

# Galois representations

Gebhard Böckle

March 16, 2012

## Abstract

This are notes for parts of my talks at the Luxembourg Winter School 2012, organized by Gabor Wiese, Lior-Bary Soroker and Sara Arias de Reyna.

## 1 Elliptic curves, modular forms and compatible systems of Galois representations

### 1.0.1 Abelian CFT vs Langlands program

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

**Basic question:** Describe all Galois extension of a number field of a certain type. Too hard!

Much of current day number theory is concerned with understanding extension  $E/F$  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  $G_F = \text{Gal}(\bar{F}/F)$  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-Janntzen-Wingberg.

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

### 1.0.2 Sources of abelian and non-abelian Galois extensions

Abelian class field theory by itself is not constructive. Over  $\mathbb{Q}$  the cyclotomic extensions generate  $\mathbb{Q}^{\text{ab}}$ . Over CM fields one can consider CM abelian varieties and their torsion representation. The theory is worked out over imaginary quadratic fields – see [Si91]. For the general case, see [Sh98].

Beginning in the late 1960's mainly due to Langlands a new approach got started. 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 of symplectic groups. Langlands program is constructive but precise conjectures are not available in all cases.

Another important source of Galois representations is étale cohomology. In fact, in all cases above, one uses étale cohomology to construct Galois representations 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 semisimple Galois representations come from automorphic forms; see [Bel09].

### 1.0.3 Applications of Galois representations from automorphic forms:

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

- (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 Fermat's Last Theorem.
- (c) Wiles proof of FLT proved sufficiently many cases of Taniyama-Shimura to deduce FLT; [Wi95, TW95].
- (d) For elliptic curves  $A$  over arbitrary totally real  $F$ , it follows that if they are modular, then their  $L$ -function has an entire continuation to the complex plane. [Taylor has proved results that under certain conditions, only using potential modularity, that in many cases the  $L$ -function of  $A/F$  has a meromorphic continuation to  $\mathbb{C}$ . See for instance [Sn09, Tay06].]
- (e) If one can show that  $\text{Sym}^n A$  is modular for all  $n \in \mathbb{N}$  and  $A/F$  an elliptic curve without CM, then the Sato-Tate conjecture on the deviation of  $\#A(k_v)$  from  $\#k_v + 1$  follows for  $A$ . See [BLGG, CHT, HSBT, Tay08].

Here is the heuristic for the Sato-Tate distribution: Let  $X$  be the set of conjugacy classes of elements in  $SU_2(\mathbb{C})$ . A representative of a conjugacy class is  $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$ . Therefore conjugacy classes can be considered as elements  $\theta \in \mathbb{R}/\pi\mathbb{Z}$ . Consider

$$SU_2(\mathbb{C}) \rightarrow X \cong [0, \pi] \stackrel{-\cos}{\cong} [-1, 1].$$

The pushforward of the measure of equi-distribution on  $SU_2(\mathbb{C})$  yields the measure with distribution  $\frac{2}{\pi} \sin^2 \theta d\theta$  on  $[0, \pi]$ , or  $\frac{2}{\pi} \sqrt{1-t^2} dt$  on  $[-1, 1]$ .

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

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

(for an elliptic curve  $A$ ) or of the numbers

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

(for  $f$  a modular form) converges to a measure on  $[-1, 1]$  with the ST-distribution

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

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  $\text{Sym}^n A$ ,  $n \in \mathbb{N}$  is explained.

#### 1.0.4 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  $F_v$ ,  $\pi_v$  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  $G_v := G_{F_v} \rightarrow G_F$  (known to be injective) from the diagram

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

- (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 outside  $S$  unramified extension of  $F$ .
- (f) For  $v$  a place not in  $S$ , fix a Frobenius automorphism  $\text{Frob}_v \in G_{F,S}$  which is unique up to conjugation. (The kernel of  $G_v \rightarrow G_{F,S}$  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.)

## 1.1 Definition of $L$ -functions and Galois representations

### 1.1.1 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 1.1.** (a) For a prime  $\ell$ , 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  $\ell$ . So in principle  $\ell$  should occur in the above notation. However part (a) of the following result clarifies this problem and shows the independence of  $\ell$ .

**Theorem 1.2** (see [Si85], [Si91]). (a) *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  $\ell$ , 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.*

### 1.1.2 On traces and characteristic polynomials

**Lemma 1.3.** *Let  $\Pi$  be a profinite group. Let  $\mathcal{F} \subset \Pi$  be a subset such that  $\Pi$  is the topological closure of the conjugacy classes of  $\mathcal{F}$ . Then any continuous semi-simple representation  $\rho: \Pi \rightarrow \mathrm{GL}_n(L)$  where  $L \in \{\mathbb{C}, \overline{\mathbb{F}_\ell}, \overline{\mathbb{Q}_\ell}\}$  is uniquely determined by the characteristic polynomials  $\mathrm{charpol}(g) \in L[T]$  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 1.4.** *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 which  $V$  is unramified.*

- (b) In the situation of (a), one has  $\det(1 - TFrob_v|V) \in \mathcal{O}_E[T]$  for all  $v \notin S$  and  $\rho$  is completely determined by these characteristic polynomials, or even the traces of  $\rho(\text{Frob}_v)$ ,  $v \notin S$ .
- (c) There exists a unique continuous semisimple  $G_F$ -representation  $\bar{V}$  with

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

*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 Remark 1.3. (c) One reduces the lattice from (b), semisimplifies the reduction and applies Remark 1.3.  $\square$

**Corollary 1.5.** *Let  $A/F$  be an elliptic curve. Then  $V_\ell(A)$  is completely characterized by the condition  $\text{Trace}(\text{Frob}_v|V_\ell(A)) = a_v(A)$  for all finite places  $v$  not dividing  $N\ell$*

### 1.1.3 Hilbert modular forms

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 adèle 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.<sup>1</sup> Set  $t = (1, \dots, 1) \in \mathbb{Z}^I$ , 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  $\mu \in \mathbb{Z}_{\geq 0}$ .

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

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

where:

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

**Definition 1.6.** 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  $f: \text{GL}_2(F) \backslash \text{GL}_2(\mathbb{A}_F) \rightarrow \mathbb{C}$  satisfying the following conditions:

- (a)  $f|_k u = f$  for all  $u \in UZ_\infty$  where  $Z_\infty = (\mathbb{R}^* \cdot \text{SO}_2(\mathbb{R}))^I \subset G_\infty$ ;
- (b) for all  $x \in G_f$ , the function  $f_x: \mathfrak{h}^I \rightarrow \mathbb{C}$  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;

---

<sup>1</sup>In H. Hida, *Hilbert modular forms and Iwasawa Theory*, Oxford Math. Monogr., Oxford University Press, Oxford, 2006. 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)  $\int_{\mathbb{A}_f/F} f\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}x\right)da = 0$  for all  $x \in \mathrm{GL}_2(\mathbb{A}_F)$  and  $da$  an additive Haar measure on  $\mathbb{F}_F/F$ .

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 1.7.** For  $x \in G_f$  one defines the Hecke operator  $[UxU]$  for a function  $f: \mathrm{GL}_2(\mathbb{A}_F) \rightarrow \mathbb{C}$  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  $x = \begin{pmatrix} \pi_v & 0 \\ 0 & 1 \end{pmatrix}$  with  $v$  not a divisor of  $N$ , one abbreviates  $T_v := [UxU]$ .

For  $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$  with  $\alpha$  a fractional ideal of  $F$  prime to  $N$  one calls  $S_\alpha$  the diamond operator for  $\alpha$ .

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

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 1.8.** *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  $\lambda$  of the ring of integers  $\mathcal{O}_f$  of  $E_f$ , there exists a unique<sup>2</sup> continuous representation  $V_\lambda(f)$  (isomorphic to  $E_{f,\lambda}^2$ ), say*

$$\rho_{f,\lambda}: G_F \rightarrow \mathrm{GL}_2(E_{f,\lambda})$$

*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  $\ell$  is the rational prime under  $\lambda$  and  $E_{f,\lambda}$  is the completion of  $E_f$  at  $\lambda$ .*

Part (a) is due to Shimura. 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  $\mathrm{GL}_2$ . See [Ca86, Tay89]

---

<sup>2</sup>See Remark 1.3 and Theorem 1.10(d).

**Definition 1.9.** Let  $f$  be a cuspidal Hecke eigenform as in the previous theorem.

- (a) The  $L$ -factor of  $f$  at  $v$  is  $L_v(f, T) := \det(1 - T\text{Frob}_v | V_\lambda(f)^{I_v})^{-1}$ .
- (b) The  $L$ -function of  $f$  is

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

**Theorem 1.10.** Let  $k_0 := \max\{k_\tau \mid \tau \in I\}$ . Then

- (a) The local  $L$ -factors are independent of  $\lambda$  (as long as  $v$  is not above  $\ell$ ).
- (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  $\Lambda$  is obtained from  $L$  by multiplication by suitable  $L$ -factors at  $\infty$  – see the references.
- (d) The representation  $V_\lambda(A)$  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 1.11.* The idea of [Ri85] is as follows: If the representation is reducible get  $\varepsilon_\ell^a \varepsilon_\ell^b$  on the diagonal up to finite order with product  $\varepsilon_\ell^{k-1}$  up to finite order (by CFT). The Ramanujan-Petersen bound yields  $2a = 2b = k - 1$ . Growth of  $L$ -function at  $s = k$  gives two contradictory bounds (cusp form versus Eisenstein series.)

### 1.1.4 Compatible systems of Galois representations I

**Definition 1.12** (Weakly compatible system). Let  $E$  be a number field and  $\mathcal{P}$  its set of finite places. Let  $S_\lambda$  consist of the places  $v$  of  $F$  such that  $v$  and  $\lambda$  lie over the same rational prime  $\ell$ . A family of  $n$ -dimensional continuous Galois representations  $(\rho_\lambda: G_F \rightarrow \text{GL}_n(E_\lambda))_{\lambda \in \mathcal{P}}$  is an  $E$ -rational weakly compatibly system (with finite ramification set  $S$ ) if

- (a) for all  $\lambda \in \mathcal{P}$ , the representation  $\rho_\lambda$  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

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

where  $E$  is canonically a subfield of  $E_\lambda$ , its completion at  $\lambda$ .

**Example 1.13.** Let  $\mu_{\ell^\infty}$  denote the set of  $\ell$ -power roots of unity in  $\bar{F}$  for some number field  $F$ . It is clearly stable under  $G_F$ . Define the  $\ell$ -adic cyclotomic character  $\varepsilon_\ell: G_F \rightarrow \text{Aut}(\mu_{\ell^\infty}) \cong \mathbb{Z}_\ell^*$  by  $g \mapsto (\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^{\varepsilon_\ell(g)})$  for all  $n$ . (This is independent of the choice of roots  $(\zeta_{\ell^n})$ .) Then  $(\varepsilon_\ell)_\ell$  forms a compatibly  $\mathbb{Q}$ -rational system with ramification set  $S = \emptyset$ .

**Theorem 1.14.** (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  $f$ .

*Remark 1.15.* 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  $(\text{Sym}^n V_\ell(A))$  of representations of dimension  $n + 1$ .

### 1.1.5 What does it mean for $A$ 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  $\ell$ -adic Tate module  $V_\ell(A)$  of  $A$  and the  $\ell$ -adic Galois representation  $V_\ell(f)$  attached to  $f$  are isomorphic for one  $\ell$  (or all  $\ell$ ).
- 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  $A_f$ .

*Remark 1.16.* (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  $0 \rightarrow K \rightarrow A \rightarrow A' \rightarrow 0$  with finite kernel  $K$ . Passing to  $\ell^\infty$ -torsion points and Tate modules, we deduce

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

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:

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



## 1.2 Weil-Deligne representations

The following is based on notes by T. Gee from the 2011 Winter School in Postech, Korea. See also 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 even further to also include primes above the characteristic of the representation?

**Answer:** Yes (later), via Fontaine's  $p$ -adic Hodge theory – and again Weil-Deligne representations.

### 1.2.1 Galois representations of local fields

#### The Weil group

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

Every element  $g$  of  $G_K = \text{Gal}(\bar{K}/K)$  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  $G_K \rightarrow G_k$  is the inertia subgroup  $I_K$ .

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

$$0 \rightarrow I_K \rightarrow W_K \rightarrow \langle \text{Frob}_K \rangle \rightarrow 0.$$

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

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

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

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

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

Let  $\xi_K: W_K \rightarrow \langle \text{Frob}_K \rangle \rightarrow \mathbb{Z}$  be character defined by  $\text{Frob}_K \mapsto 1$ . Then one has

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

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

**Theorem 1.17** (Main Thm of local CFT (one version)). *Let  $W_K^{\text{ab}}$  denote the group  $W_K/\overline{[W_K, W_K]}$ . Then there is a unique system of isomorphisms (for all extensions of  $\mathbb{Q}_p$ )*

$$\text{Art}_K : K^* \rightarrow W_K^{\text{ab}}$$

such that

- (a) if  $K'/K$  is a finite extension and  $\pi_{K'/K} : W_{K'}^{\text{ab}} \xrightarrow{\text{can}} W_K^{\text{ab}}$ , then  $\pi_{K'/K} \circ \text{Art}_{K'} = \text{Art}_K \circ N_{K'/K}$ ,
- (b) and we have a commutative square

$$\begin{array}{ccc} K^* & \xrightarrow[\sim]{\text{Art}_K} & W_K^{\text{ab}} \\ \downarrow \text{v}_K & \searrow \xi_K & \downarrow \text{can}: g \rightarrow \bar{g} \\ \mathbb{Z} & \xrightarrow{a \mapsto \text{Frob}_K^a} & \langle \text{Frob}_K \rangle \end{array}$$

**Definition 1.18** (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  $\text{End}(V)$  such that for all  $\sigma \in W_K$  one has the following analog of (1)

$$r(\sigma)Nr(\sigma)^{-1} = q_v^{-\xi_K(\sigma)}N. \quad (2)$$

*Remark 1.19.* 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 (2) is equivalent to  $r(\sigma)N = Nr(\sigma)$  for all  $\sigma \in I_K$  and  $r(\varphi)Nr(\varphi)^{-1} = q_K^{-1}N$  for  $\varphi \in W_K$  a lift of the geometric Frobenius  $\text{Frob}_K$ .

The conductor of a WD-representation is  $c(r, N) := c(r) + \dim V^{I_K} - \dim(\text{Ker}(N : V \rightarrow V)^{I_K})$  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 1.20.* (a) For a representation  $(V; r)$  of  $W_K$  and  $m \geq 1$ , define  $\text{Sp}_m(r)$  as the triple

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

with  $N$  restricted to the  $i$ -th component  $V$  that is acted on by  $r \cdot |\text{Art}_K^{-1}|_K^i$  being the isomorphism to the  $i+1$ -th component acted on by  $r \cdot |\text{Art}_K^{-1}|_K^{i+1}$ . 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  $(r|_{G_{K'}}; V; N)$  is a WD representation of  $W_{K'}$ .
- (d) If  $r$  is a representation of  $W_K$ , then for a finite index subgroup  $H$  the image  $r(H)$  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  $\chi$  of  $W_K$  such that  $r = \chi \otimes r'$ .
- (g) Let  $\sigma$  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  $(r, N)^{F\text{-ss}} := (r^{\mathrm{ss}}, N)$  is a WD-representation of  $W_K$ .

Note that by  $r^{\mathrm{ss}}$  we mean the following semisimplification: suppose the  $\alpha$  is any automorphism of a vector space over a field  $L$ . Then  $\alpha$  can be written in a unique way as  $\alpha = \alpha^{\mathrm{ss}} \cdot \alpha^{\mathrm{unip}}$  for commuting endomorphisms  $\alpha^{\mathrm{ss}}$  and  $\alpha^{\mathrm{unip}}$  such that  $\alpha^{\mathrm{ss}}$  is semisimple, i.e., it is diagonalizable over  $L^{\mathrm{alg}}$ , and  $\alpha^{\mathrm{unip}}$  is unipotent, i.e., all of its eigenvalues are one. Now one defines  $r^{\mathrm{ss}}$  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 1.21.** A WD-representation  $(r, N)$  is Frobenius semisimple if  $r$  is semisimple. (i.e.  $r(\varphi)$  is semisimple as an endom.)

**Definition 1.22.** Let  $L$  be an algebraic extension of  $\mathbb{Q}_\ell$  with  $\ell \neq p$ .

- (a)  $A \in \mathrm{GL}_n(L)$  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  $\sigma$  in  $W_K$

*Remark 1.23.* (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 1.24** (Grothendieck's Monodromy theorem). *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  $\varphi \in W_K$  of  $\mathrm{Frob}_K$  and a compatible system  $\zeta = (\zeta_n)$  of roots of unity in  $K^{\mathrm{alg}}$ . (This defines a unique  $t_{\zeta, \ell}: I_K \rightarrow \mathbb{Z}_\ell$  for all  $\ell \neq p$ .)*

*For any continuous representation  $\rho: G_K \rightarrow \mathrm{GL}(V)$ , there exists a finite extension  $K'$  of  $K$  such that  $\rho(I_{K'}) \equiv 1 \pmod{2\ell}$  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  $r : W_K \rightarrow \mathrm{GL}(V)$  is defined by

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

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

Finally for any choices  $(\varphi, \zeta)$  and  $(\varphi', \zeta')$  there is a natural isomorphism  $\mathrm{WD}_{\varphi, \zeta} \rightarrow \mathrm{WD}_{\varphi', \zeta'}$ .

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

*Remark 1.25.* Suppose  $\rho : G_K \rightarrow \mathrm{Aut}(V)$  is unramified. Then  $N = 0$  and  $r(I_K) = \{1\}$  for  $(r, N) = \mathrm{WD}(V)$ . Thus  $r$  is completely determined by  $\rho(\varphi)$  for a lift  $\varphi$  of  $\mathrm{Frob}_K$ . In other words,  $\mathrm{WD}(\rho)$  depends on the conjugacy class of  $\rho(\varphi)$ , i.e., its rational canonical form. If one passes to  $\mathrm{WD}(\rho)^{F\text{-ss}}$ , then the isomorphism type of the latter is completely determined by the characteristic polynomial  $\det(1 - T\mathrm{Frob}_K|V)$ .

**Definition 1.26** (Strictly compatible system). Let  $E$  be a number field and  $\mathcal{P}$  its set of finite places. For  $\lambda \in \mathcal{P}$  let  $S_\lambda$  denote the set of places  $v$  of a number field  $F$  such that  $v$  and  $\lambda$  lie over the same rational prime  $\ell$ . A family of  $n$ -dimensional continuous Galois representations  $(V_\lambda)_{\lambda \in \mathcal{P}}$  of  $G_F$  is an  $E$ -rational strongly compatible system (with finite ramification set  $S$ ) if

- (a) for all  $\lambda \in \mathcal{P}$ , the representation  $V_\lambda$  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

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

*Conjecture 1.27* (Fontaine, Serre, Deligne). If  $V$  is a representation that occurs in the  $\ell$ -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  $\ell$ . See [Tat79], [Fo94, Section 2.4.], [Se91, §§11,12].

**Theorem 1.28** (Carayol, Eichler-Shimura, Langlands, Deligne). For  $v$  a Hilbert modular eigenform, the family  $(V_\lambda(f))$  is a strongly compatible  $E_f$ -rational system;

*Conjecture 1.29* (Fontaine, Serre). Suppose  $A/F$  is an abelian variety. Then  $(V_p(A))$  is a strongly compatible system.

I do not know the status of the latter conjecture, i.e., whether condition (c) of Definition 1.33 holds. The thesis of A. Laskar from 2011 (Strasbourg) implies that latter conjecture if  $A$  has semistable reduction. I do not know of a reference for potentially semistable. I also do not know what is known about Frobenius semisimplicity.

### 1.3 How to deal with primes above $\ell$ ?

#### 1.3.1 An example

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

##### 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

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

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

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

with respect to a suitable basis and where  $\varepsilon_\ell$  is the  $\ell$ -adic cyclotomic character and  $\chi$  is an unramified character. Due to the Weil-paring, the determinant must be  $\varepsilon_\ell$ . Note the  $\varepsilon_\ell$  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  $\ell$  reduction is rather special as can be seen from analyzing the  $\ell$ -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 1.30.* Suppose  $A$  has good reduction and  $\pi$  denotes the Frobenius endomorphism on  $A/k_v$ , so that  $\pi$  satisfies the quadratic polynomial  $p_v(T) = T^2 - a_v T + q_v$  with integer coefficients, where  $A[p](\bar{k}_v) = q_v - a_v(a) + 1$ . Let  $\alpha, \beta \in \bar{\mathbb{Z}}$  be the roots of  $p_v$  so that  $v_{q_v}(\alpha\beta) = 1$ . It is also standard that  $A[p](\bar{k}_v^n) = q_v^n - \alpha^n - \beta^n + 1$  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, the without loss of generality  $v_{q_v}(\alpha) = 0$ . Show that  $\chi^{-1}(\mathrm{Frob}_v)$  acts on the  $p^\infty$  torsion points in the same way as  $\pi$  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  $\ell^\infty$ -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  $\ell^\infty$  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

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

**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  $\ell'$ -adic data**

If one looks at the  $\ell'$ -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:

**1.4 Fontaine's mysterious functors**

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  $D_*$ ,  $*$   $\in$  {HT, dR, cris, st} from

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

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  $B_{\mathrm{HT}}$  is the graded ring associated to  $B_{\mathrm{dR}}$ . The structures are a continuous action of  $G_K$  and

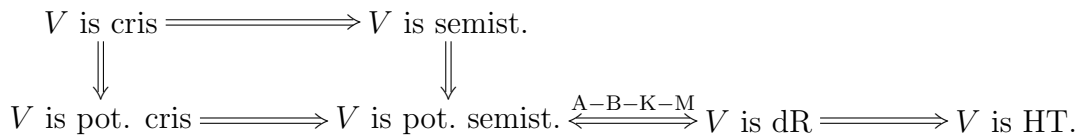
- (a) a graduation,
- (b) a filtration,
- (c) a filtration and a semilinear endomorphism  $\varphi$  (Frobenius)
- (d) a filtration and two endomorphisms  $\varphi, N$  – for more, see 1.4.1.

The rings  $B_*$  also satisfy  $B_*^{G_K} = K_*$ . One calls a representation  $\rho$  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  $B_{\mathrm{HT}}$  attaches the HT-weights (in  $\mathbb{Z}$ ) to a representation. The ring  $B_{\mathrm{dR}}$  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  $\rho$  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



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.

#### 1.4.1 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 such that  $V|_{G_{K'}}$  is semistable. Then  $D_{\text{st}}(V|_{G_{K'}}) = (D, \varphi, N, \text{Fil}^i)$  where

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

and the quadruple is equipped with an action of  $\text{Gal}(K'/K)$ , i.e., an action  $\text{Gal}(K'/K) \rightarrow \text{Aut}(D, \varphi_D, N_D, \text{Fil}^\bullet)$ . If the representation is semistable, one has  $K' = K$ , if it is potentially crystalline, then  $N = 0$  (and vice versa).

*Remark 1.31.* The quadruple  $(D, \varphi_D, N_D, \text{Fil}^i)$  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. Here  $t_H(D)$  is the index of the unique jump of the filtration of the induced filtration  $\text{Fil}^i \bigwedge^d D$  and  $t_N$  is the slope of  $\bigwedge^d \varphi_D$ .

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

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

Correspondingly one has

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

with suitable components  $D_\tau$  of  $D$ . One verifies that  $\varphi_D^{[K'_0:\mathbb{Q}_p]}$  induces an isomorphism of the  $D_\tau$  since it is  $K'_0 \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ -linear. Fix  $\tau_0$  among the  $\tau$ .

**Definition 1.32.** Let  $K, V, K', D$  be as above and let  $\varphi \in W_K$  be a lift of  $\text{Frob}_K$ . Then the WD-representation  $\text{WD}(V)$  is the triple  $(U, r, N)$  where

- (a)  $U$  is the  $\overline{\mathbb{Q}_p}$  vector space  $D_{\tau_0}$ ,

(b)  $r: W_K \rightarrow \text{Aut}_{\overline{\mathbb{Q}_p}}(U)$  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  $I_K \rightarrow \text{Gal}(K'/K)$  on  $D$  to the invariant subspace  $D_{\tau_0}$ ,
- (ii) and having  $\varphi$  act as  $\varphi_2^{-1}\varphi_1$  on  $D_{\tau_0}$  where  $\varphi_1$  is the action of  $\varphi$  via  $\text{Gal}(K'/K)$  and  $\varphi_2$  is the action  $\varphi_D^{[K_0:\mathbb{Q}_p]}$  both times on  $D$  and then restricted to the invariant subspace  $D_{\tau_0}$ ,

(c)  $N$  is the restriction of the endomorphism  $N_D$  from  $D$  to its invariant subspace  $D_{\tau_0}$ .

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  $\varphi$  is the inverse of  $\varphi_D$  (and  $N = N_D$ ).

**Note:** The eigenvalues of  $r(\varphi)$  to the power  $[K'_0 : K_0]$  are those of  $\varphi_D^{-[K'_0:\mathbb{Q}_p]}$ . Hence their  $p$ -adic valuations are up to the scalar  $[K_0 : \mathbb{Q}_p]$  the slopes (=  $p$ -adic valuations) of the eigenvalues of  $\varphi_D$ . 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.

### 1.4.2 Continuation of the above example of an elliptic curve $A/F_v$

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

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

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

(b) If  $A$  has supersingular reduction, then either  $D_{\text{cris}}(V_\ell(A))$  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  $D_{\text{cris}}(V_\ell(A))$  becomes the sum of two 1-dimensional subobjects.

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

### 1.4.3 Compatible systems III

**Definition 1.33** (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  $S_\lambda$  denote the places  $v$  of  $S$  such that  $v$  and  $\lambda$  lie over the same rational prime  $\ell$ .

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  $V_\lambda$  is unramified outside  $S \cup S_\lambda$  and potentially semistable at the places in  $S_\lambda$ ;
- (b) for all finite places  $v$  of  $F$  there exists a Frobenius semisimple WD-representation  $(r_v, N_v)$  of  $F_v$  such that

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



*Remark 1.34.* As remarked earlier, if  $v$  is not in  $S$ , then  $(r_v, N_v)$  is simply  $(\rho(\text{Frob}_v)^{\text{ss}}, 0)$ . Hence for  $v \notin S \cup S_\lambda$  one can simply write require a compatibility of characteristic polynomials

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

*Remark 1.35.* 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 1.36** (Faltings, see [Fa87]). *For a cuspidal Hecke eigenform  $f$  the representations  $(V_\lambda(f))_\lambda$  are semistable of HT-weights  $(0, k - 1)$ .*

*Remark 1.37.* 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  $\ell$  and all embeddings  $F_v \hookrightarrow \overline{\mathbb{Q}_\ell}$ . A proof in other language is contained in [Tat67].

**Theorem 1.38** (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 1.39.* 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  $\dim A$ .)

## 1.5 Refinement: Fontaine Laffaille theory

The above is not the end of the story of understanding  $\ell$ -adic Galois representations of  $\ell$ -adic fields. One also needs *integral information* on  $V(\rho)$ . Fontaine's theory above only contributes to  $\ell$ -adic information, but does not help if one studies the mod  $\ell$ -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 1.40.** A *strongly divisible module* is a free  $W$ -module  $M$  of finite type equipped with a decreasing filtration by sub- $W$ -modules  $(\text{Fil}^i M)_{i \in \mathbb{Z}}$  such that  $\text{Fil}^0 M = M$ ,  $\text{Fil}^i M = 0$  for  $i \gg 0$ , each subquotient  $M/\text{Fil}^i M$  free over  $W$  and one has a semilinear, i.e., a  $\sigma$ -linear, endomorphism  $\varphi: M \rightarrow M$  such that  $\varphi(\text{Fil}^i M) \subset p^i \text{Fil}^i M$  and  $M = \sum_{i \geq 0} p^{-i} \varphi(\text{Fil}^i M)$ .

**Theorem 1.41** (Fontaine-Laffaille). *If  $M$  is a strongly divisible module, then  $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$  is admissible, i.e., equal to  $D_{\text{cris}}(V)$  for some rank- $W$  dimensional (crystalline) representation of  $G_K$ .*

*Suppose conversely that  $V$  is a crystalline representation of  $G_K$  of HT weights between 0 and  $p - 2$  and with  $\mathbb{Q}_p$ -coefficients. Then  $D_{\text{cris}}(V)$  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 1.42.** 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  $\varphi^i: \mathrm{Fil}^i M \rightarrow M$  such that  $\varphi|_{\mathrm{Fil}^i M} = \varphi^i$  and  $M = \sum_{i \geq 0} \varphi^i(\mathrm{Fil}^i M)$ .

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

**Theorem 1.43** (Fontaine-Laffaille). *Suppose  $A$  is a finite  $W$ -algebra. If  $M$  is a Fontaine-Laffaille-module over  $A$ , then under the integral version  $T_{\mathrm{cris}}$  of  $D_{\mathrm{cris}}$  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  $T_{\mathrm{cris}}$  is a Fontaine-Laffaille-module  $M$  over  $A$ .*

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

**Theorem 1.44** (Fontaine-Laffaille + Raynaud). *Let  $\mathrm{MF}_{\mathrm{tor}}^1$  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:*

$$\mathrm{MF}_{\mathrm{tor}}^1 \xrightarrow[\mathrm{FL}]{\mathbb{R}} \{ \text{finite flat group schemes}/W \} \xrightarrow[\mathrm{Ray.}]{\cong} \{ \text{flat repns. of } G_K \}.$$

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

## 1.6 The Fontaine Mazur conjecture

The Fontaine-Mazur conjecture is the following statement:

*Conjecture 1.45* ([FM95]). Let  $F$  be a number field and  $S$  a finite set of places of  $F$ . Suppose that  $\rho: G_{F,S} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$  is continuous and irreducible and that  $\rho|_{G_v}$  is de Rham for all  $v|_\ell$ . Then  $\rho$  comes from geometry, i.e., there exists a smooth projective variety  $X$  over  $F$  such that  $\rho$  is a subquotient of some  $\ell$ -adic cohomology  $H^i(X_{\overline{F}}, \mathbb{Q}_\ell)$ .

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 1.46.* Let  $S$  be a finite set of places of  $\mathbb{Q}$ . Suppose that  $\rho: G_{\mathbb{Q},S} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$  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  $\lambda$  of the coefficient field  $E_f$  of  $f$  such that  $V(\rho) \cong V_\lambda(f)$ .

Conjecture 1.46 is proved in the majority of cases by Emerton and Kisin in [Em11] and [Ki09].

A second special case is the following:

*Conjecture 1.47.* Let  $F$  be a totally real number field. Suppose  $\rho: G_{F,S} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$  is continuous, irreducible and of weight 2, i.e., it is de Rham at all places above  $\ell$  with HT-weights  $(0, 1)$  for all places  $v|\ell$  and all embeddings  $F_v \rightarrow \overline{\mathbb{Q}_\ell}$ . Then  $\rho$  arises from a Hilbert modular form of weight  $(2, \dots, 2)$ .

Conjecture 1.47 in the form stated is completely open. A weaker assertion is given by the potential modularity results of Taylor. We follow the cases given in [Sn09]:

**Theorem 1.48** (Taylor, Deulefait (version of [Sn09])). *Suppose  $\rho$  is as in conjecture 1.47 and that its reduction mod  $p$  is absolutely irreducible, that  $p \geq 3$  and that for  $p = 5$  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 compatible system (in the strong sense)  $(\rho_\lambda: G_{F,S} \rightarrow \mathrm{GL}_n(E_\lambda))_\lambda$  for some number field  $E$  and a place  $\lambda_0$  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].

## 1.7 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  $A[p] \cong \overline{V_\varphi(f)}$  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: can assume that  $f$  has level dividing  $N$  and weight equal to 2.
- Consider the Hecke-algebra  $\mathbb{T}\Gamma_0(N)$  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  $\mathbb{T}_2(\Gamma_0(N)) \rightarrow \overline{\mathbb{F}_p} : T_v \mapsto a_v(f) \bmod \mathfrak{m}_{\overline{\mathbb{F}_p}}$ . Let  $\mathfrak{m}_{\bar{p}}$  be the kernel for our fixed  $f$ . Then the localization  $\mathbb{T}_{\bar{p}} := \mathbb{T}_2(\Gamma_0(N))_{\mathfrak{m}_{\bar{p}}}$  is a local ring.

**Proposition 1.49.** *(a)  $\mathrm{Hom}_{\mathbf{Ri}}(\mathbb{T}_{\bar{p}}, \overline{\mathbb{Q}_p})$  is in bijection with the set of cuspidal Hecke newforms of level dividing  $N$  whose associated mod  $p$  Galois representation is isomorphic to  $\bar{\rho}$ . (Mod  $p$  means mod  $\lambda$  for some  $\lambda$  over  $p$ .)*

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

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

The proposition says that any Galois representation that arises from a level  $N$  form  $g$  of weight 2 (or  $k$ ) and that is congruent to  $f \pmod{p}$  is obtained from  $\rho^{\text{mod}}$  by a ring homomorphism  $\mathbb{T}_{\bar{\rho}} \rightarrow \overline{\mathbb{Q}_p}$ . 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

$$\tilde{\rho}: G_{\mathbb{Q}} \rightarrow \text{GL}_2\left(\prod_{g \in M_{\bar{\rho}}} \mathcal{O}\right)$$

with  $\tilde{\rho}(\text{Frob}_v) = (a_v(g))_{g \in M_{\bar{\rho}}}$ . 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  $\text{Trace}(\tilde{\rho}(\text{Frob}_v)) = T_v$ . (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  $\tilde{\rho}$  belong to the subring  $\mathbb{T}_{\bar{\rho}}$ , (iv)  $\bar{\rho}$  is absolutely irreducible. Then  $\tilde{\rho}$  is already defined over  $\mathbb{T}_{\bar{\rho}}$ , and this is exactly the claim of (b)  $\square$

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 weight 0,1 (flat), 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 1.50.** *There exists a unique surjective homomorphism  $\alpha: R \rightarrow \mathbb{T}_{\bar{\rho}}$  such that*

$$\rho^{\text{mod}} \stackrel{\text{conj.}}{\sim} \alpha \circ \rho_R.$$

In the above situation one has the following result:

**Theorem 1.51 (Main Theorem [Wiles, BCDT]).** *For  $\mathbb{Q}$  have an isomorphism  $R \rightarrow \mathbb{T}_{\bar{\rho}}$ .*

Many refinements by Kisin, Khare-Wintenberger, Taylor and "his" school.

**Preview:** In the remainder of this lecture series, I shall talk about universal deformation rings and some subtleties in their definition. If time permits, I shall also explain some upper bound on its dimension. References are

- (a) [Ma87] by Mazur for basic material.
- (b) [Ki09] by Kisin for a short survey of many modern techniques.
- (c) [Ki09] by Kisin for some groundbreaking deep results on deformation theory.
- (d) [Pi07] by Pilloni for a treatment of local deformation problems for  $n = 2$  and  $p \neq \ell$ .
- (e) [CHT] by Clozel, Harris, Taylor for many local (and global) deformation functors for  $GL_n$ .
- (f) [Bö10] for a detailed lecture series by myself on the topic.

**Acknowledgements:** Many thanks go to Hendrik Verhoek for a careful proof-reading.

## References

- [BLGG] T. Barnet-Lamb, T. Gee, D. Geraghty, *The Sato-Tate conjecture for Hilbert modular forms*. J. Amer. Math. Soc. **24** (2011), no. 2, 411–469.
- [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/talks.html>
- [Ber02] L. Berger, *An introduction to the theory of  $p$ -adic representations*, arXiv:math.NT/0210184 v1, p. 18.
- [Bl06] D. Blasius, *Hilbert modular forms and the Ramanujan conjecture*. Noncommu. geometry and number theory, Aspects Math., E37, Vieweg, 2006, 35–56. see <http://www.math.ucla.edu/~blasius/papers.html>
- [Bö10] Gebhard Böckle, *Deformations of Galois representations*, Notes from a Lectures series at the CRM Barcelona, Spring 2010, [http://www.iwr.uni-heidelberg.de/groups/arith-geom/boeckle\\_old\\_design/Boeckle-Notes.pdf](http://www.iwr.uni-heidelberg.de/groups/arith-geom/boeckle_old_design/Boeckle-Notes.pdf)
- [BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
- [Bu10] K. Buzzard, *Potential modularity—a survey*. arXiv:1101.0097v2
- [Ca86] Carayol, Henri, *Sur les représentations  $\ell$ -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] Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some  $\ell$ -adic lifts of automorphic mod  $l$  Galois representations*, Pub. Math. IHES **108** (2008), 1–181.
- [Co03] Colmez, Pierre, *Les conjectures de monodromie  $p$ -adiques*. Sémin. Bourbaki, Astérisque **290** (2003), Exp. No. 897, 53–101.

- [CR62] C.W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley Interscience, New York, 1962.
- [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] Emerton M., *Local-global compatibility in the  $p$ -adic Langlands programme for  $GL_2/\mathbb{Q}$* , 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.
- [Fo94] Jean-Marc Fontaine. *Représentations  $l$ -adiques potentiellement semi-stables*. In Périodes  $p$ -adiques, Astérisque, **223** (1994), 321–347.
- [FL82] J.-M. Fontaine, G. Laffaille, *Construction de représentations  $p$ -adiques*, Ann. Sci. ENS **15** (1982), 547–608.
- [FM95] Fontaine, Jean-Marc; Mazur, Barry, *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.
- [GM09] E. Ghate, A. Mezard, *Filtered modules with coefficients*. Trans. Amer. Math. Soc. **361** (2009), no. 5, 2243–2261.
- [Ha07] Michael Harris, *The Sato Tate conjecture, : Analytic Arguments*, see <http://people.math.jussieu.fr/~harris/SatoTate/index.html>
- [HSBT] Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Preprint, 2006.
- [KR01] Khare, Chandrashekhara; Rajan, C. S. *The density of ramified primes in semisimple  $p$ -adic Galois representations*. Internat. Math. Res. Notices 2001, no. 12, 601–607.
- [KW09] Chandrashekhara Khare, Jean-Pierre Wintenberger, *Serre’s modularity conjecture (I) and (II)*, Invent. math. **178** (2009), 485–504 and 505–586
- [Ki09] Kisin M., *The Fontaine-Mazur conjecture for  $GL_2$* , J. Amer. Math. Soc. **22** (2009), 641–690.
- [Ki09] M. Kisin, *Moduli of finite flat group schemes and modularity*, Ann. of Math. **170** (2009), 1085–1180.
- [Ki09] M. Kisin, *Lecture notes on Deformations of Galois Representations*, Notes for the Clay Math. Institute 2009 Summer School on Galois Representations, June 15 - July 10, 2009, University of Hawaii. <http://www.math.harvard.edu/~kisin/>

- [Ma87] B. Mazur, *Deforming Galois representations*, in "Galois groups over  $\mathbb{Q}$ ", Y. Ihara, K. Ribet, J.-P. Serre eds, MSRI Publ. **16** (1987), 385–437, Springer, New York-Berlin, 1989..
- [Pi07] V. Pilloni, *The study of 2-dimensional  $p$ -adic Galois deformations in the  $\ell \neq p$  case*. Lecture notes for the summer school at Luminy, 2007. see <http://perso.ens-lyon.fr/vincent.pilloni/Defo.pdf>
- [RT11] A. Raghuram, Naomi Tanabe, *Notes on the arithmetic of Hilbert modular forms*. arXiv:1102.1864v1
- [Ra74] M. Raynaud, *Schémas en groupes de type  $(p, \dots, p)$* , Bull. SMF **102** (1974), 241–280.
- [Ri85] K. Ribet *On  $\ell$ -adic representations attached to modular forms II*. Glasgow Math. J. **27** (1985), 185–194.
- [Ri90] K.A. Ribet, *On modular representations of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  arising from modular forms*, Inv. Math. **100** (1990), 431–476.
- [Sai11] Saito, Takeshi, *Hilbert modular forms and  $p$ -adic Hodge theory*. Compos. Math. **145** (2009), no. 5, 1081–1113.
- [Sav05] David Savitt, *On a conjecture of Conrad, Diamond, and Taylor*. Duke Math. J. **128** (2005), no. 1, 141–197.
- [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] Serre, J.-P.: *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$* . Duke Math. J. **54** (1987), no. 1, 179–230.
- [Se91] Jean-Pierre 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.
- [Sh98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.
- [Si91] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM **151** (1991), Springer New York.
- [Si85] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106** (1985), 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] John Tate: *Number Theoretic Background*, Proceedings Symp. Pure Math. **33** (1979), 3–26.
- [Tay89] Taylor, Richard, *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] Richard Taylor, *On the meromorphic continuation of degree two L-functions*, Doc. Math. (2006), Extra Vol., 729–779.
- [Tay08] R. Taylor, *Automorphy for some  $\ell$ -adic lifts of automorphic mod  $l$  Galois representations. II*, Pub. Math. IHES **108** (2008), 183–239.
- [TW95] Taylor, R., Wiles, A., *Ring-theoretic properties of certain Hecke algebras*. Ann. Math. (2), **141** (1995), no. 3, 553–572.
- [Wi95] Wiles, A. *Modular elliptic curves and Fermat’s last theorem*. Ann. Math. (2), **141** (1995), no. 3, 443–551.