EXPLICIT p-ADIC HODGE THEORY FOR ELLIPTIC CURVES OVER $\mathbb{Q}_p$

DAVIDE LOMBARDO

Abstract. These notes introduce filtered φ-modules, filtered (φ, N)-modules, and filtered modules with descent data through the rank-two examples arising from elliptic curves over p-adic fields. The last part explains how a p-adic Hodge theoretic classification of rational Tate modules of elliptic curves over $\mathbb{Q}_p$, due to Volkov [Vol98], may be used for concrete calculations with Galois representations, as in [BFL26].

Contents

Date: Draft, July 11, 2026.

Introduction

These notes are about the passage from p-adic Galois representations to (semi)linear algebra. They are written *by a non-expert* with a specific objective in mind: understanding explicitly the images of the Galois representations attached to elliptic curves over $\mathbb{Q}_p$.

Specifically, I will try to explain some of the ideas and results in the recent preprint [BFL26]: the theorems proved there are statements about Galois images of elliptic curves, but the mechanism is p-adic Hodge-theoretic. Most of these notes are dedicated to building up the necessary background in p-adic Hodge theory; only the last lecture will be specifically about [BFL26].

0.1. **Motivation.** p-adic Hodge theory is *supposed to be* a tool to describe p-adic representations of the absolute Galois group of a p-adic field. In particular, a result of Volkov [Vol98] uses p-adic Hodge theory to give a classification of the p-adic Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ that arise from the Tate modules of elliptic curves over $\mathbb{Q}_p$. Together with Matthew Bisatt and Lorenzo Furio, we were interested in working out whether it was possible for these representations to have an image of a specific form. Despite having an in principle complete description of the relevant representations in terms of objects called *filtered φ-modules with descent data*, this turned out to be *quite hard*! These lecture notes aim to give an introduction to the objects mentioned above, make sense of the problem, and say something about its solution in [BFL26].

0.2. **What's in this course (and these notes).** I hope to prove a large part of the p-adic Hodge-theoretic classification of Galois representations attached to elliptic curves over $\mathbb{Q}_p$ and show how to compute with them. I also plan to give a gentle introduction to the period rings (specifically, giving a detailed construction of a 'small' period ring, that is still sufficient for our purposes and can serve as a jumping-off point to then study more complicated ones), and I will try to pretend that words like 'crystalline cohomology' aren't really that scary.

Also note that I do not plan to cover in class all the material contained in the notes.

0.3. **What's not in this course.** I won't go into too much detail about period rings, and I will not prove any of the hard comparison theorems between the various cohomological theories. This is all part of the background, and I will take these results for granted. In no way should these notes be considered as a replacement for even the most basic introduction to p-adic Hodge theory; their only purpose is to show some of the relevant objects in action, to possibly motivate the reader to explore them in greater detail.

0.4. **Why 'p-adic Hodge theory'?** It was recently suggested to me that it's useful to explain where the names of certain mathematical concepts or techniques come from. In the case of p-adic Hodge theory, the name reflects the fact that the theory provides p-adic analogues of the comparison phenomena familiar from classical Hodge theory. Its origins lie in Tate's study of p-divisible groups and in the 'Hodge–Tate' decomposition for abelian varieties. Tate's results were later extended to all smooth proper varieties by Faltings [Fal88]. A precise statement is as follows: if X is a smooth proper variety over a finite extension $K/\mathbb{Q}_p$, and $\mathbb{C}_p$ is the p-adic completion of the algebraic closure of K, then there is a canonical isomorphism

$$H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \simeq \bigoplus_{i+j=n} H^j(X, \Omega^i_{X/K}) \otimes_K \mathbb{C}_p(-i).$$

This is formally analogous to the complex Hodge decomposition

$$H^n(X(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \simeq \bigoplus_{i+j=n} H^j(X, \Omega^i_{X/\mathbb{C}}).$$

0.5. **Literature.** The main references I used in preparing these notes are Volkov's works [Vol01, Vol98] and the preprint [BFL26]. General references for the subject are Fontaine's articles on period rings and semistable representations [Fon94a, Fon94b], Colmez–Fontaine's work [CF00] (which in particular gives the proof that weak admissibility implies admissibility), Berger's introductory article [Ber04], and Brinon–Conrad's notes [BC09]. See also Abhinandan's expository thesis [Abh18].

Conventions and standing notation

Throughout the notes, p is a prime number and a *p-adic field* is a finite extension of $\mathbb{Q}_p$. We denote the ring of integers of K by $\mathcal{O}_K$, with maximal ideal $\mathfrak{m}_K$ and residue field k. We choose an algebraic closure $\overline{K}$ of K, write $G_K = \mathrm{Gal}(\overline{K}/K)$, and let $I_K \subseteq G_K$ be the inertia subgroup. The completion of $\overline{K}$ is denoted $\mathbb{C}_p$. We let $K_0 = W(k)[1/p]$ be the fraction field of the Witt vectors of the residue field k; equivalently, K_0 is the maximal unramified subextension of $K/\mathbb{Q}_p$.

All Galois representations in these notes are continuous. A p-adic representation of G_K is a (typically, but not always, finite-dimensional) $\mathbb{Q}_p$-vector space V equipped with a continuous $\mathbb{Q}_p$-linear action of G_K. Given an elliptic curve E/K, we define its Tate module T_pE (respectively rational Tate module V_pE) as

$$T_pE = \varprojlim_n E[p^n](\overline{K}), \qquad V_pE = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

1. p-ADIC REPRESENTATIONS AND ELLIPTIC CURVES

1.1. **What do we do today?** This is a lecture of preliminaries. We introduce Galois representations and recall some basic properties of elliptic curves over local fields, including the definition of their Galois representations. Towards the end, we start introducing the linear algebra objects that classify these Galois representations.

1.2. p-adic representations.

1.2.1. *Local fields and their absolute Galois groups.* A p-adic field K is a finite extension of $\mathbb{Q}_p$. It is complete for a discrete valuation v_K, which we normalise by requiring $v_K(\pi_K) = 1$ for a uniformiser $\pi_K \in \mathcal{O}_K$. The residue field $k = \mathcal{O}_K/\mathfrak{m}_K$ is finite of cardinality $q = p^f$. The extension degree satisfies $[K : \mathbb{Q}_p] = ef$, where $e = e(K/\mathbb{Q}_p)$ is the ramification index, defined by $(p)\mathcal{O}_K = (\pi_K^e)$, and $f = f(K/\mathbb{Q}_p)$ is the residue (or inertia) degree. The absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ fits into a canonical exact sequence

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

The group $\mathrm{Gal}(\bar{k}/k)$ is topologically generated by the *arithmetic Frobenius* $x \mapsto x^q$; the inverse of this element is called the *geometric Frobenius*. The inertia group I_K is related to ramification: for example, $\overline{K}^{I_K} =: K^{\mathrm{ur}}$ is the largest unramified extension of K (contained in the fixed algebraic closure $\overline{K}$). The group I_K contains a pro-p normal subgroup P_K, called the *wild inertia* subgroup.

1.2.2. *Unramified and tamely ramified representations.*

Definition 1.1 (Unramified representation)**.** Let V be a p-adic representation of G_K. We say that V is *unramified* if I_K acts trivially on V. Equivalently, the action of G_K factors through $\mathrm{Gal}(\bar{k}/k)$.

Unramified representations are controlled by a single linear operator, the image of Frobenius. This is the simplest (by far!) instance of a repeated theme: representations of $\mathrm{Gal}(\bar{k}/k)$ can be encoded by a linear algebra object endowed with a "Frobenius" operator. In what follows, this operator will have to be complemented by additional structures. We immediately give a simple example of this: tamely ramified representations.

Definition 1.2 (Tamely ramified representation)**.** Let $P_K \subset I_K$ be the wild inertia subgroup. A p-adic representation V of G_K is called *tamely ramified* if P_K acts trivially on V. Equivalently, the action of G_K on V factors through the tame quotient $G_K^{\mathrm{tame}} := G_K/P_K$.

The tame quotient is only slightly more complicated than the unramified quotient. There is an exact sequence

$$1 \longrightarrow I_K/P_K \longrightarrow G_K/P_K \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

The quotient G_K/P_K is the Galois group of the maximal tamely ramified extension K^{tr}/K. After choosing a uniformiser π_K of K, we have $K^{\mathrm{tr}} = K^{\mathrm{ur}}\big(\pi_K^{1/n} \mid (n,p) = 1\big)$ inside $\overline{K}$.

One can show that I_K/P_K is both pro-cyclic, say with (topological) generator τ, and pro-prime-to-p [Ser79, Chapter IV]. Letting $\Phi \in G_K/P_K$ be a lift of Frobenius (that is, an element in G_K/P_K that maps to Frobenius in $\mathrm{Gal}(\bar{k}/k)$), one has the relation

$$\Phi\tau\Phi^{-1} = \tau^q.$$

Thus a tamely ramified representation is controlled by two pieces of linear algebra: the image of Frobenius and the image of τ. Consequently, a continuous tamely ramified representation is encoded by a finite-dimensional $\mathbb{Q}_p$-vector space V together with two operators

$$F := \rho(\Phi) \in \mathrm{GL}(V), \qquad T := \rho(\tau) \in \mathrm{GL}(V),$$

satisfying

$$FTF^{-1} = T^q. \tag{1}$$

Remark 1.3. In fact, τ and Φ generate a topologically dense subgroup, with presentation $\langle \tau, \Phi \mid \Phi\tau\Phi^{-1} = \tau^q \rangle$.

Exercise 1.4. Let V be a finite-dimensional continuous $\mathbb{Q}_p$-representation of a profinite group G. Prove that V contains a G-stable $\mathbb{Z}_p$-lattice.

Exercise 1.5. Show that the operator T appearing in Equation (1) has finite order prime to p.

Hint. To prove that the order is finite, show – using Exercise 1.4 – that the subgroup generated by $\rho(\tau)$ embeds in $\mathrm{GL}_n(k)$.

This is the next simplest instance of the principle alluded to above: unramified representations are described by a single Frobenius operator; tamely ramified representations are described by a Frobenius operator together with a tame inertia operator, with a single compatibility relation.

The crux of p-adic Hodge theory is to find purely (semi)linear algebra descriptions of more general p-adic Galois representations of G_K, the difficulty being in capturing the action of the wild inertia subgroup P_K. This is hopeless in complete generality, because P_K is too complicated a group. However, we will see that for large classes of 'interesting' representations such a (semi)linear algebra description can indeed be found.

1.3. **Two technical notions: semilinearity and filtrations.**

1.3.1. *Semilinear maps.* The word *semilinear* appears constantly in p-adic Hodge theory, so it is worth recalling the precise definition.

Definition 1.6 (Semilinear map)**.** Let F be a field, let $\sigma : F \to F$ be a field automorphism, and let D and D' be F-vector spaces. A map $u : D \to D'$ is *σ-semilinear* if

$$u(x+y) = u(x) + u(y), \qquad u(ax) = \sigma(a)u(x)$$

for all $a \in F$ and all $x, y \in D$. If $D = D'$ and u is bijective, we call it a σ-semilinear automorphism.

Thus, a semilinear map is additive but not usually F-linear.

Example 1.7 (Semilinear Frobenius)**.** Let k be a perfect field of characteristic p, let[1] $K_0 = W(k)[1/p]$, and let $\sigma : K_0 \to K_0$ be the lift of the automorphism $x \mapsto x^p$ of k. In what follows, a "Frobenius" on a K_0-vector space D will usually be a σ-semilinear automorphism

$$\varphi : D \longrightarrow D.$$

In particular, for $a \in K_0$ and $x \in D$, we have $\varphi(ax) = \sigma(a)\varphi(x)$, not $a\varphi(x)$.

Remark 1.8. Suppose that k is the finite field with $q = p^f$ elements. In this case, $\sigma^f = \mathrm{id}$, and φ^f is σ^f-semilinear, that is, K_0-linear.

Lemma 1.9 (Semilinear maps and matrices)**.** *Let D be a finite-dimensional F-vector space with basis $e_1, \dots, e_d$. A σ-semilinear map $u : D \to D$ is determined by a matrix $A = (a_{ij}) \in \mathrm{Mat}_d(F)$ via*

$$u(e_j) = \sum_i a_{ij} e_i.$$

If x is the column vector of coefficients of $v \in D$ in this basis, then the column vector of $u(v)$ is $A\sigma(x)$, where σ is applied coefficientwise.

Proof. If $v = \sum_j x_j e_j$, then semilinearity gives

$$u(v) = \sum_j \sigma(x_j) u(e_j) = \sum_j \sigma(x_j) \sum_i a_{ij} e_i,$$

so the i-th coordinate of $u(v)$ is $\sum_j a_{ij}\sigma(x_j) = (A\sigma(x))_i$. □

Warning 1.10. The usual operation of conjugating a matrix changes in the semilinear setting. If P is a change-of-basis matrix, then the matrix of a σ-semilinear operator changes by

$$A \longmapsto P^{-1} A \sigma(P), \tag{2}$$

not by $P^{-1}AP$.

Exercise 1.11. Check Equation (2).

[1] here $W(k)$ denotes the ring of Witt vectors over k. In the familiar case $k = \mathbb{F}_{p^n}$, the ring $W(k)$ is the ring of integers of the unique unramified extension of $\mathbb{Q}_p$ of degree n.

1.3.2. *Filtrations.* Another technical notion that is ubiquitous in p-adic Hodge theory is that of a *filtered* vector space.

Definition 1.12 (Filtered vector space)**.** A filtered K-vector space is a K-vector space D_K equipped with a decreasing filtration by K-subspaces

$$\cdots \supseteq \mathrm{Fil}^i D_K \supseteq \mathrm{Fil}^{i+1} D_K \supseteq \cdots$$

indexed by $i \in \mathbb{Z}$. This filtration is required to be *exhaustive*, that is $\bigcup_{i\in\mathbb{Z}} \mathrm{Fil}^i D_K = D_K$, and *separated*, that is $\bigcap_{i\in\mathbb{Z}} \mathrm{Fil}^i D_K = \{0\}$. When D_K is finite-dimensional, these conditions amount to $\mathrm{Fil}^i D_K = D_K$ for $i \ll 0$ and $\mathrm{Fil}^i D_K = 0$ for $i \gg 0$.

Definition 1.13 (Dual filtration)**.** If D_K is a filtered K-vector space, the dual filtration on $D_K^\vee$ is defined by

$$\mathrm{Fil}^i(D_K^\vee) := \left\{ f \in D_K^\vee : f\left(\mathrm{Fil}^{1-i} D_K\right) = 0 \right\}.$$

Remark 1.14. As will be clear later, this definition is motivated by a 'weight philosophy': the weights of the dual filtered vector space $V^\vee$ should be the negatives of the weights of V.

1.4. **Elliptic curves.** We mentioned above that describing general p-adic representations of G_K is hopeless, but that there is a good class for which this is possible. The prototypical example of such representations are those *coming from geometry*. Roughly speaking, these are the representations afforded by the étale cohomology of a smooth proper variety over K. We will focus on the case of elliptic curves, for which these representations can be interpreted in more elementary terms via torsion points. For this reason, we now review some basic properties of elliptic curves over p-adic fields.

1.4.1. *Integral Weierstrass equations.* Let K be a p-adic field. A *generalised Weierstrass equation* for an elliptic curve is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$. If all $a_i \in \mathcal{O}_K$, the equation is called *integral*. Such an equation defines an elliptic curve if its discriminant Δ is non-zero (see [Sil09, §3.1]). The isomorphism class of such an elliptic curve over $\overline{K}$ is completely described by the j-invariant of the equation, which can be computed as a rational function of its coefficients (see again [Sil09, §3.1, especially Proposition 1.4]). A change of variables

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t$$

with $u \in K^\times$ changes the discriminant by $\Delta' = u^{-12}\Delta$. A *minimal Weierstrass equation* is an integral equation for which $v_K(\Delta)$ is minimal among all possible integral Weierstrass equations.

Remark 1.15. When $p > 3$, many discussions can be simplified by using a short Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

in which case we have

$$\Delta = -16(4A^3 + 27B^2), \qquad j = -1728\frac{(4A)^3}{\Delta}.$$

1.4.2. *Reduction of elliptic curves over local fields.* Let E/K be an elliptic curve. Reducing a Weierstrass equation with coefficients in $\mathcal{O}_K$ modulo $\mathfrak{m}_K$ gives a Weierstrass equation over the residue field k. The reduction type of E – that is, the singularities of the curve defined by the reduction of a minimal Weierstrass equation – can be described as follows. Standard references for this material are [Sil09, Chapter VII] and [Sil94, Chapter IV].

Definition 1.16 (Reduction types)**.** An elliptic curve E/K has:

(i) *good reduction* if it has a smooth proper model over $\mathcal{O}_K$ whose special fibre (the curve over k defined by the reduction of the given equations over $\mathcal{O}_K$) is an elliptic curve over k (equivalently, the discriminant of a minimal Weierstrass equation is a unit in $\mathcal{O}_K$);

(ii) *multiplicative reduction* if the identity component of the special fibre of the Néron model is a one-dimensional torus (or, in elementary terms, if the reduction of a minimal Weierstrass equation has a unique singularity which is a node);

(iii) *additive reduction* if the special fibre is neither smooth nor multiplicative (or, in elementary terms, if the reduction of a minimal Weierstrass equation has a unique singularity which is a cusp);
(iv) *semistable reduction* if it has either good or multiplicative reduction.

Definition 1.17. The curve E/K has *potentially good*, *potentially multiplicative*, or *potentially semistable* reduction if it acquires the corresponding reduction type after a finite extension of K.

All elliptic curves over p-adic fields are potentially semistable; equivalently, semistable reduction is always acquired after a finite extension. This is the elliptic curve case of the semistable reduction theorem; for the general theory of Néron models and semistable reduction, see [BLR90].

Definition 1.18 (Semistability defect)**.** Let E/K be an elliptic curve. The *semistability defect* of E/K is the minimal degree

$$e(E/K) = [L : K]$$

among finite extensions L/K for which E_L is semistable. One can always take L/K to be totally ramified. In the case $K = \mathbb{Q}_p$ and $p > 3$, the semistability defect satisfies $e(E/\mathbb{Q}_p) \in \{1, 2, 3, 4, 6\}$.

Remark 1.19. The set $\{1, 2, 3, 4, 6\}$ is not accidental: it is the set of divisors of the possible orders of the automorphism group of an elliptic curve in characteristic p.

When the reduction is good, there is a further distinction that can be made:

Definition 1.20 (Ordinary and supersingular reduction)**.** Suppose E/K has good reduction and residue field k of characteristic p. The special fibre $\tilde{E}/k$ is *ordinary* if $\tilde{E}[p](\bar{k})$ has order p, and *supersingular* if $\tilde{E}[p](\bar{k})$ is trivial.

1.4.3. *Galois representations of elliptic curves.* Let E/K be an elliptic curve. For every integer $N \geq 1$, the N-torsion group[2] $E[N]$ is by definition the subgroup of points of $E(\overline{K})$ having order dividing N. We then have

$$E[N](\overline{K}) := \{P \in E(\overline{K}) : N \cdot P = 0\} \cong (\mathbb{Z}/N\mathbb{Z})^2,$$

because[3] K has characteristic zero and multiplication by N is finite étale over $\overline{K}$. The absolute Galois group G_K acts on $E[N](\overline{K})$ via its action on the coordinates of points, and after choosing a basis of $E[N]$ this gives a representation

$$\rho_{E,N} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

We will mostly be interested in the case where N is a prime power, say $N = \ell^n$, especially when $\ell = p$, the characteristic of the residue field k. Taking $N = \ell^n$ and passing to the inverse limit over n then gives the ℓ-adic representation

$$\rho_{E,\ell^\infty} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Definition 1.21 (Tate module)**.** The ℓ-adic Tate module of E is

$$T_\ell E = \varprojlim_n E[\ell^n](\overline{K}),$$

where the transition maps are multiplication by ℓ. The rational Tate module is

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

We stress again that the most interesting case will be $\ell = p$.

Proposition 1.22. *The module $T_\ell E$ is a free $\mathbb{Z}_\ell$-module of rank 2, and $V_\ell E$ is a two-dimensional ℓ-adic representation of G_K.*

[2]when working in positive characteristic, it is better to think about the *subgroup scheme* $E[N]$, but in characteristic 0 nothing is lost by just considering its $\overline{K}$-points.

[3]for a simpler proof: embed K in $\mathbb{C}$ and use the fact that over $\mathbb{C}$ every elliptic curve is a complex torus to deduce $E[N](\overline{K}) = E[N](\mathbb{C}) \cong (\mathbb{R}/\mathbb{Z})^2[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.

Proof. For every n, the group $E[\ell^n](\overline{K})$ is noncanonically isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. The transition map $E[\ell^{n+1}](\overline{K}) \to E[\ell^n](\overline{K})$ induced by multiplication by ℓ corresponds, after choosing compatible bases, to the natural reduction map $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2 \to (\mathbb{Z}/\ell^n\mathbb{Z})^2$. Hence the inverse limit is free of rank 2 over $\mathbb{Z}_\ell$. The action of G_K on the finite torsion groups is compatible with multiplication by ℓ, hence induces an action on the inverse limit. Continuity of ρ_{E,ℓ^n} follows from the fact that it factors via the Galois group of $K(E[\ell^n])/K$, which is finite (in other words, the extension of K obtained by adjoining the coordinates of all ℓ^n-torsion points is finite over K). Continuity of ρ_{E,ℓ^∞} follows from the definition of the inverse limit topology. □

1.4.4. *The Weil pairing and the determinant.* We now focus on the case $N = p^n$. The Weil pairing gives a perfect alternating pairing

$$e_{p^n} : E[p^n](\overline{K}) \times E[p^n](\overline{K}) \longrightarrow \mu_{p^n}$$

which is *equivariant* with respect to the Galois action, that is,

$$^\sigma(e_{p^n}(P,Q)) = e_{p^n}({}^\sigma P, {}^\sigma Q)$$

for all $\sigma \in G_K$ and all $P, Q \in E[p^n]$. Passing to inverse limits gives a Galois-equivariant pairing

$$e_{p^\infty} : T_pE \times T_pE \longrightarrow T_p\mathbb{G}_m \cong \mathbb{Z}_p(1).$$

Here $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ and $\mathbb{Q}_p(1) = \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Remark 1.23. The multiplicative notation can be confusing at first:

(1) bilinearity means

$$e_{p^n}(aP + bQ, R) = e_{p^n}(P,R)^a e_{p^n}(Q,R)^b;$$

(2) similarly, the alternating property means $e_{p^n}(P,Q) = e_{p^n}(Q,P)^{-1}$.

Definition 1.24 (Cyclotomic character)**.** The p-adic cyclotomic character is the continuous character

$$\chi_p : G_K \longrightarrow \mathbb{Z}_p^\times$$

characterised by the fact that $g(\zeta) = \zeta^{\chi_p(g)}$ holds for every p-power root of unity $\zeta \in \mu_{p^\infty}$.

Proposition 1.25. *For every elliptic curve E/K, the determinant of ρ_{E,p^∞} is the cyclotomic character:*

$$\det \rho_{E,p^\infty} = \chi_p.$$

The same statement holds modulo p^n for ρ_{E,p^n}.

Proof. It suffices to prove the p-adic version of the statement. Choose a $\mathbb{Z}_p$-basis P, Q of T_pE and suppose that $\sigma \in G_K$ acts on P, Q via the matrix $\rho_{E,p^\infty}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using the Galois-equivariance of the Weil pairing, we have

$$^\sigma(e_{p^\infty}(P,Q)) = e_{p^\infty}({}^\sigma P, {}^\sigma Q) = e_{p^\infty}(aP + cQ, bP + dQ);$$

using the fact that e_{p^∞} is alternating and bilinear, from this we obtain

$$\begin{aligned} ^\sigma(e_{p^\infty}(P,Q)) &= e_{p^\infty}(aP + cQ, bP + dQ) \\ &= e_{p^\infty}(P,P)^{ab} e_{p^\infty}(P,Q)^{ad} e_{p^\infty}(Q,P)^{cb} e_{p^\infty}(Q,Q)^{cd} \\ &= e_{p^\infty}(P,Q)^{ad-bc} = e_{p^\infty}(P,Q)^{\det \rho_{E,p^\infty}(\sigma)}. \end{aligned}$$

By definition, $^\sigma(e_{p^\infty}(P,Q)) = (e_{p^\infty}(P,Q))^{\chi_p(\sigma)}$. Since the pairing is perfect, we conclude that $\det \rho_{E,p^\infty}(\sigma) = \chi_p(\sigma)$. □

Remark 1.26. It is customary to write the Galois action on $\mathbb{Z}_p(1)$ and $\mathbb{Q}_p(1)$ as *multiplication* by the cyclotomic character, that is, $^\sigma(x) = \chi_p(\sigma) \cdot x$ for $\sigma \in G_K$ and $x \in \mathbb{Z}_p(1)$. We will use this convention from now on.

1.4.5. *Relation to étale cohomology.* The representation V_pE is closely related to the first étale cohomology of E: specifically, we have

$$H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p) \cong \text{Hom}_{\mathbb{Q}_p}(V_pE, \mathbb{Q}_p).$$

We will use both V_pE and $H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)$ to study the Galois representations attached to E. This leads to slightly different conventions; we will try to be explicit about which one is being used at any given time.

1.5. **What sort of objects are we interested in?**

Warning 1.27. If you've never encountered crystalline or de Rham cohomology before, this paragraph will suddenly feel much more complicated than the rest of the material so far. For the moment, take it simply as informal motivation to consider the semilinear algebra objects that will occupy us in the next lecture.

Let K be a p-adic field and K_0 be its maximal unramified subextension. Roughly speaking, we will work with K_0-vector spaces D equipped with three structures:

(1) a "Frobenius", that is, a bijection $\varphi : D \to D$ that is semilinear with respect to the Frobenius of K_0;
(2) a filtration on $D_K := D \otimes_{K_0} K$;
(3) some "descent data", related to a base-extension from $\mathbb{Q}_p$ to K, which will be encoded by an operator as in (1).

Let $E/\mathbb{Q}_p$ be an elliptic curve with potentially good reduction, let K be a minimal Galois extension of $\mathbb{Q}_p$ such that E_K has good reduction, and let K_0 be as above. Choose a smooth proper model $\mathcal{E}/\mathcal{O}_K$, and write $\widetilde{E}/k$ for its special fibre. The Tate module V_pE is a $G_{\mathbb{Q}_p}$-representation which becomes 'crystalline' upon restriction to G_K. It is dual to $H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$. Whatever 'crystalline cohomology' is, the relevant vector space D will be

$$D = H^1_{\text{cris}}(\widetilde{E}/W(k))[1/p].$$

This is a 2-dimensional K_0-vector space. It carries a Frobenius, coming from the functoriality of crystalline cohomology. Since E was originally defined over $\mathbb{Q}_p$, there is also an action of the Galois group $\text{Gal}(K/\mathbb{Q}_p)$ that gives the descent data. In the next section, we briefly explain where the filtration on D_K comes from.

1.5.1. *Filtration.* The first de Rham cohomology of E_K/K fits into the exact sequence

$$0 \longrightarrow H^0(E, \Omega^1_{E/K}) \longrightarrow H^1_{\text{dR}}(E/K) \longrightarrow H^1(E, \mathcal{O}_E) \longrightarrow 0.$$

Both outer terms are one-dimensional over K. After extension of scalars to K, the comparison theorem between crystalline and de Rham cohomology identifies $D_K = D \otimes_{K_0} K$ with the de Rham cohomology $H^1_{\text{dR}}(E_K/K)$, and this gives D_K its Hodge filtration.

Much of p-adic Hodge theory for elliptic curves is the study of how the 'Hodge line' $H^0(E, \Omega^1_{E/K})$ sits inside $H^1_{\text{dR}}(E/K)$, relative to how Frobenius acts on this space (via the comparison with crystalline cohomology).

2. Filtered φ-modules and admissibility

2.1. **What do we do today?** We describe Fontaine's formalism of 'B-admissible' p-adic Galois representations. We introduce a category of abstract linear algebra objects called *filtered φ-modules*, define functors from p-adic Galois representations to filtered φ-modules, and state an important theorem that identifies the essential image of these functors (the so-called *admissible* modules). The practical consequence is that, in order to describe a Galois representation, one only needs to write down a filtered φ-module with certain easily checked properties.

2.2. Filtered φ-modules.

2.2.1. *Period rings.* Let V be a p-adic representation of G_K. The category of all such representations is far too large to study directly. Fontaine's idea to capture at least part of this category was to introduce certain so-called *period rings* B. These are – typically very large – $\mathbb{Q}_p$-vector spaces with a continuous G_K-action (that is, they are G_K-representations) and are endowed with extra structures, such as a "Frobenius", a filtration, or a "monodromy operator". We will make this more concrete below. One then studies

$$D_B(V) = (B \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

If B is chosen well and V has some nice properties (which are often satisfied by representations of geometric origin), $D_B(V)$ is a finite-dimensional vector space equipped with one or more additional structures (Frobenius, filtration, ...). One may then hope that $D_B(V)$ retains enough information about V that the classification of 'B-nice' (technically: B-admissible) representations reduces to the classification of the possible objects $D_B(V)$, which should hopefully be easier.

We now introduce three (names of) important period rings. The reader interested in the construction may refer to Section 2.7 below. I will say something more about these rings in lecture 4, see Section 4.6.

(i) B_{dR}, the de Rham period ring, a field extension of $\mathbb{Q}_p$ complete with respect to a valuation and endowed with a filtration. Its invariants satisfy $B_{\mathrm{dR}}^{G_K} = K$.
(ii) B_{cris}, the crystalline period ring, equipped with a Frobenius and embedded in B_{dR}, from which it inherits a filtration. Its invariants satisfy $B_{\mathrm{cris}}^{G_K} = K_0$.
(iii) B_{st}, the semistable period ring, equipped with a Frobenius and a monodromy operator N, and embedded in B_{dR} (after choosing a branch of a logarithm). Its invariants satisfy $B_{\mathrm{st}}^{G_K} = K_0$.

The construction of these rings is one of the technical foundations of p-adic Hodge theory; see Fontaine [Fon94a, Fon94b] or the introductory accounts [Ber04, BC09, Car19].

2.2.2. *The period functors.* Let $K/\mathbb{Q}_p$ be a finite extension, let k be its residue field, and let $K_0 = W(k)[1/p]$. As already explained, this is the maximal unramified subextension of K. Let σ be the absolute Frobenius on K_0, i.e., the unique lift of the automorphism $x \mapsto x^p$ of k.

Definition 2.1 (Period functors)**.** Let V be a p-adic representation of G_K. Define

$$D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K},$$

$$D_{\mathrm{cris}}(V) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K}, \qquad D_{\mathrm{st}}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

The vector space $D_{\mathrm{dR}}(V)$ is naturally a filtered K-vector space. The vector space $D_{\mathrm{cris}}(V)$ is a K_0-vector space with σ-semilinear Frobenius, and its scalar extension

$$D_{\mathrm{cris}}(V)_K = K \otimes_{K_0} D_{\mathrm{cris}}(V)$$

has a filtration induced from B_{dR}. The vector space $D_{\mathrm{st}}(V)$ is a K_0-vector space with Frobenius, a monodromy operator N (more on this later), and a filtration after extension of scalars to K.

Warning 2.2. Although B_{cris} is a subring of B_{dR} and therefore inherits the filtration $\mathrm{Fil}^i B_{\mathrm{cris}} = B_{\mathrm{cris}} \cap \mathrm{Fil}^i B_{\mathrm{dR}}$, this does not give the filtration on $D_{\mathrm{cris}}(V)$ in general. More precisely, $D_{\mathrm{cris}}(V)$ is naturally a K_0-vector space, while the 'right' filtration is only defined on $D_K = D_{\mathrm{cris}}(V) \otimes_{K_0} K$. Specifically, the filtration is transported through the isomorphism $D_{\mathrm{cris}}(V) \otimes_{K_0} K \simeq D_{\mathrm{dR}}(V)$ from the filtration

$$\mathrm{Fil}^i D_{\mathrm{dR}}(V) = \big(V \otimes_{\mathbb{Q}_p} \mathrm{Fil}^i B_{\mathrm{dR}}\big)^{G_K}.$$

The naive subspace

$$\left(V \otimes_{\mathbb{Q}_p} \mathrm{Fil}^i B_{\mathrm{cris}}\right)^{G_K} \subset D_{\mathrm{cris}}(V)$$

only records the part of the filtration which descends to K_0. When K/K_0 is ramified, the filtration need not be defined over K_0, and this naive filtration is in general too small.

The following inequalities are fundamental:

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

$$\dim_{K_0} D_{\mathrm{cris}}(V) \leq \dim_{\mathbb{Q}_p} V, \qquad \dim_{K_0} D_{\mathrm{st}}(V) \leq \dim_{\mathbb{Q}_p} V.$$

This motivates the following definitions.

Definition 2.3 (De Rham, crystalline, semistable)**.** Let V be a d-dimensional p-adic representation of G_K and let B be a period ring. We say that V is *B-admissible* if $\dim_{B^{G_K}} (B \otimes_{\mathbb{Q}_p} V)^{G_K} = \dim_{\mathbb{Q}_p} V$. Specific cases of this notion have special names: in particular, we say that V is

(i) *de Rham* if $\dim_K D_{\mathrm{dR}}(V) = d$.
(ii) *crystalline* if $\dim_{K_0} D_{\mathrm{cris}}(V) = d$.
(iii) *semistable* if $\dim_{K_0} D_{\mathrm{st}}(V) = d$.
(iv) *potentially crystalline*, respectively *potentially semistable*, if $V|_{G_L}$ is crystalline, respectively semistable, for some finite extension L/K.

There are inclusions

$$\{\text{crystalline}\} \subseteq \{\text{semistable}\} \subseteq \{\text{de Rham}\}.$$

The p-adic monodromy theorem, conjectured by Fontaine and proved by Berger, says that de Rham representations are potentially semistable [Ber02, Ber04].

Theorem 2.4 (Berger)**.** *Let $K/\mathbb{Q}_p$ be finite. Every de Rham p-adic representation of G_K is potentially semistable.*

Remark 2.5. When V is crystalline, there is a canonical isomorphism $D_{\mathrm{cris}}(V) \otimes_{K_0} K \cong D_{\mathrm{dR}}(V)$, see Section 2.7.5.

2.2.3. *Filtered φ-modules.* As we just saw, for any p-adic representation V, the K_0-vector space $D := (V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})^{G_K}$ is a K_0-vector space endowed with a Frobenius and a filtration on $D \otimes_{K_0} K$. We now define a related linear-algebra category, which captures these formal structures.

Definition 2.6 (Filtered φ-module)**.** A filtered φ-module over K is a triple

$$D = (D, \varphi, \mathrm{Fil}^\bullet D_K)$$

where:

(i) D is a finite-dimensional K_0-vector space;
(ii) $\varphi : D \to D$ is a bijective σ-semilinear map;
(iii) $D_K := K \otimes_{K_0} D$ is equipped with a decreasing, separated, exhaustive filtration by K-subspaces.

A morphism of filtered φ-modules is a K_0-linear map commuting with Frobenius and preserving the filtrations after extension of scalars to K. More explicitly, a morphism

$$u : (D_1, \varphi_1, \mathrm{Fil}^\bullet D_{1,K}) \to (D_2, \varphi_2, \mathrm{Fil}^\bullet D_{2,K})$$

is a K_0-linear map $u : D_1 \to D_2$ such that

$$u \circ \varphi_1 = \varphi_2 \circ u,$$

and for which the map

$$u_K := u \otimes_{K_0} \mathrm{id}_K : D_1 \otimes_{K_0} K \to D_2 \otimes_{K_0} K$$

satisfies $u_K(\mathrm{Fil}^i D_{1,K}) \subseteq \mathrm{Fil}^i D_{2,K}$ for every $i \in \mathbb{Z}$.

Remark 2.7.

(1) The functor D_{cris} from crystalline representations to filtered φ-modules is fully faithful. In particular, it allows one to compute interesting invariants (for example, the endomorphism ring of the representation) on the linear algebra side instead of the representation side.

(2) If V is a crystalline representation, we can recover V from $D_{\mathrm{cris}}(V)$ by the formula

$$V_{\mathrm{cris}}(D) := (B_{\mathrm{cris}} \otimes_{K_0} D)^{\varphi=1} \cap \mathrm{Fil}^0 (B_{\mathrm{dR}} \otimes_K D_K) .$$

Here $B_{\mathrm{cris}} \otimes_{K_0} D$ is viewed inside $B_{\mathrm{dR}} \otimes_K D_K$ via the natural inclusion $B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$. Equivalently,

$$V_{\mathrm{cris}}(D) = \left\{ x \in B_{\mathrm{cris}} \otimes_{K_0} D \ : \ (\varphi_{B_{\mathrm{cris}}} \otimes \varphi_D)(x) = x \text{ and } x \in \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) \right\} .$$

The Galois group G_K acts on this space through its action on the period ring B_{cris}, while acting trivially on D.

Similar comments apply for semistable representations. On the other hand, the functor D_{dR} is not fully faithful (it 'forgets too much information'), see Example 2.12 below.

We give an important definition in the case of de Rham representations. In the next section, we will reinterpret it in terms of the Hodge–Tate period ring.

Definition 2.8 (Hodge–Tate weights for de Rham representations)**.** Let V be a de Rham representation. We define

$$h_i(V) = \dim_K \mathrm{gr}^i D_{\mathrm{dR}}(V),$$

where

$$\mathrm{gr}^i D_{\mathrm{dR}}(V) := \mathrm{Fil}^i D_{\mathrm{dR}}(V) / \mathrm{Fil}^{i+1} D_{\mathrm{dR}}(V).$$

The *Hodge–Tate weights* of V are the integers i for which $h_i(V) \neq 0$, counted with multiplicity $h_i(V)$.

Example 2.9 (Trivial representation)**.** For the trivial representation $\mathbb{Q}_p$, one has

$$D_{\mathrm{cris}}(\mathbb{Q}_p) = K_0 e, \qquad \varphi(e) = e,$$

and

$$\mathrm{Fil}^0(Ke) = Ke, \qquad \mathrm{Fil}^1(Ke) = 0.$$

The unique Hodge–Tate weight is 0.

Example 2.10. Recall that $\mathbb{Q}_p(1)$ is the 1-dimensional representation of G_K corresponding to the cyclotomic character. The filtered φ-module corresponding to $\mathbb{Q}_p(1)$ is one-dimensional. In the convention used here, it is

$$D_{\mathrm{cris}}(\mathbb{Q}_p(1)) = K_0 e, \qquad \varphi(e) = p^{-1} e.$$

One sometimes says that "the Frobenius eigenvalue is p^{-1}": this means simply that, with respect to the basis vector e, the Frobenius endomorphism acts by multiplication by p^{-1}. Since φ is only K_0-semilinear, and not necessarily linear, this gives more precisely

$$\varphi(ae) = \sigma(a) p^{-1} e \qquad \text{for all } a \in K_0,$$

where σ is the arithmetic Frobenius of K_0. If $K_0 = \mathbb{Q}_p$, then $\sigma = \mathrm{id}$, so φ is genuinely linear and p^{-1} is an eigenvalue in the usual sense.

The filtration on $D_{\mathrm{cris}}(\mathbb{Q}_p(1))$ lives in the K-vector space $D_{\mathrm{cris}}(\mathbb{Q}_p(1))_K := D_{\mathrm{cris}}(\mathbb{Q}_p(1)) \otimes_{K_0} K = Ke$, and is given by

$$\mathrm{Fil}^{-1}(Ke) = Ke, \qquad \mathrm{Fil}^0(Ke) = 0.$$

In particular,

$$\mathrm{gr}^{-1} D_{\mathrm{cris}}(\mathbb{Q}_p(1))_K \cong K, \qquad \mathrm{gr}^i D_{\mathrm{cris}}(\mathbb{Q}_p(1))_K = 0 \quad \text{for } i \neq -1.$$

Thus $\mathbb{Q}_p(1)$ has Hodge–Tate weight -1 in this convention.

The dual representation

$$\mathbb{Q}_p(-1) := \mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p(1), \mathbb{Q}_p)$$

corresponds to the dual filtered φ-module. If $e^\vee$ is the dual basis vector, then

$$D_{\mathrm{cris}}(\mathbb{Q}_p(-1)) = K_0 e^\vee, \qquad \varphi(e^\vee) = p\, e^\vee.$$

Applying the definition of dual filtration (Definition 1.13) to $D_K = Ke$ with

$$\mathrm{Fil}^{-1} D_K = D_K, \qquad \mathrm{Fil}^0 D_K = 0,$$

one obtains

$$\mathrm{Fil}^1(Ke^\vee) = Ke^\vee, \qquad \mathrm{Fil}^2(Ke^\vee) = 0.$$

In particular, $\mathbb{Q}_p(-1)$ has Hodge–Tate weight 1.

Example 2.11 (Tate twists)**.** We set $\mathbb{Q}_p(i) := \mathbb{Q}_p(1)^{\otimes i}$ for $i \geq 0$ and $\mathbb{Q}_p(i) := \mathrm{Hom}(\mathbb{Q}_p(-i), \mathbb{Q}_p)$ for $i < 0$. Each of these vector spaces is in a natural way a one-dimensional Galois representation: G_K acts on $\mathbb{Q}_p(i)$ by the i-th power of the cyclotomic character.

Example 2.12 (D_{dR} is not fully faithful)**.** The functor D_{dR} takes Galois representations to filtered vector spaces. We show that it is not fully faithful. Let $K/\mathbb{Q}_p$ be a finite extension, and let

$$\chi_a, \chi_b : G_K \longrightarrow \mathbb{Q}_p^\times$$

be two unramified characters. We describe them by giving their values on (arithmetic) Frobenius: assume that

$$\chi_a(\mathrm{Frob}_K) = a, \qquad \chi_b(\mathrm{Frob}_K) = b,$$

with $a, b \in \mathbb{Z}_p^\times$ and $a \neq b$. The corresponding one-dimensional representations are not isomorphic. In fact, if

$$f : \chi_a \longrightarrow \chi_b$$

is a G_K-equivariant homomorphism, then either $f = 0$ or, since both representations are one-dimensional, f is an isomorphism. But the existence of an isomorphism would imply

$$\chi_a(\mathrm{Frob}_K) = \chi_b(\mathrm{Frob}_K),$$

contradicting $a \neq b$. Hence $\mathrm{Hom}_{G_K}(\chi_a, \chi_b) = 0$. On the other hand, one can check that both χ_a and χ_b are de Rham of Hodge–Tate weight 0. Their de Rham modules are one-dimensional filtered K-vector spaces:

$$D_{\mathrm{dR}}(\chi_a) \simeq K, \qquad D_{\mathrm{dR}}(\chi_b) \simeq K,$$

with filtration

$$\mathrm{Fil}^0 D_{\mathrm{dR}}(\chi_a) = D_{\mathrm{dR}}(\chi_a), \qquad \mathrm{Fil}^1 D_{\mathrm{dR}}(\chi_a) = 0,$$

and similarly for χ_b. Therefore every K-linear map

$$D_{\mathrm{dR}}(\chi_a) \to D_{\mathrm{dR}}(\chi_b)$$

is automatically compatible with the filtration. Thus

$$\mathrm{Hom}_{\mathrm{Fil}_K}\big(D_{\mathrm{dR}}(\chi_a), D_{\mathrm{dR}}(\chi_b)\big) \simeq K.$$

Consequently, the natural map

$$0 = \mathrm{Hom}_{G_K}(\chi_a, \chi_b) \to \mathrm{Hom}_{\mathrm{Fil}_K}\big(D_{\mathrm{dR}}(\chi_a), D_{\mathrm{dR}}(\chi_b)\big) = K$$

is not an isomorphism. In particular D_{dR}, viewed as a functor from de Rham representations to filtered K-vector spaces, is not fully faithful.

2.3. **More on Hodge–Tate weights.** We now explain a different point of view on the Hodge–Tate weights of V. We use again the convention in which the cyclotomic character $\mathbb{Q}_p(1)$ has Hodge–Tate weight -1.

Let $K/\mathbb{Q}_p$ be a finite extension, and let V be a finite-dimensional $\mathbb{Q}_p$-representation of G_K. For each integer i, define the K-vector space

$$D^i_{\mathrm{HT}}(V) := \big(\mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V\big)^{G_K},$$

where $\mathbb{C}_p$ is the p-adic completion of $\overline{K}$, and $\mathbb{C}_p(i) = \mathbb{Q}_p(i) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$. We also put

$$D_{\mathrm{HT}}(V) := \bigoplus_{i \in \mathbb{Z}} D^i_{\mathrm{HT}}(V).$$

Definition 2.13 (Hodge–Tate representation and Hodge–Tate weights)**.** A p-adic representation V of G_K is called *Hodge–Tate* if

$$\sum_{i \in \mathbb{Z}} \dim_K D^i_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p} V.$$

This is the notion of admissibility for the period ring $B_{\mathrm{HT}} := \bigoplus_{i \in \mathbb{Z}} \mathbb{C}_p(i)$. If V is Hodge–Tate, the *Hodge–Tate weights* of V are the integers i such that $D^i_{\mathrm{HT}}(V) \neq 0$, with multiplicity (also called 'Hodge–Tate numbers')

$$h_i(V) := \dim_K D^i_{\mathrm{HT}}(V).$$

Remark 2.14. Equivalently, V is Hodge–Tate if there is a G_K-equivariant decomposition

$$\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \simeq \bigoplus_{i\in\mathbb{Z}} \mathbb{C}_p(-i) \otimes_K D^i_{\mathrm{HT}}(V).$$

With the convention above, the representation $\mathbb{Q}_p(1)$ has Hodge–Tate weight -1. Indeed,

$$D^i_{\mathrm{HT}}(\mathbb{Q}_p(1)) = \big(\mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(1)\big)^{G_K} = \mathbb{C}_p(i+1)^{G_K},$$

which is nonzero precisely when $i = -1$.

Theorem 2.15. *Every de Rham representation is Hodge–Tate. If V is de Rham, then the Hodge–Tate weights can be read off from the filtered K-vector space $D_{\mathrm{dR}}(V)$, as in Definition 2.8. Both statements follow from the fact that the graded ring of B_{dR} is B_{HT}.*

Example 2.16. Let E/K be an elliptic curve. The Hodge filtration on $H^1_{\mathrm{dR}}(E/K)$ has the form

$$0 \subset \mathrm{Fil}^1 H^1_{\mathrm{dR}}(E/K) \subset \mathrm{Fil}^0 H^1_{\mathrm{dR}}(E/K) = H^1_{\mathrm{dR}}(E/K),$$

where

$$\mathrm{Fil}^1 H^1_{\mathrm{dR}}(E/K) = H^0(E, \Omega^1_{E/K})$$

is a one-dimensional K-vector space. Therefore the representation $H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)$ has Hodge–Tate weights 0 and 1. Since the rational Tate module V_pE is dual to $H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)$, it has the dual Hodge–Tate weights 0 and -1.

Remark 2.17. One should be careful about conventions. Some authors define Hodge–Tate weights with the opposite sign, so that $\mathbb{Q}_p(1)$ has weight $+1$. Most modern sources seem to agree on the convention that the Hodge–Tate weight of $\mathbb{Q}_p(1)$ is -1.

2.4. **Filtered (φ, N)-modules.** The linear algebra objects corresponding to semistable representations require one more operator.

Definition 2.18 (Filtered (φ, N)-module)**.** A filtered (φ, N)-module over K is a quadruple

$$D = (D, \varphi, N, \mathrm{Fil}^\bullet D_K)$$

where

- D is a finite-dimensional K_0-vector space,
- $\varphi : D \to D$ is a bijective σ-semilinear map,
- $N : D \to D$ is a nilpotent K_0-linear map satisfying the relation

$$N\varphi = p\varphi N, \tag{3}$$

- and $D_K = K \otimes_{K_0} D$ is equipped with a decreasing, separated, exhaustive filtration.

The operator N is called *monodromy*. Crystalline objects are the special case $N = 0$.

Remark 2.19. The factor in the relation (3) is p, not $q = \#k$, because φ denotes the lift of the absolute p-power (and not q-power) Frobenius on K_0. If k has cardinality $q = p^f$, then φ^f is K_0-linear, and iterating the relation gives

$$N\varphi^f = p^f \varphi^f N = q\varphi^f N.$$

Thus the factor q appears if one works with the K_0-linear Frobenius φ^f, rather than with the semilinear Frobenius φ.

Remark 2.20. It can be helpful to think of N as the infinitesimal version of a unipotent operator. If one writes formally $T(t) := \exp(tN)$ (which converges for every t, because N is nilpotent), then the relation $N\varphi = p\varphi N$ implies $T(t)\varphi = \varphi T(pt)$, or equivalently, $\varphi^{-1}T(t)\varphi = T(pt)$. This resembles the relation between Frobenius and tame inertia in the tame quotient of a local Galois group. If instead one uses the K_0-linear operator φ^f, where $q = p^f$, then the corresponding relation is $T(t)\varphi^f = \varphi^f T(qt)$, or equivalently

$$(\varphi^f)^{-1}T(t)\varphi^f = T(qt) = T(t)^q,$$

which is very analogous to (1). Note however that in the formula above we have $(\varphi^f)^{-1}$ where in (1) we have F – in other words, the formulas differ by an inversion. This is not a coincidence: the Frobenius operator on D is essentially the *geometric* Frobenius, which is the inverse of the arithmetic Frobenius appearing in (1).

2.5. **Admissibility.**

2.5.1. *The Hodge number.* Not every filtered φ-module D arises from an actual crystalline representation V of G_K as $D \cong D_{\mathrm{cris}}(V)$. Those φ-modules that do are called *admissible*, and one of the big successes of p-adic Hodge theory is to have given a purely linear-algebraic condition for admissibility.

Admissibility of a filtered φ-module D is expressed by comparing the *Hodge number* and the *Newton number* of every subobject of D. We start by defining the Hodge number.

Definition 2.21 (Hodge number)**.** Let D be a filtered φ-module over K. Its *Hodge number* is

$$t_H(D) = \sum_{i \in \mathbb{Z}} i \cdot \dim_K \mathrm{gr}^i(D_K),$$

where $\mathrm{gr}^i(D_K) = \mathrm{Fil}^i D_K / \mathrm{Fil}^{i+1} D_K$. If $D' \subseteq D$ is a φ-stable K_0-subspace, then $D'_K = K \otimes_{K_0} D'$ inherits a filtration by $\mathrm{Fil}^i D'_K = D'_K \cap \mathrm{Fil}^i D_K$, so D' is itself a filtered φ-module, and $t_H(D')$ is defined using this induced filtration.

Example 2.22. Suppose D_K is two-dimensional and

$$\mathrm{Fil}^0 D_K = D_K, \qquad \mathrm{Fil}^1 D_K = \ell, \qquad \mathrm{Fil}^2 D_K = 0,$$

where $\ell \subset D_K$ is a line (a 1-dimensional subspace). Then we have $\mathrm{gr}^0 D_K = D_K/\ell$ and $\mathrm{gr}^1 D_K = \ell$, so

$$t_H(D) = 0 \cdot 1 + 1 \cdot 1 = 1.$$

This is the shape of the filtration for the filtered φ-modules coming from the Galois representations of elliptic curves.

2.5.2. *The Newton number.* Let D be a finite-dimensional K_0-vector space with bijective σ-semilinear Frobenius φ. If $K_0 = \mathbb{Q}_p$, then φ is linear and one can define the Newton number as $v_p(\det \varphi)$. For general K_0, one can use the K_0-linear map φ^f, where $f = [K_0 : \mathbb{Q}_p]$ (see Remark 1.8).

Definition 2.23 (Newton number)**.** Let $f = [K_0 : \mathbb{Q}_p]$. The Newton number of D is

$$t_N(D) = \frac{1}{f} v_p\big(\det_{K_0}(\varphi^f)\big),$$

where $v_p(p) = 1$. If $D' \subseteq D$ is a φ-stable subspace, then $t_N(D')$ is defined similarly.

2.5.3. *Weak admissibility and admissibility.*

Definition 2.24 (Weakly admissible filtered φ-module)**.** A filtered φ-module D over K is *weakly admissible* if:

(i) $t_H(D) = t_N(D)$;
(ii) for every nonzero φ-stable K_0-subspace $D' \subseteq D$, one has $t_H(D') \leq t_N(D')$.

Definition 2.25 (Admissible filtered φ-module)**.** A filtered φ-module D is *admissible* if there exists a crystalline representation V of G_K such that $D \cong D_{\mathrm{cris}}(V)$ as filtered φ-modules.

The terminology is historical: weak admissibility is a condition one can check on linear algebra, while admissibility means coming from a representation. Fontaine proved that admissible implies weakly admissible. The converse is a theorem of Colmez–Fontaine.

Theorem 2.26 (Colmez–Fontaine [CF00])**.** *Every weakly admissible filtered φ-module is admissible. Equivalently, the essential image of D_{cris} (applied to crystalline representations) is precisely the category of weakly admissible filtered φ-modules.*

There is an analogue for semistable representations, which uses filtered (φ, N)-modules and a similar weak admissibility criterion (the definition is the same, but one should look at subobjects that are stable under both φ and N).

Remark 2.27. Theorem 2.26 is surprising because weak admissibility is a finite-dimensional numerical condition, while admissibility amounts to the existence of a Galois representation. In practice, the theorem allows one to construct representations by describing weakly admissible filtered modules.

2.5.4. *Newton and Hodge polygons.* We now give a different interpretation of weak admissibility, in terms of certain polygons (or, more precisely, polygonal chains) in the plane. Let D be a filtered φ-module over K. Thus D is a finite-dimensional K_0-vector space, $\varphi : D \to D$ is a bijective σ-semilinear map, and $D_K := D \otimes_{K_0} K$ is equipped with a decreasing, separated, exhaustive filtration.

First consider the Frobenius. Since φ is usually only σ-semilinear, it need not have eigenvalues in the ordinary sense. As in Remark 1.8, φ^f is a K_0-linear automorphism of D. If $\alpha_1, \dots, \alpha_d$ are the eigenvalues of φ^f in an algebraic closure of K_0, counted with multiplicity, we define the *Newton slopes* of D as

$$\lambda_j := \frac{1}{f} v_p(\alpha_j), \qquad j = 1, \dots, d.$$

As above, the *Newton number* of D is

$$t_N(D) := \sum_{j=1}^{d} \lambda_j = \frac{1}{f} v_p\big(\det_{K_0}(\varphi^f)\big).$$

The *Newton polygon* is the polygonal chain in the plane whose initial point is $(0,0)$ and whose successive slopes are the Newton slopes $\lambda_1, \dots, \lambda_d$, arranged in nondecreasing order. Thus, if

$$\lambda_1 \le \lambda_2 \le \cdots \le \lambda_d,$$

then the vertices of the Newton polygon are

$$\left(r, \sum_{j=1}^{r} \lambda_j \right), \qquad r = 0, \dots, d.$$

In particular, its endpoint is $(d, t_N(D))$.

Now consider the filtration. For each integer i, put

$$h_i(D) := \dim_K \operatorname{gr}^i D_K = \dim_K \left(\operatorname{Fil}^i D_K / \operatorname{Fil}^{i+1} D_K \right)$$

and recall that the *Hodge number* of D is

$$t_H(D) := \sum_{i \in \mathbb{Z}} i\, h_i(D).$$

The *Hodge polygon* is the polygon whose initial point is $(0,0)$ and whose successive slopes are the integers i, each repeated $h_i(D)$ times, again arranged in nondecreasing order. Its endpoint is therefore $(d, t_H(D))$.

Geometrically, the equality $t_H(D) = t_N(D)$ says that the Hodge and Newton polygons have the same endpoint. The inequalities for subobjects can be shown to be equivalent to the statement that the Newton polygon lies on or above the Hodge polygon.

Example 2.28 (Rank two with Hodge weights 0 and 1)**.** Suppose $\dim D = 2$ and the filtration has

$$\dim_K \operatorname{gr}^0 D_K = 1, \qquad \dim_K \operatorname{gr}^1 D_K = 1.$$

Then the Hodge polygon has slopes 0 and 1, so its vertices are

$$(0,0), \qquad (1,0), \qquad (2,1).$$

If the Newton slopes are also 0 and 1, the Newton polygon coincides with the Hodge polygon. This is the shape one sees for the first cohomology of an elliptic curve with good ordinary reduction. If the Newton slopes are both $1/2$, the Newton polygon is the straight line from $(0,0)$ to $(2,1)$. It lies above the Hodge polygon and has the same endpoint; this is the shape one sees for the first cohomology of an elliptic curve with supersingular good reduction.

2.6. **Examples.**

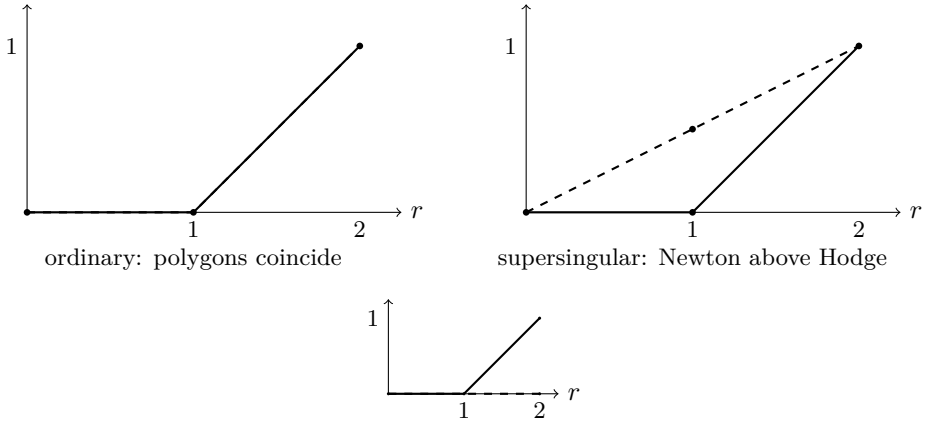

FIGURE 1. Three rank-two pictures. Solid lines indicate Hodge polygons; dashed lines indicate Newton polygons. In the first example the Hodge and Newton polygons coincide. In the second they have the same endpoint and the Newton polygon lies above the Hodge polygon. In the third the endpoints are different, so weak admissibility fails.

2.6.1. *Rank one.* The simplest admissibility computations happen for one-dimensional objects.

Proposition 2.29 (Rank-one weak admissibility)**.** *Assume $K_0 = \mathbb{Q}_p$. Let $D = \mathbb{Q}_p e$ and let $\varphi(e) = ae$ with $a \in \mathbb{Q}_p^\times$. The filtration on $D_K = Ke$ is determined by an integer h:*

$$\mathrm{Fil}^i D_K = \begin{cases} D_K, & i \leq h, \\ 0, & i > h. \end{cases}$$

Then D is weakly admissible if and only if $h = v_p(a)$.

Proof. Since D has no nonzero proper subobjects, weak admissibility is just the equality $t_H(D) = t_N(D)$. The graded vector space has a single one-dimensional graded piece in degree h, so $t_H(D) = h$. The Newton number is $t_N(D) = v_p(a)$. Hence weak admissibility is equivalent to $h = v_p(a)$. □

Example 2.30. The trivial representation has $a = 1$ and $h = 0$. The representation $\mathbb{Q}_p(1)$ has $a = p^{-1}$ and $h = -1$ in the cohomological convention.

2.6.2. *Rank two.* Potentially supersingular elliptic curves will give rise to rank-two modules whose Frobenius is fixed while the Hodge line varies. The following toy calculation captures the idea.

Proposition 2.31. *Assume $K = K_0 = \mathbb{Q}_p$. Let $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$ and suppose*

$$\varphi(e_1) = e_2, \qquad \varphi(e_2) = -pe_1.$$

Let $\ell \subset D$ be a line, and define a filtration by

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \ell, \qquad \mathrm{Fil}^2 D = 0.$$

Then $t_H(D) = t_N(D) = 1$. Since φ has no stable line over $\mathbb{Q}_p$, the module D is weakly admissible for every choice of ℓ.

Proof. The matrix of φ in the basis (e_1, e_2) is $\begin{pmatrix} 0 & -p \\ 1 & 0 \end{pmatrix}$, whose determinant is p. Hence $t_N(D) = v_p(p) = 1$. The filtration has graded pieces of dimensions 1 in degrees 0 and 1, hence $t_H(D) = 1$.

It remains to check subobjects. Since the characteristic polynomial of φ is $X^2 + p$, which has no roots in $\mathbb{Q}_p$, there are no φ-stable lines. A nonzero proper φ-stable subobject would in particular be a φ-stable line, so none exists. Thus there are no nonzero proper subobjects to test, and the equality for D proves weak admissibility. □

Remark 2.32. In the applications below, we will encounter a similar module over $\mathbb{Q}_{p^2}$ with descent data. In the next exercise (and in the next lecture) we will see that the modules described in Proposition 2.31 are all pairwise isomorphic, independently of the choice of the line ℓ. By contrast, the modules over $\mathbb{Q}_{p^2}$ we will encounter later (for which the filtration will be defined over a certain Galois extension $K/\mathbb{Q}_p$ strictly containing $\mathbb{Q}_{p^2}$) will give uncountably many distinct isomorphism classes.

Exercise 2.33. Show that all the filtered φ-modules described in Proposition 2.31 are isomorphic to one another, independently of the choice of the line ℓ.

2.7. **Appendix: a slightly less short introduction to the period rings.** This appendix gives a slightly more extended introduction to the period rings. We will say more about the construction of B_{dR} in two lectures.

2.7.1. *The tilt and the Fontaine map.* Let $\mathbb{C}_p$ be the p-adic completion of $\overline{\mathbb{Q}}_p$, and let $\mathcal{O}_{\mathbb{C}_p}$ be its ring of integers. The *tilt* of $\mathcal{O}_{\mathbb{C}_p}$ is

$$\mathcal{O}_{\mathbb{C}_p}^\flat = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p}.$$

Thus an element of $\mathcal{O}_{\mathbb{C}_p}^\flat$ is a sequence

$$x = (x_0, x_1, x_2, \ldots)$$

with $x_n \in \mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p}$ and $x_{n+1}^p = x_n$. The ring $\mathcal{O}_{\mathbb{C}_p}^\flat$ is a perfect valuation ring of characteristic p. One then forms $A_{\mathrm{inf}} = W(\mathcal{O}_{\mathbb{C}_p}^\flat)$, the ring of p-typical Witt vectors of $\mathcal{O}_{\mathbb{C}_p}^\flat$. This ring has a Frobenius induced by Frobenius on $\mathcal{O}_{\mathbb{C}_p}^\flat$. There is a canonical surjective map

$$\theta : A_{\mathrm{inf}} \longrightarrow \mathcal{O}_{\mathbb{C}_p},$$

which on Teichmüller representatives is described by $\theta([x]) = x^\sharp$. Here the *multiplicative untilt* $x^\sharp$ is defined as follows: given $x = (x_0, x_1, \ldots)$, choose arbitrary lifts $\hat{x}^{(n)} \in \mathcal{O}_{\mathbb{C}_p}$ of x_n; then

$$x^\sharp = \lim_{n \to \infty} \left(\hat{x}^{(n)}\right)^{p^n}.$$

The kernel of θ is a principal ideal.

2.7.2. *The de Rham period ring.* The ring B_{dR}^+ is the $\ker(\theta)$-adic completion of $A_{\mathrm{inf}}[1/p]$. It is a complete discrete valuation ring, and its fraction field is $B_{\mathrm{dR}} = B_{\mathrm{dR}}^+[1/t]$, where t is a suitable generator of the maximal ideal. More precisely, the element t can be obtained from a compatible system of p-power roots of unity. Choose

$$\varepsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in \mathcal{O}_{\mathbb{C}_p}^\flat,$$

where $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Then $t = \log([\varepsilon])$ is an element of B_{dR}^+ satisfying $g(t) = \chi_p(g)t$ for $g \in G_K$. The powers of t define the de Rham filtration:

$$\mathrm{Fil}^i B_{\mathrm{dR}} = t^i B_{\mathrm{dR}}^+ \quad (i \in \mathbb{Z}). \tag{4}$$

2.7.3. *The crystalline period ring.* Choose a generator $\xi \in \ker(\theta)$. For example, if $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in \mathcal{O}_{\mathbb{C}_p}^\flat$ is a compatible system of p-power roots of unity and $\mu = [\varepsilon] - 1$, then one may take $\xi = \frac{\mu}{\varphi^{-1}(\mu)}$.

The ring A_{cris} is the closure of the subring of B_{dR}^+ generated by A_{inf} and by the divided powers

$$\frac{\xi^n}{n!}, \qquad n \geq 1.$$

Definition 2.34 (Crystalline period ring)**.** The positive crystalline period ring is

$$B_{\mathrm{cris}}^+ := A_{\mathrm{cris}}[1/p].$$

Let

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

This element belongs to B_{cris}^+ and satisfies $\varphi(t) = pt$. It generates the maximal ideal $\mathrm{Fil}^1 B_{\mathrm{dR}}^+ = \ker(\theta : B_{\mathrm{dR}}^+ \to \mathbb{C}_p)$. The crystalline period ring is

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

The ring B_{cris} carries the following structures.

(i) *Galois action.* The natural action of G_K on $\mathcal{O}_{\mathbb{C}_p}$ induces an action on $\mathcal{O}_{\mathbb{C}_p}^\flat$, hence on $A_{\mathrm{inf}} = W(\mathcal{O}_{\mathbb{C}_p}^\flat)$. This action extends continuously to A_{cris}, to B_{cris}^+, and to B_{cris}.

(ii) *Frobenius.* Since $\mathcal{O}^\flat_{\mathbb{C}_p}$ is perfect of characteristic p, it has a Frobenius automorphism. This induces a (Witt vector) Frobenius on A_{inf}. The Frobenius extends to A_{cris} and hence to B^+_{cris} and B_{cris}. We denote it by
$$\varphi : B_{\mathrm{cris}} \longrightarrow B_{\mathrm{cris}}.$$
It satisfies $\varphi(t) = pt$.

(iii) *Embedding into B_{dR}.* The construction gives a natural G_K-equivariant embedding $B^+_{\mathrm{cris}} \hookrightarrow B^+_{\mathrm{dR}}$, and therefore an embedding $B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$. Through this embedding, B_{cris} inherits a filtration from B_{dR}:
$$\mathrm{Fil}^i B_{\mathrm{cris}} := B_{\mathrm{cris}} \cap \mathrm{Fil}^i B_{\mathrm{dR}}.$$

The fixed ring of B_{cris} is the maximal unramified subfield: $B_{\mathrm{cris}}^{G_K} = K_0$.

Definition 2.35. For a p-adic representation V of G_K, define
$$D_{\mathrm{cris}}(V) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$
It is a K_0-vector space that carries

(i) a Frobenius φ, induced by Frobenius on B_{cris};
(ii) a filtration on $D_{\mathrm{cris}}(V)_K := D_{\mathrm{cris}}(V) \otimes_{K_0} K$, induced by the embedding $B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$.

2.7.4. *The semistable period ring.* The semistable period ring is obtained from B_{cris} by adjoining one "logarithmic variable". Choose a uniformiser π_K of K, and choose a compatible system
$$\underline{\pi} = (\pi_0, \pi_1, \pi_2, \ldots)$$
of p-power roots of π_K, meaning that $\pi_0 = \pi_K$ and $\pi_{n+1}^p = \pi_n$ for all $n \geq 0$. Thus $\pi_n^{p^n} = \pi_K$. For $g \in G_K$, the two systems $g(\underline{\pi})$ and $\underline{\pi}$ differ by a compatible system of p-power roots of unity. More precisely, there is a unique element
$$\underline{\xi}(g) = (\xi_0(g), \xi_1(g), \xi_2(g), \ldots) \in \mathbb{Z}_p(1)$$
such that
$$g(\pi_n) = \xi_n(g)\pi_n \qquad \text{for all } n \geq 0.$$
Here $\xi_0(g) = 1$, $\xi_n(g) \in \mu_{p^n}$, and $\xi_{n+1}(g)^p = \xi_n(g)$. The map $g \mapsto \underline{\xi}(g)$ is the *Kummer cocycle* attached to the uniformiser π_K.

The informal picture is that the new variable should behave like a logarithm of $\underline{\pi}$. If g multiplies $\underline{\pi}$ by $\underline{\xi}(g)$, then this logarithm should change *additively* by the logarithm of $\underline{\xi}(g)$. Similarly, $\varphi(\underline{\pi}) = \underline{\pi}^p = (\pi_0^p, \pi_1^p, \ldots)$, so φ should act on the logarithm of $\underline{\pi}$ by multiplying it by p.

In Fontaine's rings this is made precise using Teichmüller representatives. The element $\underline{\pi}$ defines an element of A_{inf}, hence a Teichmüller lift $[\underline{\pi}]$. Similarly, $\underline{\xi}(g)$ has a Teichmüller lift $[\underline{\xi}(g)]$. The logarithm $\log([\underline{\xi}(g)])$ makes sense as an element of B_{cris}; after choosing a compatible system of p-power roots of unity, it is a $\mathbb{Z}_p$-multiple of t.

Abstractly, one defines $B_{\mathrm{st}} = B_{\mathrm{cris}}[u]$. The Galois action on B_{cris} extends to B_{st} by the formula
$$g(u) = u + \log([\underline{\xi}(g)]).$$
The Frobenius and monodromy operator are defined by
$$\varphi(u) = pu, \qquad N(u) = 1, \qquad N|_{B_{\mathrm{cris}}} = 0;$$
N is extended by requiring it to be the unique B_{cris}-derivation determined by $N(u) = 1$.

Warning 2.36. Note that N is a *derivation*, not a ring homomorphism. For example, $N(u^2) = 2uN(u) = 2u$.

With this normalisation, one has
$$N\varphi = p\varphi N.$$
Indeed, both sides send u to p, and the equality is already true on B_{cris} because N vanishes there. The same choice of $\underline{\pi}$ gives an embedding
$$\iota_{\underline{\pi}} : B_{\mathrm{st}} \hookrightarrow B_{\mathrm{dR}} :$$

this is the embedding already discussed on $B_{\mathrm{cris}} \subset B_{\mathrm{dR}}$, and it sends the variable u to $\log\left(\frac{[\underline{\pi}]}{\pi_K}\right) \in B_{\mathrm{dR}}^+$. This expression makes sense because $\theta\left(\frac{[\underline{\pi}]}{\pi_K}\right) = 1$, so the quotient lies in $1 + \ker(\theta)$ and its logarithm converges in B_{dR}^+. The formula for the Galois action above is chosen precisely so that $\iota_{\underline{\pi}}$ is G_K-equivariant: applying g gives

$$g \log\left(\frac{[\underline{\pi}]}{\pi_K}\right) = \log\left(\frac{[g(\underline{\pi})]}{\pi_K}\right) = \log([\underline{\xi}(g)]) + \log\left(\frac{[\underline{\pi}]}{\pi_K}\right).$$

Through this embedding, B_{st} inherits a filtration from B_{dR}:

$$\mathrm{Fil}^i B_{\mathrm{st}} := B_{\mathrm{st}} \cap \mathrm{Fil}^i B_{\mathrm{dR}}.$$

Finally, the ring of invariants is $B_{\mathrm{st}}^{G_K} = K_0$.

Remark 2.37. The construction depends on the choice of the compatible system $\underline{\pi}$, and the embedding into B_{dR} depends on that choice. However, the resulting category of semistable representations and the filtered (φ, N)-modules attached to them do not depend on this choice.

Definition 2.38. For a p-adic representation V of G_K, define

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

It is a K_0-vector space that carries

(i) a Frobenius φ, induced by Frobenius on B_{st};
(ii) a monodromy operator N, induced by the derivation N on B_{st};
(iii) a filtration on $D_{\mathrm{st}}(V)_K := D_{\mathrm{st}}(V) \otimes_{K_0} K$, induced by the embedding $B_{\mathrm{st}} \hookrightarrow B_{\mathrm{dR}}$.

These structures satisfy $N\varphi = p\varphi N$.

2.7.5. *Relation between D_{dR} and D_{cris}.* Finally, we discuss the isomorphism $D_{\mathrm{cris}}(V) \otimes_{K_0} K \cong D_{\mathrm{dR}}(V)$ which, as we discussed, is used to define a filtration on $D_{\mathrm{cris}}(V) \otimes_{K_0} K$. Recall that, given a p-adic representation V of G_K, we have set

$$D_{\mathrm{cris}}(V) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K} \qquad \text{and} \qquad D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

The inclusion $B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$ gives a natural K-linear map

$$\iota_V : D_{\mathrm{cris}}(V) \otimes_{K_0} K \longrightarrow D_{\mathrm{dR}}(V).$$

Explicitly, if $d \in D_{\mathrm{cris}}(V)$ and $c \in K$, then

$$\iota_V(d \otimes c) = c\, d,$$

where d is regarded as an element of $B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ via the inclusion $B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V \subset B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$. This element is G_K-invariant, because d is G_K-invariant and G_K fixes K inside B_{dR}.

Now assume that V is crystalline. By definition, the natural map

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

is an isomorphism. Extending scalars along $B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$, we obtain a B_{dR}-linear, G_K-equivariant isomorphism

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

Since

$$B_{\mathrm{dR}} \otimes_{K_0} D_{\mathrm{cris}}(V) \cong B_{\mathrm{dR}} \otimes_K \big(D_{\mathrm{cris}}(V) \otimes_{K_0} K\big),$$

taking G_K-invariants gives

$$\big(B_{\mathrm{dR}} \otimes_K \big(D_{\mathrm{cris}}(V) \otimes_{K_0} K\big)\big)^{G_K} \cong D_{\mathrm{dR}}(V).$$

When we consider the left-hand side, we see that G_K acts only on B_{dR}, and $B_{\mathrm{dR}}^{G_K} = K$. Hence we have

$$\big(B_{\mathrm{dR}} \otimes_K \big(D_{\mathrm{cris}}(V) \otimes_{K_0} K\big)\big)^{G_K} = D_{\mathrm{cris}}(V) \otimes_{K_0} K,$$

which implies

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

This isomorphism is precisely the map ι_V defined above.

3. Filtered φ-modules of elliptic curves

3.1. **What do we do today?** We describe the filtered φ-modules attached to the Galois representations of elliptic curves in terms of their (de Rham and crystalline) cohomology. We also describe the filtered φ-modules more explicitly for the cases of good and multiplicative reductions.

3.2. **Algebraic de Rham cohomology.** Let K be a field of characteristic 0, and let X/K be a smooth proper variety. The algebraic de Rham cohomology of X is the hypercohomology of the algebraic de Rham complex:

$$H^i_{\mathrm{dR}}(X/K) := \mathbb{H}^i(X, \Omega^\bullet_{X/K}).$$

Here $\Omega^\bullet_{X/K}$ denotes the complex $\mathcal{O}_X \to \Omega^1_{X/K} \to \Omega^2_{X/K} \to \cdots$, with the usual exterior derivative. For smooth proper varieties in characteristic 0, these are finite-dimensional K-vector spaces, functorial in X: a morphism $f : X \to Y$ induces a pullback map $f^* : H^i_{\mathrm{dR}}(Y/K) \to H^i_{\mathrm{dR}}(X/K)$.

The de Rham complex carries a decreasing filtration by truncation. Namely, one puts $\mathrm{Fil}^r \Omega^\bullet_{X/K} := \Omega^{\geq r}_{X/K}$, or more concretely uses the subcomplex beginning with $\Omega^r_{X/K}$. This gives a decreasing filtration on de Rham cohomology, called the Hodge filtration. For a smooth proper curve C/K, only H^0, H^1, and H^2 matter, and the filtration on $H^1_{\mathrm{dR}}(C/K)$ is especially simple. There is a canonical short exact sequence

$$0 \longrightarrow H^0(C, \Omega^1_{C/K}) \longrightarrow H^1_{\mathrm{dR}}(C/K) \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow 0.$$

If C has genus g, then $H^1_{\mathrm{dR}}(C/K)$ has dimension $2g$, and the Hodge filtration is

$$\mathrm{Fil}^0 H^1_{\mathrm{dR}}(C/K) = H^1_{\mathrm{dR}}(C/K), \qquad \mathrm{Fil}^1 H^1_{\mathrm{dR}}(C/K) = H^0(C, \Omega^1_{C/K}),$$
$$\mathrm{Fil}^2 H^1_{\mathrm{dR}}(C/K) = 0.$$

In particular, the subspace Fil^1 is the space of regular differential forms on the curve.

3.2.1. *The case of elliptic curves.* Let E/K be an elliptic curve. Suppose that E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The invariant differential is $\omega_E = dx/(2y + a_1x + a_3)$. It is a regular differential form on E, and it spans the one-dimensional space $H^0(E, \Omega^1_{E/K})$. Therefore the Hodge filtration on $H^1_{\mathrm{dR}}(E/K)$ is $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(E/K) = K\omega_E$.

For computations, it is often convenient to choose a second de Rham class which complements the invariant differential. In a short Weierstrass model $y^2 = f(x)$, with f a separable cubic, one may take $\omega = dx/y$ and $\eta = x\,dx/y$. Then ω is regular, while η has a pole at infinity but defines a de Rham cohomology class. The two classes form a basis of $H^1_{\mathrm{dR}}(E/K)$, and the Hodge filtration is given by $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(E/K) = K\omega$.

3.3. **Crystalline cohomology.** We now recall the formal properties of crystalline cohomology that will be used later. We do not give the construction. The main point is that crystalline cohomology is a p-adic cohomology theory for varieties in characteristic p which "behaves like" de Rham cohomology of a lift to characteristic 0.

Let k be a perfect field of characteristic p, let $W = W(k)$ be its ring of Witt vectors, and let $K_0 = W[1/p]$. If X/k is smooth and proper, its crystalline cohomology groups $H^i_{\mathrm{cris}}(X/W)$ are finitely generated W-modules. After inverting p, one obtains finite-dimensional K_0-vector spaces $H^i_{\mathrm{cris}}(X/W)[1/p]$.

Crystalline cohomology is contravariantly functorial. Thus, a morphism $f : X \to Y$ of smooth proper k-varieties induces a pullback map $f^* : H^i_{\mathrm{cris}}(Y/W) \to H^i_{\mathrm{cris}}(X/W)$. In particular, any endomorphism $u : X \to X$ of the special fibre acts on crystalline cohomology by pullback: $u^* : H^i_{\mathrm{cris}}(X/W) \to H^i_{\mathrm{cris}}(X/W)$.

The Frobenius on crystalline cohomology is defined using the absolute Frobenius of the special fibre. Let $F_X : X \to X$ be the absolute Frobenius morphism, which is the identity on points, while on the structure sheaf raises functions to their p-th powers. Pullback by F_X induces a Frobenius operator on crystalline cohomology. More precisely, it gives a σ-semilinear map $\varphi : H^i_{\mathrm{cris}}(X/W)[1/p] \to H^i_{\mathrm{cris}}(X/W)[1/p]$, where $\sigma : K_0 \to K_0$ is the lift of the absolute p-power Frobenius of k. If $k = \mathbb{F}_q$

with $q = p^f$, then φ^f is K_0-linear. This is the operator whose characteristic polynomial is usually compared with point counts over finite fields.

The key comparison property is the following. Suppose that X/k admits a smooth proper lift $\mathcal{X}/W$. Then crystalline cohomology of the special fibre is computed by the algebraic de Rham cohomology of the lift:

$$H^i_{\mathrm{cris}}(X/W) \cong H^i_{\mathrm{dR}}(\mathcal{X}/W).$$

More generally, if $\mathcal{X}/\mathcal{O}_K$ is a smooth proper lift over the ring of integers of a finite extension K/K_0, then one has a comparison isomorphism

$$H^i_{\mathrm{cris}}(X/W)[1/p] \otimes_{K_0} K \cong H^i_{\mathrm{dR}}(\mathcal{X}_K/K).$$

For an elliptic curve with good reduction, this says the following. Let E/K have good reduction, let $\mathcal{E}/\mathcal{O}_K$ be its smooth proper model, and let $\widetilde{E}/k$ be the special fibre. Then $H^1_{\mathrm{cris}}(\widetilde{E}/W)[1/p]$ is a two-dimensional K_0-vector space with Frobenius. After tensoring with K, it becomes $H^1_{\mathrm{dR}}(E/K)$, and therefore inherits the Hodge filtration whose Fil^1 is generated by the invariant differential of E.

3.4. **The filtered φ-module of an elliptic curve with good reduction.** Let $K/\mathbb{Q}_p$ be a finite extension, let $\mathcal{O}_K$ be its ring of integers, let k be its residue field, and put $K_0 = W(k)[1/p]$. Let $\sigma : K_0 \to K_0$ denote the lift of the absolute p-power Frobenius of k. Let E/K be an elliptic curve with good reduction, and let $\mathcal{E}/\mathcal{O}_K$ be its smooth proper model. Write $\widetilde{E}/k$ for the special fibre. For now, we use the cohomological convention: the representation attached to E is $V_E := H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)$. Thus V_E has Hodge–Tate weights 0 and 1.

Definition 3.1. The filtered φ-module attached to E/K is

$$D_{\mathrm{cris}}(E) := D_{\mathrm{cris}}(V_E) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V_E)^{G_K}.$$

It is a finite-dimensional K_0-vector space equipped with:

(i) a σ-semilinear Frobenius $\varphi : D_{\mathrm{cris}}(E) \to D_{\mathrm{cris}}(E)$, induced by Frobenius on B_{cris};
(ii) a decreasing filtration on $D_{\mathrm{cris}}(E)_K := D_{\mathrm{cris}}(E) \otimes_{K_0} K$, defined by transporting the filtration on $D_{\mathrm{dR}}(V_E)$ along the crystalline comparison isomorphism

$$D_{\mathrm{cris}}(E) \otimes_{K_0} K \simeq D_{\mathrm{dR}}(V_E).$$

The following property will be very important for us. It is a consequence of theorems of Faltings and Tsuji, which we recall in detail below (see Theorem 3.8), that we have an identification

$$D_{\mathrm{cris}}(E) \simeq H^1_{\mathrm{cris}}(\widetilde{E}/W(k))[1/p].$$

Under this identification, φ is the crystalline Frobenius and the filtration is the one induced, after tensoring with K, by the comparison isomorphism

$$H^1_{\mathrm{cris}}(\widetilde{E}/W(k))[1/p] \otimes_{K_0} K \simeq H^1_{\mathrm{dR}}(E/K).$$

In particular, the filtration on $D_{\mathrm{cris}}(E)_K$ is

$$\mathrm{Fil}^0 D_{\mathrm{cris}}(E)_K = D_{\mathrm{cris}}(E)_K, \qquad \mathrm{Fil}^1 D_{\mathrm{cris}}(E)_K = H^0(E, \Omega^1_{E/K}),$$

$$\mathrm{Fil}^2 D_{\mathrm{cris}}(E)_K = 0,$$

where Fil^1 is viewed inside $D_{\mathrm{cris}}(E)_K$ through the comparison with $H^1_{\mathrm{dR}}(E/K)$. In particular, $D_{\mathrm{cris}}(E)$ is a two-dimensional K_0-vector space.

Remark 3.2. As already pointed out, the key point to describe $D_{\mathrm{cris}}(E)$ becomes understanding the Hodge filtration on $H^1_{\mathrm{dR}}(E/K)$.

If $K = \mathbb{Q}_p$, then $K_0 = \mathbb{Q}_p$ and φ is $\mathbb{Q}_p$-linear. In this case the determinant of Frobenius is p:

$$\det(\varphi \mid D_{\mathrm{cris}}(E)) = p.$$

More generally, if k has cardinality $q = p^f$, then φ^f is K_0-linear and the determinant of φ^f is q. In fact, the characteristic polynomial of φ^f agrees with the 'characteristic polynomial of Frobenius' that may be familiar from étale cohomology. In particular, the characteristic polynomial of φ^f is $T^2 - a_q T + q$, where $q := \#k$ and $a_q := q + 1 - \#\tilde{E}(k)$.

Remark 3.3. Similarly, if E/K is an elliptic curve with semistable reduction, one can attach to E a filtered (φ, N)-module. We will not give the precise definition; the 'right' cohomology space for this setting is the first Hyodo-Kato cohomology group $H^1_{\mathrm{HK}}(\mathcal{E}_k/K_0)$.

Given the importance of the above equality of characteristic polynomials, we state it formally as a theorem.

Theorem 3.4 (Katz-Messing [KM74])**.** *Let X be a smooth proper variety over $k = \mathbb{F}_q$, with $q = p^f$. Write $W = W(k)$ and $K_0 = \operatorname{Frac} W$. Let*

$$\varphi : H^i_{\mathrm{cris}}(X/W) \otimes_W K_0 \longrightarrow H^i_{\mathrm{cris}}(X/W) \otimes_W K_0$$

be the Frobenius induced by the absolute p-power Frobenius; it is σ-semilinear, hence φ^f is K_0-linear. For every prime $\ell \neq p$ one has

$$\det\bigl(T - \varphi^f \mid H^i_{\mathrm{cris}}(X/W) \otimes_W K_0\bigr) = \det\bigl(T - \mathrm{Frob}_q \mid H^i_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_\ell)\bigr) \in \mathbb{Q}[T],$$

where Frob_q denotes geometric Frobenius.

3.5. **Good reduction and crystalline representations.** Recall the Néron–Ogg–Shafarevich criterion, proved by Serre and Tate [ST68] for general abelian varieties:

Theorem 3.5 (Néron–Ogg–Shafarevich criterion)**.** *An abelian variety A/K has good (resp. semistable) reduction if and only if, for every (equivalently, any) prime $\ell \neq p$, the Tate module $V_\ell A$ is an unramified representation of G_K (resp. a representation on which inertia acts by operators that are unipotent of class 2).*

The p-adic version of this result replaces "unramified" by "crystalline".

Theorem 3.6 (Coleman–Iovita [CI99, Theorem 4.7], Breuil [Bre00, Corollaire 1.6])**.** *Let A/K be an abelian variety. Then A has good (resp. semistable) reduction if and only if V_pA (equivalently, $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_p)$) is crystalline (resp. semistable).*

Remark 3.7. The theorem suggests that crystalline representations are the correct p-adic analogue of unramified ℓ-adic representations.

We now state precisely the comparison theorem that allows us to interpret $D_{\mathrm{cris}}(V_E)$ as the crystalline cohomology of its special fibre. The result below is the good reduction case of [Tsu99, Theorem 0.2], which also covers the more general case of semistable reduction. The good reduction case, which is the only one we will state and use, had already been proved by Faltings in [Fal89].

Theorem 3.8 (Crystalline-to-étale comparison)**.** *Let K be a finite extension of $\mathbb{Q}_p$, let k be its residue field, and put $K_0 = W(k)[1/p]$. Let $\mathcal{X}$ be a smooth proper scheme over $\mathcal{O}_K$, with generic fibre $X = \mathcal{X}_K$ and special fibre $X_k = \mathcal{X}_k$. Then, for every $i \geq 0$, the p-adic representation*

$$V^i_{\text{ét}}(X) := H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$$

is crystalline, and there is a canonical comparison isomorphism

$$B_{\mathrm{cris}} \otimes_{K_0} H^i_{\mathrm{cris}}(X_k/W(k))[1/p] \xrightarrow{\sim} B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p). \tag{5}$$

This isomorphism is compatible with the action of G_K, where G_K acts trivially on $H^i_{\mathrm{cris}}(X_k/W(k))[1/p]$, and with Frobenius, where the Frobenius on the left is the tensor product of Fontaine's Frobenius on B_{cris} and the crystalline Frobenius on $H^i_{\mathrm{cris}}(X_k/W(k))[1/p]$, and on the right is the tensor product of the Frobenius on B_{cris} and the identity on $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. After extending scalars to B_{dR}, it is also compatible with the Hodge filtration, via the canonical identification

$$K \otimes_{K_0} H^i_{\mathrm{cris}}(X_k/W(k))[1/p] \cong H^i_{\mathrm{dR}}(X/K).$$

Remark 3.9. Applying G_K-invariants to the crystalline comparison isomorphism in Equation (5) gives

$$\begin{aligned} D_{\mathrm{cris}}\bigl(H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)\bigr) &= \bigl(B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)\bigr)^{G_K} \\ &\cong \bigl(B_{\mathrm{cris}} \otimes_{K_0} H^i_{\mathrm{cris}}(X_k/W(k))[1/p]\bigr)^{G_K} \\ &= B_{\mathrm{cris}}^{G_K} \otimes_{K_0} H^i_{\mathrm{cris}}(X_k/W(k))[1/p] \\ &= H^i_{\mathrm{cris}}(X_k/W(k))[1/p]. \end{aligned}$$

Thus

$$D_{\mathrm{cris}}\big(H^i_{\text{ét}}(X_{\overline{K}},\mathbb{Q}_p)\big) \cong H^i_{\mathrm{cris}}(X_k/W(k))[1/p]$$

as K_0-vector spaces with Frobenius. The filtration is not a filtration on this K_0-vector space itself, but on its scalar extension

$$K \otimes_{K_0} D_{\mathrm{cris}}\big(H^i_{\text{ét}}(X_{\overline{K}},\mathbb{Q}_p)\big) \cong H^i_{\mathrm{dR}}(X/K).$$

In particular, if E/K is an elliptic curve with good reduction and $\mathcal{E}/\mathcal{O}_K$ is its smooth proper model, with special fibre $\widetilde{E}/k$, then

$$D_{\mathrm{cris}}\big(H^1_{\text{ét}}(E_{\overline{K}},\mathbb{Q}_p)\big) \cong H^1_{\mathrm{cris}}(\widetilde{E}/W(k))[1/p].$$

3.6. **Weakly admissible filtered φ-modules and (φ,N)-modules of elliptic curve type over $\mathbb{Q}_p$.** The Colmez-Fontaine theorem (Theorem 2.26) says that crystalline representations can be encoded by weakly admissible filtered φ-modules. If $V = H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}_p},\mathbb{Q}_p)$ is a representation coming from an elliptic curve with good reduction over $\mathbb{Q}_p$, the corresponding filtered φ-module is a $\mathbb{Q}_p$-vector space of dimension 2, has Hodge–Tate weights $0,1$, and carries a $\mathbb{Q}_p$-linear Frobenius φ with determinant p. In this section, we classify these objects abstractly; the classification will be remarkably simple to interpret in terms of elliptic curves. Although we haven't given the complete definition of the filtered (φ,N)-module corresponding to a semistable elliptic curve, we will also carry out a similar calculation for filtered (φ,N)-modules.

Setup. Since $K=\mathbb{Q}_p$, we have $K_0=\mathbb{Q}_p$, and Frobenius is an honest $\mathbb{Q}_p$-linear automorphism. A filtered (φ,N)-module of cohomological elliptic curve type is therefore a two-dimensional $\mathbb{Q}_p$-vector space D, equipped with $\varphi\in\mathrm{GL}(D)$ and $N\in\mathrm{End}_{\mathbb{Q}_p}(D)$, satisfying $N\varphi = p\varphi N$, together with a filtration of the form

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \ell, \qquad \mathrm{Fil}^2 D = 0,$$

where $\ell\subset D$ is a line. The Hodge number is $t_H(D)=0+1=1$, so weak admissibility requires $t_N(D)=v_p(\det\varphi)=1$, which is implied by $\det\varphi = p$. The problem lies in understanding the subobjects.

3.6.1. *The crystalline case.* Assume first that $N=0$. Then we are classifying filtered φ-modules (D,φ,ℓ), where $\dim_{\mathbb{Q}_p} D=2$, $\det\varphi=p$, and $\mathrm{Fil}^1 D=\ell$. Let $P_\varphi(T)=T^2-aT+p$ be the characteristic polynomial of φ. As already pointed out, we have $P_\varphi(T)=T^2-aT+p$, where $a=p+1-\#\widetilde{E}(\mathbb{F}_p)$.

Consider the weak admissibility inequalities. If $L\subset D$ is a φ-stable line and φ acts on L by λ_L, then $t_N(L)=v_p(\lambda_L)$. The induced Hodge number of L is

$$t_H(L)=\begin{cases}1, & L=\ell,\\ 0, & L\neq\ell.\end{cases}$$

Therefore weak admissibility is equivalent to the following simple condition:

$$\begin{cases}1\le v_p(\lambda_L), & \text{if } L=\ell,\\ 0\le v_p(\lambda_L), & \text{if } L\neq\ell,\end{cases}$$

for every φ-stable line $L\subset D$.

3.6.2. *Ordinary crystalline objects.* We say that the crystalline object is *ordinary* if the Newton slopes of φ are 0 and 1. Equivalently, in terms of $P_\varphi(T)=T^2-aT+p$, this is the case $v_p(a)=0$. Then $P_\varphi(T)$ has two roots in $\mathbb{Q}_p$, one of valuation 0 and one of valuation 1. We write them as α,β, where

$$v_p(\alpha)=0, \qquad v_p(\beta)=1, \qquad \alpha\beta=p.$$

Thus $D=D_{\mathrm{unit}}\oplus D_{\mathrm{mult}}$, where

$$\varphi|_{D_{\mathrm{unit}}}=\alpha, \qquad \varphi|_{D_{\mathrm{mult}}}=\beta.$$

The line D_{unit} is the slope-0 line, and D_{mult} is the slope-1 line.

The weak admissibility condition becomes especially transparent. The slope-0 line has Newton number 0. Hence it cannot be equal to the Hodge line, because if we had $\ell=D_{\mathrm{unit}}$, the inequality for D_{unit} would read $1\le 0$, contradiction. Conversely, if $\ell\neq D_{\mathrm{unit}}$, then the inequalities trivially hold. Thus we have the following classification.

Proposition 3.10 (Ordinary crystalline rank-two objects)**.** *Let D be a two-dimensional filtered φ-module over $\mathbb{Q}_p$ with $\det\varphi = p$ and filtration*

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \ell, \qquad \mathrm{Fil}^2 D = 0.$$

Assume that φ has ordinary slopes 0 and 1. Let $D_{\mathrm{unit}} \subset D$ be the slope-0 line. Then D is weakly admissible if and only if $\ell \neq D_{\mathrm{unit}}$.

Proof. The endpoint condition is automatic from $t_H(D) = 1$ and $v_p(\det\varphi) = 1$. The only proper nonzero φ-stable subobjects are the two slope lines. The slope-0 line has Newton number 0, so it cannot be the Hodge line. If the Hodge line is any other line, its induced Hodge number is 0, and the inequality is satisfied. □

We now discuss the classification up to isomorphism. Fix an ordinary Frobenius polynomial $P(T) = T^2 - aT + p$ with $v_p(a) = 0$. Equivalently, fix the unit root α; the other root is p/α. Since the two roots have different p-adic valuations, they are distinct. Hence the underlying φ-module splits canonically as the direct sum of its two eigenspaces

$$D = D_{\mathrm{unit}} \oplus D_{\mathrm{mult}},$$

where φ acts on D_{unit} by α and on D_{mult} by p/α. Note again that D_{unit} has Newton slope 0, while D_{mult} has Newton slope 1.

To classify filtered φ-modules with this fixed underlying φ-module, we must understand which choices of the Hodge line $\ell = \mathrm{Fil}^1 D$ give isomorphic objects. For this reason, we study the automorphism group of the underlying φ-module: an isomorphism between two filtered φ-modules with the same underlying (D, φ) is precisely an automorphism of the φ-module D that carries one Hodge line to the other. Thus the isomorphism classes of filtrations are the orbits of the automorphism group $\mathrm{Aut}_\varphi(D)$ acting on the set of admissible lines in D. Let us compute this automorphism group.

Proposition 3.11. *The automorphism group of the φ-module $D = D_{\mathrm{unit}} \oplus D_{\mathrm{mult}}$ is isomorphic to $\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times$, where the two factors act on D_{unit} and D_{mult}.*

Proof. Choose nonzero vectors $e_{\mathrm{unit}} \in D_{\mathrm{unit}}$ and $e_{\mathrm{mult}} \in D_{\mathrm{mult}}$. Every vector in D can be written uniquely as $xe_{\mathrm{unit}} + ye_{\mathrm{mult}}$. If $u \in \mathrm{Aut}_\varphi(D)$, then u must preserve the generalized eigenspaces of φ. Since the two eigenspaces are one-dimensional and the eigenvalues α and p/α are distinct, u sends each eigenspace to itself. Hence there exist $\lambda, \mu \in \mathbb{Q}_p^\times$ such that $u(e_{\mathrm{unit}}) = \lambda e_{\mathrm{unit}}$ and $u(e_{\mathrm{mult}}) = \mu e_{\mathrm{mult}}$. Conversely, every such pair (λ, μ) defines an automorphism commuting with φ. Therefore $\mathrm{Aut}_\varphi(D) \cong \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times$. □

We now let $\mathrm{Aut}_\varphi(D)$ act on lines. We know that the Hodge line cannot be the slope-0 line: $\ell \neq D_{\mathrm{unit}}$. There are two cases.

(1) Consider first the case $\ell = D_{\mathrm{mult}}$. Since every φ-automorphism preserves D_{mult}, this line forms an orbit by itself.
(2) Second, suppose ℓ is neither D_{unit} nor D_{mult}. Then ℓ is generated by a vector with both coordinates nonzero. After rescaling the generator, it can be written uniquely in the form $e_{\mathrm{unit}} + ce_{\mathrm{mult}}$ with $c \in \mathbb{Q}_p^\times$. The automorphism with $u(e_{\mathrm{unit}}) = e_{\mathrm{unit}}$ and $u(e_{\mathrm{mult}}) = c^{-1}e_{\mathrm{mult}}$ sends this line to $\mathbb{Q}_p(e_{\mathrm{unit}} + e_{\mathrm{mult}})$. Thus all lines different from both eigenspaces lie in a single orbit.

Consequently, the admissible Hodge lines $\ell \neq D_{\mathrm{unit}}$ fall into exactly two orbits: the line $\ell = D_{\mathrm{mult}}$, and the open orbit consisting of all lines $\ell \neq D_{\mathrm{unit}}, D_{\mathrm{mult}}$. Therefore, for a fixed ordinary Frobenius polynomial, there are only two isomorphism classes of weakly admissible filtered φ-modules.

Corollary 3.12. *Fix an ordinary polynomial $P(T) = T^2 - aT + p$ with $v_p(a) = 0$. Up to isomorphism, the weakly admissible filtered φ-modules with characteristic polynomial $P(T)$ are represented by the filtrations $\mathrm{Fil}^1 D = D_{\mathrm{mult}}$ and $\mathrm{Fil}^1 D = \mathbb{Q}_p(e_{\mathrm{unit}} + e_{\mathrm{mult}})$, where*

$$D_{\mathrm{unit}} = \mathbb{Q}_p e_{\mathrm{unit}}, \qquad D_{\mathrm{mult}} = \mathbb{Q}_p e_{\mathrm{mult}}.$$

The first case is the split, or canonical, filtration. The second case is the non-split ordinary filtration. Note that, if $P(T)$ comes from an elliptic curve, a is not arbitrary: for an elliptic curve over $\mathbb{F}_p$ it is an integer satisfying the Hasse bound $|a| \leq 2\sqrt{p}$.

Remark 3.13. The interpretation in terms of elliptic curves is as follows. Start with $\tilde{E}/k$ and its Frobenius endomorphism. By Deuring's lifting theorem, there is a unique elliptic curve E in characteristic 0 lifting $\tilde{E}$ together with its Frobenius endomorphism (in particular, the lift is a CM elliptic curve, called the *canonical lift*). If F is the endomorphism in characteristic 0 that lifts the Frobenius of $\tilde{E}$, the action of F on the p-adic Tate module / first crystalline cohomology group of E splits it as the direct sum of two eigenspaces. This is the case that corresponds to the split/canonical filtration above. Every other elliptic curve $E/\mathbb{Q}_p$ having good reduction with special fibre $\tilde{E}$ shares the same Galois representation V_pE up to isomorphism (equivalently, $H^1_{\mathrm{cris}}(\tilde{E}/\mathbb{Z}_p)[1/p]$); the filtered φ-module (up to isomorphism) that corresponds to all of these elliptic curves is that given by the non-split ordinary filtration above.

Remark 3.14. The reader familiar with elliptic curves may find it strange that uncountably many elliptic curves share the same p-adic representation. Two comments are in order: first, this only holds at the rational level (there can still be more structures at the integral level, that is, if we look at T_pE); and second, Faltings's isogeny theorem, saying that two abelian varieties have isomorphic Galois representations if and only if they are isogenous, holds only over fields that are finitely generated over the prime field. In fact, this is a way to construct a counter-example to (a putative extension of) Faltings's theorem to elliptic curves over $\mathbb{Q}_p$.

3.6.3. *Supersingular crystalline objects.* Fix again a characteristic polynomial $P_\varphi(T) = T^2 - aT + p$. Note that the Newton slopes are non-negative rational numbers with denominator at most 2 and sum 1. Hence, if they are not $0, 1$, then they must necessarily be $\frac{1}{2}, \frac{1}{2}$. We now consider this case.

In terms of $P_\varphi(T) = T^2 - aT + p$, this is the case where the Newton polygon has a single slope $1/2$. Since a is the sum of the roots of this polynomial, this implies in particular that a has positive p-adic valuation; and since it is an element of $\mathbb{Q}_p$, it means that $v_p(a) \geq 1$. Conversely, if $v_p(a) \geq 1$, then the polynomial $T^2 - aT + p$ has both slopes equal to $1/2$, as one can immediately check using the quadratic formula and the fact that the discriminant has valuation 1.

For elliptic curves over $\mathbb{F}_p$, this situation corresponds to supersingular reduction: a is an integer, and we have just shown that $p \mid a$, which – as is well known – is indeed equivalent to supersingular reduction. Note that, for $p \geq 5$, the Hasse bound $|a| \leq 2\sqrt{p}$ shows that $p \mid a$ if and only if $a = 0$.

Over $\mathbb{Q}_p$, a two-dimensional φ-module of slope $1/2$ has no nonzero proper φ-stable subspace. Indeed, a one-dimensional $\mathbb{Q}_p$-subspace stable under φ would give a Frobenius eigenvalue lying in $\mathbb{Q}_p^\times$, hence with integral p-adic valuation; but this is incompatible with the slope being $1/2$. It follows that the weak admissibility inequalities for proper subobjects are vacuous. Since $t_H(D) = 1$ and $v_p(\det \varphi) = 1$, the endpoint condition is also satisfied.

Proposition 3.15 (Supersingular crystalline rank-two objects)**.** *Let D be a two-dimensional filtered φ-module over $\mathbb{Q}_p$ with $\det \varphi = p$ and filtration*

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \ell, \qquad \mathrm{Fil}^2 D = 0.$$

Assume that the Newton slopes of φ are $\frac{1}{2}, \frac{1}{2}$. Then D is weakly admissible for every line $\ell \subset D$. Moreover, for a fixed underlying φ-module, all choices of ℓ give isomorphic filtered φ-modules.

Proof. There are no nonzero proper φ-stable $\mathbb{Q}_p$-subspaces, so there are no line inequalities. The endpoint condition holds because both the Hodge number and the Newton number are equal to 1.

It remains to explain the final assertion. Since the characteristic polynomial of φ is irreducible over $\mathbb{Q}_p$, the algebra $F := \mathbb{Q}_p[\varphi]$ is a quadratic field, and D is one-dimensional as an F-vector space. The group $F^\times$ is the automorphism group of the φ-module D. It acts transitively on the set of one-dimensional $\mathbb{Q}_p$-subspaces of D: if $L_1 = \mathbb{Q}_p x$ and $L_2 = \mathbb{Q}_p y$ with $x, y \neq 0$, multiplication by $y/x \in F^\times$ sends L_1 to L_2. Hence all Hodge lines are equivalent up to isomorphism. □

Thus, for each supersingular Frobenius polynomial $P(T) = T^2 - aT + p$, there is a single filtered isomorphism class. For $p > 3$, a concrete model for this isomorphism class is as follows:

(1) Vector space: $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$

(2) Frobenius: $\varphi(e_1) = e_2, \varphi(e_2) = -pe_1$, so that φ is represented by the matrix $\begin{pmatrix} 0 & -p \\ 1 & 0 \end{pmatrix}$ and has the right characteristic polynomial.

(3) Filtration: $\mathrm{Fil}^1 D = \mathbb{Q}_p e_1$.

Remark 3.16. If $E/\mathbb{Q}_p$ is an elliptic curve with good supersingular reduction, then its H^1_{cris} realises the filtered φ-module we just described.

In particular, note that we have proven a rather surprising theorem: for $p \geq 5$, if $E_1, E_2/\mathbb{Q}_p$ both have good supersingular reduction, then their rational p-adic Tate modules $V_p E$ are isomorphic as Galois representations! This is because on the linear algebra side there is only one object that could possibly represent their Tate modules.

3.6.4. *Summary.* For crystalline objects of (cohomological) elliptic curve type over $\mathbb{Q}_p$, we have obtained the following classification.

Reduction type	Frobenius polynomial	Slopes	# types
ordinary	$T^2 - aT + p$, $v_p(a) = 0$	$0, 1$	two
supersingular	$T^2 - aT + p$, $v_p(a) > 0$	$\frac{1}{2}, \frac{1}{2}$	one

Note in particular that there are only finitely many isomorphism classes of Galois representations $V_p E$ as E varies among the good reduction elliptic curves over $\mathbb{Q}_p$: indeed, in terms of the above table, a can only take finitely many values (it is an integer in the interval $[-2\sqrt{p}, 2\sqrt{p}]$).

3.6.5. *The semistable non-crystalline case.* We now treat the case $N \neq 0$. Since D has dimension two and N is nilpotent, one has $\operatorname{im} N = \ker N$, a line in D. Choose a basis e_0, e_1 such that

$$\operatorname{im} N = \mathbb{Q}_p e_1, \qquad N(e_0) = e_1, \qquad N(e_1) = 0.$$

The relation $N\varphi = p\varphi N$ implies that, for some $\alpha \in \mathbb{Q}_p^\times$, one may write $\varphi(e_0) = p\alpha e_0$ and $\varphi(e_1) = \alpha e_1$.

Exercise 3.17. Prove this statement, which is simple linear algebra.

The determinant is $\det \varphi = p\alpha^2$, so $\alpha = \pm 1$. The filtration is again

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \ell, \qquad \mathrm{Fil}^2 D = 0.$$

The only proper nonzero subobject stable under both φ and N is the line $\mathbb{Q}_p e_1$, with Newton number $t_N(\mathbb{Q}_p e_1) = v_p(\alpha) = 0$. If we had $\ell = \mathbb{Q}_p e_1$, then the induced Hodge number would be 1, and the weak admissibility inequality would fail. Conversely, it is easy to check that every line $\ell \neq \mathbb{Q}_p e_1$ gives a weakly admissible module. Equivalently, every admissible Hodge line has the form $\ell = \mathbb{Q}_p(e_0 + \mathcal{L} e_1)$ for a unique parameter $\mathcal{L} \in \mathbb{Q}_p$.

Proposition 3.18 (Semistable non-crystalline rank-two objects)**.** *Let D be a two-dimensional filtered (φ, N)-module over $\mathbb{Q}_p$ of cohomological elliptic-curve type, with $N \neq 0$ and $\det \varphi = p$. Then D is weakly admissible if and only if it admits a basis e_0, e_1 such that*

$$N(e_0) = e_1, \qquad N(e_1) = 0,$$

$$\varphi(e_0) = p\alpha e_0, \qquad \varphi(e_1) = \alpha e_1, \qquad \alpha = \pm 1,$$

and

$$\mathrm{Fil}^0 D = D, \qquad \mathrm{Fil}^1 D = \mathbb{Q}_p(e_0 + \mathcal{L} e_1), \qquad \mathrm{Fil}^2 D = 0$$

for some $\mathcal{L} \in \mathbb{Q}_p$.

Proposition 3.19. *Let $D(\alpha, \mathcal{L})$ denote the filtered (φ, N)-module described in Proposition 3.18, where $\alpha \in \{\pm 1\}$ and $\mathcal{L} \in \mathbb{Q}_p$. There is an isomorphism*

$$D(\alpha, \mathcal{L}) \simeq D(\alpha', \mathcal{L}')$$

of filtered (φ, N)-modules if and only if $\alpha = \alpha'$ and $\mathcal{L} = \mathcal{L}'$. Thus the isomorphism classes are parametrised by $\{\pm 1\} \times \mathbb{Q}_p$.

Proof. The line $\operatorname{im} N = \ker N$ is intrinsic: it is the unique nonzero proper subobject stable under both φ and N. On this line, φ acts by the scalar α. Therefore α is an isomorphism invariant.

Fix α. We compute the automorphisms of the underlying (φ, N)-module. Let e_0, e_1 be a basis with $N(e_0) = e_1$, $N(e_1) = 0$, $\varphi(e_0) = p\alpha e_0$, and $\varphi(e_1) = \alpha e_1$. Let u be an automorphism commuting with N and φ. Write

$$u(e_0) = ae_0 + ce_1, \qquad u(e_1) = be_0 + de_1.$$

The relation $uN = Nu$ gives $u(e_1) = N(u(e_0)) = ae_1$. Hence we must have $b = 0$ and $d = a$, and

$$u(e_0) = ae_0 + ce_1, \qquad u(e_1) = ae_1.$$

Now impose $u\varphi = \varphi u$. Applying this to e_0 gives $u(\varphi(e_0)) = u(p\alpha e_0) = p\alpha(ae_0 + ce_1)$, whereas $\varphi(u(e_0)) = \varphi(ae_0 + ce_1) = ap\alpha e_0 + c\alpha e_1$. Thus $p\alpha c = \alpha c$. Since $p \neq 1$ and $\alpha \neq 0$, this forces $c = 0$. Therefore every automorphism of the underlying (φ, N)-module is multiplication by a scalar.

It follows that such an automorphism fixes every line in D. In particular, it sends

$$\mathrm{Fil}^1 D(\alpha, \mathcal{L}) = \mathbb{Q}_p(e_0 + \mathcal{L}e_1)$$

to itself. Therefore two filtrations $\mathbb{Q}_p(e_0 + \mathcal{L}e_1)$ and $\mathbb{Q}_p(e_0 + \mathcal{L}'e_1)$ are isomorphic if and only if they are equal, which is equivalent to $\mathcal{L} = \mathcal{L}'$. This proves the claim. □

We will show below that these filtered (φ, N)-modules correspond to Tate curves over $\mathbb{Q}_p$ (for $\alpha = 1$). Their non-split quadratic twists give the modules with $\alpha = -1$.

3.7. **The semistable case and Tate curves.** The simplest non-crystalline semistable representations attached to elliptic curves come from elliptic curves with multiplicative reduction. These can be studied via the theory of the Tate curve. Standard references for the Tate curve are Tate's original account [Tat74] and Silverman's description in [Sil94, Chapter V]; the relation with Frobenius and monodromy for curves and abelian varieties with semistable reduction is treated by Coleman–Iovita [CI99].

3.7.1. *The analytic uniformisation.* Let K be a p-adic field, and let $q_E \in K^\times$ satisfy $v_K(q_E) > 0$. Equivalently, $|q_E| < 1$ for the absolute value associated with v_K. Tate constructs an elliptic curve E_{q_E}/K, called the *Tate curve with parameter* q_E, with the following properties [Tat74].

Theorem 3.20 (Tate uniformisation)**.** *Let K be a complete nonarchimedean field and let $q_E \in K^\times$ satisfy $|q_E| < 1$. There is an elliptic curve E_{q_E}/K and a G_K-equivariant analytic isomorphism*

$$E_{q_E}(\overline{K}) \simeq \overline{K}^\times / q_E^{\mathbb{Z}}.$$

Moreover, E_{q_E} has split multiplicative[4] reduction, and every elliptic curve over K with split multiplicative reduction is isomorphic over K to E_{q_E} for a uniquely determined $q_E \in K^\times$ with $v_K(q_E) > 0$.

The j-invariant of the Tate curve is given by the convergent q-expansion

$$j(E_{q_E}) = q_E^{-1} + 744 + 196884 q_E + \cdots.$$

In particular, for a Tate curve E_{q_E} one has $v_K(j(E_{q_E})) = -v_K(q_E) < 0$. Conversely, an elliptic curve E over a p-adic field K has potentially multiplicative reduction precisely when its j-invariant is non-integral. More precisely, if $v_K(j(E)) < 0$, then there is a Tate curve E_q over K with $j(E_q) = j(E)$. The curve E_q has split multiplicative reduction over K, and E is a quadratic twist of E_q over K, possibly the trivial twist. Equivalently, after passing to the quadratic extension, possibly trivial, which trivialises this twist, the curve E becomes isomorphic to the Tate curve E_q and hence has split multiplicative reduction.

Remark 3.21. The Tate uniformisation should be compared with the complex uniformisation $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. In the nonarchimedean setting, the additive group $\mathbb{C}$ is replaced by the multiplicative group $\overline{K}^\times$, and the lattice Λ is replaced by the discrete subgroup $q_E^{\mathbb{Z}}$. This may seem strange at first glance, but the point is that in the complex setting we may write $\Lambda \cong \mathbb{Z} \oplus \mathbb{Z}\tau$, and via the exponential map we get

$$\mathbb{C}/\Lambda \cong (\mathbb{C}/\mathbb{Z})/\mathbb{Z}\tau \xrightarrow{\exp(2\pi i \cdot)} \mathbb{C}^\times / \langle \exp(2\pi i \tau) \rangle,$$

so that again the uniformisation looks like the multiplicative group of an algebraically closed field modulo a multiplicative subgroup of rank 1.

[4] from the point of view of Néron models, this means that the special fibre of the Néron model is a split torus. From the elementary point of view, multiplicative reduction means that the special fibre has a node; the reduction is then called *split* if the slopes of the tangent lines at the node are rational over the ground field.

Remark 3.22. Let $J = j(E)$. Since E has split multiplicative reduction, $v(J) < 0$, so J^{-1} is topologically nilpotent. The Tate parameter is obtained by inverting the q-expansion

$$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots .$$

Thus

$$q_E = J^{-1} + 744J^{-2} + 750420J^{-3} + 872769632J^{-4} + 1102652742882J^{-5} + \cdots .$$

Equivalently, q_E is the unique element of positive valuation satisfying $j(q_E) = j(E)$.

3.7.2. *The Tate module of a Tate curve.* The exact sequence

$$0 \longrightarrow q_E^{\mathbb{Z}} \longrightarrow \overline{K}^{\times} \longrightarrow E_{q_E}(\overline{K}) \longrightarrow 0$$

allows one to compute the p-power torsion explicitly. Taking p^n-torsion one obtains an exact sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow E_{q_E}[p^n] \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0.$$

Passing to the inverse limit gives an exact sequence of $\mathbb{Z}_p[G_K]$-modules

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_pE_{q_E} \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

and after tensoring with $\mathbb{Q}_p$ we get

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V_pE_{q_E} \longrightarrow \mathbb{Q}_p \longrightarrow 0.$$

Thus the Tate module of a split multiplicative elliptic curve is an extension of the trivial representation by the cyclotomic character.

This extension can be described by a concrete cocycle. Choose a compatible system of p^n-roots of q_E: this is a collection $(q_E^{1/p^n})_{n\geq 1}$ such that $(q_E^{1/p^{n+1}})^p = q_E^{1/p^n}$ for all $n \geq 1$. Also choose a compatible system of primitive roots of unity $(\zeta_{p^n})_{n\geq 1}$. The element $(\zeta_{p^n})_n$ gives a basis of $\mathbb{Z}_p(1)$, while $(q_E^{1/p^n})_n$ gives a lift of $1 \in \mathbb{Z}_p$. For $\sigma \in G_K$ there is a unique element $c_{q_E}(\sigma) \in \mathbb{Z}_p(1)$ such that

$$\sigma(q_E^{1/p^n}) = \zeta_{p^n}^{c_{q_E,n}(\sigma)} q_E^{1/p^n} \qquad \text{for all } n,$$

where $c_{q_E,n}(\sigma)$ denotes the image of $c_{q_E}(\sigma)$ modulo p^n. With respect to the basis just described, the Galois action has the form

$$\rho_{E_{q_E},p^\infty}(\sigma) = \begin{pmatrix} \chi_p(\sigma) & c_{q_E}(\sigma) \\ 0 & 1 \end{pmatrix},$$

where $\chi_p : G_K \to \mathbb{Z}_p^{\times}$ is the cyclotomic character. The cohomology class of c_{q_E} is exactly the Kummer class of q_E under the isomorphism

$$H^1(K, \mathbb{Z}_p(1)) \simeq \varprojlim_n K^{\times}/(K^{\times})^{p^n}.$$

Thus the extension class of the Tate module 'is' essentially the Tate parameter.

3.7.3. *Description of the filtered (φ, N)-module.* We now switch conventions. The classification above was written in the cohomological convention, while the Tate uniformisation more naturally describes the 'homological' Tate module $V_pE_{q_E}$. The two descriptions are dual to one another, so nothing is lost in this change of conventions.

The representation $V_pE_{q_E}$ is semistable. We describe its filtered (φ, N)-module. Recall that the Tate uniformisation gives an exact sequence of G_K-representations

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V_pE_{q_E} \longrightarrow \mathbb{Q}_p \longrightarrow 0.$$

Hence, $D_{\mathrm{st}}(V_pE_{q_E})$ has a basis e_0, e_1 with e_1 corresponding to the $\mathbb{Q}_p(1)$-part and e_0 corresponding to the $\mathbb{Q}_p$-quotient. In this basis, the filtered (φ, N)-module is as follows.

(1) *Vector space:* $D \cong K_0e_0 \oplus K_0e_1$.
(2) *Frobenius:* $\varphi(e_0) = e_0$ and $\varphi(e_1) = p^{-1}e_1$. More precisely, φ is σ-semilinear, so
$$\varphi(ae_i) = \sigma(a)\varphi(e_i) \qquad \text{for } a \in K_0.$$
(3) *Monodromy:* $N(e_0) = e_1$ and $N(e_1) = 0$.

(4) *Filtration:* the filtration lives in

$$D_K := D \otimes_{K_0} K = Ke_0 \oplus Ke_1.$$

Fix the branch of the p-adic logarithm for which $\log(p) = 0$. Setting $\mathcal{L}(E_{q_E}) := \frac{\log(q_E)}{v_p(q_E)} \in K$, the filtration is

$$\mathrm{Fil}^{-1} D_K = D_K, \qquad \mathrm{Fil}^0 D_K = K\big(e_0 - \mathcal{L}(E_{q_E})e_1\big), \qquad \mathrm{Fil}^1 D_K = 0.$$

Remark 3.23. The description of the structure as (φ, N)-module follows (after dualising) from the classification in Proposition 3.18, since we know that $V_pE_{q_E}$ is semistable but not crystalline, see Theorem 3.6.

Let us[5] derive the filtration. The formula for $\mathrm{Fil}^0 D_K$ does not follow from the abstract shape of φ and N alone: the operators φ and N give us the (φ, N)-module, but not the position of the Hodge line. For a Tate curve, we will explicitly describe the filtration in terms of the Tate parameter q_E.

Choose a compatible system $\widetilde{q}_E = (q_E, q_E^{1/p}, q_E^{1/p^2}, \ldots)$ of p-power roots of q_E, and let f_1 denote the basis vector of the $\mathbb{Q}_p(1)$-part coming from the compatible system of roots of unity. Let f_0 be the lift of the basis vector of the quotient $\mathbb{Q}_p$ coming from $\widetilde{q}_E$. Thus, the Galois action on V_pE has the form

$$\sigma(f_1) = \chi_p(\sigma)f_1, \qquad \sigma(f_0) = f_0 + c_{q_E}(\sigma)f_1,$$

where c_{q_E} is the Kummer cocycle described above.

Recall the two basic semistable periods (see Section 2.7.4).

(1) The first is Fontaine's cyclotomic period t, which satisfies $\sigma(t) = \chi_p(\sigma)t$ for every $\sigma \in G_K$ and $\varphi(t) = pt$.
(2) The second is the logarithmic period $\log[\widetilde{q}_E] \in B_{\mathrm{st}}$ attached to the chosen system of p-power roots of q_E. It satisfies $\sigma(\log[\widetilde{q}_E]) = \log[\widetilde{q}_E] + c_{q_E}(\sigma)t$ for every $\sigma \in G_K$ and $\varphi(\log[\widetilde{q}_E]) = p\log[\widetilde{q}_E]$.

Define the following elements of $B_{\mathrm{st}} \otimes V_pE_{q_E}$:

$$x := t^{-1} \otimes f_1, \qquad y := 1 \otimes f_0 - t^{-1}\log[\widetilde{q}_E] \otimes f_1.$$

Using the above properties of t and $\log[\widetilde{q}_E]$, we see easily that both x and y are G_K-invariant, so they define elements of $D_{\mathrm{st}}(V_pE_{q_E})$. The vector x is the semistable period coming from the "multiplicative direction" $\mathbb{Q}_p(1)$, while y is the "correct" lift of the quotient direction $\mathbb{Q}_p$. In this basis, one has

$$\varphi(x) = \varphi(t^{-1}) \otimes f_1 = p^{-1}t^{-1} \otimes f_1 = p^{-1}x$$

and

$$\varphi(y) = \varphi(1) \otimes f_0 - \varphi(t^{-1}\log[\widetilde{q}_E]) \otimes f_1 = 1 \otimes f_0 - p^{-1}t^{-1} \cdot p\log[\tilde{q}_E] \otimes f_1 = y,$$

so y, x are proportional to our desired basis elements e_0, e_1. We now compute the monodromy. The operator N kills B_{cris} and differentiates in the direction of the logarithmic variable u. The element $\log[\tilde{q}_E]$ is of the form $v_p(q_E)u +$ something in B_{cris}, hence $N(\log[\widetilde{q}_E]) = v_p(q_E)$. Since $N(t) = 0$, it follows that $N(x) = 0$ and

$$N(y) = -t^{-1}N(\log[\widetilde{q}_E]) \otimes f_1 = -v_p(q_E)x.$$

Thus the basis y, x has monodromy $N(y) = -v_p(q_E)x$ and $N(x) = 0$. Since we want a basis e_0, e_1 satisfying $N(e_0) = e_1$, we set

$$e_0 := y, \qquad e_1 := -v_p(q_E)x.$$

It remains to compute the filtration. The de Rham filtration is obtained by viewing the same elements x and y inside $D_{\mathrm{dR}}(V_pE_{q_E})$.

We need to compute the intersection of $D_{\mathrm{dR}}(V_pE_{q_E})$ with $\mathrm{Fil}^0 D_{\mathrm{dR}}(V_pE_{q_E}) = \mathrm{Fil}^0 B_{\mathrm{dR}} \otimes V_pE_{q_E}$. Recall from Equation (4) that $\mathrm{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+$ is the subspace where only non-negative powers of t are allowed. In particular, we note that $y + \log[\tilde{q}_E] \cdot x = 1 \otimes f_0$ is in Fil^0.

Under the natural map $B_{\mathrm{st}} \subset B_{\mathrm{dR}}$, the element $\log[\widetilde{q}_E]$ maps to something congruent to $\log(q_E)$ modulo $\mathrm{Fil}^1 B_{\mathrm{dR}}$. Equivalently, $\log[\widetilde{q}_E] - \log(q_E)$ lies in $\mathrm{Fil}^1 B_{\mathrm{dR}}$. Since the filtration is decreasing,

[5]for a much more authoritative source, see [Bri19, §3.1]. The result I find differs by a sign from Brinon's, but note that his convention [Bri19, page 6] for the monodromy operator is $N(u) = -1$, whereas I defined $N(u) = +1$. Both conventions seem to be fairly common.

we deduce in particular that $y + \log(q_E) \cdot x$ is in $\mathrm{Fil}^0 D_{\mathrm{dR}}(V_p E_{q_E})$. In fact, it spans Fil^0, because this space is 1-dimensional. Thus, in the basis y, x one has

$$\mathrm{Fil}^{-1} D_K = D_K, \qquad \mathrm{Fil}^0 D_K = K\big(y + \log(q_E)x\big), \qquad \mathrm{Fil}^1 D_K = 0.$$

Finally we rewrite this in the monodromy-normalised basis e_0, e_1, obtaining

$$y + \log(q_E)x = e_0 - \frac{\log(q_E)}{v_p(q_E)} e_1 = e_0 - \mathcal{L}(E_{q_E}) e_1.$$

3.7.4. *Correspondence with elliptic curves.* Let $E/\mathbb{Q}_p$ have bad semistable reduction and let $D = D_{\mathrm{st}}(V_p E)$. By dualising the result of Proposition 3.18 and comparing it with the computation of the filtered (φ, N)-module of the Tate curve E_{q_E}, we find that every module classified by Proposition 3.18 with $\alpha = 1$ is the (φ, N)-filtered module corresponding to a Tate curve. An additional short argument shows that every module with $\alpha = -1$ arises as $D_{\mathrm{st}}(V_p E_{q_E}^{(d)})$ for a suitable quadratic twist of a Tate curve. Thus, every module we found on the linear algebra side does arise from an elliptic curve over $\mathbb{Q}_p$.

3.8. **A final comment.** Note that, in all the cases we have studied in this lecture (which are essentially all the semistable cases over $\mathbb{Q}_p$), it is relatively easy to compute the relevant linear-algebraic object starting from the elliptic curve. Specifically, if E has good reduction, the filtered φ-module is determined by $\#\tilde{E}(k)$, plus the information of whether or not E is the canonical lift in the ordinary case. In the multiplicative situation, the filtered (φ, N)-module is determined by the parameter q_E, which may be computed to arbitrary precision by explicit formulas in terms of the j-invariant of E (see Remark 3.22), and a sign, corresponding to whether the reduction is split multiplicative or non-split multiplicative. By contrast, in the situations that we will study in the next two lectures (potentially good supersingular reduction), it seems quite hard to compute the filtered φ-module from an explicit equation of E. Solving this problem is one of the contributions of [BFL26].

4. Filtered modules with descent data and Volkov's classification

4.1. **What do we do today?** The preceding lecture described the rank-two weakly admissible filtered (φ, N)-modules that occur for good and semistable reduction over $\mathbb{Q}_p$. We now explain what changes for elliptic curves that acquire good reduction only after a finite extension. The representation becomes crystalline over that extension, so the linear algebra is not too different from what we saw; the new datum is descent from the good reduction field back to $\mathbb{Q}_p$.

We will not prove the classification, but state the part of it needed later. The proof has two main steps. First one runs a classification of weakly admissible filtered modules, much as in the previous lecture, but now with descent data. Second, one determines which of these abstract filtered modules are realised by elliptic curves over $\mathbb{Q}_p$. The second step is geometric; we refer to [Vol98, Vol01] for the proof, and only note that it uses in an essential way the Serre-Tate theory of deformations of abelian varieties.

4.2. **Filtered φ-modules with descent data.** Let $K/\mathbb{Q}_p$ be a finite Galois extension, let k be its residue field, and put $K_0 = W(k)[1/p]$. Write $G_{K/\mathbb{Q}_p} := \mathrm{Gal}(K/\mathbb{Q}_p)$, and let σ be the absolute p-power Frobenius of K_0.

Definition 4.1 (Filtered $(\varphi, G_{K/\mathbb{Q}_p})$-module)**.** A filtered $(\varphi, G_{K/\mathbb{Q}_p})$-module over $K/\mathbb{Q}_p$ is a finite-dimensional K_0-vector space D equipped with

(1) a bijective σ-semilinear map $\varphi : D \to D$,
(2) 'descent data': a semilinear action of $G_{K/\mathbb{Q}_p}$ on D commuting with φ,
(3) a decreasing, separated, exhaustive filtration on $D_K := D \otimes_{K_0} K$ by $G_{K/\mathbb{Q}_p}$-stable K-subspaces.

In (2), semilinearity means that $g(ax) = g(a)g(x)$ for $a \in K_0$, $x \in D$, and $g \in G_{K/\mathbb{Q}_p}$.

In Fontaine's theory, representations of $G_{\mathbb{Q}_p}$ that become crystalline over K correspond to such objects. Subobjects in this category are required to be stable under both φ and the descent action, and weak admissibility is imposed by the same Hodge–Newton inequalities as before, with this restricted class of subobjects.

4.3. **The contravariant convention.** Before stating the classification, we discuss in greater detail the contravariant convention, which is different from what we have used so far. Volkov works with the rational Tate module V_pE and the contravariant functor $D^*_{\mathrm{cris},K/\mathbb{Q}_p}$. If V is a $\mathbb{Q}_p$-representation of $G_{\mathbb{Q}_p}$ that becomes crystalline over K, then

$$D^*_{\mathrm{cris},K/\mathbb{Q}_p}(V) := \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{\mathrm{cris}}).$$

This is a K_0-vector space with Frobenius, a filtration after extension of scalars to K, and descent data coming from the action of $G_{K/\mathbb{Q}_p}$. The theory we've developed so far applies essentially in the same way, except for the fact that the Hodge–Tate weights are $0, 1$ instead of $-1, 0$ (equivalently: it is the dual theory to the covariant convention we've used so far).

4.4. **The modules D_α in the potentially supersingular case.** We now record the one-parameter family of filtered modules that occurs for potentially supersingular elliptic curves of semistability defect $e \in \{3, 4, 6\}$ (see Definition 1.18).

Notation and conventions. Assume $p > 3$ and $e \mid p + 1$. Let π_e satisfy $\pi_e^e = -p$, let ζ_e be a primitive e-th root of unity, and put $K = \mathbb{Q}_p(\pi_e, \zeta_e)$. Then $K_0 = \mathbb{Q}_p(\zeta_e) = \mathbb{Q}_{p^2}$, the unique unramified quadratic extension of $\mathbb{Q}_p$. The group $G_{K/\mathbb{Q}_p}$ is generated by elements ω and τ_e with

$$\omega(\zeta_e) = \zeta_e^{-1}, \quad \omega(\pi_e) = \pi_e,$$
$$\tau_e(\zeta_e) = \zeta_e, \quad \tau_e(\pi_e) = \zeta_e \pi_e.$$

Note that ω is a lift of Frobenius (where, in this case, the Frobenius is the generator of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$, which is a quotient of $G_{K/\mathbb{Q}_p}$), while τ_e is a generator of the inertia subgroup of $G_{K/\mathbb{Q}_p}$.

Remark 4.2. It is an easy consequence of the general theory of elliptic curves over $\mathbb{Q}_p$ that any $E/\mathbb{Q}_p$ with semistability defect e acquires semistable reduction over K. One can also show that semistability defects $e \in \{3, 4, 6\}$ can only arise in the potentially good reduction case, so in our setting, E_K actually has good reduction.

Definition 4.3. For $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, define D_α as follows.

(1) As a $\mathbb{Q}_{p^2}$-vector space, $D_\alpha = \mathbb{Q}_{p^2} b_1 \oplus \mathbb{Q}_{p^2} b_2$.
(2) The Frobenius is the σ-semilinear map determined by $\varphi(b_1) = b_2$ and $\varphi(b_2) = -pb_1$.
(3) The descent action is given by $\omega(b_i) = b_i$ for $i = 1, 2$, and by $\tau_e(b_1) = \zeta_e b_1$, $\tau_e(b_2) = \zeta_e^{-1} b_2$.
(4) The filtration on $(D_\alpha)_K$ has filtered pieces $\mathrm{Fil}^0(D_\alpha)_K = (D_\alpha)_K$, $\mathrm{Fil}^2(D_\alpha)_K = 0$, and

$$\mathrm{Fil}^1(D_\alpha)_K = K\big(b_1 \otimes \pi_e^{-1} + \alpha^{-1} b_2 \otimes \pi_e\big),$$

where $\alpha^{-1} = 0$ for $\alpha = \infty$. For $\alpha = 0$, this line is understood as $K(b_2 \otimes \pi_e)$.

Remark 4.4.

- Note that the only continuous parameter in D_α is α, which may be interpreted as a coordinate for the Hodge filtration. The underlying Frobenius and descent data are fixed once e is fixed; only the filtration line moves.
- The filtration line is compatible with the descent action. For example, τ_e fixes both $b_1 \otimes \pi_e^{-1}$ and $b_2 \otimes \pi_e$, because its action on the basis is cancelled by its action on π_e. Thus the line in Definition 4.3 is $G_{K/\mathbb{Q}_p}$-stable.

Theorem 4.5 (Volkov [Vol98])**.** *Let $e \in \{3, 4, 6\}$ and let $p > 3$ be a prime with $e \mid p + 1$. For every elliptic curve $E/\mathbb{Q}_p$ with semistability defect e, there is an $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$ such that $D^*_{\mathrm{cris},K/\mathbb{Q}_p}(V_p E)$ is isomorphic to D_α. Conversely, for every $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$ there exists an elliptic curve $E/\mathbb{Q}_p$ with semistability defect e and potentially supersingular reduction such that $D^*_{\mathrm{cris},K/\mathbb{Q}_p}(V_p E) \cong D_\alpha$.*

The theorem can be viewed as a refinement of weak admissibility: weak admissibility tells us which filtered modules come from p-adic representations, while Theorem 4.5 identifies which of the relevant modules come from (potentially supersingular) elliptic curves over $\mathbb{Q}_p$.

Remark 4.6. Volkov's PhD thesis [Vol98] classifies all the relevant linear algebra objects arising from elliptic curves over $\mathbb{Q}_p$, not only in the restricted setting of Theorem 4.5.

In the rest of this lecture, we describe explicitly the inverse functor

$$\{\text{filtered } (\varphi, G_{K/\mathbb{Q}_p})\text{-modules}\} \to \{p\text{-adic Galois representations}\}.$$

This will require at least a passing acquaintance with the period ring B_{dR}.

4.5. **Witt vectors.** An important ingredient in Fontaine's construction of B_{dR} is the ring of Witt vectors. The slogan is that Witt vectors provide a canonical way of lifting a perfect ring of characteristic p to a p-adically complete ring of characteristic 0, and they do so while remembering Frobenius. We briefly review the construction.

Example 4.7. A very useful example to have in mind is that $W(\mathbb{F}_{p^n})$ is the ring of integers in the unique unramified extension of $\mathbb{Q}_p$ of degree n.

4.5.1. *Definition and operations.* Let A be a commutative ring. The ring of p-typical Witt vectors $W(A)$ is, as a set, $A^{\mathbb{N}}$, but its addition and multiplication are not componentwise. For variables $X_0, X_1, \ldots$, define the Witt polynomials

$$w_n(X_0, \ldots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n.$$

The *ghost map* is the map

$$\begin{array}{rccc} w: & W(A) & \longrightarrow & A^{\mathbb{N}} \\ & (a_0, a_1, \ldots) & \longmapsto & \big(w_0(a_0), w_1(a_0, a_1), \ldots\big). \end{array}$$

There are universal polynomials with integer coefficients defining addition and multiplication on $A^{\mathbb{N}}$ such that the ghost map becomes a ring homomorphism.

Warning 4.8. This point is a source of unending confusion. If A is a ring of characteristic p, the ghost map is rather uninteresting, because $w_n(X_0, \ldots, X_n) = X_0^{p^n}$ *as a polynomial in* $A[x_0, \ldots, x_n]$. However, the point is that the addition formulae in $W(A)$ are defined by polynomials such that the ghost map is a ring homomorphism for *any* A, including rings of characteristic 0.

Let us stress this point again: given $a = (a_0, a_1, \ldots)$ and $b = (b_0, b_1, \ldots)$ in $W(A)$, the i-th coordinate of the element $c := a + b = (c_0, c_1, c_2, \ldots)$ is given by a polynomial $S(a_0, \ldots, a_i, b_0, \ldots, b_i)$ which is *independent of the ring* A (it depends only on p and i). In the next example, we show how to determine $S_0(a_0, b_0)$ and $S_1(a_0, a_1, b_0, b_1)$. Before doing so, we point out that a good way to understand this point is to think that the Witt vectors are a ring object in the category of schemes, equipped with a morphism of ring schemes to $\mathbb{A}^{\mathbb{N}}$ (the ghost map).

Example 4.9. The first coordinate of addition is the obvious one: since w_0 is the identity, if $a+b = c$ in $W(A)$, then $c_0 = a_0 + b_0$. To see this, note that *for every ring* A we require $c_0 = w_0(c_0) = w_0(a_0) + w_0(b_0) = a_0 + b_0$.

The next coordinate can be found by imposing the equality of the next ghost components: comparing

$$w_1(c) = w_1(a + b) = w_1(a) + w_1(b) = a_0^p + pa_1 + b_0^p + pb_1$$

with

$$w_1(c) = c_0^p + pc_1 = (a_0 + b_0)^p + pc_1,$$

we obtain

$$pc_1 = pa_1 + pb_1 - ((a_0 + b_0)^p - a_0^p - b_0^p)\,.$$

This has to hold *for any ring* A, including those in which multiplication by p is injective, so the only possibility is to take

$$S_1(a_0, a_1, b_0, b_1) = a_1 + b_1 - \frac{(a_0 + b_0)^p - a_0^p - b_0^p}{p}.$$

The displayed quotient has integral coefficients as a polynomial in a_0 and b_0, even though it is written with a p in the denominator. One can iterate such computations to obtain polynomials with integer coefficients (depending only on n and p) such that

$$(a + b)_n = S_n(a_0, \ldots, a_n, b_0, \ldots, b_n).$$

4.5.2. *Teichmüller lifts.* Given $a \in A$, we write $[a]$ for the element of $W(A)$ corresponding to $(a, 0, 0, \ldots)$. This is called the *Teichmüller representative* or *Teichmüller lift* of $a \in A$. The map $a \mapsto [a]$ is easily seen to be multiplicative, but it is not additive.

4.5.3. *Frobenius and Verschiebung.* Frobenius and Verschiebung on $W(A)$ are easy to express: if A is perfect of characteristic p, we have

$$\varphi(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots), \qquad V(a_0, a_1, \ldots) = (0, a_0, a_1, \ldots),$$

and $\varphi V = V\varphi = p$ as endomorphisms of the additive group of $W(A)$. In this perfect characteristic-p case, every Witt vector has a unique convergent Teichmüller expansion

$$a = \sum_{n \geq 0} p^n [a_n], \qquad a_n \in A.$$

The ring $W(A)$ is the (unique, up to isomorphism) *strict p-ring* with residue ring A: it is p-torsion-free, p-adically complete and separated, and its reduction modulo p is A.

4.5.4. *Sources of confusion.* One of the reasons Witt vectors $W(A)$ are so confusing is that they have *three* 'natural' representations: the *Witt* components, the *Teichmüller* components, and the *ghost* components.

Warning 4.10. This is not standard notation, but I hope it's useful for me to point out the difference. Also, note that the ghost map is not injective when A has p-torsion (which is usually the case we care about when using Witt vectors), so the ghost components are not a genuine coordinate system.

The idea is that a Witt vector $a = (a_0, a_1, a_2 \ldots) \in W(A)$ can manifest in three different forms (only the first two encode a completely; the third one loses information if A has p-torsion):

- (Witt) as $a = \sum_{n \geq 0} V^n([a_n])$, see Remark 4.12 below;
- (Teichmüller) as $a = \sum_{n \geq 0} [b_n] p^n$;
- (Ghost) via the sequence $(w_0(a), w_1(a), w_2(a), \ldots) \in A^{\mathbb{N}}$, which has the advantage that operations are component-wise.

The Teichmüller components are those that correspond to the p-adic filtration. Given a, we can recursively construct the b_n as

$$b_0 = a_0, \quad b_{n+1} = a - \sum_{m=0}^{n} [b_m]p^m \in p^{n+1}W(A)/p^{n+2}W(A) \cong A.$$

Analogously, the Witt coordinates are the coordinates for the V-adic filtration: we have $a_0 = a_0$ (tautologically...) and

$$a_{n+1} = a - \sum_{m=0}^{n} V^m([a_m]) \in V^{n+1}W(A)/V^{n+2}W(A) \cong A.$$

The ghost components are given in terms of the Witt components by the explicit Witt polynomials. The next remark makes the connection between the Witt and Teichmüller components.

Remark 4.11 (Coefficients of the Teichmüller expansion)**.** Let A be a perfect $\mathbb{F}_p$-algebra. One can check (see Remark 4.12 below) that every Witt vector $a = (a_0, a_1, a_2, \ldots) \in W(A)$ can be written as

$$a = \sum_{n\geq 0}(0, \ldots, 0, \underbrace{a_n}_{\text{position } n}, 0, 0, \ldots) = \sum_{n\geq 0} V^n([a_n]).$$

On the other hand, the equality $\varphi V = p$ gives $p^n[b] = V^n([b^{p^n}])$ for every $b \in A$. Since A is perfect, we can write uniquely $a_n = (a_n^{p^{-n}})^{p^n}$ to obtain

$$a = \sum_{n\geq 0} V^n([a_n]) = \sum_{n\geq 0} V^n([(a_n^{p^{-n}})^{p^n}]) = \sum_{n\geq 0} p^n[a_n^{p^{-n}}]. \tag{6}$$

By uniqueness of the Teichmüller expansion, we get $b_n = a_n^{p^{-n}}$.

Remark 4.12. Let $w_m(X_0, \ldots, X_m) = X_0^{p^m} + pX_1^{p^{m-1}} + \cdots + p^m X_m$ be the m-th Witt polynomial. For $x \in A$, the ghost coordinates of $V^n([x]) = V^n((x, 0, 0, \ldots)) = (0, 0, \ldots, \underbrace{x}_{x_n \text{ coordinate}}, 0, \ldots)$ are

$$w_m(V^n([x])) = \begin{cases} 0, & m < n, \\ p^n x^{p^{m-n}}, & m \geq n. \end{cases}$$

Therefore, for $s_N = \sum_{n=0}^{N} V^n([a_n])$, we have

$$w_m(s_N) = \sum_{n=0}^{\min(m,N)} p^n a_n^{p^{m-n}},$$

which is precisely the m-th ghost coordinate of the Witt vector $(a_0, a_1, \ldots, a_N, 0, 0, \ldots)$. Since the addition polynomials are universal, this calculation proves the identity

$$\sum_{n=0}^{N} V^n([a_n]) = (a_0, a_1, \ldots, a_N, 0, 0, \ldots);$$

by passing to the limit in N, we obtain $(a_0, a_1, a_2, \ldots) = \sum_{n\geq 0} V^n([a_n])$.

4.6. **Fontaine's construction of B_{dR}.**

4.6.1. *The ring A_{inf}.* We now take A to be

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

this is the *perfection* of the characteristic-p ring $\mathcal{O}_{\mathbb{C}_p}/(p)$. Concretely[6], an element $x \in R$ is a sequence

$$x = (x_0, x_1, x_2, \ldots) \in (\mathcal{O}_{\mathbb{C}_p}/(p))^{\mathbb{N}}$$

such that $x_{n+1}^p = x_n$ in $\mathcal{O}_{\mathbb{C}_p}/(p)$.

Exercise 4.13. Check that R is a perfect ring: it is a ring of characteristic p and $x \mapsto x^p$ is an automorphism.

[6] if I may be forgiven for using such a word in this context...

We denote by $x^\sharp \in \mathcal{O}_{\mathbb{C}_p}$ the *untilt* of x, obtained by choosing lifts $\widehat{x}_m \in \mathcal{O}_{\mathbb{C}_p}$ of the components x_m and setting

$$x^\sharp = \lim_{m\to\infty} \widehat{x}_m^{p^m}.$$

This limit exists and is independent of the choices of the lifts. The map $x \mapsto x^\sharp$ is multiplicative, but not additive. More generally, we set

$$x^{(n)} := \lim_{m\to\infty} \widehat{x}_{m+n}^{p^m},$$

which is again a well-defined element of $\mathbb{C}_p$. Note that $x^\sharp = x^{(0)}$.

Remark 4.14. These elements $x^{(n)}$ form a compatible system, in the following sense. By definition we have $x_{n+1}^p = x_n$, so if $\widehat{x}_{m+n}$ is a lift of x_{m+n}, then $\widehat{x}_{m+n}^p$ is a lift of $x_{m+n}^p = x_{m+n-1}$. Hence

$$\left(x^{(n)}\right)^p = \lim_{m\to\infty} \left(\widehat{x}_{m+n}^p\right)^{p^m} = \lim_{m\to\infty} (\widehat{x}_{m+n-1})^{p^m} = x^{(n-1)}.$$

In particular, the knowledge of x gives, for each $n \geq 1$, a privileged choice of p^n-th root of $x^\sharp = x^{(0)} \in \mathbb{C}_p$, given by $x^{(n)}$.

Exercise 4.15. Check that for all positive k we have $(a^{p^{-k}})^\sharp = a^{(k)}$.

The valuation on R is $v_R(x) = v_p(x^\sharp)$, and its maximal ideal is denoted $\mathfrak{m}_R$. We define $A_{\mathrm{inf}} = W(R)$.

4.6.2. *Fontaine's map.* We define Fontaine's map

$$\theta : A_{\mathrm{inf}} = W(R) \longrightarrow \mathcal{O}_{\mathbb{C}_p}$$

as the unique continuous ring homomorphism satisfying $\theta([x]) = x^\sharp$ for all $x \in R$. Equivalently, if $x = \sum_{n\geq 0} p^n[x_n]$ is the Teichmüller expansion of an element of $W(R)$, then

$$\theta(x) = \sum_{n\geq 0} p^n x_n^\sharp.$$

It's not too hard to show that θ is surjective.

4.6.3. *Fontaine's cyclotomic period.* Choose a compatible system of p-power roots of unity

$$\varepsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in R, \qquad \zeta_{p^{n+1}}^p = \zeta_{p^n}, \quad \zeta_p \neq 1.$$

Fontaine's cyclotomic period is

$$t = \log([\varepsilon]) = \sum_{m\geq 1} (-1)^{m+1} \frac{([\varepsilon]-1)^m}{m}.$$

This makes sense in the $\ker(\theta)$-adic completion of $A_{\mathrm{inf}} = W(R)$, because $[\varepsilon] - 1$ is in $\ker\theta$: indeed, by definition we have

$$\theta([\varepsilon]) = \varepsilon^\sharp = 1,$$

because we can take $\hat{\varepsilon}_m = \zeta_{p^m}$ to obtain

$$\varepsilon^\sharp = \lim_{m\to\infty} (\hat{\varepsilon}_m)^{p^m} = \lim_{m\to\infty} (\zeta_{p^m})^{p^m} = 1.$$

4.6.4. *Definition of B_{dR}.* The de Rham period ring B_{dR}^+ is the completion of $A_{\mathrm{inf}}[1/p]$ with respect to the kernel of θ:

$$B_{\mathrm{dR}}^+ = \widehat{A_{\mathrm{inf}}[1/p]}^{\ker\theta}.$$

One finally defines B_{dR} as the quotient field of B_{dR}^+, or equivalently as $B_{\mathrm{dR}} = B_{\mathrm{dR}}^+[1/t]$, where t is as above. The filtration on B_{dR} is the $\ker\theta$-adic filtration on B_{dR}^+, extended after inverting t; in particular, $\mathrm{Fil}^1 B_{\mathrm{dR}}^+ = \ker(\theta : B_{\mathrm{dR}}^+ \to \mathbb{C}_p)$.

Remark 4.16. Since θ extends to a continuous ring homomorphism $B_{\mathrm{dR}}^+ \to \mathbb{C}_p$, applying θ term by term gives

$$\theta(t) = \sum_{m\geq 1} \frac{(-1)^{m+1}}{m} \theta(([\varepsilon]-1)^m) = \sum_{m\geq 1} \frac{(-1)^{m+1}}{m} \cdot 0 = 0.$$

Thus t is indeed an element of $\ker\theta$.

4.7. **Witt bivectors.** The usual Witt vectors only have coordinates indexed by $n \geq 0$. Fontaine's bivectors allow (infinitely many) negative Witt coordinates, which however are not arbitrary, in the sense that they must stay bounded with respect to the metric induced by v_R. We won't go into too many details; the interested reader may refer to [Fon82, §6.3].

The intuition is that the series $\sum_n [a_n^{p^{-n}}]p^n$ that we considered in Remark 4.11 makes sense (in $W(R)[1/p]$) also if we extend it to $n \geq -n_0$, provided that there are only finitely many non-zero summands. Taking a suitable completion (which lets us take $n_0 \to \infty$), one is led to the following definition.

Definition 4.17 (Witt bivectors)**.** The set of Witt bivectors over R, denoted $BW(R)$, is

$$BW(R) = \{(x_n)_{n\in\mathbb{Z}} \,|\, x_n \in R, \exists n_0 \in \mathbb{Z},\ \exists \varepsilon > 0 \text{ such that } v_R(x_n) > \varepsilon \text{ for all } n < n_0\}\,.$$

It is endowed with the following structures.

- Operations. For the 'finite' bivectors $\sum_{n\geq -n_0}[a_n^{p^{-n}}]p^n$, they are induced by the operations on $W(R)[1/p]$. Passing suitably to the limit, one finds for example that for $a, b \in BW(R)$ and $d = a +_{BW} b$, the zeroth component of the sum is
$$d_0 = \lim_{m\to\infty} S_m(a_{-m}, \dots, a_0; b_{-m}, \dots, b_0),$$
where S_m is the m-th Witt addition polynomial.
- Frobenius and Verschiebung: we have $\varphi((a_n)_n) = (a_n^p)_n$ and $V((a_n)_n) = (a_{n-1})_n$. These maps satisfy $\varphi V = V\varphi = p$, multiplication by p in $BW(R)$.
- Galois action. The Galois group $G_{\mathbb{Q}_p}$ acts on R, hence componentwise on $BW(R)$, and this action commutes with φ and V.
- Filtration. The ring $BW(R)$ embeds into B_{dR}; we give it the induced filtration, namely $\mathrm{Fil}^i BW(R) := BW(R) \cap \mathrm{Fil}^i B_{\mathrm{dR}}$.

The embedding into B_{dR} is constructed as follows. If a bivector $\sum_{n\geq -n_0}[a_n^{p^{-n}}]p^n$ has only finitely many negative coordinates, then this sum already lies in $W(R)[1/p] = A_{\mathrm{inf}}[1/p]$, and hence maps to B_{dR}. A result of Fontaine shows that after completing one still obtains a well-defined injection

$$\iota : BW(R) \hookrightarrow B^+_{\mathrm{cris}} \hookrightarrow B^+_{\mathrm{dR}}.$$

In particular, θ extends to $BW(R)$ by restriction from B^+_{dR}:

$$\theta_{BW} : BW(R) \longrightarrow \mathbb{C}_p, \qquad \theta_{BW}(x) = \theta_{\mathrm{dR}}(\iota(x)).$$

For a bivector $\sum_{n=N}^{\infty} p^n[x_n]$ with finite negative tail, the extension is given by the formula

$$\theta_{BW}\left(\sum_{n=N}^{\infty} p^n[x_n]\right) = \sum_{n=N}^{\infty} p^n x_n^\sharp. \tag{7}$$

For a general bivector, this formula should be treated with some care. For the special bivectors we will use later, the valuations of the coordinates grow fast enough (as $n \to -\infty$) that the corresponding Laurent series (that is, (7) for $N = -\infty$ – the series extended to all $n \in \mathbb{Z}$) does converge in $\mathbb{C}_p$.

Remark 4.18. Assuming convergence, and recalling that $\mathrm{Fil}^1 B_{\mathrm{dR}} = \ker\theta|_{B^+_{\mathrm{dR}}}$, we obtain that a Witt bivector $\sum_{n=N}^{\infty} p^n[x_n]$ is in Fil^1 if and only $\sum_{n\in\mathbb{Z}} p^n x_n^\sharp = 0$. Note that if the bivector is $\underline{a} = (a_n)_{n\in\mathbb{Z}}$, then as explained in Remark 4.11 we have $\underline{a} = \sum_n p^n[a_n^{p^{-n}}]$, and hence the condition for $\underline{a}$ to be in Fil^1 is $\sum_{n\in\mathbb{Z}} p^n \left(a_n^{p^{-n}}\right)^\sharp = 0$.

4.8. **Recovering the representation from D_α.** We now describe the inverse functor of $D^*_{\mathrm{cris},K/\mathbb{Q}_p}$ in a concrete form. Let D_α be as in Definition 4.3. One can recover the Galois representation corresponding to D_α as

$$V_\alpha := \mathrm{Hom}_{\text{filtered } \varphi\text{-modules}}(D_\alpha, BW(R)), \tag{8}$$

where the homomorphisms are taken in the category of filtered φ-modules.

Let us describe V_α explicitly. Since we are working in the setting of Theorem 4.5, we assume $p > 3$; in particular, p is odd.

(1) Set. First of all, elements of V_α are $\mathbb{Q}_{p^2}$-linear maps $u : D_\alpha \to BW(R)$, so they are uniquely determined by $u(b_1)$ and $u(b_2)$.

(2) Compatibility with Frobenius. We get

$$u(b_2) = u(\varphi(b_1)) = \varphi(u(b_1)),$$

so that u is in fact determined by $u(b_1) \in BW(R)$ alone. We also have

$$\varphi^2(u(b_1)) = \varphi(u(b_2)) = u(\varphi(b_2)) = u(-pb_1) = -pu(b_1),$$

so $u(b_1)$ satisfies the equation $\varphi^2(\underline{x}) = -p\underline{x}$. Write

$$\underline{x} = (\dots, x_{-2}, x_{-1}, x_0, x_1, x_2, \dots) = (x_n)_{n\in\mathbb{Z}} \in BW(R)$$

and recall that multiplication by p in $BW(R)$ sends $\underline{x}$ to

$$V\varphi(\underline{x}) = V(x_n^p)_{n\in\mathbb{Z}} = (x_{n-1}^p)_{n\in\mathbb{Z}},$$

while

$$-\varphi^2(\underline{x}) = (-x_n^{p^2})_{n\in\mathbb{Z}}.$$

We deduce $x_{n-1}^p = -x_n^{p^2}$, that is (since R is perfect) $x_{n-1} = -x_n^p$. Thus, $u(b_1)$ is of the form

$$u(b_1) = (\dots, -a^{p^3}, a^{p^2}, -a^p; a, -a^{p^{-1}}, a^{p^{-2}}, \cdots) = ((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}}. \tag{9}$$

Note that, in order for this to be in $BW(R)$, we need that there is some $\varepsilon > 0$ such that the valuation of $u(b_1)_n$ is at least ε for all $n < n_0$. This clearly happens if and only if the valuation of a is positive.

(3) Filtration (after extending scalars to K). This is the most interesting part. The line Fil^1 in $(D_\alpha)_K$ is by definition generated by $b_1 \otimes \pi_e^{-1} + \alpha^{-1} b_2 \otimes \pi_e$. In order for u to respect the filtration, this vector has to be sent inside the subspace $\mathrm{Fil}^1(BW(R) \otimes_{K_0} K)$, which we have described in Remark 4.18 as the kernel of (a suitable extension of) Fontaine's map θ. As a preliminary step, using Equation (6) we write

$$u(b_1) = ((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}} = \sum_{n\in\mathbb{Z}} p^n \cdot [(-1)^n a^{p^{-2n}}]$$

and

$$\varphi(u(b_1)) = ((-1)^n a^{p^{1-n}})_{n\in\mathbb{Z}} = \sum_{n\in\mathbb{Z}} p^n \cdot [(-1)^n a^{p^{1-2n}}].$$

Using (7) (the relevant convergence hypotheses are satisfied), we compute

$$\theta_{BW}(u(b_1)) = \sum_{n\in\mathbb{Z}} p^n \cdot ((-1)^n a^{p^{-2n}})^\sharp = \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{p^{-2n}})^\sharp$$

and

$$\theta_{BW}(\varphi(u(b_1))) = \sum_{n\in\mathbb{Z}} p^n \cdot ((-1)^n a^{p^{1-2n}})^\sharp = \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{p^{1-2n}})^\sharp.$$

Recall that the untilt map $b \mapsto b^\sharp$ is multiplicative, so for $k < 0$ we have $(a^{p^{-k}})^\sharp = (a^\sharp)^{p^{-k}}$, while for $k > 0$ the untilt $(a^{p^{-k}})^\sharp$ satisfies $\left((a^{p^{-k}})^\sharp\right)^{p^k} = a^\sharp$, so it is a specific p^k-th root of $a^\sharp$. By Exercise 4.15, for $k \geq 0$ we have $a^{(k)} = (a^{p^{-k}})^\sharp$. For $k < 0$, we use the notation $a^{(k)} := (a^{(0)})^{p^{|k|}}$.

Finally, we write the filtration condition in completely explicit form:

$$\begin{aligned}
0 &= \theta_{BW}\left(u(b_1 \otimes \pi_e^{-1} + \alpha^{-1} b_2 \otimes \pi_e)\right) = \pi_e^{-1} \cdot \theta_{BW}(u(b_1)) + \alpha^{-1}\pi_e \cdot \theta_{BW}(\varphi(u(b_1))) \\
&= \pi_e^{-1} \cdot \theta_{BW}\left(((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}}\right) + \alpha^{-1}\pi_e \cdot \theta_{BW}\left(((-1)^n a^{p^{1-n}})_{n\in\mathbb{Z}}\right) \\
&= \pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{p^{-2n}})^\sharp + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{p^{1-2n}})^\sharp \\
&= \pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot a^{(2n)} + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot a^{(1-2n)} \\
&= \pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{(0)})^{p^{-2n}} + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot (a^{(0)})^{p^{1-2n}}.
\end{aligned} \tag{10}$$

(4) Galois action. The absolute Galois group G_K acts on $V_\alpha \subset \mathrm{Hom}(D_\alpha, BW(R))$ by acting on the value in $BW(R)$. This action extends to $G_{\mathbb{Q}_p}$ by using the descent datum: if $g \in G_{\mathbb{Q}_p}$ and $[g^{-1}]$ denotes the image of g^{-1} in $G_{K/\mathbb{Q}_p}$, then

$$(g \cdot u)(d) := g(u([g^{-1}]d)).$$

4.9. **Final comments.** We conclude with several remarks.

(1) The last line in the chain of equalities (10) is less precise than the previous one, but it conveys the right idea: $a^{(0)}$ is a root of a certain infinite series, which however has both integer and fractional exponents.

(2) There are no issues of convergence in (10). Indeed, the valuation of the general term of the first sum is $n + p^{-2n}v(a^{(0)})$, which (since $v(a^{(0)}) > 0$) tends to infinity both as $n \to \infty$ and as $n \to -\infty$.

(3) Note that we have explicitly described the Tate module V_pE as the set of solutions in $\mathbb{C}_p$ of (10). Indeed, our V_α is a set of linear maps u, but we have proved that u depends only on $u(b_1) \in BW(R)$, and that $u(b_1)$ should be a solution of (10). This is a fairly concrete model for a complicated object such as the Tate module of an elliptic curve!

(4) The vector space structure on V_α is complicated. However, it is at least easy to describe multiplication by p, which we recall is the same as the composition $V\varphi$ on the target. Since $u \in V_\alpha$ is determined by $u(b_1)$, it suffices to compute $V\varphi(u(b_1))$: if $u(b_1) = ((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}}$ as in (9), then

$$V\varphi(u(b_1)) = ((-1)^{n-1}(a^{p^{-(n-1)}})^p)_{n\in\mathbb{Z}} = ((-1)^{n-1}a^{p^{1-n}})_{n\in\mathbb{Z}}.$$

It is easy to check that if $((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}}$ is a solution to (10), then so is $((-1)^{n-1}a^{p^{1-n}})_{n\in\mathbb{Z}}$: we are just shifting indices. More precisely, writing $\underline{x} = u(b_1) = (x_m)_{m\in\mathbb{Z}}$ and $\underline{y} = V\varphi(u(b_1)) = (x_{m-1}^p)_{m\in\mathbb{Z}}$, we can compute $\underline{y}^{(n)}$ using the lifts $\hat{y}^{(m)} = (\hat{x}^{(m-1)})^p = \hat{x}^{(m-2)}$. The fact that $u(b_1)$ is a solution of (10) gives

$$\pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot x^{(2n)} + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot x^{(1-2n)} = 0;$$

we need to show that also

$$\pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot x^{(2n-2)} + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot x^{(3-2n)} = 0.$$

Replacing $n \mapsto n+1$ in both sums, we get

$$\pi_e^{-1} \cdot \sum_{n\in\mathbb{Z}} (-1)^{n+1} p^{n+1} \cdot x^{(2n)} + \alpha^{-1}\pi_e \cdot \sum_{n\in\mathbb{Z}} (-1)^{n+1} p^{n+1} \cdot x^{(1-2n)} = 0,$$

which follows immediately upon collecting a factor of $-p$ from each sum.

(5) When $\alpha^{-1} = 0$ or $\alpha = 0$, the equation has extra symmetries: since $p^{2n} \equiv 1 \pmod 6$ and $p^{2n} \equiv 1 \pmod 4$, given a solution to the equation, we can obtain another solution by multiplying each coordinate by ζ_6 or ζ_4. This is not a coincidence: in the classification of Theorem 4.5, the cases $\alpha \in \{0, \infty\}$ correspond to E of the form $y^2 = x^3 + A$ or $y^2 = x^3 + Bx$, that is, the elliptic curves with complex multiplication by ζ_6 or ζ_4.

(6) The relatively concrete description we have given for V_pE leaves open two natural questions:

(a) What sort of information can one extract from (10)? In particular, can we describe the image of the Galois representation on V_pE?

(b) Given a concrete elliptic curve $E/\mathbb{Q}_p$ with potentially supersingular reduction and semistability defect $e \in \{3, 4, 6\}$ with $e \mid p+1$, how does one compute the invariant α corresponding to E (that is, such that $V_\alpha \cong V_pE$)? In all the cases we have seen in the previous lecture, reading off *which* linear algebra object corresponds to a given elliptic curve was (relatively) easy. In the potentially good supersingular case, Volkov's proof of Theorem 4.5 is constructive only in the other direction (given α, construct an $E/\mathbb{Q}_p$ such that $V_pE \cong V_\alpha$), and even then, the construction is extremely complicated. One of the objectives of the next lecture is to explain how to read off the parameter α from a Weierstrass equation for E.

5. Galois images of elliptic curves over $\mathbb{Q}_p$

5.1. **What do we do today?** The aim of this last lecture is to explain how the techniques described in the previous lectures have been applied in [BFL26] to explicitly describe the *images* of the Galois representations attached to elliptic curves over $\mathbb{Q}_p$ (and, as a consequence, over $\mathbb{Q}$).

5.2. **Motivation.** Let $E/\mathbb{Q}$ be an elliptic curve. In his landmark open image theorem [Ser72], Serre showed that ρ_{E,p^∞} is surjective when p is sufficiently large so long as E does not have potential complex multiplication (CM). In the same paper, he then posed a natural uniformity question: does there exist a constant N, such that $\rho_{E,p}$ (and hence also ρ_{E,p^∞}) is surjective for every prime $p > N$, uniformly in non-CM curves $E/\mathbb{Q}$? This became known as *Serre's uniformity question*. Despite substantial progress, the problem remains open, though it is conjectured to have an affirmative answer with optimal constant $N = 37$. The following result combines work of many authors.

Theorem 5.1 ([Ser81, Maz78, BP11, BPR13, Zyw15, LFL21, FL23])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p > 37$ be a prime. The image of $\rho_{E,p}$ is either $\mathrm{GL}_2(\mathbb{F}_p)$ or (conjugate to) $C_{\mathrm{ns}}^+(p)$, the normaliser of a non-split Cartan (to be defined shortly).*

Recent work has also led to significant progress towards the finer classification of possible p-adic images. When $p > 7$, Rouse–Sutherland–Zureick-Brown [RSZB22, Theorem 1.1.6] have classified the possible p-adic images unless $\mathrm{Im}\,\rho_{E,p} \subseteq C_{\mathrm{ns}}^+(p)$. In the non-split Cartan case, much less is known about the images of ρ_{E,p^n} for $n \geq 2$.

So as not to make these statements mysterious, let me recall right away what the normaliser of a non-split Cartan is.

5.2.1. *Non-split Cartans.* Let p be an odd prime. A non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is a subgroup conjugate to $\mathbb{F}_{p^2}^\times$, where $\mathbb{F}_{p^2}^\times$ acts on the two-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^2}$ by multiplication. Its normaliser is obtained by adjoining the non-trivial automorphism of $\mathbb{F}_{p^2}/\mathbb{F}_p$.

For example, if $d \in \mathbb{F}_p^\times$ is a nonsquare and we identify $\mathbb{F}_{p^2}$ with $\mathbb{F}_p[\sqrt{d}]$, then multiplication by $a+b\sqrt{d}$ in the basis $(1, \sqrt{d})$ is represented by $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$, while the non-trivial automorphism of $\mathbb{F}_{p^2}/\mathbb{F}_p$ acts by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Thus one model for $C_{\mathrm{ns}}(p)$ is

$$\left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p,\ (a,b) \neq (0,0) \right\}.$$

This group has order $p^2 - 1$ and is cyclic. Its normaliser, denoted by $C_{\mathrm{ns}}^+(p)$, is

$$\left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p,\ (a,b) \neq (0,0) \right\} \sqcup \left\{ \begin{pmatrix} a & bd \\ -b & -a \end{pmatrix} : a, b \in \mathbb{F}_p,\ (a,b) \neq (0,0) \right\}.$$

There are also obvious generalisations to subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$: we set

$$C_{\mathrm{ns}}^+(p^n) = \left\{ \begin{pmatrix} a & bd \\ \varepsilon b & \varepsilon a \end{pmatrix} : a, b \in \mathbb{Z}/p^n\mathbb{Z},\ \varepsilon \in \{\pm 1\},\ a^2 - db^2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

where d represents a non-square in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. This further generalises to $\mathrm{GL}_2(\mathbb{Z}_p)$ in the obvious way.

5.2.2. *Statement of the result.* Despite the fact that the motivation came from a problem about elliptic curves over $\mathbb{Q}$, most of the work in [BFL26] concerns elliptic curves over $\mathbb{Q}_p$, and in this lecture I will stick to this case. The most explicit form of the local result is as follows.

Theorem 5.2. *Let $p > 7$ be a prime and let $E/\mathbb{Q}_p$ be an elliptic curve with semistability defect e, and suppose that $\mathrm{Im}\,\rho_{E,p} \subseteq C_{\mathrm{ns}}^+(p)$. Then E has potentially good supersingular reduction and the following hold.*

(1) If $e \leq 2$ then $\mathrm{Im}\,\rho_{E,p^n} = C_{\mathrm{ns}}^+(p^n)$ for all $n \geq 1$.

(2) Suppose $e \geq 3$. Let j be the j-invariant of E and let n_0 be the positive integer

$$n_0 := \begin{cases} \lfloor \frac{1}{3} v(j) \rfloor & \text{if } e \in \{3, 6\} \\ \lfloor \frac{1}{2} v(j - 1728) \rfloor & \text{if } e = 4. \end{cases}$$

Let $\pi_{n_0} : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^{n_0}\mathbb{Z})$ be the canonical projection. If $p > \sqrt{n_0 + 1}$, then

$$\mathrm{Im}\, \rho_{E,p^{n_0}} \subseteq C_{\mathrm{ns}}^+(p^{n_0}) \text{ with index dividing } 3 \qquad \text{and} \qquad \mathrm{Im}\, \rho_{E,p^\infty} = \pi_{n_0}^{-1}(\mathrm{Im}\, \rho_{E,p^{n_0}}).$$

Moreover, if $e = 4$ or $p \not\equiv 2, 5 \bmod 9$, then $\mathrm{Im}\, \rho_{E,p^{n_0}} = C_{\mathrm{ns}}^+(p^{n_0})$.

This theorem gives two complementary pieces of information:

- Up to level p^{n_0}, the image of ρ_{E,p^n} remains contained in the normaliser of a non-split Cartan.
- After that level, the image starts 'growing maximally'.

The integer n_0 is therefore the exact level at which the behaviour changes from 'CM-like' or 'Cartan-like' to 'generic'. The definition of n_0 is relatively transparent: it is a measure of 'nearness' to the CM elliptic curves with j-invariant 0 or 1728, for which (as it is easy to show) the CM-like behaviour persists modulo p^n for all $n \geq 1$.

Remark 5.3. The theorem is very likely true also without the assumption $p > \sqrt{n_0 + 1}$.

Example 5.4. Let $p > 7$ be a prime with $p \equiv 3 \pmod 4$. Then the p-adic Galois representation attached to $E : y^2 = x^3 + px + p^5$ has image given by $\pi_3^{-1}(C_{\mathrm{ns}}^+(p^3))$.

I should point out that computing the image of even just ρ_{E,p^2} from the definitions would involve at the very least computing the splitting field over $\mathbb{Q}_p$ of a polynomial of degree $\frac{p^2-1}{2}$, in a situation where such splitting field is highly ramified. In practice, this seems to be completely out of computational reach even for $p = 11$.

Throughout this chapter we take $p > 7$ unless explicitly stated otherwise. Let v be the valuation on $\mathbb{C}_p$, normalised by $v(p) = 1$, and $E/\mathbb{Q}_p$ be an elliptic curve.

We use the results from Lecture 4: if E has semistability defect $e \in \{3, 4, 6\}$ and $e \mid p + 1$, then over $K = \mathbb{Q}_p(\pi_e, \zeta_e)$, with $\pi_e^e = -p$, the rational representation V_pE is described by the filtered $(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p))$-module D_α for some $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$ (see Theorem 4.5).

5.3. **Strategy of proof.** I'll start by giving a sketch of the proof strategy. This will hopefully make it clear where p-adic Hodge theory enters the picture.

(1) We start with an elliptic curve $E/\mathbb{Q}_p$ with $\mathrm{Im}\, \rho_{E,p} \subseteq C_{\mathrm{ns}}^+(p)$. Using standard tools in the theory of elliptic curves over local fields, we show that (for $p > 7$) this forces E to have potentially good supersingular reduction. If the reduction is already good over $\mathbb{Q}_p$, we know from our work in Section 3.6.3 that the p-adic representation of E is the same as the p-adic representation of a CM elliptic curve, so this case is relatively easy. The case where good reduction is acquired over a quadratic extension is not much different, so we may assume that the semistability defect is $e \in \{3, 4, 6\}$.

(2) By Theorem 4.5, we know that there is $\alpha \in \mathbb{P}_1(\mathbb{Q}_p)$ such that V_pE is isomorphic to a module V_α (see (8)) as a Galois representation.

(3) We are free to replace E by its ramified quadratic twist $E^{(p)}$. One can check that this replaces the parameter α with $p^2\alpha^{-1}$. We show that the case $v(\alpha) = 1$ is incompatible with $\mathrm{Im}\, \rho_{E,p} \subseteq C_{\mathrm{ns}}^+(p)$, so after this replacement we may assume $v(\alpha^{-1}) \geq 0$. (This is a purely technical step, that you may safely ignore.)

(4) We show that the $\mathbb{Q}_p$-representation V_pE determines uniquely the $\mathbb{Z}_p$-representation T_pE.

Remark 5.5. There is a philosophical point to be made here. More modern incarnations of p-adic Hodge theory than the one I've been describing are more adapted to working with integral (and hence torsion) representations. However, they are (to me, but I think in an absolute sense) even less computable than the Fontaine-Volkov theory, and we were unable to extract the kind of explicit information we needed from these modern theories.

Also note that, in general, inside a given $\mathbb{Q}_p$-representation of G_K there may be several stable $\mathbb{Z}_p$-lattices. These do not necessarily all give the same integral representation! See Exercise 5.6.

Exercise 5.6. Let $E/\mathbb{Q}$ be the elliptic curve [LMF26, 14.a4], namely,

$$E : y^2 + xy + y = x^3 - x.$$

Show that V_3E contains two non-homothetic, $G_{\mathbb{Q}}$-stable lattices $T_1 \cong \mathbb{Z}_3^2$ and $T_2 \cong \mathbb{Z}_3^2$ such that the Galois representations afforded by T_1, T_2 are non-isomorphic. Note that of course we have $T_1 \otimes_{\mathbb{Z}_3} \mathbb{Q}_3 \cong T_2 \otimes_{\mathbb{Z}_3} \mathbb{Q}_3 \cong V_3E$.

Hint. E is isogenous to [LMF26, 14.a2].

(5) We study in detail the series (10), which I reproduce here after rescaling by π_e and collecting terms:

$$\sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot \left((a^{(0)})^{p^{-2n}} + \alpha^{-1}\pi_e^2 \cdot (a^{(0)})^{p^{1-2n}} \right) = 0. \tag{11}$$

A careful analysis of valuations suggests that – if we only want to understand p^h-torsion points, rather than the full p-adic Tate module T_pE – only finitely many terms of the above power series are relevant. For this reason, we introduce the polynomials

$$g_h(x) := x^{p^{2h}} + \sum_{n=1}^{h} (-1)^n p^n \left(x^{p^{2h-2n}} + \alpha^{-1}\pi_e^2 x^{p^{2h+1-2n}} \right).$$

The unknown x should be considered as $a^{(2h)}$. In this way, $(a^{(0)})^{p^{-i}} = (a^{(2h)})^{p^{2h-i}}$, and replacing in (11) we find

$$\sum_{n\in\mathbb{Z}} (-1)^n p^n \cdot \left((a^{(2h)})^{p^{2h-2n}} + \alpha^{-1}\pi_e^2 \cdot (a^{(2h)})^{p^{2h+1-2n}} \right) = 0. \tag{12}$$

We truncate this to a polynomial by only keeping the terms of degree up to p^{2h}.

Remark 5.7. There's quite a bit of after-the-fact wisdom in the definition of $g_h(x)$, but one easy remark is that $\#E[p^h] = p^{2h}$, so if we want to encode the Galois action on $E[p^h]$ with a single polynomial, that polynomial better be of degree p^{2h}.

We show the following result, stated here in approximate form.

Theorem 5.8. *There is a G_K-equivariant bijection between $E[p^h]$ and the roots of $g_h(x)$ in $\overline{\mathbb{Q}}_p$.*

(6) We compute the Galois group of $g_h(x)$ over $\mathbb{Q}_p$. This is highly technical, but independent of p-adic Hodge theory, and is the step that forces us to assume the inequality $p > \sqrt{n_0 + 1}$.

(7) This gives a version of Theorem 5.2 expressed in terms of α rather than $j(E)$. The final step is to express the p-adic Hodge theoretic invariant α in terms of E. As pointed out at the end of the previous lecture, prior to [BFL26] it was not known how to do this.

5.4. **Some more details on the first steps.**

5.4.1. *The rational representation determines the integral representation.* The filtered module D_α describes the rational representation V_pE, whereas the theorem concerns the Galois action on the finite modules $E[p^n]$ (which can be seen as quotients of the integral representation T_pE). In principle, this is not a minor point: many different Galois-stable $\mathbb{Z}_p$-lattices can live inside a fixed $\mathbb{Q}_p$-representation, and they can give rise to non-isomorphic integral Galois representations (see Exercise 5.6). In our setting, the ambiguity disappears because the residual representation is irreducible.

Lemma 5.9. *Let G be a group, let V be a two-dimensional $\mathbb{Q}_p$-representation of G, and let $T, T' \subset V$ be G-stable $\mathbb{Z}_p$-lattices. Suppose that T/pT is irreducible. Then T and T' are homothetic, that is, there exists $u \in \mathbb{Q}_p^\times$ such that $T' = uT$. In particular, for every n we have $T/p^nT \cong T'/p^nT'$ as G-representations.*

Proof. After multiplying T by a power of p, choose the largest integer m such that $p^mT \subseteq T'$. By maximality, $p^{m-1}T \nsubseteq T'$. The image of p^mT in T'/pT' is a nonzero G-stable subspace. By irreducibility it is all of T'/pT'. Nakayama's lemma gives $p^mT = T'$. □

Remark 5.10. When T is the Tate module of an elliptic curve, there is a canonical isomorphism $T/p^nT \cong E[p^n]$. Thus, the previous lemma says that if $E[p]$ is an irreducible Galois representation, knowledge of V_pE is sufficient to recover the Galois representation on $E[p^n]$ for all $n \geq 1$.

For elliptic curves $E/\mathbb{Q}_p$ with $\operatorname{Im}\rho_{E,p} \subseteq C_{\mathrm{ns}}^+(p)$, one can show that $E[p]$ is in fact irreducible.

5.4.2. *'Alternative' division polynomials.* Recall the polynomial

$$g_h(x) = x^{p^{2h}} + \sum_{n=1}^{h} (-1)^n p^n \left(x^{p^{2h-2n}} + \alpha^{-1}\pi_e^2 x^{p^{2h+1-2n}} \right).$$

Let R_h be the set of its roots in $\overline{K}$. The next result says that, under the hypotheses used in the application, the roots R_h may serve as a replacement for $E[p^h]$.

Theorem 5.11 (Alternative division polynomials)**.** *Assume that $E/\mathbb{Q}_p$ has potentially supersingular reduction, semistability defect at least 3, Volkov parameter α, and $v(\alpha^{-1}) \geq 0$. If $p > \max\{\sqrt{h}, h - v(\alpha^{-1}) - 1, 3\}$, then there is a $\mathrm{Gal}(\overline{K}/K)$-equivariant bijection $E[p^h] \simeq R_h$, and $K(E[p^h]) = K(R_h)$. After giving R_h a suitable twisted action, the same bijection is compatible with the full group $G_{\mathbb{Q}_p}$.*

Sketch of proof. The key idea is the definition of the map giving the bijection. First, we note that $E[p^h] \cong \frac{T_pE}{p^hT_pE}$, and then we identify T_pE with *any* Galois-stable lattice inside $V_pE \cong V_\alpha$. A convenient choice is to take

$$T_c = \{u \in V_\alpha : u(b_1) = ((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}} \text{ with } v_R(a) \geq c\}$$

for a fixed c (and in fact, it is convenient to take $c = \frac{1}{p^{2h-2}(p^2-1)}$, where the denominator is the number of torsion points of exact order p^h).

We define a map $\Phi : T_c \to R_h$ by sending $u \in T_c$ with $u(b_1) = ((-1)^n a^{p^{-n}})_{n\in\mathbb{Z}}$ to the root of $g_h(x)$ that is closest to $a^\sharp$. This is clearly locally constant; the nontrivial work consists in showing that it is constant precisely on the cosets of p^hT_c, hence that it induces a map $\Phi : T_c/p^hT_c \to R_h$. This requires understanding the vector space structure on V_α (hence on $BW(R)$) in greater detail than I've explained in these notes.

In order to show that certain 'error terms' (that arise in comparing the infinite series (11) with the polynomial $g_h(x)$) are negligible, we need the lower bound on p given in the statement. □

Remark 5.12. An interesting feature that emerges from the proof is the fact that one can really 'see' much of the structure of $E[p^h]$ reflected in the roots of $g_h(x)$. To give a simple example: using Newton polygons, we show that the roots of $g_h(x)$ have the following valuations.

- One root of valuation ∞, corresponding to the torsion point 0.
- $p^2 - 1$ roots of valuation $\frac{1}{p^2-1}$, corresponding to the $p^2 - 1$ non-trivial p-torsion points;
- $p^4 - p^2$ roots of valuation $\frac{1}{p^2(p^2-1)}$, corresponding to the $p^4 - p^2$ torsion points in $E[p^2] \setminus E[p]$;
- $\vdots$
- $p^{2h} - p^{2h-2}$ roots of valuation $\frac{1}{p^{2h-2}(p^2-1)}$, corresponding to the $p^{2h} - p^{2h-2}$ torsion points in $E[p^h] \setminus E[p^{h-1}]$.

Another interesting feature is that the additive group structure is also not hard to read from the roots R_h themselves: using the notation Φ from the previous proof, the root $\Phi(\Phi^{-1}(r_1) + \Phi^{-1}(r_2))$ is simply the root of $g_h(x)$ closest to $r_1 + r_2$.

5.4.3. *Small level: comparison with the CM polynomial.* In the special case $\alpha = \infty$ (which we know corresponds to a CM elliptic curve), the term proportional to α^{-1} vanishes and the polynomial $g_h(x)$ becomes

$$g_h^\infty(x) = \sum_{n=0}^{h} (-1)^n p^n x^{p^{2h-2n}}.$$

Theorems 4.5 and 5.11 together identify the roots of this polynomial with $E^\infty[p^h]$, where E^∞ is a CM elliptic curve (depending on e). The Galois representation ρ_{E^∞,p^h} has image contained in the normaliser of a non-split Cartan for all h. The strategy in the range $h \leq v(\alpha^{-1}) + 1$ is to prove that g_h and g_h^∞ have the same splitting field, which we do by applying Krasner's lemma.

Proposition 5.13. *Assume the hypotheses of Theorem 5.11. If $h \leq v(\alpha^{-1}) + 1$, then the splitting fields of g_h and g_h^∞ over K coincide. Consequently* $\operatorname{Im}\rho_{E,p^h} \subseteq C_{\mathrm{ns}}^+(p^h)$*, because this is true for the CM elliptic curve E^∞.*

Thus, for h small, the mod-p^h representation of E is indistinguishable from that of a CM curve. The parameter $v(\alpha^{-1})$ measures the size of the p-adic neighbourhood of the CM point in which the torsion representation remains unchanged.

5.4.4. *Large level: maximal growth.* The complementary phenomenon begins at the next level.

Theorem 5.14 (Maximal growth)**.** *Under the same standing hypotheses, if $h = v(\alpha^{-1}) + 2$ and $p > \sqrt{h}$, then $[K(E[p^h]) : K(E[p^{h-1}])] = p^4$.*

Remark 5.15. By standard arguments, this then implies $[K(E[p^r]) : K(E[p^{r-1}])] = p^4$ for all $r \geq v(\alpha^{-1}) + 2$, and hence that $\operatorname{Im}\rho_{E,p^\infty}$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_p)$ of $\operatorname{Im}\rho_{E,p^{h-1}}$. See Exercise 5.16.

Exercise 5.16. Let p be an odd prime and G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Denote by $G(p^n)$ the image of G under the canonical projection map $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Show the following.

(1) For every $n \geq 1$, the kernel H_n of the canonical projection map $G(p^{n+1}) \to G(p^n)$ can be naturally identified with an $\mathbb{F}_p$-vector subspace of $\mathrm{Mat}_2(\mathbb{F}_p)$
(2) Considering the H_n as subspaces of $\mathrm{Mat}_2(\mathbb{F}_p)$, prove that $H_n \subseteq H_{n+1}$.
(3) Deduce in particular that if $\#H_{n_0} = p^4$ for some n_0, then $\#H_n = p^4$ for all $n \geq n_0$ and G is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_p)$ of $G(p^{n_0})$.

The proof of Theorem 5.14 has nothing to do with p-adic Hodge theory. It is a relatively elementary, but really not easy, computation in local fields. Roughly speaking, it uses the roots of $g_h(x)$ in the following way. We choose two suitable roots, say β_0 and γ_0, and construct elements $\varepsilon_r = \beta_0 - u_0\gamma_0^{h_0} - \cdots - u_{r-1}\gamma_0^{h_{r-1}}$ with carefully chosen units u_i and exponents h_i so that the valuations $v(\varepsilon_r)$ strictly increase with r. We eventually obtain an element $\varepsilon \in K(E[p^h])$ with $v(\varepsilon) = a/p^{2h}$ and $(a,p) = 1$. Hence the ramification degree of $K(E[p^h])/\mathbb{Q}_p$ is divisible by p^{2h}. Since Proposition 5.13 bounds the p-part of the ramification at level p^{h-1} by p^{2h-4}, the relative extension $K(E[p^h])/K(E[p^{h-1}])$ has ramification index (and hence degree) at least p^4. Since it cannot be larger, we must have $[K(E[p^h]) : K(E[p^{h-1}])] = p^4$.

5.5. **Computing α.**

5.5.1. *Intuition: the connection with formal logarithms.* So far all our results are expressed in terms of $v(\alpha^{-1})$. This is not yet satisfactory for explicit arithmetic: α is defined by the Hodge filtration in V_pE, and computing that filtration directly would require making a comparison between crystalline and de Rham cohomology over the ramified field K, which is very hard in practice. We can avoid this by using *formal logarithms*.

Remark 5.17. Our intuition was the following. Crystalline cohomology depends only on the special fibre, which – in our setting $e \in \{3,4,6\}$ – is essentially determined by e: it is a CM elliptic curve with j-invariant 0 or 1728. So all the information about V_α, and in particular the parameter α, must be hidden in the filtration, which – this being an elliptic curve – is simply the Hodge line $H^0(E_K, \Omega^1_E)$, or (almost equivalently) the invariant differential $\frac{dx}{2y}$ of E_K. Where else does the invariant differential show up? What distinguishes elliptic curves $\mathcal{E}$ over $\mathcal{O}_K$ with the same reduction $\tilde{E}$? Well, in some sense the information must be contained in the kernel of reduction, namely in the formal group $\widehat{\mathcal{E}}(\mathfrak{m}_K) = \ker\big(\mathcal{E}(\mathcal{O}_K) \to \widetilde{E}(k)\big)$. This is a one-dimensional p-adic analytic group, analytically isomorphic to $\mathfrak{m}_K$; the isomorphism is called the *formal logarithm*, and is obtained by formally integrating the invariant differential. Thus, we had good indication that the parameter α should be encoded by the formal logarithm, but the problem was to understand how to turn this information into the single number α.

More concretely, formal logarithms are defined as follows.

Definition 5.18. Let $t = -x/y$ be the standard parameter at the origin, and let $\widehat{E}$ be the associated formal group. The formal logarithm is the unique power series

$$\log_E(t) = t + \text{higher order terms} \in K[[t]]$$

such that

$$\log_E(F_E(t_1, t_2)) = \log_E(t_1) + \log_E(t_2),$$

where F_E is the formal group law[7] of E in the parameter t. The power series $\log_E(t)$ may be obtained by writing the invariant differential in this parameter,

$$\omega = \frac{dx}{2y} = \omega(t)\, dt,$$

and setting formally

$$\log_E(t) = \int_0^t \omega(u)\, du.$$

5.5.2. *Volkov's parameter β.* We first very briefly review an aspect of Volkov's proof of Theorem 4.5. Specifically, using Serre-Tate theory, one can construct *all* lifts $\mathcal{E}/\mathcal{O}_K$ of a given elliptic curve $\tilde{E}/\mathbb{F}_{p^2}$ (here $\mathbb{F}_{p^2}$ is the residue field of K). These turn out to be parametrised by a number $\beta \in \mathcal{O}_K$; imposing the condition that the elliptic curve corresponding to β comes by base-change from an elliptic curve defined over $\mathbb{Q}_p$ one finds that β must belong to $\mathbb{Z}_p\pi_e \cup \mathbb{Z}_p\pi_e^{e-3}$. Moreover, for given β there are (usually) two elliptic curves over $\mathbb{Q}_p$ with the same base-change to K. Volkov thus works with curves over $\mathbb{Q}_p$ denoted E^ε_β, with $\varepsilon \in \{\pm 1\}$. Going through her proof we find that, by definition, the relation with the parameter α is

$$\alpha = \begin{cases} \infty, & \beta = 0 \text{ and } \varepsilon = 1, \\ 0, & \beta = 0 \text{ and } \varepsilon = -1, \\ -p(\beta/\pi_e)^{-1}, & \varepsilon = 1,\ \beta \neq 0, \\ -p\beta/\pi_e^{e-3}, & \varepsilon = -1,\ \beta \neq 0. \end{cases}$$

We can determine both ε and β in terms of relatively familiar invariants of E.

Theorem 5.19. *Let $E/\mathbb{Q}_p$ be an elliptic curve with semistability defect e and potentially supersingular reduction. There are $\beta \in \mathbb{Z}_p\pi_e \cup \mathbb{Z}_p\pi_e^{e-3}$ and $\varepsilon \in \{-1, 1\}$ such that $E \cong E^\varepsilon_\beta$. These parameters can be computed as follows.*

- *Let Δ be the minimal discriminant of $E/\mathbb{Q}_p$. We have $\varepsilon = \begin{cases} 1 \text{ if } v(\Delta) < 6 \\ -1 \text{ if } v(\Delta) > 6. \end{cases}$*
- *Let E_L, with $L = \mathbb{Q}_p(\pi_e)$, be given by a good reduction model written in short Weierstrass form and let $t = -x/y$ be the parameter at the origin. Write the formal logarithm as $\log_{\widehat{E}}(t) = \sum_{n\geq 0} d_n t^n$. Then*

$$\beta = \lim_{k\to\infty} -\frac{p}{\pi_e}\frac{d_{p^{2k+1}}}{d_{p^{2k}}}.$$

Remark 5.20. More precisely, for every $k \geq 0$ one has the congruence

$$\beta \equiv -(p/\pi_e) d_{p^{2k+1}}/d_{p^{2k}} \pmod{\pi_e^{ke+1}},$$

so the formula is algorithmic: increasing k gives increasingly many p-adic digits of β.

The sign ε is related to descent data, and we will not say more about it. With the proper definitions in place, determining it amounts to an explicit computation with a minimal good reduction model of E_K.

[7] roughly speaking: in a neighbourhood of infinity, one can express x and y analytically in terms of the single parameter $t \in p\mathbb{Z}_p$, by an algebraic version of the implicit function theorem. Writing the addition law of two points on the elliptic curve, themselves expressed in terms of two parameters t_1, t_2, gives a formula of the shape 'the t-parameter of the sum of two points with t-parameters t_1, t_2 is a certain power series in t_1, t_2'. This is the formal group law of E.

5.5.3. *Valuation of β.* The valuation of β has an especially clean expression. If $E : y^2 = x^3 + Ax + B$ is the good reduction model over L, then the formal logarithm is given by (see [Yas13])

$$\log_{\widehat{E}}(t) = \sum_{m,n\geq 0} \binom{2m+3n}{m+2n, m, n} A^m B^n \frac{t^{4m+6n+1}}{4m+6n+1}. \tag{13}$$

Estimating the p-adic valuation of the coefficients of (13) we find that there is a unique term of minimal valuation and obtain

$$v(\beta) = \begin{cases} v(A) - 1/e, & \text{if } e \in \{3, 6\} \\ v(B) - 1/e, & \text{if } e = 4. \end{cases}$$

Since the model has good reduction over L, its discriminant is a unit, and the formulas $j = -1728(4A)^3/\Delta$ and $j - 1728 = 1728 \cdot 16 \cdot 27B^2/\Delta$ give

$$v(\beta) = \begin{cases} \frac{1}{3}v(j) - v(\pi_e), & e \in \{3, 6\}, \\ \frac{1}{2}v(j - 1728) - v(\pi_e), & e = 4. \end{cases}$$

Converting between the valuation of β and the valuation of α (which we have normalised to be non-positive) gives a formula for the valuation of α purely in terms of e and the j-invariant. Replacing this information in our previous theorems (which were expressed in terms of $v(\alpha)$) ultimately yields Theorem 5.2.

5.5.4. *Relation with formal logarithm.* It would unfortunately be too complicated to give details of the argument, so we only try to suggest the main idea. Fix a CM lift E_{CM} of the same supersingular special fibre and let Γ be its formal group. We identify a rank-2 free module $\mathcal{M}$ over $\mathcal{O}_L$ inside which 'all the possible filtrations live'. More precisely:

Definition 5.21. Let E/L be a lift of $\tilde{E}$ with formal group law $\hat{E}$ (with respect to a fixed integral model of good reduction). Following [Kaw11, p. 698] and [Fon77, IV, §4.1], we define $\mathcal{M}$ as

$$\left\{ f \in L[[t]]_0 : \frac{d}{dt} f \in \mathcal{O}_L[[t]], \quad f(x) + f(y) - f(\hat{E}(x, y)) \in \pi_e \mathcal{O}_L[[x, y]]_0 \right\} / \pi_e \mathcal{O}_L[[t]]_0,$$

and write $[f(t)]$ for the class of $f(t) \in L[[t]]_0$ in $\mathcal{M}$. Here the subscript 0 denotes power series with zero constant coefficient.

A result of Fontaine shows that $\mathcal{M}$ depends only on the special fibre $\tilde{E}$ and not on the precise lift E. In particular, this implies that $[\log_\Gamma(t)]$ is an element of $\mathcal{M}$, and one can show that $e_1 := [\log_\Gamma(t)], e_2 := -\frac{\pi_e}{p}[\log_\Gamma(t^p)]$ is a basis of $\mathcal{M}$.

By definition (more precisely, by the way Volkov applies the Serre-Tate deformation theory), the Hodge line defining a lift E_β is generated by $e_1 + \beta e_2$. On the other hand, it has a simple interpretation inside $\mathcal{M}$: it is the line $[\log_{E_\beta}(t)]$ itself! Thus, if we write

$$[\log_{\widehat{E_\beta}}(t)] = a[\log_\Gamma(t)] + b\frac{\pi_e}{p}[\log_\Gamma(t^p)] \text{ in } \mathcal{M}, \tag{14}$$

then $\beta = -\frac{b}{a}$.

Using the CM structure, it is easy to show that $\log_\Gamma(t)$ has coefficient 0 in degree $t^{p^{2k+1}}$. Comparing coefficients in (14) gives the result.

Warning 5.22. Note that (14) is equality in $\mathcal{M}$, so it is weaker than equality of coefficients. This is why we ultimately find only a limit formula for β.

References

[Abh18] Abhinandan. p-adic Galois representations and elliptic curves. Master's thesis, Université de Bordeaux, 2018. Master thesis. Available at https://www.math.u-bordeaux.fr/~ybilu/algant/documents/theses/Abhinandan.pdf.

[BC09] Olivier Brinon and Brian Conrad. p-adic Hodge theory, 2009. Lecture notes. Available at https://math.stanford.edu/~conrad/papers/notes.pdf.

[Ber02] Laurent Berger. Représentations p-adiques et équations différentielles. *Inventiones Mathematicae*, 148(2):219–284, 2002.

[Ber04] Laurent Berger. An introduction to the theory of p-adic representations. *Geometric aspects of Dwork theory*, pages 255–292, 2004.

[BFL26] Matthew Bisatt, Lorenzo Furio, and Davide Lombardo. Explicit p-adic Hodge theory for elliptic curves and non-split Cartan images. *arXiv preprint*, 2026. https://arxiv.org/abs/2603.04021.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer, 1990.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Annals of Mathematics*, 179:569–584, 2011.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[Bre00] Christophe Breuil. Groupes p-divisibles, groupes finis et modules filtrés. *Ann. of Math. (2)*, 152(2):489–549, 2000.

[Bri19] Olivier Brinon. Filtered (φ, N)-modules and semi-stable representations. In *An excursion into p-adic Hodge theory: from foundations to recent trends*, volume 54 of *Panor. Synthèses*, pages 93–129. Soc. Math. France, Paris, [2019] ©2019.

[Car19] Xavier Caruso. An introduction to p-adic period rings, 2019. https://arxiv.org/abs/1908.08424.

[CF00] Pierre Colmez and Jean-Marc Fontaine. Construction des représentations p-adiques semi-stables. *Inventiones Mathematicae*, 140(1):1–43, 2000.

[CI99] Robert Coleman and Adrian Iovita. The Frobenius and monodromy operators for curves and abelian varieties. *Duke Mathematical Journal*, 97(1):171–215, 1999.

[Fal88] Gerd Faltings. p-adic Hodge theory. *J. Amer. Math. Soc.*, 1(1):255–299, 1988.

[Fal89] Gerd Faltings. Crystalline cohomology and p-adic Galois-representations. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 25–80. Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[FL23] Lorenzo Furio and Davide Lombardo. Serre's uniformity question and proper subgroups of $c_{ns}^+(p)$. *Algebra & Number Theory (to appear)*, 2023. https://arxiv.org/abs/2305.17780.

[Fon77] Jean-Marc Fontaine. *Groupes p-divisibles sur les corps locaux*, volume No. 47-48 of *Astérisque*. Société Mathématique de France, Paris, 1977.

[Fon82] Jean-Marc Fontaine. Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. *Ann. of Math. (2)*, 115(3):529–577, 1982.

[Fon94a] Jean-Marc Fontaine. Le corps des périodes p-adiques. In *Périodes p-adiques (Bures-sur-Yvette, 1988)*, volume 223 of *Astérisque*, pages 59–111. Société Mathématique de France, 1994.

[Fon94b] Jean-Marc Fontaine. Représentations p-adiques semi-stables. In *Périodes p-adiques (Bures-sur-Yvette, 1988)*, volume 223 of *Astérisque*, pages 113–184. Société Mathématique de France, 1994.

[Kaw11] Mayumi Kawachi. Leading coefficients of isogenies of degree p over $\mathbb{Q}_p$. *Osaka J. Math.*, 48(3):691–708, 2011.

[KM74] Nicholas M. Katz and William Messing. Some consequences of the Riemann hypothesis for varieties over finite fields. *Invent. Math.*, 23:73–77, 1974.

[LFL21] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra & Number Theory*, 15(3):747–771, 2021.

[LMF26] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2026. [Online; accessed 17 June 2026].

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:Paper No. e62, 63, 2022. With an appendix with John Voight.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser79] Jean-Pierre Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, 54:323–401, 1981.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88(3):492–517, 1968.

[Tat74] John T. Tate. The arithmetic of elliptic curves. *Inventiones Mathematicae*, 23(3–4):179–206, 1974.

[Tsu99] Takeshi Tsuji. p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case. *Invent. Math.*, 137(2):233–411, 1999.

[Vol98] Maja Volkov. *Les représentations ℓ-adiques associées aux courbes elliptiques définies sur $\mathbb{Q}_p$*. PhD thesis, Université Paris-Sud, 1998. https://www.imo.universite-paris-saclay.fr/~biblio/theses/BJHTUP11_1998__0534__P0_0.pdf.

[Vol01] Maja Volkov. Les représentations ℓ-adiques associées aux courbes elliptiques sur $\mathbb{Q}_p$. *J. Reine Angew. Math.*, 535:65–101, 2001.

[Yas13] Seidai Yasuda. Explicit t-expansions for the elliptic curve $y^2 = 4(x^3 + Ax + B)$. *Proc. Japan Acad. Ser. A Math. Sci.*, 89(9):123–127, 2013.

[Zyw15] David Zywina. On the possible images of the mod ell representations associated to elliptic curves over $\mathbb{Q}$. 2015. https://arxiv.org/abs/1508.07660.