, V)$. This proves that the cup-product is 0 on $H^1_f(G_K, V) \otimes H^1_f(G_K, V^*(1))$, hence the theorem. $\qquad \square$

Another indication of the analogy between H_f^1 (when $l = p$) and H_{ur}^1 (when $l \neq p$) is the following:

Proposition 2.9. *The Kummer map* $\kappa : \widehat{K^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G_K, \mathbb{Q}_p(1))$ *identifies* $\mathcal{O}_K^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ *with* $H_f^1(G_K, \mathbb{Q}_p(1))$

Proof — Recall that $\widehat{A}$ is the p-adic completion of A. Since $\mathcal{O}_K^*$ is already p-adically complete, $\widehat{\mathcal{O}_K^*} = \mathcal{O}_K^*$ is a subgroup of $\widehat{K^*}$.

By Prop. 2.8, $\dim H_f^1(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p]$. Since the logarithm defines an isomorphism between an open (therefore finite index) subgroup of $(\mathcal{O}_K^*, \times)$ and an open subgroup of $(\mathcal{O}_K, +)$, and since such a subgroup is isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$, we also have $\dim \mathcal{O}_K^* \otimes \mathbb{Q}_p = [K : \mathbb{Q}]$. Since κ is injective, we only have to prove that $\kappa(\mathcal{O}_K^*) \subset H_f^1(G_K, \mathbb{Q}_p(1))$. To do so, we use the third construction of κ (see §2.1.2): for $x \in \mathcal{O}_K^*$, we call $T_{n,x}$ the K-subscheme of $\mathbb{G}_m$ defined by the equation $Y^{p^n} - x = 0$, which is a torsor over μ_{p^n}. The torsor $T_{n,x}$ has a natural model $\mathcal{T}_{n,x}$ over $\mathcal{O}_K$, defined over the same equation, which is not finite étale, but at least finite and faithfully flat over $\mathcal{O}_K$, and is a torsor over the finite faithfully flat group scheme $(\mu_{p^n})_{\mathcal{O}_K}$ over $\mathcal{O}_K$.

The torsor $\mathcal{T}_{n,x}$ defines an extension in the category of finite faithfully flat group schemes killed by p^n over $\mathcal{O}_K$,

$$0 \to (\mu_{p_n})_{\mathcal{O}_K} \to \mathcal{E}_{n,x} \to (\mathbb{Z}/p^n\mathbb{Z})_{\mathcal{O}_K} \to 0$$

where $(\mathbb{Z}/p^n\mathbb{Z})_{\mathcal{O}_K}$ is the constant group scheme $\mathbb{Z}/p^n\mathbb{Z}$: the extension $\mathcal{E}_{n,x}$ is the one defined by the class of $\mathcal{T}_{n,x}$ in $H_{\mathrm{fppf}}^1(\mathrm{Spec}\,\mathcal{O}_K, (\mu_{p^n})_{\mathcal{O}_K}) = \mathrm{Ext}_{\mathrm{fppf}}^1(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$. Taking the generic fiber, we also get an extension $E_{n,x}$ of $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n} in the category of finite group schemes killed by p^n over K, whose class is the class of $T_{n,x}$ in $H_{\mathrm{fppf}}^1(\mathrm{Spec}\,K, \mu_n) = H_{\mathrm{ét}}^1(\mathrm{Spec}\,K, \mu_n) = H^1(G_K, \mu_n(\bar{K}))$, that is, by definition, the class $\kappa_n(x)$.

Now we let n vary. Of course the constructions are compatible for various n, and therefore the system $(E_{n,x})$ defines a p-divisible group E_x over K, whose attached Tate module is, by construction, the extension W of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$ defined by the class $\kappa(x)$. But this p-divisible group has good reduction over $\mathcal{O}_K$, since the p-divisible group $\mathcal{E}_x$ attached to the inductive system $(\mathcal{E}_{x,n})$ is a model of it. Therefore, by the theorem of Fontaine explained in one of Conrad's talk (see [Co]), the Tate module W of E is crystalline. This proves that $\kappa(x) \in H_f^1(G_K, \mathbb{Q}_p(1))$ by Lemma 2.5. $\square$

In the same spirit, we have the important:

Proposition 2.10. *Let E be an elliptic curve over K. The Kummer isomorphism κ for E is an isomorphism $E(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} H_f^1(G_K, V_p(E))$.*

Proof — For simplicity, we treat only the case where E has good reduction over $\mathcal{O}_K$. For the general case, see [BK, Example 3.10.1].

We begin by counting dimensions. The logarithm defines an isomorphism between an open finite-index subgroup of $E(K)$ and an open subgroup of the Lie algebra of E/K, which is K, so $E(K)$ is p-adically complete (which shows in passing that the Kummer map κ as indeed for source $E(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$) and we have $\dim E(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = [K : \mathbb{Q}_p]$. On the other hand $\dim H^1_f(G_K, V_p(E)) = [K : \mathbb{Q}_p]$ by Prop. 2.8. Since κ is injective, we only have to prove that for $x \in E(K)$, $\kappa(x) \in H^1_f(G_K, \mathbb{Q}_p(E))$. For this we consider as in the third construction of the Kummer homomorphism (see §2.1.2) the torsor $T_{n,x}$ (fiber of $[p^n] : E \to E$ at x over the finite group scheme $E[p^n]$, over K) and observe that this torsor has a finite, faithfully flat model $\mathcal{T}_{n,x}$ over $\mathcal{O}_K$: consider an elliptic scheme $\mathcal{E}$ (e.g. the Néron model of E, or more simply the model defined by a minimal Weierstrass equation) over $\mathcal{O}_K$ whose generic fiber is E, and define $\mathcal{T}_{n,x}$ again as the fiber at x of the faithfully flat morphism $[p^n] : \mathcal{E} \to \mathcal{E}$. The end of the proof is exactly the same as in the above proposition.   □

2.2.2. *The variants H^1_g and H^1_e.* We keep the same notations as above. Bloch and Kato define two variants of $H^1_f(G_K, V)$, one slightly smaller $H^1_e(G_K, V)$ and one slightly bigger $H^1(G_K, V)$. They are relatively useful, though not as much as the H^1_f.

They are defined as

$$H^1_g(G_K, V) = \ker(H^1(G_K, V) \to H^1(G_K, V \otimes B_{\mathrm{dR}}))$$
$$H^1_e(G_K, V) = \ker(H^1(G_K, V) \to H^1(G_K, V \otimes B^{\phi=1}_{\mathrm{crys}}))$$

Since $B^{\phi=1}_{\mathrm{crys}} \subset B_{\mathrm{crys}} \subset B_{\mathrm{dR}}$, we have

$$H^1_e(G_K, V) \subset H^1_f(G_K, V) \subset H^1_g(G_K, V).$$

Again we have a very concrete alternative description of the H^1_g and H^1_e

Lemma 2.7. *An element of $H^1(G_K, V)$ that corresponds to an extension $0 \to V \to W \to \mathbb{Q}_p \to 0$ is in $H^1_g(G_K, V)$ (resp. in $H^1_e(G_K, V)$) if and only if the sequence $0 \to D_{dR}(V) \to D_{dR}(W) \to D_{dR}(\mathbb{Q}_p) \to 0$ (resp. $0 \to D_{crys}(V)^{\phi=1} \to D_{crys}(W)^{\phi=1} \to D_{crys}(\mathbb{Q}_p) \to 0$) is still exact. In particular, if V is de Rham, then the extension W is in H^1_g if and only if it is de Rham*

Proof — The proof is exactly the same as the one of (b) of Prop. 2.3.   □

Exercise 2.20. a.– Using Fontaine's fundamental exact sequence (see [Co])

$$0 \to \mathbb{Q}_p \to B^{\phi=1}_{\mathrm{crys}} \to B_{\mathrm{dR}}/B^+_{\mathrm{dR}} \to 0,$$

show that there exists a natural **surjective** map

$$D_{\mathrm{dR}}(V)/D^+_{\mathrm{dR}}(V) \to H^1_e(G_K, V)$$

whose kernel is $D_{\mathrm{crys}}(V)^{\phi=1}/V^{G_K}$. This map is called the *Bloch-Kato exponential* (because, in the case where $V = V_p(A)$ for an abelian variety A over K, it can be identified with the (the tensorization with $\mathbb{Q}_p$ of) the exponential map from an open subgroup of the Lie algebra of A to $A(K)$.)

b.– Deduce that if V is de Rham,

$$\dim H_e^1(G_K, V) = \dim D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}^+(V) + \dim H^0(G_K, V) - \dim D_{\mathrm{crys}}(V)^{\phi=1}.$$

The "g" in H_g^1 stands for *geometric* since geometric representations are de Rham. The "e" in H_e^1 stands for "exponential". This explains the "f" in the H_f^1, as f is just between e and g in the alphabetic order. (Others believe that f stands for "fine".)

Proposition 2.11. *Assume that V is de Rham. For the pairing between $H^1(G_K, V)$ and $H^1(G_K, V^*(1))$, the orthogonal of $H_e^1(G_K, V)$ is $H_g^1(G_K, V^*(1))$ and the orthogonal of $H_g^1(G_K, V)$ is $H_e^1(G_K, V^*(1))$.*

Of course, it is sufficient to prove one of those assertions. For the proof of this result, that we shall not use, see [BK, page 357].

Exercise 2.21. Show that if V is de Rham, then $\dim H_g^1(G_K, V) = \dim D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}^+(V) + \dim H^0(G_K, V) + \dim D_{\mathrm{crys}}(V^*(1))^{\phi=1}$.

Exercise 2.22. Check that $\dim H_e^1(G_K, \mathbb{Q}_p)$, $\dim H_f^1(G_K, \mathbb{Q}_p)$, $\dim H_g^1(G_K, \mathbb{Q}_p)$, $\dim H^1(G_K, \mathbb{Q}_p)$ are respectively $0, 1, 1, 1 + [K : \mathbb{Q}_p]$.

Exercise 2.23. Compute $\dim H_e^1(G_K, \mathbb{Q}_p(n))$, $\dim H_f^1(G_K, \mathbb{Q}_p(n))$, $\dim H_g^1(G_K, \mathbb{Q}_p(n))$, $\dim H^1(G_K, \mathbb{Q}_p(n))$ for all integers n. The answers depends on n only through the conditions $n < 0$, $n = 0$, $n = 1$, $n > 1$, so you can put them in a 4×4-table that you can write in the space below. You can check your answer on [BK, Example 3.9].

Exercise 2.24. (difficult) Let E be an elliptic curve over K. Show that

$$H_e^1(G_K, V_p(E)) = H_f^1(G_K, V_p(E)) = H_g^1(G_K, V_p(E)).$$

Exercise 2.25. (difficult) Suppose that V is de Rham. Let $x \in H_f^1(G_K, V)$, corresponding to an extension W of $\mathbb{Q}_p$ by V. Let $\varphi = \phi^q$ where q is the degree of the residue field of K over $\mathbb{F}_p$, so that φ is a linear (not semi-linear) operator on $D_{\mathrm{crys}}(W)$. Show that $x \in H_e^1(G_K, V)$ if and only if ϕ acts like the identity on its generalized eigenspace ϕ of eigenvalue 1 in $D_{\mathrm{crys}}(W)$ (the generalized eigenspace is the set of $v \in D_{\mathrm{crys}}(W)$ such that $(\phi - 1)^n v = 0$ for some natural number n, and the assertion is that we can take $n = 1$ for each such v).

2.2.3. *Analogies.* For K a finite extension of $\mathbb{Q}_l$, and V a p-adic representation, we have three natural subspaces of $H^1(G_K, V)$ if $l \neq p$, and five if $l = p$.

case $l \neq p$ $(0) \quad \subset \ H^1_{\mathrm{ur}}(G_K, V) \subset \ H^1(G_K, V)$

case $l = p$ $(0) \subset H^1_e(G_K, V) \subset \ H^1_f(G_K, V) \ \subset H^1_g(G_K, V) \subset H^1(G_K, V)$

The correct analogies between the subspaces in the case $l \neq p$ and $l = p$ are given by the vertical alignment in the above table. That is, the correct analog of the full $H^1(G_K, V)$ (resp. of $H^1_{\mathrm{ur}}(G_K, V)$, resp. of (0)) in the case $l \neq p$ is, in the case $l = p$, the subspace $H^1_g(G_K, V)$ (resp. $H^1_f(G_K, V)$, resp. $H^1_e(G_K, V)$).

Of course, this is only an analogy, so it cannot be proved and one is allowed to disagree. But we have already strongly substantiated the analogy $H^1_{\mathrm{ur}} \ / \ H^1_f$. Let us motivate the analogies $(0) \ / \ H^1_e$ and $H^1 \ / \ H^1_g$. Of course, if we want our analogies to respect orthogonality, we only have to motivate one of them, say the analogy $H^1 \ / \ H^1_g$. Now look at the formula for $\dim H^1(G_K, V) - \dim H^1_{\mathrm{ur}}(G_K, V)$ if $l \neq p$, and compare it to the formula $\dim H^1_g(G_K, V) - \dim H^1_f(G_K, V)$ if $l = p$ (from Prop. 2.8 and Exercise 2.21). They look rather similar, don't they? While if you consider $\dim H^1(G_K, V) - \dim H^1_f(G_K, V)$ the formula is more complicated.

Another argument is as follows: if V is de Rham (in the case $l = p$), an element of $x \in H^1(G_K, V)$ represents an extension W of $\mathbb{Q}_p$ by V, and $x \in H^1_g$ means that W is de Rham (see Lemma 2.7), that is, by Berger's monodromy theorem, potentially semi-stable (in the p-adic sense). But if $l \neq p$, any representation W is potentially semi-stable by Grothendieck's monodromy theorem. So the analog of H^1_g is the full H^1.

This motivates the following notations.

Notation 2.1. If K is a finite extension of $\mathbb{Q}_l$ and V a p-adic representation of G_K, and $l \neq p$, we set $H^1_e(G_K, V) = 0$, $H^1_f(G_K, V) = H^1_{\mathrm{ur}}(G_K, V)$, and $H^1_g(G_K, V) = H^1(G_K, V)$.

Exercise 2.26. Let K is a finite extension of $\mathbb{Q}_l$ and V a p-adic representation of G_K, with $l \neq p$. Show that the analog of Exercise 2.25 holds, that is: if W is an extension of $\mathbb{Q}_p$ by V corresponding to an $x \in H^1_f(V)$, then $x \in H^1_e(G_K, V)$ (that is $x = 0$ by definition) if and only if Frob acts like the identity on its generalized eigenspace of eigenvalue 1.

2.3. **Global Bloch-Kato Selmer group.** In all this §, K is a number field, and V is a geometric p-adic representation of G_K.

2.3.1. *Definitions.*

Definitions 2.6. The global Bloch-Kato Selmer group $H^1_f(G_K, V)$ is the subspace of elements x of $H^1(G_K, V)$ such that for all finites place v of K, the restriction x_v of x belongs to $H^1_f(G_K, v)$.

More generally, if S is any finite set of finite places of K, we define $H^1_{f,S}(G_K, V)$ as the subspace of elements x of $H^1(G_K, V)$ such that for all finites place v of K, the restriction x_v of x belongs to $H^1_f(G_v, V)$ if $v \notin S$, and to $H^1_g(G_K, V)$ if $v \in S$.

Finally, we call $H^1_g(G_K, V)$ the union of all $H^1_{f,S}(G_K, V)$ when S runs among finite sets of primes of K. In other words, $H^1_g(G_K, V)$ is the subspace of elements x of $H^1(G_K, V)$ such that for all finite places v of K, the restriction x_v of x belongs to $H^1_g(G_v, V)$, and such that x_v belongs to $H^1_f(G_v, V)$ for all but a finite number of v.

Recall that by definition (see §2.2.3) $H^1_f(G_v, V)$ means $H^1_{ur}(G_v, V)$ and $H^1_g(G_v, V)$ means $H^1(G_v, V)$ when v does not divides p. Of course, $H^1_{f,\emptyset} = H^1_f$, and $H^1_{f,S} \subset H^1_{f,S'}$ if $S \subset S'$.

The Bloch-Kato Selmer group $H^1_f(G_K, V)$ is an instance of a Selmer group in the sense of Definition 2.2: it is the Selmer groups $H^1_{\mathcal{L}_f}(G_K, V)$ attached to the Selmer structure $\mathcal{L}_f = (L_v)$ where $L_v = H^1_f(G_v, V)$ for all v. So is $H^1_{f,S}(G_K, V) = H^1_{\mathcal{L}_{f,S}}(G_K, V)$ where $\mathcal{L}_{f,S}$ is the Selmer structure (L_v) with $L_v = H^1_f(G_v, V)$ for $v \notin S$ and $L_v = H^1_g(G_v, V)$ if $v \in S$. In particular, they are finite-dimensional over $\mathbb{Q}_p$.

A remarkable feature about the Selmer structure $\mathcal{L}_f$ is that it is self-dual: The structure $\mathcal{L}_f^\perp$ of $V^*(1)$ is the same as its own structure $\mathcal{L}_f$, as it follows from Prop. 2.3(c) and Theorem 2.1. The duality formula for Selmer groups therefore takes a very nice form for Bloch-Kato Selmer groups:

Theorem 2.2.

$$
\begin{aligned}
\dim H^1_f(G_K, V) \;=\; & \dim H^1_f(G_K, V^*(1)) \\
& + \dim H^0(G_K, V) - \dim H^0(G_K, V^*(1)) \\
& + \sum_{v|p} \dim D_{dR}(V_{|G_v})/D^+_{dR}(V_{|G_v}) \\
& - \sum_{v|\infty} \dim H^0(G_v, V)
\end{aligned}
$$

Proof — This results from Proposition 2.7, taking into account that

- for v a finite place not dividing p, $\dim H^1_f(G_v, V) - \dim H^0(G_v, V) = 0$ by Prop. 2.3(a).
- For v a finite place dividing p,

$$
\dim H^1_f(G_v, V) - \dim H^0(G_v, V) = \dim D_{dR}(V_{|G_v})/D^+_{dR}(V_{|G_v})
$$

by Prop. 2.8 $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$

Remark 2.3. The term on the third line of the above formula,

$$\sum_{v|p} \dim D_{\mathrm{dR}}(V_{|G_v})/D_{\mathrm{dR}}^+(V_{|G_v})$$

is equal to $\sum_{k<0} m_k(V)$, where the $m_k(V)$'s are the total multiplicity of the Hodge-Tate weight k in V defined in §1.2.3. This is clear from their definition since $\dim(D_{\mathrm{dR}}(V_{|G_v})/D_{\mathrm{dR}}^+(V_{|G_v}))$ is equal to $[K_v : \mathbb{Q}_p]$ times the number of negative Hodge-Tate weights of $V_{|G_v}$, counted with multiplicity.

Similarly, the term on the fourth line $\sum_{v|\infty} \dim H^0(G_v, V)$ is by definition the term we have denoted by $a^+(V)$ in §1.2.3.

Therefore, the theorem says that

$$\begin{aligned}
\dim H_f^1(G_K, V) = \; & \dim H_f^1(G_K, V^*(1)) \\
& + \dim H^0(G_K, V) - \dim H^0(G_K, V^*(1)) \\
& + \sum_{k<0} m_k(V) \\
& - a^+(V)
\end{aligned}$$

Exercise 2.27. What does this theorem say when $V = V^*(1)$?

Exercise 2.28. a.– Show that $H_f^1(G_K, \mathbb{Q}_p) = 0$. (Hint: use the finiteness of the class group of K as well as Exercise 2.18.)

b.– Deduce from a.– that $\dim H_f^1(G_K, \mathbb{Q}_p(1)) = r_1 + r_2 - 1$ where r_1 and r_2 are the number of real and complex places of K.

To explain the arithmetic significance of the Bloch-Kato selmer groups, we look at two important examples: $V = \mathbb{Q}_p(1)$, and $V = V_p(E)$ for E an elliptic curve.

2.3.2. *The case $V = \mathbb{Q}_p(1)$.*

Proposition 2.12. *The Kummer map κ realizes an isomorphism*

$$\mathcal{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Q}_p \to H_f^1(G_K, \mathbb{Q}_p(1)).$$

Proof — Note that properly speaking, the Kummer map κ has not been defined in this context of number fields, as G_K does not satisfy the finiteness property $\mathrm{Fin}(p)$, and as K^* is not of finite type. This is of course a minor technical problem that we shall circumvent in the next paragraph.

What we have defined is a compatible family of maps $\kappa_n : K^* \otimes \mathbb{Z}/p^n\mathbb{Z} \to H^1(G_K, \mathbb{Z}/p^n\mathbb{Z}(1))$ that are isomorphisms (see Exercise 2.2). Let Σ be any finite set of finite places containing the places above p. Let $\mathcal{O}_{K,\Sigma}^*$ be the group of units of K outside Σ. If $x \in \mathcal{O}_{K,\Sigma}^* \subset K^*$, then by the proof of Prop. 2.4, $\kappa_n(x)$ is in $H^1(G_{K,\Sigma}, \mathbb{Z}/p^n\mathbb{Z}(1))$ so since $G_{K,\Sigma}$ satisfies $\mathrm{Fin}(p)$ and $\mathcal{O}_{K,\Sigma}^*$ is of finite type, we can define by taking the projective limit of the κ_n's an isomorphism $\kappa : \mathcal{O}_{K,\Sigma}^* \otimes_{\mathbb{Z}} \mathbb{Q}_p \to H^1(G_{K,\Sigma}, \mathbb{Q}_p(1))$. Of course, by construction, this κ is compatible with the local Kummer maps $\kappa : \widehat{K_v^*} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G_{K_v}, \mathbb{Q}_p(1))$ for v a place of K in Σ.

Now by Proposition 2.4 and Proposition 2.9, we see that for $x \in \mathcal{O}_{K,\Sigma}^* \otimes_{\mathbb{Z}} \mathbb{Q}_p$, $\kappa(x) \in H_f^1(G_K, \mathbb{Q}_p(1))$ if and only if $x \in \mathcal{O}_K^*$. Therefore κ induces an isomorphism $\mathcal{O}_K^* \otimes \mathbb{Q}_p \to H_f^1(G_K, \mathbb{Q}_p(1))$. $\qquad \square$

The proof easily shows that $H_{f,S}^1(G_K, \mathbb{Q}_p(1)) \simeq \mathcal{O}_{K,S}^* \otimes \mathbb{Q}_p$, where $\mathcal{O}_{K,S}^*$ is the group of S-unit sof K.

This result, relating the Bloch-Kato Selmer group of $\mathbb{Q}_p(1)$ with is a classical object of interest in arithmetic (at least since the appearance of the Pell-Fermat equation $x^2 - Dy^2 = \pm 1$) is a first indication of the number-theoretical significance of the Bloch-Kato Selmer group. The proof makes clear how the condition f of Bloch-Kato makes it related to the interesting group $\mathcal{O}_K^*$ (whose rank is the object of one of the most beautiful theorem of the nineteenth century, Dirichlet's units theorem), rather than to the much less mysterious K^* (which is a free abelian group of infinite rank times a finite cyclic group). Note that, using exercise 2.28, this result implies that $\mathrm{rk}\, \mathcal{O}_K^* = r_1 + r_2 - 1$, which is the hard part of Dirichlet units theorem.

2.3.3. *The case $V = V_p(E)$ for E an elliptic curve.* Now let E be an elliptic curve over K. Let us recall (see [Silverman] for details) that the classical p-adic Selmer group $\mathrm{Sel}_p(E)$ of E is defined as the subspace of $H^1(G_K, V_p(E))$ whose elements are the x whose restriction x_v at every finite place v belong to the image of $E(K_v)$ in $H^1(G_v, V_p(E))$ by the local Kummer map κ_v. It is known (e.g. [Silverman]) that the Kummer map induces an injection $\kappa : E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \hookrightarrow \mathrm{Sel}_p(E)$ which is an isomorphism if and only if the p-primary component $\mathrm{Cha}(E)[p^\infty]$ of the Tate-Shafarevich group $\mathrm{Cha}(E)$ of E is finite, which is conjectured to be true (as a part of Birch and Swinnerton-Dyer conjecture).

Proposition 2.13. *As subspaces of $H^1(G_K, V_p(E))$, we have*

$$\mathrm{Sel}_p(E) = H_f^1(G_K, V_p(E)).$$

In particular, the Kummer map induces an injection $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to H_f^1(G_K, V_p(E))$ which is an isomorphism if and only if $\mathrm{Cha}(E)[p^\infty]$ is finite.

Proof — This is clear, since if $v | p$, for an element of $H^1(G_v, V_p(E))$ it is equivalent by Proposition 2.10 to be in the image of $E(K_v)$ or to be in the $H_f^1(G_v, V_p(E))$; and since $v \nmid p$, we have $H_f^1(G_v, V_p(E)) = H^1(G_v, V_p(E)) = 0$ by Exercise 2.10. $\qquad \square$

This again shows that the H_f^1 is closely related to one of the most interesting abelian group of algebraic number theory, the Mordell-Weil group $E(K)$. Similar results hold for abelian varieties.

2.3.4. *Motivic interpretation and the* **other** *Bloch-Kato conjecture.* Assume that V is the p-adic realization of a motive $M \in \mathcal{M}_K$. Let $0 \neq x \in H^1_g(G_K, V)$, and let W be the extension of $\mathbb{Q}_p$ by V defined by x. We note that the p-adic representation is de Rham at places v dividing p (since V is, and x_v is in $H^1_g(G_v, V)$ – see Lemma 2.7), and unramified at almost all places (since V is, and $x_v \in H^1_f(G_v, V) = H^1_{\mathrm{ur}}(G_v, V)$ for almost all v). Should the p-adic representation W be the realization of some motive N? If by motive we understand, as we have done so far **pure** (iso-) motives, the answer is no, because such a realization should be semi-simple, and W is not.

However, according to Grothendieck, there should exist a $\mathbb{Q}$-linear abelian category $\mathcal{MM}_K$ of *mixed motives* over K, containing the category $\mathcal{M}_K$ of pure motives as a full subcategory, with realization functors Real_p toward the category of p-adic representations of G_K (for all prime p), extending those from $\mathcal{M}_K$. The category $\mathcal{MM}_K$ should be to $\mathcal{M}_K$ what the category $\mathcal{V}_K$ of all varieties over K (not necessarily proper and smooth) is to its subcategory $\mathcal{VPS}_K$. In particular, there should exist a contravariant functor $H^i : \mathcal{V}_K \to \mathcal{MM}_K$ such that $\mathrm{Real}_p \circ H^i = H^i(-, \mathbb{Q}_p)$, where $H^i(X, \mathbb{Q}_p)$ denotes for a general variety X over K the p-adic representation $H^i_{\text{ét}}(X \times_K \bar{K}, \mathbb{Q}_p)$ of G_K.

The most notable difference between $\mathcal{MM}_K$ and $\mathcal{M}_K$ is that $\mathcal{MM}_K$ should not be semi-simple (nor graded in any interesting way). If $N \in \mathcal{MM}_K$, the G_K-representation $\mathrm{Real}_p(N)$ should be unramified almost everywhere, and de Rham at places dividing p, but not semi-simple in general, nor pure of some weight (rather, it should have an increasing filtration $\mathrm{Fil}^w \mathrm{Real}_p(N)$ whose graded piece are pure geometric representation of weight w): those requirement are inspired by the known properties of the étale cohomology of general varieties over K.

Going back to our extension W of 1 by $V = \mathrm{Real}_p(M)$ representing $x \in H^1_g(G_K, V)$, it is expected that W should be $\mathrm{Real}_p(N)$ for some **mixed** motive $N \in \mathcal{M}_K$. Actually it is even expected that the functor Real_p induces an isomorphism between

$$(7) \qquad\qquad \mathrm{Ext}^1_{\mathcal{MM}_K}(\mathbb{Q}, M) \simeq H^1_g(G_K, V)$$

where $\mathbb{Q}$ is the object of $\mathcal{M}_K$ such that $\mathrm{Real}_p(\mathbb{Q}) = \mathbb{Q}_p$. This is the *motivic interpretation* of H^1_g. We should have similar interpretation for $H^1_{f,S}(G_K, V)$ by considering mixed motives over $\mathrm{Spec}\,\mathcal{O}_K - S$ instead of $\mathrm{Spec}\,K$.

Thus, the Bloch-Kato conjecture is in a sense a prediction, in terms of L-functions, of the dimension of the Ext^1-spaces in the category of mixed motives $\mathcal{M}_K$. It is also conjectured that this category has cohomological dimension 1, that is trivial Ext^i for $i \geq 2$.

Of course, the category of mixed motives $\mathcal{MM}_K$ has not yet been constructed. Nevertheless, when $M = H^i(X)$ for some $X \in \mathcal{VPS}_K$ it is possible to give a non-conjectural meaning to (what should be) $\mathrm{Ext}^1_{\mathcal{MM}_K}(\mathbb{Q}, M)$ using the K-theory of X (see [BK, page 359].) Bloch and Kato have conjectured ([BK, Conjecture 5.3]) that

when $\mathrm{Ext}^1_{\mathcal{MM}_K}(\mathbb{Q}, M)$ is defined that way, (7) holds. Many cases **other** Bloch-Kato conjecture have been proved (by Voedvodsky and other authors), and a proof of the general case has been recently announced (by Voedvodsky)

2.3.5. *Relations between* H^1_f, $H^1_{f,S}$ *and* H^1_g. It is a natural question to try to compare the dimension of $H^1_{f,S}(G_K, V)$ and $H^1_{f,S'}(G_K, V)$. Of course, it would be enough to understand completely the case $S' = S \cup \{v\}$ where v is a finite prime not in S. First, let us just state that in this case, by definition,

$$\dim H^1_{f,S}(G_K, V) \le \dim H^1_{f,S\cup\{v\}}(G_K, V) \le \dim H^1_{f,S}(G_K, V) + \dim(H^1_g(G_v, V)/H^1_f(G_v, V)).$$

By Proposition 2.8 and Exercise 2.21 in the case $v|p$, and from Proposition 2.3 in the case $v \nmid p$, we have

$$\dim(H^1_g(G_v, V)/H^1_f(G_v, V)) = \dim D_{\mathrm{crys}}((V_{|G_v})^*(1))^{\phi=1} \text{ if } v|p$$
$$\dim(H^1_g(G_v, V)/H^1_f(G_v, V)) = \dim H^0(G_v, V^*(1)) \text{ if } v \nmid p$$

In particular, when $v \nmid p$, $V_{|G_v}$ has no quotient isomorphic to $\mathbb{Q}_p(1)$, we have

$$\dim H^1_{f,S}(G_K, V) = \dim H^1_{f,S'}(G_K, V).$$

Exercise 2.29. Prove those relations.

It is not possible to prove in general a formula for $\dim H^1_{f,S}(G_K, V)$ in term of $\dim H^1_{f,S\cup\{v\}}(G_K, V)$ and local terms, without assuming again some conjectures.

Prediction 2.1 (Fontaine & Perrin-Riou). *([FPR, §II.3.3.1]) We have*

$$\dim H^1_{f,S\cup\{v\}}(G_K, V) = \dim H^1_{f,S}(G_K, V) + \dim(H^1_g(G_v, V)/H^1_f(G_v, V)).$$

Equivalently, we have

$$\dim H^1_{f,S\cup\{v\}}(G_K, V) = \dim H^1_{f,S}(G_K, V) + \dim D_{crys}((V_{|G_v})^*(1))^{\phi=1} \text{ if } v|p$$
$$\dim H^1_{f,S\cup\{v\}}(G_K, V) = \dim H^1_{f,S}(G_K, V) + \dim H^0(G_v, V^*(1)) \text{ if } v \nmid p$$

Let us explain where this prediction comes from. Applying duality both to $H^1_{f,S\cup\{v\}}(G_K, V)$ and $H^1_{f,S}(G_K, V)$, we are reduced to proving that

$$H^1_{f, \, e \text{ at } S\cup\{v\}}(G_K, V^*(1)) = H^1_{f, \, e \text{ at } S}(G_K, V^*(1)).$$

Here $H^1_{f, \, e \text{ at } S}(G_K, W)$ parametrizes extension of $\mathbb{Q}_p$ by W that are e at places of S and f anywhere else.

Exercise 2.30. Check this computation.

Therefore the prediction boils down to the fact that extension of 1 by $V^*(1)$ that are f everywhere are also e everywhere. The reason for what this is believed to be true is as follows: the extension of 1 by $V^*(1)$ should be geometric, that is appearing in the étale cohomology of some (not proper-and-smooth) variety X over K. It is expected that even in this mixed case, conjecture EC1 holds, that at every place v of K, the Frobenius (Frob$_v$ acting on W^{I_v} if v is prime to p, $\varphi = \phi^{q_v}$ acting

on $D_{\mathrm{crys}}(W_{|G_v})$ if v divides p) acts semi-simply. If this holds, then the class of the extension W is not only f but e at v, according to Exercises 2.25 and 2.26.

3. L-FUNCTIONS

For an alternative presentation of some of this material, see [FPR] or [Tay2]. In all this section, K is a number field.

3.1. **L-functions.**

3.1.1. *Euler factors.* Let V be a p-adic geometric representation of G_K. For the commodity of exposition, we suppose that an embedding of $\mathbb{Q}_p$ into $\mathbb{C}$ has been chosen. This is an ugly thing to do, as it depends on the non-enumerable axiom of choice and it is absolutely non-canonical, but actually, as we shall see, this choice shall play no role in practice.

For every finite place v of K that does not divides p, we set

$$(8) \qquad L_v(V, s) = \det(\mathrm{Id} - (\mathrm{Frob}_v^{-1} q_v^{-s})_{|V^{I_v}})^{-1}$$

Here s is a complex argument, q_v the cardinality of the residue field of K at v, and the matrix of Frob_v is seen as a complex (rather than p-adic) matrix using our embedding. The function $s \mapsto L_v(V, s)$, called an *Euler factor*, is clearly a rational (hence meromorphic) function from $\mathbb{C}$ to $\mathbb{C}$, with only a finite number of poles. It is also, formally, a power series in the variable q_v^{-s}.

Note also that when V is algebraic, the coefficients of $\det((\mathrm{Id} - \mathrm{Frob}_v^{-1} q_v^{-s})_{|V^{I_v}})^{-1}$ are algebraic numbers for almost all v by property E5 so the choice of the embedding $\mathbb{Q}_p \to \mathbb{C}$ is not really relevant, only an embedding of the field of algebraic numbers in $\mathbb{Q}_p$ to $\mathbb{C}$ matters.

For places v of V that divide p, we set

$$(9) \qquad L_v(V, s) = \det((\mathrm{Id} - \varphi^{-1} q_v^{-1})_{|D_{\mathrm{crys}}(V_{|G_v})})^{-1},$$

where $\varphi = \phi^{f_v}$, with ϕ the crystalline Frobenius and f_v the integer such that $q_v = p^{f_v}$.

3.1.2. *Formal definition of the L-function as an Euler product.*

Definition 3.1. We set formally

$$L(V, s) = \prod_{v \text{ finite place of } K} L_v(V, s).$$

More generally, for S any finite set of finite places of K, we set

$$L_S(V, s) = \prod_{v \text{ finite place of } K \text{ not in } S} L_v(V, s).$$

The product of Euler factors defining the L-function is called an *Euler product.*

Note that if $V = V_1 \oplus V_2$ as G_K-representations, then $L(V, s) = L(V_1, s)L(V_2, s)$. Since geometric representations are semi-simple, it is often enough to consider irreducible V.

Even only formally, there are many things to say about the L-function. We will only mention two of them. The first one is immediately checked, and fundamental. We shall use it frequently without comments:

$$(10) \qquad\qquad L(V(n), s) = L(V, s + n).$$

The second one needs a little computation, left as an exercise to the reader in the case where V is crystalline at all places dividing v (for the general case, see [FPR]):

Lemma 3.1. *Let V be a p-adic representation of a number field K, K_0 be a subfield of K, and $W = Ind_{G_K}^{G_{K_0}} V$. Then*

$$L(V, s) = L(W, s).$$

If S_0 a finite set of finite places of K_0 and S is the set of places of K that lies above some place of S_0, then

$$L_S(V, s) = L_{S_0}(W, s).$$

3.1.3. *Convergence.* Let V be a p-adic representation that is pure of weight $w \in \mathbb{Z}$. Assume more precisely that it is Σ-pure, where Σ is a finite set of finite places containing all places above p, and all places where V is ramified. Then by definition, for $v \notin \Sigma$, we have

$$L_v(V, s) = \prod_{i=1}^{\dim V} (1 - \alpha_{i,v}^{-1} q_v^{-s})^{-1}$$

where $\alpha_{1,v}, \dots, \alpha_{dimV,v}$ are the roots of the characteristic polynomials of Frob_v in V, and we see that $L_v(V, s)$ have no zero, and only a finite number of poles, all on the line $\Re s = w/2$.

Proposition 3.1. *Let V be a representation that is Σ-pure of weight w, with Σ as above. Then the Euler product defining $L_\Sigma(V, s)$ converges absolutely and uniformly on all compact on the domain $\Re s > w/2 + 1$.*

Proof — We have to see that $\sum_{v \notin \Sigma} \sum_{i=1}^{\dim V} \log(|1 - \alpha_{i,v}^{-1} q_v^{-s}|)$ converges absolutely and uniformly over every compact on the domain $\Re s > w/2 + 1$. Using the inequality $|\log(1 + z)| \leq |z|$, and $|\alpha_{i,v}^{-1}| = q_v^{w/2}$, we are reduced to check that the sum $\sum_{v \notin \Sigma} |q_v^{-s+w/2}|$ converges absolutely and uniformly on all compact on the same domain. But the number of places v such that $q_v = n$ for a given non-negative integer n is finite and bounded independently of n, so we are reduced to the convergence (absolutely and uniformly on all compact subsets of $\Re s > w/2 + 1$) of the sum $\sum_{n \geq 1} |n^{w/2-s}| = \sum_{n \geq 1} n^{w/2-\Re s}$, which is clear. $\qquad \square$

Corollary 3.1. *For Σ as above, the function $L_\Sigma(V, s)$ is a well-defined holomorphic function with no zero on the domain $\Re s > w/2 + 1$. The function $L(V, s)$ are well-defined meromorphic functions with no zero on the domain $\Re s > w/2 + 1$.*

Proof — The first assertion concerning $L_\Sigma(V, s)$ follows directly from the proposition. The assertion concerning $L(V, s)$ follows from the first one since it is clear that the local factors $L_v(V, s)$ for $v \notin \Sigma$ are meromorphic functions with no 0. $\square$

Prediction 3.1. *If V is geometric, and as above pure of weight w, then for all prime v, the poles of the local factors $L_v(V, s)$ lie on the line $\Re s = w/2$. As a consequence, $L(V, s)$ is holomorphic on $\Re s > w/2 + 1$.*

If V is Σ-pure, the assertion about the local factors for $v \notin \Sigma$ is clear by the definition of the weight. That the same holds for all places v would follow from the Fontaine-Mazur conjecture and assertion about étale cohomology we have not written. The consequence on $L(V, s)$ is proved as the corollary above (compare [Tay2, page 11]).

3.1.4. *Examples.* If $V = \mathbb{Q}_p$, the function $L(V, s)$ is the Dedekind zeta function $\zeta_K(s)$. It is well known to have an analytic continuation to $\mathbb{C}$ with only one pole, at $s = 1$, of order one. If $V = \mathbb{Q}_p(n)$, then $L(V, s) = \zeta_K(s + n)$.

If $V = V_p(E)$ for E an elliptic curve over K, then $V_p(E) = H^1(E, \mathbb{Q}_p)^* = H^1(E, \mathbb{Q}_p)(1)$, $L(V_p(E), s) = L(H^1(E, \mathbb{Q}_p)(1), s) = L(E, s+1)$ where $L(E, s)$ is the usual L-function of the elliptic curve.

3.1.5. *Analytic continuation and zeros.*

Conjecture 3.1. *Assume that V is a geometric p-adic representation of G_K, that is pure of weight w. Then the function $L(V, s)$ admits a meromorphic continuation on all the complex plane. The function $L(V, s)$ has no zeros on the domain $\Re s \geq w/2 + 1$. If V is irreducible, $L(V, s)$ has no poles, except if $V \simeq \mathbb{Q}_p(n)$, in which case $L(V, s)$ has a unique pole at $s = n + 1$, which is simple.*

This conjecture is known to be true if V is automorphic. Let us detail this assertion. If V is automorphic, it is attached to a cuspidal automorphic representation π of GL_d/K, where $d = \dim V$, and we have $L(V, s) = L(\pi, s)$ where $L(\pi, s)$ is the L-function attached to π in the theory of automorphic representation. That the L-function of an automorphic representation satisfies the conjecture is a result of Hecke in the case $d = 1$, of Jacquet-Langlands in the case $d = 2$, and of Jacquet-Shalika in the case $d \geq 3$.

It is widely expected that proving conjecture 3.1 will require to prove that every geometric representation is automorphic.

Let us add some cultural comments on the assertion in the conjecture that $L(V, s)$ has no zero on the domain $\Re s \geq w/2 + 1$, which will be very important for us

through its special case $L(V, w/2 + 1) \neq 0$. By construction, as we have seen, $L(V, s)$ has no zero on the open domain $\Re s > w/2 + 1$, and the new assertion is that $L(V, s)$ has no zero on the boundary of the domain of convergence, that is the line $\Re s = w/2 + 1$. In the special case $V = \mathbb{Q}_p$, $K = \mathbb{Q}$, this is the assertion that the Riemann zeta function $\zeta_{\mathbb{Q}}$ has no zero on the line $\Re s = 1$. This of course is a part of the famous hypothesis made by Riemann in 1859, in connection of the "prime number theorem", a striking statement about the distribution on prime numbers that was earlier conjectured by Gauss. In the same paper, Riemann proved the analytic continuation of $\zeta_{\mathbb{Q}}$, and determined its pole, so this was really the ancestor of Conjecture 3.1. The non-vanishing of $\zeta_{\mathbb{Q}}$ on the line $\Re s = 1$ was proved in 1896 by Hadamard and de la Vallée Poussin, and further results on the non-vanishing on the boundary of the domain of convergence for more general L-function were proved using the same ideas.

As is well known, the stronger statement that $\zeta_{\mathbb{Q}}$ has no zero on the domain $\Re s > 1/2$ is the Riemann Hypothesis, a still open conjecture and now another Clay Millennium Problem. More generally, the Grand Riemann Hypothesis predicts that for any geometric V pure of weight w, $L(V, s)$ has no zero on $\Re s > (w + 1)/2$. For a detailed exposition of the consequences of the Grand Riemann hypothesis, see [I, chapter 5]. However, be aware that there is no direct relation between the Grand Riemann Hypothesis, which is interested in the zeros of $L(V, s)$ on $(w + 1)/2 < \Re s < w/2 + 1$ and the Bloch-Kato conjecture, which is concerned by the zeros of $L(V, s)$ at integers.

3.2. The functional equation.

3.2.1. *The Gamma function and variants.* Let us recall that the Γ-function is defined as an holomorphic function for $\Re s > 1$ as

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} \ dt.$$

Its properties that we shall need are given as an exercise (or google "Gamma function"):

Exercise 3.1. a.– Show that $\Gamma(s + 1) = s\Gamma(s)$ for $\Re s \geq 1$ and that $\Gamma(1) = 1$.

b.– Show that Γ has an analytic continuation on the whole complex plane with only poles at non-positive integers $s = 0, -1, -2, -3, \ldots$, and that those poles are simple.

c.– Show that Γ has no zero.

d.– Show the duplication formula $\Gamma(s)\Gamma(s + 1/2) = 2^{1/2-2s}\sqrt{2\pi}\Gamma(2s)$.

We define two variants:

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$$
$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

Note that $\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$. The poles of $\Gamma_{\mathbb{R}}$ are at $0, -2, -4, -6, \ldots$ and those of $\Gamma_{\mathbb{C}}$ are at $0, -1, -2, -3, -4, -5, \ldots$. These poles are all simple.

3.2.2. *The completed L-function.* To state the functional equation of $L(V, s)$ we need to complete the Euler product that defines it by adding "Euler factors at infinity", which are translated of the functions $\Gamma_{\mathbb{R}}$ and $\Gamma_{\mathbb{C}}$. Morally, the precise form of those Γ factors should be deduced from the Hodge structure $\text{Hodge}(V)$ conjecturally attached to V according to the philosophy of motives (see §1.3). For a definition using this Hodge structure, see [S1] or [FPR]. Since we do not want to rely on motive theory, we give a definition of those factors assuming only that V is a representation coming from geometry that is pure of weight w, and this definition is (conjecturally) equivalent to the one given in literature.

Recall that we have defined in 1.2.3 the total multiplicity $m_k = m_k(V)$ of the Hodge-Tate weight $k \in Z$ of V and also two natural integers $a^{\pm}(V)$ which add up to $[K : \mathbb{Q}]\dim V$. We have also set $m_{<w/2} = \sum_{k<w/2} m_k$.

We set

$$L_{\infty}(V, s) = \prod_{k \in \mathbb{Z}, k<w/2} \Gamma_{\mathbb{C}}(s-k)^{m_k} \text{ if } w \text{ is odd.}$$

If w is even, we define a sign $\varepsilon = (-1)^{w/2}$, and

$$L_{\infty}(V, s) = \prod_{k \in \mathbb{Z}, k<w/2} \Gamma_{\mathbb{C}}(s-k)^{m_k} \, \Gamma_{\mathbb{R}}(s-w/2)^{a^{\varepsilon}-m_{<w/2}} \, \Gamma_{\mathbb{R}}(s-w/2+1)^{a^{-\varepsilon}-m_{<w/2}}$$

This definition may seem *ad hoc*. Since it is a definition, we cannot justify it a priori, and since it is only used in a conjecture (the functional equation), not a theorem, we cannot even say that it is the right definition that makes the theorem work. However, it is really the only natural definition that matches the various cases where we know the functional equation (Hecke characters, modular forms, etc.). We hope that the following lemma and exercise will show that it is more natural that it seems at first glance.

Lemma 3.2. *We have* $L_{\infty}(V(n), s) = L_{\infty}(V, s+n)$ *for all* $n \in \mathbb{Z}$.

Proof — It is enough to prove it for $n = 1$. Let $V' = V(1)$. We have $w(V') = w(V) - 2$, and $m_{k'}(V') = m_{k'+1}(V)$ for any $k' \in \mathbb{Z}$ (since the Hodge-Tate weights of V are those of V minus one). Therefore if in the product $\prod_{k\in\mathbb{Z},k<w(V)/2}\Gamma_{\mathbb{C}}((s+1)-k)^{m_k(V)}$ we make the change of variables $k' = k-1$, we get $\prod_{k'\in\mathbb{Z},k'<w(V')/2}\Gamma_{\mathbb{C}}(s-k')^{m_{k'}(V')}$. This already proves that $L_{\infty}(V(1), s) = L_{\infty}(V, s)$ in the case $w(V)$ (or $w(V')$, that amounts to the same) odd. For the case $w(V)$ even, we notice that

$\varepsilon(V') = -\varepsilon(V)$. But we also have $a^+(V(1)) = a^-(V)$ by definition since the action of the complex conjugation on $\mathbb{Q}_p(1)$ is -1. Therefore the two changes of sign cancel each other and we have $a^{\pm\varepsilon(V(1))}(V(1)) = a^{\pm\varepsilon(V)}(V)$. It is now easy to check that

$$\Gamma_{\mathbb{R}}((s+1) - w(V)/2)^{a^{\varepsilon(V)}(V) - m_{<w(V)/2}} \; \Gamma_{\mathbb{R}}((s+1) - w(V)/2 + 1)^{a^{-\varepsilon(V)} - m_{<w(V)/2}(V)}$$

$$= \Gamma_{\mathbb{R}}(s - w(V')/2)^{a^{\varepsilon(V')}(V') - m_{<w(V')/2}} \; \Gamma_{\mathbb{R}}(s - w(V')/2 + 1)^{a^{-\varepsilon(V')} - m_{<w(V')/2}(V')},$$

and this proves the lemma. $\square$

Exercise 3.2. Using Predictions 1.2 and 1.3, show that $L_\infty(V, s)$ has no zero and that the number of $\Gamma_{\mathbb{R}}$ factors (a $\Gamma_{\mathbb{C}}$ being worth two $\Gamma_{\mathbb{R}}$'s) in L_∞ is always $[K : \mathbb{Q}] \dim V$.

We note for further reference the following

Lemma 3.3. *If $w < 0$, the function $L_\infty(V, s)$ has no pole at $s = 0$. If $w \geq 0$ is odd, then $L_\infty(V, s)$ has a pole at $s = 0$ of order $\sum_{0 \leq k < w/2} m_k$. If $w \geq 0$ is even, then $L_\infty(V, s)$ has a pole at $s = 0$ of order $\sum_{0 \leq k < w/2} m_k + a^+ - m_{w/2}$.*

Proof — Each term of the form $\Gamma_{\mathbb{C}}(s - k)^{m_k}$ contributes to a pole at $s = 0$ (with order m_k) if and only if $k \geq 0$. So the product of those terms for $k < w/2$ gives a pole of order $\sum_{0 \leq k \leq w/2} m_k$ (which is 0 if $w < 0$) and that's all if w is odd. If w is even, we look at the factor $\Gamma_{\mathbb{R}}(s - w/2)$ and $\Gamma_{\mathbb{R}}(s - w/2 + 1)$. If $w < 0$, none of them has pole at $s = 0$, which concludes the case $w < 0$. If $w \geq 0$, and $w/2$ is even, only the factor $\Gamma_{\mathbb{R}}(s - w/2)$ has a pole at $s = 0$. Since this factors appears $a^\varepsilon - m_{w/2}$ times, and $\varepsilon = +1$ in this case, we get a contribution to the order of the pole at $s = 0$ of $a^+ - m_{w/2}$. If $w \geq 0$ and $w/2$ is odd (so in fact $w \geq 2$), then only the factor $\Gamma_{\mathbb{R}}(s - w/2 + 1)$ has a pole at $s = 0$, and the order of this pole is $a^{-\varepsilon} - m_{w/2}$, but in this case $\varepsilon = -1$, so the contribution is again $a^+ - m_{w/2}$. $\square$

We set

$$\Lambda(V, s) = L(V, s) L_\infty(V, s).$$

This is the *completed* L-function of V.

Example 3.1. Assume $V = \mathbb{Q}_p$. In this case we have $w = 0$, $m_0 = [K : \mathbb{Q}]$ ad $m_{<w/2} = 0$. We also have $\varepsilon = 1$, $a^+ = r_1 + r_2$ and $a^- = r_2$, where r_1 and r_2 are the number of real and complex places of K. We thus have $L_\infty(V, s) = \Gamma_{\mathbb{R}}(s)^{r_1 + r_2} \Gamma_{\mathbb{R}}(s + 1)^{r_2}$, and

$$\Lambda(V, s) = \zeta_K(s) \Gamma_{\mathbb{R}}(s)^{r_1 + r_2} \Gamma_{\mathbb{R}}(s + 1)^{r_2} = \zeta_K(s) \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}.$$

Formulas equivalent to this one appears in Dedekind's work (and in Riemann's work in the case $K = \mathbb{Q}$).

3.2.3. *The functional equation.* Assume as before that V comes from geometry. Then so does $V^*(1)$. Assume conjecture 3.1, so $L(V, s)$ and $L(V^*(1), s)$ and therefore $\Lambda(V, s)$ and $\Lambda(V^*, s)$ are well-defined meromorphic function on $\mathbb{C}$. Then it is conjectured that the following *functional equation* relates those two functions:

Conjecture 3.2. *There exists an entire function with no zero $\epsilon(V, s)$ such that the following holds*

$$\Lambda(V^*(1), -s) = \epsilon(V, s)\Lambda(V, s).$$

It is further conjectured that $\epsilon(V, s)$ has a very simple form, namely $s \mapsto AB^s$ for A a complex constant and B a positive real constant. For more details, see [Tay2]. This conjecture is known to be true for automorphic representations.

Example 3.2. Using the functional equation above in the case $K = \mathbb{Q}$, $V = \mathbb{Q}_p$ (which is due to Riemann), one sees that the only zeros of $\zeta_{\mathbb{Q}}$ at integers are simple zeros at $-2, -4, -6, -8, \ldots$ If K is a general number field, using the functional equation above for $V = \mathbb{Q}_p$ (which is due to Hecke), one sees that ζ_K has a zero at $s = 0$ of order $r_1 + r_2 - 1$, where r_1 is the number of real places and r_2 the number of complex places of K.

Exercise 3.3. Check carefully the computations leading to Example 3.2.

Exercise 3.4. Let V be a representation that comes from geometry and is pure of weight w. Assume Conjectures 3.1 and 3.2. Show that the only possible zeros of $L(V, s)$ outside the *critical band* $w/2 < \Re s < w/2 + 1$ are at integers $\leq w/2$, and compute the order of those zeros. They are called the *trivial zeros* of $L(V, s)$.

3.2.4. *The sign of the functional equation for a polarized representation.* The problem with the functional equation given above is that it relates two different L-functions, namely $L(V, s)$ and $L(V^*(1), s) = L(V^*, s + 1)$. When those function are equal, or at least, translates of each other, things become more interesting. In this §, we shall discuss cases where this happens.

Let V be a geometric and pure p-adic representation of G_K. For τ any automorphism of the field K, we denote V^τ the representation of G_K over the same space V, but where an element g in G_K acts on V^τ as $\sigma g \sigma^{-1}$, where σ is a fixed element of $G_{\mathbb{Q}}$ whose restriction to K is τ. The representation V^τ only depends on τ (not on σ) up to isomorphism and we have $L(V, s) = L(V^\tau, s)$ where they are defined and similarly for completed Λ-functions. Also V^τ is pure of the same weight as V.

Exercise 3.5. Check these assertions (that's easy) and prove the following partial converse: assume that K is Galois over $\mathbb{Q}$ and V and V' are two irreducible geometric and pure p-adic representations of G_K such that $L(V, s) = L(V', s)$. Then $V' \simeq V^\tau$ for some $\tau \in \mathrm{Gal}(K/\mathbb{Q})$.

Definition 3.2. We shall say that V is *polarized* if for some integer w and some $\tau \in \mathrm{Aut}(K)$, we have $V^\tau(w) \simeq V^*$. The integer w is called the weight of the polarization.

It is obvious that if V is pure and polarized, then the weight of the polarization w is the motivic weight of V.

Exercise 3.6. Prove that every representation V of dimension 1 is polarized. Prove that the representation $V_p(A)$ attached to an abelian variety A is polarized of weight -1. Prove that the representation attached to a classical modular eigenform of weight $2k$ and level $\Gamma_0(N)$ is polarized of weight $2k - 1$. Prove that if V is an irreducible polarized representation of $G_\mathbb{Q}$ of dimension 2, then the weight of the polarization is odd if and only if V is.

If V is polarized, geometric and pure of weight w, we have $\Lambda(V^*(1), s) = \Lambda(V^\tau(1 + w), s) = \Lambda(V, s + 1 + w)$. Therefore assuming Conjectures 3.1 and 3.2, the functional equation becomes

(11) $$\Lambda(V, -s + 1 + w) = \epsilon(V, s)\Lambda(V, s).$$

It involves only one L-function, $L(V, s)$, and we can talk of the *center of the functional equation* $s = (w + 1)/2$. Note that this center is $1/2$ off the domain of convergence of the Euler product, and right in the middle of the critical band (see Exercise 3.4). In particular, this center is not a pole of $L(V, s)$ (and if it is a zero, at least it is not a *trivial zero*).

In particular, since $L(V, s)$ is not identically 0, one sees that $\epsilon(V, (w+1)/2) = \pm 1$. This sign is called *the sign of the functional equation of $L(V, s)$*, or simply *the sign of $L(V, s)$*. One has the elementary but important relation, first observed by Shimura:

Proposition 3.2. *The order of the zero of $L(V, s)$ at $s = (w + 1)/2$ is odd if the sign of $L(V, s)$ is -1, and even if it is 1.*

Proof — This is clear if L is replaced by Λ in view of the functional equation (11). So we just have to show that the factor $L_\infty(V, s)$ and $L_\infty(V^*(1), s)$ have no pole and no zero at $s = (w + 1/2)$. But they both are products of functions of the form $\Gamma_\mathbb{R}(s - i)$ with $i < w/2$. The result then follows from the properties of the Γ-function. $\qquad\square$

This is especially interesting when the weight w of V is odd, because then the center of the functional equation $(w+1)/2$ is an integer. By replacing V by $V((w+1)/2)$, we can even assume that V has weight -1 and that the center of the functional equation is at 0.

Remark 3.1. The progress in the Langlands program mentioned in §1.2.4 has provided us with a vast supply of automorphic representations ρ_π that are polarized

with K totally real and $\tau = \mathrm{Id}$, or K a CM field, and τ its complex conjugacy. All representations constructed this way are also regular, that is they have distinct Hodge-Tate weights.

Conversely, it is a reasonable hope that current methods (e.g. those explained in this conference) will lead, some day, with a huge amount of work, to the proof that every irreducible geometric regular polarized representation of G_K (with K, τ as above) is automorphic, and in most cases, comes from geometry.

For other geometric representations (non-polarized especially), some completely new ideas seem required.

4. The Bloch-Kato conjecture

For an other presentation of much of this material (and more) see [BK] and [FPR].

In all this section, K is a number field, and V is a pure geometric representation of G_K. We assume that the L-function $L(V, s)$ has a meromorphic continuation to the entire plane, in accordance to Conjecture 3.1.

4.1. The conjecture.

4.1.1. *Statement.*

Conjecture 4.1 (Bloch-Kato)**.**

$$\dim H^1_f(G_K, V^*(1)) - \dim H^0(G_K, V^*(1)) = \mathrm{ord}_{s=0} L(V, s).$$

The H^0 term in the LHS is 0 unless V contains $\mathbb{Q}_p(1)$. It accounts for the pole predicted by conjecture 3.1 of $L(V, s)$. Aside the case of $\mathbb{Q}_p(1)$, it can safely be ignored.

The conjectures of Bloch-Kato relate two very different objects attached to V. The Selmer group $H^1_f(G_K, V)$ is a global invariant of V, that contains deep number-theoretical information attached to the representation V, the motives M of which it is the p-adic realization, or ultimately, the algebraic variety where it comes from (as $H^1_f(G_K, V_p(E))$ is closely related to $E(K)$); the L-function, on the other hand, is built on local information (the local Euler factors), but all this information is mixed up, and via a mysterious process of analytical continuation, gives rise to an integer, the order at $s = 0$ of the L-function. That this number should be equal to the dimension of the Bloch-Kato Selmer group for $V^*(1)$ is very mysterious indeed.

Tautologically, proving the Bloch-Kato conjecture amounts to proving two inequalities:

$$(12) \qquad \dim H^1_f(G_K, V^*(1)) \geq \mathrm{ord}_{s=0} L(V, s) + \dim H^0(G_K, V^*(1))$$

$$(13) \qquad \dim H^1_f(G_K, V^*(1)) \leq \mathrm{ord}_{s=0} L(V, s) + \dim H^0(G_K, V^*(1)).$$

The first one, the lower bound on the dimension of the Bloch-Kato Selmer group, asks us to exhibit a sufficient number of independent extensions of 1 by $V^*(1)$ in the category of representationd of G_K, whose classes lies in the H^1_f. So it is essentially a problem of constructing non-trivial extensions between Galois representations with prescribed local properties. Chris' lecture and mine will explain some of the techniques that allow us to do so. Very often those technics take a big input in the theory of automorphic forms.

The second inequality, the upper bound of the dimension of the Bloch-Kato Selmer group, seems to be accessible by very different methods, using in many cases the idea of Euler systems. We shall give a short review of the results obtained in its direction below.

4.1.2. *Two examples.* Assume first that $V = \mathbb{Q}_p$. Then $L(V, s)$ is the Dedekind Zeta function $\zeta_K(s)$, and as we have seen, $\mathrm{ord}_{s=0}\zeta_K(s) = r_1 + r_2 - 1$ (cf. Example 3.2). On the other hand, $V^*(1) = \mathbb{Q}_p(1)$ so $H^1_f(G_K, V^*(1)) \simeq \mathcal{O}^*_K \otimes_{\mathbb{Z}} \mathbb{Q}_p$ by Proposition 2.12 and $H^0(G_K, V^*(1)) \simeq 0$. Therefore the Bloch-Kato conjecture reduces in this case to

$$\mathrm{rk}_{\mathbb{Z}} \mathcal{O}^*_K = r_1 + r_2 - 1.$$

This equality is of course well known, as the Dirichlet's units theorem.

Assume now that E is an elliptic curve over K, and $V = V_p(E)$. Then $V^*(1) \simeq V$ by the Weil's pairing, so V is polarized of weight -1 in the terminology of §3.2.4. The Bloch-Kato conjectures amount to the prediction:

$$\dim H^1_f(G_K, V_p(E)) = \mathrm{ord}_{s=0}L(V_p(E), s) = \mathrm{ord}_{s=1}L(E, s).$$

As we have seen (Prop. 2.13), in this case $\dim H^1_f(G_K, V) \geq \mathrm{rk}E(K)$, with equality if $\mathrm{Cha}(E)[P^\infty]$ is finite. The Birch and Swinnerton-Dyer conjecture contains three parts, of which the first two are: $\mathrm{rk}E(K) = \mathrm{ord}_{s=1}L(E, s)$ (this part is actually one of the seven Clay's problem) and $\mathrm{Cha}(E)[p^\infty]$ is finite. Therefore, the Birch and Swinnerton-Dyer conjecture implies the Bloch-Kato conjecture for $V = V_p(E)$, and assuming its second part (the finiteness of $\mathrm{Cha}(E)[p^\infty]$), its first part is equivalent to the Bloch-Kato conjecture for $V = V_p(E)$.

4.1.3. *Prediction for representations of non-negative weight.* Now assume that the weight w of V satisfies $w \geq 0$, and for simplicity that V is irreducible. Then $V^*(1)$ has weight $w' = -2-w \leq -2$. The Euler product for $L(V^*(1), s)$ converges for $\Re s > w'/2 + 1 \geq -1 - w/2 + 1 = -w/2$, and if $V^*(1)$ satisfies conjecture 3.1, $L(V^*(1), s)$ has no zero on the domain $\Re s \geq -w/2$. In particular $\mathrm{ord}_{s=0}L(V^*(1), s) = 0$, except if $V = \mathbb{Q}_p$, where this order is -1. Applying the Bloch-Kato conjecture to $V^*(1)$, we thus get that $H^1_f(G_K, V) = 0$. Since V has weight ≥ 0, we see easily that in fact $H^1_f(G_K, V) = H^1_g(G_K, V)$. So in fact

Prediction 4.1. *If V is pure of weight $w \geq 0$, then $H^1_g(G_K, V) = 0$.*

This prediction is an important part of the Bloch and Kato's conjecture, and is still widely open. Through the motivic interpretation of the H_g^1 (see §2.3.4), it is also a consequence of the older, and still conjectural, "yoga of weights" developed by Grothendieck in the sixties. Namely, Grothendieck emphasized that motivic weights should go up in a non-trivial extension of pure motives in the categories of mixed motives $\mathcal{MM}_K$: if M' and M'' are pure motives, and $0 \to M' \to M \to M'' \to 0$ is a non trivial extension in $\mathcal{MM}_K$, one should have $w(M') < w(M'')$. (See the "definition" of $\mathcal{MM}_K$ in §2.3.4)

If V is pure of some weight w, then $\mathrm{ad}V$ is pure of weight 0, so in particular

Prediction 4.2. *For every V that is geometric and pure, $H_g^1(G_K, \mathrm{ad}V) = 0$.*

This prediction can be seen as an infinitesimal variant of the Fontaine-Mazur conjecture. Indeed, $H_g^1(G_K, \mathrm{ad}V)$ can be seen (see Kisin's lectures) as the tangent space of the deformation functor of V that parameterizes deformation that stay de Rham at all places dividing p, and unramified at almost all places, that is of deformations that stay "geometric". Now, if the Fontaine-Mazur conjecture is true, all geometric representations come from geometry, so obviously there are at most a countable number of such representations, which is not enough to make non-zero-dimensional families. Therefore, the tangent space to the (heuristic) "universal families of geometric representation" at V, which is (heuristically) $H_g^1(G_K, \mathrm{ad}V)$ should be 0.

The heuristic argument described above can actually be promoted to a proof in favorable context, and indeed, we know for example 4.2 for most V attached to modular forms, due to work of Weston and Kisin, and for some higher-dimensional polarized V attached to automorphic form, using work of Clozel-Harris-Taylor.

An other interesting observation regarding Prediction 4.1 is

Theorem 4.1. *Prediction 4.1 implies Prediction 1.2, that is if V is a pure geometric representation of weight w, then the Hodge-Tate weights of V are placed symmetrically with respect to $w/2$, that is $m_k = m_{w-k}$ for all k.*

The proof is given in the following exercise.

Exercise 4.1. a.– Prove first that is enough to prove Prediction 1.2 for $K = \mathbb{Q}$. Then prove that is also enough to prove it for K a quadratic imaginary field where p is split.

We henceforth assume that K is a quadratic imaginary field, and that p is split in K. We call v and v' the two places of K above p. Let V be a p-adic representation of G_K of dimension d, which is geometric and pure of weight w. Let $k_1 \leq \cdots \leq k_d$ be the weights of ρ at v and $k_1' \geq \cdots \geq k_d'$ be the weights of ρ at v'; the aim is to prove that if Prediction 4.1 holds then we have $k_i + k_i' = w$ for all i.

Here is a list of steps toward this goal. First, two preliminary results.

b.– Assume Prediction 4.1. Show that if V is pure of weight 0 and of dimension d, we have

$$\sum_{k<0} m_k(V) \le d, \quad \sum_{k>0} m_k(V) \le d, \quad \sum_{k\le 0} m_k(V) \ge d, \quad \sum_{k\ge 0} m_k(V) \ge d.$$

(Hint: Apply Theorem 2.2 and its following remark to V and V^* to prove the first two inequalities.)

c.– Show that for every $(a,b) \in \mathbb{Z}^2$ there exists a geometric Galois character χ of G_K whose Hodge-Tate weight at v is a and Hodge-Tate weight at v' is b. Show that such a character is pure of motivic weight $a + b$. Note that it is equivalent to prove Prediction 1.2 for V or for $V \otimes \chi$.

Now we take V as in the statement, and we always assume that Prediction 4.1 id true.

d.– Show that it is enough to prove that $k_1 + k_1' = w$ (for once it is done you could apply this result to $\Lambda^i V$ for all $i = 1, \ldots, d$).

e.– Deduce from c.– that it is enough to prove d.– in the case $w = 0$.

f.– So assume that we are in the case $w = 0$ and that $k_1 + k_1' = a$. If $a = 0$ we are done (well, you are done, because I have been done for long). By the operation $\rho \mapsto \rho^*$, the cases $a > 0$ and $a < 0$ are symmetric, so one can as well assume $a > 0$. Show that $a = 1$. (hint: using c.– we can replace V by the twist of motivic weight 0 such that $k_1' = 1$; so we have $k_1 = a - 1 \ge 0$. Using b.–, show that actually $k_1 = 0$.)

g.– Keeping the notations and hypotheses of f.– we see that the only possibilities for a are therefore 1, -1, or 0 in which case we hare done. Apply the same result to $V \otimes V$ to show that a cannot be ± 1. Therefore $a = 0$, QED.

4.2. Stability properties for the Bloch-Kato conjecture.

4.2.1. *Compatibility with the functional equation.* This is the following statement.

Theorem 4.2. *Assume that Conjectures 3.1 and 3.2 hold for V, and also Predictions 1.2 and 1.3. Then the Bloch-Kato conjecture for V is equivalent to Bloch-Kato conjecture for $V^*(1)$.*

The same is true for each inequality in Bloch-Kato conjecture, that is: (13) holds for V if and only if (13) holds for $V^*(1)$, and similarly for (12).

Proof — We only need to show that

$$(14) \quad \mathrm{ord}_{s=0} L(V, s) - \mathrm{ord}_{s=0} L(V^*(1), s) = \dim H^1_f(G_K, V^*(1))$$
$$- \dim H^0(G_K, V^*(1)) - (\dim H^1_f(G_K, V) - \dim H^0(G_K, V))$$

Since this relation is symmetric in V and $V^*(1)$, we can assume that

$$w \ge -1.$$

We first compute the LHS of (14). By the functional equation (conjecture 3.2), we have $\mathrm{ord}_{s=0}\Lambda(V,s) = \mathrm{ord}_{s=0}\Lambda(V^*(1),s)$. By Lemma 3.3, we have

$$\mathrm{ord}_{s=0}L(V,s) = \mathrm{ord}_{s=0}\Lambda(V,s) + \sum_{0\le k<w/2} m_k \text{ if } w \text{ is odd}$$

$$\mathrm{ord}_{s=0}L(V,s) = \mathrm{ord}_{s=0}\Lambda(V,s) + \sum_{0\le k<w/2} m_k + a^+ - m_{<w/2} \text{ if } w \text{ is even}$$

$$\mathrm{ord}_{s=0}L(V^*(1),s) = \mathrm{ord}_{s=0}\Lambda(V^*(1),s)$$

We thus get

$$\mathrm{ord}_{s=0}L(V,s) - \mathrm{ord}_{s=0}L(V^*(1),s) = \sum_{0\le k<w/2} m_k \text{ if } w \text{ is odd}$$

$$\mathrm{ord}_{s=0}L(V,s) - \mathrm{ord}_{s=0}L(V^*(1),s) = \sum_{0\le k<w/2} m_k + a^+ - m_{<w/2} \text{ if } w \text{ is even}$$

We now compute the RHS of (14). By the duality formula for Bloch-Kato Selmer group Theorem 2.2 this RHS is

$$\sum_{v|\infty} \dim H^0(G_v,V) - \sum_{v|p} \dim D_{\mathrm{dR}}(V_{|G_v})/D_{\mathrm{dR}}^+(V_{|G_v}) = a^+ - \sum_{k<0} m_k,$$

the last equality coming from the definition of a^+ and of m_k (see Remark 2.3)

Therefore, in the case w odd, the formula (14) that we need to prove becomes

$$\sum_{0\le k<w/2} m_k = a^+ - \sum_{k<0} m_k.$$

Grouping terms, this is equivalent to $\sum_{k<w/2} m_k = a^+$, that is $m_{<w/2} = a^+$, which follows from Predictions 1.2 and 1.3.

In the case w even, the formula (14) that we need to prove becomes

$$\sum_{0\le k<w/2} m_k + a^+ - m_{<w/2} = a^+ - \sum_{k<0} m_k,$$

which is obviously true. $\square$

Of course there are many conjectures to assume in order to make the above a non-conditional theorem. However, in practice, for the V we work with (e.g. automorphic V), we know all of them.

This compatibility result is, in my humble opinion, the most convincing single piece of evidence for the conjecture of Bloch-Kato. The functional equation relating $L(V,s)$ and $L(V^*(1),-s)$ on the one hand, and the duality formula relating $H^1_f(G_K,V)$ and $H^1_f(G_K,V^*(1),s)$ belong to two different paths in the history of mathematics, the first one to the analytic ideas (often based on Poisson's summation formula) initiated by Riemann in his study of the zeta functions, the second to the world of duality theorems in cohomology. That they give compatible formulas in the context of the Bloch-Kato conjecture seems to me a strong argument in favor of a deep link between L-functions and Selmer groups.

Corollary 4.1. *Same hypothesis as in the theorem above. Assume also that V is pure of weight $w \neq -1$. Then the lower bound (12) in Bloch-Kato conjecture hold for V.*

Proof — If the weight w satisfies $w \geq 0$, then we have seen in (4.1.3) that the RHS of the Bloch-Kato conjecture is 0, so the inequality (12) obviously holds for V. If the weight w of V satisfies $w \leq -2$, then the weight of $V^*(1)$ is ≥ 0, so (12) holds for $V^*(1)$. Therefore it holds for $V^*(1)$ by theorem 4.2. $\qquad\square$

This important result features the difference between the case $w \neq -1$ (where one only needs to prove the upper bound in the Bloch-Kato conjecture), and the case $w = -1$ (where one needs to prove both the upper and the lower bound).

4.2.2. *Compatibility with induction.*

Proposition 4.1. *If K_0 is a subfield of K, then if the Bloch-Kato conjecture holds for V if and only if it holds for $Ind_{G_K}^{G_{K_0}} V$*

This is true because both the left hand side and the right hand side of the conjectural formula are invariant by inductions. Most of the arguments necessary to prove this have been seen above. Collecting them is left as an exercise.

In particular, it is enough to prove the Bloch-Kato conjecture for $K = \mathbb{Q}$.

4.2.3. *A slightly more general conjecture.*

Conjecture 4.2. *Let S be any finite set of primes of K. We have*

$$(15) \qquad \dim H^1_{f,S}(G_K, V^*(1)) - \dim H^0(G_K, V^*(1)) = \mathrm{ord}_{s=0} L_S(V, s).$$

The classical Bloch-Kato conjecture is the case $S = \emptyset$.

Exercise 4.2. (easy) Show that this holds in the case $V = \mathbb{Q}_p$

Proposition 4.2 (Fontaine, Perrin-Riou)**.** *If Prediction 2.1 and conjecture EC1 hold for V, the above conjecture for a set S (and a given K, V) is equivalent to the conjecture for any other set S' (and the same K, V).*

Proof — We may assume that $S \subset S'$, and by induction on the cardinality of $S' - S$, that $S' = S \cup v$. In this case, by Prediction 2.1, changing S to S' adds to the RHS of (15) the term $\dim D_{\mathrm{crys}}(V_{|G_v})^{\phi=1}$ if $v|p$, (resp. $H^0(G_v, V)$ if $v \nmid p$), that is, assuming conjecture EC1, the multiplicity of the eigenvalue 1 of the crystalline Frobenius $\varphi = \phi^{f_v}$ (resp. the Frobenius) on $D^{\mathrm{crys}}(V_{|G_v})$ (resp. on V^{I_v}). Changing S to S' adds to the LHS the the order of the pole of the local factor $L_v(V, s)$ at $s = 0$. By the definitions 9 and 8 of those local factors, it is clear that we get the same terms as for the RHS. $\qquad\square$

4.3. **Results in special cases.**

4.3.1. *The case $V = \mathbb{Q}_p(n)$.* The Bloch-Kato conjecture is known for all number fields K and all integers n for $V = \mathbb{Q}_p(n)$, and more generally, all representations of the form $V = A(n)$ where A is an Artin character. Indeed, the lower bound in the Bloch-Kato conjecture results from what we have said since the motivic weight $-2n$ of $A(n)$ is never -1. The upper bound is a consequence of a theorem of Soulé relating K-theory and Galois cohomology, together with Borel's computation of the K-theory of number fields.

So in particular, for $K = \mathbb{Q}$ and $n \in \mathbb{Z}$ we have $\dim H^1_f(G_\mathbb{Q}, \mathbb{Q}_p(n)) = 1$ if $n = 3, 5, 7, 9, \ldots$ and is 0 otherwise.

4.3.2. *The case of elliptic curves over $\mathbb{Q}$ and classical modular forms.* Let $E/\mathbb{Q}$ be an elliptic curve and $V = V_p(E)(n)$ for some integer n. Or more generally, let f be a modular eigenform of level $\Gamma_1(N)$ that we assume, for the simplicity of exposition, of trivial nebentypus and even weight $k = 2k'$ (and say $p \nmid N$); take $V = V_p(f)(n)$ for some integer. The second case is indeed more general as since the Tanyama-Shimura-Weil conjecture proved by Breuil, Conrad, Diamond and Taylor, for $E/\mathbb{Q}$ an elliptic curve, there exist an f as above such that $V_p(f)(k') = V_p(E)$. For such V's, many partial results toward the Bloch-Kato conjecture are known.

In the case where $V = V_p(E)$, the Bloch-Kato conjecture is closely related to the Birch and Swinnerton-Dyer conjecture, so all results about the Birch and Swinnerton-Dyer conjecture give a result for the Bloch-Kato conjecture. For example, the combination of results of Gross-Zagier and Kolyvagin shows that for if $\mathrm{ord}_{s=0} L(V_p(E), s) \leq 1$, the Bloch-Kato conjecture is known for $V = V_p(E)$.

More generally for $V = V_p(f)(n)$, a striking result of Kato ([K]) shows that the upper bound in Bloch-Kato conjecture (13) is always true. The proof uses an Euler systems produced constructed by Kato, using ideas of Beilinson. Remember that the lower bound (12) is always known for V of weight different from -1. The bottom line is that the Bloch-Kato conjecture for $V = V_p(f)(n)$ is known for all n except $n = k' = k/2$ and that for $V_p(f)(k')$ only the lower bound needs to be proved.

So we now turn to the results for $V = V_p(f)(k')$ which has weight -1. This includes the case $V = V_p(E)$. Using his theory of "Selmer complex", Nekovar has shown that if f is ordinary at p,

$$\dim H^1_f(G_K, V) \equiv \mathrm{ord}_{s=0} L(V, s) \pmod 2.$$

This can be rephrased as *the parity of $\dim H^1_f(G_K, V)$ is the one predicted by the sign of the functional equation of $L(V, s)$.* In the case $V = V_p(E)$, this results has been recently extended (by similar methods) to the supersingular case by B.D. Kim, and been independently reproved by Dokchitser and Dokchitser.

4.3.3. *Automorphic methods.* There has been in recent years many results proving existence of non-trivial elements in $H^1_f(G_K, V)$ by automorphic methods. All those

methods are cousin, their common grand-parents being Ribet's proof of the converse of Herband's theorem (See Chris' lecture) and the theory of endoscopy and CAP forms for automorphic representation.

For example, for $V = V_p(f)(k')$ as in the preceding §, and for p ordinary, Bellaïche and Chenevier in the CM case (proved in 2002) and Skinner and Urban in the general case (announced in 2002, proved in 2005), have given an automorphic construction of a non-zero element in $H^1_f(G_K, V_p(f)(k'))$ under the assumption that the sign of $L(V_p(f), s)$ is -1. This proves that $\dim H^1_f(G_K, V) \geq 1$ if $\mathrm{ord}_{s=0}L(V)$ is odd. This is of course contained in Nekovar's result (and this is also in the CM case, a consequence of the proof of the Iwasawa conjecture for quadratic imaginary field by Rubin), but it is interesting to have a real construction of the extension in the H^1_f.

This hypothesis of ordinarity of p for f has been removed by Bellaïche and Chenevier ([BC2] if $k > 2$ (2006) and [B] if $k = 2$ (2009)). Actually this is a special case of a similar result valid for all automorphic representations V of G_K of dimension n that are polarized (for $\tau = \mathrm{Id}$ in the case $K = \mathbb{Q}$ or for τ the complex conjugation in the case K a quadratic imaginary field, with some restrictions at places dividing p) in [BC2]. A similar result has been announced by Skinner and Urban (in 2006 [SU], but the proof is not yet available in August 2011), in which the hypothesis that $\mathrm{ord}_{s=0}L(V, s)$ is odd has been weakened to $\mathrm{ord}_{s=0}L(V, s) \geq 1$.

5. Complement: a conjecture about the full H^1

5.1. **Motivation.** We have all but forgotten the space $H^1(G_{K,\Sigma}, V)$ for V a p-adic geometric representation of G_K, K a number field, and Σ a finite set of places of K containing all places above p and ∞, focussing instead on its subspace $H^1_f(G_K, V)$. Even if the H^1_f seemed more complicated at the beginning, we have seen that it was this subspace that has the nicest number-theoretical (and also motivic) interpretation, and also the simplest duality theory. So one could say: why should we care about the full $H^1(G_{K,\Sigma}, V)$? There are actually many reasons we should.

For one thing, simplicity is important, and it is quite frustrating, almost fifty years after the pioneers' work on Galois cohomology, not to be able to compute the dimension of $H^1(G_{K,\Sigma}, V)$ even for the most simple V.

Also, those spaces have also a number-theoretical significance, though quite different from the H^1_f or H^1_g. Admittedly, the $H^1(G_{K,\Sigma}, V)$ have no motivic or K-theoretical interpretation. But, for example, computing the dimension of $H^1(G_{K,\Sigma}, \mathbb{Q}_p)$ (for Σ any finite set of places containing those above p) is equivalent to proving (or disproving) the famous Leopoldt's conjecture, whose classical statement is: *the natural map $\iota : \mathcal{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \prod_{v|p} \mathcal{O}_{K_v}^*$ is injective.* This conjecture is ubiquitous in algebraic number theory, and has proved very elusive: there have been many released proofs by eminent or less eminent mathematicians which have been found faulty, and certainly many more which were refuted by their own author or a friend

before any public release[2]. But despite its importance in algebraic number theory, there is a sense that it properly belongs to transcendence theory, due in part to the fact that the two main known partial results (the proof in the case where K is abelian over $\mathbb{Q}$ or over a quadratic imaginary field by Brummer, and a lower bound on the rank of the image of ι by Waldschmidt) have proofs using heavily methods of transcendence theory. Therefore, predicting the dimension of $H^1(G_{K,\Sigma}, V)$ for various V can be seen as a generalized Leopoldt's conjecture, and can hardly be considered as non-important for number theory.

Let us add that the knowledge of the dimension of the $H^1(G_{K,\Sigma}, V)$ (and of the $H^2(G_{K,\Sigma}, V)$, which is essentially equivalent by the Euler Characteristic formula) would be useful in many situations. For example, it is needed to compute tangent spaces and obstructions in Galois deformation theory. Also, if X is a variety over K and if we want to compute the étale cohomology $H^1_{\text{ét}}(X, \mathbb{Q}_p)$ (the true cohomology of X/K this time, not of $X \times_K \bar{K}$ that we have denoted $H^i(X, \mathbb{Q}_p)$ earlier), then the natural way to proceed is to use the Grothendieck's spectral sequence $H^i(G_K, H^j_{\text{ét}}(X \times_K \bar{K}, \mathbb{Q}_p)) \Rightarrow H^{i+j}_{\text{ét}}(X, \mathbb{Q}_p)$, but this takes to know how to compute the Galois cohomology of the geometric representation $H^j_{\text{ét}}(X \times_K \bar{K}, \mathbb{Q}_p)$.

5.2. Jannsen's conjecture.

Proposition 5.1. *Let V be a p-adic geometric representationof $G_{K,\Sigma}$ and let $W = V^*(1)$. The following are equivalent:*

(i) *The natural map $H^1(G_{K,\Sigma}, W) \to \prod_{v \in \Sigma} H^1(G_v, W)$ is injective.*

(ii) *One has*

$$\dim H^1(G_{K,\Sigma}, V) = [K:\mathbb{Q}] \dim V + \dim H^0(G_{K,\Sigma}, V) - \dim H^0(G_{K,\Sigma}, V^*(1))$$
$$+ \sum_{v \in S, \ v \text{ finite}} \dim H^0(G_v, V^*(1)) - \sum_{v|\infty} \dim H^0(G_v, V)$$

(iii)

$$\dim H^2(G_{K,\Sigma}, V) = \sum_{v \in S, \ v \text{ finite}} \dim H^0(G_v, V^*(1)) - \dim H^0(G_{K,\Sigma}, V^*(1))$$

Moreover, in (ii) and (iii), the LHS is never less that the RHS.

Let us note that in $\prod_{v \in \Sigma} H^1(G_v, W)$ in (i), we can restrict the product to the v that are finite, since $H^1(G_v, W) = 0$ for v an infinite place. The RHS of the formula computing the dimension of $H^1(G_{K,\Sigma}, V)$ in (ii) is easy to compute in practice. *Proof* — Let us call K_W thw kernel of the map (i). Propososition. 2.2

---

applied to $L_v = H^1(G_v, V)$ gives

$$\dim H^1(G_{K,\Sigma}, V) = \dim K_W \dim H^0(G_{K,\Sigma}, V) - \dim H^0(G_{K,\Sigma}, V^*(1))$$
$$+ \sum_{v \in S} (\dim H^1(G_v, V) - \dim H_0(G_v, V))$$

For a finite $v \in S$, $\dim H^1(G_v, V) - \dim H^0(G_v, V) = \dim H^0(G_v, V^*(1))$ if v does not divides p, and $\dim H^1(G_v, V) - \dim H^0(G_v, V) = \dim H^0(G_v, V^*(1)) + [K_v : \mathbb{Q}_p] \dim V$ when v divided p (cf. Prop. 2.2). Summing, we get that the LHS of (ii) is equl to the RHS of (ii) plus $\dim K_W$. The equivalence between (i) and (ii) follows, as well as the fact that $\geq$ in (ii) always hold. For the equivalence between (ii) and (iii), one just applies the Euler characactersitic formula. $\qquad \square$

In 1989, a few months before Bloch and Kato, Jannsen asked ([J, Question 2, page 349]) wether the following statement hods,

Conjecture 5.1 (Jannsen). *Let V be a representation coming from geometry of $G_{K,\Sigma}$ which is pure of weight w. Assume that $w \neq -1$. Then the statements (i), (ii) and (iii) of the proposition above hold.*

Remark 5.1.   (a) While Jannsen is prudent and formulates it as an *open question* rather than a *conjecture*, we call it a conjecture without hesitation because in the case $w > -1$ (where w is the weight of V), Jannsen himself calls the statement (iii) a conjecture (cf. [J, case(b) of Conjecture (i)]) and provides serious evidence ([J, §4]) in its favor, while in the case $w < -1$, the weight $-2 - w$ of W is ≥ 0, so Prediction 4.1 (which is itself a consequence of either the conjecture of Bloch and Kato, or of Grotehendieck's yoga of weights) implies $H^1_f(\mathbb{G}_K, W) = 0$ which clearly implies (i).

    (b) The condition $w \neq -1$ is fundamental: If $V = V_p(E)$ where $E/\mathbb{Q}$ is an elliptic curve, the conjecture, extended to the case $w = -1$ would predict that $\dim H^1(G_{\mathbb{Q},\Sigma}, V_p(E)) = 1$. But we know that already the dimension of the subspace $H^1_f(G_{\mathbb{Q},\Sigma}, V_p(E))$ is at least the rank of $E(\mathbb{Q})$ and of course there are examples of E with $\mathrm{rk}E(\mathbb{Q}) > 1$. To my knowledge, there is no general conjecture predicting the dimension of $H^1(G_{K,\Sigma}, V)$ in the case $w = -1$.

The following consequence of Jannsen's conjecture is interesting:

Prediction 5.1. *Let V be a p-adic representation coming from geometry of $G_{K,\Sigma}$ which is pure of weight w. Assume that $w \neq -1$, and that $H^0(G_v, V) = 0$ for every finite $v \in S$ that does not divide v. Assume Jannsen's conjecture (for $V^*(1)$). Then the regulator map*

$$H^1_f(G_{K,\Sigma}, V) \to \prod_{v|p} H^1_f(G_v, V)$$

is injective.

Proof —   The map $H^1_f(G_{K,\Sigma}, V) \to \prod_{v \in S} H^1_f(G_v, V)$ is injective because its a restriction of the map $H^1(G_{K,\Sigma}, V) \to \prod_{v \in S} H^1(G_v, V)$ which is injective by Jannsen's conjecture. If $v \in S$ is finite and does not divide p, then by Prop. 2.3(a), $\dim H^1_f(G_v, V) = \dim H_0(G_v, V) = 0$. The prediction follows. $\square$

Exercise 5.1. (easy) For K a number field, and any Σ, show that Jannsen's conjecture is equvalent to Leopoldt's conjecture for K.

Exercise 5.2. 1.– **(easy)** Show that the conjecture predicts the following values for $d_n := \dim H^1(G_{\mathbb{Q},S}, \mathbb{Q}_p(n))$ where $n \in \mathbb{Z}$ and $S = \{p, \infty\}$: $d_n = 0$ if n is even, $n \neq 0$; $d_0 = 1$; $d_n = 1$ if n is odd.

2.– Using the fact that the conjecture of Bloch and Kato is known for $G_{\mathbb{Q},S}$, $V = \mathbb{Q}_p(n)$, show that the conjecture of Jannsen holds excepet may be for $n < 0$ even. What does (i) say for those V?

3.– **(difficult)** Show that if p is a regular prime, Jannsen's conjecture holds for $V = \mathbb{Q}_p(n)$, all n. (Use Iwasawa's main conjecture proved by Mazur-WIiles and independently by Kolyvagin)

In general, for p irregular, Jannsen's conjecture for $G_{\mathbb{Q},S}$, $V = \mathbb{Q}_p(n)$, is still open.

Exercise 5.3. (difficult) Justify the following prediction: for $E/\mathbb{Q}$ an elliptic curve with good reduction outside Σ. $\dim H^1(G_{\mathbb{Q},\Sigma}, V_p(E)) = \max(1, \mathrm{rk} E(\mathbb{Q}))$

Exercise 5.4. (difficult) Let $(V_n)_{n \in \mathbb{N}}$ and V be geometric Galois representations of $G_{K,\Sigma}$. Let T_n and T be the trace of V_n and V respectively. Assume that (T_n) converges uniformly to T.

a.– Assume Jannsen's conjecture, and that V_n and V satisfy its condition. Show that $\liminf_{n \to \infty} \dim H^1(G_{K,\Sigma}, V_n) \leq \dim H^1(G_{K,\Sigma}, V)$.

b.– Show by an example that this property of lower semi-continuity does not hold if H^1 is replaced by H^1_f.

c.– Can you prove a.– without assuming Jannsen's conjecture?

References

[An]   Yves André, *Une introduction aux motifs*, Panoramas et Synthèses, 17, Paris: Société Mathématique de France,

[A]   Andreatta, this volume

[B]   J. Bellaïche, *rank of Selmer groups in analytic families*, preprint (2009).

[BC1] J. Bellaïche & G. Chenevier, *Formes automorphes non tempérées et conjectures de Bloch-Kato*, Annales de l'ENS (2004). Also available on arxiv 02

[BC2] J. Bellaïche & G. Chenevier, *p-adic Families of Galois representations*, Astérisque, 324, SMF (2009). Also available on arxiv 0602340 (2006).

[BK]   Bloch & Kato, *Tamagawa Numbers of Motives* in *The Gorthendieck festschrift*, vol. 1, Progress in Math 89, Birkhauser, 1990

[C]   F. Calegari, *Even Galois Representations and the Fontaine-Mazur conjecture*, preprint, available on http://www.math.northwestern.edu/ fcale/

[Co]   B. Conrad & , Lectures, this volume.

[CNF]   *Cohomology of number fields*, Springer.

[FPR]   J.-M. Fontaine & B. Perrin-Riou, *Autour des conjectures de Bloch et Kato*, Motives, PSPM 55, volume 1.

[H]   M. Harris, *Hodge-De Rham structures and periods*, in [JKS], part 2, pages 573–624.

[I]   H. Iwaniec & E. Kowalski, *Analytic number theory*, AMS colloquium Publications, volume 53 (2004)

[J]   U. Jannsen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology*, in *Galois groups over* $\mathbb{Q}$ (Berkeley, CA, 1987), 315–360, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[JKS]   U. Jannsen, S. Kleiman, J.-P. Serre, editors, *Motives*, American Math. Society, PSPM 55.

[Ki]   M. Kisin, Lectures, this volume

[K]   K. Kato, $\mathfrak{p}$-*adic Hodge theory and values of zeta functions of modular forms*, 295 (2004), pp. 117–290.

[M]   S. Morel, *On the cohomology of certain non-compact Shimura varieties*, to appear in the Annals of Mathematics Studies, available on http://www.math.ias.edu/ morel/

[Mi]   J. Milne, *Arithmetic duality theorems*.

[N1]   J. Nekovar, *On the parity of ranks of Selmer groups II*, Comptes Rendus de l'Acad. Sci. Paris, Serie I, 332 (2001), No. 2, 99–104.

[N2]   J. Nekovar, *Selmer complexes*, S.M.F. Astérisque 310 (2006).

[R]   K. Rubin, Euler Systems, Annals of Math. Studies 147, (2000)

[SU]   C. Skinner & E. Urban, *Sur les déformations p-adiques de certaines représentations automorphes*, Journal Inst. Math. Jussieu **5**(4) (2006).

[SU]   C. Skinner & E. Urban, *Vanishing of L-functions and ranks of Selmer groups*, in International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zurich, 2006, pp. 473–500.

[Silverman] J. Silverman, *Arithmetic theory of Elliptic curves*, GTM, Springer

[Sh]   S. W Shin, *Odd-dimensional Galois representations arising from some conpact Shiura varieties*, preprint.

[S1]   J.-P. Serre *Facteurs locaux des fonctions Zeta des variétés algébriques*, Séminaire Delange-Pisot-Poitou, 1969/1970, numéro 19

[S2]   J.-P. Serre, *Cohomologie Galoisienne*, Springer

[T]   John Tate, *Relations between K_2 and Galois cohomology*, Inventiones Math. 36, 257–274.

[Tay1]   R. Taylor, *Remarks on a conjecture of Fontaine and Mazur* Journal of the Institute of Mathematics of Jussieu 1 (2002), 1–19.

[Tay2]   R. Taylor, *Galois representations*, long version of the talk given at the iCM 2002, available on http://www.math.harvard.edu/ rtaylor

[W]   C. Weibel, *Trieste Lectures on the Bloch-Kato conjcture*, http://www.math.rutgers.edu/ weibel/papers-dir/Bloch-Kato.pdf

E-mail address: `jbellaic@brandeis.edu`

Math Department, MS 050, Brandeis University, 415 South Street, Waltham, MA 02453