Travaux mathématiques, Volume 23 (2013), 5–35,

Galois representations

by Gebhard Böckle

Abstract

The present notes develop some basic language on Galois representations and strictly compatible families of such. As guiding examples we use elliptic curves, (Hilbert) cusp forms and the (partially conjectural) relation between the two. The notion of strict compatibility in families at ramified primes is used to motivate Weil-Deligne representations and p-adic Hodge theory à la Fontaine. The notes end with a rough sketch of how to use the concepts presented to give a proof of the modularity of elliptic curves over $\mathbb{Q}$. The emphasis throughout the notes is to explain the interrelations and usefulness of the concepts covered. Proofs are mostly omitted, but many references to the (vast) literature are given.

These notes are a slightly expanded version of parts of a lecture series at the Luxembourg Winter School 2012, organized by Gabor Wiese, Lior Bary-Soroker and Sara Arias-de-Reyna. The notes claim no originality.

MSC (2010): 11F80, 11F33, 11F41, 11F85, 11G05, 11S20, 11S37.

Contents

1 Introduction

The main focus of the present notes are Galois representations, which are an important tool in modern number theory: Galois representations provide a convenient and concrete way to represent a geometric object over a number field. Via these representations, the geometric object tells us much about quotients of the absolute Galois group of its underlying number field. Moreover Galois representations provide one with a tool to compare geometric objects: in the simplest form, such a comparison could be that two objects are related if they have isomorphic Galois representations. Already this very basic notion has deep consequences, as we shall see.

These notes do not wish to give an axiomatic treatment. They will not explain what a general "geometric object" (a motive) could mean. They focus on examples, mainly those of elliptic curves and (Hilbert) modular forms. Each example will provide us with a family of Galois representations, one member for each of the primes of the coefficient field of the object. This motivates us not only to describe the individual members, but also to place the families within the setting of compatible systems of Galois representations. We proceed in several steps:

Section 2 locates Galois representations within number theory, indicates some applications of Galois representation from automorphic forms, and fixes some notation. In Section 3 we describe, following our two main examples, a notion of compatible system that only uses unramified primes. This is enough to characterize the representation up to isomorphism. In practice it is also very useful to have a notion of compatibility at the ramified primes. This requires Weil-Deligne representations, which we introduce in Section 4. After this, the only primes that are not included into a notion of compatibility are those that divide the residue characteristic of the coefficient field of the Galois representation. This needs p-adic Hodge theory, of which we give some flavor in Section 5. The following Section 6 surveys some standard predictions of the Fontaine-Mazur conjectures which try to answer the question which Galois representations one can hope to find in geometry. The final Section 7 indicates the role of Galois representations in modularity proofs of elliptic curves – such as the proof of Fermat's Last Theorem by Wiles and Taylor-Wiles – a theme repeatedly discussed throughout the text. The material is supplemented by an extensive bibliography, to which we give detailed references in the main text.

Acknowledgements: Many thanks go to Sara Arias-de-Reyna, Hendrik Verhoek, Gabor Wiese for comments, corrections and suggestions. I would also like to thank the referee for many corrections and helpful suggestions.

2 Number theory and Galois representations

2.1 The absolute Galois group of a number field

Basic question: Describe all Galois extension of a number field of a certain type. **But** this is too difficult!

Much of current day number theory is concerned with understanding extensions E/F of a number field F and their ramification properties. In applications one is mostly concerned with the case that E/F is Galois. Since the absolute Galois group $G_F = \mathrm{Gal}(\bar{F}/F)$ is profinite, it suffices to understand all finite Galois extensions, although it is often useful to consider profinite extensions. To understand the ramification properties it is also important to understand the absolute Galois group of a local field. This is considerably simpler and for $p > 2$ it is actually solved by Koch and Jannsen-Wingberg, see [JW82].

2.2 Abelian Class Field Theory versus the Langlands program

The first main success in understanding Galois extensions of number fields is abelian class field theory. It gives a complete classification of all abelian extensions and their ramification properties.

Abelian class field theory by itself is rarely constructive. Over $\mathbb{Q}$ the cyclotomic extensions generate $\mathbb{Q}^{\mathrm{ab}}$. Over CM fields one can consider CM abelian varieties and the Galois representations attached to their torsion points. The theory over quadratic imaginary fields can be found in [Si91]. For the general CM case, see [Sh98]. Beyond this little is known. For certain conjectural constructions, see [Da04].

Beginning in the late 1960's, mainly due to Langlands a new approach developed. The abelian case was considered as the GL_1 case. Langlands idea was to use automorphic forms and representations to develop a class field theory for GL_n. Automorphic representations for a reductive group G over F should give rise to Galois representations into the dual group of G and in a vague sense all such Galois representations should come from automorphic representations and thus from modular forms. In fact to get modular forms, one needs to require some algebraicity of the automorphic representations. But this would get us too far from the topic. The so far most successful case is the group GL_2 over totally real fields. Other cases beyond these lectures are unitary groups (i.e., inner forms of GL_n) and symplectic groups. References are [AEK03], [BC09], [La03].

The Langlands program is constructive whenever one has an algebraic theory of automorphic forms. This seems to lead to a similar constraint as above: The automorphic forms have to be defined over a totally real or a CM field.

Another important source of Galois representations is étale cohomology. In fact, in all cases above, one uses étale cohomology to construct Galois represen-

tations from some geometric data. A priori étale cohomology seems to give much more representations than the theory of automorphic forms. But in the end, one might hope that all geometric semisimple Galois representations come from automorphic forms; see [Bel09].

For time constraints, I shall say nothing about the automorphic side; local Langlands correspondence, compatibilities, etc.

2.3 Applications of Galois representations from automorphic forms:

Much of the following developments go back to Wiles work on Fermat's Last theorem (FLT):

(a) The Taniyama-Shimura conjecture, which is a theorem by Breuil-Conrad-Diamond-Taylor [BCDT], states that every elliptic curve over $\mathbb{Q}$ is modular.

(b) By results of Frey, Ribet and Serre [Ri90, Se87](proved in the 80's) this implies FLT.

(c) Wiles proof of FLT established sufficiently many cases of Taniyama-Shimura to deduce FLT; [Wi95, TW95], of which good surveys are [DDT97] and [CSS].

(d) For elliptic curves A over an arbitrary totally real number field F, it follows that if they are modular, then their L-function has an entire continuation to the complex plane. Using potential modularity, Taylor has proved results that show in many cases that the L-function of A/F has a meromorphic continuation to $\mathbb{C}$. See for instance [Sn09, Tay06].

(e) If one could show that $\mathrm{Sym}^n A$ is modular for all $n \in \mathbb{N}$ and all elliptic curves A/F without CM, then the Sato-Tate conjecture on the deviation of $\#A(k_v)$ from $\#k_v + 1$ follows for A. One cannot quite show that. But one can prove potential versions of this which suffice to prove the conjecture: [BLGG, CHT, HSBT, Tay08].

Here is the heuristic for the Sato-Tate distribution: Let X be the set of conjugacy classes of elements in $\mathrm{SU}_2(\mathbb{C})$. A representative of a conjugacy class is of the form $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$. Therefore conjugacy classes can be considered as elements $\theta \in \mathbb{R}/\pi\mathbb{Z}$. Consider

$$\mathrm{SU}_2(\mathbb{C}) \to X \cong [0,\pi] \overset{-\cos}{\cong} [-1,1].$$

The pushforward of the measure of equi-distribution on $\mathrm{SU}_2(\mathbb{C})$ yields the measure with distribution $\frac{2}{\pi}\sin^2\theta \mathrm{d}\theta$ on $[0,\pi]$, or $\frac{2}{\pi}\sqrt{1-t^2}\mathrm{d}t$ on $[-1,1]$.

The ST-conjecture asserts that for $\ell \to \infty$ (or $\lambda \to \infty$), the distribution of the numbers

$$\frac{a_\ell(A)}{2\sqrt{\ell}} \in [-1,1]$$

(for an elliptic curve A without complex multiplication), and of the numbers

$$\frac{a_\lambda(f)}{2\lambda^{(k-1)/2}}$$

(for a modular form f of weight k and without complex multiplication) converges to a measure on $[-1,1]$ with the ST-distribution

$$\frac{2}{\pi}\sqrt{1-t^2}\mathrm{d}t.$$

In one lecture of the course notes [Ha07], by Michael Harris, on the proof of the Sato-Tate conjecture by Clozel, Harris, Shepherd-Barron and Taylor, the relation between the Sato-Tate conjecture and the meromorphy of the L-function of $\mathrm{Sym}^n A$, $n \in \mathbb{N}$ is explained.

2.4 Some notation

(a) For a number field F fix an algebraic closure $\bar{F} = \bar{\mathbb{Q}}$.

(b) For a place v, i.e., an equivalence class of norms on F, let F_v be the completion of F at v and fix an algebraic closure $\bar{F}_v$.

(c) If v is non-archimedean, define $\mathcal{O}_v$ as the ring of integers of F_v, π_v as a uniformizer, k_v as the residue field at v and $q_v := \#k_v$ is the order of k_v.

(d) Fix an embedding (i.e., an F-algebra homomorphism) $\bar{F} \hookrightarrow \bar{F}_v$. This yields a homomorphism of Galois groups $G_v := G_{F_v} \to G_F$ (known to be injective) from the diagram

$$\begin{array}{ccc} \bar{F} & \longrightarrow & \bar{F}_v \\ {\scriptstyle \mathrm{Gal}(\bar{F}/F)=:G_F}\big| & & \big|{\scriptstyle G_{F_v}=:G_v} \\ F & \longrightarrow & F_v \end{array}$$

(e) For a set of places S of F, denote by $G_{F,S}$ the quotient of G_F that is the Galois group of the maximal extension of F in $\bar{F}$ unramified outside S.

(f) For v a place not in S, fix a Frobenius automorphism $\mathrm{Frob}_v \in G_{F,S}$ which is unique up to conjugation. (The kernel of $G_v \to G_{F,S}$ contains the inertia subgroup of G_v and $G_v/I_v \cong G_{k_v}$ which in turn is generated by the Frobenius. We take the geometric Frobenius.)

3 L-functions and Galois representations

3.1 Elliptic curves

Let A be an elliptic curve over a number field F.
Let N be the conductor of A. It is defined as a product of local conductors.

The latter are 1 at every place of good reduction of A. If A does not have good reduction at v, then the prime corresponding to v divides N.

Definition 3.1. (a) For a prime ℓ, denote by $\mathrm{Ta}_\ell(A)$ the G_F representation on $\varprojlim A[\ell^n](\bar{F})$ and write $V_\ell(A)$ for $\mathrm{Ta}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

(b) The L-factor of A at v is $L_v(A,T) := \det(1 - T\mathrm{Frob}_v | V_\ell(A)^{I_v})^{-1}$

(c) The L-function of A is

$$L(A,s) := \prod_{v \text{ finite}} L_v(A, q_v^{-s}) \text{ for } \Re(s) \gg 0.$$

It is not clear that the L-factors are independent of ℓ. So in principle ℓ should occur in the above notation. However part (b) of the following result clarifies this problem and shows the independence of ℓ, assuming that $v \nmid \ell$.

Theorem 3.2 (see [Si85], [Si91])**.** *(a) If $v \nmid \ell$, then the representation $V_\ell(A)$ is ramified at v if and only if v divides the conductor N (Theorem of Néron-Ogg-Shafarevich).*

(b) If $v \nmid N\ell$, then $L_v(A,T)^{-1} = 1 - a_v(A)T + q_v T^2$ where $L_v(A,1)^{-1} \stackrel{!}{=} \#A(k_v)$ defines $a_v(A)$.

(c) If v divides N but not ℓ, then $L_v(A,T)$ can be computed by Tate's Algorithm.

(d) The L-function defined above converges for all $s \in \mathbb{C}$ with $\Re(s) > 3/2$.

(e) The representation $V_\ell(A)$ is semisimple.

3.2 On traces and characteristic polynomials

Lemma 3.3. *Let Π be a profinite group, let $\mathcal{F} \subset \Pi$ be a subset such that Π is the topological closure of the conjugacy classes of $\mathcal{F}$, and fix a positive integer n. Then any continuous* semi-simple *representation $\rho\colon \Pi \to \mathrm{GL}_n(L)$ where $L \in \{\mathbb{C}, \overline{\mathbb{F}_\ell}, \overline{\mathbb{Q}_\ell}\}$ is uniquely determined by the characteristic polynomials* $\mathrm{charpol}(\rho(g)) \in L[T]$ *for $g \in \mathcal{F}$.*

For $\mathbb{C}$ this is classical representation theory, for $\overline{\mathbb{F}_\ell}$ this follows from the theorem of Brauer-Nesbitt, see [CR62, 30.16]. A proof for $\overline{\mathbb{Q}_\ell}$ is in [Tay91].

Theorem 3.4. *Given $E/\mathbb{Q}_\ell$ finite and V a finite dimensional continuous linear G_F representation over E. Let k_E be the residue field of E, i.e. $k_E = \mathcal{O}_E/\mathfrak{m}_E$.*

(a) If V is semisimple, then there is a set S of density zero outside of which V is unramified.

(b) In the situation of (a), one has $\det(1 - T\mathrm{Frob}_v | V) \in \mathcal{O}_E[T]$ *for all $v \notin S$ and ρ is completely determined by these characteristic polynomials, or even the traces of $\rho(\mathrm{Frob}_v)$, $v \notin S$.*

(c) There exists a unique continuous semisimple G_F-representation $\bar{V}$ with

$$\det(1 - T\mathrm{Frob}_v|\bar{V}) \equiv \det(1 - T\mathrm{Frob}_v|V) \mod \mathfrak{m}_E \text{ in } k_E[T] \quad \forall v \notin S.$$

Proof. (a) See [KR01]. (b) Follows from the existence of a G_F-stable lattice (which is deduced from the compactness of G_F) and Lemma 3.3. (c) One reduces the lattice from (b), semisimplifies the reduction and applies Lemma 3.3. □

Corollary 3.5. *Let A/F be an elliptic curve. Then $V_\ell(A)$ is completely characterized by the condition* $\mathrm{Trace}(\mathrm{Frob}_v|V_\ell(A)) = a_v(A)$ *for all finite places v not dividing $N\ell$*

3.3 Hilbert modular forms

The following definitions are from [Tay89]. General texts on Hilbert modular forms are [BGHZ], [Fr90], [Go02], [Hi06] and references therein.

Let F be a totally real number field. Let I be the set of embeddings $F \hookrightarrow \mathbb{R}$. Denote by $\mathbb{A}_F$ the adele ring of F. Write $\mathbb{A}_F = \mathbb{A}_f \times \mathbb{A}_\infty$ for the decomposition into the finite and infinite adeles. Fix $k = (k_\tau) \in \mathbb{Z}^I$ such that $k_\tau \geq 2$ for each component. and suppose that all components have the same parity.[1] Set $t = (1, \ldots, 1) \in \mathbb{Z}^I$, and set $m = k - 2t$. Also choose $v \in \mathbb{Z}^I$ such that each $v_\tau \geq 0$, some $v_\tau = 0$ and $m + 2v = \mu t$ for some $\mu \in \mathbb{Z}_{\geq 0}$. Set $\mathfrak{h} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$.

For $f\colon \mathrm{GL}_2(\mathbb{A}_F) \to \mathbb{C}$ and $u = u_f u_\infty \in G_f \times G_\infty = \mathrm{GL}_2(\mathbb{A}_F)$ define

$$(f|_k u)(x) := j(u_\infty, \underline{i})^{-k} \det(u_\infty)^{v+k-t} f(xu^{-1})$$

where:

- $\underline{i} = (\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathfrak{h}^I$;
- $j\colon G_\infty \times \mathfrak{h}^I \to \left(\mathbb{C}^*\right)^I, \left(\begin{pmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{pmatrix}_{\tau \in I}, \left(z_\tau\right)_{\tau \in I}\right) \mapsto (c_\tau z_\tau + d_\tau)_{\tau \in I}$;
- $(\alpha_\tau)^{(n_\tau)} := \prod_{\tau \in I} \alpha_\tau^{n_\tau}$ for $(\alpha_\tau) \in (\mathbb{C}^*)^I$ and $(n_\tau) \in \mathbb{Z}^I$.

Definition 3.6. For $U \subset G_f$ a compact open subgroup one defines the space of Hilbert modular cusp forms $S_k(U)$ of level U and weight k to be the set of functions $f\colon \mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F) \to \mathbb{C}$ satisfying the following conditions:

(a) $f|_k u = f$ for all $u \in UZ_\infty$ where $Z_\infty = \left(\mathbb{R}^* \cdot \mathrm{SO}_2(\mathbb{R})\right)^I \subset G_\infty$;

(b) for all $x \in G_f$, the function $f_x\colon \mathfrak{h}^I \to \mathbb{C}$ defined by

$$uz_0 \mapsto j(u_\infty, z_0)^k \det(u_\infty)^{t-v-k} f(xu)$$

for $u \in G_\infty$ is well-defined and holomorphic;

[1] In [Hi06], Hida explains after formula (2.3.9) why without the parity condition, the space of Hilbert modular forms is zero – he uses a different but equivalent formalism, in which this statement can be formulated more meaningfully.

(c) $\int_{\mathbb{A}_F/F} f\Big(\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)x\Big)\mathrm{d}a = 0$ for all $x \in \mathrm{GL}_2(\mathbb{A}_F)$ and $\mathrm{d}a$ an additive Haar measure on $\mathbb{A}_F/F$.

Depending on the choice of level, one can also talk about a nebentype character. In any case, up to conjugation of U, there is a largest ideal N of $\mathcal{O}_F$ such that $U \supset \{g \in G_f \mid g \equiv 1 \pmod N\}$. We call N the level.

Definition 3.7. For $x \in G_f$ one defines the Hecke operator $[UxU]$ for a function $f\colon \mathrm{GL}_2(\mathbb{A}_F) \to \mathbb{C}$ as

$$[UxU]f := \sum_i f|_{x_i}$$

where $UxU = \coprod_i Ux_i$. This assignment is well defined for $f \in S_k(U)$ and defines an endomorphism in $\mathrm{End}_{\mathbb{C}}(S_k(U))$.

In the special case $x = \left(\begin{smallmatrix}\pi_v & 0\\ 0 & 1\end{smallmatrix}\right)$ with v not a divisor of N, one abbreviates $T_v := [UxU]$.

For $x = \left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$ with $\alpha = (\pi_v^{\mathrm{ord}_v(\mathfrak{a})})_v$ for a fractional ideal $\mathfrak{a}$ of F prime to N one calls $S_{\mathfrak{a}}$ the diamond operator for $\mathfrak{a}$. If $\mathfrak{a}$ is a prime ideal corresponding to the place v we simply write S_v.

Moreover, we define $\mathbb{T}_k(U)$ as the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S_k(U))$ generated by the T_v and S_v for all $v \nmid N$.

A cusp form f of weight k and level U is called an eigenform for $\mathbb{T}_k(U)$ if it is a simultaneous eigenvector for all T_v, S_v with $v \nmid N$. The eigenvalues are denoted by $a_v(f)$ and $\chi_v(f)$, respectively.

Since $\mathbb{T}_k(U)$ is commutative, eigenforms exist.

Theorem 3.8. *Let $f \in S_k(U)$ be a Hecke eigenform and write $a_v(f)$ for the eigenvalue under T_v for all v not dividing the level N of U.*

(a) The coefficient field *$E_f := \mathbb{Q}(a_v(f) \mid v \nmid N)$ is a finite extension of $\mathbb{Q}$. All $a_v(f)$, $v \nmid N$, are integral.*

(b) For any prime λ of the ring of integers $\mathcal{O}_f$ of E_f, there exists a unique[2] *continuous representation $V_\lambda(f)$ (isomorphic to $E_{f,\lambda}^2$), say*

$$\rho_{f,\lambda}\colon G_F \to \mathrm{GL}_2(E_{f,\lambda})$$

which is unramified outside $N\ell$ and satisfies

$$\det(1 - T\mathrm{Frob}_v | V_\lambda(f)) = 1 - a_v(f)T + \chi_v(f)q_vT^2 \text{ for all } v \nmid N\ell$$

where ℓ is the rational prime under λ and $E_{f,\lambda}$ is the completion of E_f at λ.

[2] See Remark 3.3 and Theorem 3.10(d).

Part (a) is due to Shimura; see [Sh71, Thm. 3.48] and [Hi06, (4.3.7)]. Part (b) follows from work of Eichler-Shimura, Deligne, Ohta, Carayol, Taylor and Blasius-Rogawski. If $[F:\mathbb{Q}]$ is odd or if f has a supercuspidal prime, then the construction takes place in the étale cohomology of a Shimura curve. Taylor's argument for $[F:\mathbb{Q}]$ even is via congruences and the Jacquet-Langlands correspondence for GL_2. See [Ca86, Tay89].

Definition 3.9. Let f be a cuspidal Hecke eigenform as in the previous theorem.

(a) The L-factor of f at v is $L_v(f,T) := \det(1 - T\mathrm{Frob}_v | V_\lambda(f)^{I_v})^{-1}$ where λ is any place of E_f such that v and λ have different residue characteristics – see Theorem 3.10(a).

(b) The L-function of f is

$$L(f,s) := \prod L_v(f, q_v^{-s}) \text{ for } \Re(s) \gg 0.$$

Theorem 3.10. *Let $k_0 := \max\{k_\tau \mid \tau \in I\}$. Then*

(a) The local L-factors are independent of the choice of λ (as long as v and λ are not above the same rational prime ℓ).

(b) The poles of the local L-factor at $v \nmid N$ are algebraic integers of absolute value $q_v^{(k_0-1)/2}$ (under any complex embedding), i.e. Weil numbers.

(c) The L-function defined above converges for all $s \in \mathbb{C}$ with $\Re(s) > \frac{k_0+1}{2}$. It has an entire continuation to the complex plane and a functional equation $\Lambda(f, k_0 - s) = \Lambda(f,s)$ where Λ is obtained from L by multiplication by suitable L-factors at ∞ – see the references.

(d) The representation $V_\lambda(f)$ is irreducible.

References: [RT11], [Sk09], [Bl06], [Sai11, Thm 2], [Ri85] for part (d), case of elliptic modular forms, [Tay97] for (d) for Hilbert modular forms.

Remark 3.11. The idea of [Ri85] is as follows: If the representation is reducible get ε_ℓ^a ε_ℓ^b on the diagonal up to finite order with product ε_ℓ^{k-1} up to finite order (by CFT). The Ramanujan-Petersson bound yields $2a = 2b = k-1$. Growth of L-function at $s = k$ gives two contradictory bounds (cusp form versus Eisenstein series.)

3.4 Compatible systems of Galois representations I (see [Se68])

Definition 3.12 (Weakly compatible system)**.** Let E be a number field and $\mathcal{P}$ its set of finite places. Let S_λ consist of the places v of F such that v and λ lie over the same rational prime ℓ. A family of n-dimensional continuous Galois representations $\big(\rho_\lambda \colon G_F \to \mathrm{GL}_n(E_\lambda)\big)_{\lambda \in \mathcal{P}}$ is an *E-rational weakly compatibly system (with finite ramification set S)* if

(a) for all $\lambda \in \mathcal{P}$, the representation ρ_λ is unramified outside $S \cup S_\lambda$;

(b) for all finite places v of F not in S there exists a polynomial $p_v(T) \in E[T]$ such that

$$p_v(T) = \det(1 - T\rho_\lambda(\mathrm{Frob}_v)) \in E_\lambda[T] \quad \forall \lambda \text{ such that } v \notin S_\lambda,$$

where E is canonically a subfield of E_λ, its completion at λ.

Example 3.13. Let μ_{ℓ^∞} denote the set of ℓ-power roots of unity in $\bar{F}$ for some number field F. It is clearly stable under G_F. Define the ℓ-adic cyclotomic character $\varepsilon_\ell \colon G_F \to \mathrm{Aut}(\mu_{\ell^\infty}) \cong \mathbb{Z}_\ell^*$ by $g \mapsto (\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^{\varepsilon_\ell(g)})$ for all n. (This is independent of the choice of roots (ζ_{ℓ^n}).) Then $(\varepsilon_\ell)_\ell$ forms a compatibly $\mathbb{Q}$-rational system with ramification set $S = \emptyset$.

Extending Definition 3.1, we shall write $V_\ell(A)$ for the rational ℓ-adic Tate module of any abelian variety A.

Theorem 3.14. *(a) If A is an abelian variety over a number field F, then the representations $V_\ell(A)$ form a $\mathbb{Q}$-rational weakly compatible system with ramification set, the set of places of F where A has bad reduction.*

(b) If f is a Hilbert modular form over a totally real field F , then the representations $V_\lambda(f)$ form an E_f-rational weakly compatible system with ramification set, the set of places of F dividing the (minimal) level N of f.

Part (a) is [ST68, Thm. 3]. Part (b) is immediate from Theorem 3.8.

Remark 3.15. Now we can meaningfully talk about the symmetric powers of an elliptic curve A/F. Namely we can mean by this the weakly compatible $\mathbb{Q}$-rational family $(\mathrm{Sym}^n V_\ell(A))$ of representations of dimension $n+1$.

3.5 What does it mean for an elliptic curve A to be modular?

- A and f have the same L-function.
  It is elementary to see that this implies $a_v(A) = a_v(f)$ for all places of F at which A has good reduction and which do not divide the level.
  Converting this into a statement about Galois representations it follows that $V_\ell(A) = V_\ell(f)$ (and $E_f = \mathbb{Q}$). Remembering that we defined L-factors at bad (or at all places) via the Galois representation (and inertia invariants), it follows that we must have equality of the remaining L-factors.

- The ℓ-adic Tate module $V_\ell(A)$ of A and the ℓ-adic Galois representation $V_\ell(f)$ attached to f are isomorphic for one ℓ (or all ℓ).

- Even better: From f one can (often, and always if $[F:\mathbb{Q}]$ is odd) construct an elliptic curve A_f (in some jacobian of a modular/Shimura curve). Then A being modular means that A is isogenous to some A_f.

The three notions above are equivalent, provided they all make sense – note that A_f is not always defined. The proof is an instructive exercise. The following remarks may be helpful.

Remark 3.16. (a) If two elliptic curves A and A' are isogenous over F, then they have the same Galois representation and thus the same L-function. Consider the isogeny $0 \to K \to A \to A' \to 0$ with finite kernel K. Passing to ℓ^∞-torsion points and Tate modules, we deduce

$$0 \to K[\ell^\infty] \to \mathrm{Ta}_\ell(A) \to \mathrm{Ta}_\ell(A') \to 0.$$

Tensoring with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$, the left hand term disappears and the other two become isomorphic.

(b) It is a deep theorem due to Faltings [Fa82], the semisimplicity conjecture of Tate, that shows that for Galois representations of abelian varieties A, A' over a number field F we have that A and A' are isogenous if and only if they have isomorphic Galois representations. Faltings proves that the following natural homomorphism is an isomorphism:

$$\underbrace{\mathrm{Hom}(A,A') \otimes_{\mathbb{Z}} \mathbb{Q}_\ell}_{\text{rational isog. } A \to A'} \longrightarrow \underbrace{\mathrm{Hom}_{\mathbb{Q}_\ell[G_F]}(V_\ell(A), V_\ell(A'))}_{G_F-\text{equiv. homom.}}.$$

4 Weil-Deligne representations

The following is based on notes by T. Gee from the 2011 Winter School in Postech, Korea. The ultimate source for this is the important article [Tat79].

Question: Can one define a refined notion of compatible system that also takes ramified primes into account?
Answer: Yes, by introducing Weil-Deligne representations.
Question: Can one refine the notion of compatible system even further to also include primes above the residue characteristic of the representation?
Answer: Yes (later), via Fontaine's p-adic Hodge theory – and again Weil-Deligne representations.

4.1 Galois representations of local fields

The Weil group

Let $K/\mathbb{Q}_p$ be a finite extension, $\mathcal{O}_K$ its ring of integers, π_K its uniformizer, $k = k_K$ its residue field of cardinality q_K. Let $\mathrm{v}_K\colon K^* \to \mathbb{Z}$ be the normalized additive valuation and $|\,|_K$ the multiplicative valuation with $|\pi_K|_K = q_K^{-1}$.

Every element g of $G_K = \mathrm{Gal}(\bar{K}/K)$ preserves $\mathcal{O}_{\bar{K}}$ and induces an automorphism of the residue field $\bar{k}$ of $\mathcal{O}_{\bar{K}}$. The kernel of the induced homomorphism $G_K \to G_k$ is the inertia subgroup I_K.

Denote by Frob_K the canonical topological generator of G_k, the geometric Frobenius, i.e., the inverse automorphism to $\bar{k} \to \bar{k} : x \mapsto x^{q_K}$. Pullback of $1 \to I_K \to G_K \to G_k \to 1$ along $\langle \mathrm{Frob}_K \rangle \to G_k$ defines the Weil group W_K in the s.e.s.

$$0 \to I_K \to W_K \to \langle \mathrm{Frob}_K \rangle \to 0.$$

Here W_K is a topological group by taking the neighborhoods of I_K (under the profinite topology of G_K) as a neighborhood basis of the identity.

The inertia subgroup

Define K^{nr} as $\bar{K}^{I_K}$. Then $K^{\mathrm{nr}} = \cup_n K(\zeta_{p^{n!}-1})$ and $\mathrm{Gal}(K^{\mathrm{nr}}/K) \to G_k$ is an isom.

Define $K^{\mathrm{tame}} := \cup_{\gcd(n,p)=1} K^{\mathrm{nr}}(\pi^{1/n})$. By Kummer theory K^{tame}/K is Galois and

$$\mathrm{Gal}(K^{\mathrm{tame}}/K) \cong \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{nr}}) \rtimes \mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \hat{\mathbb{Z}}' \rtimes \hat{\mathbb{Z}}$$

with $\hat{\mathbb{Z}}' = \prod_{\ell \neq p} \mathbb{Z}_\ell$.

Kummer theory says that $g \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{nr}})$ maps to $\hat{\mathbb{Z}}'$. Explicitly: choose a compatible system of roots of unity $\zeta := (\zeta_n)_{n \,\text{prime to}\, p} \subset K^{\mathrm{nr}}$. Define for $g \in I_K$ a sequence $t_n(g)$ in the inverse limit $\hat{\mathbb{Z}}'$ by $g(\pi^{1/n})/\pi^{1/n} = \zeta_n^{t_n(g)}$. The t_n define a surjective homomorphism $t_\zeta : I_K \to \hat{\mathbb{Z}}'$. Denote by $t_{\zeta,\ell}$ the composite of t_ζ with the projection $\hat{\mathbb{Z}}' \to \mathbb{Z}_\ell$. The kernel of $G_{K^{\mathrm{nr}}} \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{nr}})$ is the wild ramification subgroup P_K. It is the pro-p-Sylow subgroup of I_K.

Let $\xi_K\colon W_K \to \langle \mathrm{Frob}_K \rangle \to \mathbb{Z}$ be character defined by $\mathrm{Frob}_K \mapsto 1$.Then one has

$$t_\zeta(g\tau g^{-1}) = q_v^{-\xi_K(g)} t_\zeta(\tau) \tag{4.1}$$

for $\tau \in I_K$ and $g \in W_K$.

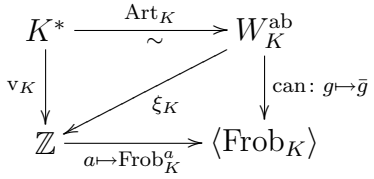
Theorem 4.1 (Main Thm of local CFT)**.** *Let W_K^{ab} denote the group $W_K/\overline{[W_K, W_K]}$. Then there is a unique system of isomorphisms (for all extensions of $\mathbb{Q}_p$)*

$$\mathrm{Art}_K : K^* \to W_K^{\mathrm{ab}}$$

such that

(a) if K'/K is a finite extension and $\pi_{K'/K} : W_{K'}^{\mathrm{ab}} \overset{\mathrm{can}}{\to} W_K^{\mathrm{ab}}$, then $\pi_{K'/K} \circ \mathrm{Art}_{K'} = \mathrm{Art}_K \circ N_{K'/K}$,

(b) and we have a commutative square



Definition 4.2 (Weil and Weil-Deligne representations)**.** Let L be a field of characteristic zero.

A representation of W_K over a field L (on a finite dimensional vector space over L) is a representation which is continuous with respect to the discrete topology on L and the one defined above for W_K.

A Weil-Deligne representation of W_K on a finite dimensional L-vector space V is a pair (r, N) (or a triple $(V; r; N)$) where r is a representation of W_K on V and N is in $\mathrm{End}(V)$ such that for all $\sigma \in W_K$ one has the following analog of (4.1)

$$r(\sigma) N r(\sigma)^{-1} = q_v^{-\xi_K(\sigma)} N. \tag{4.2}$$

Remark 4.3. For r as above the image $r(I_K)$ is finite. Moreover by considering the eigenvalues of N it easily follows that N is nilpotent. Finally, the relation (4.2) is equivalent to $r(\sigma)N = Nr(\sigma)$ for all $\sigma \in I_K$ and $r(\phi)Nr(\phi)^{-1} = q_K^{-1}N$ for $\phi \in W_K$ a lift of the geometric Frobenius Frob_K.

The conductor of a WD-representation is

$$c(r, N) := c(r) + \dim V^{I_K} - \dim(\mathrm{Ker}(N : V \to V)^{I_K})$$

where $c(r)$ is the usual Artin conductor of a discrete representation in characteristic zero. The Artin conductor of $c(r)$ can be defined as the Artin conductor $c(r')$ of the finite image representation r' from part (f) of the following exercise – r' is a twist of r by an unramified character.

Exercise 4.4. (a) For a representation $(V; r)$ of W_K and $m \geq 1$, define $\mathrm{Sp}_m(r)$ as the triple

$$\Big(\bigoplus_{i=1,\dots,m} V, \bigoplus_{i=1,\dots,m} r \cdot |\mathrm{Art}_K^{-1}|_K^{m-i}, N \Big)$$

with N restricted to the i-th component V that is acted on by $r \cdot |\mathrm{Art}_K^{-1}|_K^i$ being the isomorphism to the $i+1$-th component acted on by $r \cdot |\mathrm{Art}_K^{-1}|_K^{i+1}$. Then this defines a WD-representation.

(b) Every WD representation is isomorphic to a direct sum of representations $\mathrm{Sp}_m(r)$.

(c) If $(r; V; N)$ is a WD representation of W_K and K'/K is a finite extension, then the restriction $(r|_{G_{K'}}; V; N)$ is a WD representation of $W_{K'}$.

(d) If r is a representation of W_K, then there exists a finite index subgroup H such that $r(H)$ lies in $Z(r(W_K))$. In particular, the projective representation induced from r has finite image.

(e) There exists a representation r' of G_K (of finite image) such that r and $r'|_{W_K}$ have the same projective image, and in particular any Weil representation is a twist of a representation of G_K (of finite order) by character of W_K. (Hint: [Se77, Cor. of Thm. 4].)

(f) There exists a representation r' of G_K (of finite image) and an unramified character χ of W_K such that $r = \chi \otimes r'$.

(g) Let σ be in $W_K \setminus I_K$. Then for any $\tau \in W_K$ there exist n in $\mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$ such that $r(\sigma^m) = r(\tau^n)$.

(h) For a representation r of W_K the following conditions are equivalent: (a) r is semisimple. (b) $r(\sigma)$ is semisimple for all $\sigma \in W_K$. (c) $r(\sigma)$ is semisimple for some $\sigma \notin I_K$.

(i) If $(r; N)$ is a Weil-Deligne representation of W_K, then $(r, N)^{F-\mathrm{ss}} := (r^{\mathrm{ss}}, N)$ is a WD-representation of W_K.

Note that by r^{ss} we mean the following semisimplification: suppose the α is any automorphism of a vector space over a field L. Then α can be written in a unique way as $\alpha = \alpha^{\mathrm{ss}} \cdot \alpha^{\mathrm{unip}}$ for commuting endomorphisms α^{ss} and α^{unip} such that α^{ss} is semisimple, i.e., it is diagonalizable over L^{alg}, and α^{unip} is unipotent, i.e., all of its eigenvalues are one. Now one defines r^{ss} to mean that for any $g \in W_K$, one sets $r^{\mathrm{ss}}(g) := (r(g))^{\mathrm{ss}}$ in the sense just described. Note that since I_K has finite image under r, all elements in $r(I_K)$ are semisimple.

Definition 4.5. A WD-representation (r, N) is Frobenius semisimple if r is semisimple. (i.e. $r(\phi)$ is semisimple as an endom.)

Definition 4.6. Let L be an algebraic extension of $\mathbb{Q}_\ell$ with $\ell \neq p$.

(a) $A \in GL_n(L)$ is bounded if $\det A$ lies in $\mathcal{O}_L^*$ and $\det(1 - TA)$ in $\mathcal{O}_L[T]$.

(b) A representation r of W_K is bounded if $r(\sigma)$ is bounded for all σ in W_K

Remark 4.7. (i) In (a), the matrix A is bounded if it stabilizes an $\mathcal{O}_L$ lattice in L^n.

(ii) In (b), the representation r is bounded if and only if $r(\sigma)$ is bounded for some $\sigma \notin I_K$.

Theorem 4.8 (Grothendieck's Monodromy Theorem, [Tat79, Cor. (4.2.2)])**.** *Suppose $l \neq p$, $K/\mathbb{Q}_p$ is finite, $L/\mathbb{Q}_\ell$ is finite and V is a finite dimensional L-vector space. Fix a lift $\phi \in W_K$ of* Frob_K *and a compatible system $\zeta = (\zeta_n)$ of roots of unity in K^{alg}. (This defines a unique $t_{\zeta,\ell}\colon I_K \to \mathbb{Z}_\ell$ for all $\ell \neq p$.)*

For any continuous representation $\rho : G_K \to \mathrm{GL}(V)$, there exists a finite extension K' of K such that $\rho(I_{K'}) \equiv 1 \mod 2\ell$ for an $\mathcal{O}_L$-lattice of V stabilized by G_K and there exists a unique nilpotent endomorphism N of V such that for all $\sigma \in I_{K'}$ one has $r(\sigma) = \exp(Nt_{\zeta,\ell}(\sigma))$.

Moreover if $r : W_K \to \mathrm{GL}(V)$ is defined by

$$r(\sigma) = \rho(\sigma)\exp(Nt_{\zeta,\ell}(\phi^{-\xi_K(\sigma)}\sigma)),$$

then $(r, N) =: \mathrm{WD}(\rho)$ defines a WD-representation of W_K. The functor $\mathrm{WD} = \mathrm{WD}_{\phi,\zeta}$ defines an equivalence of categories from continuous representations ρ to bounded WD-representations (r, N).

Finally for any choices (ϕ, ζ) and (ϕ', ζ') there is a natural isomorphism

$$\mathrm{WD}_{\phi,\zeta} \to \mathrm{WD}_{\phi',\zeta'}\,.$$

Proof. Exercise: The main tool needed is the existence of an ℓ-adic logarithm. This is ensured by the condition that ρ on $I_{K'}$ has pro-ℓ image and that the matrices of this image are congruent to $1 \mod 2\ell$. Then the usual series for the log converges. □

Remark 4.9. Suppose $\rho : G_K \to \mathrm{Aut}(V)$ is unramified. Then $N = 0$ and $r(I_K) = \{1\}$ for $(r, N) = \mathrm{WD}(V)$. Thus r is completely determined by $\rho(\phi)$ for a lift ϕ of Frob_K. In other words, $\mathrm{WD}(\rho)$ depends on the conjugacy class of $\rho(\phi)$, i.e., its rational canonical form. If one passes to $\mathrm{WD}(\rho)^{F-\mathrm{ss}}$, then the isomorphism type of the latter is completely determined by the characteristic polynomial $\det(1 - T\mathrm{Frob}_K|V)$.

4.2 Compatible systems II

Definition 4.10 (Strictly compatible system)**.** Let E be a number field and $\mathcal{P}$ its set of finite places. For $\lambda \in \mathcal{P}$ let S_λ denote the set of places v of a number field F such that v and λ lie over the same rational prime ℓ. A family of n-dimensional continuous Galois representations $(V_\lambda)_{\lambda\in\mathcal{P}}$ of G_F is an *E-rational strongly compatibly system (with finite ramification set S)* if

(a) for all $\lambda \in \mathcal{P}$, the representation V_λ is unramified outside $S \cup S_\lambda$;

(b) for all finite places v of F not in S there exists a polynomial $p_v(T) \in E[T]$ such that

$$p_v(T) = \det(1 - T\mathrm{Frob}_v|V_\lambda) \in E_\lambda[T] \quad \forall\lambda \text{ such that } v \notin S_\lambda;$$

(c) for all finite places v in S there exists an Frobenius semisimple WD-representation (r_v, N_v) of F_v such that

$$\mathrm{WD}(V_\lambda|_{G_{F_v}})^{F-\mathrm{ss}} = (r_v, N_v) \quad \forall \lambda \text{ such that } v \notin S_\lambda.$$

Conjecture 4.11 (Fontaine, Serre, Deligne)**.** *If V is a representation that occurs in the ℓ-adic étale cohomology of a smooth proper variety over a local field, then its associated Weil-Deligne representation is Frobenius semisimple. Moreover the Weil-Deligne representation is independent of ℓ. See [Tat79], [Fo94c, Section 2.4.], [Se91, §§11,12].*

Theorem 4.12 (Carayol, Eichler-Shimura, Langlands, Deligne, see [Ca86])**.** *For v a Hilbert modular eigenform, the family $(V_\lambda(f))$ is a strongly compatible E_f-rational system;*

Theorem 4.13. *Suppose A/F is an abelian variety. Then $(V_p(A))$ is a strongly compatible system.*

I could not find a reference for Theorem 4.13 as stated. Strict compatibility at places of good reduction is standard. The case of semistable reduction can be deduced from the thesis of A. Laskar from 2011 (Strasbourg). According to private communication with Fontaine, the result as stated has the status of a theorem. It can be deduced from Raynaud's rigid analytic models for abelian varieties with semistable reduction. Apparently the finite Galois action of a Galois extension over which semistable or good reduction is acquired poses no problems. But a reference for the general case seems to be absent from the literature.

5 How to deal with primes above ℓ?

5.1 An example

Given A/F an elliptic curve, ℓ a rational prime, v a place of F above ℓ and with residue field k_v. What do we know about $V_\ell(A)$ restricted to a decomposition group at v?

- **good reduction at v.** If A/F_v has good reduction, then A/k_v is an elliptic curve and there is a short exact sequence

$$0 \to A^0[\ell^\infty](\bar{F}_v) \to A[\ell^\infty](\bar{F}_v) \to A[\ell^\infty](\bar{k}_v) \to 0$$

where $A^0[\ell^\infty]](\bar{F}_v)$ is given by a formal group of dimension 1 and height 1 (ordinary case) or height 2 (supersingular case) and $A[\ell^\infty](\bar{k}_v)$ is either isomorphic to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ if A/F_v is ordinary or trivial if A/F_v is supersingular.

– **ordinary subcase.** Here $V_\ell(A)|_{G_v}$ is an extension of two 1-dimensional representations and thus of the form

$$\rho_v : G_v \to \mathrm{GL}_2(\mathbb{Q}_\ell) : g \mapsto \begin{pmatrix} \varepsilon_\ell(g)\chi(g) & * \\ 0 & \chi^{-1}(g) \end{pmatrix}$$

with respect to a suitable basis and where ε_ℓ is the ℓ-adic cyclotomic character and χ is an unramified character. Due to the Weil-paring, the determinant must be ε_ℓ. Note the ε_ℓ is infinitely wildly ramified – so that there is no associated WD-representation.

– **supersingular subcase.** Now $V_\ell(A)|_{G_v}$ need not have a filtration. If $\mathrm{End}_{\bar{F}_v}(A/F_v)$ is 2-dimensional then the formal group is given by two conjugate Lubin-Tate characters and easy to describe via local class field theory. In general, the representation is absolutely irreducible and remains so over any finite index subgroup H of G_v. The mod ℓ reduction is rather special as can be seen from analyzing the ℓ-torsion group via the formal group law of A/F_v. The representation is infinitely ramified and again there is no direct way to get a WD representation.

Exercise 5.1. Suppose A has good reduction and π denotes the Frobenius endomorphism on A/k_v, so that π satisfies the quadratic polynomial $p_v(T) = T^2 - a_v T + q_v$ with integer coefficients, where $\#A(k_v) = q_v - a_v(a) + 1$. Let $\alpha, \beta \in \overline{\mathbb{Z}}$ be the roots of p_v so that $v_{q_v}(\alpha\beta) = 1$. It is also standard that $\#A(k_v^n) = q_v^n - \alpha^n - \beta^n + 1$ for k_v^n the unique extension of the finite field k_v of degree n. Show that A/k_v is supersingular if and only if $v_{q_v}(\alpha), v_{q_v}(\beta) > 0$, if and only if $v_{q_v}(\alpha) = v_{q_v}(\beta) = 1/2$. If A_v is ordinary, then without loss of generality $v_{q_v}(\alpha) = 0$. Show that $\chi^{-1}(\mathrm{Frob}_v)$ acts on the p^∞ torsion points in the same way as π and that $\chi^{-1}(\mathrm{Frob}_v) = \alpha$.

- **semistable reduction at v (here only split multiplicative reduction).** Here one uses the Tate curve of A/F_v. It shows that the Galois action on the ℓ^∞-torsion points is given by the Galois action on $\bar{F}_v^*/q^{\mathbb{Z}}$ for $q \in F_v^*$ an element of valuation strictly less than one. The ℓ^∞ torsion points are given by the set $\{q^{i/\ell^n}\zeta_{\ell^n}^j \mid i, j \in \mathbb{Z}\}$. This describes an infinite Kummer extension of F_v. The corresponding Galois extension is of the form

$$\rho_v : G_v \to \mathrm{GL}_2(\mathbb{Q}_\ell) : g \mapsto \begin{pmatrix} \varepsilon_\ell(g) & * \\ 0 & 1 \end{pmatrix}$$

- **potentially good or potentially semistable reduction (or non-split multiplicative reduction).**
The representation is as above after one restricts G_{F_v} to a suitable open subgroup (coming from the field over which good or semistable reduction is acquired).

Comparison to ℓ'-adic data.
If one looks at the ℓ'-power torsion, then the above cases correspond to unramified, unramified, semistable ($N \neq 0$) WD-representations or the general case of a WD-representation.

For the representations that arise from modular forms one has a similar behavior. The solution of the puzzle:

5.2 Fontaine's mysterious functors

References are [Ber02, Ber10, Ber12], [CB09], [Fo94a, Fo94b], [FO09], [GM09].

Let K be a finite extension of $\mathbb{Q}_p$ and K_0 the subfield of K that is maximal unramified over $\mathbb{Q}_p$. Fontaine defines functors D_*, $* \in \{\mathrm{HT}, \mathrm{dR}, \mathrm{cris}, \mathrm{st}\}$ from

$$\left\{\rho\colon G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p) \mid \rho \text{ is cont.}\right\}$$

to modules over $K_* \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell}$ for $K_* = K$, K, K_0, or K_0, respectively, with some additional structure coming from some rings B_* of Fontaine with $B_{\mathrm{cris}} \subset B_{\mathrm{st}} \subset B_{\mathrm{dR}}$ and B_{HT} is the graded ring associated to B_{dR}. The structures are a continuous action of G_K and

(a) a graduation,

(b) a filtration,

(c) a filtration and a semilinear endomorphism ϕ (Frobenius)

(d) a filtration and two endomorphisms ϕ, N – for more, see 5.3.

The rings B_* also satisfy $B_*^{G_K} = K_*$. One calls a representation ρ to be $*$ (= Hodge-Tate, de Rham, crystalline, semistable) if

$$(V(\rho)) \otimes_{\mathbb{Q}_p} B_*)^{G_K} \text{ is free over } K_* \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} \text{ of rank equal to } \dim_{\overline{\mathbb{Q}_p}} V(\rho).$$

In all cases one has $\leq$ for the rank.

The ring B_{HT} attaches the HT-weights (in $\mathbb{Z}$) to a representation. The ring B_{dR} carries a $\mathbb{Z}$-graded filtration. The property of being Hodge-Tate or de Rham is invariant under finite extensions E/K. The property of being cris and st are not invariant under such extensions. So one also has the notions of *potentially crystalline* and *potentially semistable*; for instance ρ is potentially crystalline if there exists a finite extension E/K such that $\rho|_{G_E}$ is crystalline. The implications for a representation V are described in the following diagram

$$\begin{array}{ccccccc}
V \text{ is cris} & \Longrightarrow & V \text{ is semist.} & & & & \\
\Downarrow & & \Downarrow & & & & \\
V \text{ is pot. cris} & \Longrightarrow & V \text{ is pot. semist.} & \overset{\text{A-B-K-M}}{\Longleftrightarrow} & V \text{ is dR} & \Longrightarrow & V \text{ is HT.}
\end{array}$$

The proof of Fontaine's conjecture that the notions de Rham and potentially semistable are equivalent, due to A=I. André, B=L. Berger, K=K. Kedlaya, M=Z.

Mebkhout, is described by Colmez in [Co03]. Berger proves that Crew's conjecture is equivalent to the conjecture of Fontaine, and the three other authors, independently, give a proof of Crew's conjecture.

5.3 The WD-representation of a potentially semistable $V = V(\rho)$ of rank d (after Fontaine)

Let K, V be as above and suppose K'/K is a finite Galois extension such that $V|_{G'_K}$ is semistable. Then $D_{\mathrm{st}}(V|_{G_{K'}}) = (D, \phi, N, \mathrm{Fil}^i)$ where

(a) D is a free $K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ module of rank d.
(b) $\phi_D \colon D \to D$ is $\sigma \otimes \mathrm{id}$ linear with $\sigma \colon K'_0 \to K'_0$ the Frobenius in $\mathrm{Gal}(K'_0/\mathbb{Q}_p)$,
(c) $N_D \colon D \to D$ an $K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$-linear endomorphism such that $N_D \phi_D = p \phi_D N_D$,
(d) a decreasing, separating, exhausting filtration Fil^i of $(D \otimes_{K'_0} K')$,

and the quadruple is equipped with an action of $\mathrm{Gal}(K'/K)$, i.e., an action

$$\mathrm{Gal}(K'/K) \longrightarrow \mathrm{Aut}(D, \phi_D, N_D, \mathrm{Fil}^\bullet).$$

If the representation is semistable, one has $K' = K$, if it is potentially crystalline, then $N = 0$ (and vice versa).

Remark 5.2. The quadruple $(D, \phi_D, N_D, \mathrm{Fil}^i)$ is weakly admissible - which is a characterization of the image of the mysterious functor; it means that $t_H(D) = t_N(D)$ and $t_H(D') \leq t_N(D')$ for all stable (but not necessarily free) subobjects D' of D. Here $t_H(D)$ is the index of the unique jump of the filtration of the induced filtration $\mathrm{Fil}^i \bigwedge^d D$ and t_N is the slope of $\bigwedge^d \phi_D$.

The associated WD-representation to ρ is basically obtained by forgetting the filtration, see [GM09] and [Sav05, Def. 2.15] for $K = \mathbb{Q}_p$: Observe that

$$K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} = \bigoplus_{\tau \colon K'_0 \to \overline{\mathbb{Q}_p}} \overline{\mathbb{Q}_p}.$$

Correspondingly one has

$$D = D \otimes_{K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}} K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} = \bigoplus_{\tau \colon K'_0 \to \overline{\mathbb{Q}_p}} D_\tau$$

with suitable components D_τ of D. One verifies that $\phi_D^{[K'_0 : \mathbb{Q}_p]}$ induces an isomorphism of the D_τ since it is $K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$-linear. Fix τ_0 among the τ.

Definition 5.3. Let K, V, K', D be as above and let $\phi \in W_K$ be a lift of Frob_K. Then the WD-representation $\mathrm{WD}(V)$ is the triple (U, r, N) where

(a) U is the $\overline{\mathbb{Q}_p}$ vector space D_{τ_0},

(b) $r\colon W_K \to \mathrm{Aut}_{\overline{\mathbb{Q}_p}}(U)$ is the Weil representation determined by

  (i) defining $r|_{I_K}$ as the restriction of the $K_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$-linear action $I_K \to \mathrm{Gal}(K'/K)$ on D to the invariant subspace D_{τ_0},

  (ii) and having ϕ act as $\phi_2^{-1}\phi_1$ on D_{τ_0} where ϕ_1 is the action of ϕ via $\mathrm{Gal}(K'/K)$ and ϕ_2 is the action $\phi_D^{[K_0:\mathbb{Q}_p]}$ both times on D and then restricted to the invariant subspace D_{τ_0},

(c) N is the restriction of the endomorphism N_D from D to its invariant subspace D_{τ_0}.

In the case where $K = \mathbb{Q}_p$ and K'/K is totally ramified, so that $K_0' = K_0 = \mathbb{Q}_p$, the vector space U is simply equal to D and ϕ is the inverse of ϕ_D (and $N = N_D$).

Note: The eigenvalues of $r(\phi)$ to the power $[K_0' : K_0]$ are those of $\phi_D^{-[K_0':\mathbb{Q}_p]}$. Hence their p-adic valuations are up to the scalar $[K_0 : \mathbb{Q}_p]$ the slopes (= p-adic valuations) of the eigenvalues of ϕ_D. In particular they are typically not units, and thus r is typically **unbounded**. This is therefore different from the case where K and L have different residue characteristic.

5.4 Continuation of Example 5.1 of an elliptic curve A/F_v

(a) If A has ordinary reduction, one has a short exact sequence

$$0 \to D_{\mathrm{cris}}(\mathbb{Z}_\ell(\varepsilon_\ell\chi)) \to D_{\mathrm{cris}}(V_\ell(A)) \to D_{\mathrm{cris}}(\mathbb{Z}_\ell(\chi^{-1})) \to 0$$

where the outer modules have underlying D of rank 1. Thus $D_{\mathrm{cris}}(V_\ell(A))$ is reducible.

(b) If A has supersingular reduction, then either $D_{\mathrm{cris}}(V_\ell(A))$ is a simple object and remains so after base change to any finite extension E/F_v, or there is an extension E/F_v of degree at most 2 over which $D_{\mathrm{cris}}(V_\ell(A))$ becomes the sum of two 1-dimensional subobjects.

(c) If A has semistable but non-good reduction, then $N = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $D_{\mathrm{st}}(V_\ell(A))$ has rank 2 and is reducible while $D_{\mathrm{cris}}(V_\ell(A))$ has rank 1 only; see [Ber02, p. 18].

5.5 Compatible systems III

Definition 5.4 (Strictly compatible system, strong sense)**.** Let E be a number field and $\mathcal{P}$ its set of finite places. For $\lambda \in \mathcal{P}$, and F a number field, let S_λ denote the places v of S such that v and λ lie over the same rational prime ℓ.

A family of n-dimensional continuous Galois representations $(V_\lambda)_{\lambda\in\mathcal{P}}$ of G_F is an *E-rational strictly compatibly system in the strong sense, (with finite ramification set S)* if

(a) for all $\lambda \in \mathcal{P}$, the representation V_λ is unramified outside $S \cup S_\lambda$ and potentially semistable at the places in S_λ;

(b) for all finite places v of F there exists a Frobenius semisimple WD-representation (r_v, N_v) of F_v such that

$$\mathrm{WD}(V_\lambda|_{G_{F_v}})^{F-\mathrm{ss}} = (r_v, N_v) \quad \forall \lambda \in \mathcal{P}.$$

Remark 5.5. As remarked earlier, if v is not in S, then (r_v, N_v) is simply $(\rho(\mathrm{Frob}_v)^{\mathrm{ss}}, 0)$ – this is also true for places v in $S_\lambda \setminus S$ (so that V_λ is crystalline locally at v). In particular, at $v \notin S \cup S_\lambda$ it suffices to require a compatibility of characteristic polynomials

$$p_v(T) = \det(1 - T\mathrm{Frob}_v|V_\lambda) \in E_\lambda[T] \quad \forall \lambda \text{ such that } v \notin S_\lambda;$$

Remark 5.6. One can add further conditions on compatible systems: For instance a purity of weight condition: All roots of all characteristic polynomials are Weil-number of the same weight. Etc.

Theorem 5.7 (Faltings, see [Fa87])**.** *For a cuspidal Hecke eigenform f the representations $(V_\lambda(f))_\lambda$ are semistable of HT-weights $(0, k-1)$.*

Remark 5.8. The HT weights of $V_\ell(A)$ for an abelian variety A over a number field F are 0 and 1 equally distributed over all places v of F above ℓ and all embeddings $F_v \hookrightarrow \overline{\mathbb{Q}_\ell}$. A proof in other language is contained in [Tat67].

Theorem 5.9 (T. Saito, see [Sai11])**.** *For a cuspidal Hilbert modular Hecke eigenform f the system $(V_\lambda(f))_\lambda$ is strictly compatible in the strong sense.*

Question 5.10. *Is it known that for an abelian variety A over number field F the family $(V_\ell(A))_\ell$ is strictly compatible in the strong sense? (The HT-weights are 0 and 1 each with multiplicity $\dim A$.)*

5.6 A refinement: Fontaine Laffaille theory

The above is not the end of the story of understanding ℓ-adic Galois representations of ℓ-adic fields. One also needs *integral information* on $V(\rho)$. Fontaine's theory above only contributes to ℓ-adic information, but does not help if one studies the mod ℓ-reduction. One theory that achieves this is due to Fontaine and Laffaille from [FL82].

Let $K_0/\mathbb{Q}_p$ be unramified (there are slight extensions which shall not bother us) with ring of integers W, the ring of Witt vectors of the residue field of K_0.

Definition 5.11. A *strongly divisible module* is a free W-module M of finite type equipped with a decreasing filtration by sub-W-modules $(\mathrm{Fil}^i M)_{i\in\mathbb{Z}}$ such that $\mathrm{Fil}^0 M = M$, $\mathrm{Fil}^i M = 0$ for $i \gg 0$, each subquotient $M/Fil^i M$ free over W and one has a semilinear, i.e., a σ-linear, endomorphism $\phi\colon M \to M$ such that $\phi(\mathrm{Fil}^i M) \subset p^i \mathrm{Fil}^i M$ and $M = \sum_{i\geq 0} p^{-i}\phi(\mathrm{Fil}^i M)$.

Theorem 5.12 (Fontaine-Laffaille)**.** *If M is a strongly divisible module, then $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is admissible, i.e., equal to $D_{\mathrm{cris}}(V)$ for some $\mathrm{rank}_W M$ dimensional (crystalline) representation of G_{K_0}.*
Suppose conversely that V is a crystalline representation of G_{K_0} of HT weights between 0 and $p-2$ and with $\mathbb{Q}_p$-coefficients. Then $D_{\mathrm{cris}}(V)$ contains a strongly divisible module. (Hard part.)

Let A be a W-algebra. (e.g. W or W/pW or a finite W-algebra, or ...)

Definition 5.13. A *Fontaine-Laffaille module over A* is a finitely generated $W \otimes A$-module M equipped with a decreasing filtration by sub-$W \otimes A$-modules $(\mathrm{Fil}^i M)_{i\in\mathbb{Z}}$ such that $\mathrm{Fil}^0 M = M$, $\mathrm{Fil}^i M = 0$ for $i \geq p-1$, and with a semilinear, i.e., a $\sigma \otimes \mathrm{id}_A$-linear, endomorphism $\phi^i \colon \mathrm{Fil}^i M \to M$ such that $\phi|_{\mathrm{Fil}^i M} = \phi^i$ and $M = \sum_{i\geq 0} \phi^i(\mathrm{Fil}^i M)$.

Define a torsion crystalline representation of weight k ($k \in \mathbb{N}$) to be any finite representation of G_{K_0} that can be written as T/T' where T is a Galois stable lattice in a crystalline representation of G_{K_0} with Hodge-Tate weights in $\{0, \ldots, k\}$ and $T' \subset T$ is a Galois stable sublattice. This yields a category of crystalline torsion modules.

Theorem 5.14 (Fontaine-Laffaille)**.** *Suppose A is a finite W-algebra. If M is a Fontaine-Laffaille-module over A, then under the integral version T_{cris} of D_{cris} the module M is the image of the crystalline torsion A-module.*
Conversely, if M is a torsion crystalline representation over A of weight $k \leq p-2$, then the image under T_{cris} is a Fontaine-Laffaille-module M over A.

Special case (we still assume that $K_0/\mathbb{Q}_p$ is unramified):

Theorem 5.15 (Fontaine-Laffaille + Raynaud)**.** *Let $\mathrm{MF}^1_{\mathrm{tor}}$ be the category of Fontaine-Laffaille torsion modules over W with $\mathrm{Fil}^2 = 0$ and suppose $p > 2$. Then there are equivalences of abelian categories:*

$$\mathrm{MF}^1_{\mathrm{tor}} \xrightarrow[\mathrm{FL}]{\cong} \{ \textit{finite flat group schemes/}W\} \xrightarrow[\mathrm{Ray.}]{\cong} \{ \textit{flat repns. of } G_{K_0}\}.$$

The latter applies in particular to modular forms of weigh 2 and abelian varieties (with level prime to p or conductor not divisible by p, respectively). References are [Ra74] and [FL82].

It is possible to describe finite flat group schemes over finite extensions $K/\mathbb{Q}_p$. For this rather deep theory, we refer to [Ki09b].

6 The Fontaine Mazur conjecture

The Fontaine-Mazur conjecture is the following statement:

Conjecture 6.1 ([FM95])**.** *Let F be a number field and S a finite set of places of F. Suppose that $\rho\colon G_{F,S} \to \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$ is continuous and irreducible and that $\rho|_{G_v}$ is de Rham for all $v|\ell$. Then ρ* comes from geometry*, i.e., there exists a smooth projective variety X over F such that ρ is a subquotient of some ℓ-adic cohomology $H^i(X_{\bar{F}}, \mathbb{Q}_\ell)$.*

In special cases, the conjecture can be phrased in a more concrete form, in the sense that a recipe is given where in geometry one can find the representation:

Conjecture 6.2. *Let S be a finite set of places of $\mathbb{Q}$. Suppose that $\rho\colon G_{\mathbb{Q},S} \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ is continuous and irreducible. Suppose further that $\rho|_{G_p}$ is de Rham with HT weights $0, w \geq 1$. Then there exists an elliptic cuspidal Hecke eigenform f and a place λ of the coefficient field E_f of f such that $V(\rho) \cong V_\lambda(f)$.*

Under the hypothesis that ρ is odd, conjecture 6.2 is proved in the majority of cases by Emerton and by Kisin, independently, in [Em11] and [Ki09a]. The oddness does follow from the Fontaine-Mazur conjecture, but so far it remains a technical hypothesis in basically all arguments.

A second special case is the following:

Conjecture 6.3. *Let F be a totally real number field. Suppose $\rho\colon G_{F,S} \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ is continuous, irreducible and of weight 2, i.e., it is de Rham at all places above ℓ with HT-weights $(0,1)$ for all places $v|\ell$ and all embeddings $F_v \to \overline{\mathbb{Q}_\ell}$. Then ρ arises from a Hilbert modular form of weight $(2, \ldots, 2)$.*

Conjecture 6.3 in the form stated is completely open – even if one assumes that ρ is totally odd. All known results impose severe restrictions on the ramification at places above ℓ. A weaker assertion is given by the potential modularity results of Taylor. We follow the cases given in [Sn09]:

Theorem 6.4 (Taylor,Dieulefait (version of [Sn09]))**.** *Suppose ρ is as in conjecture 6.3 and that its reduction mod ℓ is* absolutely irreducible*, that $\ell \geq 3$ and that for $\ell = 5$ some extra hypotheses are satisfied. Then*

(a) the L-function $L(\rho, s)$ has a meromorphic continuation to $\mathbb{C}$ and the expected functional equation;

(b) there exists a strictly compatibly system (in the strong sense) $(\rho_\lambda\colon G_{F,S} \to \mathrm{GL}_n(E_\lambda))_\lambda$ for some number field E and a place λ_0 such that $\rho_{\lambda_0} = \rho$.

Note that the theorem applies in particular to elliptic curves over F. The proof, as a combination of Brauer's theorem on characters and the potential modularity result by Taylor; both ideas stem from [Tay06]. Dieulefait in [Die07] observed how to deduce (b) from Taylor's results. An excellent survey of potential modularity and modularity lifting theorems is also [Bu10].

7 How to prove that $A/\mathbb{Q}$ is modular?

- Let N be the conductor of the elliptic curve A.
- We search for a cuspidal Hecke eigenform of weight 2 because A has HT-weights $\{0,1\}$.
- Choose a prime $p > 2$ (for simplicity) not dividing N for which $A[p]$ is *absolutely irreducible* and *modular*; the later means that $A[p] \cong \overline{V_\wp(f)}$ for some modular form f (any weight and level). [By Taylor, potentially, this is always possible. Wiles in [Wi95] uses $p = 3$ (but has to deal with problems coming from $p|N$) and results of Langlands and Tunnel.]
- By the weight and level part of Serre's conjecture: we can assume that f has level dividing N and weight equal to 2.
- Consider the Hecke-algebra $\mathbb{T}_2(\Gamma_0(N))$ over $\mathbb{Z}_p$ acting on $S_2(\Gamma_0(N))$ generated by T_q and S_q for primes q not dividing Np. Each Hecke-eigensystem of some eigenform $g \in S_2(\Gamma_0(N))$ yields a ring homomorphism $\mathbb{T}_2(\Gamma_0(N)) \to \overline{\mathbb{F}_p} : T_v \mapsto a_v(f) \mod \mathfrak{m}_{\overline{\mathbb{Z}_p}}$. Let $\mathfrak{m}_{\bar\rho}$ be the kernel for our fixed f. Then the localization $\mathbb{T}_{\bar\rho} := \mathbb{T}_2(\Gamma_0(N))_{\mathfrak{m}_{\bar\rho}}$ is a local ring.

Proposition 7.1. *(a)* $\mathrm{Hom}_{\mathbf{Ri}}(\mathbb{T}_{\bar\rho}, \overline{\mathbb{Q}_p})$ *is in bijection with the set of cuspidal Hecke newforms of level dividing* N *and weight* 2 *whose associated mod* p *Galois representation is isomorphic to* $\bar\rho$*. (Mod* p *means mod* λ *for some* λ *over* p*.)*

(b) There exists a Galois representation $\rho^{\mathrm{mod}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_{\bar\rho})$ *characterized completely by*

$$\mathrm{Trace}\,\rho(\mathrm{Frob}_v) = T_v \ (\textit{and}\ \det\rho(\mathrm{Frob}_v) = q_v) \quad \textit{for all } v \nmid Np.$$

The proposition says that any Galois representation that arises from a level N form g of weight 2 and that is congruent to f mod p is obtained from ρ^{mod} by a ring homomorphism $\mathbb{T}_{\bar\rho} \to \overline{\mathbb{Q}_p}$. Let $M_{\bar\rho}$ denote the set of these modular forms.

Proof. Part (a) is an elementary exercise. For (b), let $\mathcal{O}$ be the ring of integers of a finite extension K of $\mathbb{Q}_p$ that contains all coefficients of all $g \in M_{\bar\rho}$. Then there is a representation

$$\widetilde{\rho} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\prod_{g \in M_{\bar\rho}} \mathcal{O})$$

with $\widetilde{\rho}(\mathrm{Frob}_v) = (a_v(g))_{g \in M_{\bar\rho}}$. Observe that $\mathbb{T}_{\bar\rho}$ is a natural subring via the homomorphisms from (a) of $\prod_{g \in M_{\bar\rho}} \mathcal{O}$ which contains all traces $\mathrm{Trace}(\widetilde{\rho}(\mathrm{Frob}_v)) = T_v$. (under the various embeddings, T_v maps to the tuple $(a_v(g))_{g \in M_{\bar\rho}}$.) Now there is a theorem of Carayol [Ca94] and independently Serre that uses the hypothesis:

(i) $\mathbb{T}_{\bar\rho}$ is a complete noetherian local ring with finite residue field, (ii) the ring $\prod_{g\in M_{\bar\rho}} \mathcal{O}$ is semilocal with finite residue fields and it contains $\mathbb{T}_{\bar\rho}$, (iii) all traces of the representation $\widetilde{\rho}$ belong to the subring $\mathbb{T}_{\bar\rho}$, (iv) $\bar\rho$ is absolutely irreducible. Then $\widetilde{\rho}$ is already defined over $\mathbb{T}_{\bar\rho}$, and this is exactly the claim of (b) □

So now that we have a universal Galois representation for cusp forms of level N, weight 2 and fixed $\bar\rho$, the idea is to compare it to a Galois theoretically defined universal representation, that is hopefully of the same kind but defined abstractly and made so that it "contains" $V_p(A)$.

Define $(R = R_{\bar\rho,N,2},\ \rho_R)$ as the "universal deformation ring" that parameterizes all 2-dimensional p-adic Galois representation whose mod p reduction is $A[p]$, which at primes $q \mid N$ have the same WD-representation type as A, which at p are crystalline of weights 0,1 (flat)[3], and which have the same determinant as $V_p(A)$ and are unramified at all primes not dividing Np. (By the Weil-paring the latter determinant is a finite twist of the cyclotomic character.)
Such a ring was first defined and studied by Mazur. The main method to relate such rings to Hecke algebras is due to Wiles.
From the universality of R and the construction of $\mathbb{T}_{\bar\rho}$ one deduces (elementary):

Proposition 7.2. *There exists a unique surjective homomorphism $\alpha\colon R \to \mathbb{T}_{\bar\rho}$ such that*

$$\rho^{\mathrm{mod}} \overset{\mathrm{conj.}}{\sim} \alpha \circ \rho_R.$$

In the above situation one has the following result:

Main Theorem 7.1 ([Wi95, TW95, BCDT])**.** *The map $\alpha\colon R \to \mathbb{T}_{\bar\rho}$ is an isomorphism.*

There are many refinements by Clozel, Harris, Khare-Wintenberger, Kisin, Taylor and "his" school and others, of which some are listed in the bibliography, e.g. [BLGG, CHT, KW09, Ki09a, Ki09b, Tay08].

References

[AEK03] *Harmonic Analysis, the Trace Formula and Shimura Varieties*, eds. J. Arthur, D. Ellwood, R. Kottwitz, Proceedings of the Clay Mathematics Institute 2003 Summer School, The Fields Institute, Toronto, Canada, June 2–27, 2003, Clay Mathematics Proceedings, Vol. 4

[BLGG] T. Barnet-Lamb, T. Gee and D. Geraghty, *The Sato-Tate conjecture for Hilbert modular forms.* J. Amer. Math. Soc. **24** (2011), no. 2, 411–469.

[3]Remember that for simplicity we assumed that p does not divide the conductor N of A, so that $V_\ell(A)$ itself is crystalline at p of HT-weights 0,1.

[Bel09] J. Bellaïche, *Automorphic forms for unitary groups and Galois representations, Eigenvarieties of unitary groups*. Three lectures at the Clay Mathematical Institute Summer School, Honolulu, Hawaii, 2009.
`http://people.brandeis.edu/~jbellaic/AutomorphicHawaii3.pdf`

[BC09] J. Bellaïche, G. Chenevier, *Families of Galois representations and higher rank Selmer groups*, Astérisque 324 , Soc. Math. France, 2009.

[Ber02] L. Berger, *An introduction to the theory of p-adic representations*, arXiv:math.NT/0210184v1

[Ber10] L. Berger, *Galois representations and* (ϕ, Γ)*-modules*, perso.ens-lyon.fr/laurent.berger/ihp2010.php

[Ber12] L. Berger, *On p-adic Galois representations*, perso.ens-lyon.fr/laurent.berger/autrestextes.php

[Bl06] D. Blasius, *Hilbert modular forms and the Ramanujan conjecture*. Noncommutative geometry and number theory, Aspects Math., E37, Vieweg, 2006, 35–56. see
`http://www.math.ucla.edu/ blasius/papers.html`

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[BGHZ] J.-H. Bruinier, G. van der Geer, G. Harder and D. Zagier, *The 1-2-3 of modular forms*. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004. Edited by Kristian Ranestad. Universitext. Springer-Verlag, Berlin, 2008.

[La03] D. Bump, J. W. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski, S. S. Kudla, *An introduction to the Langlands program*, Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001. Edited by J. Bernstein and S. Gelbart. Birkhäuser Boston, Inc., Boston, MA, 2003.

[Bu10] K. Buzzard, *Potential modularity—a survey*. arXiv:1101.0097v2

[Ca86] H. Carayol, *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert*. Ann. Sc. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.

[Ca94] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*. Contemp. Math., **165** (1994), 213–237.

[CHT] L. Clozel, M. Harris and R. Taylor, *Automorphy for some* ℓ*-adic lifts of automorphic mod l Galois representations*, Pub. Math. IHES **108** (2008), 1–181.

[Co03] P. Colmez, *Les conjectures de monodromie p-adiques*. Sém. Bourbaki, Astérisque **290** (2003), Exp. No. 897, 53–101.

[CB09] B. Conrad and O. Brinon, *CMI Summer School Notes on p-adic Hodge Theory*,
`http://math.stanford.edu/ conrad/papers/notes.pdf`

[CSS] *Modular forms and Fermat's last theorem*. (Boston, MA, August 9–18, 1995). Ed. G. Cornell, J. H. Silverman, G. Stevens, Springer-Verlag, New York, 1997.

[CR62] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley Interscience, New York, 1962.

[Da04] H. Darmon, *Rational points on modular elliptic curves*. CBMS Regional Conf. Series in Math. **101**. AMS, Providence, RI, 2004.

[DDT97] H. Darmon, F. Diamond and R. Taylor, *Fermat's last theorem*. in Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2–140, Int. Press, Cambridge, MA, 1997.

[Die07] L. Dieulefait, *Uniform behavior of families of Galois representations on Siegel modular forms and the endoscopy conjecture*, Bol. Soc. Mat. Mexicana (3) **13** (2007), no. 2, 243–253.

[Em11] M. Emerton, *Local-global compatibility in the p-adic Langlands programme for* $\mathrm{GL}_2/\mathbb{Q}$, preprint 2011, see
`http://math.uchicago.edu/ emerton/preprints.html`

[Fa87] G. Faltings, *Hodge-Tate structures and modular forms*. Math. Ann. **278** (1987), 133–149.

[Fa82] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[Fo94a] J.-M. Fontaine. *Le corps des périodes p-adiques*. With an appendix by Pierre Colmez. Périodes p-adiques (Bures-sur-Yvette, 1988). Astérisque **223** (1994), 59–111.

[Fo94b] J.-M. Fontaine. *Représentations p-adiques semi-stables*. With an appendix by Pierre Colmez. Périodes p-adiques (Bures-sur-Yvette, 1988). Astérisque **223** (1994), 113–184.

[Fo94c] J.-M. Fontaine. *Représentations ℓ-adiques potentiellement semi-stables*. In Périodes p-adiques, Astérisque, **223** (1994), 321–347.

[FL82] J.-M. Fontaine and G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. ENS **15** (1982), 547–608.

[FO09] J.-M. Fontaine and Y. Ouyang, *Theory of p-adic Galois Representations* staff.ustc.edu.cn/˜yiouyang/galoisrep.pdf

[FM95] J.-M. Fontaine and B. Mazur, *Geometric Galois representations. Elliptic curves, modular forms, & Fermat's last theorem.* (Hong Kong, 1993), 41–78, Ser. Number Theory **I**, Int. Press, Cambridge, MA, 1995.

[Fr90] E. Freitag, *Hilbert modular forms.* Springer-Verlag, Berlin, 1990.

[GM09] E. Ghate and A. Mezard, *Filtered modules with coefficients.* Trans. Amer. Math. Soc. **361** (2009), no. 5, 2243–2261.

[Go02] E. Z. Goren, *Lectures on Hilbert modular varieties and modular forms.* With the assistance of Marc-Hubert Nicole. CRM Monograph Series **14**. AMS, Providence, RI, 2002.

[Ha07] M. Harris, *The Sato Tate conjecture: Analytic Arguments*, see `people.math.jussieu.fr/~harris/SatoTate/index.html`

[Hi06] H. Hida, *Hilbert modular forms and Iwasawa Theory*, Oxford Math. Monographs, Oxford University Press, Oxford, 2006.

[HSBT] M. Harris, N. Shepherd-Barron, R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Preprint, 2006.

[JW82] U. Jannsen and K. Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper.* Invent. Math. **70** (1982), no. 1, 71–98.

[KR01] C. Khare and C.S. Rajan, *The density of ramified primes in semisimple p-adic Galois representations.* Internat. Math. Res. Notices 2001, no. 12, 601–607.

[KW09] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I) and (II)*, Invent. math. **178** (2009), 485–504 and 505–586

[Ki09a] M. Kisin, *The Fontaine-Mazur conjecture for* GL_2, J. Amer. Math. Soc. **22** (2009), 641–690.

[Ki09b] M. Kisin, *Moduli of finite flat group schemes and modularity*, Ann. of Math. **170** (2009), 1085–1180.

[RT11] A. Raghuram and N. Tanabe, *Notes on the arithmetic of Hilbert modular forms.* arXiv:1102.1864v1

[Ra74] M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. SMF **102** (1974), 241–280.

[Ri85] K.A. Ribet *On ℓ-adic representations attached to modular forms II*. Glasgow Math. J. **27** (1985), 185–194.

[Ri90] K.A. Ribet, *On modular representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Inv. Math. **100** (1990), 431–476.

[Sai11] T. Saito, *Hilbert modular forms and p-adic Hodge theory*. Compos. Math. **145** (2009), no. 5, 1081–1113.

[Sav05] D. Savitt, *On a conjecture of Conrad, Diamond, and Taylor*. Duke Math. J. **128** (2005), no. 1, 141–197.

[Se68] J.-P. Serre, *Abelian ℓ-adic Galois representations and elliptic curves*. W.A. Benjamin, Inc, New York, 1968.

[Se77] J.-P. Serre, *Modular forms of weight one and Galois representations*. Proc. Durham Symp. on Algebraic Number Fields Acad. Press, London, 1977, 193–267.

[Se87] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54** (1987), no. 1, 179–230.

[Se91] J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*. In Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math. **55**, AMS Providence, RI, 1994, 377–400.

[ST68] J.-P. Serre and J. Tate *Good Reduction of Abelian Varieties*. Ann. Math. **88** (1968), no. 3, 492–517.

[Sh71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Publ. Math. Soc. Japan **11**, Princeton University Press, Princeton, NJ, 1971.

[Sh98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.

[Si85] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106** (1985), Springer New York.

[Si91] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM **151** (1991), Springer New York.

[Sk09] C. Skinner, *A note on the p-adic Galois representations attached to Hilbert modular forms*, Documenta Math. **14** (2009) 241–258.

[Sn09] A. Snowden, *On two dimensional weight two odd representations of totally real fields*, arXiv:0905.4266v1

[Tat67] J. Tate, *p-divisible groups*, in "Proc. Conf. on Local Fields" (Driebergen), Springer-Verlag, 1967, 158–183.

[Tat79] J. Tate: *Number Theoretic Background*, Proceedings Symp. Pure Math. **33** (1979), 3–26.

[Tay89] R. Taylor, *On Galois representations associated to Hilbert modular forms.* Invent. Math. **98** (1989), no. 2, 265–280.

[Tay91] R. Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), p. 281–332.

[Tay97] R. Taylor, *On Galois representations associated to Hilbert modular forms II.* in Elliptic Curves, Modular Forms & Fermat's Last Theorem (Hong Kong, 1993), J. Coates and S.-T. Yau, eds., International Press, 1997, 333–340.

[Tay06] R. Taylor, *On the meromorphic continuation of degree two L-functions*, Doc. Math. (2006), Extra Vol., 729–779.

[Tay08] R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic mod l Galois representations. II*, Pub. Math. IHES **108** (2008), 183–239.

[TW95] R. Taylor and A. Wiles,*Ring-theoretic properties of certain Hecke algebras.* Ann. Math. (2), **141** (1995), no. 3, 553–572.

[Wi95] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. Math. (2), **141** (1995), no. 3, 443–551.

Gebhard Böckle
Computational Arithmetic Geometry IWR (Interdisciplinary Center for Scientific Computing), University of Heidelberg
Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
gebhard.boeckle@iwr.uni-heidelberg.de