ON p-ADIC GALOIS REPRESENTATIONS

by

Laurent Berger

Contents

Introduction . . . 1
1. The Galois group of $\mathbf{Q}$ . . . 2
2. Ramification of local fields, I . . . 2
3. p-adic representations with $\ell \neq p$ . . . 3
4. Rings of periods . . . 3
5. Galois cohomology . . . 4
6. Ramification of local fields, II . . . 5
7. Cyclotomic extensions . . . 6
8. The cohomology of $\mathbf{C}_p$ . . . 6
9. Witt vectors . . . 7
10. The rings $\widetilde{\mathbf{E}}^+$ and $\widetilde{\mathbf{B}}^+$ . . . 8
11. The field $\mathbf{B}_{\mathrm{dR}}$ . . . 9
12. De Rham representations . . . 10
13. The rings $\mathbf{B}_{\max}$ and $\mathbf{B}_{\mathrm{st}}$ . . . 10
14. Crystalline and semi-stable representations . . . 11
15. Admissible filtered (φ, N)-modules . . . 13
16. The groups $H^1_*(K, V)$ . . . 14
17. A p-adic period pairing . . . 16
References . . . 17

Introduction

These are the notes for my part of the course "p-adic Galois representations and global Galois deformations". My aim was to give a short introduction to the p-adic Hodge theory necessary for formulating the local conditions imposed on deformations of p-adic representations. I also included some material on the technical tools used for proving the properties of Fontaine's rings of periods, although I usually gave no actual proofs of the results. In these notes, there are a few changes from the actual course; for example I exchanged ℓ and p in various places in order to follow the notation of the other courses.

1. The Galois group of Q

Let E be a finite extension of $\mathbf{Q}_p$, and let $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. A p-adic representation of $G_{\mathbf{Q}}$ is a finite dimensional continuous E-linear representation V of $G_{\mathbf{Q}}$. We wish to study p-adic representations of $G_{\mathbf{Q}}$, either individually or in families.

Let ℓ be a prime number (which may or may not be equal to p) and let λ be a place of $\overline{\mathbf{Q}}$ above ℓ. The group $D_\lambda = \{g \in G_{\mathbf{Q}}$ such that $g(\lambda) = \lambda\}$ is the decomposition group of λ. If λ' is another place above ℓ, then D_λ and $D_{\lambda'}$ are conjugate, and we write D_ℓ for the resulting group, which is well-defined up to conjugation in $G_{\mathbf{Q}}$.

The choice of λ is equivalent to the choice of an embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_\ell$, and this gives rise to a map $D_\ell \to G_{\mathbf{Q}_\ell}$, which is easily seen to be an isomorphism. The groups $G_{\mathbf{Q}_\ell}$ are easier to understand than $G_{\mathbf{Q}}$, thanks to ramification theory (recalled in §2).

Given a p-adic representation V, one then studies its restriction to D_ℓ for various primes ℓ, and the following result says that we do not lose too much information when doing so.

Proposition 1.1. — *If S is a set of prime numbers of density 1, and if V is a semisimple representation of $G_{\mathbf{Q}}$, then V is determined by its restriction to the D_ℓ with $\ell \in S$.*

2. Ramification of local fields, I

Let ℓ be a prime number, let K be a finite extension of $\mathbf{Q}_\ell$, and let $\mathcal{O}_K$ and $\mathfrak{m}_K$ and k_K and π_K denote its ring of integers, maximal ideal, residue field and a uniformizer respectively. Let K^{unr} denote the maximal unramified extension of K, and let K^{tame} denote the maximal tamely ramified extension of K.

The group $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/k_K)$ is isomorphic to $\widehat{\mathbf{Z}}$, and is topologically generated by $\mathrm{Fr}_m = x \mapsto x^m$ where $m = \mathrm{Card}(k_K)$. The inertia subgroup I_K of G_K is the kernel of the natural map $G_K \to \mathrm{Gal}(\overline{\mathbf{F}}_\ell/k_K)$, and we then have $I_K = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/K^{\mathrm{unr}})$. Likewise, we have

$$K^{\mathrm{tame}} = \cup_{\ell \nmid n} K^{\mathrm{unr}}(\pi_K^{1/n}),$$

so that $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) = \varprojlim_{\ell \nmid n} \mu_n$, where the map is given by

$$g \mapsto \{g(\pi_K^{1/n})/\pi_K^{1/n}\}_{n \geqslant 1}.$$

In particular, if $\alpha \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$, and if the image of $\sigma \in \mathrm{Gal}(K^{\mathrm{tame}}/K)$ in $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/k_K)$ is Fr_m, then $\sigma\alpha\sigma^{-1} = \alpha^m$. Finally, $I_K^{(\ell)} = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/K^{\mathrm{tame}})$ is the ℓ-Sylow subgroup of I_K, called the wild inertia subgroup.

3. p-adic representations with $\ell \neq p$

An easy corollary of the equation $\sigma\alpha\sigma^{-1} = \alpha^m$ is Grothendieck's monodromy theorem.

Theorem 3.1. — *If V is a p-adic representation of G_K, with K as above, and if $\ell \neq p$, then there exists a finite extension L of K, such that $V|_{I_L}$ is unipotent.*

We say that a p-adic representation V of G_K has good reduction if $V|_{I_K}$ is trivial, and we say that V is semistable if $V|_{I_K}$ is unipotent. Grothendieck's theorem above then says that every p-adic representation of G_K is potentially semistable (recall that $\ell \neq p$).

There is a useful way of describing the p-adic representations of G_K. Let K be as before, so that there is a map $n : G_K \to \widehat{\mathbf{Z}}$, defined by $\overline{g} = \mathrm{Fr}_m^{n(g)}$. The Weil group W_K is $\{g \in G_K$, such that $n(g) \in \mathbf{Z}\}$. A Weil-Deligne representation is the datum of a representation V of W_K (given by a map $\rho : W_K \to \mathrm{End}(V)$) and of a nilpotent map $N \in \mathrm{End}(V)$ such that $N\rho(g) = m^{-n(g)}\rho(g)N$.

Choose a compatible sequence $\{\zeta_{\ell^n}\}_{n\geqslant 0}$ of primitive ℓ^n-th roots of 1, and let $t : I_K \to \mathbf{Z}_\ell$ be the map determined by $g(\pi_K^{1/\ell^n}) = \zeta_{\ell^n}^{t(g)}\pi_K^{1/\ell^n}$. Choose also $\sigma \in G_K$ such that $n(\sigma) = 1$. If V is a p-adic representation of G_K, then by Grothendieck's theorem, there exists a finite extension L of K such that $\rho(g)$ is unipotent if $g \in I_L$. In this case, the map $N = \log\rho(g)/t(g) \in \mathrm{End}(V)$ is well-defined, and independent of $g \in I_L$. We attach to V a Weil-Deligne representation $(\rho_{\mathrm{WD}}, N_{\mathrm{WD}})$ on the same underlying space V, by the formulas $\rho_{\mathrm{WD}}(w) = \rho(w)\exp(-t(\sigma^{-n(w)}w)\cdot N)$ and $N_{\mathrm{WD}} = N$.

The isomophism class of the resulting representation does not depend on the choices made, and we can easily recover V from $(\rho_{\mathrm{WD}}, N_{\mathrm{WD}})$.

4. Rings of periods

From here to the end of these notes, we assume that $\ell = p$, so that K is now a finite extension of $\mathbf{Q}_p$. We would like to have a classification of p-adic representations of G_K similar to the one above, but this is harder to obtain. Indeed, let $\chi : G_K \to \mathbf{Z}_p^\times$ be the cyclotomic character, defined by $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}$. We can write $\chi = \omega\cdot\langle\chi\rangle$ with $\omega \in \mu_{p-1}$ and $\langle\chi\rangle \in 1 + p\mathbf{Z}_p$ and we can then consider $\omega^r\langle\chi\rangle^s$ with $r \in \mathbf{Z}/(p-1)\mathbf{Z}$ and $s \in \mathbf{Z}_p$. All such characters are representations of G_K but it turns out that they are "good" only if $s \in \mathbf{Z}$. It is hard to distinguish such characters merely by looking at their image or kernel, and in order to classify p-adic representations, one therefore needs more than mere ramification theory.

The main tool for doing so is Fontaine's construction of rings of periods. A ring of period if a $\mathbf{Q}_p$-algebra B, endowed with an action of G_K, and possibly some supplementary structures, compatible with the action of G_K (for example a filtration, a Frobenius map, a monodromy map...). We require that B is a domain, that (1) $\mathrm{Frac}(B)^{G_K} = B^{G_K}$ and that (2) if $y \in B$ is such that $\mathbf{Q}_p \cdot y$ is stable under G_K, then $y \in B^\times$. For example, all these conditions are automatically fulfilled if B is a field.

If V is a p-adic representation of G_K, we then define $\mathrm{D}_B(V) = (B \otimes_{\mathbf{Q}_p} V)^{G_K}$, which is a B^{G_K}-vector space. There is a natural map

$$\alpha : B \otimes_{B^{G_K}} \mathrm{D}_B(V) \to B \otimes_{\mathbf{Q}_p} V,$$

and condition (1) above implies that α is injective, so that $\mathrm{D}_B(V)$ is of dimension $\leqslant \dim_{\mathbf{Q}_p}(V)$. We say that V is B-admissible if $\mathrm{D}_B(V)$ is of dimension $\dim_{\mathbf{Q}_p}(V)$. By condition (2) above, this is the case if and only if α is surjective. If V is E-linear, then we say that it is B-admissible if the underlying $\mathbf{Q}_p$-linear representation is B-admissible.

In this way, we have defined the subcategory of B-admissible p-adic representations of G_K, inside the category of all p-adic representations of G_K. This subcategory is stable under subquotients, direct sums, tensor products and duals. If B has some supplementary structures, then these descend to $\mathrm{D}_B(V)$, and in this way we obtain some nontrivial invariants of B-admissible representations, which can then be used to classify them.

5. Galois cohomology

In this section, we give a few reminders about Galois cohomology groups. If V is a p-adic representation of G_K, then we write $H^i(K,V)$ for $H^i(G_K,V)$. We also write $h^i(V) = \dim_{\mathbf{Q}_p} H^i(K,V)$. Let V^* be the dual of V, and let $V^*(1) = V^* \otimes \chi$.

If $i = 0$, 1 or 2, then the cup product

$$\cup : H^i(K,V) \times H^{2-i}(K,V^*(1)) \to H^2(K, V \otimes V^*(1))$$

gives rise to a pairing $H^i(K,V) \times H^{2-i}(K,V^*(1)) \to H^2(K,\mathbf{Q}_p(1))$. We then have the following theorem of Tate.

Theorem 5.1. — *The groups $H^i(K,V)$ are finite dimensional $\mathbf{Q}_p$-vector spaces, they are $\{0\}$ if $i \geqslant 3$, we have $H^2(K,\mathbf{Q}_p(1)) = \mathbf{Q}_p$, the pairing $H^i(K,V) \times H^{2-i}(K,V^*(1)) \to \mathbf{Q}_p$ is perfect, and $h^0(V) - h^1(V) + h^2(V) = -[K:\mathbf{Q}_p]\dim(V)$.*

If $y \in K^\times$, let $\{y_n\}_{n \geqslant 0}$ be a sequence such that $y_0 = y$ and $y_{n+1}^p = y_n$. Let $\delta(y) : G_K \to \mathbf{Z}_p$ be the map determined by the equation $g(y_n) = \zeta_{p^n}^{\delta(y)(g)} y_n$, so that $\delta(y)(gh) = \delta(y)(g) + \chi(g)\delta(y)(h)$. We then have $\delta(y) \in H^1(K,\mathbf{Q}_p(1))$, and the map $y \mapsto \delta(y)$ is the Kummer map. It extends to a map $\delta : \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \widehat{K^\times} \to H^1(K,\mathbf{Q}_p(1))$, which is an isomorphism by Kummer theory. In particular, we have $h^1(\mathbf{Q}_p(1)) = [K:\mathbf{Q}_p]+1$, which is compatible with theorem 5.1.

If B is a ring of periods, then $W = B \otimes_{\mathbf{Q}_p} V$ is a semilinear representation of G_K: it is a free B-module, with a semilinear action of G_K. If we choose a basis of such a W, then $g \mapsto \mathrm{Mat}(g)$ gives a cocyle on G_K with values in $\mathrm{GL}_d(B)$, and choosing a different basis gives a cohomologous cocycle. In this way, we get $[W] \in H^1(G_K, \mathrm{GL}_d(B))$, and the original representation V is then B-admissible if and only if $[B \otimes_{\mathbf{Q}_p} V]$ is the trivial cohomology class. The following result, known as Hilbert's theorem 90, is then useful.

Theorem 5.2. — *If L/K is finite Galois, then* $H^1(\mathrm{Gal}(L/K), \mathrm{GL}_d(L)) = \{0\}$.

As a consequence, we see for example that if $\overline{\mathbf{Q}}_p \subset B$, then potentially B-admissible representations are already B-admissible.

We can deduce from theorem 5.2 that $H^1(\mathrm{Gal}(\overline{\mathbf{F}}_p/k_K), \mathrm{GL}_d(\overline{\mathbf{F}}_p)) = \{0\}$, and an argument of successive approximations then shows that

$$H^1(G_K/I_K, \mathrm{GL}_d(\widehat{\mathbf{Q}}_p^{\mathrm{unr}})) = \{0\}.$$

This way, we see that unramified representations of G_K are $\widehat{\mathbf{Q}}_p^{\mathrm{unr}}$-admissible.

6. Ramification of local fields, II

In this section, we collect various statements about the ramification of extensions of $\mathbf{Q}_p$, which are useful for proving some of the properties of Fontaine's rings of periods.

We give in particular a few reminders about the conductor and the different of a finite extension K/F. Let $\mathrm{val}_K(\cdot)$ be normalized by $\mathrm{val}_K(K^\times) = \mathbf{Z}$. Recall that if $u \geqslant -1$, then one defines the ramification filtration $\mathrm{Gal}(K/F)_u = \{g \in \mathrm{Gal}(K/F)$ such that $\mathrm{val}_K(gx - x) \geqslant u + 1$ for all $x \in \mathcal{O}_K\}$. Herbrand defined a function $\psi_{K/F}$, such that if we define $\mathrm{Gal}(K/F)^v = \mathrm{Gal}(K/F)_{\psi_{K/F}(v)}$, then $\mathrm{Gal}(K/F)^v$ is the image of $\mathrm{Gal}(L/F)^v$ whenever L is an extension of K. One can then define G_F^v for $v \geqslant -1$.

If K/F is Galois, then we define $K^u = K^{\mathrm{Gal}(K/F)^u}$, and if K is not Galois then we set $K^u = L^u \cap K$, where L/F is Galois and contains K. For example, we have $\mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p)^i = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p(\zeta_{p^i}))$, and therefore $\mathbf{Q}_p(\zeta_{p^n})^u \subset \mathbf{Q}_p(\zeta_{p^{\lfloor u \rfloor}})$. The conductor of K (with respect to F) is the inf of the real numbers u with $K^u = K$.

Recall also that we have the different $\mathfrak{d}_{K/F} = \check{\mathcal{O}}_K^{-1}$, where $\check{\mathcal{O}}_K$ is the dual of $\mathcal{O}_K$ with respect to the pairing $(x, y) \mapsto \mathrm{Tr}_{K/F}(xy)$. The different and conductors are related by the following formula.

Proposition 6.1. — *We have*

$$\mathrm{val}_p(\mathfrak{d}_{K/F}) = \int_{-1}^{\infty} \left(1 - \frac{1}{[K : K^u]}\right) du.$$

7. Cyclotomic extensions

Let $F = \mathbf{Q}_p$, let $F_n = \mathbf{Q}_p(\zeta_{p^n})$ for $n \geqslant 1$, and let $F_\infty = \cup_{n \geqslant 1} F_n$. We know that F_n is a totally ramified extension of F of degree $p^{n-1}(p-1)$, and also that $\mathcal{O}_{F_n} = \mathbf{Z}_p[\zeta_{p^n}]$. If $n \geqslant 1$ and $y \in F_\infty$, then $y \in F_{n+k}$ for some $k \gg 0$, and $R_n(y) = p^{-k} \mathrm{Tr}_{F_{n+k}/F_n}(y)$ does not depend on k. The map $R_n : F_\infty \to F_n$ is then a G_F-equivariant projection. We have $R_n(1) = 1$ while $R_n(\zeta_{p^{n+k}}) = 0$ if $1 \leqslant j \leqslant p^k - 1$, so that $R_n(\mathcal{O}_{F_{n+k}}) \subset \mathcal{O}_{F_n}$. This implies that if $y \in F_\infty$, then $\mathrm{val}_p(R_n(y)) \geqslant \mathrm{val}_p(y) - 1/(p^{n-1}(p-1))$, and therefore that R_n extends by uniform continuity to a projection $R_n : \widehat{F}_\infty \to F_n$. In addition, we have $R_n(y) = y$ if $y \in F_\infty$ and $n \gg 0$, so that if $y \in \widehat{F}_\infty$ then $R_n(y) \to y$ as $n \to \infty$.

Let K be a finite extension of $\mathbf{Q}_p$, let $K_n = K(\zeta_{p^n})$ for $n \geqslant 1$, and let $K_\infty = \cup_{n \geqslant 1} K_n$. If $n \gg 0$, then K_{n+1}/K_n is totally ramified of degree p, and K_n/F_n is of degree $d = K_\infty/F_\infty$ if $n \geqslant n(K)$. Proposition 6.1, and the fact that $F_n^u \subset F_{\lfloor u \rfloor}$, can be used to show that the sequence $\{p^n \mathrm{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n \geqslant 1}$ is eventually constant. In particular, if $\delta > 0$ then there exist $n(\delta) \geqslant n(K)$ such that if $n \geqslant n(\delta)$, then $\mathrm{val}_p(\mathfrak{d}_{K_n/F_n}) \leqslant \delta$. This implies that if $n \geqslant n(\delta)$, then there exists a basis $e_1, \ldots, e_d$ of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, such that $\mathrm{val}_p(e_i^*) \geqslant -\delta$.

If $y \in \mathcal{O}_{K_{n+k}}$, then we can write $y = \sum_{j=1}^d y_j e_j^*$, where $y_j = \mathrm{Tr}_{K_\infty/F_\infty}(y e_j)$ belongs to $\mathcal{O}_{F_{n+k}}$, and we set $R_n(y) = \sum_{j=1}^d R_n(y_j) e_j^*$. The resulting map $R_n : K_\infty \to K_n$ is then a G_K-equivariant projection, which satisfies $\mathrm{val}_p(R_n(y)) \geqslant \mathrm{val}_p(y) - 1/(p^{n-1}(p-1)) - \delta$, and therefore R_n extends, by uniform continuity, to a projection $R_n : \widehat{K}_\infty \to K_n$, such that $R_n(y) \to y$ as $n \to \infty$ as above.

8. The cohomology of $\mathbf{C}_p$

Let $\mathbf{C}_p$ be the p-adic completion of $\overline{\mathbf{Q}}_p$, so that $\mathbf{C}_p$ is a complete and algebraically closed field. If L is a subfield of $\overline{\mathbf{Q}}_p$, then the action of G_L on $\overline{\mathbf{Q}}_p$ extends by continuity to $\mathbf{C}_p$, and we have the following result of Ax-Sen-Tate.

Theorem 8.1. — *If $L \subset \overline{\mathbf{Q}}_p$, then $\mathbf{C}_p^{G_L} = \widehat{L}$.*

If L is as above, and $\alpha \in \overline{\mathbf{Q}}_p$, then we set $\Delta_L(\alpha) = \inf_{g \in G_L} \mathrm{val}_p(g(\alpha) - \alpha)$. The main ingredient of the proof of theorem 8.1 is the following result of Le Borgne, which improves upon a similar result of Ax.

Lemma 8.2. — *If $\alpha \in \overline{\mathbf{Q}}_p$, then there exists $\beta \in L$, with $\mathrm{val}_p(\alpha - \beta) \geqslant \Delta_L(\alpha) - 1/(p-1)$.*

Let $\psi : G_K \to \mathbf{Z}_p^\times$ be a character, which is trivial on $\ker(\chi) = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$ (for example, one could take $\psi = \chi^h$ with $h \in \mathbf{Z}$).

Theorem 8.3. — *If ψ has infinite order, then $H^0(K, \mathbf{C}_p(\psi)) = \{0\}$.*

If ψ has finite order, then Hilbert's theorem 90 implies that $\mathbf{C}_p(\psi) = \mathbf{C}_p$, and then $H^0(K, \mathbf{C}_p(\psi)) = K$ by theorem 8.1 above. We now give a sketch of the proof of theorem 8.3. If $H^0(K, \mathbf{C}_p(\psi)) \neq \{0\}$, then there exists a nonzero $y \in \mathbf{C}_p$ such that $g(y) = \psi(g)y$ for $g \in G_K$. We apply the maps R_n from §7; since $R_n(y) \to y$, we have $R_n(y) \neq 0$ for $n \gg 0$. The formula $g(R_n(y)) = \psi(g)R_n(y)$ now implies that ψ is trivial on $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K_n)$, and therefore has finite order.

By proving more refined results about K_∞, one can also prove that $H^1(K, \mathbf{C}_p(\psi)) = \{0\}$ if ψ has infinite order. Finally, $H^1(K, \mathbf{C}_p)$ is a 1-dimensional K-vector space, generated by $[g \mapsto \log_p \chi(g)]$.

9. Witt vectors

We say that a ring R is perfect if $p = 0$ and $x \mapsto x^p$ is a bijection on R. We say that a ring A is a perfect p-ring if p is a not a zero divisor, if A is separated and complete for the p-adic topology, and if A/pA is perfect. If $x \in A/pA$, we denote by $\widehat{x}$ a lift of x to A. Let $x_0 = x$ and let $x_{i+1} = x_i^{1/p}$. The sequence $\{\widehat{x}_i^{p^i}\}_{i \geqslant 0}$ then converges to an element $[x] \in A$, which is independent of all choices, and is called the Teichmüller lift of x. Every element of A can be written as $\sum_{i \geqslant 0} p^i [x_i]$ in a unique way.

Let $R = \mathbf{F}_p[\overline{X}_i^{1/p^\infty}, \overline{Y}_i^{1/p^\infty}]_{i \geqslant 0}$, and let S be the p-adic completion of $\mathbf{Z}_p[X_i^{1/p^\infty}, Y_i^{1/p^\infty}]_{i \geqslant 0}$, so that S is a perfect p-ring with residue ring R. There exist elements $\{S_i\}_{i \geqslant 0}$ and $\{P_i\}_{i \geqslant 0}$ of R such that

$$\sum_{i \geqslant 0} p^i X_i + \sum_{i \geqslant 0} p^i Y_i = \sum_{i \geqslant 0} p^i [S_i],$$
$$\sum_{i \geqslant 0} p^i X_i \times \sum_{i \geqslant 0} p^i Y_i = \sum_{i \geqslant 0} p^i [P_i].$$

If A is a perfect p-ring and $\{x_i\}_{i \geqslant 0}$ and $\{y_i\}_{i \geqslant 0}$ are two sequences of elements of R, then we have a map $\pi : S \to A$ given by $\pi(X_i) = [x_i]$ and $\pi(Y_i) = [y_i]$. By applying π to the two equations above, we see that

$$\sum_{i \geqslant 0} p^i [x_i] + \sum_{i \geqslant 0} p^i [y_i] = \sum_{i \geqslant 0} p^i [S_i(x, y)],$$
$$\sum_{i \geqslant 0} p^i [x_i] \times \sum_{i \geqslant 0} p^i [y_i] = \sum_{i \geqslant 0} p^i [P_i(x, y)],$$

so that addition and multiplication of elements of A, written as $\sum_{i \geqslant 0} p^i [x_i]$, are given by universal formulas.

Theorem 9.1. — *If R is a perfect ring, then there exists a unique perfect p-ring $W(R)$ such that $W(R)/pW(R) = R$.*

The discussion above shows that one can take $W(R) = \{\sum_{i\geqslant 0} p^i[x_i] \text{ with } x_i \in R\}$, addition and multiplication being given by the universal formulas. The ring $W(R)$ is called the ring of Witt vectors over R.

Proposition 9.2. — *If R is a perfect ring, if A is complete for the p-adic topology, and if $f : R \to A/pA$ is a homomorphism, then f lifts to a unique homomorphism $W(f) : W(R) \to A$.*

In the notation of the beginning of this section, we must have $W(f)([x]) = \lim_{n\to\infty} \widehat{f(x_n)}^{p^n}$, and it remains to check that this does give a ring homomorphism.

For example, the map $R \to R$ given by $x \mapsto x^p$ gives rise to the Frobenius map φ on $W(R)$.

Finally, if R is equipped with a valuation $\mathrm{val}(\cdot)$, then we can define semivaluations $w_k(\cdot)$ on $W(R)$ by $w_k(\sum_{i\geqslant 0} p^i[x_i]) = \min_{i\leqslant k} \mathrm{val}(x_i)$. The weak topology of $W(R)$ is the one defined by these semivaluations.

Proposition 9.3. — *If R is complete for* $\mathrm{val}(\cdot)$, *then $W(R)$ is complete for the weak topology.*

10. The rings $\widetilde{\mathbf{E}}^+$ and $\widetilde{\mathbf{B}}^+$

Fix some $0 < \delta < 1/(p-1)$, and let $I = \{x \in \mathcal{O}_{\mathbf{C}_p}, \text{ with } \mathrm{val}_p(x) \geqslant 1/(p-1) - \delta\}$. We define $\widetilde{\mathbf{E}}_I^+ = \{(x_0, x_1, \ldots) \text{ where } x_i \in \mathcal{O}_{\mathbf{C}_p}/I, \text{ and } x_{i+1}^p = x_i\}$, so that $\widetilde{\mathbf{E}}_I^+$ is a perfect ring (addition and multiplication being termwise). We have a map from $\{(x^{(0)}, x^{(1)}, \ldots) \text{ where } x^{(i)} \in \mathcal{O}_{\mathbf{C}_p}, \text{ and } (x^{(i+1)})^p = x^{(i)}\}$ to $\widetilde{\mathbf{E}}_I^+$, which can be shown to be a bijection, so that $\widetilde{\mathbf{E}}_I^+$ does not depend on I, and we denote it by $\widetilde{\mathbf{E}}^+$. If $x \in \widetilde{\mathbf{E}}^+$, we set $\mathrm{val}_{\mathbf{E}}(x) = \mathrm{val}_p(x^{(0)})$, and this defines a valuation on $\widetilde{\mathbf{E}}^+$, for which it is complete.

If $\alpha \in \overline{\mathbf{F}}_p$, then $([\alpha^{1/p^n}])_{n\geqslant 0} \in \widetilde{\mathbf{E}}^+$, and this gives an injective map $\overline{\mathbf{F}}_p \to \widetilde{\mathbf{E}}^+$. The choice of a sequence $\{\zeta_{p^n}\}_{n\geqslant 0}$ gives rise to an element $\varepsilon = (1, \zeta_p, \ldots) \in \widetilde{\mathbf{E}}^+$, and we define $\overline{\pi} = \varepsilon - 1$, so that $\mathrm{val}_{\mathbf{E}}(\overline{\pi}) = p/(p-1)$. In particular, $\overline{\mathbf{F}}_p[\![\overline{\pi}]\!] \subset \widetilde{\mathbf{E}}^+$. The theorem below is not needed in the sequel, but gives an idea of the structure of $\widetilde{\mathbf{E}}^+$.

Theorem 10.1. — *The field $\widetilde{\mathbf{E}}^+[1/\overline{\pi}]$ is the completion of the algebraic closure of $\overline{\mathbf{F}}_p(\!(\overline{\pi})\!)$.*

The more complicated definition of $\widetilde{\mathbf{E}}^+$ which we have given has the advantage of showing that $\widetilde{\mathbf{E}}^+$ is equipped with an action of $G_{\mathbf{Q}_p}$. We then set $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$ and $\widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}^+[1/p]$, and both rings are also equipped with an action of $G_{\mathbf{Q}_p}$, as well as the Frobenius map φ. The homomorphism $\widetilde{\mathbf{E}}^+ \to \mathcal{O}_{\mathbf{C}_p}/p$ extends, by theorem 9.2, to a homomorphism $\theta : \widetilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$, given explicitly by $\theta(\sum_{i\geqslant 0} p^i[x_i]) = \sum_{i\geqslant 0} p^i x_i^{(0)}$. For example, $\theta([\varepsilon]-1)=0$.

Proposition 10.2. — *The ideal* $\ker(\theta)$ *is generated by any element* $y \in \ker(\theta)$ *such that* $\mathrm{val}_{\mathbf{E}}(\overline{y}) = 1$.

This is the case with $y = ([\varepsilon]-1)/([\varepsilon^{1/p}]-1)$ (Fontaine's element ω), or with $y = [\widetilde{p}]-p$, where $\widetilde{p} \in \widetilde{\mathbf{E}}^+$ is such that $\widetilde{p}^{(0)} = p$.

11. The field $\mathbf{B}_{\mathrm{dR}}$

Let $\widetilde{\mathbf{B}}^+$ be the ring constructed in §10, and for $h \geqslant 1$, let $\mathbf{B}_h = \widetilde{\mathbf{B}}^+/\ker(\theta)^h$ (in particular, we have $\mathbf{B}_1 = \mathbf{C}_p$). We let $\mathbf{B}_{\mathrm{dR}}^+ = \varprojlim_{h\geqslant 1} \mathbf{B}_h$, so that $\mathbf{B}_{\mathrm{dR}}^+$ is a complete local ring, with maximal ideal $\ker(\theta)$ and residue field $\mathbf{C}_p$, and is also equipped with an action of $G_{\mathbf{Q}_p}$. An element $y \in \mathbf{B}_{\mathrm{dR}}^+$ is invertible if and only if $\theta(y) \neq 0$. For example, $\ker(\theta) = ([\varepsilon]-1)\mathbf{B}_{\mathrm{dR}}^+$, since $\theta([\varepsilon^{1/p}]-1) \neq 0$. We define $\mathbf{B}_{\mathrm{dR}} = \mathrm{Frac}(\mathbf{B}_{\mathrm{dR}}^+)$, so that it is a ring of periods, equipped with the additional structure of the filtration given by $\mathrm{Fil}^i \mathbf{B}_{\mathrm{dR}} = \ker(\theta)^i$.

The series $([\varepsilon]-1)-([\varepsilon]-1)^2/2+([\varepsilon]-1)^3/3-\cdots$ converges, to an element $t \in \mathbf{B}_{\mathrm{dR}}^+$ which also generates $\ker(\theta)$, so that $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}_{\mathrm{dR}}^+[1/t]$. Since $g(\varepsilon) = \varepsilon^{\chi(g)}$, we have $g(t) = \chi(g)t$.

Remark 11.1. — The ring $\mathbf{B}_{\mathrm{dR}}^+$ is isomorphic to $\mathbf{C}_p[\![t]\!]$, but only as abstract rings, and there is no such isomorphism which is compatible with the action of $G_{\mathbf{Q}_p}$ (as we'll see in §16).

The ring $\mathbf{B}_{\mathrm{dR}}^+$ is complete for the $\ker(\theta)$-adic topology, but it is also complete for a finer topology. Each ring $\mathbf{B}_h$ is a Banach space (the unit ball being the image of $\widetilde{\mathbf{A}}^+$), and this gives $\mathbf{B}_{\mathrm{dR}}^+$ the structure of a Fréchet space. Note that there is no such thing as a "p-adic topology" on $\mathbf{B}_{\mathrm{dR}}^+$.

If $P(X) \in \mathbf{Q}_p[X]$ is a polynomial with simple roots, then it splits completely in $\mathbf{C}_p$ and hence, by Hensel's lemma, it also splits completely in $\mathbf{B}_{\mathrm{dR}}^+$, since $\mathbf{B}_{\mathrm{dR}}^+/t\mathbf{B}_{\mathrm{dR}}^+ = \mathbf{C}_p$. This way, we see that $\overline{\mathbf{Q}}_p \subset \mathbf{B}_{\mathrm{dR}}^+$. A theorem of Colmez shows that actually, $\overline{\mathbf{Q}}_p$ is dense in $\mathbf{B}_{\mathrm{dR}}^+$ for its Fréchet topology.

Proposition 11.2. — *We have* $\mathbf{B}_{\mathrm{dR}}^{G_K} = K$.

To prove this, we write the exact sequence $0 \to t^{h+1}\mathbf{B}_{\mathrm{dR}}^+ \to t^h\mathbf{B}_{\mathrm{dR}}^+ \to \mathbf{C}_p(h) \to 0$, and use the computation of $H^0(K, \mathbf{C}_p(h))$ carried out in §8.

12. De Rham representations

We now carry out the constructions of §4, with $B = \mathbf{B}_{\mathrm{dR}}$. If V is a p-adic representation of G_K, then we set $\mathrm{D}_{\mathrm{dR}}(V) = (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$, which is a filtered K-vector space (if V is E-linear, then $\mathrm{D}_{\mathrm{dR}}(V)$ is a $E \otimes_{\mathbf{Q}_p} K$-module). We say that V is de Rham if it is $\mathbf{B}_{\mathrm{dR}}$-admissible. Note that since $\overline{\mathbf{Q}}_p \subset \mathbf{B}_{\mathrm{dR}}$, theorem 5.2 implies that potentially de Rham representation are de Rham. If V is de Rham, then a Hodge-Tate weight of V is an integer h, such that $\mathrm{Fil}^{-h}\mathrm{D}_{\mathrm{dR}}(V) \neq \mathrm{Fil}^{-h+1}\mathrm{D}_{\mathrm{dR}}(V)$.

The functor $\mathrm{D}_{\mathrm{dR}} : \{\text{de Rham representations}\} \to \{\text{filtered } K\text{-vector spaces}\}$ "forgets" a lot of information about V. For instance, if V is potentially unramified, then it is de Rham, but then $\mathrm{D}_{\mathrm{dR}}(V)$ is the filtered vector space for which $\mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V) = \mathrm{D}_{\mathrm{dR}}(V)$ and $\mathrm{Fil}^1\mathrm{D}_{\mathrm{dR}}(V) = \{0\}$.

The following theorem of Faltings proves a conjecture of Fontaine, and shows that representations of G_K "coming from geometry" are de Rham.

Theorem 12.1. — *If X is proper and smooth over K, and if $V = H^i_{et}(X_{\overline{\mathbf{Q}}_p}, \mathbf{Q}_p)$, then V is a de Rham representation of G_K, and $\mathrm{D}_{\mathrm{dR}}(V) = H^i_{dR}(X/K)$.*

Conversely, we have the following conjecture of Fontaine and Mazur. If F is a number field, then we say that a representation of G_F comes from geometry if it is a subquotient of the étale cohomology of some algebraic variety over F.

Conjecture 12.2. — *If F is a number field, and if V is an irreducible p-adic representation of G_F, which is unramified at almost every place of F, and which is de Rham at every place of F above p, then V comes from geometry.*

If in addition $\dim(V) = 2$ and $F = \mathbf{Q}$, then we actually expect V to come from a modular form; this has been proved in most cases by Emerton and Kisin.

13. The rings $\mathbf{B}_{\mathrm{max}}$ and $\mathbf{B}_{\mathrm{st}}$

Recall than in §10, we constructed the ring $\widetilde{\mathbf{B}}^+ = \{\sum_{k \gg -\infty} p^k[x_k], \text{ where } x_k \in \widetilde{\mathbf{E}}^+\}$. If $r \geqslant 0$, then we define a valuation $\mathrm{V}(\cdot, r)$ on $\widetilde{\mathbf{B}}^+$ by the formula

$$\mathrm{V}(x, r) = \inf_k \mathrm{val}_{\mathbf{E}}(x_k) + k\frac{pr}{p-1},$$

and we define $\widetilde{\mathbf{B}}_{[0;r]}$ to be the completion of $\widetilde{\mathbf{B}}^+$ for $\mathrm{V}(\cdot, r)$ (note that more generally, one can define some rings $\widetilde{\mathbf{B}}_{[r;s]}$, which explains the heavy notation). If $s \geqslant r$, then we have an injective map $\widetilde{\mathbf{B}}_{[0;s]} \to \widetilde{\mathbf{B}}_{[0;r]}$. The ring $\mathbf{B}^+_{\mathrm{max}}$ is $\widetilde{\mathbf{B}}_{[0;r_0]}$, where $r_0 = (p-1)/p$. It contains $\widetilde{\mathbf{B}}^+$ (and hence $\widehat{\mathbf{Q}}_p^{\mathrm{unr}}$), but also the element t defined in §11 (which belongs to $\widetilde{\mathbf{B}}_{[0;r]}$ for all $r > 0$), and we set $\mathbf{B}_{\mathrm{max}} = \mathbf{B}^+_{\mathrm{max}}[1/t]$. The Frobenius map $\varphi : \widetilde{\mathbf{B}}^+ \to \widetilde{\mathbf{B}}^+$ gives rise to a bijection $\varphi : \widetilde{\mathbf{B}}_{[0;r_0]} \to \widetilde{\mathbf{B}}_{[0;pr_0]}$, and hence to an injective map $\varphi : \mathbf{B}^+_{\max} \to \mathbf{B}^+_{\max}$. We use the ring $\mathbf{B}_{\max}$ instead of Fontaine's $\mathbf{B}_{\mathrm{cris}}$ for technical reasons, but they are almost equal; for example, $\varphi(\mathbf{B}_{\max}) \subset \mathbf{B}_{\mathrm{cris}} \subset \mathbf{B}_{\max}$.

The map $\widetilde{\mathbf{B}}^+ \to \mathbf{B}_h$ is continuous for the valuation $\mathrm{V}(\cdot, r_0)$ on $\widetilde{\mathbf{B}}^+$ and therefore extends to a continous map $\mathbf{B}^+_{\max} \to \mathbf{B}^+_{\mathrm{dR}}$. Recall that if K is a finite extension of $\mathbf{Q}_p$, then $K \subset \mathbf{B}^+_{\mathrm{dR}}$. Let $K_0 = K \cap \mathbf{Q}_p^{\mathrm{unr}}$ be the maximal unramified extension of $\mathbf{Q}_p$ contained in K, so that $K_0 \subset \mathbf{B}^+_{\max}$.

Theorem 13.1. — *The natural map $K \otimes_{K_0} \mathbf{B}^+_{\max} \to \mathbf{B}^+_{\mathrm{dR}}$ is injective.*

One can easily prove that the map $K \otimes_{K_0} \widetilde{\mathbf{B}}^+ \to \mathbf{B}^+_{\mathrm{dR}}$ is injective, and in order to prove the theorem, one needs to show that the map remains injective after completing the left hand side, which is rather delicate.

As a corollary, we get that $K \otimes_{K_0} \mathbf{B}_{\max} \to \mathbf{B}_{\mathrm{dR}}$ is also injective, and using the fact that $\mathbf{B}_{\mathrm{dR}}^{G_K} = K$, we get that $\mathrm{Frac}(\mathbf{B}_{\max})^{G_K} = K_0$.

Let u be a variable, and let $\mathbf{B}^+_{\mathrm{st}} = \mathbf{B}^+_{\max}[u]$ and $\mathbf{B}_{\mathrm{st}} = \mathbf{B}_{\max}[u]$. We extend the action of $G_{\mathbf{Q}_p}$ from $\mathbf{B}_{\max}$ to $\mathbf{B}_{\mathrm{st}}$ by $g(u) = u + a(g)t$, where $a(g)$ is defined by $g(p^{1/p^n}) = \zeta_{p^n}^{a(g)} p^{1/p^n}$. We also extend φ by $\varphi(u) = pu$, and we define a monodromy map $N : \mathbf{B}_{\mathrm{st}} \to \mathbf{B}_{\mathrm{st}}$ by $N = -d/du$, so that $N\varphi = p\varphi N$.

The series $\log([\widetilde{p}]/p) = \log(1 + ([\widetilde{p}]/p - 1))$ converges in $\mathbf{B}^+_{\mathrm{dR}}$, and if we choose $\log(p)$ (usually, we choose $\log(p) = 0$), then we can talk about $\log([\widetilde{p}]) \in \mathbf{B}^+_{\mathrm{dR}}$. We then extend the map $\mathbf{B}^+_{\max} \to \mathbf{B}^+_{\mathrm{dR}}$ to $\mathbf{B}^+_{\mathrm{st}}$, by sending u to $\log([\widetilde{p}])$, which is a $G_{\mathbf{Q}_p}$-equivariant map.

Theorem 13.2. — *The natural map $K \otimes_{K_0} \mathbf{B}^+_{\mathrm{st}} \to \mathbf{B}^+_{\mathrm{dR}}$ is injective.*

This implies that $K \otimes_{K_0} \mathbf{B}_{\mathrm{st}} \to \mathbf{B}_{\mathrm{dR}}$ is injective, and that $\mathrm{Frac}(\mathbf{B}_{\mathrm{st}})^{G_K} = K_0$. Finally, we have the following result (condition (2) of the definition of a ring of periods in §4).

Theorem 13.3. — *If $y \in \mathbf{B}_{\mathrm{st}}$ and if $\mathbf{Q}_p \cdot y$ is stable by G_K, then $y = y_0 t^h$ with $y_0 \in \widehat{\mathbf{Q}}_p^{\mathrm{unr}}$ and $h \in \mathbf{Z}$.*

In particular, such a y actually belongs to $\mathbf{B}_{\max}$, and is invertible in $\mathbf{B}_{\max}$.

14. Crystalline and semi-stable representations

We now carry out the constructions of §4, with $B = \mathbf{B}_{\max}$ or $\mathbf{B}_{\mathrm{st}}$. If V is a p-adic representation of G_K, then we set $\mathrm{D}_{\mathrm{cris}}(V) = (\mathbf{B}_{\max} \otimes_{\mathbf{Q}_p} V)^{G_K}$ and $\mathrm{D}_{\mathrm{st}}(V) = (\mathbf{B}_{\mathrm{st}} \otimes_{\mathbf{Q}_p} V)^{G_K}$. They are both K_0-vector spaces, $\mathrm{D}_{\mathrm{st}}(V)$ is a (φ, N)-module and $\mathrm{D}_{\mathrm{cris}}(V) = \mathrm{D}_{\mathrm{st}}(V)^{N=0}$ is a φ-module. We say that V is crystalline or semistable if V is $\mathbf{B}_{\max}$-admissible or $\mathbf{B}_{\mathrm{st}}$-admissible respectively. Theorem 13.2 implies that $K \otimes_{K_0} \mathrm{D}_{\mathrm{st}}(V)$ injects into $\mathrm{D}_{\mathrm{dR}}(V)$, so that if V is semistable, then it is also de Rham. The space $\mathrm{D}_{\mathrm{st}}(V)$ is then a filtered (φ, N)-module over K, that is a K_0-vector space D, with an invertible semilinear endomorphism φ, an endomorphism N such that $N\varphi = p\varphi N$, and a filtration on $D_K = K \otimes_{K_0} D$. In the next section, we'll see how technical properties of $\mathbf{B}_{\max}$ and $\mathbf{B}_{\mathrm{st}}$ translate into properties of $\mathrm{D}_{\mathrm{cris}}(\cdot)$ and $\mathrm{D}_{\mathrm{st}}(\cdot)$.

The property of being "crystalline" or "semistable" is the analogue of having "good reduction" or being "semistable" for $\ell \neq p$ as in §3. For example, we have the following result (due to Iovita for "crystalline" and to Breuil for "semistable"), which is a p-adic analogue of the Néron-Ogg-Shafarevich criterion for $\ell \neq p$.

Theorem 14.1. — *If A is an abelian variety over K, then V_pA is crystalline if and only if A has good reduction, and V_pA is semistable if and only if A has semistable reduction.*

We say that V is potentially semistable if there exists some finite Galois extension L of K, such that $V|_{G_L}$ is semistable. In this case, $\mathrm{D}_{\mathrm{st}}(V|_{G_L})$ is a filtered $(\varphi, N, \mathrm{Gal}(L/K))$-module over L. Potentially semistable representations are de Rham, and we have the following result, which may be seen as a p-adic analogue of theorem 3.1.

Theorem 14.2. — *Every de Rham representation is potentially semistable.*

Just as in §3, we can attach a Weil-Deligne representation $\mathrm{WD}(V)$ to a potentially semistable representation V of G_K. If $D = \mathrm{D}_{\mathrm{st}}(V|_{G_L})$, then D is the space of this representation, and $N_{\mathrm{WD}} = N$ and $\rho_{\mathrm{WD}}(w) = w\varphi^{-hn(w)}$ if $w \in W_K$, where W_K acts on D through $\mathrm{Gal}(L/K)$, and $q = p^h = \mathrm{Card}(k_K)$. The fact that $N\varphi = p\varphi N$ implies that $N_{\mathrm{WD}}\rho_{\mathrm{WD}}(w) = q^{-n(w)}\rho_{\mathrm{WD}}(w)N_{\mathrm{WD}}$. Contrary to the case $\ell \neq p$, this Weil-Deligne representation is not enough to recover V, since it does not take into account the filtration.

If f is a modular eigenform, then one can attach to it a p-adic representation V_pf, as well as a smooth admissible representation Π_pf of $\mathrm{GL}_2(\mathbf{Q}_p)$, and we then have the following result of Saito.

Theorem 14.3. — *If f is a modular eigenform, then V_pf is potentially semistable, and $\mathrm{WD}(V_pf)$ is the Weil-Deligne representation attached to Π_pf by the local Langlands correspondence.*

If in addition $p \nmid N$, then V_pf is crystalline, and the above theorem completely determines $\mathrm{D}_{\mathrm{cris}}(V_pf)$, because there is only one choice for the filtration (in this case, theorem 14.3 was previously proved by Scholl). We get $\mathrm{D}_{\mathrm{cris}}(V_pf)^* = D_{k,a_p}$ where $k = k(f)$ and

$a_p = a_p(f)$, and $D_{k,a_p} = Ee_1 \oplus Ee_2$ with

$$\mathrm{Mat}(\varphi) = \begin{pmatrix} 0 & -1 \\ p^{k-1} & a_p \end{pmatrix} \text{ and } \mathrm{Fil}^i D_{k,a_p} = \begin{cases} D_{k,a_p} & \text{if } i \leqslant 0, \\ Ee_1 & \text{if } 1 \leqslant i \leqslant k-1, \\ \{0\} & \text{if } i \geqslant k. \end{cases}$$

15. Admissible filtered (φ, N)-modules

By the constructions of the previous section, we have a functor $\mathrm{D}_{\mathrm{st}}(\cdot)$, from the category of semistable representations of G_K to the category of filtered (φ, N)-modules over K. In this section, we explain how technical properties of the ring $\mathbf{B}_{\mathrm{st}}$ can be used to prove some properties of the functor $\mathrm{D}_{\mathrm{st}}(\cdot)$. In particular, we will see that it is fully faithful, and give a characterization of its image.

Theorem 15.1. — *We have* $\mathbf{B}_{\max}^{\varphi=1} \cap \mathbf{B}_{\mathrm{dR}}^+ = \mathbf{Q}_p$.

As a corollary, we see that one can recover $\mathbf{Q}_p$ from the filtered (φ, N)-module structure of $\mathbf{B}_{\mathrm{st}}$, since we have $\mathbf{Q}_p = \mathbf{B}_{\mathrm{st}}^{N=0,\varphi=1} \cap \mathrm{Fil}^0 \mathbf{B}_{\mathrm{dR}}$. This way, we get the following full faithfulness result.

Corollary 15.2. — *The functor* $V \mapsto \mathrm{D}_{\mathrm{st}}(V)$ *is fully faithful.*

Indeed, if V is semistable, then $\mathbf{B}_{\mathrm{st}} \otimes_{K_0} \mathrm{D}_{\mathrm{st}}(V) = \mathbf{B}_{\mathrm{st}} \otimes_{\mathbf{Q}_p} V$, so that

$$V = (\mathbf{B}_{\mathrm{st}} \otimes_{K_0} \mathrm{D}_{\mathrm{st}}(V))^{N=0,\varphi=1} \cap \mathrm{Fil}^0(\mathbf{B}_{\mathrm{dR}} \otimes_K \mathrm{D}_{\mathrm{dR}}(V)).$$

Let us now characterize the image of $\mathrm{D}_{\mathrm{st}}(\cdot)$. If D is a 1-dimensional filtered (φ, N)-module over K, we define $t_N(D)$ to be $\mathrm{val}_p(\mathrm{Mat}(\varphi))$ and $t_H(D)$ to be the integer h such that $\mathrm{Fil}^h D_K = D_K$ and $\mathrm{Fil}^{h+1} D_K = \{0\}$. If D is of arbitrary dimension, then we let $t_N(D) = t_N(\det D)$ and $t_H(D) = t_H(\det D)$.

If V is a semistable representation, then $\det \mathrm{D}_{\mathrm{st}}(V) = \mathrm{D}_{\mathrm{st}}(\det V)$, and in the notation of theorem 13.3, we have $t_N(\mathrm{D}_{\mathrm{st}}(V)) = t_H(\mathrm{D}_{\mathrm{st}}(V)) = h$.

If D is a 1-dimensional subobject of $\mathrm{D}_{\mathrm{st}}(V)$, and $y \in D$, then $\varphi(y) = \lambda y$ for some $\lambda \in K_0$ of valuation $t_N(D)$, and $y \in \mathrm{Fil}^h D_K$ for $h = t_H(D)$. As a corollary of theorem 15.1, we get that if $h \geqslant \mathrm{val}_p(\lambda) + 1$, then $\mathbf{B}_{\max}^{\varphi=\lambda} \cap t^h \mathbf{B}_{\mathrm{dR}}^+ = \{0\}$. This implies that $t_H(D) \leqslant t_N(D)$. If D is a subobject of $\mathrm{D}_{\mathrm{st}}(V)$ of dimension r, then $\det D$ is a 1-dimensional subobject of $\mathrm{D}_{\mathrm{st}}(\Lambda^r V)$, and we can apply the above reasoning to get again $t_H(D) \leqslant t_N(D)$.

We say that a filtered (φ, N)-module D over K is admissible if $t_H(D) = t_N(D)$ and if $t_H(D') \leqslant t_N(D')$ for every subobject D' of D.

Proposition 15.3. — *If* V *is a semistable representation, then* $\mathrm{D}_{\mathrm{st}}(V)$ *is an admissible filtered* (φ, N)*-module over* K*.*

Fontaine had conjectured that conversely, every admissible filtered (φ, N)-module over K is the D_{st} of some semistable representation V of G_K, and this is now a theorem of Colmez and Fontaine.

Theorem 15.4. — *The functor* $\mathrm{D}_{\mathrm{st}}(\cdot)$ *gives rise to an equivalence of categories, between the category of semistable representations of* G_K *and the category of admissible filtered* (φ, N)*-modules over* K.

Thus in principle, one can answer any question about a semistable representation, merely by looking at the attached filtered (φ, N)-module. In practice, this can be quite hard. For example, computing the reduction modulo p of the crystalline representation attached to the filtered φ-module D_{k,a_p} given at the end of §14 is (as of January 2013) an open problem.

16. The groups $H^1_*(K, V)$

If V is a p-adic representation of G_K, then $H^1(K, V)$ classifies extensions E of $\mathbf{Q}_p$ by V, that is representations E inside the exact sequence: $0 \to V \to E \to \mathbf{Q}_p \to 0$. More generally, extensions of Y by X are classified by $H^1(K, X \otimes Y^*)$. Given some property of representations, we are interested in the subset of $H^1(K, V)$ corresponding to extensions having that property. In particular, we denote by $H^1_f(K, V)$ or $H^1_{st}(K, V)$ or $H^1_g(K, V)$ the classes of extensions which are crystalline or semistable or de Rham, respectively. If V is crystalline, then $H^1_f(K, V) = \ker(H^1(K, V) \to H^1(K, \mathbf{B}_{\max} \otimes_{\mathbf{Q}_p} V))$, and we have similar statements for H^1_{st} and H^1_g. The following result is an easy consequence of theorem 14.2, but had been proved before by Hyodo and was then seen as evidence for theorem 14.2.

Theorem 16.1. — *If* V *is semistable, then* $H^1_{st}(K, V) = H^1_g(K, V)$.

We also define $H^1_e(K, V) = \ker(H^1(K, V) \to H^1(K, \mathbf{B}_{\max}^{\varphi=1} \otimes_{\mathbf{Q}_p} V))$. Recall that by theorem 5.1, there is a perfect pairing $H^1(K, V) \times H^1(K, V^*(1)) \to \mathbf{Q}_p$. The following theorem of Bloch and Kato computes the orthogonals of the H^1_*.

Theorem 16.2. — *If* V *is a crystalline representation, then*

$$H^1_f(K, V)^\perp = H^1_f(K, V^*(1)) \text{ and } H^1_e(K, V)^\perp = H^1_g(K, V^*(1)).$$

One can compute the dimensions of the $H^1_*(K, V)$, by using the so-called fundamental exact sequence $0 \to \mathbf{Q}_p \to \mathbf{B}_{\max}^{\varphi=1} \to \mathbf{B}_{\mathrm{dR}}/\mathbf{B}_{\mathrm{dR}}^+ \to 0$, which when used along with the fact that $1 - \varphi : \mathbf{B}_{\max} \to \mathbf{B}_{\max}$ is surjective, gives rise to

$$0 \to \mathbf{Q}_p \to \mathbf{B}_{\max} \xrightarrow{x \mapsto ((1-\varphi)x, \overline{x})} \mathbf{B}_{\max} \oplus \mathbf{B}_{\mathrm{dR}}/\mathbf{B}_{\mathrm{dR}}^+ \to 0.$$

By tensoring the above exact sequence with a crystalline representation V, and taking invariants under G_K, one finds

$$0 \to V^{G_K} \to \mathrm{D}_{\mathrm{cris}}(V) \to \mathrm{D}_{\mathrm{cris}}(V) \oplus \mathrm{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V) \to H^1_f(K,V) \to 0,$$

where we use the fact that $(\mathbf{B}_{\mathrm{dR}}/\mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K} = \mathrm{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V)$, if V is de Rham. This tells us that (if we write h^1_* for $\dim_{\mathbf{Q}_p} H^1_*$)

$$h^1_f(K,V) = [K:\mathbf{Q}_p](\dim_{\mathbf{Q}_p} V - \dim_K \mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V)) + \dim_{\mathbf{Q}_p} V^{G_K}.$$

Likewise, we can prove that

$$h^1_e(K,V) = h^1_f(K,V) - \dim_{\mathbf{Q}_p} \mathrm{D}_{\mathrm{cris}}(V)^{\varphi=1},$$
$$h^1_g(K,V) = h^1_f(K,V) + \dim_{\mathbf{Q}_p} \mathrm{D}_{\mathrm{cris}}(V^*(1))^{\varphi=1}.$$

For example, let $V = \mathbf{Q}_p(r)$ and $d = [K:\mathbf{Q}_p]$. By using the above formulas, we find the following dimensions for the various $H^1_*(K,\mathbf{Q}_p(r))$.

r	$\leqslant -1$	0	1	$\geqslant 2$
$h^1(K,\mathbf{Q}_p(r))$	d	$d+1$	$d+1$	d
$*=e$	0	0	d	d
$*=f$	0	1	d	d
$*=g$	0	1	$d+1$	d

Let us make a few comments about this table.

1. For $r \geqslant 2$, we see that every extension of $\mathbf{Q}_p$ by $\mathbf{Q}_p(r)$ is crystalline.
2. For $r=1$, they are all semi-stable, and we saw in §5 that the Kummer map $\delta : \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \widehat{K^\times} \to H^1(K,\mathbf{Q}_p(1))$ is an isomorphism. The subset $H^1_f(K,\mathbf{Q}_p(1))$ then corresponds to the image of $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \widehat{\mathcal{O}_K^\times}$, which is the characteristic zero analogue of "peu ramifiées" extensions.
3. For $r=0$, the h^1 counts the number of independent $\mathbf{Z}_p$-extensions of K, and $H^1_f(K,\mathbf{Q}_p)$ corresponds to the unramified one.
4. For $r \leqslant -1$, one can (easily) show that all extensions are $\mathbf{C}_p(\!(t)\!)$-admissible, but since no nontrivial ones are $\mathbf{B}_{\mathrm{dR}}$-admissible, $\mathbf{B}_{\mathrm{dR}}$ is not isomorphic to $\mathbf{C}_p(\!(t)\!)$.

If V is de Rham, and we tensor the exact sequence $0 \to \mathbf{Q}_p \to \mathbf{B}_{\max}^{\varphi=1} \to \mathbf{B}_{\mathrm{dR}}/\mathbf{B}^+_{\mathrm{dR}} \to 0$ by V, and take G_K-invariants, then we find a connecting map: $\mathrm{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V) \to H^1_e(K,V)$, which is denoted by $\exp_V$, and called Bloch-Kato's exponential. If A is an abelian variety (or a formal group), then V_pA is de Rham, $\mathrm{D}_{\mathrm{dR}}(V_pA)/\mathrm{Fil}^0\mathrm{D}_{\mathrm{dR}}(V_pA)$ is identified with the Lie Algebra of A, and if δ_A denotes the Kummer map, then the following diagram commutes, which helps to explain the terminology.

$$\begin{array}{ccc} \mathrm{Lie}(A) & \xrightarrow{\exp} & \mathbf{Q} \otimes_{\mathbf{Z}} A(\mathcal{O}_K) \\ \| & & \downarrow \delta_A \\ \mathrm{D}_{\mathrm{dR}}(V_p A)/\mathrm{Fil}^0 \mathrm{D}_{\mathrm{dR}}(V_p A) & \xrightarrow{\exp_V} & H^1(K, V_p A) \end{array}$$

It also shows that the image of the Kummer map always lies in the H^1_e.

17. A p-adic period pairing

Let K be a finite unramified extension of $\mathbf{Q}_p$, and let G be a 1-dimensional formal group of height h over $\mathcal{O}_K$, whose addition law is given by $X \oplus Y \in \mathcal{O}_K[\![X,Y]\!]$. We denote by $[n](X)$ the "multiplication by n" power series. The Tate module of G is $T_pG = \{(u_0, u_1, \ldots)$, where $u_i \in \mathfrak{m}_{\mathbf{C}_p}$ and $u_0 = 0$ and $[p](u_{i+1}) = u_i\}$. The space $V_pG = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pG$ is a p-adic representation of G_K of dimension h, which we know is crystalline. We will see here a more precise version of this result.

A differential form on G is $\omega(X) = \alpha(X)dX$, where $\alpha(X) \in K[\![X]\!]$, and we denote by $F_\omega(X)$ the unique power series such that $dF_\omega(X) = \omega(X)$ and $F_\omega(0) = 0$. We say that

1. ω is invariant, if $F_\omega(X \oplus Y) = F_\omega(X) + F_\omega(Y)$;
2. ω is exact, if $F_\omega(X) \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$;
3. ω is of the second kind, if $F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y) \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X,Y]\!]$.

The first de Rham cohomology group of G is then given by $H^1_{dR}(G/K) = \{\text{second kind}\}/\{\text{exact}\}$. This is a K-vector space of dimension h, equipped with the filtration $\mathrm{Fil}^0 H^1_{dR} = H^1_{dR}$ and $\mathrm{Fil}^1 H^1_{dR} = \{\text{invariant}\}$ and $\mathrm{Fil}^2 H^1_{dR} = \{0\}$.

Theorem 17.1. — *If ω is of the second kind, if $u \in T_pG$, and if $\widehat{u}_n \in \widetilde{\mathbf{A}}^+$ is such that $\theta(\widehat{u}_n) = u_n$ for every $n \geqslant 0$, then*

1. *the sequence $\{p^n F_\omega(\widehat{u}_n)\}_{n \geqslant 0}$ converges in $\mathbf{B}^+_{\max}$, to an element $\int_u \omega$;*
2. *this element only depends on u and on the class of ω;*
3. *the resulting map $H^1_{dR}(G/K) \times V_pG \to \mathbf{B}^+_{\max}$ is a perfect pairing, compatible with the action of G_K and the filtrations.*

For example, if $G = \mathbf{G}_m$ and $\omega(X) = dX/(1+X)$ and $u = (0, \zeta_p - 1, \ldots)$, then one can take $\widehat{u}_n = [\varepsilon^{1/p^n}] - 1$ for $n \geqslant 0$, and then $\int_u \omega = t$.

As a consequence of theorem 17.1, we recover the fact that V_pG is crystalline, and that $\mathrm{D}_{\mathrm{cris}}(V_pG) = H^1_{dR}(G/K)^*$, using the p-adic period pairing. This construction can be extended to the case of abelian varieties.

References

[Ber04] L. Berger – "An introduction to the theory of p-adic representations", Geometric aspects of Dwork theory. Vol. I, II, Walter de Gruyter GmbH & Co. KG, Berlin, 2004, p. 255–292.

[BK90] S. Bloch and K. Kato – "L-functions and Tamagawa numbers of motives", The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, p. 333–400.

[Col92] P. Colmez – "Périodes p-adiques des variétés abéliennes", *Math. Ann.* **292** (1992), no. 4, p. 629–644.

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

[Fon94a] J.-M. Fontaine – "Le corps des périodes p-adiques", *Astérisque* (1994), no. 223, p. 59–111, With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Fon94b] J.-M. Fontaine – "Représentations ℓ-adiques potentiellement semi-stables", *Astérisque* (1994), no. 223, p. 321–347, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Fon94c] J.-M. Fontaine – "Représentations p-adiques semi-stables", *Astérisque* (1994), no. 223, p. 113–184, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Ser68] J.-P. Serre – *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Tat67] J. Tate – "p-divisible groups", Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, p. 158–183.

[Was97] L. Washington – "Galois cohomology", Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, p. 101–120.

Laurent Berger, UMPA ENS de Lyon, UMR 5669 du CNRS, IUF
E-mail : laurent.berger@ens-lyon.fr • *Url :* perso.ens-lyon.fr/laurent.berger/