An introduction to Bloch and Kato's conjecture

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, 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 needs 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 will 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}, and 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.

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

Contents

1. Geometric Galois representations 4
1.1. Representations coming from geometry 4
1.2. Geometric representations 6
1.3. Appendix: Motives 11
2. Bloch-Kato Selmer groups 12
2.1. Reminder of Galois cohomology 12
2.2. The local Bloch-Kato Selmer groups at places dividing p 22
2.3. Global Bloch-Kato Selmer group 28
3. L-functions 32
3.1. L-functions 32
3.2. The functional equation 36
4. The Bloch-Kato conjecture 40
4.1. The conjecture 40
4.2. Stability properties for the Bloch-Kato conjecture 42
4.3. Results in special cases 45
5. Complement: a conjecture about the full H^1 46
5.1. Small talk 46
5.2. The Jannsen's conjecture 47
References 48

The aim of those lectures is to introduce and to explain the number-theoretical significance of the conjecture of Bloch and Kato. This conjecture appeared in print in 1990 in The Grothendieck Festschrift, 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, still depend on unproved conjectures. A consequence is that there are several formulations of this

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") 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 proof of many results unavoidably requires a detour in characteristic p. Yet I believe that it may be easier to get a global picture of those huge sets 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) of proper and smooth variety X over K. It is conjectured (the Fontaine-Mazur conjecture) that every geometric 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). 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 that forms (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 $s = 1$

(where V^* is the dual representation of V). Motivation, examples, and stability properties of that conjecture are discussed in §4.

1. Geometric Galois representations

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

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

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 topological spaces).

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

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 $\operatorname{Spec} \mathcal{O}_{(v)}$ such that $\mathcal{X} \times \operatorname{Spec} K \simeq X$. 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 $|\mathcal{X}_v(k_v)| = \sum_{i=0}^{2n}(-1)^i \mathrm{tr}(\mathrm{Frob}_v)_{H^i(X,\mathbb{Q}_p)}$.

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. This will be discussed in Andreatta's lectures.

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. This maps extend 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 v is prime to p, and if X has good reduction at v, then the operator Frob_v of $H^i(X,\mathbb{Q}_p)$ is semi-simple (that is diagonalizable over $\bar{\mathbb{Q}}_p$.)

This is called the *semi-simplicity of Frobenius*. There are also variants for places v that divides p, and places with bad reduction. This 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 the Tate's conjecture, still widely 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 known for abelian representation (by 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), and now also for all representations of V of dimension 2 of $G_{\mathbb{Q}}$ that are odd and with distinct Hodge-Tate weights (by works of Kisin and others explained in this conference). It 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'-rational 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 precise the set Σ', we say *Σ'-pure*.

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

Exercise 1.3. 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 representations 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 $i - 2n$. □

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.*

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 weight, 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

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

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 $W = Ind_{G_K}^{G_{K_0}} V$, 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.*

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

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. □

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 $H^i(X)$.

There are actually stronger relations among the Hodge-Tate weights, but we need to assume conjectures EC2 and EC3 to prove them. Let us just mention two of them without proof (but see Exercise 1.7):

Prediction 1.2. *Let V be a p-adic representation of G_K coming from geometry. Assume Tate's conjecture (EC3). 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

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

then we have $[K:\mathbb{Q}]\dim V = 2m_{<w/2}$ is w is odd, and $[K:\mathbb{Q}]\dim V = 2m_{<w/2} + m_{w/2}$ if w is even.

We can say something more precise. Let

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

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 proved), 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 true), 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. In particular, representations attached to modular eigenforms of weight $k > 2$ (they have Hodge-Tate weights 0 and $k-1$) are odd (that is, the eigenvalue of c are 1 and -1).

Exercise 1.7. (difficult)

a.– 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.)

b.– In general, when K is any number field and V is a only a sub-quotient of an $H^i(X, \mathbb{Q}_p)$, how would you deduce the predictions from EC2 and EC3? (Hint: you can give a look at §1.3 for inspiration).

1.2.4. *Automorphic Galois representations.* We can not seriously discuss here the fundamental subject of automorphic forms and of 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 only 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 coefficient 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 there is no canonical splitting of this filtration in general, but there is one is $K = \mathbb{C}$. 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 structure of weight i* (see the definition below) ; $(H^i_\iota(X, \mathbb{Z}), H^i_{\mathrm{dR}}(X), u, (H^p(X \times \mathrm{Spec}\, \mathbb{C}, \Omega^q)_{p,q\in\mathbb{N},p+q=i})$.

Definition 1.5. A K-Hodge structure (where K is a subfield or $\mathbb{C}$, or when an embedding $\iota : K \to \mathbb{C}$ is given) is a 4-uple $(V_{\mathbb{Z}}, V_K, u, (V_{p,q})_{p,q\in\mathbb{Z}^2})$ where V_Z is a finite $\mathbb{Z}$-module, V_K a finite K vector space, u is an isomorphism $V_K \otimes_{K,\iota} \mathbb{C} \to V_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{C}$, $(V_{p,q})$ is a finite family of subspacse 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 $u(V_{\mathbb{Z}} \otimes \mathbb{R})$, 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 $\mathbb{Q}$-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 *standard conjectures* (Hodge and Lefschetz). If such standard conjectures were known and the category $\mathcal{M}_K$ constructed, then for $K = \mathbb{C}$ the functor $M \to \mathrm{Hodge}(M)$ would be fully faithful (this is the content of the Hodge conjecture). Analogously, for K a number field, the Tate EC3 and Grothendieck-Serre conjecture EC2 would imply that for any prime p the functor Real_p from $\mathcal{M}_K$ to the category of p-adic representations of G_K coming from geometry is an equivalence of categories. 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 we say, 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 to V we should be able to attach a K-Hodge structure $\mathrm{Hodge}(M)$.

2. Bloch-Kato Selmer groups

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 lecture.)

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 Fin$(p,1)$ nor Fin$(p,2)$ However, show that if Σ is a finite set of places, $G_{K,\Sigma}$ satisfies Fin(p). (use a.– and global class field theory for Fin$(p,1)$; use b.– and the theory of the Brauer group for Fin$(p,2)$. There is almost nothing to prove (e.g. [S2, Chapter II, §4.4]) for the other cases Fin(p,i), with $i > 2$).

We shall be concerned with continuous group cohomology $H^i(G,V)$ of profinite groups G satisfying 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 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 $F(p)$, 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 Fin(p) and the long exact sequences, the groups $H^i(U,A)$ are finite. By the Hochschild-Serre spectral sequence $H^i(G/U, H^j(U,A)) \to H^{i+j}(G,A)$, and since G/U is finite, the groups $H^i(G,A)$ are finite. □

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 $g_1,\dots,g_k$ be cocycles that represent a generating family of Y. Suppose $x_n \in H^i(G,\Lambda)$, $n = 0,1,2,\dots$, 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. □

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 $g_1,\dots,g_m$ 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. □

Now assume that Λ is free as a 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 $0 \to \Lambda \to V \to W \to 0$. Let $\delta_i : H^{i-1}(G, W) \to H^i(G, \Lambda)$ be the connecting morphism.

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 $H^i(G, \Lambda)$. □

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).

Now consider the $C^i(G, A)$ the continuous i-cochains from G to 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 an 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 map" 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:

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

Taking the long exact sequence, we get

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

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 maps $g \mapsto c_y(g)$ is a 1-cocycle from G_K to $A[p^n](\bar{K})$. It therefore has a class $\bar{c}_y$ in $H^1(G_K, A[p^n](\bar{K}))$. We claim that this class does not depends 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 that K is perfect to simplify. 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 $\operatorname{Spec} \bar{K}$ is an étale cover of $\operatorname{Spec} K$) 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 locally (for some Grothendieck topology) trivial object are classified by the H^1 (on the same topology) of the automorphism group sheaf of the corresponding trivial objects, such torsors are classified by the $H^1_{\text{ét}}(\operatorname{Spec} K, A[p^n]) = H^1(G_K, A[p^n](\bar{K}))$. 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 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 $H^1_{\mathrm{ur}}(G_K, V) = \ker(H^1(G_K, V) \to H^1(I_K, V))$

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 correspond 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

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

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, $\dim H^1_{\mathrm{ur}}(G_K, V) = \dim H^0(G_K/I_K, V^{I_K}) = \dim H^0(G_K, V)$. 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 $H^1_{\mathrm{ur}}(G_K, V) \otimes H^1_{\mathrm{ur}}(G_K, V^*(1))$ 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 $\dim H^1_{\mathrm{ur}}(G_K, V) + \dim H^1_{\mathrm{ur}}(G_K, V^*(1)) = \dim H^1(G_K, V)$. 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 $H^1_{\mathrm{ur}}(G_K, V) \neq H^1(G_K, V)$ is $V = \mathbb{Q}_p(1)$. Show that in this case $H^1_{\mathrm{ur}}(G_K, V) = 0$,

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 $\widehat{K^*} \otimes_{\mathbb{Z}} \mathbb{Q}_p$ with the subspace $H^1_{ur}(G_K, \mathbb{Q}_p(1))$ 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. Namely, that κ_n maps $\mathcal{O}_K^* \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}$ into $H^1_{\mathrm{ur}}(G_K, \mu_{p^n}(\bar{K}))$ which is defined as $\ker(H^1(G_K, \mu_{p^n}(\bar{K})) \to H^1(I_K, \mu_{p^n}(\bar{K})))$. Here $\mu_{p^n} = \mathbb{G}_m[p^n]$ denotes as usual the group scheme of p^n-root of 1).

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 $\operatorname{Spec} \mathcal{O}_K$, hence

locally trivial for the étale topology of $\operatorname{Spec}\mathcal{O}_K$, therefore the class $\kappa_n(x)$ of $T_{n,x}$ in $H^1_{\text{ét}}(\operatorname{Spec}K, \mu_{p^n}) = H^1(G_K, \mu_{p^n})$ lies in $H^1_{\text{ét}}(\mathcal{O}_K, \mu_{p^n}) = H^1(G_K/I_K, \mu_{p^n})$. QED.

Exercise 2.9. 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 $H^1_{\text{ur}}(G_K, V_p(E)) = 0$ 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. 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 2.10. Let V be an irreducible representation of dimension 2 of $G_{\mathbb{Q},\Sigma}$. Show that $\dim H^1(G_{K,\Sigma}, \mathrm{ad}V)$ 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 odd.

We also have an analog of local duality, but instead of one clear theorem it is a 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, 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 don't know if this lower bound is an equality. In exercise 2.10 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.*

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, $L_v = H^1_{\text{ur}}(G_v, V)$.

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 2.11. 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 $v \notin \Sigma$, $\mathcal{L}_v = H^1_{\text{ur}}(G_v, V)$. Show that $H^1_{\mathcal{L}}(G_K, V) = \ker\big(H^1(G_{K,\Sigma}, V) \to \prod_{v\in\Sigma} H^1(G_v, V)/L_v\big)$. In particular, $H^1_{\mathcal{L}}(G_K, V)$ is finite dimensional.

The most obvious choices for a component L_v of a Selmer structure are (0), $H^1(G_v, V)$ and of course $H^1_{\text{ur}}(G_v, V)$. When v is prime to p, those are the only L_v than one meets in practice. For v dividing p, see next §.

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 2.12. (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, 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 Taniyama-Weyl conjecture.

Exercise 2.13. 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 2.14. 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^1_f.* 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 $H^{\mathrm{ur}}_1(G_K, V)$ 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 $H^1_f(G_K, V) = \ker(H^1(G_K, V) \to H^1(G_K, V \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}))$.

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

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 $H^1_f(G_K, V)$ 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 $H^1_f(G_K, V)$ if and only if it is crystalline.*

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

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

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*

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

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

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

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

$$\begin{aligned} 0 \to H^0(G_K, V) &\xrightarrow{\alpha} D_{\mathrm{crys}}(V) \oplus D^+_{\mathrm{dR}}(V) \xrightarrow{\beta} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}(V) \\ &\to H^1(G_K, V) \xrightarrow{\alpha_1} H^1(G_K, V \otimes B_{\mathrm{crys}}) \oplus H^1(G_K, V \otimes B^+_{dR}) \\ &\xrightarrow{\beta_1} H^1(G_K, V \otimes B_{\mathrm{crys}}) \oplus H^1(G_K, V \otimes B_{dR}), \end{aligned} \tag{5}$$

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 $\ker \alpha_1 = H^1_f(G_K, V)$. The exact sequence (5) thus becomes

$$\begin{aligned} 0 \to H^0(G_K, V) &\overset{\alpha}{\to} D_{\mathrm{crys}}(V) \oplus D^+_{\mathrm{dR}}(V) \\ &\overset{\beta}{\to} D_{\mathrm{crys}}(V) \oplus D_{\mathrm{dR}}(V) \to H^1_f(G_K, V) \end{aligned} \tag{6}$$

Since the alternate sum of the dimension of the spaces in an exact sequence is 0, we get the result. □

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 the $t^i B_{\mathrm{dR}}/t^{i+1} B_{\mathrm{dR}} \simeq \mathbb{C}_p(i)$, 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 $\dim V = \dim_K D_{\mathrm{dR}}(V)$. □

Exercise 2.15. 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^1_f is simple and worth remembering. If $H^0(G_K, V) = 0$, then $\dim H^1_f(G_K, V)$ is $[K : \mathbb{Q}_p]$ times the number of negative Hodge-Tate weights of V.

Exercise 2.16. (easy) Show that if V is de Rham with all its Hodge-Tate weight positive, then $H^1_f(G_K, V)$ is 0. Show that V is de Rham with all its Hodge-Tate weights ≤ -2, then $H^1_f(G_K, V) = H^1(G_K, V)$.

Exercise 2.17. 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 2.18. 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 2.15 to $\dim H^0(G_K, V) + \dim H^0(G_K, V^*(1)) + [K : \mathbb{Q}_p] \dim V$, which is $\dim H^1(G_K, V)$.

Therefore, we only have to prove that the restriction of the cup product $H^1(G_K, V) \otimes H^1(G_K, V^*) \to H^2(G_K, \mathbb{Q}_p(1)) = \mathbb{Q}_p$ to $H^1_f \otimes H^1_f$ 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 sequences. This fact is used to guarantee the commutativity of the diagram below:

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

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. 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 proposition. □

Another indication of the strong analogy between H^1_f (when $l = p$) and H^1_{ur} (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 $H^1_f(G_K, \mathbb{Q}_p(1))$*

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, $\dim H^1_f(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p]$. 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 $\kappa(\mathcal{O}_K^*) \subset H^1_f(G_K, \mathbb{Q}_p(1))$. 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 $H^1_{\text{fppf}}(\operatorname{Spec} \mathcal{O}_K, (\mu_{p^n})_{\mathcal{O}_K}) = \operatorname{Ext}^1_{\text{fppf}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$. 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 $H^1_{\text{fppf}}(\operatorname{Spec} K, \mu_n) = H^1_{\text{ét}}(\operatorname{Spec} K, \mu_n) = H^1(G_K, \mu_n(\bar{K}))$, 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 $(E_{x,n})$ define 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, the Tate module W of E is crystalline. This proves that $\kappa(x) \in H^1_f(G_K, \mathbb{Q}_p(1))$ by Lemma 2.5. □

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 $E(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} H^1_f(G_K, V_p(E))$.*

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 s 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 correspond 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 2.19. a.– Using the exact sequence $0 \to \mathbb{Q}_p \to B^{\phi=1}_{\mathrm{crys}} \to B_{\mathrm{dR}}/B^+_{\mathrm{dR}}$, 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,

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

The "g" in H^1_g stands for *geometric* since geometric representations are de Rham. The "e" in H^1_e stands for "exponential". This explains the "f" in the H^1_f as f is just between e and g in the alphabetic order.

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 $H^1_e(G_K, V)$ is $H^1_g(G_K, V^*(1))$ and the orthogonal of $H^1_g(G_K, V)$ is $H^1_e(G_K, V^*(1))$.*

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

Exercise 2.21. Compute $\dim H^1_e(G_K, \mathbb{Q}_p(n))$, $\dim H^1_f(G_K, \mathbb{Q}_p(n))$, $\dim H^1_g(G_K, \mathbb{Q}_p(n))$, $\dim H^1(G_K, \mathbb{Q}_p(n))$ 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 2.22. (difficult) Let E be an elliptic curve over K. Show that

$$H^1_e(G_K, V_p(E)) = H^1_f(G_K, V_p(E)) = H^1_g(G_K, V_p(E)).$$

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 $l = p$.

$$\begin{array}{lccccccc} \text{case } l \neq p & & (0) & \subset & H^1_{\mathrm{ur}}(G_K, V) & \subset & H^1(G_K, V) & \\ \text{case } l = p & (0) \subset & H^1_e(G_K, V) & \subset & H^1_f(G_K, V) & \subset & H^1_g(G_K, V) & \subset H^1(G_K, V) \end{array}$$

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_{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 2.20). 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 $H^1_g(G_K, V) = H^1(G_K, V)$.

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.

Remember that by definition (see §2.2.3) $H^1_f(G_v, V)$ means $H^1_{\mathrm{ur}}(G_v, V)$ 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 $v \notin S$. 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,

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

  by Prop. 2.8

□

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.

Exercise 2.23. What does this theorem say when $V = V^*(1)$?

Exercise 2.24. a.– Show that $H^1_f(G_K, \mathbb{Q}_p) = 0$. (Hint: use the finiteness of the class group of K as well as Exercise 2.17.)

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

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

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

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

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 that 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 $x \in \mathcal{O}^*_{K,\Sigma} \otimes_{\mathbb{Z}} \mathbb{Q}_p$, $\kappa(x) \in H^1_f(G_K, \mathbb{Q}_p(1))$ if and only if $x \in \mathcal{O}^*_K$. Therefore κ induces an isomorphism $\mathcal{O}^*_K \otimes \mathbb{Q}_p \to H^1_f(G_K, \mathbb{Q}_p(1))$. □

The proof shows easily that $H^1_{f,S}(G_K, \mathbb{Q}_p(1)) \simeq \mathcal{O}^*_{K,S} \otimes \mathbb{Q}_p$, where $\mathcal{O}^*_{K,S}$ is the group of S-unit of 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 2.24, this result implies that $\operatorname{rk} \mathcal{O}_K^* = r_1 + r_2 - 1$, 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 that the Kummer map induces an injectionres $\kappa : E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \hookrightarrow \mathrm{Sel}_p(E)$ 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 $Sel_p(E) = H^1_f(G_K, V_p(E))$. In particular, the Kummer map induces an injection $E(K)\otimes_{\mathbb{Z}}\mathbb{Q}_p \to H^1_f(G_K, V_p(E))$ which is an isomorphism if and only if $Cha(E)[p^\infty]$ 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 $H^1_f(G_v, V_p(E))$; and since $v \not| p$, we have $H^1_f(G_v, V_p(E)) = H^1(G_v, V_p(E)) = 0$ by Exercise 2.9. □

This again shows that the H^1_f 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 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 $H^i : V_K \to \mathcal{MM}_K$ 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 $\text{Real}_p(N)$ 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 $\text{Fil}^w \text{Real}_p(N)$ 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 $V = \text{Real}_p(M)$ representing $x \in H^1_g(G_K, V)$, it is expected that W should be $\text{Real}_p(N)$ for some **mixed** motive $N \in \mathcal{M}_K$. Actually it is even expected that the functor Real_p induces an isomorphism between

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

where $\mathbb{Q}$ is the object of $\mathcal{M}_K$ such that $\text{Real}_p(\mathbb{Q}) = \mathbb{Q}_p$. 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 $\text{Spec}\, \mathcal{O}_K - S$ instead of $\text{Spec}\, K$.

Of course, the category of mixed motives $\mathcal{MM}_K$ has not 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) $\text{Ext}^1_{\mathcal{MM}_K}(\mathbb{Q}, M)$ using the K-theory of X (see [BK, page 359].) Bloch and Kato have conjectured ([BK, Conjecture 5.3]) that when $\text{Ext}^1_{\mathcal{MM}_K}(\mathbb{Q}, M)$ is defined this way, (7) holds. This **other** Bloch-Kato conjecture has now been proved.

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. To put aside trivialities, let us just state that in this case

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

In particular, when $V_{|G_v}$ has no quotient isomorphic to $\mathbb{Q}_p(1)$, one has

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

Exercise 2.25. Prove those relations.

The real challenge is when $V_{|G_v}$ has a quotient isomorphic to $\mathbb{Q}_p(1)$.

The rest of this § will be written after the conference.

3. L-functions

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 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

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

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 p^{-s}.

Note also that when V is algebraic, the coefficients of $\det((\mathrm{Frob}_v^{-1} q_v^{-s} - \mathrm{Id})_{|V^{I_v}})^{-1}$ 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 divides p, we set

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

where ϕ is the crystalline Frobenius to the power f_v, where $q_v = p_v^{f_v}$ where p_v is the prime dividing q_v.

Caveat: I am (not even completely, actually) sure that it is the correct formula only in the case where V is crystalline at v. Without access to the right books here in Hawaii, I can't check my memory that this is also the correct formula when V is only de Rham at v. This detail will be fixed after the conference.

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

Definition 3.1. We set formally (that is, as a power series in the variable p^{-s}),

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

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*.

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:

$$L(V(n),s) = L(V, s+n). \tag{10}$$

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 $\alpha_{1,v}, \ldots, \alpha_{dimV,v}$ 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 all 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) of the sum $\sum_{n \geq 1} |n^{w/2-s}| = \sum_{n \geq 1} n^{w/2 - \Re s}$, which is clear. □

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

Proof — The first assertion follows directly from the proposition. The second follows from the one if we observe that the missing factors $L_v(V,s)$ for $v \notin \Sigma$ are meromorphic functions with no zeros. □

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 was conjectured in 1859 by Riemann, who noticed that such a statement would imply 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. Riemann's argument that the non-vanishing of $\zeta_{\mathbb{Q}}$ on the line $\Re s = 1$ implies the prime number theorem was made completely rigorous later by Weierstrass. This non-vanishing result 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, Riemann also conjectured that $\zeta_{\mathbb{Q}}$ had no zero on $\Re s > 1/2$. This is the famous Riemann hypothesis, still open and now another Clay Millennium

Problem. However, this question is not related with the Bloch-Kato conjecture that we discuss in these notes.

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:

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

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 attached to the (motive underlying) V (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

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

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 if 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 $w(V)$ odd, 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

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

and this proves the lemma. □

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 $\Gamma_{\mathbb{R}}$) in L_∞ is $[K:\mathbb{Q}]\dim V$.

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 $\sum_{0\leq k\leq w/2}$ (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 $a^{+}-m_{w/2}$. □

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. 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 $-2,-4,-6,-8,\dots$ 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.

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 3.4. 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 3.5. Prove that every representation V of dimension 1 is polarized. Prove that the representation attached to an abelian variety 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

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

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. In particular, this center is not a pole of $L(V,s)$.

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 relation:

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 results thus follows from the properties of the Γ-function. □

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

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 $\mathbb{Q}_p(1)$ (as a quotient, though it should not matter since V is expected to be semi-simple). 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 among to prove two inequalities:

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

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

The first one, the lower bound on the dimension of the Bloch-Kato Selmer group, ask us to exhibit a sufficient number of independent extension of 1 by $V^*(1)$ 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 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 technics, using in many cases the ideas 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, $L(V,^*(1))$ 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^1_g (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 $\mathcal{M}_K$, 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, $H^1_g(G_K, adV) = 0$.*

This prediction can be seen as an infinitesimal variant of the Fontaine-Mazur conjecture. Indeed, $H^1_g(G_K, \mathrm{ad}V)$ 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) $H^1_g(G_K, \mathrm{ad}V)$ 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.

4.2. **Stability properties for the Bloch-Kato conjecture.**

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

Theorem 4.1. *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 $V^*(1)$. More precisely, (13) holds for V if and only if (13) holds for $V^*(1)$, and similarly for (12).

Proof — We only need to show that

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

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

$$w \geq -1.$$

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

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

We thus get

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

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

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

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

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

which is obviously true. □

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 in 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 $w < -2$, then the weight of $V^*(1)$ is ≥ 0, so (12) holds for $V^*(1)$. Therefore it holds for $V^*(1)$ by theorem 4.1. □

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.* Let S be any finite set of primes of K.

Conjecture 4.2.

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

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

Exercise 4.1. (easy) Show that this holds in the case $V = \mathbb{Q}_p$

Proposition 4.2 (Fontaine, Perrin-Riou)**.** *Under a certain assumption on V (that is called strictly geometric) that is conjecturally always satisfied but very hard to check in practice even for representations coming from geometry, 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).*

The precise statement and the proof (an application of the results of §) will be written after the conference.

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 representation of the form $V = A(n)$ where A is an Artin character. This is a consequence of a theorem of Soulé. 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 $p \not| N$); 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 in a very clever way Euler systems produced with the help of K-theory. 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 result 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.

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 and Skinner and Urban in the general case, 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 $k > 2$ and [B] if $k = 2$). 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 [SU] where the hypothesis that $\mathrm{ord}_{s=0} L(V, s)$ is odd has been weakened into $\mathrm{ord}_{s=0} L(V, s) \geq 1$.

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

5.1. **Small talk.** We have all but forgotten the space $H^1(G_{K,\Sigma}, V)$ for V a geometric representation of G_K,K a number field, focussing 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 a 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 may 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 one of its single instance $H^1(G_{K,\Sigma}, V)$ 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[1]. 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 $H^j_{\text{ét}}(X \times_K, \mathbb{Q}_p)$.

5.2. **The Jannsen's conjecture.** In 1989, a few months before Bloch and Kato, Jannsen made a conjecture that is essentially the same as the following (cf. [J])

Conjecture 5.1. *Let V be a representation coming from geometry of $G_{K,\Sigma}$ which is pure of weight w. Assume that $w \neq -1$. For simplicity, also assume that $V_{|G_v}$ does not contain $\mathbb{Q}_p(1)$ as a subquotient for all finite place $v \notin \Sigma$. Then*

$$\dim H^1(G_{K,\Sigma}, V) = \dim H^0(G_{K,\Sigma}, V) + \sum_{v|\infty} H^0(G_v, V)$$

This conjecture is equivalent to: $H^2(G_{K,\Sigma}, V) = 0$ (under the same hypothesis on V). Clearly, the inequality $\geq$ follows from the Euler-Poincaré formula. The condition on $\mathbb{Q}_p(1)$ is simply here to simplify the formula. 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 $\text{rk}E(\mathbb{Q}) > 1$. To my knowledge, there is no conjecture in the case $w = -1$.

Exercise 5.1. (difficult) Find one and prove it.

[1]Currently, there is a proof in an article on arxiv, but it has not yet been verified, and some specialists are skeptical.

Exercise 5.2. (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 (as functions on $G_{K,\Sigma}$) 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

[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

[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.

[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.

[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.

E-mail address: jbellaic@brandeis.edu

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

Ribet's lemma, generalizations, and pseudocharacters

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

Prerequisites: The prerequisites for these lectures are elementary:

(i) Theory of finite-dimensional representations of groups and algebras; Definitions and first properites of pseudocharacters (= psedurepresentations).
(iii) Very basic group cohomology.

Exercises: There are two kind of exercises, normal and difficult.

Terminology and convention: All rings and algebras are algebra with unity, but not necessarily commutative. Morphisms of rings and algebra preserve unities. Most often, a subring of a ring will have the same unity as the ring itself, but in a few cases, always explicitly mentioned, the sub ring will have a different unity (so the injection map from the subring to the ring will not be a morphism of rings).

In general, A will denote a commutative ring, and R, S shall be non necessarily commutative A-algebra.

If B is a set, and d, d' are integers, then $M_{d,d'}(B)$ is the set of matrices with d columns and d' rows and entries in B. If $d = d'$, we write $M_d(B)$ instead of $M_{d,d}(B)$. If B and C are subsets of a ring A, there is of course a multiplication map $M_{d,d'}(B) \times M_{d',d''}(C) \to M_{d,d''}(A)$.

From Chris' lecture on Ribet's theorem and my lectures on Bloch-Kato, you should have seen that constructing (non-trivial) extensions of Galois representations is often important in number theory.

In these lectures, we want to explain the fundamental tool to construct such extensions, *Ribet's lemma*. This is a purely algebraic lemma (with no reference to Galois group), and there will be no Galois group in these lectures. We will also present generalizations of this lemma, due to various authors (mainly Mazur-Wiles, and Bellaïche-Chenevier). SInce those generalization involve the notion of pseudo-representations, that we call for confusion pseudocharacters, we also develop the theory of pseudocharacters where Kisin left it, proving in particular the fundamental theorems of the theory (Taylor's theorem and Rouquier-Nyssen's theorem).

Contents

1. Ribet's Lemma 2
1.1. Reminder on lattices 2
1.2. Ribet's lemma 6
1.3. Exercises 7
1.4. Directions for a more general Ribet's lemma 8
2. Pseudocharacters 9
2.1. Preliminaries 10
2.2. Proof of Taylor's theorem 11
2.3. Proof of Rouquier and Nyssen's theorem 13
2.4. Exercises 14
3. Residually multiplicity-free pseudocharacters 15
3.1. The structure theorem 16
3.2. Total reducibility locus 17
3.3. Generalization of Ribet's lemma: the case $r = 2$ 18
3.4. Ribet's generalization: the general case 21
3.5. Exercises 22
References 22

1. Ribet's Lemma

In all this section, A is a discrete valuation domain, that is a local principal ideal domain, and K is its field of fraction. Its maximal ideal is therefore of the form πA for some π called a *uniformizer*, and any element of $x = K^*$ can be written $x = u\pi^n$ with $u \in A^*$ and $n \in \mathbb{Z}$, called the valuation $v(x)$ of x. We call k the residue field $A/\pi A$ of A.

1.1. **Reminder on lattices.**

1.1.1. *Definition of a lattice and first properties.* Let V be a vector space over K of dimension d. Since $A \subset K$, V has a structure of A-module.

Lemma and Definition 1.1. Let Λ be an A-submodule of V. The following are equivalent:

(i) Λ is a finite A-module and $K\Lambda = V$.
(ii) Λ is a finite A-module. The natural map $\Lambda \otimes_A K \to V$ (that sends $v \otimes x$ to xv) is an isomorphism.
(iii) Λ is a free A-module of rank d.

If they hold, we say that Λ is a *lattice* of V.

Proof — The equivalence between (i) and (ii) follows from two simple observations: the map $\Lambda \otimes_A K \to V$ has image $K\Lambda$ and is injective. Only the second one needs

a proof. Let $\sum v_i \otimes x_i$ with $v_i \in \Lambda$, $x_i \in K$ be an element of $\Lambda \otimes K$ that maps to 0 in V that is such that $\sum_i x_i v_i = 0 \in V$. Let us choose an n such that $\pi^n x_i \in A$ for all i (this is possible since there is a finite number of x_i's. Then we have

$$(\sum v_i \otimes x_i) = \sum v_i \otimes (\pi^{-n}\pi^n x_i) = (\sum \pi^n x_i v_i) \otimes \pi^{-n} = 0.$$

Assume (ii) holds. the A-module Λ is a finite, and torsion-free as a sub-module of V which is torsion free. Since A is a principal ideal domain, Λ is free of some rank d', and the fact that $\Lambda \otimes_A K \to V$ is an isomorphism implies that $d' = d$.

Conversely, assume (iii) holds. Then Λ is obviously finite, and $\Lambda \otimes_A K$ is a K-vector space of rank d, so the linear map $\Lambda \otimes_A K \to V$, which we have seen is injective, is also surjective by equality of dimension. □

Lemma 1.1. *If $\Lambda \subset \Lambda'$ and Λ'' is an A-module such that $\Lambda \subset \Lambda'' \subset \Lambda'$, then Λ'' is also a lattice. If Λ and Λ' are two lattices of V, so is $\Lambda + \Lambda'$. More generally, if (Λ_i) is a non-empty family of sub-lattices of a lattice Λ, then $+_i \Lambda_i$ is a lattice.*

Proof — This is clear by property (i). □

Definition 1.1. We say that two lattices Λ and Λ' are *homothetic* if there exists $x \in K^*$ such that $\Lambda = x\Lambda'$.

Obviously, to be homothetic is an equivalence relation, and x can always be chosen of the form π^n with $n \in \mathbb{Z}$.

1.1.2. *Stable lattices and representations.* Let V be a K-vector space of dimension d.

Definition 1.2. If G is a subgroup of $\mathrm{GL}_K(V)$, we say that a lattice Λ of V is *G-stable* if $G\Lambda = \Lambda$ or equivalently $G\Lambda \subset \Lambda$.

Proposition 1.1. *For G a subgroup of $\mathrm{GL}_K(V)$, the following are equivalent:*

(a) *There exists a G-stable lattice in V.*
(b) *The coefficients of the matrices of elements of G in a suitable basis of V are in A.*
(c) *The subgroup G is bounded in $\mathrm{GL}_d(K)$*

Proof — The implication (a) ⇒ (b) ⇒ (c) are clear. Let us prove (c) ⇒ (a). Let Λ be any lattice in V. Since G is bounded, there exists an $n \in \mathbb{Z}$ ($n << 0$) such that $g\Lambda \subset \pi^n \Lambda$. The sum of all $g\Lambda$ is therefore a lattice by Lemma 1.1, and is obviously stable by G. □

Corollary 1.1. *If G is a compact group, and $\rho : G \to \mathrm{GL}_K(V)$ is a continuous representation, there exists a lattice stable by ρ (i.e. a lattice Λ such that $\rho(g)\Lambda = \Lambda$ for all $g \in G$.*

Proof — Apply the proposition to $\rho(G)$, which is compact, hence bounded. □

If G is a group, and $\rho : G \to \mathrm{GL}_K(V)$ is a continuous representation, and if Λ is a stable lattice by ρ, then we denote by ρ_Λ the representation $G \to \mathrm{GL}_A(\Lambda)$ obtained by restriction. This is a continuous "representation" of G (on a free module of rank d) over A. Of course for $n \in \mathbb{N}$, $\pi^n\Lambda$ is also stable by ρ_Λ, so we can define a representation $\rho_{\Lambda,n} : G \to \mathrm{GL}_{A/\pi^n A}(\Lambda/\pi^n\Lambda)$. If we choose a basis of Λ over A, then it defines a basis of $\Lambda/\pi^n\Lambda$ over $A/\pi^n A$, and in this basis, $\rho_{\Lambda,n}$ is just the reduction modulo π^n of ρ_Λ.

When $n = 1$, $A/\pi A$ is the residue field k, so $\bar{\rho}_{\Lambda,1}$ is a representation of dimension d over the field k. We shall write $\bar{\rho}_\Lambda$ instead of $\rho_{\Lambda,1}$.

There may be various stable lattices Λ for a given ρ. For different stable lattices Λ, the representations $\bar{\rho}_\Lambda$ may be non-isomorphic (we shall see examples below). Of course, if Λ and Λ' are homothetic, then $\bar{\rho}_\Lambda$ and $\bar{\rho}_{\Lambda'}$ are isomorphic, since ρ_Λ and $\rho_{\Lambda'}$ are (the multiplication by x is an isomorphism if $\Lambda' = x\Lambda$.) In general, we have at least

Proposition 1.2. *If Λ and Λ' are two stable lattices, we have $\bar{\rho}_\Lambda^{ss} = \bar{\rho}_{\Lambda'}^{ss}$*

Here we note ρ^{ss} the semi-simplification of a representation ρ, that is the direct sum of its Jordan-Hölder factors for any Jordan-Hölder sequence.

Proof — Let $g \in G$. The polynomial characteristic of $\bar{\rho}_\Lambda(g)$ is the restriction mod π of the characteristic polynomial of $\bar{\rho}_\Lambda(g)$, which is simply the restriction of the characteristic polynomial of $\rho(g)$ (that we see in passing to be in $A[X]$), so it is the same as the polynomial characteristic of $\rho_{\Lambda'}(g)$. By the Brauer-Nesbitt theorem, this proves that $\bar{\rho}_\Lambda \simeq \bar{\rho}_\Lambda^{\mathrm{ss}}$ □

Definition 1.3. If ρ is a representation that has a stable lattice, we call $\bar{\rho}^{\mathrm{ss}}$ any of the semi-simplification $\bar{\rho}_\Lambda^{\mathrm{ss}}$ for Λ a stable lattice.

1.1.3. *The tree of* $\mathrm{GL}_2(K)$. Let V be a vector space of dimension d over K. Let X be the set of lattices in V, up to homotheties. If Λ is a lattice, we denote by $[\Lambda] \in X$ its equivalence class up to homotheties. This set has an interesting structure, of which we recall some parts, leaving proofs in exercises.

Definition 1.4. We say that two points x and x' in X are *neighbors* if they are distinct there are lattices $x = [\Lambda]$, $x' = [\Lambda']$ such that $\pi\Lambda \subset \Lambda' \subset \Lambda$.

Lemma 1.2. *Let $x = [\Lambda]$ be a point in X. There exists a natural bijection between the set of neighbors of x and the set of proper non-trivial k-subspaces of the k vector space $\Lambda/\pi\Lambda$.*

The bijection is defined as follows: if x' is a neighbor of X, then the Λ' such that $\pi\Lambda \subset \Lambda' \subset \Lambda$ is unique, Λ being fixed. We attach to x' the subspace $\Lambda'/\pi\Lambda$ of $\Lambda/\pi\Lambda$.

The relation "x and x' are neighbors" is symmetric. Therefore the set X with this notions of neighborhood is a undirected graph, and all notions of graph theory applies. For example a *path* from x to x' is a sequence $x = x_0, x_1, \ldots, x_n = x'$ of points in X such that for all $i = 0, \ldots, n-1$, x_i is a neighbor of x_{i+1}. The integer $n \geq 0$ is the length of the path, and the distance $d(x, x')$ between x and x' is the minimal length of a path from x to x' (if any). A path is said *injective* if we have $x_i \neq x_j$ for all $i, j \in \{0, \ldots, n\}$

Proposition 1.3. (a) *The graph X is connected, that is, there is a path from any point to any other.*

(b) *If $d = 2$, the graph X is simply connected, that is: for any $x, x' \in X$, $x \neq x'$, there is exactly one injective path from x to x'.*

A graph X that is connected and simply connected is called a *tree.* From now on, **we assume that** $d = 2$, so X is a tree. If k is finite, the number of neighbors of any point X is $|k| + 1$ (by Lemma 1.2), so X is a *homogeneous tree.*

In a tree, we define the *segment* $[x, x']$ as the set $\{x\}$ is $x = x'$, and as the set of points in the unique injective path from x to x' otherwise. A subset C of X is called *convex* if for all $x, x' \in C$, the segments $[x, x']$ is included in C. A *half-line* H in X is a subset of X that is an increasing union of segments of the form $[x, x_n]$ of length n for $n \in \mathbb{N}$. The point x is the *origin* of H

If $d(x, x') = n$, then we can choose lattices $x = [\Lambda]$ and $x' = [\Lambda']$ such that $\pi^n\Lambda \subset \Lambda' \subset \Lambda$. Once Λ is fixed, Λ' is unique, and the A-modules Λ/Λ' and $\Lambda'/\pi^n\Lambda$ are isomorphic to $A/\pi^n A$. Conversely, such a Λ' define a point at distance n of $[\Lambda]$.

Let $x = [\Lambda]$ be a point in X, and L be a direct summand A sub-module of rank one of Λ. Then if $\Lambda_n := L + \pi^n\Lambda$, $x_n := [\Lambda_n]$ is a point at distance n of x and L define a half-line $H(L, x) = \cup[x, x_n]$ of origin x. Conversely, assume that K is complete. If H is a half-line in X as above, with origin x, there are unique points $x_n = [\Lambda_n]$ in H such that $\pi^n\Lambda \subset \Lambda_n \subset \Lambda$ and $\Lambda/\Lambda_n \simeq A/\pi^n A$. The intersection $L := \cap_{n\in\mathbb{N}}\Lambda_n$ is a free A-submodule of rank one of Λ that is direct summand. It is canonically attached to H and Λ. and denoted by $L(H, \Lambda)$.

A convex C is bounded if and only if it contains no half-line. A bounded convex C contains a point that has at most one neighbors.

The group $Gl_K(V)$ operates on X (by $g \bullet [\Lambda] := [g\Lambda]$) through its quotient $\mathrm{PGL}_k(V)$ and preserves the graph structure. This operation is transitive.

1.2. **Ribet's lemma.** This is the following statement, that appears (as a "proposition" actually, not a lemma) in [R]

Proposition 1.4. *Assume that K is complete. Let G be a compact group, and $\rho : G \to \mathrm{GL}_K(V)$ be an irreducible representation of dimension 2. Assume that $\bar{\rho}^{ss}$ is the sum of two characters $\chi_1, \chi_2 : G \to k^*$. Then there exists a stable lattice Λ such that $\bar{\rho}_\Lambda$ is a non-trivial extension of χ_1 by χ_2.*

Remark 1.1. The characters χ_1 and χ_2 play a symmetric part in the hypotheses. Therefore, the Proposition also asserts that there exists a stable lattice Λ' such that $\bar{\rho}_{\Lambda'}$ is a non-trivial extension of χ_2 by χ_1. In this situation it is clear that $\bar{\rho}_\Lambda$ and $\bar{\rho}_{\Lambda'}$ are not isomorphic.

We shall give a proof, due to Serre, of this result, which, though it is certainly not the shortest, is probably the most illuminating. The proof will occupy the rest of this §.

Let $\rho : G \to \mathrm{GL}_K(V)$ (with $\dim V = 2$) be any representation **that has a stable lattice.**

Let X be the tree of $\mathrm{GL}_K(V)$ and C be the set of x in X that are fixed by $\rho(G)$ (which operates on X as a subgroup of $\mathrm{GL}_K(V)$). We note that if $x \in C$, and $x = [\Lambda]$, then Λ is a stable lattice for ρ (indeed by definition we have $\rho(g)\Lambda = \pi^k \Lambda$, but since $\rho(G)$ is bounded, k has to be 0). If $x \in C$ and $x = [\Lambda] = [\Lambda']$, then $\bar{\rho}_\Lambda \simeq \rho_{\Lambda'}$, therefore there is no ambiguity in calling that representation $\bar{\rho}_x$.

Lemma 1.3. *The subset C of X is non-empty and convex.*

Proof — C is non-empty because it contains $[\Lambda]$ where Λ is stable lattice by ρ. C is convex because, if x, x' are in C, the segment $g \bullet [x, x']$ is a segment of extremities x and x', so is $[x, x']$ by uniqueness. Therefore $[x, x'] \subset C$. □

Lemma 1.4. *if x is in C, then we have*

(a) *x has no neighbor in C if and only if $\bar{\rho}_x$ is irreducible*
(b) *x has exactly one neighbor in C if and only if $\bar{\rho}_x$ is reducible but indecomposable*
(c) *x has more than one neighbors in C if and only if $\bar{\rho}_x$ is decomposable (that is, the sum of two characters).*

In case (c), the numbers of neighbors in C is 2 if the two characters appearing in $\bar{\rho}_x$ are distinct. If they are equal, every neighbors of x in X is actually in C.

Proof — It is elementary that a representation of dimension 2 has no (resp. one, resp. 2, resp. all) stable line if and only if it is irreducible (resp. reducible but indecomposable, resp. decomposable in the sum of two distinct characters, resp. decomposable in the sum of two equal characters). This implies the Lemma if we

can identify "Lines stable by $\bar{\rho}_x$ in $\Lambda/\pi\Lambda$" (where $x = [\Lambda]$) and "neighbors of x in C". But that identification follows directly from the bijection of Lemma 1.2. □

Remark 1.2. In particular, $\bar{\rho}^{\mathrm{ss}}$ is irreducible if and only if C is reduced to a point, that is if and only if ρ has only one stable lattice (up to homotethies). This is clear from the lemma, since in a convex set not reduced to a point, every point has a neighbor.

Lemma 1.5. *Assume that K is complete. Then ρ is irreducible if and only if C is bounded.*

Proof — Assume C is not bounded. Then since it is convex it contains a half-line H. Let $x = [\Lambda]$ be the origin of such an half-line. Then the free A-submodule of rank one $L = L(H, \Lambda)$ of Λ is by construction stable by $\rho(G)$, so KL is a stable line in V, and ρ is not irreducible.

Assume that ρ is reducible. Then it has a stable K-line V_0. Let $L = \Lambda \cap V_0$. This is a free A-submodule of rank one, direct summand, of Λ. Let $H = H(L, x)$ be the half-line defined by L in X. By construction $H \subset C$. Therefore C is not bounded. □

Now let us go back to Ribet's lemma. We assume that ρ is irreducible (so C is bounded), but that $\bar{\rho}^{\mathrm{ss}}$ is not (so that every point of C has at least one neighbor in C). Since C is bounded and convex, it as a point x with at most one, so actually exactly one neighbor in C. Therefore $\bar{\rho}_x$ is reducible but not indecomposable, that is which is a non-trivial extension of χ_1 by χ_2 or of χ_2 by χ_1.

This simple geometric argument almost proves Ribet's lemma. "Almost", because Ribet's lemma states that we can find an x where we actually get a $\bar{\rho}_x$ that is non-trivial extension of χ_1 by χ_2, not the other direction. Of course, this only matters when $\chi_1 \neq \chi_2$. So assume that $\chi_1 \neq \chi_2$. Then every points of C has at most two neighbors. Since C is convex and bounded, this easily implies that S is a segment $[x, x']$. It is an easy exercise to see that, up to exchanging x and x', $\bar{\rho}_x$ is actually a non-trivial extension of χ_1 by χ_2 and $\bar{\rho}_{x'}$ is an extension of χ_1 by χ_2.

1.3. **Exercises.**

Exercise 1.1. If $G \subset \mathrm{GL}_K(V)$ has a stable lattice, then $\mathrm{tr}\,(G) \subset A$. Show that the converse is false, but becomes true if we assume that G is absolutely irreducible.

Exercise 1.2. Prove all the assertions of §1.1.3. They are all almost trivial, except maybe Proposition 1.3, which may need a little bit of works.

Exercise 1.3. Prove that when $d > 2$, X is not a tree. A *facet* F is a subset of X such that every two distinct elements are neighbors. Show that a maximal facet has cardinality $d + 1$. The set X with the data of al its facets has the structure of building in the sense of Tits. It is called the Bruhat-Tits building of $\mathrm{PGL}_K(X)$.

Exercise 1.4. Show that when K is not complete, the argument constructing a sub-module L of rank one in Λ attached to a half-line $H \in X$ of origin $[\Lambda]$ may fail. (actually, the sub-module L it constructs may be (0))

Exercise 1.5. Do the exercise that concludes the proof of Ribet's lemma.

In all the following exercises, we keep the notations and assumptions of Ribet's lemma, and we assume moreover that $\chi_1 \neq \chi_2$, and that char$k \neq 2$. So as we have seen the convex C is a segment.

Exercise 1.6. (difficult) Let l be the length of the segment C. Let $n = n(\rho)$ be the largest integer, if it exists, such that there exists two characters $\psi_1, \psi_2 : G \to (A/\pi^n A)^*$ such that for all $g \in G$, $\mathrm{tr}\,\rho(g) \pmod{\pi^n} = \psi_1(g) + \psi_2(g)$

a.– Show first that n exists.

The integer n can be called the *index of reducibility* of ρ: the larger is n, the "more reducible" is ρ).

b.– Show that $l = n+1$. (Hint: choose a $g_0 \in G$ such that $\chi_i(g_0) = \chi_2(g_0)$. Show that $\rho(g_0)$ is diagonalizable. In a basis of V where it is diagonal, compare $\rho(g)$ and $\rho(gg_0)$ and their traces for all $g \in G$.)

c.– Show how to construct a representation $G \to \mathrm{GL}_2(A/\pi^n A)$ which is an extension of ψ_1 by ψ_2, whore reduction modulo π is a non-trivial extension of χ_1 by χ_2. Show that this extensions generates a sub-module isomorphic to A/π^n in $\mathrm{Ext}^1_{A[G]}(\chi_2, \chi_1)$.

In the following exercise you are allowed to use the exercise 1.6.

Exercise 1.7. There exists $x \in C$ such that $\bar{\rho}_x$ is $\chi_1 \oplus \chi_2$ if and only if $n(\rho) > 1$.

Exercise 1.8. Let G' be a subgroup of G, and assume that $(\chi_1)_{|G'} \neq (\chi_2)_{|G'}$. Let C' be the subset of X fixed by $\rho(G')$.

a.– Show that C' is either a segment, or a half-line, or a line in X (define yourselves a line in X). Show that $C \subset C'$.

b.– Show that $C = C'$ if and only if for every x such that $\bar{\rho}_x$ is (reducible) indecomposable, then $(\bar{\rho}_x)_{|G'}$ is (reducible) indecomposable.

Exercise 1.9. Let G be the subgroup of $\mathrm{GL}_2(A)$ of matrices whose lower left entry is in πA (this group is the Iwahori). Let $\rho : G \to \mathrm{GL}_2(K)$ be the representation of G given by inclusion. Show that S has two points in this case, and that for every stable lattice Λ, $\bar{\rho}_\Lambda$ is semi-simple.

Exercise 1.10. Show that up to replace K by any ramified extension, we can always find a stable Λ such that $\bar{\rho}_\Lambda$ is semi-simple.

1.4. **Directions for a more general Ribet's lemma.** Ribet's Lemma cries for generalizations. First, what happens if ρ is a representation of dimension d, not necessarily 2? When we ask this question, we see that $\bar{\rho}^{\mathrm{ss}}$, if reducible, may be the

direct sum of more than 2 irreducible representation, say r irreducible representations $\bar{\rho}_1, \dots, \bar{\rho}_r$ of respective dimensions $d_1, \dots, d_r$ (with of course $d_1 + \cdots + d_r = d$, so $r \leq d$). What extensions between the $\bar{\rho}_i$ can we get?

We can go further. We have assumed that A was a complete discrete valuation domain, with fraction field K and residue field k. What if we assume that A is a general local domain, again with fraction field K and residue field k? The theory of lattices will not be so simple, and it will not be the case that ρ has always a stable free lattice, so we cannot define $\bar{\rho}^{\mathrm{ss}}$ so simply. But if we assume to begin with that ρ is a representation over A : $G \to \mathrm{GL}_d(A)$ such that $\rho : G \to \mathrm{GL}_d(K)$ is irreducible, while $\bar{\rho}^{\mathrm{ss}} = \bar{\rho}_1 \oplus \cdots \oplus \bar{\rho}_r$ is reducible, then we can ask : can we produce somehow non-trivial extensions of $\bar{\rho}_i$ by $\bar{\rho}_j$?

If A is discrete valuation ring, $\operatorname{Spec} A$ has two points, the closed point $\operatorname{Spec} k$ and the generic point $\operatorname{Spec} K$, and the hypothesis of Ribet's lemma can be rephrased as: ρ is irreducible at the generic point, but reducible at the closed point. When A is a general local domain, the geometry of $\operatorname{Spec} A$ is much richer, and it might be sensible to refine the hypothesis that ρ is irreducible at the generic point. Is there a largest closed subscheme red of $\operatorname{Spec} A$ on which ρ is reducible (in some sense, for example some sense inspired by exercise 1.6)? If so, red is a proper subscheme if and only if ρ is irreducible at the generic point, and instead of assuming that ρ is irreducible at the generic point, we can make assumption on red, presumably getting better results (that is more non-trivial extensions between the $\bar{\rho}_i$) when red is smaller. When we do so, we see that we have no need to speak of the generic point anymore, that is no need to assume that A is a domain, any local ring will do.

To go further, why should we start with a representation $\rho : G \to \mathrm{GL}_d(A)$? A pseudo-character $T : G \to A$ of dimension d is more general. When A is a d.v.r., this generality is an illusion, but for general local ring A, it is not as we shall see. So we should work with general pseudocharacters.

In the following section, we shall give a generalization of Ribet's lemma along the lines explained above. Since Kisin's talk on pseudorepresentations have been sketchy, and since we will need to go in detail, we begin by reviewing them, beginning by giving them their right names.

2. Pseudocharacters

First, pseudocharacters and pseudorepresentations are the same things. Pseudorepresentations was the term coined by Wiles, and used after by Taylor, Nyssen and others. Pseudocharacters is the better term used by Serre and Rouquier. I will use pseudocharacters

Second, when A is a commutative ring, Kisin's defined a pseudocharacter $T : G \to A$ over a group or $T : R \to A$ from an A-algebra R. Of course, the first case is a special case of the second since a pseudocharacter $T : G \to A$ defines by

linearization a pseudo-character $T : A[G] \to R$. I will work almost uniquely with the second definition (pseudocharacters over algebras) since it is more convenient and more general.

Since Kisin did not prove Taylor and Rouquier's theorem, and since I need ideas from their proof I begin by using them.

In all this §, we fix $T : R \to A$ be a pseudocharacterof dimension d. I will assume that $d!$ is invertible in A.

2.1. **Preliminaries.** Recall that $\ker T = \{x \in R,\ T(xy) = 0\, \forall y \in R\}$. It is a two-sided ideal of A (since $T(xy) = T(yx)$), and T factors through the quotient $R/\ker T$ and define a pseudocharacter $T : R/\ker T \to A$ which is *faithful*, that is which has trivial kernel.

We shall use the complicated definition of a pseudocharactermainly through a consequence of it, which can be called the *Cayley-Hamilton* theorem for a pseudocharacter.

Lemma 2.1 (Newton)**.** *There exits unique polynomials*

$$a_0, \dots, a_{d-1} \in \mathbb{Z}[1/d!][S_1, \dots, S_d]$$

such that for every complex numbers $\alpha_1, \dots, \alpha_d$ such that if $s_n = \sum_{i=1}^{d} \alpha_i^n$ for $n = 1, \dots, d$, then the polynomial $X^d + a_{d-1}(s_1, \dots, s_d)X^{d-1} + \dots + a_0(s_1, \dots, s_d)$ has roots $\alpha_1, \dots, \alpha_d$.

The proof is left as an exercise.

Definition 2.1. If $x \in R$, we call $P_{x,T}$ the polynomial $X^d + a_{d-1}(T(x), \dots, T(x^d))X^{d-1} + \dots + a_0(T(x), \dots, T(x^d)) \in A[X]$ is called the *characteristic polynomial* of x for T

Indeed, when $T = \operatorname{tr} \rho$ for $\rho : R \to M_d(A)$, then $P_{x,T}$ is the characteristic polynomial of $\rho(x)$ (exercise).

Proposition 2.1 (Cayley-Hamilton)**.** *If T is faithful, then for every $x \in R$, $P_{x,T}(x) = 0$*

Proof — Setting all the variables but one in the definition of a pseudocharacters of dimension d equal to x, and the last one equal to y, we get (after some computations) $T(P_{x,T}(x)y) = 0$. Therefore $P_{x,T}(x) \in \ker T = 0$. □

In the following set of lemmas, we assume that A is local (of maximal ideal m), and e is an idempotent of R (that is $e^2 = e$)

Lemma 2.2. *$T(e)$ is an integer between 0 and d.*

Proof — If in the definition of a pseudo-character we put all the variables equal to em we get $T(e)(T(e) - 1) \dots (T(e) - d) = 0$. At most one of the factors are in m since the difference in any two factors is an integer between $-d$ and d so is invertible in A. Therefore all factors except (maybe) one are invertible, so the last one is 0. □

Lemma 2.3. *The restriction of T to eRe (with unity e) is a pseudocharacter of dimension $T(e)$.*

Indeed, it is clear that T_e is a pseudocharacter. Its dimension is its value on the unity, hence $T(e)$.

Lemma 2.4. *If T is faithful, and $T(e) = 0$ then $e = 0$.*

Proof — Indeed, if $T(e) = 0$, then $T(e^n) = 0$ for all n, so $P_{e,T}(X) = X^d$, and by Cayley-Hamiltion, $e^d = 0$, so $e = 0$. □

Lemma 2.5. *If T is faithful, there cannot be in R a family of more than d nonzero orthogonal idempotents.*

Indeed, the sum of all those idempotents $e_1, \dots, e_k$ would be an idempotent e such that $T(e) = T(e_1) + \cdots + T(e_k) > 1 + \cdots + 1 = k > d$

Lemma 2.6. *If T is faithful, then so is T_e*

Indeed, if $x \in eRe$ is such that $T_e(xy) = 0$ for each $y \in eRe$, then take $z \in R$. We have $T(xz) = T(xze) + T(xz(1-e))$ but $T(xz(1-e)) = T((1-e)xz) = 0$ so $T(xz) = T(xze) = T(xeze) = T_e(xeze) = 0$. Since T is faithful, $x = 0$.

2.2. **Proof of Taylor's theorem.**

Theorem 2.1. *If $A = k$ is a separably closed field, $T = \operatorname{tr}\rho$ for a unique semi-simple representation $\rho : R \to M_d(A)$.*

Actually, this is a theorem of Taylor if k has characteristic 0, and Rouquier in characteristic p (with $p > d$ of course). The uniqueness of ρ has been proved in Kisin's lecture. Therefore I prove only the existence of ρ. The fundamental idea (of Rouquier's proof) is to investigate the structure of the algebra $R/\ker T$.

Lemma 2.7. *The radical J of $R/\ker T$ is trivial*

Proof — Let $x \in J$. We first prove that x is nilpotent. Indeed write $P_{x,T}(X)$ as $aX^i(1+XQ(X))$ with $a \in k, i \geq 0$. Then by Cayley-Hamilton, $ax^i(1+xQ(x)) = 0$. But $xQ(x)$ is in the radical J, so $1 + xQ(x)$ is invertible, and we get $x^i = 0$.

The second point is that a nilpotent element x in $R/\ker \mathrm{T}$ has $T(x) = 0$. There are many proofs of this fact. Here is one : we may assume by induction that $x^2 = 0$, and then putting in the definition of a pseudocharacter all the variables equal to x, on gets $T(x)^{d+1} = 0$. But k is a field...

Putting those two points together, we see that every element x of the radical J has $T(x) = 0$. For every $y \in R/\ker T$, xy is also in the radical thus we have $T(xy) = 0$. so $x = 0$. □

This lemma says that the A-algebra $R/\ker \mathrm{T}$ is semi-simple. Moreover it is integral over A (by Cayley-Hamilton) and which is more every element in R is killed by a monic polynomial in $A[X]$ of degree d. And finally there are no family of more than d orthogonal non-zero idempotents. Those three properties implies

Proposition 2.2. *$R/\ker \mathrm{T}$ is isomorphic to a product of matrix algebras over k: $M_{d1}(k) \times \cdots \times M_{d_r}(k)$.*

Note that a classical result states that semi-simple finite-dimensional algebras over k are of this form. Here we see that we can weaken the finite dimensionality, replacing it by two finiteness conditions, one on idempotents, the other on degree.

Proof — The conditions on idempotents prove that there is at most d isomorphism classes of irreducible modules over $R/\ker \mathrm{T}$. If V is one of them, then $D := \mathrm{End}_K(V)$ is a division algebra. There is a natural morphism $R \to \mathrm{End}_D(V)$. The Jacobson density theorem states that this morphism is surjective if V is finite-dimensional, and at least of dense image in the general case, in the sense that the image contains $\mathrm{End}_D(V')$ for D-subspace V' of V of arbitrary high finite dimension. But V can not be infinite dimensional because this would imply that the image of $R/\ker \mathrm{T}$, hence $R/\ker \mathrm{T}$ itself, would contain elements not killed by a unitary degree d-polynomial. Hence $R \to \mathrm{End}_D(V)$ is surjective. Since $D \subset \mathrm{End}_D(V)$, we see that every element in D is algebraic over k. Hence D is commutative, and a subfield of k. Finally we use the classical result that the center of D is separable over k to conclude $D = k$. Hence $\mathrm{End}_D(V)$ is a matrix algebra over k. We see easily, since $R/\ker \mathrm{T}$ is semi-simple, that it is isomorphic to the product of $\mathrm{End}_k(V_i)$ where V_i are the different simple modules over R.

□

Finally we get Taylor's theorem: we may replace R by $R/\ker \mathrm{T}$, which is a product of matrix algebras, and we want to show that the pseudocharacter T on it is the trace of a semi-simple representation. Using idempotents $e_1, ..., e_r$ of $R/\ker \mathrm{T}$ given by the identity elements of the matrix algebras $M_{d_i}(k)$, and results above on idempotents, we may assume that $R/\ker \mathrm{T}$ is a matrix algebra $M_{d_i}(k)$. Hence we are reduced to prove the following

Lemma 2.8. *A pseudocharacter $M_d(k) \to k$ is an integral multiple of the trace, hence is the trace of a sum of copies of the standard representation.*

Indeed, it is a trivial exercise to see that a linear form T on $M_{d_i}(k)$ that satisfies $T(xy) = T(yx)$ is a multiple of the trace, say $\alpha \mathrm{tr}$. Applying this to an idempotent e of trace 1 in $M_{d_i}(k)$, we get $\alpha = T(1)$. But we know that $T(1)$ is an integer.

This concludes the proof of existence in Taylor's theorem. As a corollary of the proof, we get that if T is irreducible (that is not the sum of two pseudo-characters of smaller dimensions), then $R/\ker T \simeq M_d(k)$.

2.3. **Proof of Rouquier and Nyssen's theorem.**

Theorem 2.2. *Let $T : R \to A$ be a pseudocharacter of dimension d. Assume that A is local and strictly Henselian*[1]*, with residue field k. Assume that $\bar{T} = T \otimes 1 : R \otimes_A k \to k$ is irreducible (not the sum of two non-zero pseudocharacters). Then $R/\ker \mathrm{T} \simeq \mathrm{M_d(A)}$, and T is the trace of a unique representation, namely $R \to R/\ker \mathrm{T} = \mathrm{M_d(A)}$.*

The uniqueness is due to Mazur and Serre and Carayol, the existence of the representation and the result on $R/\ker \mathrm{T}$ are due independently to Nyssen and Rouquier.

For the proof, we may as well replace R by $R/\ker(T)$, which simplifies notations and add the hypothesis that T is Cayley-Hamilton over R. By the above §, we have that $R \otimes k/\ker \bar{T} \simeq M_d(k)$.

As in the case of a field, the starting point is to understand the radical of R.

Lemma 2.9. *If $T : R \to A$ is faithful, and A, T has above, then the radical J of R is the inverse image of $\ker \bar{\mathrm{T}}$ in R. In other words, $R/J = (R \otimes_A k)/\ker \bar{T} \simeq M_d(k)$.*

Proof — Let J' denote the inverse image of $\ker \bar{\mathrm{T}}$ in R. It is a two-sided ideal of R. Since $R \otimes k/(\ker \bar{T})$ is a matrix algebra $M_d(k)$, hence is semi-simple, we have $J \subset J'$.

Let $x \in J'$. We will show that $1 + x \in R^*$. We have $T(xy) \in m$, for all y in R, hence $T(x^i) \in m$ for all i, so that by the Cayley-Hamilton identity $x^d \in m(A[x])$. Let us consider the commutative finite A-algebra $B := A[x]$. Then B is local with maximal ideal (m, x), as B/mB is. As a consequence, $1+x$ is invertible in B, hence in R.

As J' is a two-sided ideal of R such that $1 + J' \subset R^*$, we have $J' \subset J$. □

After this lemma we are almost done: in $R/J \simeq M_d(k)$ we have the elementary matrices $E_{i,j}$, for $i, j \in \{1, \ldots, d\}$. they satisfy

$$E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}, \quad \sum_{i=1}^{d} E_{i,i} = 1.$$

It is well known (see Bourbaki - this is the basic fact used for example in the theory of Azumaya algebra) that we can lift those elements of R/J into elements of R that we shall still denote $E_{i,j}$ that satisfy the same relations. (this works since J is the radical of R, since R is integral over A, and since A is Henselian. The proof of this "basic fact" is a clever application of Hensel's lemma).

The $E_{i,i}$ are idempotents, hence each $T(E_{i,i})$ is an integer, which is not zero since $E_{i,i} \neq 0$. Their sum has to be $T(1) = d$, so all the $T(E_{i,i})$ are 1. From this we

[1]Henselian means that Hensel's lemma is true in A. For example, if A is complete, then it is henselian. Strictly means that the residue field k is separably closed. If not, it is a basic result that we can replace A by an étale extension which is local and strictly henselian

deduce that the restriction of $T_{E_{i,i}}$ of T to $E_{i,i}RE_{i,i}$ is a faithful pseudocharacter of dimension 1. But clearly this shows that $E_{i,i}RE_{i,i}$ is isomorphic to A as an A-algebra ($T_{E_{i,i}}$ being such an isomorphism). As for $E_{i,i}RE_{j,j}$ take x in this set. Then $E_{j,i}x$ is in $E_{j,j}RE_{j,j}$ so by the above $E_{j,i}x = T(E_{j,i}x)Ej, j$. Then $x = E_{i,j}E_{j,i}x = T(E_{j,i}x)Ei, j$. This proves that $E_{i,i}RE_{j,j} = AE_{i,j}$. Form those results it is easy to see that the linear map from R to $M_d(A)$ that sends $E_{i,j}$ to the (i, j)-elementary matrix is an isomorphism of A-algebras. This proves the first part of the theorem, from which it is trivial to deduce that T is the trace of a representation as we did in the case of a base field.

2.4. **Exercises.**

Exercise 2.1. Show all non-proved assertions in §2.1.

Exercise 2.2. If B is a commutative A-algebra, show that $T \otimes 1 : R \otimes B \to B$ is a pseudocharacter of dimension d. Show that if T is faithful and B is A-flat, then $T \otimes 1$ is faithful. Show that this result may be false when B is not A-flat.

Exercise 2.3. Let $A = \mathbb{R}$ and $\mathbb{H}$ be the field of quaternions. Show that $T : \mathbb{H} \to \mathbb{R}$, $T(a + bi + cj + dk) = a$ is a pseudocharacter on $\mathbb{H}$ that does not come from a representation.

Exercise 2.4. Test: Let k be an algebraically closed field, and R a k-algebra. If $T : R \to k$ is a pseudocharacter of some dimension, and $R/\ker T = M_n(k)$, is T necessarily irreducible?

Exercise 2.5. If $T : R \to A$ is a pseudocharacter, we call $\mathrm{CH}(T)$ the two-sided ideal of R generated by the $P_{x,T}(x)$ for $x \in R$. We say that T is *Cayley-Hamilton* if $\mathrm{CH}(T) = 0$.

a.– Show that $\mathrm{CH}(T) \subset \ker T$. Show that faithful implies Cayley-Hamilton.

b.– Deduce that T factors through a pseudocharacter $T : R/\mathrm{CH}(T) \to A$, which is Cayley-Hamilton.

c.– Show that with the notation of exercise 2.2, we have $\mathrm{CH}(T \otimes 1) = \mathrm{CH}(T)B$ (even when B is not A-flat). In particular, if T is Cayley-Hamilton, then so is $T \otimes 1$.

d.– **(difficult)** If $T : R \to A$ is Cayley-Hamilton, and $R/\ker T \simeq M_d(A)$, then T is faithful and $R \simeq M_d(A)$.

e.– **(difficult)** Deduce the global form of Rouquier's theorem (with a simpler proof than Rouquier's) : If A is any commutative ring (with $d!$ invertible in A), and $T : R \to A$ is a pseudocharacter of dimension d such that at every closed point m of $\mathrm{Spec}\, A$, $T \otimes 1 : R \otimes A/m \to A/m$ is absolutely irreducible, then $R/\ker T$ is an Azumaya algebra over A (Remark: if you don't knot what is an Azumaya algebra, that's not a problem. You only need to know that an algebra over A whose base

change to any local ring at closed points of $\operatorname{Spec} A$ is a matrix algebra M_d is an Azumaya algebra)

Exercise 2.6. a.– Let k be a field, and $T : R \to k$ be a pseudocharacter. Assume that the $T \otimes 1 : R \otimes \bar{k} \to \bar{k}$ is the trace of a representation ρ that is irreducible. (We say that T is absolutely irredicible). Show that $R/\ker T$ is a central simple algebra. (you might need to use exercise 2.2)

b.– By mimicking the proof of Rouquier-Nyssen theorem, show that if A is a local Henselian ring wuth residue field k finite, and $T : R \to A$ is a pseudocharacter such that $\bar{T}$ is absolutely irreducible, then T is the trace of a representation. (This statement contains the one used by Mark Kisin).

3. Residually multiplicity-free pseudocharacters

We keep the notations of Rouquier and Nyssen's theorem: $T : R \to A$ be a pseudocharacter of dimension d. the ring A is a local and strictly henselian ring, with residue field k, maximal ideal m. To simplify the exposition, we shall also assume that A is noetherian and reduced (none of these hypotheses is really necessary), and we call K its total fraction ring: K is a finite product of field.

Rouquier and Nyssen's theorem is fine, but for the generalizations of Ribet's lemma it is not enough: We definitely need to work without the assumption that $\bar{T} = T \otimes 1 : R \otimes k \to k$ is irreducible.

If $\bar{T}$ is not irreducible, it is a sum of irreducible characters, each of them being, by Taylor-Rouquier's theorem, the trace of a unique irreducible representation. So we can write

$$T = \operatorname{tr} \bar{\rho}_1 \oplus \cdots \oplus \bar{\rho}_r.$$

We shall call $d_1, \ldots, d_r$ the dimensions of $\bar{\rho}_1, \ldots, \bar{\rho}_r$, so that $d_1 + \cdots + d_r = d$.

We will make the following simplifying assumption: for $i \neq j$, $\bar{\rho}_i \not\simeq \rho_j$. We call a T that satisfies this hypothesis *residually multiplicity free*. Important part of the theory we shall expose below can be done without this hypothesis, that is for general T (see [C]), but the theory is simpler in the residually multiplicity free case and this case is sufficient for our purposes.

Our aim is, for T residually multiplicity free as above, to study, as we have done in the more specific cases, the structure of $R/\ker T$ (we shall see this way that such T are not necessarily trace of representations), to define and show how to compute the (total) reducibility locus of T in $\operatorname{Spec} A$ (the maximal closed subscheme on which T is as reducible as it as at the closed point), and to prove the analog of Ribet's lemma (how we can use T to construct non-trivial extensions between the $\bar{\rho}_i$)

3.1. **The structure theorem.** We shall determine the structure of the A-algebra $R/\ker T$. It will not always be a matrix algebra $M_d(A)$. Instead, it will be a generalized matrix algebra (of type $d_1, \dots, d_r$) in the following sense:

Lemma and Definition 3.1. Let $A_{i,j}$, $i,j = 1, \dots, r$ be fractional ideals of A (that is finite type A-submodules of K) such that

(a) $A_{i,i} = A$ for all i
(b) $A_{i,j}A_{j,k} \subset A_{i,k}$ for all i, j, k.
(c) $A_{i,j}A_{j,i} \subset m$.

Consider elements a of $M_d(K)$ as matrices by blocks of size $(d_1, \dots, d_r)$: call $a_{i,j} \in M_{d_i,d_j}(K)$ the bloch (i,j). Let S be the subset of $M_d(K)$ of elements a such that all the entries of $a_{i,j}$ are in $A_{i,j}$. That is to say:

$$S = \begin{pmatrix} M_{d_1}(A_{1,1}) & M_{d_1,d_2}(A_{1,2}) & \dots & M_{d_1,d_r}(A_{1,r}) \\ M_{d_2,d_1}(A_{2,1}) & M_{d_2}(A_{2,2}) & \dots & M_{d_2,d_r}(A_{2,r}) \\ \vdots & \vdots & \ddots & \vdots \\ M_{d_r,d_1}(A_{r,1}) & M_{d_r,d_2}(A_{r,2}) & \dots & M_{d_r}(A_{r,r}) \end{pmatrix}$$

Then

(i) S is a A-subalgebra of $M_d(K)$ (with same unity Id).
(ii) The trace $M_d(K) \to K$ induces a map $\mathrm{tr} : S \to A$ which is a pseudo-character of degree d.
(iii) The map $r_i : S \otimes_A k \to M_{d_i}(k)$ induced by $a \mapsto a_{i,i}$ is an irreducible representation of $S \otimes_A k$, and $r_i \not\simeq r_j$ if $i \neq j$. We have $\bar{t}r = \mathrm{tr}\ r_1 + \cdots + \mathrm{tr}\ r_d$. In particular, the pseudo-character tr is residually multiplicity free.

The algebra S is called the *generalized matrix algebra* of type $(d_1, \dots, d_r)$, attached to the families of fractional ideal $(A_{i,j})$.

Proof — It is clear that S is an A-submodule, and properties (b) show that S is stable by multiplication, while (a) shows that S contains Id. This proves (i). Property (a) implies that tr sends S to A, and it is a pseudocharacter of dimension d since $\mathrm{tr} : M_d(K) \to K$ is. This proves (ii). A simple computation using (c) shows that r_i is a morphism of algebras, and since it is clearly surjective, it is an irreducible representation. The rest of (iii) is clear. □

Theorem 3.1. *Let $T : R \to A$ be a residually multiplicity free pseudocharacters as above. There exists a generalized matrix algebra S of type $(d_1, \dots, d_r)$ attached to the families of fractional ideal $(A_{i,j})$, and an A-isomorphism of algebras $f : R/\ker T \to S$ such that* $\mathrm{tr} \circ f = T$.

Remark 3.1. The ideals $A_{i,j}$ are not uniquely determined. Actually it is clear that if $(x_i)_{i=1,\dots,r}$ is a families of elements of K^*, then the ideals

$$A'_{i,j} = x_i^{-1} x_j A_{i,j} \tag{1}$$

satisfy the same relations (a), (b), (c), and that the generalized matrix algebra S' attached to the $(A'_{i,j})$ is A-isomorphic to S with an isomorphism compatible with traces. So we can change the $A_{i,j}$ up to a transformation 1. Actually, it can be shown that the families $(A_{i,j})$ is well-defined, up to a transformation of the type 1.

We shall use this theorem again and again. For T a residually multiplicity-free pseudocharacter, we shall call $A_{i,j}$ fractional ideals as in the theorem. The fact that the $A_{i,j}$ are well-determined only up to a transformation of type 1 will not matter, since as the reader can check, all constructions using the $A_{i,j}$ below will actually be invariant by this transformation.

Proof — (Sketch) We can and do assume that T is faithful. We now want to prove that R is a generalized matrix algebra of type $(d_1, \dots, d_r)$.

Since the character $\bar{T} : R \otimes_A k \to k$, $\bar{T} = \operatorname{tr} \bar{\rho}_1 \oplus \cdots \oplus \operatorname{tr} \bar{\rho}_r$ is the sum of r non isomorphic representation, we have (see the proof of Taylor's theorem above) $(R \otimes k)/\ker \bar{T} = \bar{\rho}_1(R \otimes k) \times \cdots \times \bar{\rho}_r(R \otimes k) = M_{d_1}(k) \times \dot{\times} M_{d_r}(K)$. Let ϵ_i be the identity of $M_{d_i}(K)$ seen as an element of $R/\ker \bar{T}$. Then the ϵ_i's form an orthogonal family of idempotents of sum 1. Recall that by Lemma 2.9, the kernel of the surjective map $R \to R \otimes k \to (R \otimes k)/\ker \bar{T}$ is the radical J of R. Therefore, we can lift the families ϵ_i to a families e_i of orthogonal idempotents of R of sum 1.

Looking at the subalgebra $e_i R e_i$ of R (with unity e_i) and mimicking the proof of Rouquier-Nyssen's theorem, it is not hard to prove that $e_i R e_i \simeq M_{d_i}(A)$ for all $i = 1, \dots, r$ (by considering the elementary matrices $E_{\alpha,\beta} \in M_{d_i}(k)$ seen as elements of $R \otimes k/\ker \bar{T}$ and by lifting then to $e_i R e_i$).

Now if $i \neq j$, then $e_i R e_j$ as an obvious structure of left $e_i R e_i \simeq M_{d_i}(A)$-module and right $e_j R e_j \simeq M_{d_j}(A)$. By Yoneda's theory, $e_i R e_j$ is isomorphic, for its bimodule structure, to $M_{d_i,d_j}(A_{i,j})$ for some A-modules $A_{i,j}$.

Moreover, the multiplication in R induces map $e_i R e_j \otimes e_j R e_k \to e_i R e_k$. Again by Yoneda's theory, those maps are induced by morphisms of A-modules $\psi_{i,j,k} : A_{i,j} \otimes_A A_{j,k} \to A_{i,k}$.

So we already can write $R = \oplus_{i,j} e_i R e_j \simeq \oplus_{i,j} M_{d_i,d_j}(A_{i,j})$. Here the $\simeq$ is an isomorphism of algebra, where the right hand side is given an algebra structure using matrix multiplication and the $\psi_{i,j,k}$. To check that the RHS is a generalized matrix algebra, we only have to prove that the A-modules $A_{i,j}$ are finite type and can be embedded in K in such a way that the maps $\psi_{i,j,k} : A_{i,j} \otimes_A A_{j,k} \to A_{i,k}$ becomes induced by the multiplication of K. We leave this to the reader. □

3.2. **Total reducibility locus.**

Theorem 3.2. *Let $T : R \to A$ be a residually multiplicity free characters as above. There exists a smallest ideal I of A, such $T \otimes 1 : R \otimes A/I \to A/I$ is the sum of r non-zero pseudocharacters. We have $I = \sum_{i,j=1,\dots,r \;\; i \neq j} A_{i,j} A_{j,i}$, where the fractional ideals $A_{i,j}$ are as in the structure theorem*

For the proof, that relies heavily on the structure theorem, see [BC]. We just note that, with the notation of the structure theorem, if $\sum_{i,j=1,\dots,r \quad i\neq j} A_{i,j}A_{j,i} \subset I$, then it is easy to see that $T \otimes 1 : R \otimes A/I \to A/I$ is the sum of r non-zero pseudocharacters. Indeed, the maps $r_i : R \xrightarrow{f} S \to M_{d_i}(A/I)$ induced by $a \mapsto a_{i,i} \pmod I$ are easily seen to me morphisms of algebra, so their trace $\operatorname{tr} r_i$ defines pseudocharacters $R \otimes A/I \to A/I$ (of dimension d_i) and one has $T \otimes 1 = \sum_{i=1}^{r} \operatorname{tr} r_i$. What is harder is to prove the converse: that if on some ideal I $T \otimes 1 : R \otimes A/I \to A/I$ is the sum of r characters, then $\sum_{i,j=1,\dots,r \quad i\neq j} A_{i,j}A_{j,i} \subset I$.

Definition 3.1. We call I the (total) *reducibility ideal* of T and $\operatorname{Spec} A/I$ the (total) *reducibility locus* of T.

Remark 3.2.
(i) We can consider other reducibility conditions. For example, for $1 < s \leq r$, we can ask wether there exists a smallest ideal I such that $T \otimes 1 : R \otimes A/I \to A/I$ is the sum of s non-zero pseudocharacters. Or, given a partition of $\{1, \dots, r\} = P_1 \coprod P_2 \coprod \cdots \coprod P_s$, we can ask wether there exists a smallest ideal I such that $T \otimes 1 : R \otimes A/I \to A/I$ is the sum of s non-zero pseudocharacters $T_1, \dots, T_s$ such that for $l = 1, \dots, s$, $T_l \otimes 1 : R \otimes k \to k$ is equal to $\sum_{i \in P_l} \operatorname{tr} \rho_i$. It can be shown that those general reducibility ideal always exist. For example, for the one attached to a partition $P_1 \coprod \cdots \coprod P_s$, the smallest I is $+_{i,j \text{ not in the same } P_l} A_{i,j}A_{j,i}$.
(ii) If we do not assume that T is residually multiplicity free, the reducibility ideal may not exist.

Finally, let J be any proper ideal of A containing the (total) reducibility ideal of T. The pseudocharacter $T \otimes 1 : R \otimes A/J \to A/J$ is the sum of r pseudocharacters $T_1, \dots T_r : R \otimes A/J \to A/J$. It can be shown that the T_i are unique, that is we do not have another decomposition of $T \otimes 1$ as a sum of r pseudocharacters, up to renumbering of course.

Up to renumbering the T_i, we can assume that $\bar{T}_i = T_i \otimes 1 : R \otimes k \to k$ is $\operatorname{tr} \bar{\rho}_i$. It can be shown that the T_i are unique, that is we do not have another decomposition of $T \otimes 1$ as a sum of r pseudocharacters. By Rouquier and Nyssen's theorem, there exists a unique representation $\rho_i : R \otimes A/J \to M_{d_i}(A/J)$ of trace T_i. The representation ρ_i is a lift (or a deformation, if you like) of $\bar{\rho}_i$ to A/J.

3.3. **Generalization of Ribet's lemma: the case $r = 2$.** Before going to the general case, which is combinatorially involved, we dwell a little bit on the case where $\bar{T}$ is the sum of $r = 2$ irreducible pseudocharacters $\operatorname{tr} \bar{\rho}_1$ and $\operatorname{tr} \bar{\rho}_2$. The dimension d of T is still unrestricted, and so is the nature of the local ring A (beside being strictly henselian, Noetherian and reduced, as usual). The ideas in this case mainly come from [MW], though they use a different terminology (Wiles had not invented yet pseudorepresentations), and are in a more restricted situation ($d = 2$, A is finite over a d.v.r, etc.)

In this case the structure theorem takes a very simple form: there are two fractional ideals B and C of A, with $BC \subset m$, and an isomorphism

$$f : R/\ker T \to S = \begin{pmatrix} M_{d_1}(A) & M_{d_1,d_2}(B) \\ M_{d_2,d_1}(C) & M_{d_2}(A) \end{pmatrix}$$

that is compatible with traces. The proper ideal $I = BC$ of A is the reducibility ideal of A.

Proposition 3.1. *Let J be any proper ideal of A that contains I. As we have seen at the end of §3.2, the representations $\bar{\rho}_i$ have canonical lifts $\rho_i : R \otimes A/J \to M_{d_i}(A/J)$. There exists natural injective maps of A-modules*

$$\iota_B : \mathrm{Hom}_A(B, A/J) \to \mathrm{Ext}^1_{R\otimes A/J}(\rho_1, \rho_2) \tag{2}$$

$$\iota_C : \mathrm{Hom}_A(C, A/J) \to \mathrm{Ext}^1_{R\otimes A/J}(\rho_2, \rho_1) \tag{3}$$

Proof — We only treat the first case, the second being symmetric. The proof is by direct computation: for $r \in R$, let us call $f(r)$ its image in S, and $a(r) \in M_{d_1}(A)$, $b(r) \in M_{d_1,d_2}(B)$, $c(r) \in M_{d_2,d_1}(C)$, $d(r) \in M_{d_2}(A)$ be its block constituents. We have the multiplication relations $a(rr') = a(r)a(r') + b(r)c(r')$ in $M_{d_1}(A)$, $b(rr') = a(r)b(r') + b(r)d(r')$ in $M_{d_1,d_2}(B)$, and similarly for the other constituents. Note in particular that $b(r)c(r') \in M_{d_1}(BC) \subset M_{d_1}(J)$ so $a(rr') \equiv a(r)a(r') \pmod J$, and similarly for d. Actually, by construction $a(r) \pmod J = \rho_1(r)$ in $M_{d_1}(A/J)$ and $d(r) \pmod J = \rho_2(r)$.

Now let $l : B \to A/J$ be a morphism of A-modules. We consider the map $\rho_l : R \otimes A/J \to M_d(A/J)$ defined by

$$\rho_l(r \otimes 1) = \begin{pmatrix} (a(r) & (\mathrm{mod}\ J) & l(b(r)) & \\ 0 & & d(r) & (\mathrm{mod}\ J) \end{pmatrix},$$

where $l(b(r))$ is the matrix in $M_{d_1,d_2}(A/J)$ obtained from $b(r)$ by applying l to each coefficients.

We claim that ρ_l is a morphism of algebras. Indeed, it obviously respects the addition, and for the multiplication only the upper right corner may be a problem. So we check : the upper right corner of $\rho_l(rr')$ is $l(b(rr')) \in M_{d_1,d_2}(A/J)$. The upper right corner of $\rho_l(r)\rho_l(r')$ is $a(r)l(b(r')) + b(r)l(d(r')) = l(a(r)b(r') + b(r)d(r'))$ since l is A-linear. Now we see that the two upper-tight corner are the same by the multiplication formula for b given above.

Since ρ_l is a morphism of algebras, it is a representation of $R \otimes A/J$. But clearly it contains $a = \rho_1$ as a sub-representation and $d = \rho_2$ as a quotient. Therefore ρ_l is an extension of ρ_2 by ρ_1. Hence a map $\iota_B : l \mapsto \rho_l$, $\mathrm{Hom}_A(B, A/J) \to \mathrm{Ext}^1_{R\otimes A/J}(\rho_1, \rho_2)$. This map is clearly linear from the definition of ρ_l. It remains to show that is is injective. Assume that the extension ρ_l is trivial. This does not imply that $l(b(r)) = 0$ for all $r \in R$ but this clearly implies that $l(b(r)) = 0$ for r such that $\rho_1(r) = 0$ and $\rho_2(r) = 0$. But f is surjective, so we can find r such that

$a(r) = 0$, $d(r) = 0$, and $b(r)$ is arbitrary in $M_{d_1,d_2}(B)$. So we see that l is 0 on B, which proves the injectivity of the map $l \mapsto \rho_l$. □

The generalization of Ribet's lemma is the combination of this proposition and the fact that BC is reducibility ideal.

Do you see why it is a generalization of Ribet's lemma? Maybe not. Let me be explicit. Assume as in the hypotheses of Ribet's lemma that A is discrete valuation domain, of fraction field K, and that $T = \operatorname{tr} \rho$ where ρ is a representation that is irreducible over K, but such that $\bar{\rho}^{\mathrm{ss}} = \bar{\rho}_1 \oplus \bar{\rho}_2$. Since ρ is irreducible over K, the reducibility locus is a proper subscheme of $\operatorname{Spec} A$, that is to say, the reducibility ideal $I = BC$ is not 0. Therefore, neither B nor C is 0. SInce they are fractional ideals of A, and A is principal, this does not leave us much choice: both B and C are as A-modules isomorphic to A (and as fractional ideals, they are of the form $\pi^b B$ and $\pi^c C$ with $b, c \in \mathbb{Z}$, $b + c \geq 1$). Now apply the proposition for $J = m = (\pi)$. Of course $\operatorname{Hom}_A(B, A/m) = k$ ad similarly for C, and the proposition tells us that the spaces $\operatorname{Ext}^1_{R\otimes k}(\bar{\rho}_1, \bar{\rho}_2)$ and $\operatorname{Ext}^1_{R\otimes k}(\bar{\rho}_2, \bar{\rho}_1)$ have dimension at least one. This is Ribet's lemma.

Now in the same situation as above, we are not obliged to take $J = m = (\pi)$. We can take any J that contains the reducibility ideal $I = BC$. Say $J = I$. Then the proposition tells us that the module $\operatorname{Ext}^1_{R\otimes A/I}(\rho_1, \rho_2)$ contains a module isomorphic to A/I. Since $I = (\pi^n)$, where n is defined in exercise 1.6, we get the result of that exercise.

But the most interesting aspect of our generalization of Ribet's Lemma is that A can be a much more general local ring that a d.v.r, with dimension greater than one and an rich geometry of its own. To get a sense of what our results says in general, let us focus on the case $J = m$, that is when we only are interested in constructing extensions of $\bar{\rho}_1$ by $\bar{\rho}_2$ over $A/m = k$ (instead of extensions of ρ_1 by ρ_2 over A/J). The A-module $\operatorname{Hom}_A(B, A/m) = \operatorname{Hom}_k(B/mB, k)$ is now the dual vector space of the k-vector space B/mB. By Nakayama's lemma, its dimension is the minimal number of elements of a generating family of B: let's call that $g(B)$. Therefore, the proposition says that

$$\dim_k \operatorname{Ext}^1_{R\otimes k}(\bar{\rho}_1, \bar{\rho}_2) \geq g(B),$$

that is we can construct $g(B)$ independent extensions of $\bar{\rho}_2$ by $\bar{\rho}_1$. Similarly,

$$\dim_k \operatorname{Ext}^1_{R\otimes k}(\bar{\rho}_2, \bar{\rho}_1) \geq g(C).$$

Now what can we say about $g(B)$ and $g(C)$. Well, $BC = I$, the reducibility ideal. It follows immediately that $g(B)g(C) \geq g(I)$. The number $g(I)$ is the minimal number of generators of I. It is at least equal to the codimension of $\operatorname{Spec} A/I$ in $\operatorname{Spec} A$, that is the codimension of the irreducibility locus. That is the smaller is the reducibility locus, the larger has to be $g(I)$, so the larger has to be $g(B)g(C)$, and the more extensions we construct. This is intuitive.

A special case that we will meet in practice is when the irreducibility locus is the smallest possible : the closed point of Spec A, that is $I = m$. In this case, we have $g(B)g(C) \geq g(m)$. But $g(m)$ is by Nakayama's lemma the dimension of m/m^2, which is the cotangent space of Spec A at its closed point. If d is the Krull dimension of A, we thus have $g(m) \geq d$, with equality if and only if A is regular ring by the theorem of Auslander-Buschbaum. In particular $g(B)g(C) \geq d$, and if A happens to be non-regular, $g(B)g(C) > d$. The geometry of A comes into the play.

3.4. **Ribet's generalization: the general case.**

Theorem 3.3. *Let $i, j \in \{1, \ldots, r\}$, $i \neq j$. Let J be an ideal containing the reducibility ideal I. Let $A'_{i,j} = +_{k \neq i,j} A_{i,k}A_{k,j}$. (We have obviously $A'_{i,j} \subset A_{i,j}$.) There exists a natural injective map of A-modules:*

$$\iota_{i,j} : \mathrm{Hom}_A(A_{i,j}/A'_{i,j}, A/J) \hookrightarrow \mathrm{Ext}^1_{R \otimes A/J}(\rho_j, \rho_i)$$

where ρ_i and ρ_j are the representations defined at the end of §3.2.

The construction of $\iota_{i,j}$ and proof of its injectivity if similar to the proof of Proposition 3.1. See [BC].

One can find that this method of construction of extensions (by hand, by giving explicitly the matrix representation of the extension) is much less elegant than Ribet's method which provides explicitly a free A-module Λ with G-action (a lattice) and see the extension in $\Lambda/m\Lambda$. Esthetic questions aside, it shall be useful in application to have a construction *a la ribet* of extensions. We can do that, but we have to give up the freeness assumption of the module.

Theorem 3.4. *Let $i \in \{1, \ldots, r\}$. There exists a natural finite torsion-free A-module M_i with as structure of R-modules, whose trace on the $M_i \otimes K$ is T (in particular M_i has generic rank d), and such that*

(i) *The $R \otimes k$-module $M_i \otimes k$ has semi-simplification $\oplus_{j=1}^r \bar{\rho}_j^{n_j}$ where the n_j are integers ≥ 1, and $n_i = 1$. Moreover $\bar{\rho}_i$ is a quotient of $M_i \otimes k$.*

(ii) *For J as in theorem 3.3, and $j \neq i$, every extension of ρ_i by ρ_j over A/J whose classes lies on the image of $\iota_{i,j}$ appears as a subquotient of M_i.*

Actually one takes M_i the injective hull of $\bar{\rho}_i$ in the category of $R/\ker T$-modules. We can show that as an A-module, $M_i = \oplus_{j=1}^d A_{i,j}^{d_j}$. For the proof, see [BC].

It can be proved (see [BC]) that all extension of ρ_i by ρ_j that appears as a subquotient of an R-module M which is finitely generated and torsion free as an A-module, and whose character of $M \otimes K$ is T appears in the image of $\iota_{i,j}$. In other words, the $\iota_{i,j}$ construction see all extensions that it is possible to construct using T.

3.5. **Exercises.**

Exercise 3.1. Let $A = \mathbb{Z}_p$, and let $R = A[X]$. Let $\rho : R \to M_2(A)$ be the morphism that sends X to the matrix $\begin{pmatrix} 1 & 1 \\ p^2 & 1 \end{pmatrix}$, and $T = \mathrm{tr}\,\rho$. Show that $T : R \to \mathbb{Z}_p$ is a pseudo-character of dimension 2, but that it is not residually multipilicty free. Show that $I = (p^2)$ is the smallest ideal of A such that $T \otimes 1 : R \otimes A/I$ is the sum of two non zero pseudo-characters. Show however that $T \otimes A/I$ is the sum of two pseudo-characters in several different ways.

Exercise 3.2. (difficult) Show by an example, that for a non-residually multiplicity free pseudocharacters, the reducibility ideal may not exist (of course, A has to be not a d.v.r)

Exercise 3.3. Let k be a field and $A = k[[X, Y, X]]/(XY - Z^2)$. Show that A is complete d.v.r with residue field k, and is a Noetherian domain. Let us call $K = \mathrm{Frac}(A)$. Let $B = XA + ZA \subset A$ and $C = A + (Y/Z)A \subset K$. Show that $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ is a generalized matrix algebra, and that its trace $T = \mathrm{tr}$ is a residually multiplicity free pseudocharacter of dimension 2. Show that T is not the trace of any representation $R \to M_2(A)$.

Exercise 3.4. (difficult) Assume that A is a unique factorization domain. Show that every residually multiplicity-free pseudocharacter$T : R \to A$ (for any A-algebra R) of dimension d (any d) is the trace of a representation $R \to M_d(A)$. (Hint : do first the case $r = 2$, which is simpler). It can e shown that the converses also hold: if every residually multiplicity-free pseudocharacter$T : R \to A$ of dimension d is the trace of a representation $R \to M_d(A)$, then A is a UFD.

Exercise 3.5. Prove theorem 3.3.

Exercise 3.6. With the notations of §3.3, and assuming that A is a domain (so that K is its fraction field).

a.– show that $T \otimes 1 : R \otimes K \to K$ is irreducible if and only if $B \neq 0$ and $C \neq 0$.

b.– **(difficult)** Assuming that T is the trace of a representation and that $I = m$, show that $max(g(B), g(C)) \geq g(I)$.

References

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

[C] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings* , preprint 2008

[R] K. Ribet, *A modular construction of unramified extension of* $\mathbb{Q}(\mu_p)$, inventiones math. 1976

[MW] B. Mazur & A. Wiles, *the main conjecture*

E-mail address: jbellaic@brandeis.edu

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

Automorphic forms for unitary groups and Galois representations Eigenvarieties of unitary groups

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

Prerequisites: The prerequisites for these lectures are:

(i) Notions on algebraic groups.
(ii) If possible, classical modular forms, and their adelic interpretation.
(iii) For the eigenvarieties part, some notion of rigid analytic geometry.

Notations: During most of the lecture, F will be a number field. The ring of adèles wil be denoted by $\mathbb{A}_F$ or simply $\mathbb{A}$. It is a product $\mathbb{A}_F = \mathbb{A}_{F,f} \times \mathbb{A}_{F,\infty}$ of finite adèles $\mathbb{A}_{F,f} = \mathbb{A}_f$ and infinite adèles $\mathbb{A}_{F,\infty} = \mathbb{A}_\infty = F \otimes_{\mathbb{Q}} \mathbb{R}$. When g is an adèle (or an idèle, or an adèle-valued point of a group scheme over F) we denote by g_f and g_∞ its finite and infinite componen. We often identify g_f with the adèle (or idèle, etc.) which ha has the same finite components and 0 (or 1) at all infinite component, and similarly for g_∞ so that $g = g_f + g_\infty$)or $g = g_f g_\infty$).

We shall denote by $\bar{\mathbb{Q}}$ the set of complex numbers that are algebraic over $\mathbb{Q}$. So $\bar{\mathbb{Q}}$ is supposed to be embedded in $\mathbb{C}$.

Contents

1. Unitary groups 2
1.1. Generalities 2
1.2. Unitary groups over totally real number fields 4
1.3. Adelic points of G 4
1.4. Local theory 5
2. Automorphic representations for G 8
2.1. Automorphic forms 9
2.2. Automorphic representations 9
2.3. Decomposition of automorphic representations 10
3. Galois representations 11
3.1. set-up 11
3.2. Existence 11
3.3. Properties 11

3.4. Hodge-Tate weights 12
4. The set of all automorphic forms of level U 13
References 15

This lecture is about automorphic forms and representations for unitary groups, and their attached Galois representations. The very existence of those attached representations is a recent progress that constitutes one of the most important achievement in the still largely open Langlands' program. It has been the result of a huge collective work of many mathematicians over more than thirty years (realizing an initial sketch, incredibly accurate in retrospect, of Langlands in the seventies). It is absolutely out of question to give or even tho sketch the proof of this existence in this paper.

The aim of this lecture is only to provide a short and intuitive introduction to automorphic forms and representations for unitary groups, and to state the existence and main properties of their attached Galois representations. Even simply giving a proper and workable definition of automorphic representations for a general unitary group is a task that cannot be properly done in less than 100 pages. There are many technical difficulties (especially at the archimedean places), which, through important, are not essential to the intuitive understanding of the notions. To avoid most of those difficulties, I will only consider a special case, namely unitary groups that are definite, that is compact at all archimedean places. While there are many arithmetical applications for which this special case may be sufficient, considering the general case is necessary in many other (including some that might be explained by Chris using Eisenstein series, which only exists for non-definite unitary groups) and moreover, the construction of Galois representations requires to consider non-definite places.

A natural question is: why unitary groups? The short answer is simply: because they are (with a few sporadic other cases, most notably Sp_4) the only algebraic group for which we know, at this point, how to attach Galois representation to automorphic representations. We should be able to do the same to many other automorphic representations (e.g. all algebraic automorphic representations for GL_n) but it seems that some very difficult new ideas are missing in order to do that.

1. Unitary groups

1.1. **Generalities.** Let k be a field of characteristic 0 (to simplify), and E be an étale algebra of degree 2 of k (that is to say, either E is $k \times k$ or it is a extension of degree 2 of E). The algebra E has only one non-trivial k-automorphism that we note c. Let V be a free k-module of rank n, and $q : V \times V \to E$ be a non-degenrate

c-Hermitian form. (That is to say, $q(x,y)$ is E-linear in x and c-semilinear in y, we have $q(x,y) = c(q(y,x))$ for all $x, y \in V$, and $q(x,y) = 0\ \forall y \in V$ implies $x = 0$.)

To these data (k, E, V, q) we can attach an algebraic group over k.

Definition 1.1. The *unitary group G attached to* (k, E, V, q) is the algebraic group whose functor of points is

$$G(R) = \{g \in \mathrm{GL}_{E\otimes_k R}(V \otimes_k R), \quad q(gx, gy) = q(x,y) \forall x, y \in V \otimes_k R\}.$$

for all k-algebra R. In the case where E is a field (rather than $k \times k$) we shall say that G is a true unitary groups.

Exercise 1.1. This definition implicitly assumes that the functor $R \mapsto G(R)$ is representable by a scheme over k. Prove it.

Intuitively, this is not very complicated. The k-points of the unitary group are the set of E-linear automorphism of V that preserves the hermitian form q. Similarly for R-points.

Example 1.1. Take $k = \mathbb{R}$, $E = \mathbb{C}$, $V = \mathbb{C}^n$ and

$$q((x_1, \dots, x_n), (y_1, \dots, y_n) = x_1 c(y_1) + \dots x_p c(y_p) - x_{p+1} c(y_{p+1}) - \dots - x_n c(y_n).$$

Then the unitary group attached to these date is denoted $U(p, n-p)$. The set of real points $U(p, n-p)(\mathbb{R})$ is the classical unitary group of signature $(p, n-p)$ in the sense of undergraduate mathematics. It is compact if and only if $p = 0$ or $p = n$. Note that $U(p, n-p)$ is isomorphic to $U(n-p, p)$. It is not hard that any true unitary groups over $\mathbb{R}$ is isomorphic to one of those $U(p, n-p)$.

Proposition 1.1. *If E is $k \times k$, then the unitary group G is isomorphic to* GL_n. *The is isomorphism is well-defined up to inner automorphism if we chose one of the two k-morphism $E \to k$.*

Proof — Let $p : E \to k$ be a k-morphism. The choice of p makes the isomorphism $E = k \times k$ (as k-algebra canonical, by saying tjat p is the first projection on $k \times k$. Let $V_0 = V \otimes_{E,p} k$. We construct an morphism of functors $G(R) \to \mathrm{GL}_R(V_0 \otimes_k R)$ by sending $g \in G(R)$ (an E-automorphism on $V \otimes_E R$) to its action on $V \otimes_E R \otimes_E k = V_0 \otimes_k R$. We leave to the reader to check that is an isomorphism. □

Now, let k' be any extension of k. We can consider $E' = E \otimes_k k'$ which is still an etale algebra over k' (but not that if E was a field, this may fail for E', hence the interest of the generality adopted), $V' = V \otimes_E E'$ which is still free of rank n over E, and q' the natural extension of q to V'. To the data (k', E', V', q') one can attach an unitary group G' over k'. It is clear from the definition that G' is $G \times_k k'$.

1.2. **Unitary groups over totally real number fields.** Let F be a totally real finite extension of $\mathbb{Q}$, and E be a quadratic extension of E that is imaginary.. Let c be the non-trivial automorphism of E over F. let V be an E-vector space of dimension n and q be a non-degenerate c-hermitian form on V. To (F, E, V, q) one can attach a unitary group G over F.

To get a better understanding of G we analyze the groups $G_v = G \times_F F_v$ for all places v of F.

If v is **archimedean**, then by assumption v is real, that is $F_v = \mathbb{R}$, and $E_v = \mathbb{C}$, while c induces the complex conjugation on $\mathbb{C}$. The group G_v is therefore $\mathbb{R}$-isomorphic to a group $\mathrm{U}(p_v, n - p_v)$ for some $0 \leq p_v \leq n$ as in example 1.1.

Definition 1.2. We shall say that G is *definite* if G_v is compact (that is $p_v = 0$ or $p_v = n$) for all real places v of F.

If v is **finite and split** in E, then $E \otimes_F F_v$ is not a field, but is isomorphic to $F_v \times F_v$. Therefore, the group G_v which is the unitary group attached to $(F_v, E \otimes_F F_v, \dots, \dots)$ is by Prop 1.1 isomorphic to GL_n over F_v. The choice of one of the two F_v-morphisms$E \otimes_F F_v$ to F_V, that is of one of the two places of E above v makes this isomorphism canonical, up to conjugation.

If v is *finite and either inert or ramified* in E, then E_v is a quadratic extension of F_v, so G_v is a true unitary groups of v.

The point to remember (for beginners) is that even a true unitary group over F becomes GL_n at basically one place of F over two: the places that are split in E. This will be very helpful later.

1.3. **Adelic points of G.** Let G be a unitary group as in the preceding §. Since the ring of adèles $\mathbb{A} = \mathbb{A}_F$ is an F-algebra (via the diagonal embeding), it make sense to talk of the group $G(\mathbb{A}_F)$. SInce G is linear, that is a subgroup of GL_m for some m, $G(\mathbb{A}_f) \subset M_m(\mathbb{A}_F) = \mathbb{A}_F^{m^2}$ which allots to give a natural topology on $G(\mathbb{A}_F)$, namely the coarsest that is finer that the topology of $\mathbb{A}_F^{m^2}$ and for which $x \mapsto x^{-1}$ is continuous. This topology is easily been seen to be independent of the choices. We shall need a good understanding of this group and of its natural topology.

Let $\mathcal{G}$ be a model of G over $\operatorname{Spec} \mathcal{O}_F[1/f]$ where $f \in \mathcal{O}_F - \{0\}$, that is a group scheme over this scheme whose generic fiber is G. Then for all v prime to f, the modeles define a subgroup $\mathcal{G}(\mathcal{O}_v)$ of $G(F_v)$ which is compact when v is finite. We can therefore form the restricted product $\prod'_{v \text{ places of } F} G(F_v)$ with respect to the subgroups $\mathcal{G}(\mathcal{O}_v)$.

Lemma 1.1. *This restricted product with its restricted product locally compact topology is independant of the model $\mathcal{G}$ chosen and is naturally isomorphic, as a topological group, with $G(\mathbb{A}_F)$.*

The same lemma of course holds for the finite adèles $G(\mathbb{A}_{F,f}) = \prod'_{v \text{ finite}} G(F_v)$ We have $G(\mathbb{A}_F) = G(\mathbb{A}_{F,f}) \times G(\mathbb{A}_{F.\infty})$.

The group $G(F)$ can be embedded diagonally in $G(\mathbb{A}_F)$. Its image is discrete. If G is definite, then $G(F)$ is discrete in $G(\mathbb{A}_{F,f})$ and the quotient is compact.

1.4. **Local theory.** In order to understand automorphic representations, we need to remind (without any proof) a very little part of the very important and still active theory of representations of p-adic Lie group.

1.4.1. *Brief review on smooth representations.* In this § only, G will be a group where there is basis of neighborhood of 1 made of compact open subgroups U.

Exercise 1.2. Prove that such a group is locally compact and totally disconnected. What about the converse?

Let k be a field of characteristic 0. By a *smooth representation* V of G over k we mean a k-vector space (not finite dimensional in general) with a continuous action of G such that for every vector $v \in V$, there exists a compact open subgroup U in G such that v is invariant by U.

A smooth representation is *admissible* if for every open subgroup U of G, V^U is finite dimensional over k.

Let us fix a (left invariant, but since in practice our G will be *unimodular*, this doesn't really matter) Haar measure dg on G, normalized such that the measure of some open compact subgroup U_0 is 1. Then is is easily seen that the measure of any other compact open subgroup will be a rational, hence an element in k.

We denote by $\mathcal{H}(G,k)$ the spaces of function from G to k that are locally constant and have compact support. This space as a natural product : the convolution of functions $(f_1 * f_2)(g) = \int_G f_1(x) f_2(x^{-1}g)\ dx$. Indeed, since f_1 and f_2 are in $\mathcal{H}(G,k)$, the integral is actually a finite sum, an what is more a finite sum of terms that are products of a value of f_1, a value of f_2, and the measure of a compact open subgroup. So the integral really defines a k-valued function, and it is easy to check that $f_1 * f_2 \in \mathcal{H}(G,k)$. This product makes $\mathcal{H}(G,k)$ an algebra, which is not commutative if G is not, and which is general has no unity (the unity would be a Dirac at 1, which is not a function on G if G is not discrete). If V is a smooth representation of G it has a natural structure of $\mathcal{H}(G,k)$-module by $f.v = \int_G f(g) g.v\ dg$. The algebra $\mathcal{H}(G,k)$ is called the *algebra of the group* G over k.

Let U be a compact open subgroup of G. Let $\mathcal{H}(G,U,k)$ be the set of functions form G to k that have compact support and that are both left and right invariant by U. This is easily seen to be a subalgebra of $\mathcal{H}(G,k)$, with unity (the unity is the characteristic function of U times a normalization factor depending on the Haar measure). The algebra $\mathcal{H}(G,U,k)$ is called the *Hecke algebra of* G *w.r.t* U over k. We have $\mathcal{H}(G,k) = \cup_U \mathcal{H}(G,U,k)$ and in particular we see that if G is not

commutative, the $\mathcal{H}(G,U,k)$ are not for U small enough. The Hecke algebra are important because of the following trivial property:

Lemma 1.2. *Let V be a smooth representation of G (over k). Then the spaces of invariant V^U has a natural structure of $\mathcal{H}(G,U,k)$-modules.*

Indeed, if $v \in V^U \subset$, and $f \in \mathcal{H}(G,U,k) \subset \mathcal{H}(G,k)$, $f.v$ is easily seen to be in V^U.

If there is one thing to remember about Hecke algebras it is this lemma, not the definition. In Jeopardy style : define the Hecke Algebra of G relatively to U... "What acts on V^U when V is a (smooth) representation of G? "

We will apply this theory to groups $G(F_v)$ when G is a unitary group as above and v is a finite place of F.

Exercise 1.3. Let k' be an extension of k.

a.— Show that if V is a smooth representation of G over k, then $V \otimes_k k'$ is a smooth representation of G over k'.

b.– Show that the formation of V^U commutes to the extesions k'/k.

c.– Show that $\mathcal{H}(G,U,k) \otimes_k k' = \mathcal{H}(G,U,k')$.

Exercise 1.4. Let $\mathcal{C}(G,k)$ and $\mathcal{C}(G/U,k)$ be the space of smooth functions from G and G/U to k.

a.– Show that they both are smooth representation of G (for the left translations)

b.– Show $\mathcal{C}(G,k)^U = \mathcal{C}(G/U,k)$. Therefore $\mathcal{H}(G,U,k)$ acts on $\mathcal{C}(G,U,k)$. Show that this action commutes to the G-action.

c.– Show that $\mathcal{H}(G,U,k)$ is actually naturally isomorphic to $\mathrm{End}_G(\mathcal{C}(G/U,k))$.

Exercise 1.5. a.– Show that $V \mapsto V^U$ is an exact functor form the category from smooth representation of G over k to $\mathcal{H}(G,U,k)$-module. This functor takes admissible representations to $\mathcal{H}(G,U,k)$ that are finite dimensional.

b.– Let $W = V^U$, $W' \subset W$ a sub-$\mathcal{H}(G,U,k)$-module, and $V' \subset V$ the subrepresentation of V generated by W'. Show that $V'^U = W$.

c.– Deduce that if V is irreducible as a representation of G, than V^U is irreducible as a $\mathcal{H}(G,U,k)$-module

Note that in general the functor defined in a.– above is not fully faithful (even on admissible rep.) and that the converse of c.– is false.

1.4.2. *Maximal compact subgroups.* If v is a finite place of F that splits in E, then $G(F_v) \simeq \mathrm{GL}_n(F_v)$. It is an easy fact that all maximal compact subgroups of $\mathrm{GL}_n(F_v)$ are conjugate (and conjugate to $\mathrm{GL}_n(\mathcal{O}_v)$.

If v is a finite place that does not spit in E, then $G(F_v)$ is a true unitary groups. It is not true that all maximal compact subgroups of $G(F_v)$ are conjugate, though there are only finitely many conjugacy class. If v is inert, then there is one class whose elements have maximal volume (for a fixed Haar measure), and we call compact of this class *maximal hyperspecial* compact subgroup of $G(F_v)$. We shall neglect places of F that ramify in E since there only in finite number.

Back to the case v split, we shall call any maximal compact subgroup hyperspecial.

Proposition 1.2 (Tits)**.** *Let $\mathcal{G}$ be a model of G over $\mathrm{Spec}\,\mathcal{O}_F[1/f]$. Then $\mathcal{G}(\mathcal{O}_v)$ is a maximal compact hyperspecial subgroup of $G(F_v)$ for almost all finite places v.*

Corollary 1.1. *Any compact open subgroup of $G(\mathbb{A}_f)$ contains a compact open subgroup of the form $\prod_v U_v$ with U_v a compact open subgroup of $G(F_v)$ for all v, with U_v maximal hyperspecial for almost all v.*

1.4.3. *Spherical Hecke algebras and unramified representations.* Let v be a place of F (not ramified in E), and K_v be a maximal compact hyperspecial subgroup of $G(F_v)$. Let k be any field of characteristic 0.

Proposition 1.3. *The algebra $\mathcal{H}(G(F_v), K_v, k)$ is commutative*

This fact is not a tautology. As we have seen, $\mathcal{H}(G(F_v), U)$ will certainly be non commutative for small enough compact open subgroups. The fact that it is commutative for K_v a well chosen maximal compact subgroup is what relates ultimately the theory of automorphic forms to commutative algebra, and is at the basis of all modern development ($R = T$. eigenvarieties, etc.) Instance of this phenomenon were first noticed by Poincare in his paper on the shape of Saturn's rings. The proposition above is due I guess, to Bruhat, and dates back to the early fifties.

Actually we can even determine the structure of the Hecke algebra $\mathcal{H}(G(F_v), K_v, k)$. We shall only need it in the case v split, so $\mathcal{H}(G(F_v), K_v, k) = \mathcal{H}(\mathrm{GL}_n(F_v), \mathrm{GL}_n(\mathcal{O}_v), k)$.

Proposition 1.4 (Satake)**.** *There exists an isomorphism of k-algebras*

$$\mathcal{H}(\mathrm{GL}_n(F_v), \mathrm{GL}_n(\mathcal{O}_v), k) \simeq k[T_1, \ldots, T_{n-1}, T_n, T_n^{-1}]$$

that sends T_i to the characteristic function of

$$\mathrm{GL}_n(\mathcal{O}_v)\, diag(\pi, \ldots, \pi, 1, \ldots, 1)\mathrm{GL}_n(\mathcal{O}_v),$$

where the number of π's is i.

Lemma and Definition 1.1. Let V be a smooth irreducible representation of $G(F_v)$ over k, and K_v a maximal hyperspecial subgroup of G. The statements $V^{K_v} \neq 0$ and $\dim_1 V^{K_v} = 1$ are equivalent. We call V *unramified* if they hold.

Actually this lemma follows from the proposition 1.3 above as follows: we can easily (see exercise 1.3) reduce to the case k algebraically closed and then since if V is irreducible, V^K is as a $\mathcal{H}(G, K_v, k)$-module (see exercise 1.5), hence has dimension one since the latter is commutative.

Here is an important observation: If V is unramified, V^{K_v} has dimension 1 and $\mathcal{H}(G(F_v), K_v, k)$ acts on V^{K_v}. Therefore, V determines a character

$$\psi_{V,v} : \mathcal{H}(G(F_v), K_v, k) \to k. \tag{1}$$

It is a theorem (that we shall not use) that V is uniquely determined by ψ_V.

The information containing in $\psi_{V,v}$ (that is the list of values $\psi_V(T_1), \dots, \psi_V(T_n)$ in k, the latter being non-zero), can be summarized in a polynomial, the Satake polynomial.

Definition 1.3. The Satake polynomial of V is the polynomial

$$P_{V,v}(X) = X^n - \psi_{V,v}(T_1)X^{n-1} + \psi_{V,v}(T_2)X^{n-2} - \dots + (-1)^n \psi_{V,v}(T_n) \in k[X].$$

Important caveat: This is not the correct normalization (for what follows). Actually coefficients should be multiplied by suitable integral power (or perhaps half-integral power) of the cardinality of the residue field. The correct form is to be found in Harris-Taylor's book. Without access to this book here , this would be an excessive effort (so close to the beach) to retrieve the correct coefficients. I'll put them after the conference.

Exercise 1.6. Prove Proposition 1.4 for $n = 2$, as follows. Replace first $\mathrm{GL}_2(K_v)$ by $G = \mathrm{PGL}_2(K_v)$ and K by the image of $\mathrm{GL}_2(\mathcal{O}_v)$ in G. Proceed as follows:

a.– Construct an isomorphism of G-representations $\mathcal{C}(G/K, k) = \mathcal{C}(X, k)$ where X is the tree of $\mathrm{PGL}_2(K_v)$ defined in the lectures note son Ribet's lemma, and $\mathcal{C}(X, k)$ the set of functions from X to k with finite support. Deduce (use exercise 1.4) an ismorphism of algebras $\mathcal{H}(G, K, k) \simeq \mathrm{End}_{k[G]}(\mathcal{C}(X, k))$.

b.– Let T_1 be the characteristic function of $K\mathrm{diag}\pi, 1K$. Show that this element of $\mathcal{H}(G, K, k)$, seen as an operator on $\mathcal{C}(X, k)$ by the baoce isomorphsim, sends a function f on X to the function $f'(x) = \sum_{y \text{ neighbor of } x} f(y)$.

c.– Deduce that $\mathcal{H}(G, K, k) = \mathbb{C}[T_1]$. Conclude.

2. Automorphic representations for G

We now fix a data (F, E, V, q) as in the preceding §and we assume that the group G is definite.

2.1. **Automorphic forms.**

Definition 2.1. A function $f : G(\mathbb{A}_F) = G(\mathbb{A}_{F,f}) \times G(\mathbb{A}_{F,\infty}) \to \mathbb{C}$ is said *smooth*, if it is continuous and if $f(g_f, g_\infty)$ is $\mathbb{C}^\infty$ as a function of g_∞ (for g_f fixed) and is locally constant with compact support as a function of g_f (for g_∞ fixed).

Definition 2.2. A function $f : G(\mathbb{A}_F) \to \mathbb{C}$ is called *automorphic* (or an *automorphic form*) if it is smooth, left-invariant by $G(F)$, and if it generates a finite dimensional spaces under $G(\mathbb{A}_{F,f})$. The space of all automorphic forms is called $A(G)$.

The space $A(G)$ has a natural hermitian product

$$(f, f') = \int_{G(F)\backslash G(\mathbb{A}_F} f(g)\bar{f}'(g)\ dg,$$

, which makes it a pre-Hermitian space (not a Hermitian space, since it is not complere). It has a natural action of $G(\mathbb{A}_F)$ by right translation, which preserves the hermitian product, so $A(G)$ is a pre-unitary representation.

2.2. **Automorphic representations.** An irreducible representation π of $G(\mathbb{A})$ is said *admissible* if, writing $\pi = \pi_f \otimes \pi_\infty$ where π_f is an irreducible representation of $G(\mathbb{A}_f)$ and π_∞ is an irreducible representation of $G(\mathbb{A}_\infty)$, then π_f is admissible.

Theorem 2.1. *The representation $A(G)$ is the direct sum of irreducible admissible representations of $G(\mathbb{A})$:*

$$A(G) = \bigoplus_\pi m(\pi)\pi, \tag{2}$$

where π describes all the (isomorphism classes of) irreducible admissible representations of $G(\mathbb{A})$, and $m(\pi)$ is the (always finite) multiplicity of π in the above space.

It will be convenient to denote by Irr the set (of isomorphism classes) of irreducible complex continuous (hence finite dimensional) representations of $G(\mathbb{A}_{F,\infty})$. For $W \in \mathrm{Irr}$, we define $A(G, W)$ to be the $G(\mathbb{A}_{F,f})$-representation by right translation on the space of smooth vector valued functions $f : G(\mathbb{A}_{F,f}) \longrightarrow W^*$ such that $f(\gamma g) = \gamma_\infty f(g)$ for all $g \in G(\mathbb{A}_{F,f})$ and $\gamma \in G(\mathbb{F})$.

Proof — (Sketch) As $G(\mathbb{A}_{F,\infty})$ is compact the action of this group on $A(G)$ is completely reducible, hence as $G(\mathbb{A}_F) = G(\mathbb{A}_{F,\infty}) \times G(\mathbb{A}_{F,f})$-representation we have:

$$A(G) = \bigoplus_{W \in Irr} W \otimes (A(G) \otimes W^*)^{G(\mathbb{A}_{F,\infty})}.$$

But we check at once that the restriction map $f \mapsto f_{|1\times G(\mathbb{A}_{F,f})}$ induces a $G(\mathbb{A}_{F,f})$-equivariant isomorphism

$$(A(G) \otimes W^*)^{G(\mathbb{A}_{F,\infty})} \simeq A(G, W).$$

As a consequence, the compactness of $G(F)\backslash G(\mathbb{A}_f)$ shows, by classical arguments that $A(G)$ is admissible, which together with the pre-unitariness of $A(G,W)$ proves the lemma. □

Definition 2.3. An irreducible representation π of $G(\mathbb{A})$ is said to be *automorphic* if $m(\pi) \neq 0$.

Automorphic representations (for definite unitary groups) are always algebraic, in the following sense.

Proposition 2.1. *If π is automorphic, the representation π_f has a model over $\bar{\mathbb{Q}}$.*

Proof — Let $W \in \mathrm{Irr}$ and let us restrict it to $G(F) \hookrightarrow G(\mathbb{A}_{F,\infty})$. As is well known W comes from an algebraic representation of G, hence the inclusion $\bar{\mathbb{Q}} \subset \mathbb{C}$ equips W with a $\bar{\mathbb{Q}}$-structure $W(\bar{\mathbb{Q}})$ which is $G(\bar{\mathbb{Q}})$-stable. As a consequence, the obviously defined space $A(G, W(\bar{\mathbb{Q}}))$ provides a $G(\mathbb{A}_f)$-stable $\bar{\mathbb{Q}}$-structure on $A(G,W)$, and the results follows. □

Definition 2.4. We say that a compact open subgroup U of $G(\mathbb{A}_f)$ is a *level* for an automorphic form π if $\pi^U \neq 0$. Equivalently $\pi_f^U \neq 0$. Or we say simply that π has level U. The weight of π is simply the finite dimensional representation π_∞.

Of course, if $U' \subset U$ and then if π has level U it has also level U'.

It is not hard to see that there exists only a finite number of automorphic representations with a fixed level and weight. (We shall not use it, but it fixes the ideas).

2.3. **Decomposition of automorphic representations.** Recall that if $(V_i)_{i\in I}$ is a family of vector spaces, with $W_i \subset V_i$ a given dimension 1 subspace defined for almost all i (that is forall i except for a finite set J_0 of I), then the restricted tensor product $\bigotimes'_{i\in I} V_i$ is defined as the inductive limit of $\bigotimes'_{i\in J} V_i \otimes \bigotimes_{i\in I-J} W_i$ over the filtering set ordered by inclusion, of finite subsets J (containing J_0) of I.

Theorem 2.2. *Every admissible irreducible representation π_f of $G(\mathbb{A}_{F,f})$ can be written in a unique way as a restricted tensor product $\pi_f = \otimes'_{v \text{ finite place}} \pi_v$ where π_v is a irreducible admissible representation of $G(F_v)$, and π_v is unramified for almost all v. More precisely, if $\pi_f^U \neq 0$ where $U = \prod_v U_v$, then $\pi_v^{U_v} \neq 0$.*

In particular, an automorphic representation $\pi = \pi_f \otimes \pi_\infty$ has components π_v at all places v of F: For finite v these are the components π_v of π_f in the above sense, and for infinite v, simply the component of π_∞ in the usual sense. If π_f has level $U = \prod_v U_v$, with U_v hyperspecial for all v except those in a finite set of places Σ, then π_v is unramified for $v \notin \Sigma$.

3. Galois representations

3.1. **set-up.** Let π be an automorphic representation of level U, and assume that U contains $\prod_v U_v$. Let $\Sigma(U)$ be the set of places v of F such that

(i) the place v splits in E

(ii) U_v is a compact maximal (necessariy hyperspecial) of $G(F_v)$

If $v \in \Sigma(U)$, then π_v is an unramified representation of $G(F_v)$, defined over $\bar{\mathbb{Q}}$. The choice of one of the two places w of v defines an isomorphism (up to conjugacy) $G(F_v) \simeq \mathrm{GL}_n(F_v)$, so allows us to see π_v as a well-determined up to isomorphism representation of $\mathrm{GL}_n(F_v)$. To such a representation one can attach its Satake polynomial, that we shall denote by $P_{\pi,w}(X)$.

3.2. **Existence.** The following theorem may now be considered as proven (even if some details have not yet appeared in print).

Let us fix an embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$.

Theorem 3.1. *Let p be a prime. There exists a unique semi-simple Galois representations $\rho_\pi : G_E \to \mathrm{GL}_n(\mathbb{Q}_p)$ such that at all places v of F in $\Sigma(U)$ such that v does not divide p, then for the two places w of E above v, ρ_π is unramified at w, and the characteristic polynomial of $\rho_\pi(\mathrm{Frob}_w)$ has coefficients in $\bar{\mathbb{Q}}$ and is equal to $P_{\pi,w}$.*

Note that the representation ρ_π is a representation of G_E, not of G_F Let us prove the uniqueness: The set of w above a place in $\Sigma(\pi)$ has density one in G_E. Therefore by Cebotarev, the set of such Frob_w in G_E is dense, and in particular the character of ρ_π is well determined by our condition. Therefore so is ρ_π since it is assumed semi-simple. (the proof of existence is about five thousand times longer).

3.3. **Properties.** The representation ρ_π enjoys many more properties. Let us give the most important ones.

(i) The non trivial automorphic $c \in \mathrm{Gal}(E/F)$ induces by conjugation an outer automorphism of G_E, still denoted c. We have $\rho_\pi^c = \rho_\pi^*(1-n)$. In particular ρ_π is polarized in the sense of my notes on Bloch-Kato.

This is easy by looking at the form of the characteristic polynomials $P_{\pi,w}$ and $P_{\pi,w'}$ where w and w' are the two places above v, where v is as in the theorem. Of course, I have not been explicit enough about the normalization so that you can check the details.

(ii) If v is any place of F where π is unramified, and w is a place of E above v, then ρ_π is unramified at v. (this is contained in the theorem for v split, but this also true for v inert.) In particular ρ_π is unramified almost everywhere.

(iii) For v split, and w above v, the restriction of ρ_π to G_{E_w} corresponds by Local Langlands to the representation π_v of $G(F_v)$ seen as a representation of $\mathrm{GL}_n(F_v)$ using the isomorphism determined by w. This determines what

happens at all split v, for π unramified or not at v. (the analog statement for v non-split is not known in full generality so far).

(iv) The representations ρ_π is de Rham at all places dividing p and the Hodge-Tate weights are determined by π_∞. The representation ρ_π is even crystalline at those places w of E that are unramified above places v of F such that π_v is unramified. The crystalline Frobenius slope are determined by π_∞ and $P_{\pi,w}$.

(v) The representation ρ_π is geometric. (This follows from (ii) and (iv)). In most cases (technically, if π_∞ is regular – see below), it is know by construction that ρ_π actually comes from geometry. If ρ_π is irreducible, it is pure of motivic weight, $1-n$.

(vi) The L-function $L(\rho_\pi, s)$ satisfy all conjectures about L-functions sated in my BK notes (continuation, no zeros on the boundary of the domain of convergence, no poles exceot trivial case, functional equation).

Note that ρ_π is not irreducible in general. We can construct examples (*endoscopic* forms and *C.A.P* forms) of π for which ρ_π is reducible, and even some where its constituents have not all the same motivic weights (in those cases though, the set of motivic weights is an arithmetic progression of ratio 1). However, for a large class of representations π called *stable* (defined as those π whose base change to GL_n/E is cuspidal), it is expected that ρ_π is irreducible. It is known so far only if $n \leq 3$ (Blasius-Rogawsky for $n=3$), $n=4$ if $F=\mathbb{Q}$ and $\pi^c = \pi$ (Ramakrishna) or any n and E but π_v square integrable at some place v of F split in E (Taylor-Yoshida).

3.4. **Hodge-Tate weights.** We here explain how the weight π_∞ of π determine the HT weights of ρ_π. For simplicity, we do so only in the case where $F=\mathbb{Q}$ and p splits in F. In this case π_∞ is simply a representation of the compact Lie group $U(n)(\mathbb{R})$, necessarily finitely dimensional.

If $\underline{m} := (m_1, \dots, m_n) \in \mathbb{Z}^n$ satisfies $m_1 \geq m_2 \geq \cdots \geq m_n$, we denote by $W_{\underline{m}}$ the rational (over $\mathbb{Q}$), irreducible, algebraic representation of GL_m whose highest weight relative to the upper triangular Borel is the character[1]

$$\delta_{\underline{m}} : (z_1, \cdots, z_n) \mapsto \prod_{i=1}^{n} z_i^{m_i}.$$

For any field F of characteristic 0, we get also a natural irreducible algebraic representation $W_{\underline{m}}(F) := W \otimes_{\mathbb{Q}} F$ of $\mathrm{GL}_n(F)$, and it turns out that they all have this form, for a unique $\underline{m}$.

Let us fix an embedding $E \hookrightarrow \mathbb{C}$, which allows us to see $\mathrm{U}(n)(\mathbb{R})$ as a subgroup of $\mathrm{GL}_n(\mathbb{C})$ well defined up to conjugation (see Prop.1.1). So for $\underline{m}$ as above, we can view $W_{\underline{m}}(\mathbb{C})$ as a continuous representation of $\mathrm{U}(n)(\mathbb{R})$. As is well known, the set of all $W_{\underline{m}}(\mathbb{C})$ is a system of representants of all equivalence classes of irreducible

[1]This means that the action of the diagonal torus of GL_n on the unique $\mathbb{Q}$-line stable by the upper Borel is given by the character above.

continuous representations of $\mathrm{U}(m)(\mathbb{R})$. We will say that $W_{\underline{m}}$ has *regular weight* if $m_1 > m_2 > \cdots > m_n$.

So by the above $\pi_\infty = W_{\underline{m}}(\mathbb{C})$. The identification depends on an embedding of E to $\mathbb{C}$ hence an embedding of E to the field $\bar{\mathbb{Q}}$ of algebraic number in $\mathbb{C}$, hence via the chosen embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$, an embedding $E \hookrightarrow \bar{\mathbb{Q}}_p$, that is a place w of E above p.

Proposition 3.1. *The Hodge-Tate weights of* $(\rho_\pi)_{|G_{E_w}}$ *are* $k_1 = -m_1 + 1, k_2 = -m_2 + 2, \ldots, k_n = -m_n + n$.

Note that the Hodge-Tate weights are always distinct (this is a consequence of our working with a definite unitary group, analog to the fact that "modular forms of weight 1 (that is of HT weights 0 and 0) are not quaternionic modular forms"). When π_∞ is regular, two Hodge-Tate weights are never consecutive numbers.

Exercise 3.1. a.– If w' is the other place of E above p, what are the Hodge-Tate weights of $(\rho_\pi)_{|G_{E_{w'}}}$?

b.– Is your answer conform to prediction 2.1 in the BK notes ?

4. The set of all automorphic forms of level U

We begin to move slowly toward the definition of eigenvariety.

From now, for simplicity we shall assume that $F = \mathbb{Q}$.

We shall fix an open compact subgroup U of $G(\mathbb{A}_f)$ as in 3.1, of which we keep all notations. We consider automorphic representations of level U, but any weight.

Let $\Sigma = \Sigma(U)$ be as above the set of places of F that are split in v and such that U_v is hyperspecial. Let $\mathcal{H}_\Sigma = \otimes_{v \notin \Sigma} \mathcal{H}(G(\mathbb{Q}_v), U_v, \bar{\mathbb{Q}})$. This is a commutative $\bar{\mathbb{Q}}$-algebra. Every automorphic representation π of level U defines a character

$$\psi_\pi : \mathcal{H}_\Sigma \to \bar{\mathbb{Q}} :$$

This characters sends a $T \in \mathcal{H}(G(\mathbb{Q}_v), U_v, \bar{\mathbb{Q}})$ to its eigenvalues on $\pi_v^{U_v}$ for all $v \in \Sigma$.

The character ψ_π contains a lot of the information of interest about π. In particular it determines the Galois representation ρ_π.

Let $\mathcal{Z}_U$ be the set of all characters of the form $\psi_\pi : \mathcal{H}_\Sigma \to \bar{\mathbb{Q}}$ of the form ψ_π for some automorphic π of level U. The set $\mathcal{Z}_U$ is enumerable, and there is of course a surjective map $\pi \to \psi_\pi$ from the set of automorphic forms of level U to $\mathcal{Z}_U$. This map is not injective in general (its fiber are called (approximately) the L-packets for $G(\mathbb{A})$.) As we have just noticed, the map $\pi \mapsto \rho_\pi$ factors through $\mathcal{Z}_U$.

We want to understand the set $\mathcal{Z}_U$.

Let us choose a topology on $\mathcal{Z}_U$ as follows. Let $|\ |$ be an absolute value of $\bar{\mathbb{Q}}$. We put a metric (that could take infinite value) on $\mathcal{Z}_U$ by saying that $d(\psi, \psi') = \sup_{v \in \Sigma,\ w|v,\ i=1,\ldots,n} |\psi(T_{i,w}) - \psi'(T_{i,w})|$. This determines a topology of $\mathcal{Z}_U$.

It is a fact that if $|\ |$, the set $\mathcal{Z}_U$ for that topology is discrete. There is not much to say about this: There is no continuous archimedean families of automorphic forms for a definite unitary group. (Of course, for a non-definite unitary groups, there are the families of Eisensteins series studied by Langlands).

Now let p be a prime and assume that $|\ |$ is a p-adic absolute value of $\bar{\mathbb{Q}}$. (Say for compatibility the one induced by the embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ we have already chosen). Then it is a fundamental fact, the basis of the theory of eigenvarieties, that $\mathcal{Z}_U$ is **not discrete**. Actually, we shall see that no point in $\mathcal{Z}_U$ is isolated. (I believe this point was first observed by Serre, though Ramanujan and Swinnerton-Dyer are precursors)

In that respect, $\mathcal{Z}_U$ is closely analog to $\mathbb{Z}$: $\mathbb{Z}$ has an archimedean topology, for which it is discrete, and a p-adic topology (for each p), for which it is not discrete, and even without isolated point. Can we put the analogy further. By the completion process, the points of $\mathbb{Z}$ (the integers) can be p-adically interpolated to define points of $\mathbb{Z}_p$ (p-adic numbers). Can the points of $\mathcal{Z}_U$ (the automorphic forms) can be p-adically interpolated to define more general object (p-adic automorphic forms)? As we shall see, yes. Let us put the the analogy further again. The topological space $\mathbb{Z}$ is a Zariski-dense subset of the set of $\mathbb{Q}_p$-points $\mathbb{Z}_p = B^1(\mathbb{Q}_p)$ of the rigid analytic variety $B^1 = \mathrm{Sp}\,\mathbb{Q}_p < T >$. Can we find a natural rigid analytic variety $\mathcal{E}$ such that $\mathcal{Z}_U \subset \mathcal{E}(\mathbb{Q}_p)$ in the same way? Until we precise our requirement on $\mathcal{E}$, the question is a little bit too vague to have an interesting answer. So let us try to precise it.

We fix an embedding $E \subset \mathbb{C}$, and we assume that p is split in E, and that U_p is a maximal compact (so that $p \in \Sigma$). As we have seen, this determines a place w of E above p and for every π of level U, a set of integers $k_1(\pi) < \cdots < k_n(\pi)$ (as in Prop **??**). Let $\mathbb{Z}^n_<$ be the set of such n-uples of integers. The integers $k_1(\pi), \ldots, k_n(\pi)$ are the weights of $(\rho_\pi)_{|G_{E_w}}$. Therefore, they only depends on ρ_π, so they only depend on ψ_π. We thus have a map $\kappa : \mathcal{Z}_U \to \mathbb{Z}^n_<$, which attaches to ψ_π the uple $(k_1(\pi), \ldots, k_n(\pi)$.

Proposition 4.1. *The map κ has finite fibers. If we put on $\mathbb{Z}^n_<$ the topology such that $(k_1, \ldots, k_n)$ is close to $(k'_1, \ldots, k'_n)$ if and only if $k_i \equiv k'_i \pmod{(p-1)p^m}$ for big m, then κ is continuous.*

Proof — The fact that κ has finite fibers results from the fact that there exits only a finite number of automorphic forms with fixed level and weight. To prove that it is continuous, we note that $\psi_\pi \mapsto \rho_\pi$ is by definition continuous for the p-adic topology. The fact that the weights of ρ are continuous in ρ is a result of Wittenberger (with a recent different proof by Berger-Colmez). The proposition follows. □

Now it easy, and standard, to interpolate the topological $\mathbb{Z}^n_<$ by defining the rigid analytic space $\mathcal{W}$ over $\mathbb{Q}_p$ whose set of R-points are $\mathcal{W}(R) = \mathrm{Hom}_{\mathrm{cont}}((\mathbb{Z}_p^*)^n, R^*)$ where R is any $\mathbb{Q}_p$-affinoid algebra. Indeed, we can see $\mathbb{Z}^n_<$ as a subset of $W(\mathbb{Q}_p)$ by sending $(k_1, \ldots, k_n)$ to the continuous morphim of groups $(z_1, \ldots, z_n) \mapsto z_1^{k_1} \ldots z_n^{k_n}$ from $(\mathbb{Z}_p^*)^n$ to $\mathbb{Q}_p^*$, and the induced topology on $\mathbb{Z}^n_<$ is precisely the $\pmod{(p-1)p^m}$ we have put on it. The space $\mathcal{W}$ (geometrically a disjoint union of $(p-1)^n$ copies of a unit ball) is called the *the weight space*.

Now in view of Prop 4.1, it is natural to ask the question : can we find a natural rigid analytic space $\mathcal{E}$ over $\mathbb{Q}_p$ with a locally finite map $\kappa : \mathcal{E} \to W$ such that we can see $\mathcal{Z}_U$ (with its p-adic topology) as a subset of $\mathcal{E}(\mathbb{Q}_p)$, Zariski-dense in U, such that the restricion of κ to $\mathcal{Z}_U$ has image in $\mathbb{Z}^n_<$ and is just the map κ defined above?

Unfortunately, the answer is no. I have missed a turn somewhere...

To be continued

References

E-mail address: jbellaic@brandeis.edu

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