p-adic Galois representations

Tamás Szamuely

Notes by Davide Lombardo

Disclaimer. Rough first draft. Any and all mistakes are due to the scribe!

Contents

1 18.01.2024 – Introduction

1.1 First definitions

Let K be a field with separable closure K^s. Denote by G the absolute Galois group $G := \mathrm{Gal}(K^s/K)$. By Galois theory, there is a correspondence

$$\{\text{finite quotients of } G\} \longleftrightarrow \{\text{finite Galois extensions } L/K\},$$

and in fact $G = \varprojlim_L \mathrm{Gal}(L/K)$, where the limit is taken over the finite Galois extensions L of K. Hence, G is an inverse limit of finite groups. Such a group is called a *profinite group* and carries a natural topology (the *profinite topology*): the profinite limit can be seen as a subgroup of the product $\prod_L \mathrm{Gal}(L/K)$, and it carries the subspace topology, where each finite group $\mathrm{Gal}(L/K)$ is given the discrete topology. For this topology, G is compact and totally disconnected, and there is a correspondence

$$\{\text{open subgroups of } G\} \longleftrightarrow \{\text{finite separable extensions } L/K\}.$$

We now define Galois representations. Let ℓ be a prime number and recall the ring $\mathbb{Z}_\ell := \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$ of ℓ-adic integers. This is a profinite ring; its field of fractions

$$\mathbb{Q}_\ell := \mathrm{Frac}(\mathbb{Z}_\ell)$$

is the field of ℓ-adic numbers. It has a locally compact topology, inherited from $\mathbb{Z}_\ell$. The standard n-dimensional vector space $\mathbb{Q}_\ell^n$ then has a natural (product) topology; so does the ring of endomorphisms $\mathrm{End}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell^n)$, which we identify with $\mathrm{Mat}_{n\times n}(\mathbb{Q}_\ell)$ and equip again with the product topology. The subgroup

$$\mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell^n) \subset \mathrm{End}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell^n)$$

then inherits the subspace topology, which makes it into a topological group. Finally, if V is any finite-dimensional $\mathbb{Q}_\ell$-vector space, any choice of basis induces an isomorphism $V \cong \mathbb{Q}_\ell^n$ for a suitable integer n, and via this isomorphism we get a topology on V, $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ and $\mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.

Exercise 1.1. *The topology on V does not depend on the chosen isomorphism $V \cong \mathbb{Q}_\ell^n$.*

Definition 1.2. An ℓ-adic Galois representation of G is a continuous homomorphism $\rho : G \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ where V is a finite-dimensional $\mathbb{Q}_\ell$-vector space. Equivalently, it is the datum of a finite-dimensional $\mathbb{Q}_\ell$-vector space equipped with a continuous action of G.

Remark 1.3. One can also reformulate the definition of ℓ-adic Galois representations in terms of $\mathbb{Q}_\ell[G]$-modules, but some care is needed to formulate the topological conditions.

Remark 1.4. A *lattice* in V is a finitely generated free $\mathbb{Z}_\ell$-module $L \subset V$ that generates V over $\mathbb{Q}_\ell$. Notice that any finitely-generated $\mathbb{Z}_\ell$-submodule of V is torsion-free, hence free by the structure theorem. In particular, the natural map $L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \xrightarrow{\sim} V$ is an isomorphism.

Lemma 1.5. *If V is an ℓ-adic representation of G, then V contains a G-stable lattice.*

Proof. Let $L \subset V$ be any lattice (for example, the $\mathbb{Z}_\ell$-span of a basis). Consider $U := \{g \in G : \rho(g)L \subseteq L\}$: it is an *open* subgroup of G (because the action is continuous). We justify this fact more carefully. A basis of open neighbourhoods of the origin in $\mathbb{Z}_\ell^n$ is given by $(\ell^k \mathbb{Z}_\ell)^n$. As a consequence, identifying $\mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ to $\mathrm{GL}_n(\mathbb{Q}_\ell)$, neighbourhoods of an element $g \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ are invertible matrices of the form $g + \ell^k M$ for some $M \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_\ell)$. However, any matrix of the form $\ell^k M$ with M having integral entries preserves any lattice, which shows the above claim.

Since G is compact, the open subgroup U has finite index, and we can consider

$$\sum_{g \in G} \rho(g)L \subset V :$$

it is clearly a G-stable subset, and it's a lattice since we are only adding finitely many distinct lattices (indeed, we could equivalently sum over representatives for G/U), so the result is still a finitely-generated $\mathbb{Z}_\ell$-module. □

Given an ℓ-adic Galois representation V, the previous lemma yields a finitely-generated free $\mathbb{Z}_\ell$-module $L' \subset V$ with a continuous representation $G \to \mathrm{Aut}_{\mathbb{Z}_\ell}(L')$.

Definition 1.6. A $\mathbb{Z}_\ell$-representation of G is a finitely-generated $\mathbb{Z}_\ell$-module M together with a continuous homomorphism $G \to \mathrm{Aut}_{\mathbb{Z}_\ell}(M)$.

Remark 1.7.
1. We do *not* require M to be torsion-free! In particular, this definition contains the notion of (continuous) Galois representations in an $\mathbb{F}_\ell$-vector space.
2. M is isomorphic to the inverse limit of its finite quotients: $M \cong \varprojlim_n M/\ell^n M$, where $M/\ell^n M$ is finite. There is a G-action on $M/\ell^n M$ for every n, and the isomorphism is compatible with the G-action on both sides.

   The interest of this remark is of course that it is often possible to reduce questions about $\mathbb{Z}_\ell$-representations to questions about finite representations.

Given a finitely generated free $\mathbb{Z}_\ell$-module M that is a $\mathbb{Z}_\ell$-representation of G, we get an ℓ-adic representation of G by taking $V := M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and setting

$$g \cdot (m \otimes \lambda) = (g \cdot m) \otimes \lambda \quad \forall g \in G.$$

Hence, we can go back and forth between free $\mathbb{Z}_\ell$-representations of G and ℓ-adic representations. Note however that this is not a bijective correspondence: in general, a given ℓ-adic representation has many G-stable lattices.

1.2 Examples

1.2.1 The cyclotomic character

Let ℓ be a prime different from the characteristic of K. Let μ_{ℓ^n} be the group of ℓ^n-th roots of unity in K^s. Define

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n},$$

where the transition maps are

$$\begin{array}{ccc} \mu_{\ell^n} & \to & \mu_{\ell^{n-1}} \\ \omega & \mapsto & \omega^\ell. \end{array}$$

The group G acts on μ_{ℓ^n} for all n (in a way that is compatible with the transition maps), hence there is an induced action ($\mathbb{Z}_\ell$-representation)

$$\chi : G \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(\mu)) \cong \mathbb{Z}_\ell^\times.$$

To justify the last isomorphism, note that for every n we have

$$\mathrm{Aut}_{\mathbb{Z}_\ell}(\mu_{\ell^n}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times,$$

and these isomorphisms are compatible for different n in the obvious sense. By passing to the limit,

$$\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(\mu)) \cong \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times \cong \mathbb{Z}_\ell^\times.$$

We further set $V_\ell(\mu) := T_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$: it is a 1-dimensional ℓ-adic representation of G, corresponding to a homomorphism

$$G \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(\mu)) \cong \mathbb{Q}_\ell^\times.$$

We can make the representation χ more explicit. Let $\omega \in T_\ell(\mu)$ be represented by the sequence $(\omega_n)_n$, where $\omega_n \in \mu_{\ell^n}$. By definition,

$$g(\omega) = (g(\omega_n))_n = (\omega_n^{\chi_n(g)})_n,$$

where $\chi_n(g)$ is an element in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$. We can then consider $\chi(g) \in \mathbb{Z}_\ell^\times = \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ as the compatible sequence $(\chi_n(g))_n$.

Definition 1.8. The map χ constructed above is called the *ℓ-adic cyclotomic chracter.*

Notation 1.9. *We write $\mathbb{Z}_\ell(1) := T_\ell(\mu)$ and $V_\ell(1) := V_\ell(\mu)$. For every $i > 0$ we then set*

$$\mathbb{Z}_\ell(i) := \mathbb{Z}_\ell(i)^{\otimes i}, \quad \mathbb{Q}_\ell(i) := \mathbb{Q}_\ell(i)^{\otimes i}.$$

The G-action is given by

$$g(w_1 \otimes \cdots \otimes w_i) = g(w_1) \otimes \cdots \otimes g(w_i).$$

As a $\mathbb{Z}_\ell$-module, $\mathbb{Z}_\ell(i)$ is simply $\mathbb{Z}_\ell$, but the Galois action is given by the i-th power of the cyclotomic character.

For $i < 0$ we further define

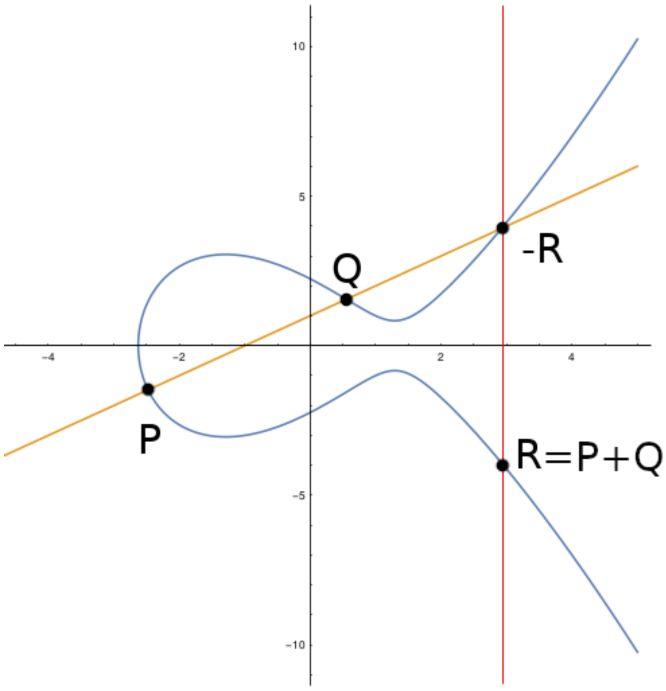
$$\mathbb{Z}_\ell(i) := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell(-i), \mathbb{Z}_\ell), \quad \mathbb{Q}_\ell(i) := \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell(-i), \mathbb{Q}_\ell).$$

1.2.2 Elliptic curves

Let E be an elliptic curve over K, that is, a smooth projective connected curve of genus 1 over K together with a rational point $0 \in E(K)$. Assuming $\mathrm{char}(K) \neq 2, 3$, the curve E can be described by a homogeneous equation

$$Y^2 Z = X^3 + AXZ^2 + BZ^3 \subset \mathbb{P}^2_K,$$

with the point 0 being $[0 : 1 : 0]$.



Rational points on elliptic curves form a group: given two points $P, Q \in E(K)$, the line through P and Q meets E in precisely another point $-R = (x, y)$ (counting with multiplicity). The point $R = (x, -y)$ is then the sum of P and Q. When $P = Q$, one takes the 'line through P and Q' to be the tangent to E at P.

Theorem 1.10. *This construction makes $E(K)$ into an abelian group.*

We have the following fundamental fact:

Theorem 1.11. *Let ℓ be a prime different from the characteristic of K. Denote by*

$$E[\ell^n] = \{P \in E(K^s) \mid \ell^n P = 0\}$$

the set of ℓ^n-th torsion points of E. The group $E[\ell^n]$ is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$.

Define the *ℓ-adic Tate module of E* as

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

with transition maps given by

$$\begin{array}{ccc} E[\ell^{n+1} & \to & E[\ell^n] \\ P & \mapsto & \ell P. \end{array}$$

Since G acts on each group $E[\ell^n]$ (compatibly for different n), we get an induced action of G on $T_\ell(E)$ which makes it into a (2-dimensional) $\mathbb{Z}_\ell$-representation of G. Correspondingly, we have a 2-dimensional ℓ-adic representation of G given by

$$V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Generalisation: abelian varieties An abelian variety over K is a smooth projective connected variety A defined over K with a 'geometrically defined' abelian group structure on A (that is to say, the maps giving multiplication and inverse are morphisms of algebraic varieties; the origin of the group law is given by a K-rational point).

Example 1.12. Any product of elliptic curves $E_1 \times E_2 \times \cdots \times E_n$ is an abelian variety. So is the Jacobian of any smooth projective curve C.

Theorem 1.13. *For every prime $\ell \neq \mathrm{char}(K)$, the ℓ^n-torsion subgroup*

$$A[\ell^n] := \{P \in A(K^s) : \ell^n P = 0\}$$

is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, where $g = \dim A$.

As in the case of elliptic curves, we have $2g$-dimensional $\mathbb{Z}_\ell$- and $\mathbb{Q}_\ell$-representations of G, given by

$$T_\ell(A) := \varprojlim_n A[\ell^n], \quad V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

1.2.3 The ultimate generalisation: étale cohomology groups

Let X be a smooth algebraic variety over K and let $\overline{X} := X \times_K K^s$. For every prime $\ell \neq \mathrm{char}(K)$, étale cohomology provides us with certain finite-dimensional $\mathbb{Q}_\ell$-vector spaces $H^i(\overline{X}, \mathbb{Q}_\ell)$, called the *$\ell$-adic étale cohomology groups of $\overline{X}$*. When K is a subfield of $\mathbb{C}$, one has

$$H^i(\overline{X}, \mathbb{Q}_\ell) \cong \left(\varprojlim_n H^i_{\mathrm{sing}}(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z}) \right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The construction of $H^i(\overline{X}, \mathbb{Q}_\ell)$ ensures that there is a continuous action of G on it, which yields finite-dimensional ℓ-adic representations of G.

Theorem 1.14. *When X is an abelian variety, we have*

$$H^1(\overline{X}, \mathbb{Q}_\ell) \cong V_\ell(A)^\vee$$

and more generally

$$H^i(\overline{X}, \mathbb{Q}_\ell) \cong \Lambda^i H^1(\overline{A}, \mathbb{Q}_\ell).$$

1.3 About the case $K = \mathbb{Q}$

For the rest of this section we take $K = \mathbb{Q}$. Fix a prime p and embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Choose algebraic closures $\overline{\mathbb{Q}}, \overline{\mathbb{Q}_p}$ in a compatible way:

$$\begin{tikzcd} \overline{\mathbb{Q}} \arrow[r, hook] \arrow[d, dash] & \overline{\mathbb{Q}_p} \arrow[d, dash] \\ \mathbb{Q} \arrow[r, hook] & \mathbb{Q}_p \end{tikzcd}$$

This choice induces an embedding of $G_p := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ in G, given by $g \mapsto g|_{\overline{\mathbb{Q}}}$. If V is an ℓ-adic representation of G, we get ℓ-adic representations of G_p for all p.

1.3.1 Structure of G_p

There is an exact sequence

$$1 \to I_p \to G_p \to \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to 1,$$

where I_p is called the *inertia group*. Furthermore, there is a splitting of inertia as

$$1 \to P \to I_p \to \prod_{\ell \neq p} \mathbb{Z}_\ell \to 1,$$

where $P \triangleleft I_p$ is the unique pro-p-Sylow of I_p (called the *wild inertia* subgroup). Since P is the unique p-Sylow, it is characteristic in I_p, hence normal in G_p. The quotient $\prod_{\ell \neq p} \mathbb{Z}_\ell$ is called the *tame inertia* group.

1.3.2 The action of wild p-inertia on ℓ-adic representations

Let $\ell \neq p$ and let V be an ℓ-adic representation of G_p. Choose a G_p-stable lattice $L \subset V$, from which we get a $\mathbb{Z}_\ell$-representation

$$G_p \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Z}_\ell).$$

For every positive integer r, set

$$N_r := \ker\left(\mathrm{GL}_n(\mathbb{Z}_\ell) \to \mathrm{GL}_n(\mathbb{Z}/\ell^r\mathbb{Z})\right).$$

Note that N_1/N_r is a finite ℓ-group (by induction: N_r/N_{r+1} has a natural structure of $\mathbb{F}_\ell$-vector space). As a consequence, N_1 is a pro-ℓ group, and therefore $\rho(P) \cap N_1 = \{1\}$, because p is different from ℓ (hence there are no non-trivial maps from a pro-p group to a pro-ℓ one). Clearly, this implies that $\rho(P)$ injects into the finite group $\mathrm{GL}_n(\mathbb{F}_\ell)$. So, up to replacing $\mathbb{Q}_p$ by a finite extension, we may assume that P acts trivially. (For example, take the kernel U of $G \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Z}_\ell) \to \mathrm{GL}_n(\mathbb{F}_\ell)$: this is an open subgroup of G, corresponding to a finite extension L of $\mathbb{Q}_p$. The p-inertia of L acts trivially.)

This argument of course breaks down completely for p-adic representations. The main aim of this course is to study p-adic representations of G_p, where the action of I_p is in fact very rich.

1.3.3 Examples

Elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve. Suppose that E has good reduction at ℓ (in elementary terms, this means that there is an equation for $E/\mathbb{Q}$ that has integral coefficients and remains non-singular after reduction modulo ℓ). Denote by $\overline{E}$ the reduction of E modulo ℓ. Take $V = V_\ell(E)$: then I_p acts trivially on V for all $\ell \neq p$. This can be proved as follows: it is not hard to show that the reduction map

$$E[\ell^h] \to \overline{E}(\overline{\mathbb{F}_p})$$

is injective. This map is also clearly Galois-equivariant. Moreover, by definition, I_p acts trivially on $\overline{E}(\overline{\mathbb{F}_p})$, so I_p acts trivially on $E[\ell^h]$ for all h, as claimed.

In fact, we have the following famous result:

Theorem 1.15 (Néron-Ogg-Shafarevich)**.** *Let A be an abelian variety over $\mathbb{Q}$. Then A has good reduction at p if and only if I_p acts trivially on $V_\ell(A)$ for some prime $\ell \neq p$ (equivalently, for all primes $\ell \neq p$).*

It is easy to see that A has good reduction for all but finitely many primes (by general principles, the smooth morphism $A \to \mathrm{Spec}(\mathbb{Q})$ extends to a smooth morphism $\mathcal{A} \to \mathrm{Spec}\,\mathbb{Z}[1/N]$ for some N, and any prime not dividing N is then a prime of good reduction). This begs the question: can there be a condition at $\ell = p$ that detects good reduction?

Representations coming from geometry. Let V be an ℓ-adic representation 'coming from geometry', e.g., étale cohomology groups of varieties. (We will later give a precise definition of 'coming from geometry'.)

Theorem 1.16 (Grothendieck's monodromy theorem)**.** *Let $\ell \neq p$. There is an open subgroup U of I_p that acts unipotently on V (that is, every element in $\rho(U)$ is of the form $\mathrm{Id} + N$, where N is nilpotent).*

Again, this begs the question: what about $\ell = p$?

1.4 What is this class about?

Plan of the course:

(I) Fontaine's classification of p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ via (φ, Γ)-modules. This has many applications, for example to the p-adic Langlands programme, or to the construction of the Emerton-Gee stack, a moduli space of deformations of p-adic representations (that are not studied directly, but via their (φ, Γ)-modules).

(II) Representations coming from geometry & Fontaine's rings. In particular, we will define the properties that correspond to 'good reduction' and 'unipotent action up to finite index' for p-adic representations.

(III) The Fargues-Fontaine curve. This is a geometric object related to p-adic Galois representations.

Literature.

- Fontaine-Ouyang: Theory of p-adic representations. Available at https://www.imo.universite-paris-saclay.fr/~fontaine/galoisrep.pdf

- Brinon-Conrad: CMI Summer School on p-adic Hodge theory. Available at

https://math.stanford.edu/~conrad/papers/notes.pdf

1.5 Classifications of mod-p representations of fields of characteristic $p > 0$

Definition 1.17. Let E be a field of characteristic $p > 0$. A φ-module over E is an E-vector space M together with a map $\varphi : M \to M$ that is semi-linear with respect to the absolute Frobenius of E, that is, the map

$$\begin{array}{rccc} \sigma : & E & \to & E \\ & x & \mapsto & x^p. \end{array}$$

Here, *semi-linear* means that φ satisfies

$$\varphi(\lambda m) = \sigma(\lambda)\varphi(m), \quad \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \quad \forall \lambda \in E, m, m_1, m_2 \in M.$$

Notation 1.18. *If M is an E-vector space, we define $\sigma^* M$ to be $E \otimes_{E,\sigma} M$, where the left factor E is an E-module via the map σ. Explicitly, in $\sigma^* M$ we have*

$$\lambda \otimes \mu m = \lambda \mu^p \otimes m = \mu^p(\lambda \otimes m).$$

Definition 1.19. A φ-module M over E is *étale* if $\dim_E M < \infty$ and the natural map

$$\begin{array}{rccc} \Phi : & \sigma^* M & \to & M \\ & \lambda \otimes m & \mapsto & \lambda \varphi(m) \end{array}$$

is an isomorphism.

Remark 1.20. If $e_1, \ldots, e_d$ is an E-basis of M, we can write

$$\varphi(e_i) = \sum_{j=1}^{d} a_{ij} e_j$$

and Φ maps $1 \otimes e_i$ to $\sum_{j=1}^{d} a_{ij} e_j$. The φ-module is étale if and only if Φ is surjective, if and only if the matrix $A = (a_{ij})$ is invertible.

Étale φ-modules over E form a category (the morphisms are E-linear maps compatible with φ).

Lemma 1.21. *This category is abelian.*

Proof. This is a sequence of more or less easy verifications. The only non-trivial point is the following. Let $\rho : M_1 \to M_2$ be a morphism of φ-modules with kernel K and cokernel C. What we have to show is that, if M_1, M_2 are étale, then so are C and K. This follows from a diagram chase in the commutative exact diagram

$$\begin{tikzcd} 0 \arrow[r] & \sigma^* K \arrow[r] \arrow[d, "\Phi_K"'] & \sigma^* M_2 \arrow[r] \arrow[d, "\Phi_1"'] & \sigma^* M_2 \arrow[r] \arrow[d, "\Phi_2"'] & \sigma^* C \arrow[r] \arrow[d, "\Phi_C"'] & 0 \\ 0 \arrow[r] & K \arrow[r] & M_2 \arrow[r] & M_2 \arrow[r] & C \arrow[r] & 0. \end{tikzcd}$$

Precisely, one gets $\ker(\Phi_K) = \operatorname{coker}(\Phi_C) = 0$, and since we are dealing with finite-dimensional vector spaces (and spaces that are aligned vertically have the same dimension over E) this implies that Φ_K, Φ_C are isomorphisms. $\square$

Remark 1.22. The category of φ-modules is even an abelian tensor category, and in fact a neutral Tannakian category.

1.5.1 Key construction: associating a φ-module to a Galois representation

Let $G = \mathrm{Gal}(E^s/E)$ and let V be a finite-dimensional $\mathbb{F}_p$-vector space with a continuous G-action. Note that the topology on the finite set V is the discrete one. Define

$$D_E(V) := \left(E^s \otimes_{\mathbb{F}_p} V\right)^G,$$

where G acts on $E^s \otimes_{\mathbb{F}_p} V$ via

$$g(\lambda \otimes v) = g(\lambda) \otimes g(v) \quad \forall g \in G, \lambda \in E^s, v \in V.$$

The E-vector space $D_E(V)$ is a φ-module via

$$\varphi(\lambda \otimes v) := \lambda^p \otimes v.$$

Remark 1.23. Note that the φ-module structure is well-defined: if $\lambda \otimes v \in E^s \otimes_{\mathbb{F}_p} V$ is fixed by all $g \in G$, then for all $g \in G$ we have

$$g(\varphi(\lambda \otimes v)) = g(\lambda^p \otimes v) = g(\lambda^p) \otimes g(v) = g(\lambda)^p \otimes g(v) = \varphi(g(\lambda \otimes v)) = \varphi(\lambda \otimes v),$$

hence $\varphi(\lambda \otimes v)$ is also in $(E^s \otimes_{\mathbb{F}_p} V)^G = D_E(V)$.

Lemma 1.24. *$D_E(V)$ is an étale φ-module.*

Proof. We postpone until next time the proof that $\dim_E D_E(V)$ is is finite; in fact, $\dim_E D_E(V) = \dim_{\mathbb{F}_p}(V)$. This will be an immediate consequence of Galois descent, see Remark 2.2.

Let $v_1, \ldots, v_d$ be an $\mathbb{F}_p$-basis of V and let $e_1, \ldots, e_d$ be an E-basis of $D_E(V)$. Write

$$e_i = \sum_{j=1}^{d} b_{ij} \otimes v_j, \quad b_{ij} \in E^s.$$

Let $B = (b_{ij}) \in \mathrm{GL}_d(E^s)$. We have

$$\varphi(e_i) = \sum_{j=1}^{d} b_{ij}^p \otimes v_j = \sum_{j=1}^{d} a_{ij} e_j,$$

where $A = (a_{ij})$ is the matrix of Remark 1.20. It follows from these formulas that $A = B^{-1}\varphi(B)$. In particular, we have

$$\det(A) = \det(B)^{-1} \det(\varphi(B)) = \det(B)^{p-1} \neq 0,$$

hence $\det(A) \neq 0$ and therefore $D_E(V)$ is an étale φ-module by Remark 1.20. $\square$

Our first objective is to prove the following classification result for continuous G-representations with values in $\mathbb{F}_p$-vector spaces:

Theorem 1.25 (Katz, Fontaine)**.** *The map*

$$V \mapsto D_E(V)$$

induces an equivalence of categories

$$\left\{\begin{array}{c} \textit{finite-dimensional } \mathbb{F}_p\textit{-vector} \\ \textit{spaces with continuous} \\ G\textit{-action} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \textit{étale } \varphi\textit{-modules} \\ \textit{over } E \end{array}\right\}.$$

2 25.01.2024

2.1 Recap

Let E be a field of characteristic $p > 0$ and V be a finite-dimensional $\mathbb{F}_p$-vector space equipped with a continuous action of $G := \mathrm{Gal}(E^s/E)$. We introduced a functor

$$D_E(V) := (E^s \otimes_{\mathbb{F}_p} V)^G,$$

where the invariants are taken for the diagonal action

$$g \cdot (\lambda \otimes v) = g(\lambda) \otimes g(v).$$

It is a φ-module via

$$\varphi(\lambda \otimes v) = \lambda^p \otimes v.$$

We have seen (Lemma 1.24) that this φ-module is étale, that is, $\sigma^* D_E(V) \xrightarrow{\sim} D_E(V)$, where

$$\sigma^* M := E \otimes_{\sigma, E} M.$$

We aim to show Theorem 1.25. We note that the quasi-inverse of the functor D_E will be given by

$$V_E(M) := \{y \in E^s \otimes_E M : \varphi(y) = y\} =: (E^s \otimes_E M)^{\varphi=1},$$

where the φ-action on $E^s \otimes_E M$ is $\varphi(\lambda \otimes m) = \lambda^p \otimes \varphi(m)$, and the G-action on $V_E(M)$ is

$$g(\lambda \otimes m) = g(\lambda) \otimes m.$$

2.2 Descent lemmas

Lemma 2.1 (Galois descent, Speiser)**.** *Let K/k be a Galois extension of fields with group G. Let W be a K-vector space with a continuous semi-linear G-action, that is,*

$$\sigma(\lambda \cdot v) = \sigma(\lambda) \cdot \sigma(v) \quad \forall \lambda \in K, v \in V, \sigma \in G.$$

The natural map

$$W^G \otimes_k K \xrightarrow{\sim} W$$

is an isomorphism

Remark 2.2. This proves in particular that $D_E(V)$ is finite-dimensional and that its dimension over E is equal to the $\mathbb{F}_p$-dimension of V.

Lemma 2.3 (Katz). *Let E^s be a separably closed field of characteristic $p > 0$ and let M be an étale φ-module over E^s. The natural map*

$$M^{\varphi=1} \otimes_{\mathbb{F}_p} E^s \xrightarrow{\sim} M$$

Lemmas 2.1 and 2.3 imply Theorem 1.25. The modules $D_E(V), V_E(M)$ are finite-dimensional by Lemmas 2.1 and 2.3. Moreover,

$$V_E(D_E(V)) = \left(\left(E^s \otimes_{\mathbb{F}_p} V\right)^G \otimes_E E^s\right)^{\varphi=1}.$$

By Lemma 2.1, $\left(E^s \otimes_{\mathbb{F}_p} V\right)^G \otimes_E E^s$ is isomorphic to $E^s \otimes_{\mathbb{F}_p} V$, and by definition of the ϕ-action, the fixed points of ϕ in this vector space are exactly $1 \otimes V \cong V$. Finally,

$$D_E(V_E(M)) = \left((E^s \otimes_E M)^{\varphi=1} \otimes_E E^s\right)^G,$$

and using Lemma 2.3 we have $(E^s \otimes_E M)^{\varphi=1} \otimes_{\mathbb{F}_p} E^s \cong E^s \otimes_E M$. Taking G-invariants (and recalling that G only acts on the left) we get back M. $\square$

Exercise 2.4. *Complete the proof by checking that the natural map in the statement of Lemma 2.3 is an isomorphism of étale φ-modules (and not just an isomorphism of vector spaces).*

We now prove Lemmas 2.1 and 2.3. We start by recalling the following classical fact:

Lemma 2.5 (Dedekind). *If G is the Galois group of a finite extension K/k, the elements of G are linearly independent in the K-vector space of functions $K \to K$.*

Proof of Lemma 2.1. If K/k is infinite, choose a basis $\mathcal{B}$ of W over K. Since W is finite-dimensional, there is a normal open subgroup U in G fixing $\mathcal{B}$ element-wise (this follows from the fact that the action is continuous: the stabiliser of each basis element is an open subgroup; if H is the intersection of these stabilisers, then clearly H is open, hence has finite index, and U can be taken to be the intersection of the finitely many conjugates of H). Clearly $W^U \otimes_{K^U} K \xrightarrow{\sim} W$, because W^U contains $\mathcal{B}$, and K-linear combinations of elements of $\mathcal{B}$ span W. Moreover,

$$W^G \otimes_k K \cong \left((W^U)^{G/U} \otimes_k K^U\right) \otimes_{K^U} K:$$

this formula shows that the special case of the lemma when K/k is finite implies the general case. Indeed, K^U/K is finite; if we have the lemma in this case, then

$$\left((W^U)^{G/U} \otimes_k K^U\right) \otimes_{K^U} K \cong \left(W^U\right) \otimes_{K^U} K \cong W.$$

Hence, we can assume that K/k is a finite extension and that G is a finite group. Consider the map

$$W^G \otimes_k K \to W.$$

Surjectivity. It suffices to show that every linear map $\varphi : W \to K$ such that $\varphi|_{W^G \otimes_k K} = 0$ is the zero map. Let $\sigma_1, \ldots, \sigma_n$ be the elements of G and fix $w \in W$. For $x \in K$, consider $w_x := \sum_i \sigma_i(x)\sigma_i(w) \in W^G$. By assumption, $\varphi(w_x) = 0$, because w_x vanishes on the G-invariants and w_x is invariant by construction. On the other hand, by linearity,

$$0 = \varphi(w_x) = \sum_i \sigma_i(x)\varphi(\sigma_i(w)) \quad \forall x \in K,$$

hence by Lemma 2.5 we obtain $\varphi(\sigma_i(w)) = 0$ for all i. In particular, for $\sigma_i = \mathrm{id}$ we get $\varphi(w) = 0$, as desired (recall that w was arbitrary, so we have shown that φ is the zero map).

Injectivity. Consider an element $w_1 \otimes b_1 + \cdots + w_r \otimes b_r \in \left(W^G \otimes_k K\right) \setminus \{0\}$, where $w_i \in W^G$ and $b_i \in K$ for all i. Assume by contradiction that its image in W is zero, that is,

$$\sum b_i w_i = 0.$$

We may assume that r is minimal, hence in particular the w_i are linearly independent over k. By rescaling, we can also assume $b_1 = 1$. Since the w_i are linearly independent over k, it follows that one of the b_i with $i > 1$ is not in k. Without loss of generality, assume $b_2 \notin k$. There exists $\sigma \in G$ such that $\sigma(b_2) \neq b_2$. The element

$$\sigma\left(w_1 \otimes b_1 + \cdots + w_r \otimes b_r\right) - \left(w_1 \otimes b_1 + \cdots + w_r \otimes b_r\right)$$

is in the kernel and admits a representation with a smaller r, contradiction. Indeed, note that

$$\sigma\left(w_1 \otimes 1 + \cdots + w_r \otimes b_r\right) = w_1 \otimes 1 + w_2 \otimes \sigma(b_2) + \cdots + w_r \otimes \sigma(b_r)$$

since $b_1 = 1$ and $w_i \in W^G$ for all i, so on taking the difference we obtain

$$\sigma\left(w_1 \otimes 1 + \cdots + w_r \otimes b_r\right) - \left(w_1 \otimes b_1 + \cdots + w_r \otimes b_r\right) = \sum_{i=2}^{r} w_i \otimes (b_i - \sigma(b_i)).$$

□

We now give two proofs of Lemma 2.3. One is Katz's original proof: it is short, but needs a theorem on algebraic groups. The other relies on a more elementary linear-algebraic argument.

Proof of Lemma 2.3, version 1 (Katz). Let $e_1, \ldots, e_m$ be a basis of M. We wish to find $g \in \mathrm{GL}_n(E^s)$ such that

$$g(e_1), \ldots, g(e_n)$$

is φ-invariant, that is,

$$\varphi(g(e_i)) = g(e_i) \Leftrightarrow \sigma(g)\varphi(e_i) = g(e_i) \Leftrightarrow \sigma(g)Ae_i = g(e_i),$$

where A is the matrix of φ with respect to the basis $\{e_1, \ldots, e_n\}$ (note that φ is only a linear map on $\sigma^* M$). Thus, we need an element $g \in \mathrm{GL}_n(E^s)$ such that

$$\sigma(g^{-1})g = A \in \mathrm{GL}_n(E^s).$$

Lang's isogeny theorem gives that, if G is any connected algebraic group over a finite field $\mathbb{F}$, the map

$$g \mapsto \sigma(g^{-1})g$$

is surjective (with finite kernel). This implies the claim. □

Proof of Lemma 2.3, version 2 (Schneider). We begin with the following fact:
Claim. We have

$$0 < \dim_{\mathbb{F}_p} M^{\varphi=1} \leq \dim_{E^s} M.$$

To prove the claim, we start with the second inequality. Suppose that $m_1, \dots, m_r \in M^{\varphi=1}$ are linearly independent over $\mathbb{F}_p$, but not over E^s. We may assume that r is minimal. Assume for instance

$$m_1 = \sum_{i=2}^{r} \alpha_i m_i, \quad \alpha_i \in E^s.$$

By definition, every m_i is φ-invariant, so

$$m_1 = \varphi(m_1) = \sum_{i=2}^{r} \varphi(\alpha_i m_i) = \sum_{i=2}^{r} \alpha_i^p m_i \Rightarrow \sum_{i=2}^{r} (\alpha_i^p - \alpha_i)\, m_i = 0.$$

By minimality of r, this gives $\alpha_i^p = \alpha_i$, hence $\alpha_i \in \mathbb{F}_p$ for all $i > 1$. This contradicts the linear independence over $\mathbb{F}_p$ and establish the desired inequality (the $\mathbb{F}_p$-dimension of invariants does not exceed the E^s-dimension of invariants, which certainly does not exceed the E^s-dimension of M).

We now show that there exists at least one nontrivial φ-invariant vector. Fix $m \in M \setminus \{0\}$ and let r be minimal such that

$$m, \varphi(m), \dots, \varphi^r(m)$$

are linearly dependent. We have a relation

$$\varphi^r(m) = \sum_{i=0}^{r-1} \alpha_i \varphi^i(m),$$

and by minimality the α_i are unique. Since M is étale, independence of $m, \dots, \varphi^{r-1}(m)$ implies independence of $\varphi(m), \varphi^2(m), \dots, \varphi^r(m)$, which implies that $\alpha_0 \neq 0$. We look for an element $m' \in M^{\varphi=1}$ in the form

$$m' = \sum_{i=0}^{r-1} \lambda_i \varphi^i(m)$$

for some choice of $\lambda_i \in E^s$ to be determined. We try to impose

$$0 = m' - \varphi(m') = \sum_{i=0}^{r} \left(\lambda_i - \lambda_{i-1}^p\right) \varphi^i(m)$$

with $\lambda_{-1} = \lambda_r = 0$. Uniqueness of the α_i implies that we must choose $\lambda_i - \lambda_{i-1}^p = \lambda \alpha_i$ for a fixed $\lambda \in E^s$ (independent of i). Clearly this equation determines λ_i from λ (starting from $\lambda_{-1} = 0$), and gives

$$\lambda_r = \alpha_0^{p^r} \lambda^{p^r} + \alpha_1^{p^{r-1}} \lambda^{p^{r-1}} + \dots + \alpha_r \lambda.$$

This quantity should be zero. Consider the polynomial

$$f = \alpha_0^{p^r} x^{p^r} + \alpha_1^{p^{r-1}} x^{p^{r-1}} + \dots + \alpha_r x \in E^s[x].$$

The parameter λ we are trying to choose should be a root of this polynomial. The polynomial f is separable, because its derivative is $\alpha_r = -1$; it follows that f has roots in E^s. Taking any such root as λ completes the proof of the claim.

We now show that the claim implies the lemma. We proceed by induction on $d = \dim_{E^s} M$. For $d = 1$, the Claim gives $\dim_{\mathbb{F}_p} M^{\varphi=1} = 1$ and we are done: any nonzero element in $M^{\varphi=1}$ is an $\mathbb{F}_p$-basis for $M^{\varphi=1}$, hence an E^s-basis for M. For the inductive step, suppose $d > 1$. Choose $m_1 \in M^{\varphi=1} \setminus \{0\}$ (such an element exists by the Claim). Denote by $\overline{M}$ the quotient $M/\langle m_1 \rangle$: this inherits a φ-modules structure since m_1 is φ-invariant, and this φ-module structure is étale (count dimensions). By induction, $\overline{M}^{\varphi=1}$ has an $\mathbb{F}_p$-basis $\overline{m_2}, \ldots, \overline{m_d}$. Choose representatives $m_2', \ldots, m_d' \in M$ of $\overline{m_2}, \ldots, \overline{m_d}$. These lifts are not necessarily φ-invariants, but $\varphi(m_i') - m_i'$ is of the form $\alpha_i m_1$. For every i, the polynomial

$$y^p - y + \alpha_i$$

is separable, hence has a root λ_i in E^s. Finally, we set

$$m_i = m_i' + \lambda_i m_1 :$$

we then have

$$\varphi(m_i) = \varphi(m_i') + \lambda_i^p m_1 = m_i' + (\alpha_i + \lambda_i^p) m_1 = m_i' + \lambda_i m_1 = m_i.$$

The elements $m_1, \ldots, m_d$ thus form a basis of $M^{\varphi=1}$. □

2.3 Continuous representations of G on finitely-generated $\mathbb{Z}_p$-modules

Let E be a field of characteristic p. We fix a Cohen ring $\mathcal{O}_{\mathcal{E}}$ with residue field E and call $\mathcal{E}$ the fraction field of $\mathcal{O}_{\mathcal{E}}$. This means in particular that $\mathcal{O}_{\mathcal{E}}$ is a complete DVR of characteristic 0 with maximal ideal (p) and residue field E.

Remark 2.6. If E is perfect, $\mathcal{O}_{\mathcal{E}}$ is unique and is the ring of Witt vectors. In general, if E is an arbitrary field of characteristic p, the ring $\mathcal{O}_{\mathcal{E}}$ exists and is unique, but not up to *unique* isomorphism.

The endomorphism

$$\begin{array}{rccc} \sigma : & E & \to & E \\ & x & \mapsto & x^p \end{array}$$

lifts (non-uniquely) to $\varphi : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ (e.g., because $\mathcal{O}_{\mathcal{E}}$ is formally smooth over $\mathbb{Z}_p$, or because it is not very hard to construct φ by hand). We fix choices of $\mathcal{O}_{\mathcal{E}}$ and φ.

Definition 2.7. A φ-module M over $\mathcal{O}_{\mathcal{E}}$ is an $\mathcal{O}_{\mathcal{E}}$-module equipped with a map $\varphi : M \to M$ which is semi-linear with respect to $\varphi : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$. It is étale if it is finitely generated and

$$\Phi : \varphi^* M \to M$$

is an isomorphism, where $\varphi^* M := \mathcal{O}_{\mathcal{E}} \otimes_{\varphi, \mathcal{O}_{\mathcal{E}}} M$.

Remark 2.8. Note that M is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$ if and only if M/pM is an étale φ-module over $\mathcal{O}_{\mathcal{E}}/p\mathcal{O}_{\mathcal{E}} \cong E$ (Nakayama's lemma). This implies that étale φ-modules over E are the same as étale φ-modules over $\mathcal{O}_{\mathcal{E}}$ that are killed by p.

We now look for an analogue of E^s in the context of $\mathcal{O}_{\mathcal{E}}$-modules. We fix compatible separable closures $\mathcal{E}^s$ of $\mathcal{E}$ and E^s of E. Inside $\mathcal{E}^s$ we consider the maximal unramified extension of $\mathcal{O}_{\mathcal{E}}$. Its completion $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$ is a Cohen ring with residue field E^s. The map $\varphi : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ extends uniquely to $\varphi : \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$ (this can be checked by hand, but also follows from the fact that the maximal unramified extension is ind-étale over $\mathcal{O}_{\mathcal{E}}$ and is dense in its completion $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$). Let $\widehat{\mathcal{E}^{\mathrm{nr}}}$ be the fraction field of $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$. We have analogues of the descent lemmas from the previous section:

Lemma 2.9. *Let N be a finitely-generated $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$-module with a semi-linear G-action (where $G := \mathrm{Gal}(E^s/E)$). The natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N^G \xrightarrow{\sim} N.$$

is an isomorphism.

Lemma 2.10. *Let M be an étale φ-module over $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$. The natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathbb{Z}_p} M^{\varphi=1} \xrightarrow{\sim} M$$

is an isomorphism.

Remark 2.11. The key point here is that $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$ is faithfully flat over $\mathcal{O}_{\mathcal{E}}$ (both the maximal unramified extension and the completion are). Lemmas 2.9 and 2.10 imply in particular

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}^{G} = \mathcal{O}_{\mathcal{E}}, \quad \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}^{\varphi=1} = \mathbb{Z}_p$$

and that N^G and $M^{\varphi=1}$ are finitely generated, respectively over $\mathcal{O}_{\mathcal{E}}$ and over $\mathbb{Z}_p$. (If there is a surjective morphism $R^n \to M$ after a finite flat extension, there was already a surjective morphism from a free module before the extension: this follows since the cokernel is zero after tensoring by the flat extension if and only if it was zero to begin with.)

Proof of Lemma 2.9. In the light of Remark 2.8, if N is killed by p, the statement reduces to Lemma 2.1. Now suppose that N is killed by p^n for some n. Consider the exact sequence

$$0 \to N[p] \to N \to N/N[p] \to 0, \tag{1}$$

where $N[p]$ is the p-torsion submodule of N. Taking Galois cohomology,

$$0 \to N[p]^G \to N^G \to (N/N[p])^G \to H^1(G, N[p]) = (0),$$

where the final vanishing comes from the fact that $N[p] \cong (E^s)^r$ for some r (in turn, this follows from the fact that $N[p]$ has a G-invariant basis by Lemma 2.1: any E^s-vector space with a G-invariant basis is isomorphic to $(E^s)^r$ as a G-module).

Tensoring (1) by $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$ (which is flat over $\mathcal{O}_{\mathcal{E}}$) we get

$$0 \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N[p] \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N/N[p] \to 0.$$

This can be completed to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N[p] & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N/N[p] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N[p] & \longrightarrow & N & \longrightarrow & N/N[p] & \longrightarrow & 0 \end{array}$$

where the first vertical arrow is an isomorphism by Lemma 2.1 and the last one is an isomorphism by induction on n. The middle one is therefore also an isomorphism, and we are done. $\square$

[[I couldn't understand the proof of the next lemma any more, so I came up with a slight variant. Please double check.]]

Proof of Lemma 2.10. We begin with the case of finitely generated torsion modules M. We establish this case by reduction to the case $M = M[p]$, which is Lemma 2.3. We need to check that

$$0 \to M[p]^{\varphi=1} \to M^{\varphi=1} \to (M/M[p])^{\varphi=1} \to 0$$

is exact, at which point the proof works as in Lemma 2.9. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & M[p] \arrow[r] \arrow[d, "\varphi-1"'] & M \arrow[r] \arrow[d, "\varphi-1"'] & M/M[p] \arrow[r] \arrow[d, "\varphi-1"'] & 0 \\ 0 \arrow[r] & M[p] \arrow[r] & M \arrow[r] & M/M[p] \arrow[r] & 0. \end{tikzcd} \tag{2}$$

The snake lemma gives

$$0 \to M[p]^{\varphi=1} \to M^{\varphi=1} \to (M/M[p])^{\varphi=1} \to \operatorname{coker}\left(M[p] \xrightarrow{\varphi-1} M[p]\right),$$

so it suffices to show that the first vertical arrow in (2) is surjective, that is, $M[p] = (\varphi - 1)^{-1}M[p]$. Again we have $M[p] \cong (E^s)^r$ as a φ-module over E^s (use Lemma 2.3 to find an invariant basis), and $E^s = (\varphi - 1)E^s$ because for all $a \in E^s$ the polynomial $y^p - y + a$ is separable, hence has a root.

Finally, by passing to the inverse limit over quotients M/p^nM, we obtain the lemma for arbitrary finitely-generated modules M. $\square$

Now let N be a finitely-generated $\mathbb{Z}_p$-module with a continuous action of G. We define

$$D_{\mathcal{E}}(N) := \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathbb{Z}_p} N\right)^G,$$

where the G-action on the tensor product is

$$g(\lambda \otimes n) = g(\lambda) \otimes g(n).$$

This is a φ-module via $\varphi(\lambda \otimes n) = \varphi(\lambda) \otimes n$.

Lemma 2.12. *The φ-module $D_{\mathcal{E}}(N)$ is étale.*

Proof. It is finitely generated by Lemma 2.3. To prove

$$\varphi^* D_{\mathcal{E}}(N) \xrightarrow{\sim} D_{\mathcal{E}}(N)$$

we may tensor with $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$ (which is faithfully flat). So we need to check that

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D_{\mathcal{E}}(N) \cong \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathbb{Z}_p} N$$

is étale over $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}}$, which can be checked modulo p. This is the content of Lemma 1.24. $\square$

Theorem 2.13. *The map $N \mapsto D_{\mathcal{E}}(N)$ induces an equivalence of categories*

$$\left\{ \begin{array}{c} \textit{finite-dimensional } \mathbb{Z}_p\textit{-modules} \\ \textit{with continuous } G\textit{-action} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{étale } \varphi\textit{-modules} \\ \textit{over } \mathcal{O}_{\mathcal{E}} \end{array} \right\}.$$

A quasi-inverse is given by

$$V_{\mathcal{E}}(M) := \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M\right)^{\varphi=1}.$$

Proof. Same as Theorem 1.25, replacing Lemmas 2.1 and 2.3 with Lemmas 2.9 and 2.10. ☐

2.4 $\mathbb{Q}_p$-representations

Recall that every finite-dimensional continuous representation V of G over $\mathbb{Q}_p$ contains a G-invariant $\mathbb{Z}_p$-lattice N (Lemma 1.5).

Definition 2.14. A φ-module over $\mathcal{E} = \mathrm{Frac}(\mathcal{O}_{\mathcal{E}})$ is an $\mathcal{E}$-vector space with a semi-linear action. It is étale if it contains a φ-stable $\mathcal{O}_{\mathcal{E}}$-lattice that is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$.

Corollary 2.15. *The functor*

$$V \mapsto D_{\mathcal{E}}(V) := \left(\widehat{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathbb{Q}_p} V\right)^G$$

induces an equivalence of categories

$$\left\{ \begin{array}{c} \textit{finite-dimensional } \mathbb{Q}_p\textit{-vector} \\ \textit{spaces with continuous} \\ G\textit{-action} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{étale } \varphi\textit{-modules} \\ \textit{over } \mathcal{E} \end{array} \right\}.$$

Proof. Follows from Theorem 2.13 after inverting p (recall that a p-adic representation automatically admits a stable lattice, while we are imposing the existence of a stable lattice on the side of φ-modules). ☐

3 01.02.2024 – Perfectoid fields and the tilting correspondence

In the previous lecture we have classified (in terms of φ-modules) the representations of the absolute Galois group of a field of characteristic p. We now develop some of the language of perfectoid fields, which will allow us to transfer these results to the case of local fields of characteristic zero.

Definition 3.1. An $\mathbb{F}_p$-algebra R is **perfect** if the map $R \to R$ given by $x \mapsto x^p$ is an isomorphism.

Example 3.2. The ring $R = \mathbb{F}_p[x^{1/p^\infty}] = \bigcup_n \mathbb{F}_p[x^{1/p^n}]$ is the free perfect $\mathbb{F}_p$-algebra on one generator.

Definition 3.3. A **strict p-ring** is a p-adically complete ring A such that p is not a zero-divisor in A and $A/(p)$ is perfect.

Example 3.4. 1. $\mathbb{Z}_p$ is a strict p-ring with $\mathbb{Z}_p/(p) \cong \mathbb{F}_p$.

2. The p-adic completion of $\mathbb{Z}[p^{1/p^\infty}]$ is a strict p-ring A such that $A/(p) \cong \mathbb{F}_p[x^{1/p^\infty}]$.

Fact 3.5. The functor $A \mapsto A/(p)$ induces an equivalence of categories

$$\{\text{strict } p\text{-rings}\} \longleftrightarrow \{\text{perfect } \mathbb{F}_p\text{-algebras}\}.$$

A quasi-inverse sends R to the ring of Witt vectors over R.

Remark 3.6. If A is a strict p-ring, the canonical projection $A \to A/(p)$ has a unique multiplicative retraction

$$\rho : A/(p) \to A,$$

called the **Teichmüller lift**.

Idea of the construction. Given $\overline{a} \in A/(p)$, we obtain $\rho(a)$ as follows: take elements $b_n \in A$ such that $b_n^{p^n} \equiv \overline{a} \pmod p$ and define $\rho(a) = \lim_{n\to\infty} b_n^{p^n}$.

More generally, let B be a p-adically complete ring, R be perfect, and $\overline{\varphi} : R \to B/(p)$ be a ring map. There exists a unique multiplicative map $\varphi : R \to B$ lifting $\overline{\varphi}$. This implies that there exists a unique ring map $W(R) \to B$ lifting $\overline{\varphi}$. The definition of this latter map is

$$\sum_i [r_i]p^i \mapsto \sum_i \varphi([r_i])p^i.$$

Definition 3.7. Let B be a p-adically complete ring. The **tilt** of B is

$$B^\flat := \varprojlim_{x \mapsto x^p} B/(p).$$

Thus, an element of $B^\flat$ is a sequence $(b_0, b_1, \ldots)$ with $b_i = b_{i+1}^p$. This is a perfect $\mathbb{F}_p$-algebra.

Remark 3.8. Remark 3.6 implies that for every perfect $\mathbb{F}_p$-algebra R we have

$$\mathrm{Hom}(W(R), B) \xrightarrow{\sim} \mathrm{Hom}(R, B^\flat).$$

Indeed, given $\varphi : R \to B/(p)$, for every $r \in R$ we have a sequence $(r_0 = r, r_1, r_2, \ldots)$ where $r_{i+1}^p = r_i$ (since R is perfect) and we can define a map $R \to B^\flat$ by sending r to $(\varphi(r_0), \varphi(r_1), \varphi(r_2), \ldots)$.

In particular, for $R = B^\flat$, the identity in $\mathrm{Hom}(R, B^\flat)$ corresponds to a unique map $W(B^\flat) \to B$, called the **Fontaine map**.

Definition 3.9. An **analytic field** is a field K, complete with respect to a multiplicative non-archimedean norm $\|\cdot\|$ (explicitly, this means that $\|\cdot\|$ is a function from K to $\mathbb{R}_{\geq 0}$ that satisfies $\|x\| = 0$ iff $x = 0$, $\|x \cdot y\| = \|x\| \cdot \|y\|$ and $\|x + y\| \leq \max(\|x\|, \|y\|)$). We define

$$\mathcal{O}_K = \{x \in K : \|x\| \leq 1\}, \quad M_K = \{x \in K : \|x\| < 1\}.$$

The ring $\mathcal{O}_K$ is local, with maximal ideal M_K. We denote by $\kappa := \mathcal{O}_K/M_K$ the residue field. If $\mathrm{char}(K) = 0$ and $\mathrm{char}(\kappa) = p > 0$, we say that K is of **mixed characteristic**.

Remark 3.10. This definition of analytic field is not standard in the literature.

Remark 3.11. One can show that $\mathcal{O}_K$ is integrally closed. If $\pi \in \mathcal{O}_K$ is such that $\|\pi\| \in (0,1)$, then the ring $\mathcal{O}_K$ is also π-adically complete.

Definition 3.12. An analytic field K is **perfectoid** if

1. the norm group $\|K\| \subset \mathbb{R}_{\geq 0}$ is not discrete;
2. on $\mathcal{O}_K/(p)$ (note that this is not κ), the map $x \mapsto x^p$ is surjective.

Remark 3.13. $\mathbb{F}_p$-algebras for which $x \mapsto x^p$ is surjective (but not necessarily an isomorphism) are sometimes called **semi-perect**.

Example 3.14.
1. $\mathbb{Q}_p$ and its finite extensions are not perfectoid, because their norm groups are discrete.
2. The field $\mathbb{C}_p$ (completion of an algebraic closure of $\mathbb{Q}_p$) is perfectoid.
3. Exercise: in characteristic $p > 0$, an analytic field is perfectoid if and only if it is perfect.
4. $\mathbb{F}_p((x^{1/p^\infty}))$, the field of fractions of $\widehat{\mathbb{F}_p[x^{1/p^\infty}]}$, where $\widehat{\cdot}$ denotes x-adic completion.
5. Key example: $K = \widehat{\mathbb{Q}_p(p^{1/p^\infty})}$, where $\widehat{\cdot}$ is p-adic completion. The ring of integers is
$$\mathcal{O}_K = \widehat{\mathbb{Z}_p[p^{1/p^\infty}]}, \text{ where } \mathbb{Z}_p[p^{1/p^\infty}] = \varinjlim_{x_n \mapsto x_{n+1}^p} \mathbb{Z}_p[x_n]/(x_n^{p^n} - p).$$
The quotient $\mathcal{O}_K/(p)$ is isomorphic to $\varinjlim_{x_n \to x_{n+1}^p} \mathbb{F}_p[x_n]/(x_n^{p^n}) \cong \mathbb{F}_p[x^{1/p^\infty}]/(x)$. Since $\mathbb{F}_p[x^{1/p^\infty}]$ is perfect, its quotient by (x) satisfies condition (2) in the definition of a perfectoid field.
6. $K = \widehat{\mathbb{Q}_p(\omega^{1/p^\infty})}$, where ω is a primitive p-th root of unity and $\widehat{\cdot}$ denotes p-adic completion. Here we have
$$\mathcal{O}_K = \widehat{\mathbb{Z}_p[\omega^{1/p^\infty}]};$$
since $\mathbb{Z}_p[\omega]/(p) \cong \mathbb{F}_p[x]/(x^{p-1})$ (with $x \leftrightarrow (1-\omega)$), one sees that $\widehat{\mathbb{Z}_p[\omega^{1/p^\infty}]}/(p)$ is a quotient of $\mathbb{F}_p[x^{1/p^\infty}]$, so that (2) in the definition of a perfectoid space holds.

3.1 Tilting a perfectoid field

Let K be a perfectoid field of mixed characteristic. Consider
$$\mathcal{O}_K^\flat = \varprojlim_{x \mapsto x^p} \mathcal{O}_K/(p).$$
We have a natural map $\overline{\varphi} : \mathcal{O}_K^\flat \to \mathcal{O}_K/(p)$, given by the projection on the first component of the inverse limit. We then get a multiplicative map $\varphi : \mathcal{O}_K^\flat \to \mathcal{O}_K$, see Remark 3.6. The composition
$$\mathcal{O}_K^\flat \xrightarrow{\varphi} \mathcal{O}_K \xrightarrow{\|\cdot\|} \mathbb{R}_{\geq 0}$$
gives a multiplicative non-archimedean norm $\|\cdot\|_\flat$ on $\mathcal{O}_K^\flat$ (we will check this fact below in Lemma 3.15). We set $K^\flat := \mathrm{Frac}(\mathcal{O}_K^\flat)$. Note that $\mathcal{O}_K^\flat$ is a domain: this is implied by the existence of a multiplicative norm. Indeed, $xy = 0$ implies $\|xy\|_\flat = 0$, hence $\|x\|_\flat = 0$ or $\|y\|_\flat = 0$, so $x = 0$ or $y = 0$.

Lemma 3.15. *The function $\|\cdot\|_\flat$ is a non-archimedean norm.*

Proof. Multiplicativity and the property $\|x\|_\flat = 0$ if and only if $x = 0$ are obvious. We check the non-archimedean triangular inequality. We have

$$\begin{aligned}\|x+y\|_\flat &= \|\lim_{n\to\infty}(x_n+y_n)^{p^n}\| = \lim_{n\to\infty}\|x_n+y_n\|^{p^n} \\ &\leq \max\left(\lim_{n\to\infty}\|x_n\|^{p^n}, \lim_{n\to\infty}\|y_n\|^{p^n}\right) = \max\left(\|x\|_\flat, \|y\|_\flat\right).\end{aligned}$$

□

Theorem 3.16. *Extending $\|\cdot\|_\flat$ multiplicatively to $K^\flat$ defines a perfect analytic field of characteristic $p > 0$ with $\mathcal{O}_{K^\flat} = \mathcal{O}_K^\flat$.*

For the proof of Theorem 3.16 we will need the following lemma.

Lemma 3.17. *The following hold.*

1. *the map $x \mapsto x^p$ is surjective on $\|K\| \subset \mathbb{R}_{\geq 0}$.*
2. *$\|\mathcal{O}_K^\flat\|_\flat = \|\mathcal{O}_K\|$.*

Proof. 1. Since $\|K^\times\|$ is not discrete by assumption, $\|K^\times|\|$ is not $\|p\|^{\mathbb{Z}}$. Hence, $\|K^\times\|$ is multiplicatively generated by the norms of a certain set $S \cup S^{-1}$, where $S = \{y \in K^\times : \|p\| < \|y\| \leq 1\}$. (The key remark is that if y is an element of S that is not a unit, p/y is also in S, and therefore $\|p\|$ lies in the subgroup generated by the norms of the elements in S.)

Fix $y \in S$. As $x \mapsto x^p$ is surjective modulo p, there exists $x \in K^\times$ such that $y - x^p \in p\mathcal{O}_K$. It follows that

$$\|y - x^p\| \leq \|p\|, \text{ but } \|y\| > \|p\|;$$

by the non-archimedean triangular inequality, this is only possible if $\|y\| = \|x^p\| = \|x\|^p$.

2. The inclusion $\|\mathcal{O}_K^\flat\|_\flat \subseteq \|\mathcal{O}_K\|$ is obvious by construction (the norm on $\mathcal{O}_K^\flat$ is induced by the norm on $\mathcal{O}_K$). For the other inclusion, fix $y \in \mathcal{O}_K$. By part (1), there exist $m \in \mathbb{Z}$ and $x \in \mathcal{O}_K$ such that $\|x\|^{p^m} = \|y\|$ and $\|p\| < \|x\| \leq 1$. We now show that $\|x\| \in \|\mathcal{O}_K^\flat\|_\flat$, and therefore $\|y\| \in \|\mathcal{O}_K^\flat\|_\flat$.

Let $\overline{x} = x \bmod (p)$. Since $x \mapsto x^p$ is surjective on $\mathcal{O}_K/(p)$ (by definition of a perfectoid field), we can find an element

$$x^\flat = (\overline{x}, \overline{x_1}, \ldots) \in \mathcal{O}_K^\flat = \varprojlim_{x\mapsto x^p} \mathcal{O}_K/(p).$$

Recall that $\varphi(x^\flat) = \lim_{n\to\infty} x_n^{p^n}$, where x_n lifts $\overline{x_n}$ to $\mathcal{O}_K$. By definition,

$$\|x^\flat\|_\flat = \|\varphi(x^\flat)\|.$$

On the other hand,

$$\|\varphi(x^\flat) - x\| = \|\lim_{n\to\infty} x_n^{p^n} - x\| \leq \lim_{n\to\infty}\|x_n^{p^n} - x\| \leq \|p\|$$

since $x_n^{p^n} \bmod (p) = x \bmod (p)$. As $\|x\| > \|p\|$, a cancellation argument with the non-archimedean triangular inequality gives $\|x_n^{p^n}\| = \|x\|$ for n large enough, and therefore $\|\varphi(x^\flat)\| = \lim_n \|x_n^{p^n}\| = \|x\|$.

□

Proof of Theorem 3.16. We need to check that given $x, y \in K^\flat$ we have

$$\|x+y\|_\flat \leq \max(\|x\|_\flat, \|y\|_\flat).$$

We find $m < 0$ such that $\frac{x}{(q^\flat)^m}, \frac{y}{(q^\flat)^m}$ belong to $\mathcal{O}_K$, where $q \in K^\times$ satisfies $\|p\| < \|q\| \leq 1$ and $q^\flat$ is such that $\|q^\flat\|_\flat = \|q\|$. The rescaled elements $\frac{x}{(q^\flat)^m}, \frac{y}{(q^\flat)^m}$ satisfy the desired inequality by Lemma 3.15, and by rescaling, the original ones do, too. Completeness is easy.

We still have to check that the ring of integers of $K^\flat$ is $\mathcal{O}_K^\flat$ (that is, the tilt of $\mathcal{O}_K$). Take an element $x = y/z$ with $y, z \in \mathcal{O}_K^\flat$. Suppose that x is in the ring of integers of $K^\flat$: then we have

$$\|\varphi(y)\| = \|y\|_\flat \leq \|z\|_\flat = \|\varphi(z)\|.$$

For $n \geq 0$, we let $y_n := y^{1/p^n}$ and $z_n := z^{1/p^n}$. By assumption,

$$\|\varphi(y_0)\| \leq \|\varphi(z_0)\|,$$

and since φ is multiplicative we get $\|\varphi(y_n)\| \leq \|\varphi(z_n)\|$ for all $n \geq 0$. Here $\varphi(y_n), \varphi(z_n)$ are elements in $\mathcal{O}_K$, and the inequality on their norms gives the existence of an element $x_n \in \mathcal{O}_K$ such that

$$\varphi(y_n) = \varphi(z_n)x_n.$$

One checks immediately that $x_{n+1}^p = x_n$, and setting $\overline{x_n} := x_n \bmod (p)$ we get an element $\overline{x} := (\overline{x_0}, \overline{x_1}, \ldots) \in \mathcal{O}_K^\flat$ that satisfies $y = z\overline{x}$. This means that $x = \frac{y}{z} = \overline{x}$ is in $\mathcal{O}_K^\flat$. Since $x \in \mathcal{O}_{K^\flat}$ was arbitrary, this shows the inclusion $\mathcal{O}_{K^\flat} \subseteq \mathcal{O}_K^\flat$.

Conversely, given an element $x \in \mathcal{O}_K^\flat$, the definition shows immediately that

$$\|x\|_\flat = \|\varphi(x)\| \leq 1,$$

and therefore x is in $\mathcal{O}_{K^\flat}$. □

Example 3.18. We describe the tilt of our examples of perfectoid fields.

1. Let $K = \widehat{\mathbb{Q}_p(p^{1/p^\infty})}$. In this case we know that $\mathcal{O}_K/(p) \cong \mathbb{F}_p[x^{1/p^\infty}]/(x)$. By definition, the tilt is

$$\varprojlim_{x \to x^p} \mathbb{F}_p[x^{1/p^\infty}]/(x);$$

by Exercise 3.24 below, this is isomorphic to

$$\varprojlim_{i \to \infty} \mathbb{F}_p[x^{1/p^\infty}]/(x^i) = \mathbb{F}_p\widehat{[x^{1/p^\infty}]}.$$

This implies that $K^\flat$ is $\mathbb{F}_p((x^{1/p^\infty}))$.

2. Let $K = \widehat{\mathbb{Q}_p(\omega^{1/p^\infty})}$. We have seen that

$$\mathbb{Z}_p[\omega^{1/p^\infty}]/(p) \cong \mathbb{F}_p[x^{1/p^\infty}]/(x^{p-1}).$$

Using the fact that $\varprojlim_{x\mapsto x^p} B \cong \varprojlim_{x\mapsto x^p} B/I$ for any ideal I such that $I^p = (0)$, one sees that the tilt is the same as in example (1).

The second example above shows that different perfectoid fields may have the same tilt! However, the next result shows that this phenomenon cannot happen if one restricts to the extensions of a *given* perfectoid field:

Theorem 3.19 (Kedlaya-Liu, Scholze (independently)). *Let K be a perfectoid field. The functor $L \mapsto L^\flat$ induces an equivalence of categories*

$$\{\textit{finite extensions of } K\} \leftrightarrow \{\textit{finite extensions of } K^\flat\}.$$

Remark 3.20. Scholze upgrades this to an equivalence of categories of analytic spaces over K and $K^\flat$.

Corollary 3.21. *There is an isomorphism of absolute Galois groups*

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\sim} \mathrm{Gal}\left(\overline{K^\flat}/K^\flat\right).$$

Proof. For any field F, the category of separable finite extensions E/F is anti-equivalent to the category of finite sets with a continuous transitive action of $\mathrm{Gal}(F^s/F)$. The functor giving the equivalence sends the extension E/F to $\mathrm{Hom}_F(E, F^s)$. Moreover, for every profinite group G the category of finite sets with (transitive) continuous G-action determines G up to isomorphism. The statement follows from these facts and Theorem 3.19. $\square$

Remark 3.22. Corollary 3.21 is originally a theorem of Fontaine and Wintenberger (at least in the cases $K = \widehat{\mathbb{Q}_p(p^{1/p^\infty})}$ and $K = \widehat{\mathbb{Q}_p(\omega^{1/p^\infty})}$).

Remark 3.23. There is no analogue of Corollary 3.21 for the field $K = \mathbb{Q}_p$: there is no field F of characteristic p such that $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \cong \mathrm{Gal}(F^s/F)$. A simple way to see this is that the p-cohomological dimension of $\mathrm{Gal}(F^s/F)$ is ≤ 1, while $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ has p-cohomological dimension ≥ 2, because $H^2(\mathbb{Q}_p, \mu_p) \cong \mathbb{Z}/p\mathbb{Z}$.

Exercise 3.24. *Show that there is an isomorphism*

$$\varprojlim_{x\to x^p} \mathbb{F}_p[x^{1/p^\infty}]/(x) \cong \varprojlim_{i\to\infty} \mathbb{F}_p[x^{1/p^\infty}]/(x^i).$$

Solution 3.25. Elements of the left-hand side are given by collections $(q_j(x))_j$, where each $q_j(x)$ is in $\mathbb{F}_p[x^{1/p^\infty}]/(x)$ and the compatibility condition is

$$q_{j+1}(x^p) = q_j(x) \bmod (x).$$

Elements of the right-hand side are given by collections $(r_i(x))_i$, where each $r_i(x)$ is in $\mathbb{F}_p[x^{1/p^\infty}]/(x^i)$ and the compatibility condition is $r_{i+1}(x) \equiv r_i(x) \pmod{x^i}$. We define explicit homomorphisms in both directions:

1.
$$\begin{array}{rccc} \alpha: & \varprojlim_{x\to x^p} \mathbb{F}_p[x^{1/p^\infty}]/(x) & \cong & \varprojlim_{i\to\infty} \mathbb{F}_p[x^{1/p^\infty}]/(x^i) \\ & (q_j(x)) & \mapsto & (q_i(x^{p^i}) \bmod (x^i))_i. \end{array}$$

Each term $q_i(x^{p^i}) \bmod (x^i)$ is a well-defined element of the quotient $\mathbb{F}_p[x^{1/p^\infty}]/(x^i)$: if $q_i'(x), q_i''(x) \in \mathbb{F}_p[x^{1/p^\infty}]$ are both representatives for $q_i(x) \in \mathbb{F}_p[x^{1/p^\infty}]/(x)$, then $q_i''(x) = q_i'(x) + xs(x)$, hence

$$q_i''(x^{p^i}) = q_i'(x^{p^i}) + x^{p^i}s(x^{p^i}),$$

and $x^{p^i}s(x^{p^i}) = 0 \bmod x^i$ since $p^i \geq i$ for all $i \geq 0$. Moreover, the collection $(q_i(x^{p^i}))_i$ is compatible: using the fact that we are in characteristic p we obtain

$$q_{i+1}(x^{p^{i+1}}) = q_{i+1}(x^p)^{p^i} = (q_i(x) \bmod (x))^{p^i} = q_i(x)^{p^i} \bmod (x^{p^i}) = q_i(x^{p^i}) \bmod (x^{p^i}),$$

and in particular $q_{i+1}(x^{p^{i+1}})$ and $q_i(x^{p^i})$ are congruent modulo x^i. Finally, it is easy to check that α is a ring homomorphism.

2. Conversely, we define

$$\begin{array}{rccc} \beta: & \varprojlim_{i\to\infty} \mathbb{F}_p[x^{1/p^\infty}]/(x^i) & \cong & \varprojlim_{x\to x^p} \mathbb{F}_p[x^{1/p^\infty}]/(x) \\ & (r_i(x))_i & \mapsto & (r_{(j+1)p^j}(x^{1/p^j}) \bmod (x))_j. \end{array}$$

(An easier way to interpret the map β is that we have a formal series $r \in \mathbb{F}_p\widehat{[x^{1/p^\infty}]}$ and we take $q_i(x) = r(x^{1/p^i}) \bmod (x)$.)
Since $r_{(j+1)p^j}(x)$ is well-defined modulo $(x^{(j+1)p^j})$, when evaluating at x^{1/p^j} we get a well-defined element modulo $(x^{(j+1)p^j/p^j})$, and in particular modulo (x). Moreover, the collection $(q_j)_j = (r_{(j+1)p^j}(x^{1/p^j}) \bmod (x))_j$ is compatible. Indeed, using that $r_{(j+2)p^{j+1}}$ is congruent to $r_{(j+1)p^j}$ modulo $x^{(j+1)p^j}$ (so we can fix representatives with $r_{(j+2)p^{j+1}} = r_{(j+1)p^j} + x^{(j+1)p^j}s$ for some $s \in \mathbb{F}_p[x^{1/p^\infty}]$), we obtain

$$\begin{aligned} q_{j+1}(x^p) &= r_{(j+2)p^{j+1}}(x^{p/p^{j+1}}) = r_{(j+2)p^{j+1}}(x^{1/p^j}) \\ &= \left(r_{(j+1)p^j} + x^{(j+1)p^j}s\right)(x^{1/p^j}) = r_{(j+1)p^j}(x^{1/p^j}) + x^{j+1}s(x^{1/p^j}) \\ &= q_j(x) \bmod (x^{(j+1)}), \end{aligned}$$

and in particular the equality holds modulo (x). One checks without difficulty that β is a ring homomorphism.

It now suffices to show that $\alpha \circ \beta$ and $\beta \circ \alpha$ are the identity on their respective domains. This is essentially true by definition: for example,

$$\beta(\alpha((q_j)_j)) = \beta\left((q_i(x^{p^i}))_i\right) = \left(q_{(j+1)p^j}(x^{p^{(j+1)p^j - j}})\right)_j,$$

and using the relation

$$q_{j+t}(x^{p^t}) = q_j(x)$$

with $t = (j+1)p^j - j$ we get

$$q_{(j+1)p^j}(x^{p^{(j+1)p^j - j}}) = q_{j+t}(x^{p^t}) = q_j(x),$$

as desired. Similarly,

$$\alpha(\beta((r_i)_i)) = \alpha\left(\left(r_{(j+1)p^j}(x^{1/p^j})\right)_j\right) = \left(r_{(i+1)p^i}(x)\right)_i = (r_i(x))_i,$$

where the last equality follows from the fact that $r_{(i+1)p^i}(x) \equiv r_i(x) \bmod (x^i)$ since $(i+1)p^i \geq i$.

4 08.02.2024 – The tilting correspondence

We now prove Theorem 3.19, whose statement we reproduce here:

Theorem 4.1. *Let K be a perfectoid field. The functor $L \mapsto L^\flat$ induces an equivalence of categories*

$$\{\textit{finite extensions of } K\} \leftrightarrow \{\textit{finite extensions of } K^\flat\}.$$

Recall the definition of $K^\flat$. Letting as usual $\mathcal{O}_K = \{x \in K : \|x\| \leq 1\}$, we set

$$\mathcal{O}_K^\flat = \varprojlim_{x \mapsto x^p} \mathcal{O}_K/(p).$$

This is a perfect integral domain, and $K^\flat$ is defined as the fraction field of $\mathcal{O}_K^\flat$. We showed (Theorem 3.16) that $K^\flat$ is a perfect (hence perfectoid) field of characteristic $p > 0$. In particular, we introduced a norm on $K^\flat$, defined as follows. The natural map $\mathcal{O}_K^\flat \to \mathcal{O}_K/(p)$ lifts to a multiplicative map $\mathcal{O}_K^\flat \xrightarrow{\varphi} \mathcal{O}_K$, and for $y \in \mathcal{O}_K^\flat$ we defined

$$\|y\|_\flat = \|\varphi(y)\|.$$

We also showed (Lemma 3.17) that $\|\mathcal{O}_K\| = \|\mathcal{O}_K^\flat\|_\flat \subset \mathbb{R}_{\geq 0}$. In particular, we can fix an element $p^\flat \in \mathcal{O}_K^\flat$ with $\|p^\flat\|_\flat = \|p\|$.

Corollary 4.2. *There is a canonical isomorphism $\mathcal{O}_K/(p) \cong \mathcal{O}_K^\flat/(p^\flat)$.*

Proof. The kernel of the natural map $\mathcal{O}_K^\flat \twoheadrightarrow \mathcal{O}_K/(p)$ is $\{a \in \mathcal{O}_K^\flat : \varphi(a) \in p\mathcal{O}_K\}$. We have

$$\{a \in \mathcal{O}_K^\flat : \varphi(a) \in p\mathcal{O}_K\} = \{a \in \mathcal{O}_K^\flat : \|\varphi(a)\| \leq \|p\|\},$$

which by definition is the same as

$$\{a \in \mathcal{O}_K^\flat : \|a\|_\flat \leq \|p^\flat\|_\flat\}.$$

We saw last time (see the proof of Theorem 3.16) that $\|a\|_\flat \leq \|p^\flat\|_\flat$ is equivalent to $a \in (p^\flat)$, which concludes the proof. ☐

4.1 The $\sharp$ functor

Let $E/K^\flat$ be a (finite) field extension.

Remark 4.3. The construction does not need the finiteness assumption, but we will only use this case.

We define

$$\mathcal{O}_E^\sharp := W(\mathcal{O}_E) \otimes_{W(\mathcal{O}_K^\flat)} \mathcal{O}_K$$

and

$$E^\sharp := \mathrm{Frac}(W(\mathcal{O}_E) \otimes_{W(\mathcal{O}_K^\flat)} \mathcal{O}_K),$$

where the map $W(\mathcal{O}_K^\flat) \to \mathcal{O}_K$ is the Fontaine map (that is, the ring map coming from φ via the universal property of the Witt vectors, see Remark 3.8).

Remark 4.4. The ring $W(\mathcal{O}_E) \otimes_{W(\mathcal{O}_K^\flat)} \mathcal{O}_K$ is an integral domain. In any case, for the moment we take Frac to mean the total ring of fractions.

Proposition 4.5. *$E^\sharp$ is a perfectoid field with tilt $(E^\sharp)^\flat = E$.*

Remark 4.6. More generally, this holds for any $E \subset K^\flat$ that is perfectoid. When $E/K^\flat$ is finite, since $K^\flat$ is perfect and complete, then E is automatically perfect (hence perfectoid). On the other hand, note that it is not clear that every finite extension L/K is perfectoid!

The next lemma is fundamental.

Lemma 4.7. *If K is perfectoid, the Fontaine map $\tilde{\varphi} : W(\mathcal{O}_K^\flat) \to \mathcal{O}_K$ is surjective. Its kernel is a principal ideal, generated by an element*

$$\xi = \sum [r_i] p^i,$$

where $\|r_0\|_\flat = \|p\|$ and r_1 is a unit.

Definition 4.8 (Kedlaya)**.** An element ξ as in the lemma is called *primitive*.

Proof of Lemma 4.7.
Surjectivity. Consider $\tilde{\varphi} \bmod (p) : \mathcal{O}_K^\flat \to \mathcal{O}_K/(p)$, which is surjective by Corollary 4.2. Moreover, $\mathcal{O}_K$ is p-adically complete. The claim now follows from the following general fact (a version of Nakayama's lemma). More precisely, we conclude by applying Lemma 4.9 to the image of $\tilde{\varphi}$ and the ideal $I = (p)$.

Lemma 4.9. *Let R be a ring, complete with respect to the topology generated by an ideal I. If the classes of $x_1, \dots, x_r \in R$ in R/I generate it, then $x_1, \dots, x_r$ generate R.*

Kernel. Choose $p^\flat$ with $\|p\| = \|p^\flat\|_\flat = \|\varphi(p^\flat)\|$. By definition, this means $\varphi(p^\flat) = pu$ with $u \in \mathcal{O}_K^\times$. By surjectivity of $\tilde{\varphi}$, there exists $\tilde{u} \in W(\mathcal{O}_K^\flat)$ such that $\tilde{\varphi}(\tilde{u}) = u$. Note that $\tilde{u}$ is a unit, because it is modulo p. Define

$$\xi := [p^\flat] - p\tilde{u} \in W(\mathcal{O}_K^\flat),$$

where $[p^\flat]$ is a Teichmüller lift of $p^\flat$. It is clear that ξ is in the kernel of $\tilde{\varphi}$, because

$$\tilde{\varphi}(\xi) = \tilde{\varphi}([p^\flat]) - p\tilde{\varphi}(\tilde{u}) = \varphi(p^\flat) - pu = 0.$$

Suppose now that b is an element in $\ker \tilde{\varphi}$. Since $\xi \bmod (p) = p^\flat$, and since by Corollary 4.2 the kernel of $\tilde{\varphi} \bmod (p)$ is generated by $p^\flat$, we obtain

$$\ker(\tilde{\varphi}) \subset (\xi, p).$$

Write $b = a_1\xi + b_1 p$, where $a_1, b_1 \in W(\mathcal{O}_K)$. Applying $\tilde{\varphi}$ we get

$$0 = \tilde{\varphi}(b) = \tilde{\varphi}(a_1)\tilde{\varphi}(\xi) + p\tilde{\varphi}(b_1) = p\tilde{\varphi}(b_1).$$

As $\tilde{\varphi}(b_1) \in \mathcal{O}_K$, which is an integral domain, we obtain $\tilde{\varphi}(b_1) = 0$. We can then repeat: write $b_1 = a_2\xi + b_2 p$ and observe that b_2 is also in the kernel. By completeness, this allows us to ultimately write $b = \left(\sum_{i=1}^{\infty} a_i p^{i-1}\right)\xi$, as desired. $\square$

Proof of Proposition 4.5. Let $E/K^\flat$ be a finite extension. It is well-known that $\mathcal{O}_E/\mathcal{O}_{K^\flat}$ is a finite module (finiteness of integral closures). This implies that $W(\mathcal{O}_E)/W(\mathcal{O}_K^\flat)$ is also finite (using that the Witt rings are p-adically complete and Lemma 4.9). It follows that

$$W(\mathcal{O}_E) \otimes_{W(\mathcal{O}_K^\flat)} K$$

is a finite étale K-algebra, hence a product $\prod K_i$ of fields. We will prove later that there is in fact only one field in this product.

Claim 1. $\mathcal{O}_E^\sharp$ is p-adically complete.

To see this, consider the multiplication-by-ξ map

$$\cdot\xi : W(\mathcal{O}_E) \to W(\mathcal{O}_E) :$$

this is injective modulo p, because $W(\mathcal{O}_E)/(p) \cong \mathcal{O}_E$ is an integral domain, and ξ mod $(p) = p^\flat$ is non-zero. By induction on n, multiplication by ξ is injective as a map $W(\mathcal{O}_E)/(p^n) \to W(\mathcal{O}_E)/(p^n)$. More precisely, consider the sequences

$$\begin{tikzcd}
0 \arrow[r] & pW(\mathcal{O}_E)/(p^{n+1}) \arrow[r] \arrow[d, "\cdot\xi"'] & W(\mathcal{O}_E)/(p^{n+1}) \arrow[r] \arrow[d, "\cdot\xi"'] & W(\mathcal{O}_E)/(p) \arrow[r] \arrow[d, "\cdot\xi"'] & 0 \\
0 \arrow[r] & pW(\mathcal{O}_E)/(p^{n+1}) \arrow[r] & W(\mathcal{O}_E)/(p^{n+1}) \arrow[r] & W(\mathcal{O}_E)/(p) \arrow[r] & 0.
\end{tikzcd}$$

The left and right vertical arrows are injective, hence so is the middle one.

Consider now the following sequence, where we can pass to the inverse limit because inverse limits are exact in the context of p-adically complete rings:

$$0 \longrightarrow \varprojlim_n W(\mathcal{O}_E)/(p^n) \xrightarrow{\cdot\xi} \varprojlim_n W(\mathcal{O}_E)/(p^n) \longrightarrow \varprojlim_n W(\mathcal{O}_E)/(\xi, p^n) \to 0 \qquad (3)$$

Note that $\varprojlim_n W(\mathcal{O}_E)/(\xi, p^n)$ is isomorphic to $\varprojlim \mathcal{O}_E^\sharp/(p^n)$ by Lemma 4.7.

The various terms in (3) are isomorphic to $W(\mathcal{O}_E), W(\mathcal{O}_E)$ and $\varprojlim \mathcal{O}_E^\sharp/(p^n)$, hence

$$\mathcal{O}_E^\sharp \cong \operatorname{coker}(\cdot\xi : W(\mathcal{O}_E) \to W(\mathcal{O}_E)) \cong \varprojlim \mathcal{O}_E^\sharp/(p^n).$$

This shows that $\mathcal{O}_E^\sharp$ is p-adically complete. We can now show that $W(\mathcal{O}_E) \otimes_{W(\mathcal{O}_K^\flat)} K$ is a field. If not,

$$\mathcal{O}_E^\sharp \cong R_1 \times \cdots \times R_\ell$$

is a product of p-adically complete rings, hence $\mathcal{O}_E^\sharp/(p)$ has nontrivial idempotents. But $\mathcal{O}_E^\sharp/(p) \cong \mathcal{O}_E/(p^\flat)$, so (by completeness) $\mathcal{O}_E$ would have nontrivial idempotents, which is obviously not the case.

Claim 2. An element $x \in \mathcal{O}_E^\sharp$ satisfies $\|x\| \le \|p\|$ if and only if $x \in p\mathcal{O}_E^\sharp$.

The 'if' part is obvious. For the converse, consider the map

$$\mathcal{O}_E \twoheadrightarrow \mathcal{O}_E^\flat/(p) \cong W(\mathcal{O}_E)/(\xi, p) = \mathcal{O}_E/(\xi \bmod (p)) = \mathcal{O}_E/(p^\flat).$$

By Claim 1 (the p-adic completeness of $\mathcal{O}_E^\flat$), this lifts to $\mathcal{O}_E \xrightarrow{\varphi} \mathcal{O}_E^\sharp$ extending $\mathcal{O}_{K^\flat} \xrightarrow{\varphi} \mathcal{O}_K$. Recall that in proving Claim 1 we have also shown that $\mathcal{O}_E^\sharp$ is isomorphic to $W(\mathcal{O}_E)/(\xi)$. Suppose now that $x \in \mathcal{O}_E^\sharp$ satisfies $\|x\| \le \|p\|$. If x is the class of $a \in W(\mathcal{O}_E)$, we have

$$a = \sum [r_i]p^i \Rightarrow \|x\| = \|\sum \varphi(a_i)p^i\| \le \|p\|$$

by assumption. Thus,

$$\|a_0\|_\flat = \|\varphi(a_0)\| \le \|p\| = \|p^\flat\|_\flat,$$

and therefore $a_0 = p^\flat b_0$ for some $b_0 \in \mathcal{O}_E$. Now lift b_0 to some $b \in W(\mathcal{O}_E)$. Then

$$a - \xi b \bmod (p) = a_0 - p^\flat b_0 = 0,$$

hence $a - \xi b \in pW(\mathcal{O}_E)$. Modding out by ξ we finally get $x \in pW(\mathcal{O}_E)/(\xi) = p\mathcal{O}_E^\sharp$.

Now, Claims 1 and 2 imply that $\mathcal{O}_E^\sharp$ is complete with respect to $\|\cdot\|$ (because it is p-adically complete, and the norm topology and the p-adic topology can be compared thanks to the second claim). Moreover, letting as above $E^\sharp = \mathrm{Frac}(\mathcal{O}_E^\sharp)$, we have

$$\mathcal{O}_E^\sharp = \{x \in E^\sharp : \|x\| \le 1\}.$$

To see this, let $x \in E^\sharp$. There exist $m \in \mathbb{Z}, y \in \mathcal{O}_E$ such that $x = yp^{-m}$. If $\|x\| \le 1$, then $\|y\| \le \|p\|^m$, which by induction implies $y \in p^m\mathcal{O}_E^\sharp$. It follows that $x \in \mathcal{O}_E^\sharp$. The converse implication is obvious.

Moreover, $E^\sharp$ is perfectoid: it's an extension of the perfectoid field K, so its norm group cannot be discrete (because $\|K^\times\|$ is already non-discrete), and the map $x \mapsto x^p$ is surjective on the quotient $\mathcal{O}_E^\sharp/(p) \cong \mathcal{O}_E/(p^\flat)$. This latter fact holds because $\mathcal{O}_E$ is perfect, and any quotient of a perfect ring has the property that $x \mapsto x^p$ is surjective.

Finally, one checks on the definitions that $(\mathcal{O}_E^\sharp)^\flat \cong E$. $\square$

Exercise 4.10. *Check the isomorphism* $(\mathcal{O}_E^\sharp)^\flat \cong E$.

Lemma 4.11. *Let $E/K^\flat$ be a finite Galois extension. Then $E^\sharp/K$ is also Galois, and* $\mathrm{Gal}(E/K^\flat) \cong \mathrm{Gal}(E^\flat/K)$.

Proof. Let $\sigma \in \mathrm{Gal}(E/K^\flat)$. As usual, σ acts on $\mathcal{O}_E$ fixing $\mathcal{O}_{K^\flat}$, hence also on $W(\mathcal{O}_E)$ fixing $W(\mathcal{O}_K^\flat) = W(\mathcal{O}_{K^\flat})$. Finally, ξ is in $W(\mathcal{O}_K^\flat)$, so $\sigma(\xi) = \xi$ and σ induces an action on $W(\mathcal{O}_K^\flat)/(\xi) \cong \mathcal{O}_E^\sharp$, and therefore an action on the fraction field $E^\sharp$. Call the induced map $\sigma^\sharp \in \mathrm{Aut}(E^\sharp/K)$. Conversely, an element $\sigma \in \mathrm{Aut}(E^\sharp/K)$ acts on $\mathcal{O}_E^\sharp$, hence also on the perfection

$$\varprojlim_{x \mapsto x^p} \mathcal{O}_E^\sharp/(p) \cong \mathcal{O}_E.$$

Thus, we get an element $\sigma^\flat \in \mathrm{Gal}(E/K^\flat)$. One checks that $\sigma \mapsto \sigma^\flat$ and $\sigma \mapsto \sigma^\sharp$ are inverses of each other. Thus, we have an isomorphism

$$\mathrm{Gal}(E/K^\flat) \cong \mathrm{Aut}(E^\sharp/K) =: G.$$

To complete the proof, we need to show that $E^\sharp/K$ is Galois, or equivalently $(E^\sharp)^G = K$. What we do know is that $W(\mathcal{O}_E)^G = W(\mathcal{O}_K^\flat)$. Consider the exact sequence (given by Lemma 4.7)

$$0 \to W(\mathcal{O}_E) \xrightarrow{\xi} W(\mathcal{O}_E) \to \mathcal{O}_E^\sharp \to 0.$$

Inverting p we get

$$W(\mathcal{O}_E)[\frac{1}{p}] \xrightarrow{\xi} W(\mathcal{O}_E)[\frac{1}{p}] \to E^\sharp \to 0,$$

where $W(\mathcal{O}_E)[p^{-1}]$ and $E^\sharp$ are $\mathbb{Q}$-vector spaces with G-action. Write

$$0 \to V \to W(\mathcal{O}_E)[p^{-1}] \to E^\sharp \to 0$$

and take the associated long exact sequence in Galois cohomology:

$$0 \to V^G \to (W(\mathcal{O}_E)[p^{-1}])^G \to (E^\sharp)^G \to H^1(G, V) = 0,$$

where the last 0 comes from the fact that multiplication by the order of G acts as an automorphism on the $\mathbb{Q}$-vector space V. Since $(W(\mathcal{O}_E)[p^{-1}])^G = K$ surjects onto $(E^\sharp)^G$, we must have $(E^\sharp)^G = K$ as desired. □

To finish the proof of Theorem 3.19 we need to recall Krasner's lemma:

Lemma 4.12 (Krasner)**.** *Let K be an analytic field, $f \in K[x]$. Suppose that $f(x)$ is irreducible. Let $\alpha \in \overline{K}$ be a root of $f(x)$ and let $\varepsilon := \min\{\|\alpha - \alpha_i\| : \alpha_i \in \overline{K}, f(\alpha_i) = 0\}$. Given $\beta \in \overline{K}$ such that $\|\alpha - \beta\| < \varepsilon$, the field $K(\alpha)$ is contained in $K(\beta)$.*

Proof. Let $L \supseteq K(\beta)$ be the splitting field of $f(x)$ over $K(\beta)$. We show that for every $\sigma \in \mathrm{Gal}(L/K(\beta))$ we have $\sigma(\alpha) = \alpha$. We have

$$\|\beta - \sigma(\alpha)\| = \|\sigma(\beta) - \sigma(\alpha)\| = \|\sigma(\beta - \alpha)\| = \|\beta - \alpha\| < \varepsilon.$$

This implies

$$\|\sigma(\alpha) - \alpha\| \leq \min\{\|\sigma(\alpha) - \beta\|, \|\beta - \alpha\|\} = \|\beta - \alpha\| < \varepsilon,$$

hence $\sigma(\alpha)$ must be α (as it cannot be one of the other roots α_i). □

We will prove the following lemma:

Lemma 4.13. *If K is a perfectoid field such that $K^\flat$ is algebraically closed, then K itself is algebraically closed.*

Assuming for the moment Lemma 4.13 we can finally prove Theorem 3.19.

Proof of Theorem 3.19. Fix an algebraic closure $\overline{K}/K$ and an algebraic closure $\overline{K^\flat}$ of $K^\flat$. Inside $\overline{K}$, take $K_0 := \bigcup_{[E:K^\flat]<\infty} E^\sharp \subseteq \overline{K}$. It is easy to see that the completion $\widehat{K_0}$ is perfectoid (this follows from the fact that it is complete, together with Proposition 4.5). Its tilt $(\widehat{K_0})^\flat$ is a tilt of $\widehat{\overline{K^\flat}}$, hence it is algebraically closed. By Lemma 4.13 we obtain that $\widehat{K_0}$ is algebraically closed. Since K_0 is dense in $\widehat{K_0}$, Krasner's lemma (Lemma 4.12) shows that every $f \in K[x]$ has a root in K_0, so $K_0 = \overline{K}$. The theorem now follows from the correspondence for finite Galois extensions proved in Lemma 4.11 (every finite separable extension is contained in a finite Galois extension, and the Galois groups on both sides of the tilting correspondence match by Lemma 4.11). □

Proof of Lemma 4.13. Suppose L/K is a finite extension of degree $d \geq 2$. Let $f \in \mathcal{O}_K[x]$ be a minimal polynomial for L/K of degree greater than 1. There exists $g(x) \in \mathcal{O}_K^\flat[x]$ such that $f(x) \bmod (p) = g(x) \bmod (p^\flat)$ as polynomials with coefficients in $\mathcal{O}_K/(p) \cong \mathcal{O}_K^\flat/(p^\flat)$. Since $K^\flat$ is algebraically closed, there is $\alpha \in K^\flat$ that is a root of g. (In fact, since g can be taken to be monic, we can assume that α is in $\mathcal{O}_{K^\flat}$.)

Let $\varphi : \mathcal{O}_K^\flat \to \mathcal{O}_K$ be the Teichmüller lift and let $y_1 = \varphi(\alpha) \in \mathcal{O}_K$. By construction, $f(y_1) = 0 \bmod (p)$, or equivalently, $\|f(y_1)\| \leq \|p\|$. By Lemma 3.17, $\|\mathcal{O}_K\| = \|\mathcal{O}_K^\flat\|_\flat$, and $x \mapsto x^d$ is surjective on $\|\mathcal{O}_K^\flat\|$ because $K^\flat$ is algebraically closed. Therefore, there exists $c_1 \in \mathcal{O}_K$ such that $\|c_1\|^d = \|f(y_1)\|$. Define

$$f_1 := c_1^{-d} f(c_1 x + y_1) :$$

it is a monic irreducible polynomial in $K[x]$, and $\|f_1(0)\| = 1$. This implies that all roots of f_1 have norm 1 (because they all have the same norm by irreducibility, and the product of the norms is $\|f(0)\| = 1$), and therefore $f_1(x)$ has coefficients in $\mathcal{O}_K$. We now proceed inductively. For every $n \geq 0$, we construct $y_n, c_n \in \mathcal{O}_K$ and $f_n \in \mathcal{O}_K[x]$ such that:

1. $f_0 = f$;
2. $\|c_n\|^d = \|f_{n-1}(y_n)\| \leq \|p\|$;
3. $f_n = c_n^{-d} f_{n-1}(c_n x + y_n)$.

From this, one obtains

$$\begin{aligned}
&\|f(c_1 \cdots c_n y_{n+1} + c_1 \cdots c_{n-1} y_n + \cdots + c_1 c_2 y_3 + c_1 y_2 + y_1)\| \\
&\qquad = \|c_1^d f_1(c_2 \cdots c_n y_{n+1} + c_2 \cdots c_{n-1} y_n + \cdots + c_2 y_3 + y_2)\| \\
&\qquad = \|c_1\|^d \|c_2^d f_2(c_3 \cdots c_n y_{n+1} + c_3 \cdots c_{n-1} y_n + \cdots + y_3)\| \\
&\qquad = \cdots = \prod_{i=1}^n \|c_i\|^d \cdot \|f_n(y_{n+1})\| \leq \|p\|^{n+1}
\end{aligned}$$

and

$$\|c_1 \cdots c_i\| \leq \|p\|^{i/d} \quad \forall i.$$

We can therefore consider

$$y := \sum_{n=1}^{\infty} \left(\prod_{i=1}^{n-1} c_i \right) y_n,$$

which by the above estimates makes sense as an element of $\mathcal{O}_K$ and is a root of f, contradiction. □

5 22.02.2024 – (φ, Γ)-modules and some p-adic Hodge theory

5.1 (φ, Γ)-modules

Let $\omega \in \overline{\mathbb{Q}_p}$ be a primitive p-th root of unity and consider the Galois extensions

$$\mathbb{Q}_p \subset \mathbb{Q}_p(\omega^{1/p^\infty}) \subset \overline{\mathbb{Q}_p} \subset \mathbb{C}_p.$$

We introduce the following notation for Galois groups:

1. $G = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$;
2. $H = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\omega^{1/p^\infty}))$
3. $\Gamma = G/H = \mathrm{Gal}(\mathbb{Q}_p(\omega^{1/p^\infty})/\mathbb{Q}_p)$.

The p-adic completion K of $\mathbb{Q}_p(\omega^{1/p^\infty})$ is a perfectoid field, with tilt $K^\flat$ isomorphic to $\mathbb{F}_p((x^{1/p^\infty}))$. Recall that this identification essentially comes from the isomorphism

$$\frac{\mathbb{Z}_p[\omega]}{(p)} \cong \mathbb{F}_p[x]/(x^{p-1}).$$

The field $\mathbb{C}_p$ is also perfectoid; we denote its tilt by $\mathbb{C}_p^\flat$. It is algebraically closed. This can be shown directly, but it also follows from the tilting correspondence (Theorem 3.19): the finite extensions of $\mathbb{C}_p^\flat$ correspond bijectively to the finite extensions of $\mathbb{C}_p$ (of which there is only one, namely $\mathbb{C}_p$ itself).

The tilting correspondence also shows that $\mathrm{Gal}(\overline{K}/K)$ is isomorphic to $\mathrm{Gal}(\overline{K^\flat}/K^\flat)$. On the other hand, there is a canonical isomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\omega^{1/p^\infty})) \xrightarrow{\sim} \mathrm{Gal}(\overline{K}/K) :$$

this follows from the fact that $\mathbb{Q}_p(\omega^{1/p^\infty})$ is Henselian[1], and the absolute Galois group of a Henselian field is isomorphic to the absolute Galois group of its completion. To be even more precise, finite separable extensions of a Henselian field correspond bijectively to finite separable extensions of the completion. For similar reasons, there is an isomorphism

$$\mathrm{Gal}(\overline{K^\flat}/K^\flat) \cong \mathrm{Gal}(\overline{\mathbb{F}_p((x))}/\mathbb{F}_p((x))).$$

We now choose a sequence $(\omega_n)_{n\in\mathbb{N}}$ such that $\omega_0 = 1, \omega_1 = \omega$ and $\omega_{n+1}^p = \omega_n$ for all $n \geq 1$. This sequence defines an element of

$$\varprojlim_{x\mapsto x^p} \mathcal{O}_{\overline{\mathbb{Q}_p}}/(p) = \varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/(p) =: \mathcal{O}_{\mathbb{C}_p}^\flat.$$

We call this element $\overline{\omega}$, we denote by $[\overline{\omega}]$ its Teichmüller representative in $W(\mathcal{O}_{\mathbb{C}_p}^\flat)$, and we define $\pi := [\overline{\omega}] - 1$. Note that the reduction modulo p of π is exactly the element x that appears in the description of the field $\mathbb{F}_p((x^{1/p^\infty}))$. Moreover, there is a bijection *of sets*

$$W(\mathcal{O}_{\mathbb{C}_p^\flat}) \cong (\mathcal{O}_{\mathbb{C}_p^\flat})^{\mathbb{N}}$$

[1] a valued field such that the valuation extends *uniquely* to any finite extension.

given by

$$\sum [a_n]p^n \longleftrightarrow (a_n).$$

We can then equip $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ with the topology induced by that of $\mathcal{O}_{\mathbb{C}_p^\flat}$.

One checks that $W(\mathcal{O}_{\mathbb{C}_p}^\flat) = W(\mathcal{O}_{\mathbb{C}_p^\flat})$ is complete with respect to this ('weak') topology, see Exercise 5.1. This implies that there is an injection

$$\mathbb{Z}_p[[\pi]] \hookrightarrow W(\mathcal{O}_{\mathbb{C}_p}^\flat)$$

(by definition of the topology, see Exercise 5.1 again). We thus get an embedding

$$\mathbb{Z}_p((\pi)) \hookrightarrow W(\mathbb{C}_p^\flat),$$

where $W(\mathbb{C}_p^\flat)$ is a Cohen ring, hence in particular p-adically complete. In turn, this implies that there is an embedding of

$$\mathcal{O}_{\mathcal{E}} := \widehat{\mathbb{Z}_p((\pi))} \hookrightarrow W(\mathbb{C}_p^\flat).$$

The ring $\mathcal{O}_{\mathcal{E}}$ is Cohen, with residue field $E := \mathbb{F}_p((x))$. The Frobenius on E lifts to an endomorphism $\varphi : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$. We can impose

$$\varphi(\pi) = \varphi([\overline{\omega}] - 1) = [\overline{\omega}]^p - 1 = (1+\pi)^p - 1.$$

The Galois group Γ also acts on $\overline{\omega}$, via the cyclotomic character χ. Hence, there is an action on $\mathcal{O}_{\mathcal{E}}$ via

$$\sigma(\pi) = \sigma([\overline{\omega}] - 1) := [\sigma(\overline{\omega})] - 1.$$

Exercise 5.1. *Check that*

1. *the weak topology on $W(\mathcal{O}_{\mathbb{C}_p}^\flat)$ is complete.*
2. *there is an injection $\mathbb{Z}_p[[\pi]] \hookrightarrow W(\mathcal{O}_{\mathbb{C}_p}^\flat)$.*

We may embed $\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}$, the maximal unramified extension of $\mathcal{O}_{\mathcal{E}}$, in $W(\mathbb{C}_p^\flat)$. Also the p-adic completion $\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}}$ embeds in $W(\mathbb{C}_p^\flat)$. We now observe that G acts on $\mathcal{O}_{\overline{\mathbb{Q}_p}}$, hence on $\mathcal{O}_{\overline{\mathbb{Q}}_p}^\flat = \mathcal{O}_{\mathbb{C}_p}^\flat$, hence on its fraction field $\mathbb{C}_p^\flat$, and finally on $W(\mathbb{C}_p^\flat)$. This action preserves $\mathcal{O}_{\mathcal{E}} \subset W(\mathbb{C}_p^\flat)$ and induces the Γ-action on it. It also preserves $\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}}$.

Recall now that we have isomorphisms

$$H \cong \mathrm{Gal}(\overline{K^\flat}/K^\flat) \cong \mathrm{Gal}(\overline{E}/E).$$

By Theorem 2.13, the functor

$$N \mapsto \left(\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}} \otimes_{\mathbb{Z}_p} N\right)^H$$

induces an equivalence of categories

$$\left\{ \begin{array}{c} \text{finite-dimensional} \\ \mathbb{Z}_p\text{-representation of } H \end{array} \right\} \leftrightarrow \{\text{étale } \varphi\text{-modules over } E\}$$

If furthermore N carries an action not only of H, but of the whole group G, then the H-invariants $\left(\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} N\right)^H$ carry an action of $G/H \cong \Gamma$.

Definition 5.2 ((φ, Γ)-module, Fontaine)**.** A (φ, Γ)-module over $\mathcal{O}_{\mathcal{E}}$ is a φ-module with Γ-action. It is called *étale* if the underlying φ-module is étale.

Theorem 5.3 (Fontaine)**.** *The functor*

$$N \mapsto \left(\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}} \otimes_{\mathbb{Z}_p} N\right)^H$$

induces an equivalence of categories

$$\left\{ \begin{matrix} \textit{finitely generated} \\ \mathbb{Z}_p\textit{-representation of } G \end{matrix} \right\} \leftrightarrow \{\textit{étale } (\varphi, \Gamma)\textit{-modules over } E\}.$$

A quasi-inverse is given by

$$M \mapsto \left(\widehat{\mathcal{O}_{\mathcal{E}}^{\mathrm{nr}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M\right)^{\varphi=1},$$

where the G-action is given by

$$g(\lambda \otimes m) := g(\lambda) \otimes \overline{g}(m),$$

where $\overline{g} \in \Gamma$ is the class of g modulo H.

Remark 5.4.

1. A similar result holds for finite-dimensional $\mathbb{Q}_p$-representations.
2. This theorem admits a generalisation to $\mathrm{Gal}(\overline{F}/F)$, where F is a finite extension of $\mathbb{Q}_p$.
3. Caveat: one should be careful with topology. Since we only want to consider continuous Galois representations, to get an actual equivalence of categories we also need to impose a continuity condition on our (φ, Γ)-modules (specifically, that the Γ-action is continuous for the weak topology induced by $W(\mathbb{C}_p^\flat)$).

5.2 An introduction to p-adic Hodge theory

5.2.1 Some motivation from complex Hodge theory

Let X be a smooth projective variety over $\mathbb{C}$. Let X^{an} be the associated analytic space over $\mathbb{C}$. We have the Hodge decomposition

$$H^n(X^{\mathrm{an}}, \mathbb{C}) \cong \bigoplus_{p+q=n} H^{p,q},$$

where $H^{p,q} = H^q\left(X^{\mathrm{an}}, \Omega^p_{X^{\mathrm{an}}}\right)$. Complex conjugation acts on $\mathbb{C}$, hence also on $H^n(X^{\mathrm{an}}, \mathbb{C})$, and $\overline{H^{p,q}} = H^{q,p}$.

We try to interpret part of this theorem within the realm of algebraic geometry. Consider the holomorphic de Rham complex

$$\Omega^\bullet_{X^{\mathrm{an}}} := \left[\mathcal{O}_{X^{\mathrm{an}}} \xrightarrow{d} \Omega^1_{X^{\mathrm{an}}} \xrightarrow{d} \Omega^2_{X^{\mathrm{an}}} \to \cdots\right],$$

where the differentials d satisfy

$$d(\omega_1 \wedge \omega_2) = d\omega_1 \wedge \omega_2 + (-1)^p \omega_1 \wedge \omega_2,$$

for all $\omega_1 \in \Omega^p_{X^{\mathrm{an}}}, \omega_2 \in \Omega^q_{X^{\mathrm{an}}}$. Since this gives a resolution of the sheaf $\mathbb{C}$ ('holomorphic Poincaré lemma'), there is an isomorphism

$$H^n(X^{\mathrm{an}}, \mathbb{C}) \cong \mathbb{H}^n(X^{\mathrm{an}}, \Omega^\bullet_{X^{\mathrm{an}}}) =: H^n_{dR}(X^{\mathrm{an}}),$$

where $\mathbb{H}$ denotes hypercohomology.

We observe that $\Omega^\bullet_{X^{\mathrm{an}}}$ has a descending filtration by subcomplexes

$$\Omega^{\geq p}_{X^{\mathrm{an}}} := [0 \to 0 \to 0 \to \cdots \to 0 \to \Omega^p_{X^{\mathrm{an}}} \to \Omega^{p+1}_{X^{\mathrm{an}}} \to \cdots].$$

Using the spectral sequence of filtrations, we get a spectral sequence

$$E_1^{p,q} = H^q(X^{\mathrm{an}}, \Omega^p_{X^{\mathrm{an}}}) \Rightarrow H^{p+q}_{dR}(X^{\mathrm{an}})$$

that induces the (Hodge) filtration $F^0 \supset F^1 \supset \cdots$ on $H^{p+q}_{dR}(X^{\mathrm{an}})$. A fundamental fact is that this spectral sequence degenerates already on page 1, hence $F^p/F^{p+1} \cong H^q(X^{\mathrm{an}}, \Omega^q_{X^{\mathrm{an}}})$. Using complex conjugation, we define $\mathcal{H}^{p,q} = F^p \cap \overline{F^q}$.

Theorem 5.5 (Complex conjugation splits the Hodge filtration)**.** *The natural map $\mathcal{H}^{p,q} \to F^p/F^{p+1}$ is an isomorphism. Therefore, $\mathcal{H}^{p,q} \cong H^q(X^{\mathrm{an}}, \Omega^p)$.*

Theorem 5.5 is one of the main statements of Hodge theory that can only be proved by analytic means.

We now move completely to the algebraic world. On X we also have the algebraic de Rham complex,

$$\Omega^\bullet_X := [\mathcal{O}_X \xrightarrow{d} \Omega^1_X \xrightarrow{d} \Omega^2_X \xrightarrow{d}\to \cdots],$$

and we still have a spectral sequence

$$E_1^{p,q} = H^q(X, \Omega^p) \Rightarrow H^{p+q}_{dR}(X).$$

There are natural maps $H^q(X, \Omega^p_X) \to H^q(X^{\mathrm{an}}, \Omega^p_{X^{\mathrm{an}}})$ and $H^n_{dR}(X) \to H^n_{dR}(X^{\mathrm{an}})$. Serre's GAGA theorem implies that when X is smooth and projective these maps are isomorphisms.

Theorem 5.6 (Deligne-Illusie)**.** *The algebraic spectral sequence degenerates at E_1, so we have a Hodge filtration on the algebraic de Rham cohomology.*

However, there is no algebraic Poincaré lemma! So all we know (passing via the complex theory) is that

$$H^n(X^{\mathrm{an}}, \mathbb{C}) \cong \bigoplus_{p+q=n} H^q(X, \Omega^p).$$

There is no meaningful algebraic comparison with singular cohomology with $\mathbb{C}$-coefficients (which after all is hard to define in the algebraic world). On the other hand, étale cohomology allows us to define

$$H^n(X, \mathbb{Q}_p) = \varprojlim_r H^n_{\text{ét}}(X, \mathbb{Z}/p^r\mathbb{Z}) \otimes \mathbb{Q}.$$

Over $\mathbb{C}$, this does not compare to (algebraic) de Rham cohomology. However, over $\mathbb{C}_p$ (and even over $\mathbb{Q}_p$) it does! This is the starting point of p-adic Hodge theory.

5.2.2 Some results in p-adic Hodge theory

Let $K/\mathbb{Q}_p$ be a finite extension. Denote by G_K the absolute Galois group of K. We know that G acts on $\mathbb{C}_p$, and also on $\mathbb{Z}_p(i) := \varprojlim_r \mu_{p^r}^{\otimes i}$, on $\mathbb{Q}_p(i) = \mathbb{Z}_p(i) \otimes \mathbb{Q}$, and on $\mathbb{C}_p(i) := \mathbb{Q}_p(i) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$.

Theorem 5.7 (Ax-Sen-Tate [Ax70, Tat67])**.** *We have*

$$(\mathbb{C}_p(i))^{G_K} = \begin{cases} K, & \text{if } i = 0 \\ 0, & \text{if } i > 0. \end{cases}$$

Theorem 5.8 (The Hodge-Tate decomposition; Faltings)**.** *Let X be a smooth projective variety over K. There exists a canonical isomorphism*

$$H^n_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \cong \bigoplus_q H^q(X, \Omega^{n-q}) \otimes_K \mathbb{C}_p(q-n)$$

of G_K-modules.

Remark 5.9. The result holds more generally for X not necessarily projective using logarithmic differentials.

Example 5.10. For $n = 1$ we get

$$H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \left(H^0(X, \Omega^1_X) \otimes \mathbb{C}_p(-1)\right) \oplus \left(H^1(X, \mathcal{O}_X) \otimes \mathbb{C}_p\right).$$

When X is an abelian variety, we have

$$H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \left(\varprojlim_r X^\vee_{\overline{K}}[p^r]\right) \otimes \mathbb{Q}(-1).$$

If X is an elliptic curve, $X^\vee \cong X$, and we get that the Tate module decomposes as the direct sum of $\mathbb{C}_p$ and $\mathbb{C}_p(1)$.

Fontaine reformulated these results in terms of a certain ring B_{HT}.

Definition 5.11. Define

$$B_{\text{HT}} := \bigoplus_{n\in\mathbb{Z}} \mathbb{C}_p(i) :$$

it is a $\mathbb{C}_p$-algebra endowed with a G_K-action. Also define the K-algebra

$$H^n_{\text{Hdg}}(X) := \bigoplus_{q=0}^{n} H^q(X, \Omega^{n-q}_X).$$

Faltings' theorem can then be expressed as follows:

Theorem 5.12 (Faltings)**.** *There is a G_K-equivariant isomorphism of graded $\mathbb{C}_p$-algebras*

$$H^n_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{HT}} \cong H^n_{\text{Hdg}}(X) \otimes_K B_{\text{HT}}.$$

Note that here there are non-trivial G_K actions only on $H^n_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$ and B_{HT}: the Galois action on $H^n_{\text{Hdg}}(X)$ is trivial.

Moreover, the Ax-Sen-Tate theorem (Theorem 5.7) can be rephrased as $B_{\mathrm{HT}}^{G_K} \cong K$. Combining the two theorems we then obtain

$$H^n_{\mathrm{Hdg}}(X) \cong \left(H^n_{\text{ét}(X_{\overline{K}},\mathbb{Q}_p} \otimes B_{\mathrm{HT}}\right)^{G_K},$$

which shows how that one can recover $H^n_{\mathrm{Hdg}}(X)$ from $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$.

The next natural question is then whether one can recover $H^n_{dR}(X)$ from $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. To answer this question, Fontaine has defined a complete discrete valued field $B_{\mathrm{dR}} \supset \overline{K}$, endowed with a G_K-action and a G_K-equivariant decreasing filtration $\mathrm{Fil}^i B_{\mathrm{dR}}$, such that

$$\mathrm{Fil}^i B_{\mathrm{dR}} / \mathrm{Fil}^{i+1} B_{\mathrm{dR}} \cong \mathbb{C}_p(i).$$

In other words, the associated graded ring of B_{dR} is B_{HT}.

Theorem 5.13 (Faltings)**.** *For every n there is a G_K-equivariant isomorphism of filtered $\overline{K}$-algebras*

$$H^n_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \cong H^n_{\mathrm{dR}}(X) \otimes_K B_{\mathrm{dR}}.$$

The Ax-Sen-Tate theorem (Theorem 5.7) implies

$$B_{dR}^{G_K} \cong K,$$

and therefore

$$\left(H^n_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}\right)^{G_K} \cong H^n_{\mathrm{dR}}(X),$$

which recovers de Rham cohomology together with its Hodge filtration.

Note that from Theorem 5.13 one obtains Theorem 5.12 by passing to the associated graded rings.

5.2.3 The construction of B_{dR} (Fontaine)

Start with $\mathcal{O}_{\mathbb{C}_p}$ and take its tilt $\mathcal{O}^\flat_{\mathbb{C}_p}$. There is a map

$$\overline{\varphi} : W(\mathcal{O}^\flat_{\mathbb{C}_p}) \to \mathcal{O}_{\mathbb{C}_p},$$

induced by the generalised Teichmüller construction. We have seen that $\overline{\varphi}$ is surjective and its kernel is generated by a single element ξ (Lemma 4.7). Inverting p we get a map

$$\vartheta : W(\mathcal{O}^\flat_{\mathbb{C}_p})[p^{-1}] \twoheadrightarrow \mathbb{C}_p.$$

The kernel of ϑ is obviously still generated by ξ. We define

$$B^+_{\mathrm{dR}} := \varprojlim_r W(\mathcal{O}^\flat_{\mathbb{C}_p})[p^{-1}]/(\xi^r),$$

that is, the ξ-adic completion of $W(\mathcal{O}^\flat_{\mathbb{C}_p})$. It is a complete DVR with uniformiser ξ. The field B_{dR} is the fraction field of B^+_{dR}. The filtration Fil^i is given by $\mathrm{Fil}^i B_{\mathrm{dR}} := B^+_{\mathrm{dR}} \cdot \xi^i$ for all $i \in \mathbb{Z}$.

Note that $\mathcal{O}_{\mathbb{C}_p}$ has a G_K-action, so $W(\mathcal{O}^\flat_{\mathbb{C}_p})$ has a G_K-action, which is inherited by B^+_{dR} and B_{dR} since ξ is G_K-invariant. We will show next time that $\mathrm{Fil}^i / \mathrm{Fil}^{i+1} \cong \mathbb{C}_p(i)$ as G_K-modules.

Proposition 5.14. *There is a natural G_K-equivariant embeding of $\overline{\mathbb{Q}_p} = \overline{K}$ in B_{dR}^+.*

Proof. We know that $\mathcal{O}_{\mathbb{C}_p}$ is a complete local ring with residue field $\overline{\mathbb{F}_p}$. Notice that this residue field is a quotient of $\mathcal{O}_{\mathbb{C}_p}/(p)$; moreover, the ideal defining the quotient $\mathcal{O}_{\mathbb{C}_p}/(p) \to \overline{\mathbb{F}_p}$ is topologically nilpotent (this is necessary for our next argument, which relies on formal smoothness). Consider the commutative diagram

$$\begin{tikzcd}
\overline{\mathbb{F}_p} \arrow[r, "\mathrm{id}"] & \overline{\mathbb{F}_p} \\
\mathbb{F}_p \arrow[u] \arrow[r] & \mathcal{O}_{\mathbb{C}_p}/(p) \arrow[u]
\end{tikzcd}$$

Since $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is formally étale, we get a unique lift $\overline{\rho} : \overline{\mathbb{F}_p} \to \mathcal{O}_{\mathbb{C}_p}/(p)$. Since $\overline{\mathbb{F}_p}$ is perfect, $\overline{\rho}$ induces a map $\overline{\mathbb{F}_p} \to \mathcal{O}_{\mathbb{C}_p}^\flat = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/(p)$, and therefore a map

$$\mathbb{Q}_p^{\mathrm{nr}} = W(\overline{\mathbb{F}_p})[p^{-1}] \to W(\mathcal{O}_{\mathbb{C}_p}^\flat)[p^{-1}] \to B_{\mathrm{dR}}^+.$$

We now have a similar diagram

$$\begin{tikzcd}
\overline{\mathbb{Q}_p} \arrow[r] & \mathbb{C}_p \\
\mathbb{Q}_p^{\mathrm{nr}} \arrow[u] \arrow[r] & B_{\mathrm{dR}}^+ \arrow[u]
\end{tikzcd}$$

By formal étaleness of $\overline{\mathbb{Q}_p}$ over $\mathbb{Q}_p^{\mathrm{nr}}$, we get a unique lift $\overline{\mathbb{Q}_p} \to B_{\mathrm{dR}}^+$. By uniqueness, this lift must be G_K-equivariant. $\square$

Remark 5.15. This proof might look overly complicated (after all, the extension $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ is formally étale, so we could have obtained an embedding of $\overline{\mathbb{Q}_p}$ directly, without passing through $\overline{\mathbb{Q}_p}^{\mathrm{nr}}$), but we will need the partial steps in the proof in what follows.

6 29.02.2024

6.1 Review of the construction of B_{dR}

We begin by recalling the comparison theorem between étale and de Rham cohomology, that we stated earlier as Theorem 5.13:

Theorem 6.1. *Let $K/\mathbb{Q}_p$ be a finite extension, X/K a proper smooth variety, $G = \mathrm{Gal}(\overline{\mathbb{Q}_p}/K)$. There is a canonical isomorphism*

$$H^n_{\acute{e}t}(\overline{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \cong H^n_{\mathrm{dR}}(X) \otimes_K B_{\mathrm{dR}}.$$

Corollary 6.2.
$$\left(H^n_{\acute{e}t}(\overline{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}\right)^G = H^n_{\mathrm{dR}}(X).$$

The construction of the ring B_{dR} appearing in these statements goes as follows. There is a surjective map

$$W\left(\mathcal{O}_{\mathbb{C}_p}^\flat\right) \xrightarrow{\tilde{\varphi}} \mathcal{O}_{\mathbb{C}_p},$$

which induces the surjective Fontaine map

$$\vartheta : W(\mathcal{O}_{\mathbb{C}_p}^\flat)[1/p] \to \mathbb{C}_p.$$

The kernel of ϑ is principal (Lemma 4.7), generated by ξ, and we define B_{dR}^+ as

$$B_{\mathrm{dR}}^+ = \varprojlim W(\mathcal{O}_{\mathbb{C}_p}^\flat)[1/p]/(\xi^h);$$

the field B_{dR} is its fraction field $B_{\mathrm{dR}} = \mathrm{Frac}(B_{\mathrm{dR}}^+) = B_{\mathrm{dR}}^+[\xi^{-1}]$. The ring B_{dR}^+ is a complete DVR with residue field $\mathbb{C}_p$ and maximal ideal ξ. The field B_{dR} carries a natural filtration, indexed by $i \in \mathbb{Z}$, given by $\mathrm{Fil}^i B_{\mathrm{dR}} := B_{\mathrm{dR}}^+ \cdot \xi^i$.

6.2 The pieces of the filtration on B_{dR}

We shall prove:

Proposition 6.3. *For every i, the quotient $\mathrm{Fil}^i B_{\mathrm{dR}}/\mathrm{Fil}^{i+1} B_{\mathrm{dR}}$ is isomorphic to $\mathbb{C}_p(i)$ as a Galois module.*

Corollary 6.4. *One has $(B_{\mathrm{dR}}^+)^G = B_{\mathrm{dR}}^G = K$.*

Proof of Corollary 6.4. By Ax-Sen-Tate (Theorem 5.7), $\mathbb{C}_p(i)^G = K$ for $i = 0$ and $\mathbb{C}_p(i)^G = (0)$ for $i \neq 0$. We proceed by induction. For B_{dR}^+, we have

$$0 \to \mathrm{Fil}^{i+1} B_{\mathrm{dR}}^+ \to \mathrm{Fil}^i B_{\mathrm{dR}}^+ \to \mathbb{C}_p(i) \to 0;$$

for $i > 0$, taking G-invariants we obtain

$$0 \to \left(\mathrm{Fil}^{i+1} B_{\mathrm{dR}}^+\right)^G \to \left(\mathrm{Fil}^i B_{\mathrm{dR}}^+\right)^G \to 0,$$

so $\left(\mathrm{Fil}^{i+1} B_{\mathrm{dR}}^+\right)^G \cong \left(\mathrm{Fil}^i B_{\mathrm{dR}}^+\right)^G$ for all $i \geq 1$. Thus, the Galois invariants in $\mathrm{Fil}^1 B_{\mathrm{dR}}^+$ are actually contained in the intersection $\bigcap_{i\geq 0} \mathrm{Fil}^i B_{\mathrm{dR}}^+$, which is trivial. This shows that $(\mathrm{Fil}^1 B_{\mathrm{dR}}^+)^G = (0)$. Taking G-invariants in the sequence

$$0 \to \mathrm{Fil}^1 B_{\mathrm{dR}}^+ \to B_{\mathrm{dR}}^+ \to \mathbb{C}_p \to 0$$

then shows that $(B_{\mathrm{dR}}^+)^G$ injects into $\mathbb{C}_p^G = K$, hence is equal to it. For the case of B_{dR}, proceed by descending induction on i. $\square$

To prove the proposition, we introduce Fontaine's famous element t. Recall that we have an element

$$\overline{\omega} \in \mathcal{O}_{\mathbb{C}_p}^\flat = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/(p)$$

given by the collection $(1, \omega, \omega_2, \omega_3, \ldots)$, where $\omega^p = 1$ and $\omega_i^p = \omega_{i-1}$. This $\overline{\omega}$ has a Teichmüller lift $[\overline{\omega}]$. We compute

$$\vartheta([\overline{\omega}] - 1) = \tilde{\varphi}([\overline{\omega}] - 1) = \varphi(\overline{\omega}) - 1 = 0.$$

This shows that $[\overline{\omega}]-1$ is in $\ker \vartheta$. Since B_{dR}^+ is complete with respect to the $\ker \vartheta$-topology, we can define

$$t := \log[\overline{\omega}] = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{([\overline{\omega}] - 1)^n}{n}.$$

Lemma 6.5. *The element t generates* $\ker\vartheta$*, hence* $\mathrm{Fil}^i B_{\mathrm{dR}}^+ = B_{\mathrm{dR}}^+ t^i$.

Remark 6.6. This element t is the analogue of $2\pi i \in \mathbb{C}$, at least in the following sense: $2\pi i$ generates the kernel of exp, and $\vartheta(\exp(t)) = 1$. Moreover, t is a p-adic period for the line minus one point.

Proof (case $p > 2$). It is enough to prove that $t \in \mathrm{Fil}^1 B_{\mathrm{dR}}^+ \setminus \mathrm{Fil}^2 B_{\mathrm{dR}}^+$. Given the explicit formula defining t and our previous observation that $t \in \ker\vartheta$, this is equivalent to showing that $[\overline{\omega}] - 1$ is in $\mathrm{Fil}^1 B_{\mathrm{dR}}^+ \setminus \mathrm{Fil}^2 B_{\mathrm{dR}}^+$. Recall that $\ker(\vartheta)$ is contained in $(p, [p^\flat])$, so it's enough to show that

$$\|[\overline{\omega}] - 1\|_\flat > \|p\|^2.$$

By definition,

$$\|[\overline{\omega}] - 1\|_\flat = \lim_{n\to\infty} \|\omega_n - 1\|^{p^n},$$

and basic algebraic number theory shows that

$$\|\omega_n - 1\| = \|p\|^{1/(p-1)p^{n-1}}.$$

Hence, $\|[\overline{\omega}] - 1\| = \|p\|^{p/(p-1)}$, which is greater than $\|p\|^2$ since $p > 2$. ☐

Proof of Proposition 6.3. The quotients of the filtration are all $\mathbb{C}_p$ since B_{dR}^+ is a complete DVR with residue field $\mathbb{C}_p$. Thus, we only have to check the Galois action. By definition, G acts on $\overline{\omega}$ via the cyclotomic character χ:

$$\forall g \in G, \quad g(\overline{\omega}) = \overline{\omega}^{\chi(g)},$$

and formally

$$g(t) = g(\log[\overline{\omega}]) = \log[\overline{\omega}]^{\chi(g)} = \chi(g)\log[\overline{\omega}] = \chi(g)t.$$

(Checking the validity of this formula is actually a rather annoying topological exercise that we leave to the reader.) ☐

Remark 6.7. Fontaine proved the formula

$$\left(\varprojlim \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}[p^n]\right) \otimes \mathbb{Q} \cong \mathbb{C}_p(1),$$

which suggests a relation between differentials (hence de Rham cohomology) and $\mathbb{C}_p(1)$. Beilinson has recently given a construction of B_{dR} starting from differentials.

6.3 Fontaine's formalism

Definition 6.8. Let V be a finite-dimensional $\mathbb{Q}_p$-representation of G. We define

$$D_{\mathrm{dR}}(V) := \left(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V\right)^G.$$

It is a vector space over $B_{\mathrm{dR}}^G = K$. We define a map

$$\alpha_V : B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V) \to B_{\mathrm{dR}} \otimes_K B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V \xrightarrow{\text{mult}} B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V.$$

Remark 6.9. The letters B and D are in honour of Barsotti and Dieudonné, respectively.

Lemma 6.10. *The map α_V is injective.*

Proof. Let $v_1, \ldots, v_n \in D_{\mathrm{dR}}(V)$ be linearly independent over K. We show that they are linearly independent over B_{dR}. By induction on n. The case $n = 1$ is trivial; for $n > 1$, suppose

$$v_1, \ldots, v_n$$

are linearly dependent over B_{dR}. By induction, $v_1, \ldots, v_{n-1}$ are linearly independent over B_{dR}, so we can write

$$v_n = \sum_{i=1}^{n-1} b_i v_i \quad b_i \in B_{\mathrm{dR}}^{\times}.$$

For any $g \in G$, we have $g(v_n) = v_n$, hence

$$v_n = g(v_n) = \sum_{i=1}^{n-1} g(b_i v_i) = \sum_{i=1}^{n-1} g(b_i) v_i.$$

Taking the difference,

$$0 = \sum_i (g(b_i) - b_i) v_i = 0,$$

and since the v_i are linearly independent, this gives $g(b_i) = b_i$ for all g, hence $b_i \in K$, but this means that $v_1, \ldots, v_n$ are linearly dependent over K, contradiction. □

Corollary 6.11. *We have*

$$\dim_K D_{\mathrm{dR}}(V) \leq \dim_{\mathbb{Q}_p} V.$$

Definition 6.12 (Fontaine)**.** The G-representation V is **de Rham** if α_V is an isomorphism.

Corollary 6.13. *V is de Rham if and only if* $\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p}(V)$.

Example 6.14.

1. $\mathbb{Q}_p(n)$ is de Rham for all n (using Ax-Sen-Tate).
2. $H^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p)$ is de Rham for all n (Faltings, a consequence of Theorem 6.1). More generally, $H^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p)(i)$ is de Rham for all n, i: this follows from Faltings's theorem and the general formalism due to Fontaine, which shows that tensor products and duals of de Rham representations are de Rham.

.

6.4 Hodge-Tate representations

Recall that we defined

$$B_{\mathrm{HT}} := \bigoplus_{n \in \mathbb{Z}} \mathbb{C}_p(n) = \mathrm{gr}^{\bullet}_{\mathrm{Fil}} B_{\mathrm{dR}}.$$

Definition 6.15 (Hodge-Tate representation)**.** Define

$$D_{\mathrm{HT}}(V) := (B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V)^G$$

and

$$\beta_V : B_{\mathrm{HT}} \otimes_K D_{\mathrm{HT}}(V) \to B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V.$$

We say that V is **Hodge-Tate** if β_V is an isomorphism.

Proposition 6.16. *V is Hodge-Tate if and only if* $\dim_K D_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p}(V)$.

Remark 6.17. This is completely analogous to Corollary 6.13, but the proof is much harder, and requires a refined version of the Ax-Sen-Tate theorem.

Corollary 6.18. *If V is de Rham, then it is Hodge-Tate.*

Proof. Since B_{HT} is the associated graded ring of B_{dR} we have

$$\dim_K D_{\mathrm{dR}}(V) \leq \dim_K D_{\mathrm{HT}}(V),$$

and $\dim_K D_{\mathrm{HT}}(V) \leq \dim_{\mathbb{Q}_p}(V)$ always holds. Thus, if V is de Rham, we have

$$\dim_K D_{dR}(V) = \dim_{\mathbb{Q}_p}(V) \Rightarrow \dim_K D_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p}(V).$$

□

Remark 6.19.

1. The converse is not true.
2. If V is Hodge-Tate, there exist finitely many indices i such that $(V \otimes_{\mathbb{Q}_p} \mathbb{C}_p(i))^G \neq (0)$. These i are called the **Hodge-Tate (HT) weights** of V.

Example 6.20.

1. $\mathbb{Q}_p(n)$ has HT weight $-n$.
2. Let E be an elliptic curve. Then $H^1_{\text{ét}}(E, \mathbb{Q}_p)$ has HT weights $0, -1$.
3. Let X be smooth and proper over K. Then HT weights of $H^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p)$ are in the interval $[-n, 0]$.

Conjecture 6.21 (Fontaine-Mazur)**.** *Let F be a number field and let V be a finite-dimensional $\mathbb{Q}_p$-representation of* $\mathrm{Gal}(\overline{F}/F)$*. We say that V* ***comes from geometry*** *if it appears as a subquotient of some $H^n(\overline{X}, \mathbb{Q}_p)(i)$ (where X/F is smooth and proper). The following are equivalent:*

1. *V comes from geometry;*
2. *for all but finitely many primes $\ell \neq p$, the inertia groups of the primes above ℓ act trivially on V; moreover, V is de Rham when considered as a representation of the decomposition group of every prime of F above p.*

6.5 Crystalline representations

Motivating question: Theorem 6.1 allows one to recover de Rham cohomology from étale cohomology, but not the other way around. We would like, at least in some cases, to be able to go in the opposite direction.

Facts. Let k be a perfect field of characteristic $p > 0$, let $W = W(k)$ be the ring of Witt vectors, and X/k be a smooth proper variety. One can define crystalline cohomology groups $H^n_{\mathrm{cris}}(X/W)$, which are finitely generated W-modules. The absolute Frobenius $X \to X$ induces a φ-module structure on $H^n_{\mathrm{cris}}(X/W)$ (with respect to the lift of Frobenius on the Witt vectors). Moreover, $\varphi \otimes \mathbb{Q}$ is an isomorphism. If Z is a proper smooth scheme over $\operatorname{Spec} W$ such that $Z \times_W k \cong X$, then $H^n_{\mathrm{cris}}(X/W) \cong H^n_{\mathrm{dR}}(Z/W) := \mathbb{H}^n\left(Z, \Omega^\bullet_{Z/W}\right)$. Note the miraculous fact that the left-hand side only depends on the special fibre!

Let A be any complete DVR of mixed characteristic $(0,p)$, with residue field k. There is a canonical map $W(k) \hookrightarrow A$. Let K be the fraction field of A and K_0 be the fraction field of $W(k)$, seen as a subset of K. Note that there is a lift of Frobenius to W, hence to K_0, but not necessarily to K.

Theorem 6.22 (Berthelot, Ogus). *If Y is a smooth proper variety over* $\operatorname{Spec} A$ *such that $Y \times_A k \cong X$, then*

$$H^n_{\text{cris}}(X/W) \otimes_W K \cong H^n_{\text{dR}}(Y \times_A K).$$

Definition 6.23 (Filtered φ-module). A **filtered φ-module** over K_0 is a φ-module M over K_0 such that $M \otimes_{K_0} K$ admits a descending filtration $\operatorname{Fil}^i M$ that is exhaustive and separated.

Corollary 6.24. *The group $H^n_{\text{cris}}(X/K) \otimes_W K_0$ has a natural structure of filtered φ-module: the lift of Frobenius gives the φ-module structure, and $(H^n_{\text{cris}}(X/K) \otimes_W K_0) \otimes_{K_0} K \cong H^n_{\text{dR}}(Y \times_A K)$ has its natural filtration.*

Assume now that $A = \mathcal{O}_K$, where $K/\mathbb{Q}_p$ is a finite extension. Fontaine constructed a K_0-subalgebra B_{cris} of B_{dR} which is stable under G and equipped with a φ-module structure over K_0. Moreover, the natural map

$$K \otimes_{K_0} B_{\text{cris}} \to B_{\text{dR}}$$

is injective, so $K \otimes_{K_0} B_{\text{cris}}$ inherits a filtration from $\operatorname{Fil}^i B_{\text{dR}}$.

Facts.

1. $B^G_{\text{cris}} = K_0$.
2. $B^{\varphi=1}_{\text{cris}} \cap \operatorname{Fil}^0 = \mathbb{Q}_p$ ('fundamental exact sequence of p-adic Hodge theory' – an elementary but long calculation).

Theorem 6.25 (Faltings). *Let $Y/\mathcal{O}_K$ be proper and smooth, $\overline{Y} := Y \times_{\mathcal{O}_K} \overline{K}$, and $X = Y \times_{\mathcal{O}_K} k$. There is a natural isomorphism*

$$H^n_{\text{cris}}(X/W) \otimes_W B_{\text{cris}} \cong H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{cris}}.$$

This isomorphism is compatible with the actions of G and φ, and – after tensoring by K over K_0 – with Fil^i.

Remark 6.26.

1. H^n_{cris} has the trivial Galois action; everything else carries an interesting Galois action.
2. H^n_{cris} has a φ-module structure, and so does B_{cris}; $H^n_{\text{ét}}$ has the trivial φ-module structure;
3. after tensoring by K, there is a filtration on $H^n_{\text{cris}} \otimes_W K$ and on B_{cris}, but not on étale cohomology.

Corollary 6.27. *We can recover the de Rham cohomology of Y as*

$$H^n_{\text{dR}}(Y \times_{\mathcal{O}_K} K) \cong \left(H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{cris}}\right)^G \otimes_{K_0} K.$$

This is not new with respect to Theorem 6.1; however, we can now go in the other direction:

$$H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_p) \cong (H^n_{\text{cris}}(X/W) \otimes_W B_{\text{cris}})^{\varphi=1} \cap \operatorname{Fil}^0.$$

Definition 6.28 (Crystalline representation, Fontaine)**.** Let V be a finite-dimensional $\mathbb{Q}_p$-representation of G. We define

$$D_{\mathrm{cris}}(V) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^G.$$

The map $V \mapsto D_{\mathrm{cris}}(V)$ defines a functor

$$\{\mathbb{Q}_p\text{-representations of } G\} \to \{\text{filtered } \varphi\text{-modules}\}.$$

We say that V is **crystalline** if the natural map $B_{\mathrm{cris}} \otimes_{K_0} D_{\mathrm{cris}}(V) \to B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V$ is an isomorphism.

Example 6.29.

1. $H^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p)$ is crystalline (Theorem 6.25 and Corollary 6.27).
2. If A is an abelian variety over K, the rational p-adic Tate module $V_p(A) := \left(\varprojlim_n A[p^n]\right) \otimes \mathbb{Q}$ is crystalline if and only if A has good reduction.

Lemma 6.30. *If V is crystalline, then it is de Rham (hence Hodge-Tate).*

Proof. If V is crystalline, then $\dim_{K_0} D_{\mathrm{cris}}(V) = \dim_{\mathbb{Q}_p}(V)$ (easy by replacing B_{cris} with its fraction field in the definition of crystalline representations). On the other hand, $K \otimes_{K_0} B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$, so tensoring with K gives an injective homomorphism

$$K \otimes_{K_0} D_{\mathrm{cris}}(V) \hookrightarrow D_{\mathrm{dR}}(V).$$

Now the argument proceeds 'as usual': one has $\dim_K D_{\mathrm{dR}}(V) \leq \dim_{\mathbb{Q}_p} V = \dim_{K_0} D_{\mathrm{cris}}(V)$, hence the above injection is an isomorphism, and so $\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p}(V)$ and V is de Rham. $\square$

Lemma 6.31. *The functor*

$$D_{\mathrm{cris}} : \{\mathbb{Q}_p\text{-}\textit{representations of } G\} \to \{\textit{filtered } \varphi\textit{-modules}\}$$

is fully faithful.

Proof. Given a map $\psi : D_{\mathrm{cris}}(V) \to D_{\mathrm{cris}}(V')$, we need to construct a map $\psi_V : V \to V'$ inducing ψ. We obtain ψ_V by applying the functor $M \mapsto M^{\varphi=1} \cap \mathrm{Fil}^0$. $\square$

This raises the natural question of describing the essential image of D_{cris}. We'll talk about this next time, using the theory of the Fargues-Fontaine curve.

6.5.1 Construction of B_{cris}

We only give a quick sketch. Consider the ring $W(\mathcal{O}^\flat_{\mathbb{C}_p}) \hookrightarrow W(\mathcal{O}^\flat_{\mathbb{C}_p})[1/p]$. We let A^0_{cris} be the $W(\mathcal{O}^\flat_{\mathbb{C}_p})$-submodule of $W(\mathcal{O}^\flat_{\mathbb{C}_p})[1/p]$ generated by $\frac{\xi^m}{m!}$ for $m \in \mathbb{Z}$. This is a subring. Define A_{cris} as the p-adic completion of A^0_{cris} and set $B^+_{\mathrm{cris}} = A_{\mathrm{cris}}[1/p]$. Finally, we define B_{cris} as $B^+_{\mathrm{cris}}[1/t]$. One should check (nasty topological exercise...) that B_{cris} embeds in B_{dR}.

6.6 Semistable representations

This paragraph is formally very similar to the description of B_{cris} given above. Fontaine constructed a K_0-subalgebra B_{st} of B_{dR}, sitting between B_{cris} and B_{dR}. The ring B_{st} is 'simply' a polynomial ring over B_{cris}. It is equipped with a G-action and a φ-module structure over K_0 extending that of B_{cris}. It further has a monodromy operator $N : B_{\mathrm{st}} \to B_{\mathrm{st}}$ such that $B_{\mathrm{cris}} = \ker N$. (Note that, since B_{st} is generated by a single transcendental element over B_{cris}, the operator N is completely determined by the image of this transcendental element). The natural map

$$K \otimes_{K_0} B_{\mathrm{st}} \to B_{\mathrm{dR}}$$

is injective, so $K \otimes_{K_0} B_{\mathrm{st}}$ inherits a filtration from $\mathrm{Fil}^i B_{\mathrm{dR}}$.

Facts.

1. $B_{\mathrm{st}}^G = K_0$.
2. $B_{\mathrm{st}}^{\varphi=1,N=0} \cap \mathrm{Fil}^0 = \mathbb{Q}_p$.

Now assume $Y/\mathcal{O}_K$ is proper and semistable[2]. Hyodo and Kato constructed cohomology groups $H^n_{\mathrm{HK}}(X/W)$ that are φ-modules over W, equipped with a monodromy operator N. There is an isomorphism

$$H^n_{\mathrm{HK}}(X/W) \otimes_W K \cong H^n_{\mathrm{dR}}(Y \times_{\mathcal{O}_K} K).$$

Theorem 6.32 (Tsuji)**.** *Let $Y/\mathcal{O}_K$ be proper and semistable, $\overline{Y} := Y \times_{\mathcal{O}_K} \overline{K}$, and $X = Y \times_{\mathcal{O}_K} k$. There is a natural isomorphism*

$$H^n_{\mathrm{HK}}(X/W) \otimes_W B_{\mathrm{st}} \cong H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{st}}.$$

This isomorphism is compatible with the actions of G, φ and N, and – after tensoring by K over K_0 – with Fil^i.

There is an obvious definition of semistable representations, and crystalline implies semistable implies de Rham. This gives a fully faithful functor from $\mathbb{Q}_p$-representations of G to filtered (φ, N)-modules.

6.7 Around the semistable reduction conjecture

Motivation. Suppose that $Y/\mathcal{O}_K$ has semistable reduction. Consider the ℓ-adic cohomology groups $H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_\ell)$ for $\ell \neq p$. The inertia group $I \subset G$ acts via its tame quotient $\mathbb{Z}_\ell(1)$ and the images of its elements are unipotent matrices. If A is unipotent, we can define

$$\log(A) := \sum_{m=1}^{\infty} (-1)^{m+1} \frac{(A - \mathrm{Id})^m}{m},$$

which is really a finite sum. The resulting operator is nilpotent, and is called the *monodromy operator* on $H^n_{\text{ét}}(\overline{Y}, \mathbb{Q}_\ell)$. (We apply this to a pro-generator of the image of inertia.) Moreover, Y has good reduction if and only if this operator vanishes.

Grothendieck proved that, if Y/K is proper and smooth, there exists a finite extension K'/K such that $I \cap \mathrm{Gal}(\overline{K}/K')$ acts unipotently. In other words, ℓ-adic cohomology behaves as predicted by the potential semistable reduction conjecture. The next theorem shows that a similar statement holds for all de Rham representations.

[2]see for example `https://stacks.math.columbia.edu/tag/0CDB` for a careful discussion of this notion.

Theorem 6.33 (Berger, André, Kedlaya, Mebkhout)**.** *If V is a de Rham representation of G, there exists a finite extension K' of K such that the restriction to* $\mathrm{Gal}(\overline{\mathbb{Q}_p}/K')$ *is semistable in the sense of Fontaine.*

Remark 6.34. This is Berger's translation of a result obtained independently by André, Kedlaya and Mebkhout in the context of p-adic differential equations.

7 07.03.2024 – The Fargues-Fontaine curve

Let $K/\mathbb{Q}_p$ be a finite extension, with ring of integers $\mathcal{O}_K$ and residue field k. Denote by G the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. We write $W(k) \hookrightarrow \mathcal{O}_K$ for the ring of Witt vectors of k and denote by K_0 the fraction field of $W(k)$. We have a diagram of inclusions

$$\begin{tikzcd} K \arrow[r] & \overline{\mathbb{Q}_p} \arrow[r] & \mathbb{C}_p \\ \mathcal{O}_K \arrow[u] \arrow[r] & \mathcal{O}_{\overline{\mathbb{Q}_p}} \arrow[u] \arrow[r] & \mathcal{O}_{\mathbb{C}_p} \end{tikzcd}$$

There is a canonical surjection $W(\mathcal{O}_{\mathbb{C}_p}^\flat) \twoheadrightarrow \mathcal{O}_{\mathbb{C}_p}$, which after inverting p leads to Fontaine's map

$$\vartheta : W(\mathcal{O}_{\mathbb{C}_p}^\flat)[\frac{1}{p}] \to \mathbb{C}_p,$$

whose kernel is contained in $(p, [p^\flat])$ and is generated by an element ξ. We have introduced the complete DVR

$$B_{\mathrm{dR}}^+ := \varprojlim_r W(\mathcal{O}_{\mathbb{C}_p}^\flat)[\frac{1}{p}]/(\xi^r),$$

whose fraction field is (by definition) B_{dR}. We note that

$$\bigcap_r (\xi^r) = (0)$$

already in $W(\mathcal{O}_{\mathbb{C}_p}^\flat)$, and hence the map $W(\mathcal{O}_{\mathbb{C}_p}^\flat)[1/p] \to B_{\mathrm{dR}}^+$ is injective. We further let

$$A_{\mathrm{cris}}^0 := W(\mathcal{O}_{\mathbb{C}_p}^\flat)\text{-submodule of } W(\mathcal{O}_{\mathbb{C}_p}^\flat)[1/p] \text{ generated by } \{\frac{\xi^m}{m!} \mid m \geq 0\}.$$

This is a subring, and we defined A_{cris} to be the p-adic completion of A_{cris}^0 and $B_{\mathrm{cris}}^+ := A_{\mathrm{cris}}[1/p]$. One can check, by non-trivial calculations, that $A_{\mathrm{cris}}^0 \hookrightarrow B_{\mathrm{dR}}^+$ induces an embedding $A_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}^+$, hence also an embedding $B_{\mathrm{cris}}^+ \hookrightarrow B_{\mathrm{dR}}^+ \hookrightarrow B_{\mathrm{dR}}$. We further defined

$$t := \sum_{n \geq 1} (-1)^{n+1} \frac{([\overline{\omega}] - 1)^n}{n} \in B_{\mathrm{dR}}^+.$$

Lemma 7.1. *The element t is in A_{cris}.*

Proof. We have

$$\vartheta([\overline{\omega}] - 1) = 0,$$

so (since $\ker \vartheta = (\xi)$) we have $[\overline{\omega}] - 1 = b\xi$ for some $b \in W(\mathcal{O}_{\mathbb{C}_p}^\flat)$. This implies

$$\frac{([\overline{\omega}] - 1)^n}{n} = (n-1)! b^n \frac{\xi^n}{n!},$$

and since $(n-1)!$ converges to 0 in the p-adic topology, the series converges and is in the completion of the submodule generated by $\frac{\xi^m}{m!}$, that is, the sum is in A_{cris}. □

Definition 7.2. We let

$$B_{\mathrm{cris}} := B_{\mathrm{cris}}^+[1/t] \hookrightarrow B_{\mathrm{dR}}.$$

Lemma 7.3. *The lift of Frobenius $\varphi : W(\mathcal{O}_{\mathbb{C}_p}^\flat) \to W(\mathcal{O}_{\mathbb{C}_p}^\flat)$ extends to A_{cris}^0.*

Proof. By definition, $\varphi(\xi) \equiv \xi^p \bmod p$, so we can write $\varphi(\xi) = \xi^p + bp$ for some $b \in W(\mathcal{O}_{\mathbb{C}_p}^\flat)$. We write

$$\varphi(\xi) = p\left((p-1)!\frac{\xi^p}{p!} + b\right),$$

so that

$$\varphi\left(\frac{\xi^m}{m!}\right) = \frac{p^m}{m!}\left((p-1)!\frac{\xi^p}{p!} + b\right)^m,$$

which is in $W(\mathcal{O}_{\mathbb{C}_p}^\flat)[\xi^p/p!] \subseteq A_{\mathrm{cris}}^0$. □

Corollary 7.4. *The action of φ extends to $A_{\mathrm{cris}}, B_{\mathrm{cris}}^+$, and $B_{\mathrm{cris}} = B_{\mathrm{cris}}^+[1/t]$.*

Proof. We compute

$$\begin{aligned} \varphi(t) &= \varphi(\log([\overline{\omega}])) = \log([\overline{\omega}]^p) \\ &= \log([\overline{\omega}^p]) = p\log[\overline{\omega}] = p \cdot t. \end{aligned}$$

□

Fact. There is an injective map $K_{K_0} B_{\mathrm{cris}} \to B_{\mathrm{dR}}$.

Taking Galois invariants, we get

$$(K \otimes_{K_0} B_{\mathrm{cris}})^G \hookrightarrow B_{\mathrm{dR}}^G = K,$$

and since $(K \otimes_{K_0} B_{\mathrm{cris}})^G = K \otimes_{K_0} B_{\mathrm{cris}}^G$ we obtain $B_{\mathrm{cris}}^G = K_0$. Recall that B_{dR} is a complete valued field, and the valuation filtration (corresponding to $B_{\mathrm{dR}}^+ \cdot \xi^i$) is denoted by Fil^i.

Fact. $B_{\mathrm{cris}}^{\varphi=1} \cap \mathrm{Fil}^0 B_{\mathrm{dR}} = \mathbb{Q}_p$. Note that $\mathrm{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+$. Moreover,

$$B_{\mathrm{cris}}^{\varphi=p^k} \cap \mathrm{Fil}^0 B_{\mathrm{dR}} = (B_{\mathrm{cris}}^+)^{\varphi=p^k}.$$

There exists an exact sequence

$$0 \to \mathbb{Q}_p \to B_{\mathrm{cris}}^{\varphi=1} \to B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0,$$

coming from similar exact sequences

$$0 \to \mathbb{Q}_p \to B_{\mathrm{cris}}^{\varphi=1} \cap \mathrm{Fil}^i \to \mathrm{Fil}^i B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0 \tag{4}$$

for all $i \leq 0$. These sequences are called the *fundamental sequence of p-adic Hodge theory.*

If V is a finite-dimensional $\mathbb{Q}_p$-representation of G, we defined

$$D_{\mathrm{cris}}(V) = \left(B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V\right)^G.$$

This is a K_0-vector space with a φ-structure (hence it's a φ-module over K_0). Moreover, $D_{\mathrm{cris}}(V) \otimes_{K_0} K$ inherits a filtration from B_{dR}. The representation V is called **crystalline** if the natural map

$$B_{\mathrm{cris}} \otimes_{K_0} D_{\mathrm{cris}}(V) \to B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V$$

is an isomorphism.

Fact. The representation V is crystalline if and only if $\dim_{K_0} D_{\mathrm{cris}}(V) = \dim_{\mathbb{Q}_p} V$.

Fontaine checked that, if V is crystalline, then φ is bijective on $D_{\mathrm{cris}}(V)$.

Fact. The functor

$$\begin{array}{ccc} \{\mathbb{Q}_p\text{-representations of } G\} & \to & \left\{ \begin{array}{c} \text{filtered } \varphi\text{-modules over} \\ K_0 \text{ with bijective } \varphi \end{array} \right\} \\ V & \mapsto & D_{\mathrm{cris}}(V) \end{array}$$

is fully faithful. One can recover V from $D_{\mathrm{cris}}(V) =: D$ as $V = D^{\varphi=1} \cap \mathrm{Fil}^0$. An important question is to characterise the essential image of this functor.

7.1 The curve

Reference. M. Morrow, Séminaire Bourbaki: The Fargues-Fontaine curve and diamonds [Mor19].

7.1.1 Motivation

What is $\mathbb{P}^1_{\mathbb{C}}$? There are many possible constructions and interpretations, of which we list a few:

1. $\mathbb{P}^1_{\mathbb{C}} = \mathbb{A}^1_{\mathbb{C}} \cup \{\infty\}$.

2. Points of $\mathbb{P}^1_{\mathbb{C}}$ correspond to discrete valuations on $\mathbb{C}(z) = \operatorname{Frac} \mathbb{C}[z]$. Under this correspondence, points of $\mathbb{A}^1_{\mathbb{C}}$ correspond to irreducible polynomials in $\mathbb{C}[z]$, and ∞ corresponds to z^{-1}, that is, to the valuation given by $f \mapsto v_\infty(f) = -\deg f$ if $f \in \mathbb{C}[z]$.

3. In algebraic geometry, one defines $\mathbb{P}^1_{\mathbb{C}}$ as $\operatorname{Proj} \mathbb{C}[z_0, z_1]$.

   Remark 7.5. In general, if A is a ring graded by $\mathbb{N}$, points of $\operatorname{Proj}(A)$ correspond to homogeneous prime ideals $P \subset A$ not containing the ideal $A_+ = \bigoplus_{i>0} A_i$. The topology on $\operatorname{Proj} A$ is generated by the basic open sets

   $$D_+(f) = \{P \in \operatorname{Proj}(A) : f \notin P\}.$$

   The structure sheaf is characterised by

   $$\mathcal{O}(D_+(f)) = A_{(f)} = \{\text{elements of degree 0 in the localisation } A_f\}.$$

In the case of the projective line, points of $\mathbb{P}^1_{\mathbb{C}}$ correspond to homogeneous polynomials of degree 1 in z_0, z_1. The affine line is $D_+(z_1)$, and the point at infinity is $V_+(z_1) = \mathbb{P}^1_{\mathbb{C}} \setminus D_+(z_1)$.

4. Define an increasing filtration on $\mathbb{C}[z]$ by taking

$$\operatorname{Fil}_i \mathbb{C}[z] = \{f \in \mathbb{C}[z] : \deg f \leq i\} = \{f \in \mathbb{C}[z] : v_\infty(f) \geq -i\}.$$

As graded rings, we have an isomorphism

$$\mathbb{C}[z_0, z_1] \cong \bigoplus_{i=0}^{\infty} \operatorname{Fil}_i \mathbb{C}[z],$$

where the map is given by sending z_0 to z and z_1 to 1. It follows that

$$\mathbb{P}^1_{\mathbb{C}} = \operatorname{Proj} \mathbb{C}[z_0, z_1] \cong \operatorname{Proj}\left(\bigoplus_{i=0}^{\infty} \operatorname{Fil}_i \mathbb{C}[z]\right).$$

7.1.2 Construction of the curve

Consider $B_{\text{cris}} \subset B_{\text{dR}}$ and denote by v_{dR} the discrete valuation on B_{dR}. Recall that $\operatorname{Fil}^i B_{\text{dR}} = \{x \in B_{\text{dR}} : v_{\text{dR}}(x) \geq i\}$; it's a descending filtration. We define an increasing filtration by

$$\operatorname{Fil}_i = \{x \in B_{\text{dR}} : v(x) \geq -i\}.$$

We still have $\operatorname{Fil}_0 B_{\text{dR}} = \operatorname{Fil}^0 B_{\text{dR}} = B^+_{\text{dR}}$. The fundamental sequences of p-adic Hodge theory (Equation (4)) give

$$B_{\text{cris}}^{\varphi=1} \cap \operatorname{Fil}_i B_{\text{dR}} \cong B_{\text{cris}}^{\varphi=p^i} \cap \operatorname{Fil}_0 B_{\text{dR}} = (B^+_{\text{cris}})^{\varphi=p^i},$$

with the isomorphism induced by $b \mapsto bt^i$ (to see that this makes sense, recall that $t \in \operatorname{Fil}^1 \setminus \operatorname{Fil}^2$ and that $\varphi(t) = pt$). Consider the graded ring

$$\bigoplus_{i=0}^{\infty}\left(B_{\text{cris}}^{\varphi=1} \cap \operatorname{Fil}_i B_{\text{dR}}\right) = \bigoplus_{i=0}^{\infty} (B^+_{\text{cris}})^{\varphi=p^i}.$$

Definition 7.6. The Fargues-Fontaine curve is

$$X^{\text{FF}} := \operatorname{Proj}\left(\bigoplus_{i=0}^{\infty} (B^+_{\text{cris}})^{\varphi=p^i}\right).$$

Fargues and Fontaine proved many properties of their curve:

1. $\bigoplus_{i=0}^{\infty} (B^+_{\text{cris}})^{\varphi=p^i}$ is a UFD and all prime elements are of degree 1, so they lie in $(B^+_{\text{cris}})^{\varphi=p}$. One of these is t, which corresponds to a point $\infty \in X^{\text{FF}}$.

2. $X^{\text{FF}} \setminus \{\infty\} = \operatorname{Spec} B^{\varphi=1}_{\text{cris}}$.

3. X^{FF} is a connected, regular, separated Noetherian scheme of Krull dimension 1 over $\mathbb{Q}_p$, so it 'looks like' a curve. However, it is *not* of finite type.

4. The closed points of X^{FF} (equivalently, all points except for the generic one) are in bijection with

$$\left\{ \begin{array}{c} \text{pairs } (K,\iota), \text{ where } K \text{ is a perfectoid field} \\ \text{such that } K^\flat \cong \mathbb{C}_p^\flat \\ \text{and } \iota \text{ is a fixed isomorphism } K^\flat \cong \mathbb{C}_p^\flat \end{array} \right\} / \sim .$$

The equivalence relation is $(K_1,\iota_1) \sim (K_2,\iota_2)$ if there exists an isomorphism $\rho : K_1 \to K_2$ such that the induced isomorphism $\rho^\flat : K_1^\flat \cong K_2^\flat$ fits in a commutative diagram

$$\begin{tikzcd} \mathbb{C}_p^\flat \arrow[r, "\iota_1"] \arrow[d, "\mathrm{Frob}^r"'] & K_1^\flat \arrow[d, "\rho^\flat"] \\ \mathbb{C}_p^\flat \arrow[r, "\iota_2"'] & K_1^\flat \end{tikzcd}$$

for some r.

7.1.3 Galois representations as vector bundles on the curve

We begin by recalling some basic definitions.

Definition 7.7. A **vector bundle** over a scheme X is a map $V \to X$ which is locally isomorphic to $\mathbb{A}^n \times U \to U$ and such that on the intersections of the elements of the open covering the transition maps are linear. The number n is locally constant; we assume that V is connected, so there is a well-defined global rank n that we denote by $\mathrm{rank}(V)$.

A local section on an open U is a map $U \to V_U$. The set of local sections defines a finitely-generated free $\mathcal{O}_X$-module. Other important invariants are

$$\deg(V) := \deg(\Lambda^n V)$$

and

$$\mu := \mathrm{slope}(V) := \frac{\deg V}{\mathrm{rank}(V)}.$$

We say that a vector bundle V is **semistable** if $\mu(V') \leq \mu(V)$ for every sub-bundle V' of V.

Remark 7.8. If X is a regular curve, then the line bundle $\Lambda^n V$ corresponds to a divisor $\sum n_P P$, and the degree is the sum of the coefficients n_P.

Fargues & Fontaine have classified vector bundles on X^{FF}. They are completely decomposable, and the indecomposable elements are indexed by the rational numbers: for each $r \in \mathbb{Q}$, there is precisely one indecomposable vector bundle V_r with $\mu(V_r) = r$.

Corollary 7.9. *The functor*

$$V \mapsto V \otimes_{\mathbb{Q}_p} \mathcal{O}_{X^{\mathrm{FF}}}$$

defines an equivalence of categories between finite-dimensional $\mathbb{Q}_p$-vector spaces and semistable vector bundles of slope 0 *on X^{FF}.*

Corollary 7.10. *Vector spaces with an action of a group G correspond to semistable vector bundles of slope* 0 *with a G-action.*

We now use this corollary to construct Galois representations starting from filtered φ-modules: with a filter φ-module we associate a vector bundle. If this vector bundle is semistable of rank 0, then it is essentially a vector space, which will be our representation.

Remark 7.11. Vector bundles on $\mathbb{P}^1_{\mathbb{C}}$ are described by:

1. a finitely-generated free $\mathbb{C}[z]$-module M;
2. a finitely-generated free $\mathbb{C}[z^{-1}]$-module M^-;
3. an isomorphism $M \otimes_{\mathbb{C}[z]} \mathbb{C}[z, z^{-1}] \cong M^- \otimes_{\mathbb{C}[z^{-1}]} \mathbb{C}[z, z^{-1}]$.

By flat descent, since $\mathbb{C}[[z^{-1}]]$ is faithfully flat over $\mathbb{C}[z]$, these data can equivalently be encoded by M and a finitely-generated free module M_∞ over $\mathbb{C}[[z^{-1}]]$ together with an isomorphism

$$M \otimes_{\mathbb{C}[z]} \mathbb{C}((z^{-1})) \cong M_\infty \otimes_{\mathbb{C}[[z^{-1}]]} \mathbb{C}((z^{-1})).$$

The same techniques, applied in the context of X^{FF}, give the following. Given:

1. a finitely-generated free $B_{\mathrm{cris}}^{\varphi=1}$-module M;
2. a finitely-generated free B_{dR}^+-module M_{dR};
3. an isomorphism $M \otimes_{B_{\mathrm{cris}}^{\varphi=1}} B_{\mathrm{dR}} \cong M_{\mathrm{dR}} \otimes_{B_{\mathrm{dR}}^+} B_{\mathrm{dR}}$,

we get a vector bundle on X^{FF}.

Remark 7.12. Note that the completion of $\operatorname{Frac} B_{\mathrm{cris}}^{\varphi=1} \subset B_{\mathrm{dR}}$ with respect to the valuation norm on B_{dR} is B_{dR} itself. This follows from the fundamental sequence (4), which shows the density of $B_{\mathrm{cris}}^{\varphi=1}$ in B_{dR}.

Application. Suppose now that D is a filtered φ-module over K_0 that is finitely generated with bijective φ. Recall that the filtration is naturally defined on $D \otimes_{K_0} K$. Consider the pair

$$(M, M_{\mathrm{dR}}) = \left((B_{\mathrm{cris}} \otimes_{K_0} D)^{\varphi=1}, \mathrm{Fil}^0(B_{\mathrm{dR}}^+ \otimes_K (D \otimes_{K_0} K))\right).$$

One checks, using Lemma 2.3 and (4), that the data of D also induces an isomorphism

$$M \otimes_{B_{\mathrm{cris}}^{\varphi=1}} B_{\mathrm{dR}} \cong M_{\mathrm{dR}} \otimes_{B_{\mathrm{dR}}^+} B_{\mathrm{dR}}.$$

We thus get a vector bundle V_D over X^{FF}. This vector bundle has a G-action, coming from the G-action on B_{cris} and on B_{dR}^+. Assume that V_D is semi-stable of slope 0. Corollary 7.10 then gives a $\mathbb{Q}_p$-representation of G, and one checks that, if $D = D_{\mathrm{cris}}(V)$ for a crystalline representation V, then the representation attached to V_D is the V we started with.

Remark 7.13. There is a way to express the condition that V_D is semi-stable of slope 0 purely in terms of D. These are the conditions that Fontaine called *weak admissibility.*

References

[Ax70] James Ax. Zeros of polynomials over local fields—The Galois action. *J. Algebra*, 15:417–428, 1970.

[Mor19] Matthew Morrow. The Fargues-Fontaine curve and diamonds [d'après Fargues, Fontaine, and Scholze]. *Astérisque*, (414):Exp. No. 1150, 533–571, 2019.

[Tat67] J. T. Tate. p-divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin-New York, 1967.