GALOIS REPRESENTATIONS AND (φ, Γ)-MODULES
Course given at IHP in 2010

by

Laurent Berger

Contents

1. Introduction

These are notes for my course given at IHP in January – March 2010. They have not been seriously revised in a long time, so use them at your own risk.

2. Hensel's lemma and Newton polygons

Recall the following easy but very useful theorem.

***Theorem 2.1* (The fixed point theorem).** — *If X is a complete metric space and if $f : X \to X$ satisfies $d(f(x), f(y)) \leqslant \lambda \cdot d(x, y)$ for some $0 \leqslant \lambda < 1$, then f admits a unique fixed point x_f in X.*

If $d(\cdot, \cdot)$ is ultrametric and if $y \in X$, then $d(y, x_f) \leqslant d(y, f(y))$.

***Theorem 2.2* (Hensel's lemma).** — *Let A be a domain that is complete for a valuation $\mathrm{val}(\cdot)$ which is $\geqslant 0$ on A. If $P(X) \in A[X]$ and if α_0 is an element of A such that $P(\alpha_0)/P'(\alpha_0)^2 \in A$ and $\mathrm{val}(P(\alpha_0)/P'(\alpha_0)^2) = \varepsilon > 0$, then there exists $\alpha \in A$ such that $P(\alpha) = 0$ and $\mathrm{val}(\alpha - \alpha_0) \geqslant \varepsilon + \mathrm{val}(P'(\alpha_0))$.*

Proof. — For $n \geqslant 0$, let $\alpha_{n+1} = \alpha_n - P(\alpha_n)/P'(\alpha_n)$. We show by induction on n that $P(\alpha_n)/P'(\alpha_n)^2 \in A$ and that $\mathrm{val}(P(\alpha_n)/P'(\alpha_n)^2) \geqslant 2^n\varepsilon$. This true for $n = 0$ by hypothesis.

There exist polynomials $(P')^{[h]}(X) \in A[X]$ such that

$$\begin{aligned} P'(\alpha_{n+1}) &= P'(\alpha_n) + \frac{P(\alpha_n)}{P'(\alpha_n)} \cdot (P')^{[1]}(\alpha_n) + \cdots + \left(\frac{P(\alpha_n)}{P'(\alpha_n)}\right)^{d-1} (P')^{[d-1]}(\alpha_n) \\ &= P'(\alpha_n)\left(1 + \frac{P(\alpha_n)}{P'(\alpha_n)^2}\beta_n\right), \end{aligned}$$

with $\beta_n \in A$ so that $P'(\alpha_n)$ and $P'(\alpha_{n+1})$ differ by a unit of A. Likewise,

$$\begin{aligned} P(\alpha_{n+1}) &= P(\alpha_n) - \frac{P(\alpha_n)}{P'(\alpha_n)}P^{[1]}(\alpha_n) + \left(\frac{P(\alpha_n)}{P'(\alpha_n)}\right)^2 P^{[2]}(\alpha_n) - \cdots \pm \left(\frac{P(\alpha_n)}{P'(\alpha_n)}\right)^d P^{[d]}(\alpha_n) \\ &\in \left(\frac{P(\alpha_n)}{P'(\alpha_n)}\right)^2 A, \end{aligned}$$

so that $P(\alpha_{n+1})/P'(\alpha_{n+1})^2 \in (P(\alpha_n)/P'(\alpha_n)^2)\cdot A$ which proves the claim by induction on n.

This shows that $\alpha_n \to \alpha$ where $P(\alpha)=0$ and $\mathrm{val}(\alpha-\alpha_0) \geqslant \mathrm{val}(P(\alpha_0)/P'(\alpha_0))$ which proves the theorem. □

We now give a stronger version of Hensel's lemma. In order to do this, we recall the definition of the resultant of two polynomials. Let $W_d = \{P(X) \in K[X] \text{ of degree } \leqslant d-1\}$. If $P(X)$ and $Q(X)$ are of degrees $\deg(P)\leqslant n$ and $\deg(Q)\leqslant m$, then we have a map $\theta_{P,Q} : W_m \oplus W_n \to W_{m+n}$ given by $(U,V)\mapsto (PU+QV)$ and the resultant $\mathrm{res}(P,Q)$ of P and Q is the determinant of $\theta_{P,Q}$ in the bases $\{1,X,\dots,X^{d-1}\}$ of W_d.

If $P(X)=a_0+\cdots+a_dX^d \in K[X]$, then the Gauss norm of P is defined by $|P|_G = \sup_i |a_i|$ (so called because Gauss' lemma says that this gives a multiplicative norm on $K[X]$). The strong version of Hensel's lemma is the following theorem.

Theorem 2.3. — *If $P,Q,R\in\mathcal{O}_K[X]$ and $0\leqslant\lambda<1$ and $m,n\geqslant 0$ are such that:*

1. $\deg(P)=m+n$ *and* $\deg(Q)=n$ *and* $\deg(R)=m$*;*
2. $\deg(P-QR)\leqslant m+n-1$ *and* $|P-QR|_G\leqslant\lambda|\mathrm{res}(Q,R)|^2$*,*

then there exist polynomials $\tilde{Q}$ and $\tilde{R}$ such that:

1. $\deg(\tilde{Q}-Q)\leqslant n-1$ *and* $|\tilde{Q}-Q|_G\leqslant\lambda|\mathrm{res}(Q,R)|$*;*
2. $\deg(\tilde{R}-R)\leqslant m-1$ *and* $|\tilde{R}-R|_G\leqslant\lambda|\mathrm{res}(Q,R)|$*;*
3. $P=\tilde{Q}\tilde{R}$*.*

Proof. — If $\mathrm{res}(Q,R)=0$ then we're done because $P=QR$. If $\rho=|\mathrm{res}(Q,R)|\neq 0$, then the map $\theta_{Q,R}: W_m\oplus W_n\to W_{m+n}$ is invertible and we call $\varphi: W_m\oplus W_n\to W_m\oplus W_n$ the map defined by $\varphi(U,V)=\theta_{Q,R}^{-1}(P-QR-UV)$. If $U,V\in B(0,\lambda\rho)$, then we have $|P-QR-UV|_G\leqslant\sup(|P-QR|_G,|UV|_G)\leqslant\lambda\rho^2$ and therefore $|\varphi(U,V)|_G\leqslant\lambda\rho$ since $\det\theta_{Q,R}^{-1}=\mathrm{res}(Q,R)^{-1}$. In other words, the map φ preserves the ball $B(0,\lambda\rho)^2$. If (U,V) and (U',V') belong to $B(0,\lambda\rho)^2$, then:

$$\begin{aligned}|\varphi(U,V)-\varphi(U',V')|_G &= |\theta_{Q,R}^{-1}(UV-U'V')|_G\\ &\leqslant \rho^{-1}|UV-U'V'|_G\\ &\leqslant \rho^{-1}|U(V-V')+V'(U-U')|_G\\ &\leqslant \lambda|(U-U',V-V')|_G\end{aligned}$$

so that φ is a contracting map. By the fixed point theorem, φ admits a (unique) fixed point and if $\varphi(U,V)=(U,V)$, then $QU+RV=P-QR-UV$ so that $P=(Q+V)(R+U)$ and we have the required factorization of P. □

The theory of Newton polygons allows one to compute the valuations of the roots of polynomial from the valuation of its coefficients; it can therefore be seen as an analogue of Descartes' rule of signs. Let K be a field endowed with the valuation $\mathrm{val}_p(\cdot)$.

If $P(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$, then the Newton polygon $\mathrm{NP}(P)$ is the lower convex hull of the points $(0, \mathrm{val}_p(a_0))$, $(1, \mathrm{val}_p(a_1))$, $\ldots$, $(d, \mathrm{val}_p(a_d))$. The Newton polygon $\mathrm{NP}(P)$ is therefore a finite union of segments of increasing slopes, starting at $(0, \mathrm{val}_p(a_0))$ and finishing at $(d, \mathrm{val}_p(a_d))$. The first segment can possibly be of slope $-\infty$ (if $a_0 = 0$). A slope of $\mathrm{NP}(P)$ is the slope of one of these segments, and the length of a segment is the length of its component along the x-axis.

Theorem 2.4. — *If $P(X) \in K[X]$, then the number of roots of P in $\overline{K}$ with valuation λ is equal to the length of the segment of $\mathrm{NP}(P)$ with slope $-\lambda$.*

Proof. — We can divide $P(X)$ by a_d and assume that $P(X)$ is monic. Assume that P has d_1 roots of valuation λ_1 and d_2 roots of valuation λ_2, etc, d_k roots of valuation λ_k with $\lambda_1 > \cdots > \lambda_k$. The coefficient a_i is $\pm$ the sum of all possible products of $d-i$ roots. In particular, $a_{d_1+\cdots+d_{s-1}}$ is the sum of a term of valuation $d_s\lambda_s + \cdots + d_k\lambda_k$ and of terms which are all of valuation $> d_s\lambda_s + \cdots + d_k\lambda_k$ so that

$$\mathrm{val}_p(a_{d_1+\cdots+d_{s-1}}) = d_s\lambda_s + \cdots + d_k\lambda_k$$

Likewise, if $0 \leqslant i \leqslant d_s$, then

$$\mathrm{val}_p(a_{d_1+\cdots+d_{s-1}+i}) \geqslant (d_s - i)\lambda_s + d_{s+1}\lambda_{s+1} + \cdots + d_k\lambda_k$$

with equality if $i = 0$ or if $i = d_s$ so that $\mathrm{NP}(P)$ has a segment of slope $-\lambda_s$ and length d_s. □

Corollary 2.5. — *If K is complete and if $P(X) \in K[X]$, then we have a decomposition $P(X) = \prod_\lambda P_\lambda(X)$ with $P_\lambda(X) \in K[X]$ having all its roots of valuation λ.*

Exercises

1. Let $f_1, \ldots, f_n \in \mathcal{O}_K[X_1, \ldots, X_n]$ be multivariate polynomials and suppose that $a = (a_1, \ldots, a_n) \in \mathcal{O}_K^n$ is such that $f_i(a_1, \ldots, a_n) \in \det(J(a))^2\mathfrak{m}_K$. Prove that there exists $b \in a + \det(J(a))\mathfrak{m}_K^n$ such that $f_i(b) = 0$ for all i.
2. Check that if $A = \mathcal{O}_K$ then the strong version of Hensel's lemma implies the "usual" one.

3. Holomorphic functions

Reference for this section: [**Laz62**].

Let E be a closed subfield of $\mathbf{C}_p$ and let $f(X)=\sum_{n\in\mathbf{Z}} a_n X^n$ with $a_n\in E$. If I is an interval of $\mathbf{R}\cup\{+\infty\}$ and if $A(I)=\{z\in\mathbf{C}_p \text{ with } \mathrm{val}_p(z)\in I\}$, then $f(X)$ converges on $A(I)$ if and only if $\mathrm{val}_p(a_n)+n\mu\to+\infty$ as $n\to\pm\infty$ for every $\mu\in I$. This applies with I being either open or closed at each endpoint. We then say that $f(X)$ is holomorphic on the annulus $A(I)$. If $\mu\in I$, then we set $\mathrm{V}(f,\mu)=\min_{n\in\mathbf{Z}}(\mathrm{val}_p(a_n)+n\mu)$. We denote by $\mathcal{H}(I)$ the ring of holomorphic functions on $A(I)$ and by $\mathcal{B}(I)$ the subring of bounded functions on $A(I)$. If I is closed, then $\mathcal{B}(I)=\mathcal{H}(I)$. The ring $\mathcal{H}(I)$ is endowed with the Fréchet topology defined by the valuations $\{\mathrm{V}(\cdot,\mu)\}_{\mu\in I}$, and it is complete for that topology.

The Newton polygon $\mathrm{NP}(f)$ is the lower convex hull of the set $\{(n,\mathrm{val}_p(a_n))\}_{n\in\mathbf{Z}}$ in the plane. It is therefore a union of segments of increasing slopes and possibly a half-line. The length of a segment is the length of its projection on the x-axis (or, if the segment is a half-line, of the longest piece between two points of the form $(n,\mathrm{val}_p(a_n))$). The first and last piece of $\mathrm{NP}(f)$ may be of infinite length or of slope $\mp\infty$. If $+\infty\in I$, then $A(I)$ is a disk so that $f(X)=\sum_{n\geqslant 0} a_n X^n$ and by convention $\mathrm{NP}(f)$ only starts at $x=0$.

Example 3.1. — Let $I=]0;+\infty]$ so that $A(I)$ is the open unit disk.

1. If $f(X)=\log(1+X)$, then $\mathrm{NP}(f)$ has one segment of slope $-\infty$ and length 1, and for each $n\geqslant 1$, it has a segment of slope $-1/(p^{n-1}(p-1))$ and length $p^{n-1}(p-1)$.
2. If $f(X)=\sum_{n\geqslant 0} X^n$, then $\mathrm{NP}(f)$ is a horizontal half-line, a segment of length ∞.
3. If $f(X)=\sum_{n\geqslant 0} p^n X^{n^2}$, then $\mathrm{NP}(f)$ is a horizontal half-line, a segment of length 0.

Theorem 3.2. — *If $f(X)\in\mathcal{H}(I)$ and if $s\in I$, then*

1. *the number of zeroes of $f(X)$ in $A(I)$ with valuation s is equal to the length of the segment of $\mathrm{NP}(f)$ whose slope is $-s$;*
2. *if $s\neq\pm\infty$ is such a slope, then there exists a unique polynomial $P_s(X)\in E[X]$ with $P_s(0)=1$ such that $f(X)=P_s(X)g(X)$ with $g(X)\in\mathcal{H}(I)$, $\mathrm{NP}(P_s)$ is the piece of slope $-s$ of $\mathrm{NP}(f)$, and $\mathrm{NP}(g)$ is $\mathrm{NP}(f)$ without the piece of slope $-s$;*
3. *if $A(I)$ is a disk, then the same is true with $P_\infty(X)=X^\ell$ where ℓ is the length of the piece of $\mathrm{NP}(f)$ of slope $-\infty$.*

Corollary 3.3. — *If $f(X)\in\mathcal{H}(I)$, then $f(X)\in\mathcal{B}(I)$ if and only if f has finitely many zeroes in $A(I)$.*

Proof. — Let $r=\inf(I)$ and $s=\sup(I)$. A function $f(X)\in\mathcal{H}(I)$ is bounded if and only if $\mathrm{val}_p(a_n)+nr$ is bounded from below as $n\to+\infty$ and $\mathrm{val}_p(a_n)+ns$ is bounded from below as $n\to-\infty$.

If f has finitely many zeroes in $A(I)$ then (1) of theorem 3.2 implies that implies that $\mathrm{NP}(f)$ has finitely many segments of slope $\leqslant -r$ and if $(m, \mathrm{val}_p(a_m))$ is the endpoint of the last such segment, then $a_n - a_m \geqslant -r(n-m)$ so that $\mathrm{val}_p(a_n) + nr$ is bounded from below as $n \to +\infty$. The case $n \to -\infty$ is symmetrical.

Suppose now that $f(X) \in \mathcal{B}(I)$ □

Corollary 3.4. — *If $f(X) \in \mathcal{H}(I)$ has no zeroes in $A(I)$, then $f(X) \in \mathcal{B}(I)^\times$.*

Proof. — If $f(X) \in \mathcal{H}(I)$ has no zeroes in $A(I)$, then by corollary 3.3, $f(X) \in \mathcal{B}(I)$. □

Corollary 3.5. — *The ring $\mathcal{B}(I)$ is a PID.*

Proof. — Let J be an ideal of $\mathcal{B}(I)$. For each $f(X) \in J$, we can write $f(X) = P_f(X)f^\times(X)$ where $P_f(X)$ is a polynomial and $f^\times(X) \in \mathcal{B}(I)^\times$. The ideal of $E[X]$ generated by the $P_f(X)$ is principal and if $P(X)$ denotes a generator of that ideal, then $J = P(X) \cdot \mathcal{B}(I)$. □

We now assume that E is a finite extension of $\mathbf{Q}_p$. A divisor D on $A(I)$ is a sequence of polynomials $\{P_s(X)\}_{s\in I}$ such that $\mathrm{NP}(P_s)$ is a segment of slope $-s$ and such that for any closed interval $J \subset I$, the set of $s \in J$ with $P_s(X) \neq 1$ is finite. If $f(X) \in \mathcal{H}(I)$, then $\mathrm{div}(f)$ is the set of polynomials resulting from theorem 3.2.

Proposition 3.6. — *If $f(X) \in \mathcal{H}(I)$, then $\mathrm{div}(f)$ is a divisor on $A(I)$ and if D is a divisor on $A(I)$, then there exists $f(X) \in \mathcal{H}(I)$ such that $\mathrm{div}(f) = D$.*

Theorem 3.7. — *If $D = \{P_s(X)\}_{s\in I}$ is a divisor on $A(I)$ and if $Q_s(X) \in E[X]$ satisfies $\deg(Q_s) < \deg(P_s)$ for every $s \in I$, then there exists $f \in \mathcal{H}(I)$ such that $f - Q_s$ is divisible by P_s for every $s \in I$.*

Corollary 3.8. — *The ring $\mathcal{H}(I)$ is a Bezout domain.*

Exercises

1. The Newton polygon of f is the graph of the Legendre transform of $\mathrm{V}(f, \cdot)$ (the function $\lambda \mapsto \sup_{\mu\in\mathbf{R}}(\mathrm{V}(f,\mu) - \lambda\mu)$).
2. Let $t = \log(1+X) = X - X^2/2 + X^3/3 - \cdots$ and for $n \geqslant 1$, let $Q_n(X) = \Phi_{p^n}(1+X) = ((1+X)^{p^n} - 1)/((1+X)^{p^{n-1}} - 1)$.
   (a) Prove that t is a holomorphic function on the open unit disk, and that t has a zero at $X = 0$ as well as $p^{n-1}(p-1)$ zeroes of valuation $1/(p^{n-1}(p-1))$ for every $n \geqslant 1$;
   (b) Prove that $p^{-n}\binom{p^n}{k} \to (-1)^{k-1}/k$ as $n \to \infty$ and that $t = \lim_{n\to\infty}((1+X)^{p^n} - 1)/p^n$;
   (c) Prove that $t = X \cdot \prod_{n=1}^{+\infty} Q_n(X)/p$. What are the zeroes of t?

4. Ramification of local fields

Let K be a finite extension of $\mathbf{Q}_p$ and let L be a finite extension of K. Let val_L be the valuation on L normalized so that $\mathrm{val}_L(L^\times) = \mathbf{Z}$. If $g \in \mathrm{Gal}(L/K)$, we set $i_L(g) = \inf_{x\in\mathcal{O}_L} \mathrm{val}_L(g(x)-x)$ and if $u \in \mathbf{R}_{\geqslant -1}$ we define

$$\mathrm{Gal}(L/K)_u = \{g \in \mathrm{Gal}(L/K) \text{ such that } i_L(g) \geqslant u+1\}.$$

We know that $\mathrm{Gal}(L/K)_u$ is a normal subgroup of $\mathrm{Gal}(L/K)$, that $\mathrm{Gal}(L/K)_{-1} = \mathrm{Gal}(L/K)$ and that $\mathrm{Gal}(L/K)_u = \{1\}$ if $u \gg 0$. Furthermore, if $-1 < u \leqslant 0$, then $\mathrm{Gal}(L/K)_u$ is the inertia subgroup of $\mathrm{Gal}(L/K)$. If $u \in \mathbf{Z}_{\geqslant 0}$ and if π_L is a uniformizer of L, then we also have

$$\mathrm{Gal}(L/K)_u = \left\{ g \in \mathrm{Gal}(L/K)_0 \text{ such that } \frac{g(\pi_L)}{\pi_L} \in 1+\mathfrak{m}_L^u \right\},$$

and $\mathrm{Gal}(L/K)_1$ is the wild inertia subgroup of $\mathrm{Gal}(L/K)$.

If $L/K/F$ is a tower of galois extensions, then $\mathrm{Gal}(L/K)_u = \mathrm{Gal}(L/K) \cap \mathrm{Gal}(L/F)_u$ but it is not true in general that $\mathrm{Gal}(K/F)_u$ is the image of $\mathrm{Gal}(L/F)_u$ in $\mathrm{Gal}(L/K)$ (see exercise 1). However, one is usually interested in fixing the base field and varying the extension and one changes the numbering of the filtration so that it becomes compatible with quotients. If L/F is a Galois extension and $u \in \mathbf{R}_{\geqslant -1}$ set

$$\varphi_{L/F}(u) = \int_0^u \frac{dt}{[\mathrm{Gal}(L/F)_0 : \mathrm{Gal}(L/F)_t]}.$$

This defines a continuous, piecewise affine, increasing and concave homeomorphism $\varphi_{L/F} : \mathbf{R}_{\geqslant -1} \to \mathbf{R}_{\geqslant -1}$ called Herbrand's function. Let $\psi_{L/F} : \mathbf{R}_{\geqslant -1} \to \mathbf{R}_{\geqslant -1}$ be its inverse function and define $\mathrm{Gal}(L/F)^v = \mathrm{Gal}(L/F)_{\psi_{L/F}(v)}$. Herbrand's theorem is then the following statement.

Theorem 4.1. — *If $L/K/F$ is a tower of Galois extensions, then $\mathrm{Gal}(K/F)^v$ is the image of $\mathrm{Gal}(L/F)^v$ in $\mathrm{Gal}(K/F)$.*

For example, if $F_n = \mathbf{Q}_p(\zeta_{p^n})$ then $\mathrm{Gal}(F_n/\mathbf{Q}_p)^i = \mathrm{Gal}(F_n/F_i)$.

Let K be a finite extension of $\mathbf{Q}_p$ and let L be a finite extension of K. The bilinear form $L \times L \to K$ given by $(x,y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerate and if I is a fractional ideal of L, we set $\check{I} = \{y \in L \text{ such that } \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } x \in I\}$. The different of the extension L/K is the ideal $\mathfrak{d}_{L/K} = \check{\mathcal{O}}_L^{-1}$. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and if $P(T)$ is the minimal polynomial of α, then $\mathfrak{d}_{L/K}$ is generated by $P'(\alpha)$. In particular, if L/K is a Galois extension, then $\mathrm{val}_L(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(|\mathrm{Gal}(L/K)_t| - 1)dt$.

Lemma 4.2. — *If L/K is a finite extension and if I is an ideal of $\mathcal{O}_L$ then*

$$v_K(\mathrm{Tr}_{L/K}(I)) = \lfloor v_K(I \cdot \mathfrak{d}_{L/K}) \rfloor.$$

Proof. — By definition, we have $\mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K$ if and only if $x \in \mathfrak{d}_{L/K}^{-1}$ so that if I is an ideal of $\mathcal{O}_L$ and J is an ideal of $\mathcal{O}_K$ then $\mathrm{Tr}_{L/K}(I) \subset J$ if and only if $I \subset \mathfrak{d}_{L/K}^{-1} \cdot J$. In particular, $\mathrm{Tr}_{L/K}(I)$ is the smallest ideal J of $\mathcal{O}_K$ such that $J \cdot \mathcal{O}_L$ contains $I \cdot \mathfrak{d}_{L/K}$, which implies the lemma. □

Let F be a fixed field, for example $F = \mathbf{Q}_p$. By theorem 4.1 (Herbrand's theorem), the upper numbering of the groups $\mathrm{Gal}(K/F)$ is compatible with the quotient maps so that if we set $K^u = K^{\mathrm{Gal}(K/F)^u}$ then $K^u = K \cap L^u$ for any extension L of K. Note that if K is a finite extension of F, then there exists $u(K) \in \mathbf{R}_{\geqslant 0}$ such that $K = K^u$ if $u \geqslant u(K)$. The conductor of K (over F) is the infimum of the real numbers u such that $K = K^u$.

Proposition 4.3. — *If K is a finite extension of $\mathbf{Q}_p$, then*

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

Lemma 4.4. — *We have $F_n^u \subset F_{\lfloor u \rfloor}$.*

Exercises

1. Let $F = \mathbf{Q}_p(\zeta_p)$ and $K = \mathbf{Q}_p(\zeta_{p^2})$ and $L = \mathbf{Q}_p(\zeta_{p^2}, p^{1/p})$. For $0 \leqslant i \leqslant p-1$, let $K_i = \mathbf{Q}_p(\zeta_p, p^{1/p}\zeta_{p^2}^i)$. Using all of these extensons, prove that the lower numbering is not compatible with quotients.
2. * It is known that there exist nontrivial field extensions $K/\mathbf{C}_p$ such that $\mathrm{val}_p(K^\times) = \mathbf{Q}$ and $k_K = \overline{\mathbf{F}}_p$. Can you find one?
3. Prove that if $a, b \in \mathbf{Z}_{\geqslant 0}$ then $\mathrm{val}_p(\binom{a+b}{a})$ is the number of carries when adding a and b in base b.

5. Ax and Ax-Sen-Tate's theorems

We start this chapter with a well-known result.

Theorem 5.1. — *If F is a complete valued field, then $\widehat{F^{\mathrm{alg}}}$ (the completion of the algebraic closure of F) is algebraically closed.*

Proof. — We prove by induction on $\deg(P)$ that every polynomial $P(X) \in \widehat{F^{\mathrm{alg}}}[X]$ of degree $\geqslant 1$ has a root. We may assume that $P(X) \in \mathcal{O}_{\widehat{F^{\mathrm{alg}}}}[X]$ is monic. Write $P(X) = \lim P_n(X)$ with $P_n(X) \in F^{\mathrm{alg}}[X]$, and let $\alpha_n \in F^{\mathrm{alg}}$ be a root of $P_n(X)$ so that $P(X) \to 0$. If $P'(\alpha_n)$ does not converge to 0, then Hensel's lemma implies that for $n \gg 0$, α_n gives

rise to a root of $P(X)$. If $P'(\alpha_n) \to 0$, then the induction hypothesis implies that $P'(X)$ decomposes in $\widehat{F^{\mathrm{alg}}}[X]$ and then α_n converges to one of its roots, which is then also a root of $P(X)$. □

Theorem 5.2. — *If F is a valued field of characteristic p, then F^{sep} is dense in F^{alg}.*

Proof. — If $y \in F^{\mathrm{alg}}$, then there exists $n \geqslant 1$ such that $y^{p^n} = \alpha \in F^{\mathrm{sep}}$ and we may assume that $v(\alpha) \geqslant 0$. Let π denote some element of F with $v(\pi) > 0$, and let y_i be a root of the separable polynomial $Y^{p^n} - \pi^i Y - \alpha = 0$. We then have $(y - y_i)^{p^n} = \pi^i y_i$ so that $y_i \to y$ as $i \to +\infty$ which proves the theorem. □

The next result, the theorem of Ax, Sen and Tate, is harder than the preceding two.

Theorem 5.3. — *If F is a complete p-adic field and if $K \subset F^{\mathrm{alg}}$, then $\widehat{F^{\mathrm{alg}}}^{G_K} = \widehat{K}$.*

Before we prove this theorem, we need to establish two lemmas.

Lemma 5.4. — *Let $P(X) \in F^{\mathrm{alg}}[X]$ be a monic polynomial of degree n, all of whose roots satisfy $\mathrm{val}_p(\alpha) \geqslant c$ for some constant c.*

1. *If $n = p^k d$ with $p \nmid d$ and $q = p^k$, then $P^{(q)}(X)$ has a root β satisfying $\mathrm{val}_p(\beta) \geqslant c$.*
2. *If $n = p^{k+1}$ and $q = p^k$, then $P^{(q)}(X)$ has a root β satisfying*

$$\mathrm{val}_p(\beta) \geqslant c - \frac{1}{p^k(p-1)}.$$

Proof. — If we write $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ then $\mathrm{val}_p(a_i) \geqslant (n-i)\cdot c$ and $1/q! \cdot P^{(q)}(X) = \sum_{i=0}^{n-q} \binom{n-i}{q} a_{n-i} X^{n-i-q}$. The product of the roots of $P^{(q)}(X)$ is then $\pm a_q / \binom{n}{q}$ so that there is at least one root β satisfying

$$\mathrm{val}_p(\beta) \geqslant \frac{1}{n-q}\left((n-q)c - \mathrm{val}_p\binom{n}{q}\right).$$

The lemma follows from the fact that in case (1), we have $\mathrm{val}_p(\binom{n}{q}) = 0$ while in case (2), we have $\mathrm{val}_p(\binom{n}{q}) = 1$. □

If $\alpha \in F^{\mathrm{alg}}$, let $\Delta_K(\alpha) = \inf_{g \in G_K} \mathrm{val}_p(g(\alpha) - \alpha)$.

Lemma 5.5. — *If $\alpha \in F^{\mathrm{alg}}$, then there exists $\delta \in K$ such that $\mathrm{val}_p(\alpha - \delta) \geqslant \Delta_K(\alpha) - p/(p-1)^2$.*

Proof. — We prove by induction on $n = [K(\alpha) : K]$ that we can find such a δ with

$$\mathrm{val}_p(\alpha - \delta) \geqslant \Delta_K(\alpha) - \sum_{k=0}^{m} \frac{1}{p^k(p-1)}$$

where p^{m+1} is the largest power of p which is $\leqslant n$.

Let $Q(X)$ be the minimal polynomial of α over K. Lemma 5.4 applied to $P(X) = Q(X+\alpha)$ gives us an element $\delta = \beta + \alpha$ such that $\mathrm{val}_p(\delta - \alpha) \geqslant c$ or $\mathrm{val}_p(\delta - \alpha) \geqslant c - 1/p^k(p-1)$ depending on the nature of n. We then have $[K(\beta) : K] < [K(\alpha) : K]$ while either $\Delta_K(\delta) \geqslant \Delta_K(\alpha)$ or $\Delta_K(\delta) \geqslant \Delta_K(\alpha) - 1/p^k(p-1)$. This allows us to finish the induction. □

Note that by a result of Le Borgne (see [**LB10**]), the constant $p/(p-1)^2$ above can be improved to $1/(p-1)$ which is then optimal.

Proof of theorem 5.3. — If $\alpha \in \widehat{F^{\mathrm{alg}}}$ then we can write $\alpha = \lim \alpha_n$ with $\alpha_n \in F^{\mathrm{alg}}$. We then have $\Delta_K(\alpha_n) \to +\infty$ and lemma 5.5 gives us a sequence $\{\delta_n\}_{n\geqslant 1}$ with $\delta_n \in K$ and $\mathrm{val}_p(\alpha_n - \delta_n) \to +\infty$ so that α is a limit of elements of K. □

Exercises

1. If F is a field of characteristic p, then show that $F^{\mathrm{alg}} = (F^{\mathrm{sep}})^{\mathrm{rad}}$ and $F^{\mathrm{alg}} = (F^{\mathrm{rad}})^{\mathrm{sep}}$.

6. Witt vectors

We say that a ring A is a perfect p-ring if $R = A/pA$ is a perfect ring, p is not a zero divisor in A and A is separated and complete for the p-adic topology. For each $x \in R$, let $\hat{x} \in A$ be a lift of x. If $x_0 = x \in R$ and if for each $i \geqslant 0$ we choose $x_i \in R$ such that $x_{i+1}^p = x_i$ then the sequence $(\hat{x}_i^{p^i})_{i\geqslant 0}$ converges in A to an element $[x]$ which only depends on x, and which is called the Teichmüller lift of x. The set $\{[x]\}_{x\in R}$ is a set of representatives of R in A so that every element $a \in A$ can be written in a unique way as $a = \sum_{i\geqslant 0} p^i[a_i]$ with $a_i \in R$.

Let S be the p-adic completion of $\mathbf{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$ so that S is a perfect p-ring and $S/pS = \mathbf{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$. Note that $X_i \in S$ is the Teichmüller lift of $X_i \in S/pS$ and likewise for Y_i. There exist elements $S_i \in S/pS$ and $P_i \in S/pS$ 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 if we choose some elements $\{x_i\}_{i\geqslant 0}$ and $\{y_i\}_{i\geqslant 0}$ in $R = A/pA$, then let $\pi : S \to A$ be the ring homomorphism determined by $X_i \mapsto [x_i]$ and $Y_i \mapsto [y_i]$.

If we apply π to the above formulas, then we get :

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

so that addition and multiplication are given by universal formulas.

Let J be some set, let $R_J = \mathbf{F}_p[X_j^{p^{-\infty}}]_{j\in J}$ and let S_J be the p-adic completion of $\mathbf{Z}_p[X_j^{p^{-\infty}}]_{j\in J}$ so that S_J is a perfect p-ring and $S_J/pS_J = R_J$. If R is any perfect ring in which $p=0$, then R is a quotient of R_J for some J by a perfect ideal I. We then set $W(I) = \{\sum_{i\geqslant 0} p^i[x_i]$ where $x_i \in I$ for all $i \geqslant 0\}$ so that $W(I)$ is an ideal of S_J.

Theorem 6.1. — *If R is a perfect ring in which $p=0$ then there exists a unique perfect p-ring $W(R)$ such that $W(R)/pW(R) = R$. If R' is another perfect ring in which $p=0$ then any $f : R \to R'$ lifts to a unique $W(f) : W(R) \to W(R')$.*

Proof. — Write $R = R_J/I$ as above and set $W(R) = S_J/W(I)$ so that we have $W(R)/pW(R) = S_J/(W(I)+pS_J) = R_J/I = R$. The definition of $W(I)$ shows that if $x \in S_J$ satisfies $px \in W(I)$, then $x \in W(I)$ so that p is not a zero divisor in $W(R)$. The ring S_J is complete for the p-adic topology and hence so is $W(R)$. Finally, $\cap_{n\geqslant 0}(p^n S_J + W(I)) = W(I)$ so that $W(R)$ is separated.

Any perfect p-ring A such that $A/pA = R$ is then the set of of elements of the form $\sum_{i\geqslant 0} p^i[x_i]$ with the x_i's in R, addition and multiplication being given by the formulas above so that two such rings are canonically isomorphic.

If $f : R \to R'$ is a homomorphism, then the unique $g : A \to A'$ lifting f is given by $g(\sum_{i\geqslant 0} p^i[x_i]) = \sum_{i\geqslant 0} p^i[f(x_i)]$. Indeed, the formulas for $+$ and $\times$ recalled above show that g thus defined commutes with $+$ and $\times$. □

The ring $W(R)$ is therefore well-defined and is called the ring of Witt vectors with coefficients in R. It is simply the set of elements of the form $\sum_{i\geqslant 0} p^i[x_i]$ with the x_i's in R, addition and multiplication being given by the formulas above. The Frobenius map φ on $W(R)$ is given by $\varphi = W(y \mapsto y^p)$.

We now show a generalization of the last assertion of theorem 6.1.

Theorem 6.2. — *If A is a ring which is complete for the p-adic topology and if R is a perfect ring of characteristic p, then a map $f : R \to A/pA$ lifts to $W(f) : W(R) \to A$.*

Proof. — If $x \in R$, let $x^{(n)}$ denote the p^n-th root of x in R and let $\hat{f} : R \to A$ be any set-theoretic lift of f to A. The sequence $\{\hat{f}(x^{(n)})^{p^n}\}_{n\geqslant 0}$ is then convergent and its limit depends only on x. We define $W(f)([x]) = \lim_{n\to\infty} \hat{f}(x^{(n)})^{p^n}$ (since $W(f)$ lifts f, this

definition is imposed and hence $W(f)$ is unique). Every element of $W(R)$ can be written as $\sum_{k\geqslant 0} p^k[x_k]$ and we set $W(f)(\sum_{k\geqslant 0} p^k[x_k]) = \sum_{k\geqslant 0} p^k W(f)([x_k])$. This gives us the formula for $W(f)$ and since $W(f)([x]\cdot[y]) = W(f)([x])\cdot W(f)([y])$, we only need to show that $W(f)$ is additive. We show this modulo p^{n+1} for all $n \geqslant 1$, using the fact that $W(f)([x]) = \hat{f}(x^{(n)})^{p^n} \bmod p^{n+1}$.

In the p-adic completion of $\mathbf{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$ considered above, we have

$$(X_0 + pX_1 + \cdots + p^n X_n) + (Y_0 + pY_1 + \cdots + p^n Y_n) \equiv [S_0] + p[S_1] + \cdots + p^n[S_n] \bmod p^{n+1},$$

where the S_i belong to $\mathbf{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$. If $S_{k,n} \in \mathbf{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$ is a p^n-th root of S_k and $\hat{S}_{k,n}$ is a lift of $S_{k,n}$ to $\mathbf{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$ then in this ring we have

$$(X_0 + pX_1 + \cdots + p^n X_n) + (Y_0 + pY_1 + \cdots + p^n Y_n) \\ \hat{\mathrm{E}} \equiv \hat{S}_{0,n}^{p^n} + p\hat{S}_{1,n}^{p^n} + \cdots + p^n \hat{S}_{n,n}^{p^n} \bmod p^{n+1}.$$

If $x_0, \ldots, x_n \in R$ and $y_0, \ldots, y_n \in R$ then by applying the above formula to $X_i = \hat{f}(x_i^{(n)})^{p^n}$ and $Y_i = \hat{f}(y_i^{(n)})^{p^n}$, we find that

$$\hat{f}(x_0^{(n)})^{p^n} + p\hat{f}(x_1^{(n)})^{p^n} + \cdots + p^n\hat{f}(x_n^{(n)})^{p^n} + \hat{f}(y_0^{(n)})^{p^n} + p\hat{f}(y_1^{(n)})^{p^n} + \cdots + p^n\hat{f}(y_n^{(n)})^{p^n} \\ \hat{\mathrm{E}} \equiv \hat{S}_{0,n}(\hat{f}(x_i^{(n)})^{p^n}, \hat{f}(y_i^{(n)})^{p^n})^{p^n} + \cdots + p^n\hat{S}_{n,n}(\hat{f}(x_i^{(n)})^{p^n}, \hat{f}(y_i^{(n)})^{p^n})^{p^n} \bmod p^{n+1}.$$

Since $W(f)([x_k]) = \hat{f}(x_k^{(n)})^{p^n} \bmod p^{n+1}$ and likewise for the y_k's and since

$$W(f)([S_k(x_i, y_i)]) = \hat{S}_{k,n}(\hat{f}(x_i^{(n)})^{p^n}, \hat{f}(y_i^{(n)})^{p^n})^{p^n} \bmod p^{n+1},$$

the above formula says that

$$\sum_{k=0}^{n} p^k W(f)([x_k]) + \sum_{k=0}^{n} p^k W(f)([y_k]) \equiv \sum_{k=0}^{n} p^k W(f)([S_k(x_i, y_i)]) \bmod p^{n+1}$$

and therefore that $W(f)$ is indeed additive. □

If A is complete for the p-adic topology as above (later on, we'll take $A = \mathcal{O}_{\mathbf{C}_p}$), let $\mathrm{Perf}(A/pA) = \varprojlim_{x\mapsto x^p} A/pA$ so that $\mathrm{Perf}(A/pA)$ is a perfect ring of characteristic p. If $x = (x_0, x_1, \ldots) \in \mathrm{Perf}(A/pA)$ and for each i we choose a lift $\hat{x}_i \in A$ of x_i then the sequence $\{\hat{x}_i^{p^i}\}_{i\geqslant 0}$ converges in A to an element $f(x) = x^{(0)}$ which only depends on x.

Corollary 6.3. — *The map $\theta : W(\mathrm{Perf}(A/pA)) \to A$ given by $\sum_{i\geqslant 0} p^i[x_i] \mapsto \sum_{i\geqslant 0} p^i x_i^{(0)}$ is a ring homomorphism.*

Exercises

1. If A is a perfect p-ring and $a \in A$, then $a = [\overline{a}]$ if and only if a is a p^∞-th power in A.
2. If k is a perfect field of characteristic p, then $W(k)[1/p]$ is a field. In general, which elements of $W(R)$ are invertible?

3. State and prove an analogue of proposition 16.1 for the P_i's.
4. Compute S_0 and S_1 and P_0 and P_1.
5. Prove that if A is a perfect p-ring, then θ is an isomorphism.
6. Prove that the map θ is surjective if and only if $x \mapsto x^p$ is surjective on A/pA.
7. Prove that if $x, y \in W(R)$, then $w_k(xy) \geqslant \inf_{i+j \leqslant k}(w_i(x) + w_j(y))$.
8. Modify the proof of proposition 16.4 to show that the map $R^{\mathbf{Z}_{\geqslant 0}} \to W(R)$ given by $(x_i)_{i \geqslant 0} \mapsto \sum_{i \geqslant 0} p^i [x_i]$ is a homeomorphism.

7. Galois cohomology

Let G and M be topological groups, with a continuous action of G on M. We define $H^0(G, M) = M^G$, the set of fixed points in M under the action of G.

A cocyle on G with values in M is a continuous map $c : G \to M$ such that $c(gh) = c(g) \cdot g(c(h))$. If c is a cocyle and $m \in M$, then $g \mapsto m^{-1} \cdot c(g) \cdot g(m)$ is another cocycle which is said to be cohomologous to c. This defines an equivalence relation on the set of cocyles, and $H^1(G, M)$ is the set of equivalence classes of cocyles under this equivalence relation. An element of $H^1(G, M)$ is trivial if it is in the class of the cocycle $g \mapsto 1$, that is if it can be represented by a cocyle of the form $g \mapsto m \cdot g(m)^{-1}$ for some $m \in M$.

Suppose that R is a topological ring with a continuous action of G, that X is a free R-module of finite rank d with a semilinear action of G and that $e = \{e_1, \ldots, e_d\}$ is a basis of X. If we denote by $\mathrm{Mat}_e(g)$ the matrix of $g \in G$ in the basis e, then $g \mapsto \mathrm{Mat}_e(g)$ is a cocyle on G with values in $\mathrm{GL}_d(R)$. Furthermore, if f is another basis of X and if M is the matrix of f in e, then $\mathrm{Mat}_f(g) = M^{-1} \cdot \mathrm{Mat}_e(g) \cdot g(M)$. In this way, one can associate to the semilinear representation X a well-defined class $[X] \in H^1(G, \mathrm{GL}_d(R))$. This way, we get a natural bijection between $H^1(G, \mathrm{GL}_d(R))$ and the set of isomorphism classes of semilinear representations of G on free R-modules of rank d.

Suppose now that M is an R-module with an action of G, and that E is an extension of R by M, that is an R-module with an action of G which sits in an exact sequence $0 \to M \to E \to R$. If $e \in E$ is some element of E which maps to $1 \in R$ and $g \in G$, then $e - g(e) \in M$ and the map $g \mapsto e - g(e)$ is a cocyle on G with values in M. If we choose a different e, then we get a cohomologous cocyle, and therefore we can associate to E a class $[E] \in H^1(G, M)$. This way, we get a natural bijection between $H^1(G, M)$ and the set of isomorphism classes of extensions R by M. If $0 \to X \to E \to Y \to 0$ is an exact sequence of R-modules with a continuous action of G, then we have a long exact sequence :

$$0 \to X^G \to E^G \to Y^G \xrightarrow{\delta} H^1(G, X) \to H^1(G, E) \to H^1(G, Y),$$

where the map $\delta : Y^G \to H^1(G, X)$ is defined as follows : if $y \in Y^G$ is the image of $e \in E$, then $\delta(y)(g) = e - g(e)$.

Let G and M be topological groups as above and let H be a closed normal subgroup of G. We then have a restriction map $\mathrm{res} : H^1(G, M) \to H^1(H, M)$ defined by $\mathrm{res}(c)(h) = c(h)$ and an inflation map $\mathrm{inf} : H^1(G/H, M^H) \to H^1(G, M)$ defined by $\mathrm{inf}(c)(g) = c(\overline{g})$. Note that G acts on $H^1(H, M)$ by $g(c)(h) = g(c(g^{-1}hg)$ and that the action $H \subset G$ on $H^1(H, M)$ is trivial so that G/H acts on $H^1(H, M)$.

Theorem 7.1. — *If G, M and H are as above, then :*

1. $\mathrm{res}(H^1(G, M)) \subset H^1(H, X)^{G/H}$*;*
2. $\mathrm{res}(c) = 0$ *if and only if* $c \in \mathrm{inf}(H^1(G/H, M^H))$*.*

In other words, there is an exact sequence of pointed sets :

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{inf}} H^1(G, M) \xrightarrow{\mathrm{res}} H^1(H, X)^{G/H}.$$

Proof. — If $c \in H^1(G, M)$ and $g \in G$, then $g(c)(h) = c(g)^{-1}c(h)h(c(g))$ so that $g(c)$ is cohomologous to c and therefore $c(g) \in H^1(H, X)^{G/H}$ which proves (1). We have $(\mathrm{res} \circ \mathrm{inf})(c)(h) = c(1) = 1$ so that $\mathrm{res} \circ \mathrm{inf} = 0$, and conversely if $\mathrm{res}(c) = 0$ then we can assume that c is actually trivial on H and then $c(gh) = c(g)$ so that c is inflated from G/H and $h(c(g)) = c(hg)c(h)^{-1} = c(g \cdot g^{-1}hg) = c(g)$ so that $c \in \mathrm{inf}(H^1(G/H, M^H))$. □

Theorem 7.2. — *If L/K is a finite Galois extension and $G = \mathrm{Gal}(L/K)$, then :*

1. $H^1(G, \mathrm{GL}_d(L)) = \{1\}$*;*
2. $H^1(G, L) = \{0\}$*.*

Proof. — Choose some $U \in H^1(G, \mathrm{GL}_d(L))$. For $\alpha \in L$, define $P(\alpha) = \sum_{g \in G} g(\alpha)U(g)$. The cocyle relation gives us $U(g) \cdot g(P(\alpha)) = P(\alpha)$ so that in order to prove (1), it is enough to show that there exists some $\alpha \in L$ such that $P(\alpha)$ is invertible.

We do this in the case when L is infinite (the case of a finite field is treated in exercise 4). Let $\{X_g\}_{g \in G}$ be a set of variables indexed by the elements of G, and consider the multivariable polynomial $Q(\{X_g\}_{g \in G}) = \det(\sum_{g \in G} X_g U(g))$. This polynomial is nonzero because the $U(g)$'s are invertible, and Artin's theorem on the algebraic independance of characters then gives us the existence of an $\alpha \in L$ such that $Q(\{g(\alpha)\}_{g \in G}) \neq 0$ so that $P(\alpha)$ is invertible, which proves (1).

In order to prove (2), choose some $f \in H^1(G, L)$ and consider the cocyle $[U : g \mapsto \left(\begin{smallmatrix} 1 & f(g) \\ 0 & 1 \end{smallmatrix}\right)] \in H^1(G, \mathrm{GL}_2(L))$. Item (1) gives us a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $U(g) \cdot g(M) = M$. Since M is invertible, either c or d is $\neq 0$, say c. The relation $U(g) \cdot g(M) = M$ tells

us that $g(c)=c$ for all $g\in G$ so that $c\in K$ and also that $g(a)+f(g)g(c)=a$ so that $f(g)=a/c-g(a/c)$ and f is indeed trivial. □

Corollary 7.3. — *Let L/K be a Galois extension with $G=\mathrm{Gal}(L/K)$ and give L the discrete topology. If we consider only continuous cocycles, then $H^1(G,\mathrm{GL}_d(L))=\{1\}$ and $H^1(G,L)=\{0\}$.*

Proof. — In both cases, such a cocyle factors through a finite quotient $\mathrm{Gal}(M/K)$ of $\mathrm{Gal}(L/K)$ and the field generated over K by all the possible values of the cocycle is also a finite extension of K so that we are in the situation of theorem 7.2. □

Proposition 7.4. — *Let π be a topologically nilpotent element of a ring A which is complete for the π-adic topology and in which π is not a zero divisor, let G be a group which acts continuously on A (with $\pi\in A^G$) and let $R=A/\pi A$.*

If $H^1(G,\mathrm{GL}_d(R))$ and $H^1(G,R)$ are both trivial, and if the map $\mathrm{GL}_d(A)\to\mathrm{GL}_d(R)$ is surjective, then $H^1(G,\mathrm{GL}_d(A))$ and $H^1(G,A)$ are both trivial.

Proof. — If $U\in H^1(G,\mathrm{GL}_d(A))$ then $\overline{U}\in H^1(G,\mathrm{GL}_d(R))$ so that by the triviality of $H^1(G,\mathrm{GL}_d(R))$ and the surjectivity of the map $\mathrm{GL}_d(A)\to\mathrm{GL}_d(R)$, there exists a matrix $M_0\in\mathrm{GL}_d(A)$ with $M_0^{-1}\cdot U(g)\cdot g(M_0)\in\mathrm{Id}+\pi\mathrm{M}_d(A)$. Assume that we have constructed matrices $M_0,\dots,M_{k-1}$ with $M_j\in\mathrm{Id}+\pi^j\mathrm{M}_d(A)$ such that

$$M_{k-1}^{-1}\cdots M_0^{-1}\cdot U(g)\cdot g(M_0\cdots M_{k-1})=\mathrm{Id}+\pi^kC(g)\in\mathrm{Id}+\pi^k\mathrm{M}_d(A),$$

and note that $\overline{C}\in H^1(G,\mathrm{M}_d(R))$. If we write $M_k=\mathrm{Id}+\pi^kR_k$, then

$$\hat{\mathrm{E}}M_k^{-1}\cdots M_0^{-1}\cdot U(g)\cdot g(M_0\cdots M_k)=\mathrm{Id}+\pi^k(C(g)+R_k-g(R_k))+\mathrm{O}(\pi^{k+1}),$$

and the triviality of $H^1(G,R)$ allows us to find R_k such that

$$M_k^{-1}\cdots M_0^{-1}\cdot U(g)\cdot g(M_0\cdots M_k)\in\mathrm{Id}+\pi^{k+1}\mathrm{M}_d(A).$$

The infinite product $\prod_{k=0}^{+\infty}M_k$ converges to a matrix M such that $M^{-1}\cdot U(g)\cdot g(M)=\mathrm{Id}$, which proves that $H^1(G,\mathrm{GL}_d(A))$ is indeed trivial. The proof of the triviality of $H^1(G,A)$ is similar (and easier). □

Exercises

1. Check that if M is abelian, then $H^1(G,M)$ has a natural group structure.
2. The semilinear representation X is trivial (in the sense that $X\simeq R^d$ as semilinear representations of G) if and only if $[X]$ is trivial.
3. Using theorem 7.2, prove that if L/K is a finite Galois extension and η is a character of $\mathrm{Gal}(L/K)$ then $L(\eta)=L$ as $\mathrm{Gal}(L/K)$-modules.

4. In the proof of theorem 7.2, suppose that L is a finite field. Artin's theorem now gives you some $\alpha \in \overline{L}$ such that $P(\alpha)$ is invertible. Using the cocycle relation, show that $P(\alpha) \in \mathrm{GL}_d(L)$ so that the theorem is proved in this case also.
5. If G is finite and M is an A-module with $|G|$ invertible in A, then $H^1(G, M) = \{0\}$.
6. Let $G = \overline{\langle g \rangle}$ be a topologically cyclic group and let M be an abelian topological group on which G acts continuously.
   (a) Prove that the map $H^1(G, M) \to M/(1-g)$ given by $c \mapsto c(g)$ is well-defined and injective.
   (b) Prove that if G is infinite and M is finite, then this map is bijective (hint: if $m \in M$, then define $c(g^i) = (1 + g + \cdots + g^{i-1})m$. Let $k \geqslant 1$ be such that $kM = 0$ and let $n \geqslant 1$ be such that $(g^n - 1)M = 0$. Prove that the image of $c(g^i)$ in M only depends on i mod nk so that $h \mapsto c(h)$ extends to G).
   (c) Prove that the above map is still bijective if M is profinite or p-adically complete or a p-adic Banach space.

8. The Dieudonné-Manin theorem

In this section, we follow the exposition of [**Zin84**].

Let k be a perfect field of characteristic p and let $K = W(k)[1/p]$ which is endowed with the absolute frobenius $\sigma = W(x \mapsto x^p) : K \to K$. A φ-module is a finite dimensional K-vector space D along with a bijective map $\varphi : D \to D$ which is σ^a-semilinear for some $a \in \mathbf{Z} \setminus \{0\}$. The fact that k is perfect implies that $\sigma^a(K) = K$ so that the kernel and image of φ are K-vector subspaces of D.

We say that D is effective if there exists a $W(k)$-lattice M of D such that $\varphi(M) \subset M$. If M is any lattice of D, let $a_n = a_n(M)$ be the largest integer such that $\varphi^n(M) \subset p^{a_n}M$. In particular, we have $a_{n+m} \geqslant a_n + a_m$ so that the sequence a_n/n converges to $\lambda = \sup_{n \geqslant 1} a_n/n$. If M' is another lattice, then there are integers e and f such that $p^e M \subset M'$ and $p^f M' \subset M$, so that $a_n(M) - a_n(M')$ is bounded independently of n and λ does not depend on the choice of M. Note that if we set $\tilde{\varphi} = p^{-s}\varphi^r$, then $\tilde{\lambda} = r\lambda - s$.

Let $h = \dim_K(D)$ be the height of D.

Lemma 8.1. — *If M is a lattice of D such that $\varphi^{h+1}(M) \subset p^{-1}M$, then there exists a lattice M' of D such that $\varphi(M') \subset M'$.*

Proof. — For $0 \leqslant j \leqslant h+1$, let $M_j = M + \varphi(M) + \cdots + \varphi^j(M)$ so that $M \subset M_0 \subset M_1 \subset \cdots \subset M_{h+1} \subset p^{-1}M$. Since the k-vector space $p^{-1}M/M$ is of dimension h, there has to exist some $0 \leqslant j \leqslant h$ such that $M_j = M_{j+1}$ and if we set $M' = M_j$ then $\varphi(M') \subset M_{j+1} = M'$. □

Lemma 8.2. — *If D is a φ-module, then :*

1. *$\lambda \geqslant 0$ if and only if D is effective;*

2. *if* $\lambda > 0$, *then* $\lambda \geqslant 1/h$.

Proof. — If D is effective, then $a_n \geqslant 0$ for all n and hence $\lambda \geqslant 0$ also. If $\lambda > 0$, then $a_n \geqslant 0$ for some $n \gg 0$ so that then there is some lattice M such that $\varphi^n(M) \subset M$ and if we set $M' = M + \varphi(M) + \cdots + \varphi^{n-1}(M)$, then $\varphi(M') \subset M'$ so that D is effective. If $\lambda = 0$, then consider D with $\tilde{\varphi} = p\varphi^{h+1}$ so that $\tilde{\lambda} = 1$. The $\tilde{\varphi}$-module D is then effective and lemma 8.1 above then implies that the φ-module D is itself effective which proves (1).

In order to prove (2), note that $\lambda > 0$ if and only if φ is nilpotent on M/pM. Since M/pM is a k-vector space of dimension h, φ is nilpotent if and only if $\varphi^h = 0$ on M/pM which then implies that $\lambda \geqslant 1/h$. □

Proposition 8.3. — *If D is a φ-module, then $\lambda = s/r$ where $r, s \in \mathbf{Z}$ and $1 \leqslant r \leqslant h$.*

Proof. — By exercise 2, we can find $r, s \in \mathbf{Z}$ and $1 \leqslant r \leqslant h$ such that $|r\lambda - s| \leqslant 1/(h+1)$ and we then set $\tilde{\varphi} = p^{-s}\varphi^r$ so that $|\tilde{\lambda}| \leqslant 1/(h+1)$. Since $\tilde{\lambda} \geqslant -1/(h+1)$, item (1) of lemma 8.2 above implies that $p\tilde{\varphi}^{h+1}$ is effective and lemma 8.1 then implies that $\tilde{\varphi}$ is effective so that $\tilde{\lambda} \geqslant 0$. Finally, since $\tilde{\lambda} \leqslant 1/(h+1) < 1/h$, item (2) of lemma 8.2 implies that $\tilde{\lambda} = 0$ so that $\lambda = s/r$. □

Lemma 8.4. — *If M is a $W(k)$-lattice of D stable under φ, then one can write $M = M_0 \oplus M_{>0}$ where $\varphi : M_0 \to M_0$ is a bijection and $\varphi : M_{>0} \to M_{>0}$ is topologically nilpotent.*

Proof. — If $n \geqslant 1$, then M/p^nM is both artinian and noetherian so that there exists an integer $k \gg 0$ such that $\cap_{j\geqslant 0}\mathrm{im}(\varphi^j) = \mathrm{im}(\varphi^k)$ and $\cup_{j\geqslant 0}\ker(\varphi^j) = \ker(\varphi^k)$. If $x \in M/p^nM$, then we can write $\varphi^{2k}(x) = \varphi^k(y)$ so that $x = (x - \varphi^k(y)) + \varphi^k(y)$ and hence $\mathrm{im}(\varphi^k) + \ker(\varphi^k) = M/p^nM$. It is immediate that $\mathrm{im}(\varphi^k) \cap \ker(\varphi^k) = \{0\}$ so that $M/p^nM = (M/p^nM)_0 \oplus (M/p^nM)_{>0}$ with $(M/p^nM)_0 = \mathrm{im}(\varphi^k)$ and $(M/p^nM)_{>0} = \ker(\varphi^k)$. This decomposition is compatible with projective limits and hence gives a decomposition of M itself. □

If D is a φ-module, we say that D is pure of slope $\lambda = s/r \in \mathbf{Q}$ if D admits a lattice M on which $p^{-s}\varphi^r$ is a bijection. By exercise 3, the slope is then well-defined.

Theorem 8.5. — *If D is a φ-module, then there exist rational numbers $\lambda_1 < \cdots < \lambda_k$ such that we can write $D = \oplus_{i=1}^k D_i$ where each D_i is pure of slope λ_i.*

Proof. — Let λ be defined as above, so that by proposition 8.3, we have $\lambda = s/r$ and if we set $\tilde{\varphi} = p^{-s}\varphi^r$ then $\tilde{\lambda} = 0$ and $(D, \tilde{\varphi})$ is effective so that by lemma 8.2, D admits a

lattice M which is $\tilde{\varphi}$-stable. In lemma 8.4, note that $M_0 \neq 0$ since $\tilde{\lambda} = 0$ so that we have a non-trivial decomposition $M = M_0 \oplus M_{>0}$ and M_0 and $M_{>0}$ are both stable under φ. By inverting p, we get a corresponding decomposition of the φ-module D as $D_\lambda \oplus D_{>\lambda}$ and the theorem follows by induction. □

In the notation of theorem 8.5 above, the λ_i's are the slopes of φ and λ defined before is then the least slope of φ on D.

A φ-module over a field k of characteristic p is a finite dimensional k-vector space V with a map $\varphi : V \to V$ which is σ^a-semilinear for some $a \in \mathbf{Z} \setminus \{0\}$ and such that $\mathrm{Mat}(\varphi) \in \mathrm{GL}_{\dim(V)}(k)$.

Theorem 8.6. — *If k is a separably closed field of characteristic p and if V is a φ-module over k with $a \geqslant 1$, then :*

1. *V admits a basis of elements fixed by φ;*
2. *$1 - \varphi : V \to V$ is surjective.*

Proof. — Choose some element $e_0 \in V$ and set $e_i = \varphi^i(e_0)$ and let d be the dimension of $\mathrm{vect}(\{e_i\}_{i \geqslant 0})$ so that we can write $e_d = a_0 e_0 + \cdots + a_{d-1} e_{d-1}$. The equation

$$\varphi(b_0 e_0 + \cdots + b_{d-1} e_{d-1}) = b_0 e_0 + \cdots + b_{d-1} e_{d-1}$$

is then equivalent to the system :

$$\begin{cases} b_0 = b_{d-1}^q a_0, \\ b_i = b_{i-1}^q + b_{d-1}^q a_i \quad \text{for } 1 \leqslant i \leqslant d-1. \end{cases}$$

In particular, if we set $x = b_{d-1}$, then x and the a_i's determine the other b_j's provided that x satisfies the equation

$$x = a_0^{q^{d-1}} x^{q^d} + a_1^{q^{d-2}} x^{q^{d-1}} + \cdots + a_{d-1} x^q.$$

Since k is separably closed and the polynomial

$$a_0^{q^{d-1}} X^{q^d - 1} + a_1^{q^{d-2}} X^{q^{d-1} - 1} + \cdots + a_{d-1} X^{q-1} - 1$$

is separable, the above equation has at least one nonzero solution which gives us a $v \neq 0$ in $V^{\varphi=1}$. By induction, item (1) of the theorem tells us that $V/k \cdot v$ admits a basis of elements fixed by φ. Finally, since $(1-\varphi)(xv) = (x - x^q)v$ and the polynomials $X^q - X + a$ are separable, the map $1 - \varphi : k \cdot v \to k \cdot v$ is surjective and V therefore admits a basis of elements fixed by φ which proves (1). The fact that $1 - \varphi : k \cdot v \to k \cdot v$ is surjective if $\varphi(v) = v$ and item (1) then imply item (2). □

If A is a ring which is complete for the p-adic topology, such that $A/pA = k$ with k as above, and which is endowed with a frobenius σ lifting $x \mapsto x^p$, then a φ-module over A is a free A-module of finite rank V with a map $\varphi : V \to V$ which is σ^a-semilinear for some $a \in \mathbf{Z} \setminus \{0\}$ and such that $\mathrm{Mat}(\varphi) \in \mathrm{GL}_{\dim(V)}(A)$.

Corollary 8.7. — *If V is a φ-module over a ring A as above and $a \geqslant 1$, then :*

1. *V admits a basis of elements fixed by φ;*
2. *$1 - \varphi : V \to V$ is surjective.*

Proof. — Successive approximation. □

Note that if k is algebraically closed (instead of merely separably closed), then both results above are true for all $a \in \mathbf{Z} \setminus \{0\}$.

Let k be an algebraically closed field and let $K = W(k)[1/p]$. If $\lambda = s/r \in \mathbf{Q}$ is a rational number where s/r is in lowest terms, we denote by E_λ the elementary φ-module over K of slope λ given by $E_\lambda = \oplus_{i=0}^{r-1} K e_i$ where

$$\begin{cases} \varphi(e_0) = e_1 \\ \qquad \vdots \\ \varphi(e_{r-2}) = e_{r-1} \\ \varphi(e_{r-1}) = p^s e_0. \end{cases}$$

Proposition 8.8. — *The φ-module E_λ above is irreducible.*

Proof. — Suppose that $D \subset E_\lambda$ is stable under φ. By theorem 8.5, D is a direct sum of pure φ-modules so we can assume that D is pure of some slope d/h. By corollary 8.7 applied to $\tilde{\varphi} = p^{-d}\varphi^h$, there exists $y \in D$ such that $\varphi^h(y) = p^d y$. If we write $y = \sum_{i=0}^{r-1} y_i e_i$ then the equation $\varphi^{rh}(y) = p^{rd} y$ implies that $p^{sh}\varphi^{rh}(y_i) = p^{rd} y_i$ which is only possible if $sh = rd$ so that $s/r = d/h$. Since s/r is in lowest terms, we have $h \geqslant r$ so that $D = E_\lambda$ which is therefore irreducible. □

Theorem 8.9. — *If k is an algebraically closed field and $K = W(k)[1/p]$ and D is a φ-module over K, then there is an decomposition $D = E_{\lambda_1}^{m_1} \oplus \cdots \oplus E_{\lambda_k}^{m_k}$ and each m_λ depends only on D.*

Proof. — We first prove the existence of such a decomposition. By theorem 8.5, we can write $D = \oplus D_i$ where each D_i is pure of some slope λ_i and therefore we can assume that D is pure of slope $\lambda = s/r$. By corollary 8.7 applied to $p^{-s}\varphi^r$, D then admits a basis consisting of elements of $D^{\varphi^r = p^s}$. If $y \in D^{\varphi^r = p^s}$ then it gives rise to a map $E_\lambda \to D$ given by $(a_0 + a_1\varphi + \cdots + a_{r-1}\varphi^{r-1})e_0 \mapsto (a_0 + a_1\varphi + \cdots + a_{r-1}\varphi^{r-1})y$ and since E_λ

is irreducible by proposition 8.8, this map is injective if $y \neq 0$. More generally, if we have $y_1, \ldots, y_m \in D^{\varphi^r=p^s}$ giving rise to an injective map $E_\lambda^m \to D$, then either this map is surjective or we can take any y_{m+1} outside of its image and the resulting map $E_\lambda^{m+1} \to D$ will still be injective since E_λ is irreducible. This proves the existence of the decomposition.

In order to prove that m_λ only depends on D, note that $E_\mu^{\varphi^r=p^s} = 0$ if $\mu \neq s/r$ (see exercise 4) so that $m_\lambda = \dim_{\mathbf{Q}_{p^r}} D^{\varphi^r=p^s}$ depends only on D. □

Corollary 8.10. — *The decomposition in theorem 8.5 is unique.*

Exercises

1. (problem 98 of [**PS98**]) Let $\{a_n\}_{n\geqslant 1}$ be a sequence of real numbers such that $a_{n+m} \geqslant a_n + a_m$. Prove that a_n/n converges to $\sup_{n\geqslant 1} a_n/n$. The limit may be infinite in general; why is it finite above?
2. If $\lambda \in \mathbf{R}$ and $h \geqslant 1$, then by considering the images of $0\cdot\lambda$, $1\cdot\lambda$, …, $h\cdot\lambda$ in $\mathbf{R}/\mathbf{Z}$ seen as a circle, prove that there exists $r, s \in \mathbf{Z}$ with $1 \leqslant r \leqslant h$ such that $|r\lambda - s| \leqslant 1/(h+1)$.
3. Prove that if D is pure of some slope, then λ as defined at the beginning of §8 is equal to that slope, which is therefore well-defined.
4. Prove that $E_\mu^{\varphi^r=p^s} = 0$ if $\mu \neq s/r$.
5. Compute the decomposition of $\mathrm{Hom}(E_\lambda, E_\mu)$.
6. Prove that if $k = \mathbf{F}_p$, then the slopes of a φ-module are the p-adic valuations of the eigenvalues of φ.

9. Ramification of the cyclotomic extension

Reference: [**Tat67**]. Let $F = \mathbf{Q}_p$ and $F_n = \mathbf{Q}_p(\zeta_{p^n})$ for $n \geqslant 1$. We know that F_n is a totally ramified extension of F of degree $p^{n-1}(p-1)$ and that $\mathcal{O}_{F_n} = \mathbf{Z}_p[\zeta_{p^n}]$ which allows us to work easily in the extension F_∞/F. If K is a finite extension of $\mathbf{Q}_p$ and $K_n = K(\zeta_{p^n})$ for $n \geqslant 1$, the above properties are no longer necessarily true and in this chapter, we prove a statement whose purpose is to make up for this problem.

Let $\chi : G_K \to \mathbf{Z}_p^\times$ be the cyclotomic character. Since $\chi(G_F) = \mathbf{Z}_p^\times$ and G_K is an open subgroup of G_F, the group $\chi(G_K)$ is an open subgroup of $\mathbf{Z}_p^\times$ and therefore contains $1 + p^n\mathbf{Z}_p$ for $n \gg 0$. If $n \gg 0$, the extension K_{n+1}/K_n is then totally ramified of degree p. In addition, the sequence $\{[K_n : F_n]\}_{n\geqslant 1}$ is decreasing and eventually equal to $d = [K_\infty : F_\infty]$.

Theorem 9.1. — *If K is a finite extension of $F = \mathbf{Q}_p$, then $\{p^n \mathrm{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n\geqslant 1}$ is bounded.*

Proof. — Applying proposition 4.3, we get

$$[K_n : F]\mathrm{val}_p(\mathfrak{d}_{K_n/F}) = \int_{-1}^{\infty}([K_n : F] - [K_n^u : F])du,$$
$$[K_n : F]\mathrm{val}_p(\mathfrak{d}_{F_n/F}) = \int_{-1}^{\infty}([K_n : F] - [K_n : F_n][F_n^u : F])du.$$

By subtracting, we get

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

There exists a constant $u(K)$ such that if $u > u(K)$, then $K^u = K$. In this case, we have $K_n^u F_n = K_n$ as well as $K_n^u \cap F_n = F_n^u$ so that $[K_n : F_n][F_n^u : F] = [K_n^u : F]$ and therefore

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

Since $[K_n : F_n] \leqslant [K : F]$ and $F_n^u \subset F_{\lfloor u \rfloor}$ by lemma 4.4, the integrand above is bounded independantly of n which proves the theorem. □

In particular, the sequence $\{\mathrm{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n\geqslant 1}$ converges to 0 and therefore given $\delta > 0$, we can find for all $n \gg 0$ a basis $e_1, \ldots, e_d$ of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$ such that $\mathrm{val}_p(e_i^*) \geqslant -\delta$.

Proposition 9.2. — *If L/K is a finite extension, then $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty}) = \mathfrak{m}_{K_\infty}$.*

Proof. — Let $n \gg 0$ be large enough so that the map $\mathrm{Gal}(K_{n+k}/F_{n+k}) \to \mathrm{Gal}(K_n/F_n)$ is an isomorphism for all $k \geqslant 0$. Lemma 4.2 shows that we have $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n}) = \mathfrak{m}_{K_n}^{c_n}$ where $c_n = \lfloor v_{K_n}(\mathfrak{m}_{L_n} \cdot \mathfrak{d}_{L_n/K_n})\rfloor$ and theorem 9.1 implies that the sequence $\{v_{K_n}(\mathfrak{d}_{L_n/K_n})\}_{n\geqslant 1}$ is bounded. This shows that there exists some constant c such that $c_n \leqslant c$ for all $n \gg 0$ and hence that $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n}) \supset \mathfrak{m}_{K_n}^c$ for all $n \gg 0$.

If $x \in \mathfrak{m}_{K_\infty}$ then $x \in \mathfrak{m}_{K_n}^c$ for $n \gg 0$ so that $x \in \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n})$. □

If $n \gg 0$ is large enough, then $[K_n : F_n] = [K_\infty : F_\infty]$ and therefore the natural map $\mathrm{Gal}(K_{n+k}/F_{n+k}) \to \mathrm{Gal}(K_n/F_n)$ is an isomorphism. If $e_1, \ldots, e_d$ is a basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, then it is also a basis of K_{n+k} over F_{n+k} (but not necessarily of $\mathcal{O}_{K_{n+k}}$ over $\mathcal{O}_{F_{n+k}}$). Furthermore if $e_1^*, \ldots, e_d^*$ denotes the dual basis, then $e_i^* \in \mathfrak{d}_{K_n/F_n}^{-1}$ so that if $\delta > 0$ is given and $n \gg 0$ then $\mathrm{val}_p(e_i^*) \geqslant -\delta$.

Proposition 9.3. — *If $\delta > 0$ then if $n \gg 0$ and $x \in \mathcal{O}_{K_{n+1}}$ and $g \in \mathrm{Gal}(K_{n+1}/K_n)$, then*

$$\mathrm{val}_p(g(x) - x) \geqslant \frac{1}{p-1} - \delta.$$

In particular, if $x \in \mathcal{O}_{K_{n+1}}$ then

$$\mathrm{val}_p(\mathrm{N}_{K_{n+1}/K_n}(x) - x^p) \geqslant \frac{1}{p-1} - \delta.$$

Proof. — If $x_i = \mathrm{Tr}_{K_{n+1}/F_{n+1}}(xe_i)$, then $x_i \in \mathcal{O}_{F_{n+1}}$ and $x = \sum_{i=1}^d x_i e_i^*$. Since $\mathcal{O}_{F_{n+1}} = \mathcal{O}_{F_n}[\zeta_{p^{n+1}}]$, we have $\mathrm{val}_p(g(x_i) - x_i) \geqslant 1/(p-1)$, so that the first assertion of the lemma is true if we choose n large enough so that $\mathrm{val}_p(e_i^*) \geqslant -\delta$. The second assertion follows from the first by writing $\mathrm{N}_{K_{n+1}/K_n}(x) = \prod_{g \in \mathrm{Gal}(K_{n+1}/K_n)} g(x)$. □

Corollary 9.4. — *If $\delta > 0$ and if I denotes the ideal of elements x with $\mathrm{val}_p(x) \geqslant 1/(p-1) - \delta$, then the map $x \mapsto x^p : \mathcal{O}_{K_{n+1}}/I \to \mathcal{O}_{K_n}/I$ is surjective if $n \gg 0$.*

Proof. — Let π_{n+1} be a uniformizer of K_{n+1} so that every $x \in \mathcal{O}_{K_{n+1}}$ can be written as $x = \sum_{i \geqslant 0} \pi_{n+1}^i [x_i]$ with $x_i \in k_{K_{n+1}} = k_{K_\infty}$ if $n \gg 0$. We then have $x^p = \sum_{i \geqslant 0} \pi_{n+1}^{pi} [x_i^p]$ mod I and by lemma 9.3, $\mathrm{N}_{K_{n+1}/K_n}(\pi_{n+1}) - \pi_{n+1}^p \in I$ so that $x^p \in \mathcal{O}_{K_n}/I$. The surjectivity of the map then follows from the fact that if $\pi_n = \mathrm{N}_{K_{n+1}/K_n}(\pi_{n+1})$, then π_n is a uniformizer of $\mathcal{O}_{K_n}$ so that if $y \in \mathcal{O}_{K_n}$ then we can write $y = \sum_{i \geqslant 0} \pi_n^i [y_i]$ with $y_i \in k_{K_\infty}$ and y is then the image of $\sum_{i \geqslant 0} \pi_{n+1}^i [y_i^{1/p}]$. □

Exercises

1. Prove that in theorem 9.1, the sequence $\{p^n \mathrm{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n \geqslant 1}$ is eventually constant.
2. Check that if G is a compact group and $f : G \to \mathbf{C}_p$ is a continuous cocyle then there exists $k \in \mathbf{Z}$ such that $f(G) \subset p^k \mathcal{O}_{\mathbf{C}_p}$. Check also that if $\ell \in \mathbf{Z}$ then there is an open subgroup H of G such that $f(H) \subset p^\ell \mathcal{O}_{\mathbf{C}_p}$.
3. Prove that $H^1(G_K, \mathbf{C}_p)$ is generated by the cocyle $g \mapsto \log_p \chi(g)$.

10. Tate's normalized traces

Reference: [**Tat67**]. If $x \in F_\infty$ and $n \geqslant 1$, then $x \in F_{n+k}$ for $k \gg 0$ and $R_n(x) = p^{-k} \mathrm{Tr}_{F_{n+k}/F_n}(x)$ does not depend on $k \gg 0$. This defines a F_n-linear projection $R_n : F_\infty \to F_n$ which commutes with the action of G_F. Note also that $R_n \circ R_m = R_{\min(m,n)}$.

Lemma 10.1. — *If $k \geqslant 0$ and $n \geqslant 1$, then*

$$R_n(\zeta_{p^{n+k}}^j) = \begin{cases} 1 & \text{if } j = 0, \\ 0 & \text{if } 1 \leqslant j \leqslant p^k - 1. \end{cases}$$

Proof. — The formula follows from the fact that $\mathrm{Tr}_{F_{n+k}/F_n}(\zeta_{p^{n+k}}^j) = \zeta_{p^{n+k}}^j \sum_{\eta^{p^k}=1} \eta^j$. □

The above lemma along with the fact that $\mathcal{O}_{F_{n+k}} = \mathcal{O}_{F_n}[\zeta_{p^{n+k}}]$ implies that $R_n(\mathcal{O}_{F_\infty}) \subset \mathcal{O}_{F_n}$ and that $R_n(\pi_n^j \mathcal{O}_{F_\infty}) \subset \pi_n^j \mathcal{O}_{F_n}$ (where $\pi_n = \zeta_{p^n} - 1$ is a uniformizer of F_n) so that we have the following continuity estimate for the R_n's.

Corollary 10.2. — *If $x \in F_\infty$ then $\mathrm{val}_p(R_n(x)) > \mathrm{val}_p(x) - \mathrm{val}_p(\zeta_{p^n} - 1)$.*

In particular, the maps R_n extend by uniform continuity to maps $R_n : \hat{F}_\infty \to F_n$ satisfying the above properties. If $x \in F_\infty$ then $R_n(x) = x$ if $n \gg 0$ so that if $x \in \hat{F}_\infty$ then $R_n(x) \to x$ as $n \to \infty$.

Since $R_n : \hat{F}_\infty \to F_n$ is a continuous projection, we have $\hat{F}_\infty = F_n \oplus X_n$ where $X_n = \ker(R_n)$. Let $\gamma_n \in \Gamma_F$ be a topological generator of Γ_{F_n} (this is equivalent to $\mathrm{val}_p(\chi(\gamma_n) - 1) = n$, so that $\gamma_n^{p^k}$ is then a topological generator of $\Gamma_{F_{n+k}}$).

Proposition 10.3. — *If $\alpha \in \mathbf{Z}_p^\times$ then the map $1 - \alpha\gamma_n : X_n \to X_n$ is invertible and $\mathrm{val}_p((1-\alpha\gamma_n)^{-1}x) \geqslant \mathrm{val}_p(x) - 1/(p-1) - \mathrm{val}_p(\zeta_{p^n} - 1)$.*

Proof. — We first show that the map $1 - \alpha\gamma_n : X_n \to X_n$ is injective. If $\alpha = 1$, this follows from Ax-Sen-Tate's theorem and the fact that $F_n \cap X_n = \{0\}$, so assume that $\alpha \neq 1$. If $x \in X_n$ satisfies the equation $(1-\alpha\gamma_n)x = 0$ then $(1-\alpha\gamma_n)R_{n+k}(x) = 0$ for all $k \geqslant 0$ and this implies that $\alpha^{p^k}\gamma_n^{p^k}(R_{n+k}(x)) = R_{n+k}(x)$ so that $R_{n+k}(x) = 0$ and then $x = \lim R_{n+k}(x) = 0$ (if $p = 2$ and $\alpha = -1$ then this does not work).

We now show that the map is surjective. Let $F_{n+k}^* = \oplus_{j=1,\ p\nmid j}^{p^k-1} F_n \cdot \zeta_{p^{n+k}}^j$ so that $F_{n+k} = F_n \oplus F_{n+1}^* \oplus \cdots \oplus F_{n+k}^*$ and $F_{n+k} \cap X_n = F_{n+1}^* \oplus \cdots \oplus F_{n+k}^*$. If $x = \sum_{j=1,\ p\nmid j}^{p^k-1} x_j \zeta_{p^{n+k}}^j$ with $x_j \in \mathcal{O}_{F_n}$ then

$$x = (1 - \alpha^{p^{k-1}}\gamma_n^{p^{k-1}}) \sum_{j=1}^{p^k-1} x_j \frac{\zeta_{p^{n+k}}^j}{1 - \alpha^{p^{k-1}}\zeta_p^j}.$$

Since $\mathrm{val}_p(1 - \alpha^{p^{k-1}}\zeta_p^j) \leqslant 1/(p-1)$ and

$$\frac{1}{1-\alpha\gamma_n} = \frac{1 - \alpha^{p^{k-1}}\gamma_n^{p^{k-1}}}{1-\alpha\gamma_n} \cdot \frac{1}{1 - \alpha^{p^{k-1}}\gamma_n^{p^{k-1}}},$$

we get that $1 - \alpha\gamma_n : F_{n+k}^* \to F_{n+k}^*$ is invertible and

$$\mathrm{val}_p((1-\alpha\gamma_n)^{-1}x) \geqslant \mathrm{val}_p(x) - 1/(p-1) - \mathrm{val}_p(\zeta_{p^n} - 1)$$

if $x \in F_{n+k}^*$ by corollary 10.2. The proposition follows by uniform continuity. □

Using the results of §9, we now extend the above results to $\hat{K}_\infty$. If $n \gg 0$ is large enough, then $[K_n : F_n] = [K_\infty : F_\infty]$ and therefore the natural map $\mathrm{Gal}(K_{n+k}/F_{n+k}) \to \mathrm{Gal}(K_n/F_n)$ is an isomorphism. If $e_1, \ldots, e_d$ is a basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, then it is also a basis of K_{n+k} over F_{n+k}. Furthermore if $e_1^*, \ldots, e_d^*$ denotes the dual basis, then $e_i^* \in \mathfrak{d}_{K_n/F_n}^{-1}$ so that if $\delta > 0$ is given and $n \gg 0$ then $\mathrm{val}_p(e_i^*) \geqslant -\delta$. If $x \in \mathcal{O}_{K_{n+k}}$ then we can write $x = \sum_{i=1}^d x_i e_i^*$ where $x_i = \mathrm{Tr}_{K_{n+k}/F_{n+k}}(xe_i) \in \mathcal{O}_{F_{n+k}}$. We then define $R_n(x) = \sum_{i=1}^d R_n(x_i)e_i^*$ which defines a projection $R_n : \hat{K}_\infty \to K_n$.

Proposition 10.4. — *If $\varepsilon > 0$ and $n \gg 0$, then the maps $R_n : \hat{K}_\infty \to K_n$ defined above satisfy*

$$\mathrm{val}_p(R_n(x)) \geqslant \mathrm{val}_p(x) - \varepsilon.$$

Proof. — If we write $x = \sum_{i=1}^d x_i e_i^*$ where $x_i = \mathrm{Tr}_{K_{n+k}/F_{n+k}}(xe_i) \in \mathcal{O}_{F_{n+k}}$ then

$$\begin{aligned} \mathrm{val}_p(x_i) &> \mathrm{val}_p(x) - \mathrm{val}_p(\zeta_{p^{n+k}} - 1) \text{ by } F_{n+k}\text{-linearity}, \\ \mathrm{val}_p(R_n(x_i)) &> \mathrm{val}_p(x_i) - \mathrm{val}_p(\zeta_{p^n} - 1) \text{ by corollary 10.2}, \\ \mathrm{val}_p(e_i^*) &\geqslant -\delta \text{ if } \delta > 0 \text{ and } n \gg 0. \end{aligned}$$

The proposition follows from taking $\delta = \varepsilon/3$ and $n \gg 0$ so that $\mathrm{val}_p(\zeta_{p^n} - 1) < \varepsilon/3$. □

Proposition 10.5. — *If $\delta > 0$ and $n \gg 0$ and $\alpha \in \mathbf{Z}_p^\times$, then $1 - \alpha\gamma_n : X_n \to X_n$ is invertible and*

$$\mathrm{val}_p((1-\alpha\gamma_n)^{-1}x) \geqslant \mathrm{val}_p(x) - \frac{1}{p-1} - \delta.$$

Proof. — If $x \in \hat{K}_\infty$ then we can write $x = \sum_{i=1}^d x_i e_i^*$ with $x_i = \mathrm{Tr}_{K_\infty/F_\infty}(xe_i) \in \hat{F}_\infty$ and $x \in X_n$ if and only if $x_i \in \hat{F}_\infty \cap X_n$ for all i. We then have

$$(1-\alpha\gamma_n)x = \sum_{i=1}^d (1-\alpha\gamma_n)x_i \cdot e_i^*$$

from which the invertibility and the estimate follow by using propositions 10.3 and 10.4. □

11. Lubin-Tate groups

Reference: [**LT65**]. In this section, we recall some of the theory of formal groups, and the relationship between Lubin-Tate modules and class field theory. We work over a ring R which is a domain (the theory of formal groups works without this assumption but we do not need this degree of generality).

We start by recalling the definition and basic properties of formal groups and Lubin-Tate modules.

Definition 11.1. — A (1-dimensional) formal group over R is not a group but rather a "formal group law", that is a power series $G(X,Y) \in R[\![X,Y]\!]$ which satisfies the following properties.

1. $G(X,0) = X$ and $G(0,Y) = Y$;
2. $G(X,G(Y,Z)) = G(G(X,Y),Z)$;
3. $G(X,Y) = G(Y,X)$.

For example, one could take $G(X,Y)=X+Y$ (which gives the additive formal group $\mathbf{G}_a$) or $F(X,Y)=X+Y+XY$ (which gives the multiplicative formal group $\mathbf{G}_m$) or also the formal group associated to an elliptic curve. Note that if K is a local field and $R=\mathcal{O}_K$, then $G(X,Y)$ can be used to define a group structure on $\mathfrak{m}_K$ by the formula $x\oplus y=G(x,y)$.

Given a formal group G, there exists a unique $i(X)\in R[\![X]\!]$ such that $G(X,i(X))=0$ and this gives the inverse. Given two formal groups F and G, a homomorphism $h:F\to G$ is a power series $h(X)\in R[\![X]\!]$ such that $h(F(X,Y))=G(h(X),h(Y))$. We say that h is an isomorphism if there exists $h^{-1}(X)\in R[\![X]\!]$ such that $h\circ h^{-1}(X)=X$ and this is the case if and only if $h'(0)$ is a unit of R. If G is a formal group and $m\in\mathbf{Z}$, then we have "multiplication by m" maps $[m]:G\to G$ defined by $[0](X)=0$ and $[m+1](X)=G([m]X,X)$ and $[m-1](X)=G([m]X,i(X))$. We have $[m]'(0)=m$.

A differential form on G is $\omega(X)=D(X)dX$ where $D(X)\in R[\![X]\!]$. Given a power series $A(X,Y)\in R[\![X,Y]\!]$ in which we consider Y to be a "constant", we have $\omega(A(X,Y))=D(A(X,Y))A_X(X,Y)dX$ where $A_X(X,Y)=dA/dX$. We say that ω is invariant if $\omega(G(X,Y))=\omega(X)$. This implies that $D(Y)=D(0)/G_X(0,Y)$ so that an invariant differential form is determined by $D(0)$. We say that ω is normalized if $D(0)=1$. There exists a unique normalized invariant differential form which we denote by ω_F. If $h:F\to G$ is a homomorphism between two formal groups, then $\omega_G\circ h=h'(0)\omega_F$.

Suppose that $\mathbf{Q}\subset R$. If $\omega(X)$ is a differential form, denote by $I_\omega(X)$ the unique power series such that $dI_\omega(X)=\omega(X)$ and $I_\omega(0)=0$. The logarithm of the formal group is the power series $\log_G(X)=I_{\omega_G}(X)$. We then have $\log_G(G(X,Y))=X+Y$ so that $\log_G$ gives rise to an isomorphism from G to the additive formal group $\mathbf{G}_a$. For example, if $G=\mathbf{G}_m$, then $\log_{\mathbf{G}_m}(X)=\log(1+X)$. If R does not contain $\mathbf{Q}$, there is of course no such isomorphism in general.

We now define Lubin-Tate modules for finite extensions of $\mathbf{Q}_p$. Let K be a finite extension of $\mathbf{Q}_p$ and let $R=\mathcal{O}_K$. We let q denote the cardinal of k_K.

Definition 11.2. — A formal $\mathcal{O}_K$-module G is a formal group G over $\mathcal{O}_K$ together with a ring homomorphism $\mathcal{O}_K\to\mathrm{End}_{\mathcal{O}_K}(G)$ denoted by $a\mapsto[a]$ such that $[a](X)=aX+\mathrm{O}(X^2)$ if $a\in\mathcal{O}_K$.

Now choose a uniformizer π_K of K

Definition 11.3. — A Lubin-Tate module G over $\mathcal{O}_K$ for π_K is a formal $\mathcal{O}_K$-module G such that $[\pi_K](X)=X^q \bmod \pi_K$.

For example if $K = \mathbf{Q}_p$, then the group $\mathbf{G}_m$ is a Lubin-Tate module over $\mathbf{Z}_p$ for the uniformizer p, with $[a](X) = (1+X)^a - 1 = \sum_{k \geqslant 0} \binom{a}{k} X^k$.

A power series $\varphi(X) \in \mathcal{O}_K[\![X]\!]$ such that $\varphi(X) = \pi_K X + \mathrm{O}(X^2)$ and $\varphi(X) = X^q \bmod \pi_K$ is called a Lubin-Tate power series. A usual (but by no means canonical) choice for a Lubin-Tate power series is $\varphi(X) = \pi_K X + X^q$.

Theorem 11.4. — *If $\varphi(X) \in \mathcal{O}_K[\![X]\!]$ is a Lubin-Tate power series, then there exists a Lubin-Tate module G_φ over $\mathcal{O}_K$ for π_K such that $[\pi_K](X) = \varphi(X)$.*

If $\varphi(X)$ and $\psi(X)$ are two Lubin-Tate power series, then G_φ and G_ψ are isomorphic as formal $\mathcal{O}_K$-modules.

Note however that two Lubin-Tate modules over $\mathcal{O}_K$ for two different uniformizers are never isomorphic over $\mathcal{O}_K$.

Let K be a finite extension of $\mathbf{Q}_p$ as before, let π_K be a uniformizer of K and let $\varphi(X)$ be some Lubin-Tate power series. Theorem 11.4 gives us a Lubin-Tate module G over $\mathcal{O}_K$ whose isomorphism class only depends on π_K. This formal group can be used to define an $\mathcal{O}_K$-module structure on $\mathfrak{m}_{\mathbf{C}_p}$ which then becomes some twisted open unit disk. We denote by $G[\pi_K^n]$ the set of $\alpha \in \mathfrak{m}_{\mathbf{C}_p}$ such that $[\pi_K^n](\alpha) = 0$ and the Tate module TG of the Lubin-Tate module G (!) is defined by

$$TG = \varprojlim_n G[\pi_K^n] = \{(\alpha_0, \alpha_1, \ldots) \text{ where } \alpha_0 = 0,\ \alpha_n \in \mathfrak{m}_{\mathbf{C}_p} \text{ and } [\pi_K](\alpha_{n+1}) = \alpha_n\}.$$

This makes TG into an $\mathcal{O}_K$-module with an action of G_K. One could also define $T_pG = \varprojlim_n G[p^n]$ and it's a simple exercise to show that TG and T_pG are naturally isomorphic. Note also that if G_1 and G_2 are isomorphic as Lubin-Tate modules over $\mathcal{O}_K$, then TG_1 and TG_2 are isomorphic.

If $K = \mathbf{Q}_p$ and $G = \mathbf{G}_m$, then $\mathbf{G}_m[p^n] = \{\zeta - 1 \text{ where } \zeta^{p^n} = 1\}$.

Proposition 11.5. — *The module TG is a free $\mathcal{O}_K$-module of rank 1 and if $\alpha \in \mathcal{O}_K$, then $TG/\alpha = G[\alpha]$.*

By proposition 11.5, the group of $\mathcal{O}_K$-linear automorphisms of TG is isomorphic to $\mathcal{O}_K^\times$ and since G_K acts on TG, we get a character $\chi_K : G_K \to \mathcal{O}_K^\times$ which is determined by $g(\alpha_n) = [\chi_K(g)](\alpha_n)$. This character depends on the choice of π_K. For example, if $K = \mathbf{Q}_p$ and $\pi_K = p$, then χ_K is the cyclotomic character.

Let $\alpha = (\alpha_0, \alpha_1, \ldots)$ denote a generator of TG and let $K_n = K(\alpha_n)$ and $K_\infty = \cup_{n \geqslant 1} K_n$.

Theorem 11.6. — *The field K_n depends only on π_K, and furthermore:*

1. *K_n/K is totally ramified of degree $q^{n-1}(q-1)$ and α_n is a uniformizer of K_n;*

2. $\mathrm{Gal}(K_\infty/K_n) = 1 + \pi_K^n \mathcal{O}_K$ *(for $n = 0$, we get $\mathrm{Gal}(K_\infty/K) = \mathcal{O}_K^\times$);*
3. $K_\infty \cdot K^{\mathrm{unr}}$ *is the maximal abelian extension of K.*

The group $\mathrm{Gal}(K_\infty/K)$ is endowed with the upper ramification filtration while $\mathcal{O}_K^\times$ is filtered by the subgroups $1 + \pi_K^n \mathcal{O}_K$.

Proposition 11.7. — *The isomorphism $\mathrm{Gal}(K_\infty/K) = \mathcal{O}_K^\times$ respects the filtrations.*

Corollary 11.8. — *If L/K is an abelian galois extension, then the jumps of the upper ramification filtration on $\mathrm{Gal}(L/K)$ are integers.*

Exercises

1. Show that if a power series satisfies (1) and (2) of definition 11.1, then it satisfies (3).
2. Show that the conclusion of exercise 1 can fail if R is not a domain, for example by taking $R = \mathbf{F}_p[\epsilon]/\epsilon^2$ and $F(X, Y) = X + Y + \epsilon XY^p$.
3. Show that if p is prime, then $[p](X) \in pR[\![X]\!] + R[\![X^p]\!]$.

12. Periods of Lubin-Tate groups

Reference: [**Fou09**]. Later on we'll study the map $H^1(G_K, \mathbf{Q}_p) \to H^1(G_K, \mathbf{C}_p)$. The elements of $H^1(G_K, \mathbf{Q}_p)$ are just group homomorphisms $G_K \to \mathbf{Q}_p$ and they can be written as K-linear combinations of unramified maps and of the maps $g \mapsto \log \sigma \circ \chi_K(g)$ where σ runs over all embeddings $K \to \overline{\mathbf{Q}}_p$. The following theorem is then the main result of this §, and by taking $\alpha_\sigma = \log(\beta_\sigma)$, it implies that if $\sigma \neq \mathrm{Id}$, then there exists an element $\beta_\sigma \in \mathbf{C}_p$ such that we have $\log \sigma \circ \chi_K(g) = g(\beta_\sigma) - \beta_\sigma$.

Theorem 12.1. — *If $\sigma \neq \mathrm{Id}$, then there exists an element $\alpha_\sigma \in \mathbf{C}_p^\times$ such that we have $\sigma \circ \chi_K(g) = g(\alpha_\sigma)/\alpha_\sigma$.*

Later on we'll show that if $\sigma = \mathrm{Id}$, then there is no such element. The proof of theorem 12.1 requires a few preliminary results. Let K be a finite extension of $\mathbf{Q}_p$, with uniformizer π_K and index of ramification e_K and let G be a Lubin-Tate module over $\mathcal{O}_K$ for π_K. It makes things a bit easier to take $[\pi_K](X) = \pi_K X + X^q$ but this is not necessary. If $\sigma \in \mathrm{Hom}(K, \overline{\mathbf{Q}}_p)$, then let $q_\sigma = p^{n(\sigma)}$ be the integer $0 \leqslant q_\sigma \leqslant q-1$ such that $\overline{\sigma} : k_K \to \overline{\mathbf{F}}_p$ is given by $x \mapsto x^{q_\sigma}$. If $A(X) = \sum_{n \geqslant 0} a_n X^n \in K[\![X]\!]$ is a power series, then we write $A^\sigma(X)$ for $\sum_{n \geqslant 0} \sigma(a_n) X^n \in \sigma(K)[\![X]\!]$.

Lemma 12.2. — *If $x, y \in \mathfrak{m}_{\mathbf{C}_p}$ satisfy $x = y \bmod \pi_K^n$ and $\sigma \in \mathrm{Hom}(K, \overline{\mathbf{Q}}_p)$, then $[\pi_K]^\sigma(x) = [\pi_K]^\sigma(y) \bmod \pi_K^{n+1}$.*

Let $\eta = (\eta_0, \eta_1, \ldots) \in TG$ be a generator of the rank 1 $\mathcal{O}_K$-module TG. We have $[\pi_K]^\sigma(\eta_{n+1}^{q_\sigma}) = \eta_n^{q_\sigma} \bmod \pi_K$ and therefore, lemma 12.2 applied repeatedly implies that $[\pi_K^{n+1}]^\sigma(\eta_{n+1}^{q_\sigma}) = [\pi_K^n]^\sigma(\eta_n^{q_\sigma}) \bmod \pi_K^{n+1}$. This shows that the sequence $\{[\pi_K^n]^\sigma(\eta_n^{q_\sigma})\}_{n\geqslant 0}$ converges in $\mathfrak{m}_{\mathbf{C}_p}$ to an element μ_σ.

If $g \in G_K$, then $g(\eta_n) = [\chi_K(g)](\eta_n)$ and by raising this to the q_σ-th power, we get $g(\eta_n^{q_\sigma}) = [\chi_K(g)]^\sigma(\eta_n^{q_\sigma}) \bmod \pi_K$. Applying lemma 12.2 repeatedly gives us $g(\mu_\sigma) = [\chi_K(g)]^\sigma(\mu_\sigma)$.

Lemma 12.3. — *We have:*

$$\mathrm{val}_p(\mu_\sigma) = \begin{cases} \frac{q_\sigma}{e_K(q-1)} + \frac{1}{e_K} & \text{if } n(\sigma) \neq 0, \\ \frac{1}{e_K(q-1)} + \mathrm{val}_p(\sigma(\pi_K) - \pi_K) & \text{if } n(\sigma) = 0. \end{cases}$$

Proof of theorem 12.1. — If we put $\alpha_\sigma = \log_G^\sigma(\mu_\sigma)$, then $g(\alpha_\sigma) = \sigma \circ \chi_K(g) \cdot \alpha_\sigma$. Lemma 12.3 and an examination of the Newton polygon of $\log_G(X)$ implies that we have :

$$\mathrm{val}_p(\alpha_\sigma) = \begin{cases} \frac{q_\sigma}{e_K(q-1)} + \frac{1}{e_K} & \text{if } n(\sigma) \neq 0, \\ \frac{1}{e_K(q-1)} + \mathrm{val}_p(\sigma(\pi_K) - \pi_K) & \text{if } n(\sigma) = 0. \end{cases}$$

This implies that $\alpha_\sigma \neq 0$ if $\sigma \neq \mathrm{Id}$ and this finishes the proof. □

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

References: [**Tat67**], [**Sen73**] and [**Sen81**]. We now apply the results of §9 and §10 to the computation of $H^0(G_K, \mathbf{C}_p(\psi))$ and $H^1(G_K, \mathbf{C}_p(\psi))$ where $\psi : G_K \to \mathbf{Z}_p^\times$ is a continuous character which is trivial on H_K so that ψ is a character of Γ_K. We start with $H^0(G_K, \mathbf{C}_p(\psi))$; note that if ψ is of finite order, then by theorem 7.2 (Hilbert's theorem 90, see exercise 3 of chapter 7) we have $\mathbf{C}_p(\psi) = \mathbf{C}_p$ so that $H^0(G_K, \mathbf{C}_p(\psi)) = K$ by theorem 5.3 (the Ax-Sen-Tate theorem).

Theorem 13.1. — *If $\psi : \Gamma_K \to \mathbf{Z}_p^\times$ is of infinite order, then $H^0(G_K, \mathbf{C}_p(\psi)) = \{0\}$.*

Proof. — First of all, $H^0(G_K, \mathbf{C}_p(\psi)) \subset \hat{K}_\infty(\psi)$ by theorem 5.3 (the Ax-Sen-Tate theorem) so we need to prove that if $x \in \hat{K}_\infty$ is such that $g(x) = \psi^{-1}(g)x$ then $x = 0$. Since the maps R_n of §10 commute with the action of G_K we also have $g(R_n(x)) = \psi^{-1}(g)R_n(x)$ and since ψ has infinite order, $K_n(\psi)^{G_K} = \{0\}$ so that $R_n(x) = 0$ for all n. Since $R_n(x) \to x$ as $n \to \infty$, we have $x = 0$. □

We now compute $H^1(G_K, \mathbf{C}_p(\psi))$. Theorem 7.1 (the inflation-restriction sequence) gives us an exact sequence

$$0 \to H^1(\Gamma_K, \mathbf{C}_p(\psi)^{H_K}) \to H^1(G_K, \mathbf{C}_p(\psi)) \to H^1(H_K, \mathbf{C}_p(\psi)),$$

and we first prove that $H^1(H_K, \mathbf{C}_p(\psi)) = \{0\}$.

Lemma 13.2. — *If $f : H_K \to p^n\mathcal{O}_{\mathbf{C}_p}$ is a continuous cocycle, then there exists $x \in p^{n-1}\mathcal{O}_{\mathbf{C}_p}$ such that the cohomologous cocyle $g \mapsto f(g) - (x - g(x))$ has values in $p^{n+1}\mathcal{O}_{\mathbf{C}_p}$.*

Proof. — Let L/K be a finite extension such that $f(H_L) \subset p^{n+2}\mathcal{O}_{\mathbf{C}_p}$. Lemma 9.2 gives us $y \in p^{-1}\mathcal{O}_{L_\infty}$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(y) = 1$. Let Q be a set of representatives of H_K/H_L and let $x_Q = \sum_{h\in Q} h(y)f(h)$ so that if $g \in H_K$ then $g(x_Q) = x_{g(Q)} - f(g)$ and hence $f(g) - (x_Q - g(x_Q)) = x_{g(Q)} - x_Q$. The cocyle relation and the choice of L tells us that $x_{g(Q)} - x_Q \in p^{n+1}\mathcal{O}_{\mathbf{C}_p}$ so that we can take $x = x_Q$. □

Corollary 13.3. — *We have $H^1(H_K, \mathbf{C}_p(\psi)) = \{0\}$.*

Proof. — Since ψ is trivial on H_K we have $H^1(H_K, \mathbf{C}_p(\psi)) = H^1(H_K, \mathbf{C}_p)(\psi)$ and it is enough to show that $H^1(H_K, \mathbf{C}_p) = \{0\}$. Let $f : H_K \to \mathbf{C}_p$ be a cocycle, and let $k \in \mathbf{Z}$ be such that $f(H_K) \subset p^k\mathcal{O}_{\mathbf{C}_p}$. Set $f_0 = f$ so that $f_j(H_K) \subset p^{k+j}\mathcal{O}_{\mathbf{C}_p}$ for $j = 0$. If $j \geqslant 0$, lemma 13.2 gives us $x_j \in p^{k+j-1}\mathcal{O}_{\mathbf{C}_p}$ such that if we set $f_{j+1}(g) = f_j(g) - (x_j - g(x_j))$, then $f_{j+1}(H_K) \subset p^{k+j+1}\mathcal{O}_{\mathbf{C}_p}$. We then have $f(g) = \sum_{j\geqslant 0} x_j - g(\sum_{j\geqslant 0} x_j)$. □

Theorem 13.4. — *We have $H^1(G_K, \mathbf{C}_p(\psi)) = \{0\}$ if ψ is of infinite order and $H^1(G_K, \mathbf{C}_p(\psi))$ is a K-vector space of dimension 1 if ψ is of finite order.*

Proof. — By the inflation-restriction sequence

$$0 \to H^1(\Gamma_K, \mathbf{C}_p(\psi)^{H_K}) \to H^1(G_K, \mathbf{C}_p(\psi)) \to H^1(H_K, \mathbf{C}_p(\psi))$$

recalled above, the fact that $\mathbf{C}_p(\psi)^{H_K} = \hat{K}_\infty(\psi)$ and the fact that $H^1(H_K, \mathbf{C}_p(\psi)) = \{0\}$ by corollary 13.3, the natural map $H^1(\Gamma_K, \hat{K}_\infty(\psi)) \to H^1(G_K, \mathbf{C}_p(\psi))$ is an isomorphism. Let γ be a topological generator of Γ_K (if $p = 2$ and $\Gamma_K \simeq \mathbf{Z}_2^\times$, the proof needs to be modifed slightly) so that $H^1(\Gamma_K, \hat{K}_\infty(\psi)) = \hat{K}_\infty(\psi)/1 - \gamma$.

If $n \gg 0$, we have a decomposition $\hat{K}_\infty(\psi) = K_n(\psi) \oplus X_n(\psi)$ and by proposition 10.5, the operator $1 - \gamma_n : X_n(\psi) \to X_n(\psi)$ is invertible. Since $1 - \gamma_n/1 - \gamma \in \mathbf{Z}_p[[\Gamma_K]]$, the operator $1-\gamma : X_n(\psi) \to X_n(\psi)$ is also invertible so that $\hat{K}_\infty(\psi)/1-\gamma = K_n(\psi)/1-\gamma$. If ψ is of infinite order, then $1-\gamma : K_n(\psi) \to K_n(\psi)$ is injective so that $K_n(\psi)/1-\gamma = \{0\}$ and we are done. If ψ is of finite order, then $K_n(\psi) = K_n$ by Hilbert's theorem 90 and $K_n(\psi)/1 - \gamma$ is then a 1-dimensional K-vector space. □

Proposition 13.5. — *The 1-dimensional K-vector space $H^1(G_K, \mathbf{C}_p)$ is generated by the cocyle $[g \mapsto \log_p \chi(g)]$.*

Proof. — The proof of theorem 13.4 and exercise 6 from chapter 7 show that the inflation map $H^1(\Gamma_K, K_n) \to H^1(G_K, \mathbf{C}_p)$ is an isomorphism so that if γ is a topological generator of Γ_K, then the map $K/(1-\gamma) \to H^1(G_K, \mathbf{C}_p)$ given by $\alpha \mapsto [g \mapsto (\overline{g}-1)/(\gamma-1)\alpha]$ is an isomorphism. The proposition follows from the fact that if $\overline{g} = \gamma^k$ with $k \in \mathbf{Z}$, then $(\overline{g}-1)/(\gamma-1)\alpha = k\alpha$ so that the above cocyle is given by a multiple of $g \mapsto \log_p \chi(g)$. □

We now give an explicit formula for the map $H^1(G_K, \mathbf{Q}_p) \to H^1(G_K, \mathbf{C}_p)$. In §11, we constructed a map $\chi_K : G_K \to \mathcal{O}_K^\times$ whose restriction to I_K does not depend on the choice of a uniformizer π_K and is an isomorphism from $I(K^{\mathrm{ab}}/K) \to \mathcal{O}_K^\times$. If $f \in \mathrm{Hom}(\mathcal{O}_K^\times, \mathbf{Q}_p)$, then there exists a well-defined $\beta_f \in K$ such that $f(y) = \mathrm{Tr}_{K/\mathbf{Q}_p}(\beta_f \cdot \log_p(y))$ and therefore we get a map $H^1(G_K, \mathbf{Q}_p) \to K$ which we still denote by $f \mapsto \beta_f$.

Proposition 13.6. — *The map $H^1(G_K, \mathbf{Q}_p) \to H^1(G_K, \mathbf{C}_p)$ is given by*

$$f \mapsto \beta_f \cdot [g \mapsto \log_p \chi(g)].$$

Proof. — If $f \in H^1(G_K, \mathbf{Q}_p)$, then by the above discussion we can write $f(g) = \mathrm{Tr}_{K/\mathbf{Q}_p}(\beta_f \cdot \log_p \chi_K(g)) + c(g)$ where $c(g)$ is an unramified map. By proposition 7.4, there exists $z \in \hat{\mathbf{Q}}_p^{\mathrm{nr}}$ such that $c(g) = g(z) - z$. We have

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}_p}(\beta_f \cdot \log_p \chi_K(g)) &= \sum_{\sigma : K \to \overline{\mathbf{Q}}_p} \sigma(\beta_f \cdot \log_p \chi_K(g)) \\ &= \beta_f \cdot \mathrm{Tr}_{K/\mathbf{Q}_p}(\log_p \chi_K(g)) + \sum_{\sigma : K \to \overline{\mathbf{Q}}_p} (\sigma(\beta_f) - \beta_f) \cdot \sigma(\log_p \chi_K(g)).\end{aligned}$$

For each $\sigma \neq \mathrm{Id}$, theorem 12.1 gives us $\alpha_\sigma \in \mathbf{C}_p$ such that $\sigma(\log_p \chi_K(g)) = g(\alpha_\sigma) - \alpha_\sigma$. Class field theory tells us that $\mathrm{Tr}_{K/\mathbf{Q}_p}(\log_p \chi_K(g)) = \log_p \chi(g)$ and therefore, if we set $y = z + \sum_{\sigma : K \to \overline{\mathbf{Q}}_p} (\sigma(\beta_f) - \beta_f) y_\sigma$, then $f(g) = \beta_f \cdot \log_p \chi(g) + (gy - y)$ which proves the proposition. □

Corollary 13.7. — *If $\eta : G_K \to \mathbf{Z}_p^\times$ is a character and if there exists $y \in \mathbf{C}_p^\times$ such that $\eta(g) = g(y)/y$, then there exists a finite extension L of K such that $\eta|_L$ is unramified.*

Proof. — Let $f \in H^1(G_K, \mathbf{Q}_p)$ be defined by $f(g) = \log_p \eta(g)$. We have $f(g) = g(\log_p y) - \log_p y$ so that the image of $f \in H^1(G_K, \mathbf{C}_p)$ is trivial and proposition 13.6 implies that $\log_p \eta$ is trivial on $I(K^{\mathrm{ab}}/K)$ which proves the corollary. □

The same proof shows that if $\rho : G_K \to \mathrm{GL}_d(\mathbf{Q}_p)$ is an abelian representation such that $\rho(g) = g(M)M^{-1}$ for some $M \in \mathrm{GL}_d(\mathbf{C}_p)$, then ρ is potentially unramified. This is a special case the following theorem of Sen.

Theorem 13.8. — *If $\rho : G_K \to \mathrm{GL}_d(\mathbf{Q}_p)$ is such that $\rho(g) = g(M)M^{-1}$ for some $M \in \mathrm{GL}_d(\mathbf{C}_p)$, then ρ is potentially unramified.*

The proof of this theorem in the general non-abelian case is quite complicated, and not given in this course.

14. The field $\widetilde{\mathbf{E}}$ and its subrings

References: [**Fon90**] and [**Fon94a**]. The first ring which we define is $\widetilde{\mathbf{E}}^+ = \{(x_0, x_1, \ldots)$ where $x_i \in \mathcal{O}_{\mathbf{C}_p}/I$ and $x_{i+1}^p = x_i\}$, addition and multiplication being componentwise. We denote by θ_i the map $x \mapsto x_i$ so that $\theta_i(x) = \theta_{i+1}(x)^p$. If $x \in \widetilde{\mathbf{E}}^+$, then for each i choose a lift $\hat{x}_i \in \mathcal{O}_{\mathbf{C}_p}$ of x_i. The sequence $\hat{x}_{i+j}^{p^j}$ then converges as $j \to +\infty$ to some $x^{(i)} \in \mathcal{O}_{\mathbf{C}_p}$ which only depends on x. The natural multiplicative map $\varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbf{C}_p} \to \widetilde{\mathbf{E}}^+$ is therefore a bijection. We use either description of $\widetilde{\mathbf{E}}^+$ in the sequel. If $x \in \widetilde{\mathbf{E}}^+$, we define $\mathrm{val}_{\mathbf{E}}(x) = \mathrm{val}_p(x^{(0)})$. The ring $\widetilde{\mathbf{E}}^+$ is a perfect ring of characteristic p, and the function $\mathrm{val}_{\mathbf{E}} : \widetilde{\mathbf{E}}^+ \setminus \{0\}$ is a valuation for which it is complete. Note that $\overline{\mathbf{F}}_p$ maps into $\widetilde{\mathbf{E}}^+$ by $\alpha \mapsto ([\alpha^{1/p^n}])_{n \geqslant 0}$ and that the residue field of $\widetilde{\mathbf{E}}^+$ is $\overline{\mathbf{F}}_p$.

Lemma 14.1. — *If $P \subset Q$ are two subsets of $\widetilde{\mathbf{E}}^+$ then P is dense in Q if and only if $\theta_n(P) = \theta_n(Q)$ for all $n \geqslant 0$.*

Proof. — Note that if $x \in \widetilde{\mathbf{E}}^+$ then $\theta_n(x) = 0$ if and only if $\mathrm{val}_{\mathbf{E}}(x) \geqslant p^{n+1}\mathrm{val}_p(I)$. If $\theta_n(P) = \theta_n(Q)$ for all $n \geqslant 0$, then given $y \in Q$ this implies that for any $M > 0$ there exists $x \in P$ with $\mathrm{val}_{\mathbf{E}}(x - y) \geqslant M$ and hence that P is dense in Q. The reverse implication is similar. □

Let $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in \widetilde{\mathbf{E}}^+$ and $\pi = \varepsilon - 1$ so that $\mathrm{val}_{\mathbf{E}}(\pi) = p/(p-1)$. We define $\widetilde{\mathbf{E}} = \widetilde{\mathbf{E}}^+[1/\pi]$ so that $\widetilde{\mathbf{E}}$ is a perfect field of characteristic p, which contains $\mathbf{F}_p(\!(\pi)\!)$. We denote by φ the map $x \mapsto x^p$ on $\widetilde{\mathbf{E}}$. The group $G_{\mathbf{Q}_p}$ acts on $\mathbf{C}_p$ and this gives a continuous action of $G_{\mathbf{Q}_p}$ on $\widetilde{\mathbf{E}}$.

Theorem 14.2. — *The field $\widetilde{\mathbf{E}}$ is algebraically closed.*

Proof. — It is enough to prove that every monic polynomial $P(T) \in \widetilde{\mathbf{E}}^+[T]$ has a root in $\widetilde{\mathbf{E}}$, and we do this by induction on the degree of $P(T)$. Let $P_n(T)$ denote $\theta_n(P) \in (\mathcal{O}_{\mathbf{C}_p}/I)[T]$ and for each n, choose some monic lift $\tilde{P}_n(T) \in \mathcal{O}_{\mathbf{C}_p}[T]$ of P_n. Since $\mathbf{C}_p$ is algebraically closed, the polynomial $\tilde{P}_n(T)$ has a root $\tilde{\alpha}_{n,n} \in \mathcal{O}_{\mathbf{C}_p}$. Let $\alpha_n \in \widetilde{\mathbf{E}}$ be an Element such that $\alpha_{n,n} \in \mathcal{O}_{\mathbf{C}_p}/I$ is the image of $\tilde{\alpha}_{n,n} \in \mathcal{O}_{\mathbf{C}_p}$. We then have $P(\alpha_n) \to 0$ as $n \to \infty$. If $P'(\alpha_n)$ does not converge to 0, then theorem 2.2 (Hensel's lemma) tells

us that for $n \gg 0$, $P(T)$ has a root close to some α_n and we are done. If $P'(\alpha_n) \to 0$, then by induction $P'(T)$ has $d-1$ roots in $\widetilde{\mathbf{E}}$ and $\{\alpha_n\}_{n\geqslant 0}$ then converges to one of them, which is then also a root of $P(T)$. □

15. The action of Galois on $\widetilde{\mathbf{E}}$

References: [**Fon90**] and [**Fon94a**]. Let L be a finite extension of $\mathbf{Q}_p$ and recall that $H_L = \ker(\chi : G_L \to \mathbf{Z}_p^\times) = \mathrm{Gal}(\overline{\mathbf{Q}}_p/L_\infty)$. Let $\widetilde{\mathbf{E}}_L^+$ be the set of $x \in \widetilde{\mathbf{E}}^+$ such that $x_i \in \mathcal{O}_{L_\infty}/I$ for all $i \geqslant 0$ and let $\widetilde{\mathbf{E}}_L = \widetilde{\mathbf{E}}_L^+[1/\pi]$ so that $\widetilde{\mathbf{E}}_L$ is a perfect field. Note that corollary 9.4 implies that the map $x \mapsto x^p : \mathcal{O}_{L_\infty}/I \to \mathcal{O}_{L_\infty}/I$ is surjective so that $\theta_n : \widetilde{\mathbf{E}}_L^+ \to \mathcal{O}_{L_\infty}/I$ is surjective for all $n \geqslant 0$.

Lemma 15.1. — *We have* $\widetilde{\mathbf{E}}_L = \widetilde{\mathbf{E}}^{H_L}$.

Proof. — The fact that $\widetilde{\mathbf{E}}_L \subset \widetilde{\mathbf{E}}^{H_L}$ is immediate; conversely, if $x \in (\widetilde{\mathbf{E}}^+)^{H_L}$ then $x^{(j)} \in \mathcal{O}_{\mathbf{C}_p}^{H_L} = \hat{\mathcal{O}}_{L_\infty}$ by theorem 5.3 (the theorem of Ax-Sen-Tate) so that $x_j \in \mathcal{O}_{L_\infty}/I$ and $x \in \widetilde{\mathbf{E}}_L^+$. □

Proposition 15.2. — *If K is a finite extension of $\mathbf{Q}_p$ then :*

1. $\widetilde{\mathbf{E}}_K^{\mathrm{alg}} = \cup_{L/K}\widetilde{\mathbf{E}}_L$;
2. $\widetilde{\mathbf{E}}_K^{\mathrm{alg}}$ *is dense in* $\widetilde{\mathbf{E}}$;
3. $\mathrm{Gal}(\widetilde{\mathbf{E}}_K^{\mathrm{alg}}/\widetilde{\mathbf{E}}_K) = H_K$.

Proof. — If L/K is finite, then lemma 15.1 implies that $\widetilde{\mathbf{E}}_K = \widetilde{\mathbf{E}}_L^{\mathrm{Gal}(L_\infty/K_\infty)}$ so that $\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K$ is a finite Galois extension by Artin's lemma. Conversely, if $\mathbf{F} \subset \widetilde{\mathbf{E}}$ is some finite extension of $\widetilde{\mathbf{E}}_K$ then it is generated by finitely many elements having finitely many conjugates. The group H_K acts on those elements and some open subgroup of finite index fixes all of them, so that there exists L/K finite such that $\mathbf{F} \subset \widetilde{\mathbf{E}}_L$. This and the fact that $\widetilde{\mathbf{E}}$ is algebraically closed (theorem 14.2) prove item (1).

The fact that the map $x \mapsto x^p : \mathcal{O}_{L_\infty}/I \to \mathcal{O}_{L_\infty}/I$ is surjective implies that $\theta_n(\widetilde{\mathbf{E}}_L^+) = \mathcal{O}_{L_\infty}/I$ and then item (1) implies that $\theta_n(\widetilde{\mathbf{E}}_K^{\mathrm{alg},+}) = \cup_{L/K}\mathcal{O}_{L_\infty}/I = \mathcal{O}_{\mathbf{C}_p}/I$ for all $n \geqslant 0$ so that by lemma 14.1, $\widetilde{\mathbf{E}}_K^{\mathrm{alg},+}$ is dense in $\widetilde{\mathbf{E}}^+$ and this implies item (2).

Finally, the fact that $\widetilde{\mathbf{E}}_K = \widetilde{\mathbf{E}}_L^{\mathrm{Gal}(L_\infty/K_\infty)}$ implies that $\mathrm{Gal}(\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K) = \mathrm{Gal}(L_\infty/K_\infty)$ by Artin's lemma and item (3) follows from this and item (1). □

Now let $\mathbf{E}_{\mathbf{Q}_p} = \mathbf{F}_p(\!(\pi)\!)$ which is a subfield of $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ since $H_{\mathbf{Q}_p}$ fixes π. We also define $\mathbf{E} = \mathbf{E}_{\mathbf{Q}_p}^{\mathrm{sep}} \subset \widetilde{\mathbf{E}}$. The group $H_{\mathbf{Q}_p}$ acts on $\mathbf{E}$ and therefore we have a map $H_{\mathbf{Q}_p} \to \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$.

Lemma 15.3. — *The field* $\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{rad}}$ *is dense in* $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$.

Proof. — By lemma 14.1, it is enough to prove that $\theta_n(\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{rad},+}) = \mathcal{O}_{F_\infty}/I$ for all $n \geqslant 0$. Note that $\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{rad},+}$ contains $\mathbf{F}_p$ and $\varepsilon^{p^{-k+n}}$ for all $k \geqslant 0$ and since $\mathcal{O}_{F_\infty} = \mathbf{Z}_p[(\zeta_{p^k})_{k\geqslant 0}]$ and $\theta_n(\varepsilon^{p^{-k+n}}) = \zeta_{p^k}$ we are done. □

Theorem 15.4. — *The map $H_{\mathbf{Q}_p} \to \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$ is an isomorphism.*

Proof. — Lemma 15.3 implies that $\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{alg}}$ is dense in $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^{\mathrm{alg}}$ and the fact that $\mathbf{E} = \mathbf{E}_{\mathbf{Q}_p}^{\mathrm{sep}}$ is dense in $\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{alg}}$ by theorem 5.2 (Ax's theorem) along with item (2) of proposition 15.2 imply finally that $\mathbf{E} = \mathbf{E}_{\mathbf{Q}_p}^{\mathrm{sep}}$ is dense in $\widetilde{\mathbf{E}}$.

The map $H_{\mathbf{Q}_p} \to \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$ is therefore injective, since if $h \in H_{\mathbf{Q}_p}$ acts trivially on $\mathbf{E}$ then it acts trivially on $\widetilde{\mathbf{E}}$ by continuity and by items (2) and (3) of proposition 15.2 above, this implies that $h = 1$. Finally, if $h \in \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$, then h extends by continuity to a map on $\widetilde{\mathbf{E}}$ trivial on $\mathbf{E}_{\mathbf{Q}_p}^{\mathrm{rad}}$ and so on $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ which therefore comes from an element of $H_{\mathbf{Q}_p}$ again by items (2) and (3) of proposition 15.2. □

Theorem 15.5. — *If K is a finite extension of $\mathbf{Q}_p$ then $H^1(H_K, \mathbf{E}) = \{0\}$ and if $d \geqslant 1$ then $H^1(H_K, \mathrm{GL}_d(\mathbf{E})) = \{1\}$ (here the cocycles are continuous for the discrete topology).*

Proof. — This follows from theorem 15.4 above and corollary 7.3 (Hilbert's theorem 90 for infinite extensions). □

If K is a finite extension of $\mathbf{Q}_p$, we then set $\mathbf{E}_K = \mathbf{E}^{H_K}$ and this is a finite extension of $\mathbf{E}_{\mathbf{Q}_p}$ on which the quotient group Γ_K acts. For example, if $K = \mathbf{Q}_p$ and $\gamma \in \Gamma_K$ then $\gamma(f(\pi)) = f((1+\pi)^{\chi(\gamma)} - 1)$ (this is true if $\chi(\gamma) \in \mathbf{Z}_{\geqslant 0}$ and therefore for all $\gamma \in \Gamma_K$ by continuity). The notation $\mathbf{E}_K$ is a bit misleading because $\mathbf{E}_K$ only depends on K_∞.

Lemma 15.6. — *If π_K is a uniformizer of $\mathbf{E}_K$ then $\mathbf{E}_K = k_{K_\infty}(\!(\pi_K)\!)$.*

Proof. — Since $\mathbf{E}_K$ is a finite extension of $\mathbf{E}_{\mathbf{Q}_p} = \mathbf{F}_p(\!(\pi)\!)$, the lemma follows from the structure theorem for local fields of equal characteristic and the fact that the residue field of $\mathbf{E}_K$ is $\overline{\mathbf{F}}_p^{H_K} = k_{K_\infty}$. □

Corollary 15.7. — *If L/K is a finite extension, then the inertia index and ramification index of $\mathbf{E}_L$ over $\mathbf{E}_K$ are given by $f(\mathbf{E}_L/\mathbf{E}_K) = f(L_\infty/K_\infty)$ and $e(\mathbf{E}_L/\mathbf{E}_K) = e(L_\infty/K_\infty)$.*

Exercises

1. If x and y belong to $\mathcal{O}_{\mathbf{C}_p}$ and $\mathrm{val}_p(x-y) = \alpha > 0$, then $\mathrm{val}_p(x^p - y^p) \geqslant \min(p\alpha, \alpha^p)$.
2. Let K be a finite extension of $\mathbf{Q}_p$. Prove that $\mathfrak{m}_{\widetilde{\mathbf{E}}}^{G_K} = \{0\}$ and then that $\widetilde{\mathbf{E}}^{G_K} = k_K$. To which infinite extensions of $\mathbf{Q}_p$ does this argument extend to?
3. Check that π is transcendental over $\mathbf{F}_p$ and that the map $\mathbf{F}_p[\![\pi]\!] \to \widetilde{\mathbf{E}}$ is injective.

4. Show that if K is a finite extension of $\mathbf{Q}_p$ then $\mathbf{E}_K^+$ is the set of $x \in \widetilde{\mathbf{E}}^+$ such that $x_i \in \mathcal{O}_{K_i}/I$ for all $i \gg 0$.
5. Show that if K is a finite unramified extension of $\mathbf{Q}_p$ then $\mathbf{E}_K = k_K(\!(\pi)\!)$. Can you also describe $\mathbf{E}_K$ if K is tamely ramified?
6. Give an example where k_{K_∞} is larger than k_K.
7. Compute the valuation of $\mathfrak{d}_{\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}}$ in terms of the constant of exercise 1 of chapter 9.
8. Let K be a finite extension of $\mathbf{Q}_p$. Using exercise 2, prove that $\widetilde{\mathbf{B}}^{G_K} = K_0$ where K_0 is the maximal unramified extension of $\mathbf{Q}_p$ in K.
9. Prove that if we write $[\varepsilon] - 1 = [\pi] + p[\beta_1] + p^2[\beta_2] + \cdots$, then $\mathrm{val}_{\mathbf{E}}(\beta_i) \geqslant p^{1-i}/(p-1)$.
10. Let V be a p-adic representation of G_K such that $\widetilde{\mathbf{B}} \otimes_{\mathbf{Q}_p} V = \widetilde{\mathbf{B}}^d$ as semilinear $\widetilde{\mathbf{B}}$-representations of G_K. Prove that $V|_{I_K}$ is trivial.
11. Prove that G_K acts continuously on $\tilde{\mathbf{A}}$ for the weak topology but not for the strong (p-adic) topology.
12. Prove that the map $\mathbf{A}^+ \to \mathbf{E}^+$ is surjective.

16. Witt vectors over valued rings

The ring $W(R)$ is complete for the p-adic topology, but if R itself admits some topology, then we can define a finer topology on $W(R)$. In all the cases that we'll need, R is complete for some valuation.

Proposition 16.1. — *Let $S_n \in S/pS = \mathbf{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geqslant 0}$ be the element defined as above by*

$$\sum_{n\geqslant 0} p^n[X_n] + \sum_{n\geqslant 0} p^n[Y_n] = \sum_{n\geqslant 0} p^n[S_n(X_j, Y_j)].$$

1. *S_n is a (genuine) polynomial in $\{X_i^{p^{i-n}}\}_{0\leqslant i\leqslant n}$ and in $\{Y_i^{p^{i-n}}\}_{0\leqslant i\leqslant n}$;*
2. *S_n is homogeneous of degree 1 if each X_i and Y_i is of weight 1;*
3. *S_n is of the form $S_n = (X_n + Y_n) + (X_{n-1}^{p^{-1}} + Y_{n-1}^{p^{-1}})R_{n,n-1} + \cdots + (X_0^{p^{-n}} + Y_0^{p^{-n}})R_{n,0}$ where $R_{n,i} \in S/pS$.*

Proof. — If $i \geqslant 0$ and $\hat{S}_i$ is any lift of S_i, then $[S_i] = \hat{S}_i(X^{1/p^{n-i}}, Y^{1/p^{n-i}})^{p^{n-i}} \bmod p^{n-i+1}$ so that S_n is the image in S/pS of

$$\frac{X_0 + \cdots + p^n X_n + Y_0 + \cdots + p^n Y_n - \hat{S}_0(X^{1/p^n}, Y^{1/p^n})^{p^n} - \cdots - p^{n-1}\hat{S}_{n-1}(X^{1/p}, Y^{1/p})^p}{p^n},$$

from which items (1), (2) and (3) of the proposition result by induction. □

Let $\mathrm{val}(\cdot)$ be some valuation on R for which it is complete (note that since R is perfect, this valuation is non-discrete unless it is trivial) and let $\mathcal{O}_R$ denote the integers of R for $\mathrm{val}(\cdot)$. If $k \geqslant 0$, consider the map $w_k : W(R) \to \mathbf{R} \cup \{+\infty\}$ given by $w_k(x) = \inf_{i\leqslant k} \mathrm{val}(x_i)$ if $x = \sum_{i\geqslant 0} p^i[x_i]$. If $x \in W(R)$, then $w_k(x) = +\infty$ if and only if $x \in p^{k+1}W(R)$ and if $x, y \in W(R)$, then $w_k(x+y) \geqslant \inf(w_k(x), w_k(y))$ so that w_k is a semi-valuation on $W(R)$.

Definition 16.2. — The weak topology on $W(R)$ is the one defined by the semi-valuations w_k.

This means that if $\{a_n\}_{n\geqslant 1}$ is a sequence of elements of $W(R)$ and $a \in W(R)$, then $a_n \to a$ for the weak topology if and only if $w_k(a_n - a) \to 0$ for all $k \geqslant 1$.

Lemma 16.3. — *If $a, b \in W(\mathcal{O}_R) + p^{n+1}W(R)$ and $n \geqslant 0$, then*

1. $\mathrm{val}(a_n - b_n) \geqslant p^{-n} w_n(a-b)$,
2. $w_n(a-b) \geqslant \min_{k\leqslant n} p^{-k} v(a_{n-k} - b_{n-k})$.

Proof. — We have $a - b = \sum_{k\geqslant 0} p^k [D_k(a_i, b_i)]$ where $D_k(X_i, Y_i) = S_k(X_i, Y_i)$ so that by (3) of proposition 16.1, there exist $c_0, \dots, c_{n-1} \in \mathcal{O}_R$ such that

$$a_n - b_n = D_n(a_k, b_k) - (a_{n-1} - b_{n-1})^{1/p} c_{n-1} - \cdots - (a_0 - b_0)^{1/p^n} c_0$$

and since $\mathrm{val}(D_n(a_k, b_k)) \geqslant w_n(a-b)$ by definition, (1) results by induction on n.

We also have $w_n(a-b) = \min_{k\leqslant n} \mathrm{val}(D_k(a_i, b_i))$ and (3) of proposition 16.1 implies that $\mathrm{val}(D_k(a_i, b_i)) \geqslant \min_{j\leqslant k} p^{-j} v(a_{k-j} - b_{k-j})$ which proves (2) since $p^{-j} v(a_{k-j} - b_{k-j}) = p^{n-k} \cdot p^{-(n-k)-j} v(a_{n-((n-k)+j)} - b_{n-((n-k)+j)})$. □

Proposition 16.4. — *The ring $W(R)$ is complete for the weak topology.*

Proof. — Let $(x^{(i)})_{i\geqslant 0}$ be a sequence of elements of $W(R)$, and write $x^{(i)} = \sum_{k\geqslant 0} p^k [x_k^{(i)}]$. We will prove that if $n \geqslant 0$, then the sequence $(x^{(i)})_{i\geqslant 0}$ is Cauchy for $w_0(\cdot), \dots, w_n(\cdot)$ if and only if the sequences $(x_k^{(i)})_{i\geqslant 0}$ are Cauchy for $0 \leqslant k \leqslant n$. This implies that $W(R)$ is complete for the weak topology if R is complete for $\mathrm{val}(\cdot)$.

Suppose that $(x^{(i)})_{i\geqslant 0}$ is Cauchy for $w_0(\cdot), \dots, w_n(\cdot)$. We can assume that $w_k(x^{(i)} - x^{(j)}) \geqslant 0$ for all i, j and $0 \leqslant k \leqslant n$. There exists $\alpha \in \mathcal{O}_R$ such that $\alpha x_k^{(0)} \in \mathcal{O}_R$ for $0 \leqslant k \leqslant n$ and by replacing $x^{(0)}$ with $[\alpha]x^{(0)}$ we can also assume that $x^{(0)} \in W(\mathcal{O}_R) + p^{n+1}W(R)$. This implies that $x^{(i)} \in W(\mathcal{O}_R) + p^{n+1}W(R)$ for all $i \geqslant 1$. Item (1) of lemma 16.3 now implies that the sequences $(x_k^{(i)})_{i\geqslant 0}$ are Cauchy for $0 \leqslant k \leqslant n$. The converse statement follows in a similar manner from item (2) of lemma 16.3. □

17. The rings $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{B}}$

Reference: [**Fon90**]. Let $\tilde{\mathbf{A}} = W(\tilde{\mathbf{E}})$ be the ring of Witt vectors over $\tilde{\mathbf{E}}$ and let $\tilde{\mathbf{B}} = \tilde{\mathbf{A}}[1/p]$. By exercise 2 of the section on Witt vectors, $\tilde{\mathbf{B}}$ is a field. This field is equipped with the frobenius $\varphi = W(x \mapsto x^p)$ and an action of $G_{\mathbf{Q}_p}$ lifting the action of $G_{\mathbf{Q}_p}$ on $\tilde{\mathbf{E}}$. We also denote by π the element $[\varepsilon] - 1 \in \tilde{\mathbf{A}}$ so that the image of π in $\tilde{\mathbf{E}}$ is $\pi = \varepsilon - 1$. We then have $\varphi(\pi) = (1+\pi)^p - 1$ and $g(\pi) = (1+\pi)^{\chi(g)} - 1$ if $g \in G_{\mathbf{Q}_p}$.

We cannot construct Witt vectors over $\mathbf{E}$ because it is not perfect, so we use a different method to construct a field $\mathbf{B} = \mathbf{A}[1/p]$ which is stable under φ and $G_{\mathbf{Q}_p}$ and such that $\mathbf{A}/p\mathbf{A} = \mathbf{E}$. Let $\mathbf{A}_{\mathbf{Q}_p}$ be the p-adic completion of $\mathbf{Z}_p[\![\pi]\!][1/\pi]$ inside $\tilde{\mathbf{A}}$ and let $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[1/p]$ so that $\mathbf{B}_{\mathbf{Q}_p}$ is a local field whose residue field is $\mathbf{E}_{\mathbf{Q}_p}$. We say that a finite extension is unramified if the residual extension is separable and the degree of the extension is equal to the degree of the extension of the residue fields.

Lemma 17.1. — *If $K/\mathbf{Q}_p$ is a finite extension, then there exists a unique finite unramified extension $\mathbf{B}_K/\mathbf{B}_{\mathbf{Q}_p}$ contained in $\widetilde{\mathbf{B}}$ and whose residue field is $\mathbf{E}_K$.*

Proof. — One can take $\mathbf{B}_K = \mathbf{B}_{\mathbf{Q}_p}[y]$ where y is a root of a polynomial whose reduction modulo p is the minimal polynomial of a primitive element of $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$. □

Let $\mathbf{B}$ be the p-adic completion of the maximal unramified extension of $\mathbf{B}_{\mathbf{Q}_p}$ inside $\widetilde{\mathbf{B}}$. If we set $\mathbf{A} = \tilde{\mathbf{A}} \cap \mathbf{B}$, then $\mathbf{A}/p\mathbf{A} = \mathbf{E}$ and furthermore, $\mathbf{B}$ is stable under φ and the action of $G_{\mathbf{Q}_p}$ because of its definition. Finally, we have $\mathrm{Aut}(\mathbf{B}/\mathbf{B}_{\mathbf{Q}_p}) = \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p}) = H_{\mathbf{Q}_p}$ and for each finite extension $K/\mathbf{Q}_p$ we have $\mathbf{B}_K = \mathbf{B}^{H_K}$ since $(\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{unr}})^{H_K} = (\hat{\mathbf{B}}_{\mathbf{Q}_p}^{\mathrm{unr}})^{H_K}$ by theorem 5.3 (the Ax-Sen-Tate theorem).

Theorem 17.2. — *If K is a finite extension of $\mathbf{Q}_p$ then $H^1(H_K, \mathbf{A}) = \{0\}$ and if $d \geqslant 1$ then $H^1(H_K, \mathrm{GL}_d(\mathbf{A})) = \{1\}$ (where the cocycles are continuous for the p-adic topology).*

Proof. — This follows from corollary 15.5 above and proposition 7.4. □

Proposition 17.3. — *If $\pi_K \in \mathbf{A}_K$ is such that $\overline{\pi}_K \in \mathbf{E}_K$ is a uniformizer, then $\mathbf{A}_K$ is the p-adic completion of $\mathcal{O}_{K_0'}[\![\pi_K]\!][1/\pi_K]$ where K_0' is the maximal unramified extension of $\mathbf{Q}_p$ in K_∞.*

Proof. — If R_K denotes the p-adic completion of $\mathcal{O}_{K_0'}[\![\pi_K]\!][1/\pi_K]$, then $R_K/pR_K = \mathbf{E}_K$ by lemma 15.6 and therefore the inclusion map $R_K \to \mathbf{A}_K$ is surjective modulo p. Since R_K is p-adically complete, the map is an isomorphism. □

We conclude this section with a few words about the topology of $\widetilde{\mathbf{B}}$. There is the p-adic topology, which makes $\widetilde{\mathbf{B}}$ into a Banach space whose unit ball is $\tilde{\mathbf{A}}$, but there is also the weak topology from definition 16.2. Recall that if $k \geqslant 0$, we consider the map $w_k : \tilde{\mathbf{A}} \to \mathbf{R} \cup \{+\infty\}$ given by $w_k(x) = \inf_{i \leqslant k} \mathrm{val}_{\mathbf{E}}(x_i)$ if $x = \sum_{i \geqslant 0} p^i [x_i]$ and that the weak topology on $\tilde{\mathbf{A}}$ is the one defined by the semi-valuations w_k. The weak topology on $\widetilde{\mathbf{B}}$ is the inductive limit topology on $\widetilde{\mathbf{B}} = \cup_{k \geqslant 1} p^{-k} \tilde{\mathbf{A}}$. Note that if $\tilde{p}$ is any element of $\widetilde{\mathbf{E}}$ such that $\tilde{p}^{(0)} = p$ and if $U_{k,n} = p^k \tilde{\mathbf{A}} + [\tilde{p}]^n \tilde{\mathbf{A}}^+$, then the weak topology on $\widetilde{\mathbf{B}}$ is the

one for which a basis of neighborhoods of 0 is given by the $\{U_{k,n}\}_{k,n\geqslant 0}$. Proposition 16.4 implies the following.

Proposition 17.4. — *The ring $\tilde{\mathbf{A}}$ is complete for the weak topology.*

The group $G_{\mathbf{Q}_p}$ acts on $\widetilde{\mathbf{B}}$ by isometries for both the p-adic and the weak topology. On the other hand, φ is an isometry for the p-adic topology but is merely continuous for the weak topology since $w_k(x) = pw_k(x)$.

18. Fontaine's (φ,Γ)-modules

Reference: [**Fon90**]. Let K be a finite extension of $\mathbf{Q}_p$ and let R be one of the rings $\mathbf{E}_K$, $\mathbf{A}_K$ or $\mathbf{B}_K$ so that R is equipped with a frobenius φ and an action of $\Gamma_K = G_K/H_K$.

Definition 18.1. — A (φ,Γ)-module over R is a free R-module D of finite rank d which is equipped with a semilinear frobenius φ such that $\mathrm{Mat}(\varphi) \in \mathrm{GL}_d(R)$ and a commuting and continuous (for the weak topology) semilinear action of Γ_K.

If D is a (φ,Γ)-module over $\mathbf{B}_K$ then we say that D is étale if there is a basis of D in which $\mathrm{Mat}(\varphi) \in \mathrm{GL}_d(\mathbf{A}_K)$.

The fact that $\mathrm{Mat}(\varphi) \in \mathrm{GL}_d(R)$ does not depend on the choice of basis and is equivalent to the condition that D has a basis of elements which belong to $\varphi(\mathrm{D})$. Note that if we choose a basis of D and $P = \mathrm{Mat}(\varphi)$ and $G = \mathrm{Mat}(\gamma)$ where $\gamma \in \Gamma_K$ then the condition that φ and γ commute as semilinear operators is equivalent to $P\varphi(G) = G\gamma(P)$.

Proposition 18.2. — *If W is an $\mathbf{F}_p$-linear representation of G_K of dimension d and if we set $\mathrm{D}(W) = (\mathbf{E}\otimes_{\mathbf{F}_p} W)^{H_K}$ then $\mathrm{D}(W)$ is a (φ,Γ)-module over $\mathbf{E}_K$ of dimension d and $\mathbf{E}\otimes_{\mathbf{E}_K}\mathrm{D}(W) = \mathbf{E}\otimes_{\mathbf{F}_p} W$ so that $W = (\mathbf{E}\otimes_{\mathbf{E}_K}\mathrm{D}(W))^{\varphi=1}$.*

Proof. — If W is an $\mathbf{F}_p$-linear representation of G_K of dimension d, then its restriction to H_K defines a class $[W] \in H^1(H_K, \mathrm{GL}_d(\mathbf{F}_p))$ and by extending scalars from $\mathbf{F}_p$ to $\mathbf{E}$ we get a class in $H^1(H_K, \mathrm{GL}_d(\mathbf{E}))$. This last group is trivial by theorem 15.5 which means that $\mathbf{E}\otimes_{\mathbf{F}_p} W$ is isomorphic to $\mathbf{E}^d$ as a semilinear $\mathbf{E}$-representations of H_K. In particular, if we set $\mathrm{D}(W) = (\mathbf{E}\otimes_{\mathbf{F}_p} W)^{H_K}$ then $\mathrm{D}(W)$ is an $\mathbf{E}_K$ vector space of dimension d which is stable under φ and the action of Γ_K. Finally, the facts that $\mathbf{E}\otimes_{\mathbf{F}_p} W \simeq \mathbf{E}^d$ and $\mathrm{D}(W) \simeq \mathbf{E}_K^d$ (not as (φ,Γ)-modules!) imply that $\mathbf{E}\otimes_{\mathbf{E}_K}\mathrm{D}(W) = \mathbf{E}\otimes_{\mathbf{F}_p} W$. □

The exact same proof with $\mathbf{A}$ instead of $\mathbf{E}$ and theorem 17.2 instead of theorem 15.5 gives us the corresponding result below.

Proposition 18.3. — *If T is a $\mathbf{Z}_p$-representation of G_K which is free of rank d and if we set $\mathrm{D}(T) = (\mathbf{A} \otimes_{\mathbf{Z}_p} T)^{H_K}$ then $\mathrm{D}(T)$ is a (φ, Γ)-module over $\mathbf{A}_K$ of rank d and $\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}(T) = \mathbf{A} \otimes_{\mathbf{Z}_p} T$ so that $T = (\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}(T))^{\varphi=1}$.*

Finally if V is a $\mathbf{Q}_p$-linear representation of G_K then we get étale (φ, Γ)-modules out of the $\mathrm{D}(\cdot)$ construction.

Proposition 18.4. — *If V is a $\mathbf{Q}_p$-linear representation of G_K of dimension d and if we set $\mathrm{D}(V) = (\mathbf{B} \otimes_{\mathbf{Q}_p} V)^{H_K}$ then $\mathrm{D}(V)$ is an étale (φ, Γ)-module over $\mathbf{B}_K$ of dimension d and $\mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D}(V) = \mathbf{B} \otimes_{\mathbf{Q}_p} V$ so that $V = (\mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D}(V))^{\varphi=1}$.*

Proof. — The representation V admits a G_K-stable lattice T and since $\mathbf{A} \otimes_{\mathbf{Z}_p} T \simeq \mathbf{A}^d$ as semilinear $\mathbf{A}$-representations of H_K we have $\mathbf{B} \otimes_{\mathbf{Z}_p} V \simeq \mathbf{B}^d$ as semilinear $\mathbf{B}$-representations of H_K which implies the result as in the proof of proposition 18.2. The (φ, Γ)-module $\mathrm{D}(V)$ is étale since $\mathrm{D}(V) = \mathbf{B}_K \otimes_{\mathbf{A}_K} \mathrm{D}(T)$. □

We now define a functor in the opposite direction. If D is a (φ, Γ)-module over either $\mathbf{E}_K$ or $\mathbf{A}_K$ or $\mathbf{B}_K$ then we set $W(\mathrm{D}) = (\mathbf{E} \otimes_{\mathbf{E}_K} \mathrm{D})^{\varphi=1}$ or $T(\mathrm{D}) = (\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D})^{\varphi=1}$ or $V(\mathrm{D}) = (\mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D})^{\varphi=1}$.

Proposition 18.5. — *If D is a (φ, Γ)-module of dimension d over $\mathbf{E}_K$ then $W(\mathrm{D}) = (\mathbf{E} \otimes_{\mathbf{E}_K} \mathrm{D})^{\varphi=1}$ is an $\mathbf{F}_p$-vector space of dimension d and $\mathbf{E} \otimes_{\mathbf{F}_p} W(\mathrm{D}) = \mathbf{E} \otimes_{\mathbf{E}_K} \mathrm{D}$.*

Proof. — Since $\mathbf{E} \otimes_{\mathbf{E}_K} \mathrm{D}$ is a φ-module over $\mathbf{E}$ and $\mathbf{E}$ is separably closed, theorem 8.6 tells us that $\mathbf{E} \otimes_{\mathbf{E}_K} \mathrm{D}$ has a basis of elements fixed by φ which implies the proposition. □

Proposition 18.6. — *If D is a (φ, Γ)-module of rank d over $\mathbf{A}_K$ then $T(\mathrm{D}) = (\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D})^{\varphi=1}$ is a free $\mathbf{Z}_p$-module of rank d and $\mathbf{A} \otimes_{\mathbf{Z}_p} T(\mathrm{D}) = \mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}$.*

Proof. — Since $\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}$ is a φ-module over $\mathbf{A}$ and $\mathbf{A}/p\mathbf{A} = \mathbf{E}$ where $\mathbf{E}$ is separably closed, corollary 8.7 tells us that $\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}$ has a basis of elements fixed by φ which implies the proposition. □

Proposition 18.7. — *If D is an étale (φ, Γ)-module of dimension d over $\mathbf{B}_K$ then $V(\mathrm{D}) = (\mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D})^{\varphi=1}$ is a $\mathbf{Q}_p$-vector space of dimension d and $\mathbf{B} \otimes_{\mathbf{Q}_p} V(\mathrm{D}) = \mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D}$.*

Proof. — Since D is étale, it is of the form $\mathbf{B}_K \otimes_{\mathbf{A}_K} \mathrm{D}_0$ where D_0 is a (φ, Γ)-module over $\mathbf{A}_K$ and proposition 18.6 tells us that $\mathbf{A} \otimes_{\mathbf{A}_K} \mathrm{D}_0 = \mathbf{A} \otimes_{\mathbf{Z}_p} T(\mathrm{D}_0)$ where $T(\mathrm{D}_0)$ is a free $\mathbf{Z}_p$-module of rank d so that $\mathbf{B} \otimes_{\mathbf{B}_K} \mathrm{D} = \mathbf{B} \otimes_{\mathbf{Q}_p} V(\mathrm{D})$ where $V(\mathrm{D}) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T(\mathrm{D}_0)$ is a $\mathbf{Q}_p$-vector space of dimension d. □

If we put all of the above propositions together, we find the following theorem.

Theorem 18.8. — *The functor $V \mapsto \mathrm{D}(V)$ defines equivalences of categories :*

$$\{\mathbf{F}_p\text{-linear representations of } G_K\} \to \{(\varphi,\Gamma)\text{-modules over } \mathbf{E}_K\},$$
$$\{\text{free } \mathbf{Z}_p\text{-representations of } G_K\} \to \{(\varphi,\Gamma)\text{-modules over } \mathbf{A}_K\},$$
$$\{\mathbf{Q}_p\text{-linear representations of } G_K\} \to \{\text{étale } (\varphi,\Gamma)\text{-modules over } \mathbf{B}_K\}.$$

Proof. — The functors defined in proposition 18.2, 18.3 and 18.4 and the functors defined in propositions 18.5, 18.6 and 18.7 are inverse of each other. □

The upshot of this theorem is that although it is in general impossible to give an explicit description of a p-adic representation, a (φ,Γ)-module is a very explicit object. Indeed, the group Γ_K can be seen as a subgroup of $\mathbf{Z}_p^\times$ via the cyclotomic character and is therefore topologically generated by one element $\gamma \in \Gamma_K$ (unless $p=2$ and $\Gamma_K \simeq \mathbf{Z}_2^\times$ which is generated by two elements). In order to give concretely a (φ,Γ)-module over R, it is therefore enough to give two matrices $P = \mathrm{Mat}(\varphi)$ and $G = \mathrm{Mat}(\gamma)$ satisfying some semilinear commutation relation. By the results of §15, the rings $\mathbf{E}_K$ and $\mathbf{A}_K$ and $\mathbf{B}_K$ are rings of power series and if $K/\mathbf{Q}_p$ is not too complicated, then we know the formulas for the map φ and the action of Γ_K.

Let $\delta : \mathbf{Q}_p^\times \to \mathbf{Z}_p^\times$ be a character, and let $\mathbf{A}_{\mathbf{Q}_p}(\delta)$ be the rank one (φ,Γ)-module $\mathbf{A}_{\mathbf{Q}_p}(\delta) = \mathbf{A}_{\mathbf{Q}_p} \cdot e_\delta$ where $\varphi(e_\delta) = \delta(p)e_\delta$ and $\gamma(e_\delta) = \delta(\chi(\gamma))e_\delta$. Let $T(\delta)$ be the rank one representation of $G_{\mathbf{Q}_p}$ over $\mathbf{Z}_p$ attached to δ by local class field theory, which is therefore given by $g \mapsto \mu_{\delta(p)}^{-1} \cdot \delta(\chi(\gamma))$ where μ_λ is the unramified character sending the arithmetic frobenius to λ^{-1} (so that if we normalize class field theory to send the geometric frobenius to p then $\mu_\lambda(p) = \lambda$).

Proposition 18.9. — *We have $\mathrm{D}(T(\delta)) = \mathbf{A}_{\mathbf{Q}_p}(\delta)$, and every rank one (φ,Γ)-module over $\mathbf{A}_{\mathbf{Q}_p}$ if of the form $\mathbf{A}_{\mathbf{Q}_p}(\delta)$.*

We now give examples of (φ,Γ)-modules over $\mathbf{E}_{\mathbf{Q}_p}$.

If n is an integer $\geqslant 1$, choose $\pi_n \in \overline{\mathbf{Q}}_p$ such that $\pi_n^{p^n-1} = -p$. The fundamental character of level n defined in §1.7 of [**Ser72**], $\omega_n : I_{\mathbf{Q}_p} \to \overline{\mathbf{F}}_p^\times$ is given by $\omega_n(g) = \overline{g(\pi_n)/\pi_n} \in \overline{\mathbf{F}}_p^\times$ for $g \in I_{\mathbf{Q}_p}$. This definition does not depend on the choice of π_n and shows that ω_n extends to a character $G_{\mathbf{Q}_{p^n}} \to \mathbf{F}_{p^n}^\times$. With this definition, ω_n is actually the reduction mod p of the Lubin-Tate character associated to the uniformizer p of the field $\mathbf{Q}_{p^n}$. If $1 \leqslant h \leqslant p^n - 2$ is primitive, the characters $\omega_n^h, \omega_n^{ph}, \ldots, \omega_n^{p^{n-1}h}$ of $I_{\mathbf{Q}_p}$ are pairwise distinct. If $\lambda \in \overline{\mathbf{F}}_p^\times$ is such that $\lambda^n \in \mathbf{F}_p^\times$, let $W_\lambda = \{\alpha \in \overline{\mathbf{F}}_p \text{ such that } \alpha^{p^n} = \lambda^{-n}\alpha\}$ so that W_λ is a $\mathbf{F}_{p^n}$-vector space of dimension 1 and hence a $\mathbf{F}_p$-vector space of dimension n. By composing the map $\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{nr}}(\pi_n)/\mathbf{Q}_p) \xrightarrow{\sim} \mathbf{F}_{p^n}^\times \rtimes \hat{\mathbf{Z}}$ with the

map $\mathbf{F}_{p^n}^\times \rtimes \hat{\mathbf{Z}} \to \mathrm{End}_{\mathbf{F}_p}(W_\lambda)$ given by $(x,0) \mapsto m_x^h$ (where m_x is the multiplication by x map) and by $(1,1) \mapsto (\alpha \mapsto \alpha^p)$ we get an n-dimensional $\mathbf{F}_p$-linear representation of $G_{\mathbf{Q}_p}$ which is isomorphic to $(\mathrm{ind}_{G_{\mathbf{Q}_{p^n}}}^{G_{\mathbf{Q}_p}} \omega_n^h) \otimes \mu_\lambda$ after extending scalars and whose determinant is $\omega^h \mu_{-1}^{n-1} \mu_\lambda^n$ so that if $\lambda^n = (-1)^{n-1}$ then the determinant is ω^h and we call $\mathrm{ind}(\omega_n^h)$ the representation thus constructed; it is then uniquely determined by the two conditions $\det \mathrm{ind}(\omega_n^h) = \omega^h$ and $\mathrm{ind}(\omega_n^h)|_{I_{\mathbf{Q}_p}} = \oplus_{i=0}^{n-1} \omega_n^{p^i h}$ since $(\mathrm{ind}_{G_{\mathbf{Q}_{p^n}}}^{G_{\mathbf{Q}_p}} \omega_n^h) \otimes \mu_{\lambda_1} = (\mathrm{ind}_{G_{\mathbf{Q}_{p^n}}}^{G_{\mathbf{Q}_p}} \omega_n^h) \otimes \mu_{\lambda_2}$ if and only if we have $\lambda_1^n = \lambda_2^n$. If $\gamma \in \Gamma$, then let $f_\gamma(X) = \omega(\gamma)X/\gamma(X) \in 1 + X\mathbf{F}_p[\![X]\!]$.

Proposition 18.10. — *The (φ,Γ)-module $\mathrm{D}(\mathrm{ind}(\omega_n^h))$ is defined over $\mathbf{F}_p(\!(X)\!)$ and admits a basis $e_0,\dots,e_{n-1}$ in which $\gamma(e_j) = f_\gamma(X)^{hp^j(p-1)/(p^n-1)} e_j$ if $\gamma \in \Gamma$ and $\varphi(e_j) = e_{j+1}$ for $0 \leqslant j \leqslant n-2$ and $\varphi(e_{n-1}) = (-1)^{n-1} X^{-h(p-1)} e_0$.*

More explicit examples can be found, for instance, in [**Ber11**].

Exercises

1. Let D be a (φ,Γ)-module over $\mathbf{B}_K$ so that $\widetilde{\mathrm{D}} = \widetilde{\mathbf{B}} \otimes_{\mathbf{B}_K} \mathrm{D}$ is a φ-module over $\widetilde{\mathbf{B}}$. Prove that D is étale if and only if $\widetilde{\mathrm{D}}$ is pure of slope zero in the sense of §8.
2. Prove that every finite dimensional $\mathbf{Q}_p$-linear continuous representation V of a compact group G admits a $\mathbf{Z}_p$-lattice T stable under G.
3. State and prove an analogue of theorem 18.8 for representations which are free $\mathbf{Z}/p^n\mathbf{Z}$-modules of finite rank.
4. Choose $h \geqslant 1$, let $\Phi_p(X)$ be the p-th cyclotomic polynomial and let $P = \left(\begin{smallmatrix} 0 & -1 \\ \Phi_p(1+X)^h & 0 \end{smallmatrix}\right)$.
   (a) Prove that if $\gamma \in \Gamma$, then there exist uniquely defined power series $f_\gamma(X)$ and $g_\gamma(X)$ belonging to $1 + X\mathbf{Z}_p[\![X]\!]$ such that if we set $G_\gamma = \left(\begin{smallmatrix} f_\gamma(X) & 0 \\ 0 & g_\gamma(X) \end{smallmatrix}\right)$, then $P \cdot \varphi(G_\gamma) = G_\gamma \cdot \gamma(P)$ so that P and the $\{G_\gamma\}_{\gamma\in\Gamma}$ define a two-dimensional (φ,Γ)-module over $\mathbf{A}_{\mathbf{Q}_p}$.
   (b) Compute the reduction modulo p and the determinant of this (φ,Γ)-module.
   (c) Prove that if V_h is the associated representation of $G_{\mathbf{Q}_p}$, then the restriction of V_h to $G_{\mathbf{Q}_{p^2}}$ is the direct sum of two characters.
   (d) * Can you compute these two characters?
5. Let V be a $\mathbf{Q}_p$-representation of G_K and let $\mathrm{D}(V)$ be the associated (φ,Γ)-module. If L is a finite extension of K, then show that $\mathrm{D}(V|_{G_L}) = \mathbf{B}_L \otimes_{\mathbf{B}_K} \mathrm{D}(V)$.
6. Let V be a $\mathbf{Q}_p$-representation of G_L and let $\mathrm{D}(V)$ be the associated (φ,Γ)-module. If L is a finite extension of K, then compute $\mathrm{D}(\mathrm{Ind}_{G_L}^{G_K} V)$.

19. The Colmez-Sen-Tate conditions

Reference: [**BC08**]. Let $\widetilde{\Omega}$ be a $\mathbf{Q}_p$-algebra and let $\mathrm{val}_\Omega : \widetilde{\Omega} \to \mathbf{R} \cup \{+\infty\}$ be a map such that

1. $\mathrm{val}_\Omega(x) = +\infty$ if and only if $x = 0$;
2. $\mathrm{val}_\Omega(x+y) \geqslant \min(\mathrm{val}_\Omega(x), \mathrm{val}_\Omega(y))$;

3. $\mathrm{val}_\Omega(xy) \geqslant \mathrm{val}_\Omega(x) + \mathrm{val}_\Omega(y)$;
4. $\mathrm{val}_\Omega(p) > 0$ and $\mathrm{val}_\Omega(px) = \mathrm{val}_\Omega(p) + \mathrm{val}_\Omega(x)$ if $x \in \widetilde{\Omega}$.

The map val_Ω can be used to define a separated topology on $\widetilde{\Omega}$ and we assume that $\widetilde{\Omega}$ is complete with respect to that topology so that it is a Banach space. Suppose that $\widetilde{\Omega}$ is equipped with an action of G_K such that $\mathrm{val}_\Omega(g(x)) = \mathrm{val}_\Omega(x)$ for all $g \in G_K$ and $x \in \widetilde{\Omega}$. We say that $\widetilde{\Omega}$ satisfies the Colmez-Sen-Tate conditions if there exists three constants c_1, c_2 and c_3 in $\mathbf{R}_{\geqslant 0}$ such that (CST1), (CST2) and (CST3) below are fulfilled.

(CST1) For every finite extensions M/L of K, there exists $\alpha \in \widetilde{\Omega}^{H_M}$ such that $\mathrm{val}_\Omega(\alpha) > -c_1$ and $\mathrm{Tr}_{M_\infty/L_\infty}(\alpha) = 1$.

(CST2) For every finite extension L of K, there exists $n(L) \in \mathbf{Z}_{\geqslant 1}$ and an increasing sequence $\{\Omega_{L,n}\}_{n \geqslant n(L)}$ of closed sub $\mathbf{Q}_p$-algebras of $\widetilde{\Omega}^{H_L}$ along with maps $R_{L,n} : \widetilde{\Omega}^{H_L} \to \Omega_{L,n}$ satisfying the following properties
   1. if $x \in \widetilde{\Omega}^{H_L}$ then $\mathrm{val}_\Omega(R_{L,n}(x)) \geqslant \mathrm{val}_\Omega(x) - c_2$ and $R_{L,n}(x) \to x$ as $n \to \infty$;
   2. if L_2/L_1 is finite, then $\Omega_{L_1,n} \subset \Omega_{L_2,n}$ and $R_{L_2,n}$ restricted to $\widetilde{\Omega}^{H_{L_1}}$ is $R_{L_1,n}$;
   3. $R_{L,n}$ is $\Omega_{L,n}$-linear and is the identity on $\Omega_{L,n}$;
   4. if $g \in G_K$ then $g(\Omega_{L,n}) = \Omega_{g(L),n}$ and $g \circ R_{L,n} = R_{g(L),n} \circ g$.

(CST3) For every finite extension L of K, there exists $m(L) \geqslant n(L)$ such that if $\gamma \in \Gamma_L$ and $n \geqslant \max(n(\gamma), m(L))$, then $1-\gamma$ is invertible on $X_{L,n} = (1 - R_{L_n})(\widetilde{\Omega}^{H_L})$ and we have $\mathrm{val}_\Omega((\gamma-1)^{-1}(x)) \geqslant \mathrm{val}_\Omega(x) - c_3$ if $x \in X_{L,n}$.

Note that by (CST2), $R_{L,n}$ is the identity on $\mathrm{im}(R_{L,n}) = \Omega_{L,n}$ so that $R_{L,n}$ is an idempotent and $\widetilde{\Omega}^{H_L} = \ker(R_{L,n}) \oplus \mathrm{im}(R_{L,n}) = X_{L,n} \oplus \Omega_{L,n}$. Let $\Omega_{L,\infty} = \cup_{n \geqslant 0} \Omega_{L,n}$ so that $\Omega_{L,\infty}$ is dense in $\widetilde{\Omega}^{H_L}$ by (CST2).

As we'll see later, a typical example of an algebra $\widetilde{\Omega}$ satisfying the Colmez-Sen-Tate conditions is $\widetilde{\Omega} = \mathbf{C}_p$ with $\Omega_{L,n} = L_n$ and $R_{L,n}$ equal to the maps R_n from §10. The main point of these definitions is that if $\widetilde{\Omega}$ satisfies the Colmez-Sen-Tate conditions, then we can greatly simplify the cocycles $G_K \to \mathrm{GL}_d(\widetilde{\Omega})$.

If $M = (m_{ij})$ is a matrix, then we set $\mathrm{val}_\Omega(M) = \min \mathrm{val}_\Omega(m_{ij})$. If $\mathrm{val}_\Omega(1-M) = c > 0$ then M is invertible with inverse $\sum_{j \geqslant 0}(1-M)^j$ so that $\mathrm{val}_\Omega(1 - M^{-1}) = c$. If R is a subring of $\widetilde{\Omega}$, then in order to lighten the notation, we denote by $\mathrm{GL}_d(c, R)$ the group of matrices $M \in \mathrm{GL}_d(R)$ such that $\mathrm{val}_\Omega(1-M) \geqslant c$.

Theorem 19.1. — *If $\widetilde{\Omega}$ satisfies the Colmez-Sen-Tate conditions and if U is a cocycle on G_K with values in $\mathrm{GL}_d(\widetilde{\Omega})$, then there exists a finite extension L/K and a matrix $M \in \mathrm{GL}_d(\widetilde{\Omega})$ such that the cocycle on G_L given by $\tilde{U} : g \mapsto M^{-1} \cdot U(g) \cdot g(M)$ is trivial on H_L and has values in $\mathrm{GL}_d(\Omega_{L,n})$ for some $n \gg 0$.*

The proof of this result will be given after we establish a few lemmas.

Lemma 19.2. — *If $a > c_1$ and U is a cocycle on H_L with values in $\mathrm{GL}_d(a, \widetilde{\Omega})$ then there exists $M \in \mathrm{GL}_d(a - c_1, \widetilde{\Omega})$ such that the cocyle $g \mapsto M^{-1} \cdot U(g) \cdot g(M)$ has values in $\mathrm{GL}_d(a+1, \widetilde{\Omega})$.*

Proof. — Let N be a finite Galois extension of L such that $U(H_N) \subset \mathrm{GL}_d(a+1+c_1, \widetilde{\Omega})$ and let $\alpha \in \widetilde{\Omega}^{H_N}$ be such that $\mathrm{val}_\Omega(\alpha) \geqslant -c_1$ and $\mathrm{Tr}_{N_\infty/L_\infty}(\alpha) = 1$. If Q is a system of representatives of H_L/H_N then let $M_Q = \sum_{h \in Q} h(\alpha) U(h)$ so that $M_Q \in \mathrm{GL}_d(a - c_1, \widetilde{\Omega})$ and the cocycle relation implies that $U(g) \cdot g(M_Q) = M_{g(Q)}$ if $g \in H_L$. We then have

$$M_Q^{-1} \cdot U(g) \cdot g(M_Q) = 1 + M_Q^{-1}(M_{g(Q)} - M_Q) \in \mathrm{GL}_d(a+1, \widetilde{\Omega}),$$

so that we can take $M = M_Q$. □

Corollary 19.3. — *If $a > c_1$ and U is a cocycle on H_L with values in $\mathrm{GL}_d(a, \widetilde{\Omega})$ then there exists $M \in \mathrm{GL}_d(a - c_1, \widetilde{\Omega})$ such that $U(g) = M \cdot g(M)^{-1}$.*

Proof. — The preceding lemma gives us by induction a sequence of matrices $\{M_k\}_{k \geqslant 0}$ with $M_k \in \mathrm{GL}_d(a - c_1 + k, \widetilde{\Omega})$ such that the cocycle

$$g \mapsto M_k^{-1} \cdots M_0^{-1} \cdot U(g) \cdot g(M_0) \cdots g(M_k)$$

has values in $\mathrm{GL}_d(a + k + 1, \widetilde{\Omega})$ and we can then take $M = \prod_{k \geqslant 0} M_k$. □

Lemma 19.4. — *If $a \geqslant c_2 + c_3 + 1$ and $b \geqslant \max(a + c_2, 2c_2 + 2c_3 + 1)$ and $\gamma \in \Gamma_L$ and $n \geqslant \max(n(L), n(\gamma))$ and $U = 1 + U_1 + U_2$ with*

$$U_1 \in \mathrm{M}_d(\Omega_{L,n}) \text{ and } \mathrm{val}_\Omega(U_1) \geqslant a$$
$$U_2 \in \mathrm{M}_d(\widetilde{\Omega}^{H_L}) \text{ and } \mathrm{val}_\Omega(U_2) \geqslant b,$$

then there exists $M \in \mathrm{GL}_d(b - c_2 - c_3, \widetilde{\Omega}^{H_L})$ such that $M^{-1} \cdot U \cdot \gamma(M) = 1 + V_1 + V_2$ with

$$V_1 \in \mathrm{M}_d(\Omega_{L,n}) \text{ and } \mathrm{val}_\Omega(V_1) \geqslant a$$
$$V_2 \in \mathrm{M}_d(\widetilde{\Omega}^{H_L}) \text{ and } \mathrm{val}_\Omega(V_2) \geqslant b + 1.$$

Proof. — By conditions (CST2) and (CST3), we can write $U_2 = R_{L,n}(U_2) + (1 - \gamma)(V)$ where $\mathrm{val}_\Omega(R_{L,n}(U_2)) \geqslant b - c_2 \geqslant a$ and $\mathrm{val}_\Omega(V) \geqslant b - c_2 - c_3$. We then have

$$(1+V)^{-1} \cdot U \cdot \gamma(1+V) = (1 - V + V^2 - \cdots)(1 + U_1 + U_2)(1 + \gamma(V)),$$

so that

$$\mathrm{val}_\Omega((1+V)^{-1} \cdot U \cdot \gamma(1+V) - (1 + U_1 + R_{L,n}(U_2))) \geqslant b + 1,$$

and we can take $M = 1 + V$. □

Corollary 19.5. — *If $b \geqslant 2c_2+2c_3+1$ and $U \in \mathrm{GL}_d(b,\widetilde{\Omega}^{H_L})$ then there exists $M \in \mathrm{GL}_d(b-c_2-c_3,\widetilde{\Omega}^{H_L})$ such that $M^{-1}\cdot U\cdot\gamma(M)\in\mathrm{GL}_d(\Omega_{L,n})$.*

Proof. — The preceding lemma gives us by induction a sequence of matrices $\{M_k\}_{k\geqslant 0}$ with $M_k\in\mathrm{GL}_d(b-c_2-c_3+k,\widetilde{\Omega})$ such that we can write

$$M_k^{-1}\cdots M_0^{-1}\cdot U\cdot\gamma(M_0)\cdots\gamma(M_k)=1+U_{k,1}+U_{k,2}$$

with

$$U_{k,1}\in\mathrm{M}_d(\Omega_{L,n}) \text{ and } \mathrm{val}_\Omega(U_1)\geqslant b-c_2$$
$$U_{k,2}\in\mathrm{M}_d(\widetilde{\Omega}^{H_L}) \text{ and } \mathrm{val}_\Omega(U_2)\geqslant b+k,$$

and we can then take $M=\prod_{k\geqslant 0}M_k$. □

Proof of theorem 19.1. — If we choose some $c\geqslant c_1+2c_2+2c_3+1$, then there exists a finite extension L/K such that the cocyle U restricted to G_L has values in $\mathrm{GL}_d(c,\widetilde{\Omega})$. Corollary 19.3 then gives us a matrix $M_1\in\mathrm{GL}_d(c-c_1,\widetilde{\Omega}^{H_L})$ such that $U(h)=M_1\cdot h(M_1)^{-1}$ if $h\in H_L$ so that by theorem 7.1 (the inflation-restriction sequence), U comes by inflation from some cocycle on Γ_L with values in $\mathrm{GL}_d(c-c_1,\widetilde{\Omega}^{H_L})$.

Choose some $\gamma\in\Gamma_L$ such that $n=n(\gamma)\geqslant m(L)$ and let $U=U(\gamma)$ now so that $U\in\mathrm{GL}_d(2c_2+2c_3+1,\widetilde{\Omega}^{H_L})$. Corollary 19.5 gives us a matrix $M_2\in\mathrm{GL}_d(c_2+c_3+1,\widetilde{\Omega}^{H_L})$ such that $M_2^{-1}\cdot U\cdot\gamma(M_2)\in\mathrm{GL}_d(\Omega_{L,n})$. Let $M=M_1M_2$ and let $\tilde{U}:G_L\to\mathrm{GL}_d(\widetilde{\Omega})$ be the cocyle defined by $\tilde{U}(g)=M^{-1}\cdot U(g)\cdot g(M)$, so that $\tilde{U}$ is trivial on H_L and satisfies $U(g)\in\mathrm{GL}_d(\Omega_{L,n})$ if $g\in G_L$ and $n(\overline{g})\geqslant n$. The theorem is now proved if we replace L with L_n. □

Theorem 19.6. — *If W is a free $\widetilde{\Omega}$-module of rank d with an action of G_K then there exists a finite extension L of K and an $\Omega_{L,\infty}$-submodule $W_{L,\infty}$ of W^{H_L} which is free of rank d and stable under Γ_L and such that $W=\widetilde{\Omega}\otimes_{\Omega_{L,\infty}}W_{L,\infty}$.*

Proof. — If we choose a basis of W, then the map $c: g\mapsto\mathrm{Mat}(g)$ belongs to $H^1(G_K,\mathrm{GL}_d(\widetilde{\Omega}))$, and theorem 19.1 gives us a finite extension L of K and a basis of W whose elements belong to W^{H_L} and which generates an $\Omega_{L,\infty}$-submodule $W_{L,\infty}$ of W^{H_L} which is free of rank d and stable under Γ_L which proves the theorem. □

Proposition 19.7. — *If $\gamma\in\Gamma_L$ and $n\geqslant\max(n(\gamma),m(L))$ and $M_1\in\mathrm{GL}_{d_1}(c_3,\Omega_{L,n})$ and $M_2\in\mathrm{GL}_{d_2}(c_3,\Omega_{L,n})$ and if $B\in\mathrm{M}_{d_1\times d_2}(\widetilde{\Omega}^{H_L})$ is such that $BM_2=M_1\gamma(B)$, then $B\in\mathrm{M}_{d_1\times d_2}(\Omega_{L,n})$.*

Proof. — Let $C = B - R_{L,n}(B)$ so that C has coefficients in $X_{L,n}$ and $CM_2 = M_1\gamma(C)$. We have

$$\begin{aligned}\gamma(C) - C &= M_1^{-1}CM_2 - C \\ &= (M_1^{-1}-1)CM_2 + M_1^{-1}C(M_2-1) - (M_1^{-1}-1)C(M_2-1),\end{aligned}$$

so that $\mathrm{val}_\Omega(\gamma(C)-C) > \mathrm{val}_\Omega(C) + c_3$ which contradicts (CST3) unless $C = 0$ so that $C = 0$ and $B = R_{L,n}(B) \in \mathrm{M}_{d_1\times d_2}(\Omega_{L,n})$. □

Theorem 19.8. — *If W is a free $\widetilde{\Omega}$-module of rank d with an action of G_K and if L is a finite extension of K and if $W_{L,\infty}$ is an $\Omega_{L,\infty}$-submodule of W^{H_L} which is free of rank d and stable under Γ_L and such that $W = \widetilde{\Omega}\otimes_{\Omega_{L,\infty}} W_{L,\infty}$ and if $X_{L,\infty}$ is an $\Omega_{L,\infty}$-submodule of W^{H_L} which is free of finite rank and stable under Γ_L then $X_{L,\infty} \subset W_{L,\infty}$.*

Proof. — Since $W = \widetilde{\Omega}\otimes_{\Omega_{L,\infty}} W_{L,\infty}$ the space W has a basis of elements which belong to $W_{L,\infty}$. Let B be the matrix of a basis of $X_{L,\infty}$ in the chosen basis of $W_{L,\infty}$. If $\gamma \in \Gamma_L$ then $B\cdot \mathrm{Mat}_X(\gamma) = \mathrm{Mat}_W(\gamma)\cdot\gamma(B)$. We can choose γ close enough to 1 so that $\mathrm{val}_\Omega(\mathrm{Mat}_W(\gamma)-1) > c_3$ and $\mathrm{val}_\Omega(\mathrm{Mat}_X(\gamma)-1) > c_3$. If n is large enough, then $\mathrm{Mat}_W(\gamma)$ and $\mathrm{Mat}_X(\gamma)$ have coefficients in $\Omega_{L,n}$ and $n \geqslant \max(n(\gamma), m(L))$ so that proposition 19.7 applies and B has coefficients in $\Omega_{L,n} \subset \Omega_{L,\infty}$ and therefore $X_{L,\infty} \subset W_{L,\infty}$ which proves the theorem. □

This theorem implies in particular that the module $W_{L,\infty}$ constructed in theorem 19.6 is stable under G_K. Note that we would like theorem 19.6 to be true without having to take a finite extension L/K. This amounts to having $W_{L,\infty} = \Omega_{L,\infty}\otimes_{\Omega_{K,\infty}} W_{L,\infty}^{\mathrm{Gal}(L_\infty/K_\infty)}$ with $W_{L,\infty}^{\mathrm{Gal}(L_\infty/K_\infty)}$ free of rank d over $\Omega_{K,\infty}$. In practice, one can usually prove that this is true using Galois descent but this requires additional information which depends on the properties of $\widetilde{\Omega}$.

20. Example: Sen theory

References: [**BC08**] and [**Sen81**]. The first algebra $\widetilde{\Omega}$ to which we apply the methods of the previous section is $\widetilde{\Omega} = \mathbf{C}_p$. The theorem of Ax-Sen-Tate implies that $\widetilde{\Omega}^{H_K} = \hat{K}_\infty$ and the results of §10 tell us that $\widetilde{\Omega}$ satisifes the Colmez-Sen-Tate conditions, with the maps $R_{L,n}$ being the maps R_n from §10. In particular, if W is a semilinear $\mathbf{C}_p$-representation of G_K, then theorem 19.6 tells us that there exists a finite extension L of K such that $W = \mathbf{C}_p\otimes_{L_\infty} W_{L,\infty}$ where $W_{L,\infty} \subset W^{H_L}$ is stable under G_L. Furthermore, theorem 19.8 tells us that $W_{L,\infty}$ is stable under G_K. Hilbert's theorem 90 applied to the extension L_∞/K_∞ then implies that if we write $W_{K,\infty} = W_{L,\infty}^{H_K}$ then $W_{L,\infty} = L_\infty\otimes_{K_\infty} W_{K,\infty}$ so that

$W = \mathbf{C}_p \otimes_{K_\infty} W_{K,\infty}$ where $W_{K,\infty} \subset W^{H_K}$ is stable under G_K. It is customary to write $\mathrm{D}_{\mathrm{Sen}}(W)$ for $W_{K,\infty}$.

Let $e = \{e_1, \ldots, e_d\}$ be a basis of $\mathrm{D}_{\mathrm{Sen}}(W)$. If $\gamma \in \Gamma_K$ then for $n \gg 0$, $\mathrm{Mat}_e(\gamma) \in \mathrm{GL}_d(K_n)$ so that if we write $D_n = \oplus_{i=1}^d K_n \cdot e_i$ then for $n \gg 0$, D_n is stable under Γ_n which acts by K_n-linear operators. If $n \gg 0$ and $\gamma \in \Gamma_n$ then $\|1-\gamma\| < 1$ and the series which defines $\log(\gamma) = \log(1-(1-\gamma))$ converges to a K_n-linear operator on D_n. The map $\Theta_n = \log(\gamma)/\log_p \chi(\gamma)$ does not depend on the choice of γ and $\Theta_{n+1}|D_n = \Theta_n$. Since we have $\mathrm{D}_{\mathrm{Sen}}(W) = \cup_{n \gg 0} D_n$, these maps glue to a K_∞-linear map $\Theta_W : \mathrm{D}_{\mathrm{Sen}}(W) \to \mathrm{D}_{\mathrm{Sen}}(W)$ called the Sen operator. Its eigenvalues in $\overline{\mathbf{Q}}_p$ are called the Sen weights of W. This way we get a functor $W \mapsto (\mathrm{D}_{\mathrm{Sen}}(W), \Theta_W)$ from the category of $\mathbf{C}_p$-representations of G_K to the category of K_∞-vector spaces with a linear map.

Proposition 20.1. — *If W is a $\mathbf{C}_p$-representation of G_K then the characteristic polynomial of Θ_W on $\mathrm{D}_{\mathrm{Sen}}(W)$ has coefficients in K.*

Proof. — More generally, let $f : V \to V$ be a L-linear map which commutes with a group G of semilinear automorphisms of V. If $g \in G$, then $\mathrm{Mat}(f \circ g) = \mathrm{Mat}(f) \cdot \mathrm{Mat}(g)$ while $\mathrm{Mat}(g \circ f) = \mathrm{Mat}(g) \cdot g(\mathrm{Mat}(f))$ so that if $f \circ g = g \circ f$ then $g(\mathrm{Mat}(f))$ is conjugate to $\mathrm{Mat}(f)$ and they have the same characteristic polynomial. This implies that this polynomial has coefficients in L^G. The proposition follows from applying this to $\Theta_W : \mathrm{D}_{\mathrm{Sen}}(W) \to \mathrm{D}_{\mathrm{Sen}}(W)$ and $G = \Gamma_K$. □

Proposition 20.2. — *If W a $\mathbf{C}_p$-representation of G_K then the following conditions are equivalent:*

1. *W is isomorphic to $\mathbf{C}_p(h_1) \oplus \cdots \oplus \mathbf{C}_p(h_d)$ with $h_i \in \mathbf{Z}$;*
2. *Θ_W is semisimple with eigenvalues $h_1, \ldots, h_d \in \mathbf{Z}$.*

Proof. — The fact that (1) implies (2) is straightforward and we now prove that (2) implies (1). The formula $\Theta_V = \log(\gamma)/\log_p \chi(\gamma)$ implies that if $\mathrm{val}_p(\log_p \chi(\gamma)) \gg 0$, then we can write $\gamma = \exp(\log_p \chi(\gamma) \cdot \Theta_V)$. If $\mathrm{D}_{\mathrm{Sen}}(W)$ is as in (2) then we can write $\mathrm{D}_{\mathrm{Sen}}(W) = \oplus_{h \in \mathbf{Z}} \mathrm{D}_{\mathrm{Sen}}(W)^{\Theta_W = h}$ where each summand is stable under Γ_K. There exists then an open subgroup Γ_n of Γ_K such that $\gamma(e) = \chi(\gamma)^h e$ if $e \in \mathrm{D}_{\mathrm{Sen}}(W)^{\Theta_W = h}$ and $\gamma \in \Gamma_n$. Hilbert's theorem 90 implies that the semilinear K_∞-representation $\mathrm{D}_{\mathrm{Sen}}(W)^{\Theta_W = h}$ of Γ_K is isomorphic to $K_\infty(h)$. The formula $W = \mathbf{C}_p \otimes_{K_\infty} \mathrm{D}_{\mathrm{Sen}}(W)$ now implies (1). □

Suppose that W satisfies the conditions of proposition 20.2 and let $e_1, \ldots, e_d$ be a basis of W in which $g(e_i) = \chi(g)^{h_i} e_i$ so that $\mathrm{D}_{\mathrm{Sen}}(W) = \oplus_{i=1}^d K_\infty \cdot e_i$. Let $\mathrm{D}^n_{\mathrm{Sen}}(W) = \oplus_{i=1}^d K_n \cdot e_i$.

Proposition 20.3. — *If W is as above and $X \subset \mathrm{D}_{\mathrm{Sen}}(W)$ is a finite dimensional K_n-vector space stable under Γ_K and which has a basis on which Γ_n acts by integer powers of χ, then $X \subset \mathrm{D}^n_{\mathrm{Sen}}(W)$.*

Proof. — Suppose that $e_{d+1} \in \mathrm{D}_{\mathrm{Sen}}(W)$ satisfies $g(e_{d+1}) = \chi(g)^{h_{d+1}} e_{d+1}$ for all $g \in \Gamma_n$. The elements $e_1, \dots, e_{d+1}$ are linearly dependent in $\mathrm{D}_{\mathrm{Sen}}(W)$ so that we can write $\sum_{i=1}^{d+1} \lambda_i e_i = 0$ with $\lambda_i \in F_\infty$. We can assume that this relation has minimal length and then by letting Γ_n act we find that $\lambda_i/\lambda_j \in F_\infty^{\Gamma_n = \chi^{h_i - h_j}}$ which is either 0 or F_n. In any case, we find that $e_{d+1} \in \mathrm{D}^n_{\mathrm{Sen}}(W)$. □

If V is a representation of $G_{\mathbf{Q}_p}$ then we denote by $\mathrm{D}_{\mathrm{Sen}}(V)$ and Θ_V the invariants of $\mathbf{C}_p \otimes_{\mathbf{Q}_p} V$ constructed above. If $\mathbf{C}_p \otimes_{\mathbf{Q}_p} V$ satisfies the conditions of proposition 20.2, then we say that V is a Hodge-Tate representation, and its Hodge-Tate weights are the integers $h_1, \dots, h_d$.

21. Overconvergent elements

References: [**CC98**] and [**Col08**]. Recall that we defined the maps $w_k : \tilde{\mathbf{A}} \to \mathbf{R} \cup \{+\infty\}$ by $w_k(x) = \inf_{i \leqslant k} \mathrm{val}_{\mathbf{E}}(x_i)$ if $x = \sum_{i \geqslant 0} p^i [x_i]$. If $x \in \tilde{\mathbf{A}}$, then $w_k(x) = +\infty$ if and only if $x \in p^{k+1}\tilde{\mathbf{A}}$ and if $x, y \in \tilde{\mathbf{A}}$, then $w_k(x+y) \geqslant \inf(w_k(x), w_k(y))$ and $w_k(xy) \geqslant \inf_{i+j \leqslant k}(w_i(x) + w_j(y))$.

Lemma 21.1. — *If $r > 0$ and $s(r) = pr/(p-1)$ and if $x = \sum_{k \geqslant 0} p^k [x_k] \in \tilde{\mathbf{A}}$, then*

1. *$\mathrm{val}_{\mathbf{E}}(x_k) + k \cdot s(r) \to \infty$ if and only if $w_k(x) + k \cdot s(r) \to \infty$;*
2. *in this case, $\min_{k \geqslant 0}(\mathrm{val}_{\mathbf{E}}(x_k) + k \cdot s(r)) = \min_{k \geqslant 0}(w_k(x) + k \cdot s(r))$.*

Proof. — Let $s = s(r)$ and $v_k = \mathrm{val}_{\mathbf{E}}(x_k)$ and $w_k = w_k(x)$ so that $w_k = \min(v_0, \dots, v_k)$ and there exists an increasing function $i : \mathbf{Z}_{\geqslant 0} \to \mathbf{Z}_{\geqslant 0}$ such that $w_k = v_{i(k)}$ and $i(k) \leqslant k$.

Let us prove (1). Since $v_k \geqslant w_k$ one implication is obvious, so assume that $v_k + ks \to \infty$. If $\{i(k)\}_{k \geqslant 0}$ is bounded then $w_k \geqslant v_{i(k)} + ks \to \infty$ while if $i(k) \to \infty$ then $v_{i(k)} + i(k)s \to \infty$ and therefore so does $w_k + ks = v_{i(k)} + i(k)s + (k - i(k))s$.

Les us now prove (2). It is clear that $\min(v_k + ks) \geqslant \min(w_k + ks)$ and since $w_k + ks = v_{i(k)} + i(k)s + (k - i(k))s$ and $k - i(k) \geqslant 0$, we also have $w_k + ks \geqslant \min(v_i + is)$ which proves the reverse inequality. □

If $r > 0$ and $s(r) = pr/(p-1)$, let $\tilde{\mathbf{A}}^{\dagger, r}$ be the set of $x \in \tilde{\mathbf{A}}$ such that $w_k(x) + k \cdot s(r) \geqslant 0$ for all $k \geqslant 0$ and $w_k(x) + k \cdot s(r) \to \infty$ as $k \to \infty$. Note that $\tilde{\mathbf{A}}^+ \subset \tilde{\mathbf{A}}^{\dagger, r}$ for all $r > 0$.

Lemma 21.2. — *The set $\tilde{\mathbf{A}}^{\dagger,r}$ is a subring of $\tilde{\mathbf{A}}$ which is stable under the action of $G_{\mathbf{Q}_p}$ and such that $\varphi:\tilde{\mathbf{A}}^{\dagger,r}\to\tilde{\mathbf{A}}^{\dagger,pr}$ is a bijection.*

Proof. — The fact that $\tilde{\mathbf{A}}^{\dagger,r}$ is stable under $+$ and $\times$ follows from the inequalities for $w_k(x+y)$ and $w_k(xy)$ recalled above, and the assertions concerning the action of $G_{\mathbf{Q}_p}$ and φ follow from the formulas $w_k(g(x))=w_k(x)$ if $g\in G_{\mathbf{Q}_p}$ and $w_k(\varphi(x))=pw_k(x)$. □

Let $\widetilde{\mathbf{B}}^{\dagger,r}=\tilde{\mathbf{A}}^{\dagger,r}[1/p]$. If $x\in\tilde{\mathbf{A}}^{\dagger,r}$ then we set $\mathrm{V}(x,r)=\min_{k\geqslant 0}(w_k(x)+k\cdot s(r))$ which makes $\mathrm{V}(\cdot,r)$ into a function on $\tilde{\mathbf{A}}^{\dagger,r}$ which satisfies $\mathrm{V}(px,r)=s(r)+\mathrm{V}(x,r)$ so that we can extend $\mathrm{V}(\cdot,r)$ to $\widetilde{\mathbf{B}}^{\dagger,r}$.

Lemma 21.3. — *The function $\mathrm{V}(\cdot,r)$ satisifes the following properties:*

1. $\mathrm{V}(x,r)=\infty$ *if and only if* $x=0$;
2. $\mathrm{V}(x+y,r)\geqslant\min(\mathrm{V}(x,r),\mathrm{V}(y,r))$;
3. $\mathrm{V}(\varphi(x),pr)=p\cdot\mathrm{V}(x,r)$;
4. $\mathrm{V}(xy,r)=\mathrm{V}(x,r)+\mathrm{V}(y,r)$.
5. $\mathrm{V}(px,r)=s(r)+\mathrm{V}(x,r)$ *and* $\mathrm{V}([\alpha]x,r)=\mathrm{val}_{\mathbf{E}}(\alpha)+\mathrm{V}(x,r)$ *if* $\alpha\in\widetilde{\mathbf{E}}$.

Proof. — Items (1), (2) and (3) as well as the fact that $\mathrm{V}(xy,r)\geqslant\mathrm{V}(x,r)+\mathrm{V}(y,r)$ are straightforward consequences of the properties of the maps w_k. Let us now prove that $\mathrm{V}(xy,r)=\mathrm{V}(x,r)+\mathrm{V}(y,r)$. Let k be the smallest integer such that $\mathrm{val}_{\mathbf{E}}(x_k)+ks(r)=\mathrm{V}(x,r)$ and let ℓ be the corresponding integer for y. If we set $x_>=[x_0]+\cdots+p^{k-1}[x_{k-1}]$, then $x=x_>+p^k[x_k]+\cdots$ and likewise for y so that $xy=x_>(p^k[x_k]+\cdots)+y_>(p^\ell[x_\ell]+\cdots)+p^{k+\ell}[x_ky_\ell]+p^{k+\ell+1}z$. We have $\mathrm{V}(xy,r)=\mathrm{V}(p^{k+\ell}[x_ky_\ell]+p^{k+\ell+1}z)$ and since $w_{k+\ell}(p^{k+\ell}[x_ky_\ell]+p^{k+\ell+1}z)=\mathrm{val}_{\mathbf{E}}(x_k)+\mathrm{val}_{\mathbf{E}}(y_\ell)=\mathrm{V}(x,r)+\mathrm{V}(y,r)-(k+\ell)s(r)$, we see that $\mathrm{V}(xy,r)=\mathrm{V}(x,r)+\mathrm{V}(y,r)$. □

If $x=\sum p^k[x_k]\in\widetilde{\mathbf{B}}^+$, we also define $\mathrm{V}(x,0)=\inf_k\mathrm{val}_{\mathbf{E}}(x_k)$ and the above properties are still satisfied. Beware that $\tilde{\mathbf{A}}^{\dagger,r}$ is not the ring of integers of $\widetilde{\mathbf{B}}^{\dagger,r}$ for $\mathrm{V}(\cdot,r)$ (for example, if $r=(p-1)/p$ then $\mathrm{V}([\tilde{p}]/p,r)=0$). It is however true that $x\in\tilde{\mathbf{A}}^{\dagger,r}$ if and only if $x\in\widetilde{\mathbf{B}}^{\dagger,r}\cap\tilde{\mathbf{A}}$ and $\mathrm{V}(x,r)\geqslant 0$ and we have the following result.

Lemma 21.4. — *If $x=\sum_{k\gg-\infty}p^k[x_k]\in\widetilde{\mathbf{B}}^{\dagger,r}$ satisfies $\mathrm{V}(x,r)\geqslant 0$ and if we set $x^-=\sum_{k\geqslant 0}p^k[x_k]$ and $x^+=\sum_{k\leqslant -1}p^k[x_k]$ then $x^-\in\tilde{\mathbf{A}}^{\dagger,r}$ and $x^+\in\widetilde{\mathbf{B}}^+$ and $\mathrm{V}(x^\pm,u)\geqslant\mathrm{V}(x,u)$ for all $u\geqslant r$.*

Proof. — For each $k\in\mathbf{Z}$, we have $\mathrm{val}_{\mathbf{E}}(x_k)+ks(r)\geqslant 0$ so that $x^-\in\tilde{\mathbf{A}}^{\dagger,r}$ and if $k\leqslant -1$, then $x_k\in\widetilde{\mathbf{E}}^+$ and hence $x^+\in\widetilde{\mathbf{B}}^+$. The inequalities $\mathrm{V}(x^\pm,u)\geqslant\mathrm{V}(x,u)$ for all $u\geqslant r$ are straightforward consequences of the definition of $\mathrm{V}(\cdot,u)$. □

The function $\mathrm{V}(\cdot, r)$ defines a separated topology on $\tilde{\mathbf{A}}^{\dagger,r}$. Note that by property (4) above, if $x \in \tilde{\mathbf{A}}^{\dagger,r}$ and $a \in \widetilde{\mathbf{E}}^{+}$ with $\mathrm{val}_{\mathbf{E}}(a) \geqslant 0$, then $\mathrm{V}(x, r) \geqslant \mathrm{val}_{\mathbf{E}}(a)$ if and only if $x \in [a]\tilde{\mathbf{A}}^{\dagger,r}$.

Lemma 21.5. — *The ring $\tilde{\mathbf{A}}^{\dagger,r}$ is complete for the topology defined by $\mathrm{V}(\cdot, r)$.*

Proof. — Let $\{x_i\}_{i\geqslant 0}$ be a sequence of $\tilde{\mathbf{A}}^{\dagger,r}$ which converges to zero. We have $\mathrm{V}(x_i, r) \to +\infty$ so that for each $k \geqslant 0$, we have $w_k(x_i) \to +\infty$ and since $\tilde{\mathbf{A}}$ is complete for the weak topology by proposition 17.4, the series $\sum_{i=0}^{\infty} x_i$ converges to some $x \in \tilde{\mathbf{A}}$. Since $w_k(x_i) + ks(r) \geqslant 0$ for all i and k, the same is true for $w_k(x) + ks(r)$ so that $x \in \tilde{\mathbf{A}}^{\dagger,r}$ and given $C > 0$, there exists i_C such that $w_k(x_i) + ks(r) \geqslant 0$ for all $i \geqslant i_C$ and k so that $\sum_{i=0}^{\infty} x_i \to x$ for $\mathrm{V}(\cdot, r)$. □

Lemma 21.6. — *If $\{x_i\}_{i\geqslant 0}$ is a sequence of elements of $\tilde{\mathbf{A}}^{+}$ which converges to 0 for the weak topology and if $r > 0$, then $\mathrm{V}(x_i, r) \to \infty$.*

Proof. — If $M > 0$, let $k \geqslant 0$ be such that $ks(r) \geqslant M$. Since for each fixed j, $w_j(x_i) \to \infty$ as $i \to \infty$, there exists i_0 such that $w_j(x_i) \geqslant M$ if $0 \leqslant j \leqslant k-1$ and $i \geqslant i_0$. This and the fact that $w_\ell(x_i) \geqslant 0$ for all ℓ implies that if $i \geqslant i_0$ then $\mathrm{V}(x_i, r) \geqslant M$. □

Lemma 21.7. — *If $x \in \widetilde{\mathbf{B}}^{\dagger,r} \cap \tilde{\mathbf{A}}$ and $n \geqslant 0$ then $\varphi^{-n}(x) \in \widetilde{\mathbf{B}}^{\dagger,r} \cap \tilde{\mathbf{A}}$. Furthermore, if $\mathrm{V}(x, r) \geqslant 0$ then $\mathrm{V}(\varphi^{-n}(x), r) \geqslant 0$ and otherwise if $\delta > 0$ then $\mathrm{V}(\varphi^{-n}(x), r) \geqslant -\delta$ if $n \gg 0$.*

Proof. — If $x \in \widetilde{\mathbf{B}}^{\dagger,r} \cap \tilde{\mathbf{A}}$ and $n \geqslant 0$ then $\varphi^{-n}(x) \in \widetilde{\mathbf{B}}^{\dagger,r/p^n} \cap \tilde{\mathbf{A}}$ and we use the fact that $\widetilde{\mathbf{B}}^{\dagger,r/p^n} \subset \widetilde{\mathbf{B}}^{\dagger,r}$. If $x = \sum_{k\geqslant 0} p^k[x_k]$, then

$$\mathrm{V}(\varphi^{-n}(x), r) = \min_{k\geqslant 0}(p^{-n}\mathrm{val}_{\mathbf{E}}(x_k) + ks(r)) \geqslant p^{-n}\mathrm{V}(x, r),$$

from which the two inequalities follow. □

The rings defined above are all stable under the action of $G_{\mathbf{Q}_p}$. If K is a finite extension of $\mathbf{Q}_p$ then we set $\widetilde{\mathbf{B}}^{\dagger,r}_K = (\widetilde{\mathbf{B}}^{\dagger,r})^{H_K}$ and $\mathbf{B}^{\dagger,r} = \widetilde{\mathbf{B}}^{\dagger,r} \cap \mathbf{B}$ as well as $\mathbf{B}^{\dagger,r}_K = (\mathbf{B}^{\dagger,r})^{H_K} \subset \mathbf{B}_K$. We also have corresponding definitions for $\tilde{\mathbf{A}}^{\dagger,r}_K$ and $\mathbf{A}^{\dagger,r}$ and $\mathbf{A}^{\dagger,r}_K$.

Lemma 21.8. — *If $r \geqslant 1$ then $\pi/[\overline{\pi}]$ is a unit of $\tilde{\mathbf{A}}^{\dagger,r}_K$ and if in addition $r \in \mathbf{Z}$, then every $y \in \tilde{\mathbf{A}}^{\dagger,r}_K$ can be written as $y = \sum_{k\geqslant 0} y_k(p/\pi^r)^k$ where $y_k \in \tilde{\mathbf{A}}^{+}_K$ and $y_k \to 0$ for the weak topology.*

Proof. — By exercise 9 of section 14, we have $\pi = [\overline{\pi}] + \sum_{i\geqslant 1} p^i[\beta_i]$ with $\mathrm{val}_{\mathbf{E}}(\beta_i) \geqslant p^{1-i}/(p-1)$ so that $\pi/[\overline{\pi}] = 1 + z$ with $\mathrm{V}(z, r) > 0$ if $r \geqslant 1$ and then $\pi/[\overline{\pi}]$ is a unit of $\tilde{\mathbf{A}}^{\dagger,r}_K$.

If $y \in \tilde{\mathbf{A}}_K^{\dagger,r}$ then we can write $y = \sum_{k\geqslant 0} p^k[z_k]$ with $z_k \in \widetilde{\mathbf{E}}_K$ satisying $\mathrm{val}_{\mathbf{E}}(z_k)+ks(r) \geqslant 0$ and $\to \infty$ as $k \to \infty$ so that $y = \sum_{k\geqslant 0}(p/[\overline{\pi}^r])^k[\pi^r z_k]$ and $[\overline{\pi}^r z_k] \in \tilde{\mathbf{A}}_K^+$ and $\to 0$ for the weak topology. To prove the lemma, it is therefore enough to show that $p/[\overline{\pi}^r]$ can be written as $\sum_{k\geqslant 1} x_k(p/\pi^r)^k$ with $x_k \in \tilde{\mathbf{A}}_K^+$ and $x_k \to 0$ for the weak topology. We have

$$\frac{p}{[\overline{\pi}^r]} = \frac{p}{\pi^r}\frac{\pi^r}{[\overline{\pi}^r]} = \frac{p}{\pi^r}\left(1+\frac{p}{[\overline{\pi}^r]}\beta\right)^r = \frac{p}{\pi^r}\left(1+\frac{p}{[\overline{\pi}^r]}z\right),$$

where $\beta = \sum_{i\geqslant 1} p^{i-1}[\overline{\pi}^{r-1}\beta_i] \in (p,[\overline{\pi}])\tilde{\mathbf{A}}_K^+$ so that $p/[\overline{\pi}^r] = \sum_{k\geqslant 1} z^{k-1}(p/\pi^r)^k$. □

Corollary 21.9. — *If $r > 1$ and $a \in \mathbf{Z}_p^\times$, then $(1-[\varepsilon^a])/[\overline{\pi}]$ is a unit of $\tilde{\mathbf{A}}_K^{\dagger,r}$.*

Finally, note that if $s \geqslant r$, then $\widetilde{\mathbf{B}}^{\dagger,r} \subset \widetilde{\mathbf{B}}^{\dagger,s}$ and we let $\widetilde{\mathbf{B}}^\dagger = \cup_{r>0}\widetilde{\mathbf{B}}^{\dagger,r}$ which makes it into a subring of $\widetilde{\mathbf{B}}$ stable under φ and the action of $G_{\mathbf{Q}_p}$.

Lemma 21.10. — *The ring $\widetilde{\mathbf{B}}^\dagger$ is a field.*

Proof. — If $x = \sum_{k\geqslant k_0} p^k[x_k] \in \widetilde{\mathbf{B}}^\dagger$, then $x = p^{k_0}[x_{k_0}]y$ where $y = \sum_{k\geqslant 0} p^k[y_k]$ with $y_k = x_{k+k_0}/x_{k_0}$. Since $\widetilde{\mathbf{B}}^\dagger = \cup_{r>0}\widetilde{\mathbf{B}}^{\dagger,r}$ there exists $r > 0$ such that $y \in \widetilde{\mathbf{B}}^{\dagger,r}$ and hence $w_0(y) = 0$ and $w_k(y) + s(r)\cdot k \to \infty$. Possibly replacing r by a larger number, we can assume that $w_k(y) + s(r)\cdot k > 0$ for all $k \geqslant 1$ so that $y = 1+z$ with $\mathrm{V}(z,r) > 0$ and y is then invertible in $\tilde{\mathbf{A}}^{\dagger,r}$ by lemma 21.5. □

This implies that $\mathbf{B}^\dagger$ and hence $\mathbf{B}_K^\dagger$ are also fields. Recall that by proposition 17.3, the field $\mathbf{B}_K$ can be seen as the set of certain power series with bounded coefficients. By proposition 22.3 below, the field $\mathbf{B}_K^\dagger$ is the subfield of $\mathbf{B}_K$ consisting of elements $f(\pi_K)$ where $f(X)$ converges on some annulus of outer radius 1 and inner radius < 1, hence the name "overconvergent elements".

The last result of this chapter is a weak version of the statement that $\widetilde{\mathbf{B}}^\dagger$ is henselian inside $\widetilde{\mathbf{B}}$ (if you know what this means, you should also be able to prove it).

Proposition 21.11. — *If $P(X) \in \tilde{\mathbf{A}}^+[X]$ and $\overline{\alpha} \in \widetilde{\mathbf{E}}$ is such that $P(\overline{\alpha}) = 0$ and $P'(\overline{\alpha}) \neq 0$ in $\widetilde{\mathbf{E}}$, then there exists $r \gg 0$ and $\alpha \in \tilde{\mathbf{A}}^{\dagger,r}$ such that $P(\alpha) = 0$.*

Proof. — If $\beta_0 = [\overline{\alpha}]$, then $P(\beta_0)/P'(\beta_0)^2 \in \widetilde{\mathbf{B}}^\dagger \cap p\tilde{\mathbf{A}}$ so that there exists $r_0 > 0$ such that $P(\alpha_0)/P'(\alpha_0)^2 \in \tilde{\mathbf{A}}^{\dagger,r}$ and $\mathrm{V}(P(\alpha_0)/P'(\alpha_0)^2, r) > 0$ if $r \geqslant r_0$ (see exercise 3). Hensel's lemma (theorem 2.2) gives us $\alpha \in \tilde{\mathbf{A}}^{\dagger,r}$ such that $P(\alpha) = 0$ which proves the theorem. Note that the proof of theorem 2.2 shows directly that the image of α in $\widetilde{\mathbf{E}}$ is $\overline{\alpha}$. □

22. Overconvergent power series

References: [**CC98**] and [**Col08**].

Lemma 22.1. — *There exists $r(K) > 0$ and $\pi_K \in \mathbf{A}_K^{\dagger,r(K)}$ whose image $\overline{\pi}_K$ in $\mathbf{E}_K$ is a uniformizer and such that $\pi_K/[\overline{\pi}_K]$ is a unit.*

Proof. — Let $\overline{\pi}_K$ in $\mathbf{E}_K$ be a uniformizer and let $P(X) \in \mathbf{A}_{\mathbf{Q}_p}^+[X]$ be a monic polynomial whose reduction modulo p is the minimal polynomial of $\overline{\pi}_K$ over $\mathbf{E}_{\mathbf{Q}_p}$. Proposition 21.11 gives us a root $\pi_K \in \tilde{\mathbf{A}}^{\dagger,r}$ of $P(X)$ which lifts $\overline{\pi}_K$. Since $P(X) \in \mathbf{A}[X]$, we have $\pi_K \in \mathbf{B}$ and π_K is the desired element. Finally, $\pi_K/[\overline{\pi}_K]$ is a unit of $\mathbf{A}^{\dagger,r}$ if $r \gg 0$ which finishes the proof. □

The following result is an analogue of proposition 17.3; here e_K is the ramification index of K_∞/F_∞ so that $\mathrm{val}_{\mathbf{E}}(\overline{\pi}) = e_K \mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)$. If $s > 0$ and if L is a finite extension of $\mathbf{Q}_p$ then a power series $f(X) = \sum_{n\in\mathbf{Z}} a_n X^n$ with coefficients in $\mathcal{O}_L$ converges on $C[s;\infty[= \{X \in \mathbf{C}_p \text{ such that } 1/s \geqslant \mathrm{val}_p(X) > 0\}$ if and only if $\mathrm{val}_p(a_n) + n/s \to +\infty$. In addition,

$$\mathrm{val}_p \sup_{z\in C[s;\infty[} |f(z)|_p = \min(\min_{n\in\mathbf{Z}} \mathrm{val}_p(a_n) + n/s, \min_{n\in\mathbf{Z}} \mathrm{val}_p(a_n)).$$

Let $e_K = [K_\infty : F_\infty]$ and $C_K[r;\infty[= C[re_K;\infty[$.

Proposition 22.2. — *If $r > r(K)$ and $\pi_K \in \mathbf{A}_K^{\dagger,r}$ is as above, then $\mathbf{A}_K^{\dagger,r}$ is the set of $f(\pi_K)$ where $f(X)$ is a power series with coefficients in $\mathcal{O}_{K_0'}$ which converges and is bounded by 1 on $C_K[r;\infty[$.*

Proof. — If $f(X) = \sum_{n\in\mathbf{Z}} a_n X^n$ is such a power series, then $a_n\pi_K^n \in \mathbf{A}_K^{\dagger,r}$ and $\mathrm{V}(a_n\pi_K^n, r) \to \infty$ as $n \to \pm\infty$ so that the series $f(\pi_K)$ converges to an element of $\mathbf{A}_K^{\dagger,r}$.

Conversely by proposition 17.3, any element of $\mathbf{A}_K$ can be written as a power series $f(\pi_K) = \sum_{n\in\mathbf{Z}} a_n\pi_K^n$ with $a_n \in \mathcal{O}_{K_0'}$ and we need to show that if $f(\pi_K) \in \mathbf{A}_K^{\dagger,r}$ then $\mathrm{val}_p(a_n) + n/re_K \geqslant 0$ and $\to \infty$. It is enough to prove this assuming that $f(\pi_K) = \sum_{n\leqslant -1} a_n\pi_K^n$.

If $i \geqslant 0$, let $f_i^*(\pi_K) = p^{-i}\sum_{\mathrm{val}_p(a_n)=i} a_n\pi_K^n$ so that $f(\pi_K) = \sum_{i\geqslant 0} p^i f_i^*(\pi_K)$ and let n_i be the smallest of the n's such that $\mathrm{val}_p(a_n) = i$. We can write $f_i^*(\pi_K) = p^{-i}a_{n_i}\pi_K^{n_i}(1+\mathrm{O}(\pi_K))$ and therefore by lemma 22.1, $f_i^*(\pi_K) = [\overline{\pi}_K]^{n_i}u_i$ where u_i is a unit of $\tilde{\mathbf{A}}_K^{\dagger,r(K)}$.

If $k \geqslant 0$, then $w_k(f(\pi_K)) \geqslant \min_{0\leqslant i\leqslant k} w_k(p^i f_i^*(\pi_K))$ and since u_i is a unit of $\tilde{\mathbf{A}}_K^{\dagger,r(K)}$ we have

$$w_k(f(\pi_K)) \geqslant \min_{0\leqslant i\leqslant k} n_i \mathrm{val}_{\mathbf{E}}(\overline{\pi}_K) - (k-i)s(K),$$

where $s(K)=s(r(K))$ and in addition, we have $w_k(f(\pi_K))=n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)$ if $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)<\min_{0\leqslant i\leqslant k-1}n_i\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)-(k-i)s(K)$. The same inequalities are true with $s=s(r)$ instead of $s(K)$ since $s>s(K)$ so that

$$w_k(f(\pi_K))+ks\geqslant\min_{0\leqslant i\leqslant k}n_i\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+is,$$

with equality if $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+ks<\min_{0\leqslant i\leqslant k-1}n_i\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+is$. Since $w_k(f(\pi_K))+ks\geqslant 0$ for all k because $f(\pi_K)\in\mathbf{A}_K^{\dagger,r}$ we find (see exercise 4) that $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+ks\geqslant 0$ for all k. Going back to the stronger inequality, we get

$$w_k(f(\pi_K))+ks\geqslant\min_{0\leqslant i\leqslant k}n_i\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+is+(k-i)(s-s(K)),$$

with equality if $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+ks<\min_{0\leqslant i\leqslant k-1}n_i\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+is+(k-i)(s-s(K))$ and (see exercise 5) this tells us that $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+ks\to\infty$.

Since n_k is the smallest n such that $\mathrm{val}_p(a_n)=k$ and $\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)=p/((p-1)e_K)$, we have $n_k\mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)+ks\geqslant 0$ and $\to\infty$ if and only if $\mathrm{val}_p(a_n)+n/re_K\geqslant 0$ and $\to\infty$. □

Theorem 22.3. — *If $r>r(K)$ and $\pi_K\in\mathbf{A}_K^{\dagger,r}$ is as above, then the map $f(X)\mapsto f(\pi_K)$ from the set of power series with coefficients in K_0' which converge and are bounded on $C[re_K;\infty[$ to $\mathbf{B}_K^{\dagger,r}$ is an isomorphism.*

Corollary 22.4. — *If $r>r(K)$, then $\mathbf{B}_K^{\dagger,r}$ is a principal ideal domain.*

Proof. — This follows from theorem 22.3 and the results of §3. □

Corollary 22.5. — *The space $\mathbf{B}_K^{\dagger,r}$ is closed in $\widetilde{\mathbf{B}}^{\dagger,r}$.*

Proposition 22.6. — *If K is a finite extension of $\mathbf{Q}_p$ and if $r\gg 0$, then $\mathbf{B}_K^{\dagger,r}$ is a free $\mathbf{B}_{\mathbf{Q}_p}^{\dagger,r}$-module of rank $[K_\infty:F_\infty]$.*

Proof. — By Artin's lemma, the extension $\mathbf{B}_K^{\dagger}/\mathbf{B}_{\mathbf{Q}_p}^{\dagger}$ is of degree $d=[K_\infty:F_\infty]$ and if $e_1,\dots,e_d$ denotes a basis then there exists $r>0$ such that $e_i\in\mathbf{B}_K^{\dagger,r}$ so that $\mathbf{B}_K^{\dagger,r}$ contains $\oplus_{i=1}^d\mathbf{B}_{\mathbf{Q}_p}^{\dagger,r}e_i$ and is therefore free of rank $\geqslant d$ by corollary 22.4. By extending scalars from $\mathbf{B}_{\mathbf{Q}_p}^{\dagger,r}$ to $\mathbf{B}_{\mathbf{Q}_p}^{\dagger}$ we see that the rank is d. □

Exercises

1. Prove that $\cap_{r>0}\tilde{\mathbf{A}}^{\dagger,r}=\tilde{\mathbf{A}}^{+}$. What is $\cap_{r>0}\widetilde{\mathbf{B}}^{\dagger,r}$?
2. Prove that if $x\in\tilde{\mathbf{A}}^{\dagger,r}$ then $x\in\tilde{\mathbf{A}}^{\dagger,s}$ for all $s\geqslant r$ and that $s\mapsto\mathrm{V}(x,s)$ is an increasing function of s which is eventually equal to $w_0(x)$ if $w_0(x)\neq+\infty$.
3. Prove that if $x\in\widetilde{\mathbf{B}}^{\dagger}\cap p\tilde{\mathbf{A}}$ (so that $w_0(x)=+\infty$), then $x\in\tilde{\mathbf{A}}^{\dagger,r}$ for $r\gg 0$ and that the function $s\mapsto\mathrm{V}(x,s)$ is increasing and converges to $+\infty$.
4. Let $\{a_k\}_{k\geqslant 0}$ and $\{b_k\}_{k\geqslant 0}$ be two sequences of real numbers with $a_k\geqslant 0$ for all k, $a_0=b_0$ and $a_k=b_k$ if $b_k<\min_{0\leqslant i\leqslant k-1}b_i$. Prove that $b_k\geqslant 0$ for all k.

5. If $\lambda > 0$, let $\{a_k\}_{k\geqslant 0}$ and $\{b_k\}_{k\geqslant 0}$ be two sequences of $\mathbf{R}_{\geqslant 0}$ with $a_k \geqslant \min_{0\leqslant i\leqslant k} b_i + \lambda(k-i)$ for all k, $a_0 = b_0$ and $a_k = b_k$ if $b_k < \min_{0\leqslant i\leqslant k-1} b_i + \lambda(k-i)$. Prove that if $a_k \to \infty$, then $b_k \to \infty$.
6. Prove that if K is a finite extension of $\mathbf{Q}_p$ and $\mathbf{B}_K^+ = \mathbf{B}^+ \cap \mathbf{B}_K$, then $\mathbf{B}_K^+ = \mathbf{B}_{K_0'}^+$.

23. The action of Γ_K

References: [**CC98**] and [**Col08**]. We now study the action of Γ on $\mathbf{B}_K^{\dagger,r}$.

Lemma 23.1. — *If $\gamma \in \Gamma$ and $r \geqslant p^{n(\gamma)}$, then $\mathrm{V}(\gamma(\pi)-\pi, r) \geqslant p^{n(\gamma)}\mathrm{val}_{\mathbf{E}}(\overline{\pi})$.*

Proof. — If we write $\gamma(\pi)-\pi = \sum_{k\geqslant 0}[x_k]$, then the choice of r implies that $\mathrm{val}_{\mathbf{E}}(x_k) + ks(r) \geqslant p^{n(\gamma)}\mathrm{val}_{\mathbf{E}}(\overline{\pi})$ for all $k \geqslant 1$ so that it is enough to prove that $\mathrm{val}_{\mathbf{E}}(x_0) \geqslant p^{n(\gamma)}\mathrm{val}_{\mathbf{E}}(\overline{\pi})$. This follows from the fact that:

$$\begin{aligned}\gamma(\overline{\pi}) - \overline{\pi} &= (1+\overline{\pi})^{\chi(\gamma)} - (1+\overline{\pi}) \\ &= (1+\overline{\pi})(1+\overline{\pi}^{p^{n(\gamma)}} + \mathrm{O}(\overline{\pi}^{p^{n(\gamma)}+1})) - (1+\overline{\pi}) \in \overline{\pi}^{p^{n(\gamma)}}\widetilde{\mathbf{E}}^+.\end{aligned}$$

□

Proposition 23.2. — *If K is a finite extension of $\mathbf{Q}_p$ then there exists $m_0(K)$ and C_K such that if $\gamma \in \Gamma_K$ with $n(\gamma) \geqslant m_0(K)$ and $r \geqslant p^{n(\gamma)}$ then*

$$\mathrm{V}((1-\gamma)x, r) \geqslant \mathrm{V}(x,r) + p^{n(\gamma)}\mathrm{val}_{\mathbf{E}}(\overline{\pi}) - C_K$$

if $x \in \mathbf{B}_K^{\dagger,r}$.

Proof. — Choose some $r > r(K)$ and let $P(X) \in \mathbf{A}_{\mathbf{Q}_p}^+[\![X]\!]$ be the minimal polynomial of π_K over $\mathbf{A}_K^{\dagger,r}$ as in the proof of lemma 22.1 so that $\gamma(\pi)-\pi$ divides $P(\gamma(\pi_K)) - P(\pi_K)$. We have

$$P(\gamma(\pi_K)) = P(\pi_K) + (\gamma(\pi_K)-\pi_K)\left(P'(\pi_K) + \sum_{j\geqslant 2}(\gamma(\pi_K)-\pi_K)^{j-1}P^{[j]}(\pi_K)\right).$$

There exists $m_0(K)$ such that if $n(\gamma) \geqslant m_0(K)$ and $r \geqslant p^{n(\gamma)}$ then $\mathrm{V}(P'(\pi_K), r) = \mathrm{val}_{\mathbf{E}}(P'(\overline{\pi}_K))$ and $\mathrm{V}(\gamma(\pi_K)-\pi_K, r) > \mathrm{V}(P'(\pi_K), r)$. If this is the case, then the above equation tells us that $\mathrm{V}(\gamma(\pi_K)-\pi_K, r) \geqslant \mathrm{V}(\gamma(\pi)-\pi, r) - \mathrm{val}_{\mathbf{E}}(P'(\overline{\pi}_K))$.

If $x \in \mathbf{B}_K^{\dagger,r}$ then $x = x(\pi_K) = \sum_{n\in\mathbf{Z}} x_n \pi_K^n$ and we can write

$$x(\gamma(\pi_K)) - x(\pi_K) = \sum_{k\geqslant 1} x^{[k]}(\pi_K)\pi_K^k(\gamma(\pi_K)/\pi_K - 1)^k$$

so that $\gamma(x(\pi_K)) - x(\pi_K) = (\gamma(\pi_K)/\pi_K - 1)y(\pi_K)$ with $\mathrm{V}(y,r) \geqslant \mathrm{V}(x,r)$ which implies the result with $C_K = \mathrm{val}_{\mathbf{E}}(P'(\overline{\pi}_K)) + \mathrm{val}_{\mathbf{E}}(\overline{\pi}_K)$ by lemma 23.1. □

Proposition 23.3. — *There exists $m(K)$ such that if $\gamma\in\Gamma_K$ with $n(\gamma)\geqslant m(K)$ and $s\geqslant p^{n(\gamma)+1}$ and $1\leqslant i\leqslant p-1$, then*

1. *the map $1-\gamma:[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})\to[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})$ is invertible;*
2. *$\mathrm{V}((1-\gamma)^{-1}y,s)\geqslant\mathrm{V}(y,s)-p^{n(\gamma)}\mathrm{val}_{\mathbf{E}}(\overline{\pi})$ if $y\in[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})$.*

Proof. — Write $\chi(\gamma)=1+p^nu$ with $u\in\mathbf{Z}_p^\times$ so that $n=n(\gamma)$, and define $f:[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})\to[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})$ by $f(x)=x/(1-[\varepsilon^{p^niu}])$. By corollary 21.9, the element

$$\frac{1-[\varepsilon^{p^niu}]}{[\overline{\pi}]^{p^n}}=\varphi^n\left(\frac{1-[\varepsilon^{iu}]}{[\overline{\pi}]}\right)$$

is a unit of $\tilde{\mathbf{A}}_K^{\dagger,s}$ and therefore $\mathrm{V}(f(x),s)\geqslant\mathrm{V}(x,s)-p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})$.

A short computation shows that if $x=[\varepsilon]^i\varphi(z)$, then

$$x-f((1-\gamma)x)=\frac{[\varepsilon^{p^niu}]}{1-[\varepsilon^{p^niu}]}[\varepsilon]^i\varphi((\gamma(z)-z).$$

Since $z\in\mathbf{B}_K^{\dagger,s/p}$ and $s/p\geqslant p^{n(\gamma)}$, proposition 23.2 implies that $\mathrm{V}(\gamma(z)-z,s/p)\geqslant\mathrm{V}(z,s/p)+p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})-C_K$ so that

$$\begin{aligned}\mathrm{V}(x-f((1-\gamma)x),s)&\geqslant\mathrm{V}(\varphi(\gamma(z)-z),s)-p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})\\&\geqslant p\cdot\mathrm{V}(\gamma(z)-z,s/p)-p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})\\&\geqslant p\cdot\mathrm{V}(z,s/p)+p^{n+1}\mathrm{val}_{\mathbf{E}}(\overline{\pi})-pC_K-p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})\\&\geqslant\mathrm{V}(x,s)+p^n(p-1)\mathrm{val}_{\mathbf{E}}(\overline{\pi})-pC_K.\end{aligned}$$

If $y\in[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})$ and $p^n(p-1)\mathrm{val}_{\mathbf{E}}(\overline{\pi})-pC_K>0$, then the above inequality shows that the map $x\mapsto x-f((1-\gamma)x-y)$ is a contraction, and since $[\varepsilon]^i\varphi(\mathbf{B}_K^{\dagger,s/p})$ is complete for the topology defined by $\mathrm{V}(\cdot,s)$ by corollary 22.5, this map admits a unique fixed point $x=x(y)$ which then satifsfies $(1-\gamma)x=y$ and this proves (1). In addition, we have $\mathrm{V}(x,s)\geqslant\mathrm{V}(f(y))\geqslant\mathrm{V}(y,s)-p^n\mathrm{val}_{\mathbf{E}}(\overline{\pi})$, which proves (2). □

24. The CST conditions for overconvergent elements

Reference: [**Col08**]. In this section, we prove that if $r>0$, then the ring $\widetilde{\Omega}=\widetilde{\mathbf{B}}^{\dagger,r}$ satisfies the Colmez-Sen-Tate conditions with $\Omega_{K,n}=\varphi^{-n}(\mathbf{B}_K^{\dagger,p^nr})$ for $\mathrm{val}_\Omega=\mathrm{V}(\cdot,r)$ and for some maps $R_{K,n}:\widetilde{\mathbf{B}}_K^{\dagger,r}\to\varphi^{-n}(\mathbf{B}_K^{\dagger,p^nr})$ which we define below. To simplify the proofs, we assume that r is an integer $\geqslant1$ (it is enough to take $r=1$).

We start with condition (CST1) which is the easiest and is satisfied for any $c_1>0$.

Proposition 24.1. — *If $\delta>0$ and if L/K is a finite extension, then there exists $\alpha\in\widetilde{\mathbf{B}}_L^{\dagger,r}$ such that $\mathrm{V}(\alpha,r)>-\delta$ and $\mathrm{Tr}_{L_\infty/K_\infty}(\alpha)=1$.*

Proof. — On $\widetilde{\mathbf{E}}_L$ the map $\mathrm{Tr}_{L_\infty/K_\infty}(\cdot)$ coincides with $\mathrm{Tr}_{\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K}(\cdot)$ by proposition 15.2 and since $\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K$ is separable, there exists $\beta \in \widetilde{\mathbf{E}}_L$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(\beta) = 1$. Furthermore we can replace β with $\varphi^{-n}(\beta)$ and hence assume that $\mathrm{val}_{\mathbf{E}}(\beta)$ is as small as we wish. We have $\mathrm{Tr}_{L_\infty/K_\infty}([\beta]) = 1 + \sum_{k\geqslant 1} p^k[x_k]$ in $\tilde{\mathbf{A}}$ with $\mathrm{val}_{\mathbf{E}}(x_k) \geqslant \mathrm{val}_{\mathbf{E}}(\beta)$. If $\mathrm{val}_{\mathbf{E}}(\beta)$ is small enough, then $\mathrm{V}(\sum_{k\geqslant 1} p^k[x_k], r) > 0$ so that $1 + \sum_{k\geqslant 1} p^k[x_k]$ is a unit in $\tilde{\mathbf{A}}^{\dagger,r}$ and $\mathrm{V}([\beta], r) = \mathrm{val}_{\mathbf{E}}(\beta) > -\delta$ so that $\alpha = [\beta]/\mathrm{Tr}_{L_\infty/K_\infty}([\beta])$ will do. □

We now define the maps $R_{K,n}$. If $n \geqslant 0$, let $S_n = \{a/p^n \text{ with } 0 \leqslant a \leqslant p^n - 1\}$ so that S_n is a set of representatives for $p^{-n}\mathbf{Z}_p/\mathbf{Z}_p$ and let $S = \cup_{n\geqslant 0} S_n$ so that S is a set of representatives for $\mathbf{Q}_p/\mathbf{Z}_p$. Remark that if x belongs to a perfect ring and $i \in S$, then x^i is well defined. If $\{x_i\}_{i\in S}$ is a sequence indexed by S, we say that $x_i \to 0$ if for any open neighborhood U of 0, the set $\{i \in S \text{ such that } x_i \notin U\}$ is finite.

Lemma 24.2. — *Every $x \in \widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ can be written in a unique way as $x = \sum_{i\in S} \varepsilon^i a_i(x)$ where $a_i(x) \in \mathbf{E}_{\mathbf{Q}_p}$ and $a_i(x) \to 0$. In addition, $x \in \widetilde{\mathbf{E}}^+_{\mathbf{Q}_p}$ if and only if $a_i(x) \in \mathbf{E}^+_{\mathbf{Q}_p}$.*

Proof. — We have $\mathbf{E}^+_{\mathbf{Q}_p} = \mathbf{F}_p[\![\pi]\!]$ with $\pi = \varepsilon - 1$ so that every $x \in \varphi^{-n}(\mathbf{E}^+_{\mathbf{Q}_p})$ can be written as $\sum_{i\in S_n} \varepsilon^i a_i(x)$ with $a_i(x) \in \mathbf{E}^+_{\mathbf{Q}_p}$. The functions $a_i(\cdot)$ extend by linearity to $\varphi^{-n}(\mathbf{E}_{\mathbf{Q}_p})$ and if $k \in \mathbf{Z}$, then $x \in \pi^k \widetilde{\mathbf{E}}^+_{\mathbf{Q}_p}$ if and only if $a_i(x) \in \pi^k \mathbf{E}^+_{\mathbf{Q}_p}$ which implies

$$\mathrm{val}_{\mathbf{E}}(x) - \mathrm{val}_{\mathbf{E}}(\pi) < \min \mathrm{val}_{\mathbf{E}}(a_i(x)) \leqslant \mathrm{val}_{\mathbf{E}}(x)$$

so that the functions $x \mapsto a_i(x)$ are uniformly continuous on $\cup_{n\geqslant 0}\varphi^{-n}(\mathbf{E}_{\mathbf{Q}_p})$. By lemma 15.3, $\mathbf{E}^{\mathrm{rad}}_{\mathbf{Q}_p} = \cup_{n\geqslant 0}\varphi^{-n}(\mathbf{E}_{\mathbf{Q}_p})$ is dense in $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ so that the functions a_i extend to $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ and every $x \in \widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ can be written as $\sum_{i\in S} \varepsilon^i a_i(x)$ with $a_i(x) \in \mathbf{E}_{\mathbf{Q}_p}$ and $a_i(x) \to 0$.

Finally if $\sum_{i\in S} \varepsilon^i a_i = 0$ and if we set $x_n = \sum_{i\in S_n} \varepsilon^i a_i$ then $x_n \in \varphi^{-n}(\mathbf{E}_{\mathbf{Q}_p})$. Since $a_i = a_i(x_n)$ and $x_n \to 0$, we have $a_i = 0$ for all $i \in S$. □

Recall that by proposition 17.3, $\mathbf{A}_{\mathbf{Q}_p}$ is the p-adic completion of $\mathbf{Z}_p[\![\pi]\!][1/\pi]$ so that $\mathbf{A}^+_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p} \cap \tilde{\mathbf{A}}^+ = \mathbf{Z}_p[\![\pi]\!]$ and also $\varphi^{-n}(\mathbf{A}_{\mathbf{Q}_p}) = \oplus_{i\in S_n}[\varepsilon^i]\mathbf{A}_{\mathbf{Q}_p}$.

Corollary 24.3. — *Every $x \in \tilde{\mathbf{A}}_{\mathbf{Q}_p}$ can be written in a unique way as $x = \sum_{i\in S}[\varepsilon^i]a_i(x)$ where $a_i(x) \in \mathbf{A}_{\mathbf{Q}_p}$ and $a_i(x) \to 0$ for the weak topology. In addition, $x \in \tilde{\mathbf{A}}^+_{\mathbf{Q}_p}$ if and only if $a_i(x) \in \mathbf{A}^+_{\mathbf{Q}_p}$ for every $i \in S$.*

Proof. — If M denotes the set of $x = \sum_{i\in S}[\varepsilon^i]a_i(x)$ where $a_i(x) \in \mathbf{A}_{\mathbf{Q}_p}$ and $a_i(x) \to 0$ for the weak topology, then lemma 24.2 above shows that the map $M \to \tilde{\mathbf{A}}_{\mathbf{Q}_p}$ is bijective modulo p, and hence bijective. If M^+ denotes the set of $x = \sum_{i\in S}[\varepsilon^i]a_i(x)$ where $a_i(x) \in \mathbf{A}^+_{\mathbf{Q}_p}$ and $a_i(x) \to 0$ for the weak topology, then the same argument shows that $M^+ \to \tilde{\mathbf{A}}^+_{\mathbf{Q}_p}$ is bijective. □

If $x \in \tilde{\mathbf{A}}_{\mathbf{Q}_p}$ then corollary 24.3 shows that we can write $x = \sum_{i\in S}[\varepsilon^i]a_i(x)$ where $a_i(x) \in \mathbf{A}_{\mathbf{Q}_p}$ and $a_i(x) \to 0$. We then define maps $R_{\mathbf{Q}_p,n} : \tilde{\mathbf{A}}_{\mathbf{Q}_p} \to \varphi^{-n}(\mathbf{A}_{\mathbf{Q}_p})$ for $n \geqslant 0$ by $R_{\mathbf{Q}_p,n}(x) = \sum_{i\in S_n}[\varepsilon^i]a_i(x)$. These maps extend to $\widetilde{\mathbf{B}}_{\mathbf{Q}_p}$ by $\mathbf{Q}_p$-linearity.

Proposition 24.4. — *The map $R_{\mathbf{Q}_p,n} : \widetilde{\mathbf{B}}_{\mathbf{Q}_p} \to \varphi^{-n}(\mathbf{B}_{\mathbf{Q}_p})$ defined above is $\varphi^{-n}(\mathbf{B}_{\mathbf{Q}_p})$-linear and is the identity on $\varphi^{-n}(\mathbf{B}_{\mathbf{Q}_p})$. If $r \in \mathbf{Z}_{\geqslant 1}$, then:*

1. *$R_{\mathbf{Q}_p,n}(\tilde{\mathbf{A}}^{\dagger,r}_{\mathbf{Q}_p}) \subset \tilde{\mathbf{A}}^{\dagger,r}_{\mathbf{Q}_p}$;*
2. *if $y \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathbf{Q}_p}$ then $\mathrm{V}(R_{\mathbf{Q}_p,n}(y), r) \geqslant \mathrm{V}(y,r) - p/(p-1)$;*
3. *if $y \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathbf{Q}_p}$ then $\mathrm{V}(R_{\mathbf{Q}_p,n}(y) - y, r) \to +\infty$ as $n \to +\infty$.*

Proof. — The fact that $R_{\mathbf{Q}_p,n}$ is $\varphi^{-n}(\mathbf{B}_{\mathbf{Q}_p})$-linear and is the identity on $\varphi^{-n}(\mathbf{B}_{\mathbf{Q}_p})$ follows from the uniqueness in corollary 24.3.

If $y \in \tilde{\mathbf{A}}^{\dagger,r}_{\mathbf{Q}_p}$ then lemma 21.8 implies that we can write $y = \sum_{k\geqslant 0} y_k(p/\pi^r)^k$ where $y_k \in \tilde{\mathbf{A}}^{+}_{\mathbf{Q}_p}$ and $y_k \to 0$ for the weak topology. Item (1) then follows from the fact that $R_{\mathbf{Q}_p,n}(y) = \sum_{k\geqslant 0} R_{\mathbf{Q}_p,n}(y_k)(p/\pi^r)^k$ and the fact that $R_{\mathbf{Q}_p,n}(\tilde{\mathbf{A}}^{+}_{\mathbf{Q}_p}) \subset \tilde{\mathbf{A}}^{+}_{\mathbf{Q}_p}$ by corollary 24.3 and that $R_{\mathbf{Q}_p,n}$ is continuous for the weak topology.

If $y \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathbf{Q}_p}$ then since $\mathrm{V}(\pi, r) = p/(p-1)$, there exist $k, \ell \in \mathbf{Z}$ such that $p^k\pi^\ell y \in \tilde{\mathbf{A}}^{\dagger,r}_{\mathbf{Q}_p}$ and $0 \leqslant \mathrm{V}(p^k\pi^\ell y, r) < p/(p-1)$. We then have $R_{\mathbf{Q}_p,n}(p^k\pi^\ell y) \in \tilde{\mathbf{A}}^{\dagger,r}_{\mathbf{Q}_p}$ by (1) so that $\mathrm{V}(R_{\mathbf{Q}_p,n}(p^k\pi^\ell y), r) \geqslant 0$ which implies (2).

Finally (3) follows from the formula for $R_{\mathbf{Q}_p,n}$, the fact that $R_{\mathbf{Q}_p,n}(x) \to x$ for the weak topology if $x \in \tilde{\mathbf{A}}^{+}_{\mathbf{Q}_p}$ and lemma 21.6. □

If K is a finite extension of $\mathbf{Q}_p$ then Artin's lemma tells us that $\widetilde{\mathbf{B}}_K/\widetilde{\mathbf{B}}_{\mathbf{Q}_p}$ and $\mathbf{B}^\dagger_K/\mathbf{B}^\dagger_{\mathbf{Q}_p}$ are both finite extensions of degree $d = [K_\infty : F_\infty]$ and we choose a basis $e_1, \dots, e_d$ of $\mathbf{B}^\dagger_K$ over $\mathbf{B}^\dagger_{\mathbf{Q}_p}$.

Lemma 24.5. — *If $e_1, \dots, e_d$ is a basis of $\mathbf{B}^\dagger_K$ over $\mathbf{B}^\dagger_{\mathbf{Q}_p}$ and if $m \geqslant 0$, then $\varphi^{-m}(e_1), \dots, \varphi^{-m}(e_d)$ is a basis of $\widetilde{\mathbf{B}}_K$ over $\widetilde{\mathbf{B}}_{\mathbf{Q}_p}$.*

Proof. — We have a map $\mathbf{B}^\dagger_K \otimes_{\mathbf{B}^\dagger_{\mathbf{Q}_p}} \widetilde{\mathbf{B}}_{\mathbf{Q}_p} \to \widetilde{\mathbf{B}}_K$ and proposition 32.4 implies that this map is injective. It is then surjective by comparing dimensions, which proves the lemma for $m = 0$. The case $m \geqslant 0$ results from the fact that $\varphi : \widetilde{\mathbf{B}}_K \to \widetilde{\mathbf{B}}_K$ is a bijection. □

If $e_1^*, \dots, e_d^*$ denotes the dual basis and $m \geqslant 0$ and if $x \in \widetilde{\mathbf{B}}_K$ then $x = \sum_{i=1}^d x_i\varphi^{-m}(e_i^*)$ with $x_i = \mathrm{Tr}_{K_\infty/F_\infty}(x\varphi^{-m}(e_i))$. We then define $R_{K,n}(x) = \sum_{i=1}^d R_{\mathbf{Q}_p,n}(x_i)\varphi^{-m}(e_i^*)$ for $n \geqslant m$. A simple computation shows that the maps $R_{K,n}$ thus defined do not depend on the choice of the basis or on the choice of m and that $R_{K,n}(\widetilde{\mathbf{B}}_K) \subset \varphi^{-n}(\mathbf{B}_K)$. We can now prove that $\widetilde{\mathbf{B}}^{\dagger,r}$ satisfies condition (CST2). Let c_2 be any real number $> p/(p-1)$.

Proposition 24.6. — *The map $R_{K,n} : \widetilde{\mathbf{B}}_K \to \varphi^{-n}(\mathbf{B}_K)$ defined above is $\varphi^{-n}(\mathbf{B}_K)$-linear and is the identity on $\varphi^{-n}(\mathbf{B}_K)$. If $r \in \mathbf{Z}_{\geqslant 1}$, then there exists $n(K)$ such that if $n \geqslant n(K)$, then:*

1. *$R_{K,n}(\widetilde{\mathbf{B}}_K^{\dagger,r}) \subset \widetilde{\mathbf{B}}_K^{\dagger,r} \cap \varphi^{-n}(\mathbf{B}_K) = \varphi^{-n}(\mathbf{B}_K^{\dagger,p^n r})$;*
2. *if $y \in \widetilde{\mathbf{B}}_K^{\dagger,r}$ then $\mathrm{V}(R_{K,n}(y), r) \geqslant \mathrm{V}(y,r) - c_2$;*
3. *if $y \in \widetilde{\mathbf{B}}_K^{\dagger,r}$ then $\mathrm{V}(R_{K,n}(y) - y, r) \to +\infty$ as $n \to +\infty$.*

Proof. — The fact that $R_{K,n}$ is $\varphi^{-n}(\mathbf{B}_K)$-linear and is the identity on $\varphi^{-n}(\mathbf{B}_K)$ follows from the corresponding assertion in proposition 24.4 and we now prove the other ones.

If $e_1, \dots, e_d$ is a basis of $\mathbf{B}_K^{\dagger}$ over $\mathbf{B}_{\mathbf{Q}_p}^{\dagger}$ as above, then there exists $s > 0$ such that the e_i and e_i^* belong to $\mathbf{B}_K^{\dagger,s}$ and if $p^m r \geqslant s$, then $\varphi^{-m}(e_i) \in \varphi^{-m}(\mathbf{B}_K^{\dagger,p^m r}) \subset \widetilde{\mathbf{B}}_K^{\dagger,r}$ which implies (1) with $n(K) = m$. We can multiply the e_i's by $p^k \pi^\ell$ for suitable k and ℓ so that $\mathrm{V}(\varphi^{-m}(e_i), r) \geqslant 0$ and $e_i^* \in \tilde{\mathbf{A}}_K$. We then have $\mathrm{V}(\varphi^{-n}(e_i), r) \geqslant 0$ for all $n \geqslant m$ and furthermore if $\delta = c_2 - p/(p-1) > 0$ then $\mathrm{V}(\varphi^{-n}(e_i^*), r) \geqslant -\delta$ if $n \geqslant n(\delta)$ and we set $n(K) = \max(n(\delta), m)$. Items (2) and (3) then follow from these inequalities and the corresponding items in proposition 24.4. □

Note that by being a little more careful, we can prove proposition 24.6 above with any $c_2 > 0$. We finally prove that (CST3) holds. The main technical tool is proposition 23.3.

Proposition 24.7. — *There exists $c_3 > 0$ and $m(K) \geqslant n(K)$ such that if $\gamma \in \Gamma_K$ and $n \geqslant \max(n(\gamma), m(K))$, then*

1. *$1 - \gamma$ is invertible on $(1 - R_{K,n})\widetilde{\mathbf{B}}_K^{\dagger,r}$;*
2. *$\mathrm{V}((1-\gamma)^{-1}x, r) \geqslant \mathrm{V}(x,r) - c_3$ if $x \in (1 - R_{K,n})\widetilde{\mathbf{B}}_K^{\dagger,r}$.*

Proof. — Let $m(K) \geqslant n(K)$ be as in proposition 23.3. If $y \in \widetilde{\mathbf{B}}_K^{\dagger,r}$ and if $n \geqslant m(K)$, then by (3) of proposition 24.6, and using the fact that $S_m = S_{m-1} \sqcup \sqcup_{i=1}^{p-1} i p^{-m} + S_{m-1}$ for $m \geqslant 1$, we can write $y = R_{K,n}(y) + \sum_{m \geqslant n+1} \sum_{i=1}^{p-1} y_{m,i}$ where

$$y_{m,i} = [\varepsilon^{ip^{-m}}] R_{K,m-1}([\varepsilon^{-ip^{-m}}]y) \in \varphi^{-m}([\varepsilon]^i \varphi(\mathbf{B}_K^{\dagger, rp^{m-1}})),$$

and $\mathrm{V}(y_{m,i}, r) \geqslant \mathrm{V}(y,r) - c_2$ by (3) of proposition 24.6.

Choose some $\gamma \in \Gamma_K$ and assume that $n \geqslant n(\gamma) \geqslant m(K)$. Proposition 23.3 tells us that $1 - \gamma$ is invertible on $[\varepsilon]^i \varphi(\mathbf{B}_K^{\dagger, rp^{m-1}})$ and that

$$\mathrm{V}((1-\gamma)^{-1}\varphi^m(y_{m,i}), rp^m) \geqslant \mathrm{V}(\varphi^m(y_{m,i}), rp^m) - p^{n(\gamma)} \mathrm{val}_{\mathbf{E}}(\overline{\pi}),$$

so that

$$\mathrm{V}((1-\gamma)^{-1} y_{m,i}, r) \geqslant \mathrm{V}(y_{m,i}, r) - p^{n(\gamma)-m} \mathrm{val}_{\mathbf{E}}(\overline{\pi})$$

and then $(1-R_{K,n})(y)=(1-\gamma)\sum_{m\geqslant n+1}\sum_{i=1}^{p-1}(1-\gamma)^{-1}y_{m,i}$ which proves the proposition with $c_3=c_2+1/(p-1)+p^{-m(K)}C$. □

25. Overconvegent (φ,Γ)-modules

References: [**BC08**] and [**Col08**]. Using the fact that $\widetilde{\mathbf{B}}^{\dagger,r}$ satisfies the Colmez-Sen-Tate conditions, we get the following result.

Proposition 25.1. — *If V is a p-adic representation of G_K then there exists a finite extension L of K and $s(V)>0$ such that if $s\geqslant s(V)$, then $(\widetilde{\mathbf{B}}^{\dagger,s}\otimes_{\mathbf{Q}_p}V)^{H_L}$ admits a $\mathbf{B}_L^{\dagger,s}$-submodule $\mathrm{D}_L^{\dagger,s}$ which is free of rank d and stable under the action of G_K and such that $\widetilde{\mathbf{B}}^{\dagger,s}\otimes_{\mathbf{Q}_p}V=\widetilde{\mathbf{B}}^{\dagger,s}\otimes_{\mathbf{B}_L^{\dagger,s}}\mathrm{D}_L^{\dagger,s}$ and $\mathbf{B}_L^{\dagger}\otimes_{\mathbf{B}_L^{\dagger,s}}\mathrm{D}_L^{\dagger,s}\subset\widetilde{\mathbf{B}}^{\dagger}\otimes_{\mathbf{Q}_p}V$ is stable under φ.*

Proof. — If we set $\mathbf{B}_{L,\infty}^{\dagger,r}=\cup_{n\gg 0}\varphi^{-n}(\mathbf{B}_L^{\dagger,rp^n})$, then theorem 19.6 gives us a finite extension L of K and a $\mathbf{B}_{L,\infty}^{\dagger,r}$-module $\mathrm{D}_{L,\infty}^{\dagger,r}\subset(\widetilde{\mathbf{B}}^{\dagger,r}\otimes_{\mathbf{Q}_p}V)^{H_L}$ which is stable under the action of G_K and such that $\widetilde{\mathbf{B}}^{\dagger,r}\otimes_{\mathbf{Q}_p}V=\widetilde{\mathbf{B}}^{\dagger,r}\otimes_{\mathbf{B}_{L,\infty}^{\dagger,r}}\mathrm{D}_{L,\infty}^{\dagger,r}$.

If $e_1,\dots,e_d$ denote a basis of $\mathrm{D}_{L,\infty}^{\dagger,r}$ then there exists $n\gg 0$ such that the matrices of all $g\in G_K$ in that basis belong to $\mathrm{GL}_d(\varphi^{-n}(\mathbf{B}_L^{\dagger,rp^n}))$ so that the $\mathbf{B}_L^{\dagger,rp^n}$-submodule $\mathrm{D}_L^{\dagger,rp^n}$ of $(\widetilde{\mathbf{B}}^{\dagger,rp^n}\otimes_{\mathbf{Q}_p}V)^{H_L}$ generated by $\varphi^n(e_1),\dots,\varphi^n(e_d)$ is free of rank d and stable under the action of G_K.

Theorem 19.8 implies that $\mathrm{D}_{L,\infty}^{\dagger,rp^{n+1}}$ is generated by either $\varphi^n(e_1),\dots,\varphi^n(e_d)$ or by $\varphi^{n+1}(e_1),\dots,\varphi^{n+1}(e_d)$ so that the matrix of φ in the basis $\varphi^n(e_1),\dots,\varphi^n(e_d)$ has coefficients in $\mathbf{B}_{L,\infty}^{\dagger,rp^{n+1}}$ and for $m\gg 0$, the matrix of φ in the basis $\varphi^{n+m}(e_1),\dots,\varphi^{n+m}(e_d)$ has coefficients in $\mathbf{B}_L^{\dagger,rp^{n+m+1}}$. This proves the proposition with $s(V)=rp^{n+m+1}$ and $\mathrm{D}_L^{\dagger,s}$ the $\mathbf{B}_L^{\dagger,s}$-module generated by $\varphi^{n+m}(e_1),\dots,\varphi^{n+m}(e_d)$ if $s\geqslant s(V)$. □

If V is a p-adic representation, let $\mathrm{D}(V)$ be the (φ,Γ)-module associated to V.

Theorem 25.2. — *If V is a p-adic representation of G_K then the $\mathbf{B}_K^{\dagger}$-vector space $\mathrm{D}^{\dagger}(V)=(\mathbf{B}^{\dagger}\otimes_{\mathbf{Q}_p}V)^{H_K}$ is of dimension d and contains a basis of $\mathrm{D}(V)$.*

Proof. — Proposition 25.1 provides us with a finite extension L of K and a $\mathbf{B}_L^{\dagger}$-module $\mathrm{D}_L^{\dagger}=\mathbf{B}_L^{\dagger}\otimes_{\mathbf{B}_L^{\dagger,s}}\mathrm{D}_L^{\dagger,s}$ which is a (φ,Γ)-module over $\mathbf{B}_L^{\dagger}$. The $\mathbf{B}_L$-vector space $\mathrm{D}_L=\mathbf{B}_L\otimes_{\mathbf{B}_L^{\dagger}}\mathrm{D}_L^{\dagger}$ is then a (φ,Γ)-module over $\mathbf{B}_L$ and we have $\widetilde{\mathbf{B}}\otimes_{\mathbf{B}_L}\mathrm{D}_L=\widetilde{\mathbf{B}}\otimes_{\mathbf{Q}_p}V$ so that D_L is étale (consider the $\mathbf{A}_L$-lattice $\mathrm{D}_L\cap\tilde{\mathbf{A}}\otimes_{\mathbf{Z}_p}T$ where T is a lattice of V). By theorem 18.8, it comes from some p-adic representation W. Moreover, we have

$$W=(\mathbf{B}\otimes_{\mathbf{B}_L^{\dagger}}\mathrm{D}_L^{\dagger})^{\varphi=1}\subset(\widetilde{\mathbf{B}}\otimes_{\mathbf{Q}_p}V)^{\varphi=1}=V,$$

so that $W = V$ and $\mathrm{D}_L^\dagger \subset \widetilde{\mathbf{B}}^\dagger \otimes_{\mathbf{Q}_p} V \cap \mathbf{B} \otimes_{\mathbf{Q}_p} V = \mathbf{B}^\dagger \otimes_{\mathbf{Q}_p} V$. The space $\mathrm{D}_L^\dagger$ contains a basis of $\mathrm{D}_L(V) = (\mathbf{B} \otimes_{\mathbf{Q}_p} V)^{H_L}$ and so does $\mathrm{D}_L^\dagger(V) = (\mathbf{B}^\dagger \otimes_{\mathbf{Q}_p} V)^{H_L}$. This proves the theorem with L instead of K and to finish the proof, we use Galois descent.

Since $\mathbf{B}_K^\dagger = (\mathbf{B}_L^\dagger)^{\mathrm{Gal}(L_\infty/K_\infty)}$, the Galois group of $\mathbf{B}_L^\dagger/\mathbf{B}_K^\dagger$ is isomorphic to $\mathrm{Gal}(L_\infty/K_\infty)$ by Artin's lemma and Hilbert's theorem 90 implies that $H^1(\mathrm{Gal}(L_\infty/K_\infty), \mathrm{GL}_d(\mathbf{B}_L^\dagger)) = \{1\}$ so that $\mathrm{D}^\dagger(V) = \mathrm{D}_L^\dagger(V)^{H_K}$ is a $\mathbf{B}_K^\dagger$-vector space which is also a (φ, Γ)-module and satisfies $\mathrm{D}_L^\dagger(V) = \mathbf{B}_L^\dagger \otimes_{\mathbf{B}_K^\dagger} \mathrm{D}^\dagger(V)$ which proves the theorem. □

Corollary 25.3. — *The functor $V \mapsto \mathrm{D}^\dagger(V)$ defines an equivalence of categories:*

$$\{\mathbf{Q}_p\text{-linear representations of } G_K\} \to \{\text{étale } (\varphi, \Gamma)\text{-modules over } \mathbf{B}_K^\dagger\}.$$

Given theorem 18.8, one can also see the above equivalence of categories as a descent theorem, since it says that the functor $\mathrm{D}^\dagger \mapsto \mathbf{B}_K \otimes_{\mathbf{B}_K^\dagger} \mathrm{D}^\dagger$ gives rise to an equivalence of categories {étale (φ, Γ)-modules over $\mathbf{B}_K^\dagger$} $\to$ {étale (φ, Γ)-modules over $\mathbf{B}_K$}, and it is amusing that the corresponding equivalence is not true for mere φ-modules.

Proposition 25.4. — *If V is a p-adic representation of G_K then there exists $r(V)$ such that if $r \geqslant r(V)$, then the $\mathbf{B}_K^{\dagger,r}$-module $\mathrm{D}^{\dagger,r}(V) = (\mathbf{B}^{\dagger,r} \otimes_{\mathbf{Q}_p} V)^{H_K}$ is free of rank d and $\mathbf{B}^{\dagger,r} \otimes_{\mathbf{B}_K^{\dagger,r}} \mathrm{D}^{\dagger,r}(V) = \mathbf{B}^{\dagger,r} \otimes_{\mathbf{Q}_p} V$.*

Proof. — If $e_1, \dots, e_d$ is a basis of $\mathrm{D}^\dagger(V)$ over $\mathbf{B}^\dagger$ and $v_1, \dots, v_d$ is a basis of V, then there exists $r(V)$ such that the matrix of the e_i's in the v_j's belongs to $\mathrm{GL}_d(\mathbf{B}^{\dagger,r(V)})$. If $r \geqslant r(V)$, then $\mathrm{D}^{\dagger,r}(V)$ is the free $\mathbf{B}_K^{\dagger,r}$-module generated by $e_1, \dots, e_d$ and the result follows. □

Exercises

1. * Prove that if $\mathrm{D}^\dagger \subset \mathrm{D}(V)$ is a finite dimensional $\mathbf{B}_K^\dagger$-vector space stable under φ and Γ_K then $\mathrm{D}^\dagger \subset \mathrm{D}^\dagger(V)$.

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

Reference: [**Fon94a**]. Let $\widetilde{\mathbf{E}}^+$ be the ring constructed in chapter 14. Since $\widetilde{\mathbf{E}}^+$ is a perfect ring of characteristic p, we can construct $\tilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$ the ring of Witt vectors over $\widetilde{\mathbf{E}}^+$ and $\widetilde{\mathbf{B}}^+ = \tilde{\mathbf{A}}^+[1/p]$. Note that $\tilde{\mathbf{A}}^+ \subset \tilde{\mathbf{A}}$ and $\widetilde{\mathbf{B}}^+ \subset \widetilde{\mathbf{B}}$ so that they are endowed with the p-adic and the weak topology. The rings $\tilde{\mathbf{A}}^+$ and $\widetilde{\mathbf{B}}^+$ are both stable under the map φ and the action of $G_{\mathbf{Q}_p}$. Furthermore, one can apply the Witt vector constructions to the ring $A = \mathcal{O}_{\mathbf{C}_p}$ for which $\mathrm{Perf}(\mathcal{O}_{\mathbf{C}_p}/p) = \widetilde{\mathbf{E}}^+$ and we get a ring homomorphism $\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$ given by $\theta : \sum_{i \geqslant 0} p^i [x_i] \mapsto p^i x_i^{(0)}$. This map extends naturally to θ :

$\widetilde{\mathbf{B}}^+ \to \mathbf{C}_p$. By exercise 6 of the section on Witt vectors, θ is surjective. It is however not injective since for example $\theta([\varepsilon]-1)=0$.

Proposition 26.1. — *The kernel of $\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$ is a principal ideal generated by any element $y \in \tilde{\mathbf{A}}^+$ such that $\theta(y)=0$ and $\mathrm{val}_{\mathbf{E}}(\overline{y})=1$.*

Proof. — By reducing modulo p, the map θ becomes a map $\theta : \widetilde{\mathbf{E}}^+ \to \mathcal{O}_{\mathbf{C}_p}/p\mathcal{O}_{\mathbf{C}_p}$ (which is given by $x \mapsto x^{(0)} \bmod p$) and if $x \in \ker(\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p})$ then $\overline{x} \in \ker(\theta : \widetilde{\mathbf{E}}^+ \to \mathcal{O}_{\mathbf{C}_p}/p\mathcal{O}_{\mathbf{C}_p})$ so that $\mathrm{val}_{\mathbf{E}}(\overline{x}) \geqslant 1$ and $\overline{x}/\overline{y} \in \widetilde{\mathbf{E}}^+$ so that there exists $a \in \tilde{\mathbf{A}}^+$ such that $x - ay \in \ker(\theta) \cap p\tilde{\mathbf{A}}^+$. This implies that the inclusion map $y\tilde{\mathbf{A}}^+ \to \ker(\theta)$ is surjective modulo p and it is therefore surjective by Nakayama's lemma. □

The above proposition can be applied with $y=([\varepsilon]-1)/([\varepsilon^{1/p}]-1)$ (Fontaine's element ω) or with $y=[\tilde{p}]-p$ where $\tilde{p} \in \widetilde{\mathbf{E}}^+$ is any element such that $\tilde{p}^{(0)}=p$. Note that θ commutes with the action of $G_{\mathbf{Q}_p}$ but that $\ker(\theta)$ is not stable under φ, as for example $\theta(\varphi([\tilde{p}]-p))=p^p-p\neq 0$.

For $h \geqslant 1$, let $\mathbf{B}_h$ be the ring $\mathbf{B}_h = \widetilde{\mathbf{B}}^+/\ker(\theta)^h$. We have $\mathbf{B}_1=\mathbf{C}_p$ and for every $h \geqslant 1$, there is a surjective map $\mathbf{B}_{h+1} \to \mathbf{B}_h$. The ring $\mathbf{B}_{\mathrm{dR}}^+$ is defined as $\mathbf{B}_{\mathrm{dR}}^+ = \varprojlim_h \mathbf{B}_h$. Since $\mathbf{B}_{\mathrm{dR}}^+/\ker(\theta)=\mathbf{C}_p$ is a field and $\mathbf{B}_{\mathrm{dR}}^+$ is by definition complete for the $\ker(\theta)$-adic topology, any element $x \in \mathbf{B}_{\mathrm{dR}}^+$ such that $\theta(x)\neq 0$ is invertible. In particular, the kernel of $\theta : \mathbf{B}_{\mathrm{dR}}^+ \to \mathbf{C}_p$ is generated by $[\varepsilon]-1$.

If we let $t_h = ([\varepsilon]-1) - ([\varepsilon]-1)^2/2 + \cdots \pm ([\varepsilon]-1)^{h-1}/(h-1)$ then $t_h \in \mathbf{B}_h$ and the t_h form a compatible system of elements and therefore define an element

$$t = \sum_{k\geqslant 1} (-1)^{k-1} \frac{([\varepsilon]-1)^k}{k} \in \mathbf{B}_{\mathrm{dR}}^+.$$

Lemma 26.2. — *If $g \in G_{\mathbf{Q}_p}$ then $g(t)=\chi(g)t$.*

Proof. — If $F(X)=X-X^2/2+\cdots\pm X^{h-1}/(h-1)$, then $F(X) \equiv \log(1+X) \bmod X^h$ so that if $a \in \mathbf{Z}_p$ then $F((1+X)^a-1) \equiv aF(X) \bmod X^h$ in $\mathbf{Q}_p[\![X]\!]$. Since $t_h=F([\varepsilon]-1)$ and $g([\varepsilon])=[\varepsilon^{\chi(g)}]=(1+([\varepsilon]-1))^{\chi(g)}$, we have $g(t_h)=\chi(g)t_h$ in $\mathbf{B}_h$ and therefore $g(t)=\chi(g)t$. □

The element t has the property that $t/([\varepsilon]-1)$ is a unit in $\mathbf{B}_{\mathrm{dR}}^+$ so that the kernel of $\theta : \mathbf{B}_{\mathrm{dR}}^+ \to \mathbf{C}_p$ is also generated by t. Any element $x \in \mathbf{B}_{\mathrm{dR}}^+ \setminus \{0\}$ can then be written as $x=t^h x_0$ where $x_0 \in \mathbf{B}_{\mathrm{dR}}^+$ and $\theta(x_0)\neq 0$ so that $\mathbf{B}_{\mathrm{dR}}=\mathbf{B}_{\mathrm{dR}}^+[1/t]$ is a field. The structure theorem for local fields implies that $\mathbf{B}_{\mathrm{dR}} \simeq \mathbf{C}_p(\!(t)\!)$ as abstract fields. There is however no such isomorphism which is natural in any sense (see for instance exercise 3). We endow

$\mathbf{B}_{\mathrm{dR}}$ with the filtration $\mathrm{Fil}^h\mathbf{B}_{\mathrm{dR}} = t^h\mathbf{B}^+_{\mathrm{dR}}$. By proposition 26.2, this filtration is stable under the action of $G_{\mathbf{Q}_p}$.

Let us now define the natural topology on $\mathbf{B}^+_{\mathrm{dR}}$. For $h \geqslant 1$, we have a map $\tilde{\mathbf{A}}^+ \to \mathbf{B}_h$ whose image does not contain any $\mathbf{Q}_p$-line (since the image of $\tilde{\mathbf{A}}^+$ in $\mathbf{B}_1 = \mathbf{C}_p$ is $\mathcal{O}_{\mathbf{C}_p}$) and we define a valuation V_h on $\mathbf{B}_h$ by $V_h(x) = \sup\{n \in \mathbf{Z} \text{ such that } p^{-n}x \in \mathrm{im}(\tilde{\mathbf{A}}^+)\}$. Note that $\ker(\theta)^h$ is a closed subspace of $\tilde{\mathbf{B}}^+$ for the p-adic topology and that the norm defined by $V_h(\cdot)$ on $\tilde{\mathbf{B}}^+/\ker(\theta)^h$ is equivalent to the quotient norm. In particular, $\mathbf{B}_h$ is complete for $V_h(\cdot)$ and is therefore a Banach space. The space $\mathbf{B}^+_{\mathrm{dR}} = \varprojlim_h \mathbf{B}_h$ is then endowed with the structure of a Fréchet space, and this is the natural topology on $\mathbf{B}^+_{\mathrm{dR}}$. The topology on $\mathbf{B}_{\mathrm{dR}}$ is the inductive limit topology on $\mathbf{B}_{\mathrm{dR}} = \cup_{h\geqslant 1} t^{-h}\mathbf{B}^+_{\mathrm{dR}}$ which gives $\mathbf{B}_{\mathrm{dR}}$ the topology of an LF space. It is important to note that there is no such thing as a "p-adic topology" on $\mathbf{B}^+_{\mathrm{dR}}$. We now look at the action of $G_{\mathbf{Q}_p}$ on $\mathbf{B}_{\mathrm{dR}}$.

Proposition 26.3. — *Every non-constant polynomial $P(T) \in \mathbf{Q}_p[T]$ has a root in $\mathbf{B}^+_{\mathrm{dR}}$.*

Proof. — We can assume that $P(T)$ has simple roots. Since $\mathbf{C}_p$ is algebraically closed, there exists $\overline{y} \in \mathbf{C}_p$ such that $P(\overline{y}) = 0$ and since $\mathbf{B}^+_{\mathrm{dR}}/t\mathbf{B}^+_{\mathrm{dR}} = \mathbf{C}_p$, there exists $y \in \mathbf{B}^+_{\mathrm{dR}}$ such that $P(y) \in t\mathbf{B}^+_{\mathrm{dR}}$. Suppose that we have $y_h \in \mathbf{B}^+_{\mathrm{dR}}$ such that $P(y_h) \in t^h\mathbf{B}^+_{\mathrm{dR}})$. We then have $P(y_h + t^h z) = P(y_h) + t^h z P'(y_h) + \mathrm{O}(t^{h+1})$. Since $P(T)$ has simple roots, $P'(y_h) \neq 0$ and therefore there exists $y_{h+1} \equiv y_h \bmod t^h$ such that $P(y_h) \in t^h\mathbf{B}^+_{\mathrm{dR}})$. The sequence $\{y_h\}_{h\geqslant 1}$ converges to $y \in \mathbf{B}^+_{\mathrm{dR}}$ such that $P(y) = 0$. □

Every non-constant polynomial $P(T) \in \mathbf{Q}_p[T]$ therefore admits $\deg(P)$ roots in $\mathbf{B}^+_{\mathrm{dR}}$ so that for every $x \in \overline{\mathbf{Q}}_p$ we can find a well defined $\tilde{x} \in \mathbf{B}^+_{\mathrm{dR}}$ such that $\theta(\tilde{x}) = x$.

Corollary 26.4. — *We have a $G_{\mathbf{Q}_p}$-equivariant inclusion $\overline{\mathbf{Q}}_p \subset \mathbf{B}^+_{\mathrm{dR}}$ compatible with the map θ.*

Note that by a theorem of Colmez (see the appendix to [**Fon94a**]), $\overline{\mathbf{Q}}_p$ is actually dense in $\mathbf{B}^+_{\mathrm{dR}}$.

Proposition 26.5. — *If K is a finite extension of $\mathbf{Q}_p$ then $\mathbf{B}_{\mathrm{dR}}^{G_K} = K$.*

Proof. — If $h \in \mathbf{Z}$, then we have an 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 by taking G_K-invariants we find

$$0 \to (t^{h+1}\mathbf{B}^+_{\mathrm{dR}})^{G_K} \to (t^h\mathbf{B}^+_{\mathrm{dR}})^{G_K} \to \mathbf{C}_p(h)^{G_K},$$

and $\mathbf{C}_p(h)^{G_K} = \{0\}$ unless $h = 0$ by theorem 13.1. If we apply this to $h \ll 0$ and go up, we find that $\mathbf{B}_{\mathrm{dR}}^{G_K} = (\mathbf{B}^+_{\mathrm{dR}})^{G_K}$. If we apply it to $h = 1$ and go up, we find that for any $h \geqslant 1$, the map $(t^h\mathbf{B}^+_{\mathrm{dR}})^{G_K} \to (t\mathbf{B}^+_{\mathrm{dR}})^{G_K}$ is an isomorphism so that $(t\mathbf{B}^+_{\mathrm{dR}})^{G_K} = \{0\}$.

Finally if we take $h=0$, then we find that the map $(\mathbf{B}^+_{\mathrm{dR}})^{G_K}\to\mathbf{C}_p^{G_K}$ is injective. Since $\mathbf{C}_p^{G_K}=K$ by theorem 5.3 (Ax-Sen-Tate's theorem) and $K\subset\mathbf{B}^+_{\mathrm{dR}}$ by corollary 26.4, the map $(\mathbf{B}^+_{\mathrm{dR}})^{G_K}\to K$ is an isomorphism. □

27. The ring $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ and its subrings

Reference: [**Ber02**]. If $s\geqslant r$ then we define a valuation $\mathrm{V}(\cdot,[r;s])$ on $\widetilde{\mathbf{B}}^{\dagger,r}$ (or on $\widetilde{\mathbf{B}}^+$ if $r=0$) by

$$\mathrm{V}(f,[r;s])=\min(\mathrm{V}(f,r),\mathrm{V}(f,s)),$$

so that $\mathrm{V}(f,[r;s])=\min_{u\in[r;s]}\mathrm{V}(f,u)$. Let $\widetilde{\mathbf{B}}_{[r;s]}$ denote the completion of $\widetilde{\mathbf{B}}^{\dagger,r}$ (or $\widetilde{\mathbf{B}}^+$ if $r=0$) for $\mathrm{V}(\cdot,[r;s])$ and let $\tilde{\mathbf{A}}_{[r;s]}$ denote the ring of integers of $\widetilde{\mathbf{B}}_{[r;s]}$ for $\mathrm{V}(\cdot,[r;s])$. Note that $\tilde{\mathbf{A}}_{[r;s]}$ is also the p-adic completion of $\{x\in\widetilde{\mathbf{B}}^{\dagger,r}\text{ with }\mathrm{V}(x,[r;s])\geqslant 0\}$. The action of $G_{\mathbf{Q}_p}$ extends to the rings $\tilde{\mathbf{A}}_{[r;s]}$ and $\widetilde{\mathbf{B}}_{[r;s]}$ and the frobenius gives a bijective map $\varphi:\tilde{\mathbf{A}}_{[r;s]}\to\tilde{\mathbf{A}}_{[pr;ps]}$. In particular, the rings $\tilde{\mathbf{A}}_{[0;r]}$ and $\widetilde{\mathbf{B}}_{[0;r]}$ are stable under φ which is injective on them.

Definition 27.1. — If $r_0=(p-1)/p$ then the ring $\tilde{\mathbf{A}}_{[0;r_0]}$ is also denoted by $\mathbf{A}_{\max}$ and the ring $\widetilde{\mathbf{B}}_{[0;r_0]}$ is also denoted by $\mathbf{B}^+_{\max}$.

Lemma 27.2. — *Every element of $\tilde{\mathbf{A}}_{[r_0;r_0]}$ can be written as $\sum_{j\in\mathbf{Z}}a_j([\tilde{p}]/p)^j$ where $a_j\to 0$ (p-adically) as $j\to\pm\infty$ and likewise every element of $\tilde{\mathbf{A}}_{[0;r_0]}$ can be written as $\sum_{j\geqslant 0}a_j([\tilde{p}]/p)^j$ where $a_j\to 0$ (p-adically) as $j\to+\infty$.*

Proof. — If $x=\sum_{k\geqslant 0}p^k[x_k]\in\tilde{\mathbf{A}}^{\dagger,r_0}$ then $\mathrm{V}(x,r_0)=\inf_k(\mathrm{val}_{\mathbf{E}}(x_k)+k)$ so that the ring of integers of $\widetilde{\mathbf{B}}^{\dagger,r_0}$ for $\mathrm{V}(\cdot,r_0)$ is the set of $x=\sum_{k\gg-\infty}p^k[x_k]$ such that $\mathrm{val}_{\mathbf{E}}(x_k)+k\geqslant 0$ for all k. The ring $\tilde{\mathbf{A}}^+[p/[\tilde{p}],[\tilde{p}]/p]$ is dense in this ring of integers of $\widetilde{\mathbf{B}}^{\dagger,r_0}$ and the valuation $\mathrm{V}(\cdot,r_0)$ is equivalent to $\mathrm{val}_p(\cdot)$ which proves the first statement of the lemma. The second statement is proved in an analogous way. □

The set of valuations $\{\mathrm{V}(\cdot,[r;s])\}_{s\geqslant r}$ defines a Fréchet topology on $\widetilde{\mathbf{B}}^{\dagger,r}$ and we denote by $\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ the completion of $\widetilde{\mathbf{B}}^{\dagger,r}$ for that topology. The ring $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ is then defined by $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}=\cup_{r\geqslant 0}\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$. The completion of $\widetilde{\mathbf{B}}^+$ for the set of valuations $\{\mathrm{V}(\cdot,r)\}_{r\geqslant 0}$ is denoted by $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ so that if $r_n=p^{n-1}(p-1)$, then we have $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}=\cap_{n\geqslant 1}\widetilde{\mathbf{B}}_{[0;r_n]}=\cap_{n\geqslant 1}\varphi^n(\mathbf{B}^+_{\max})$. The ring $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ is a subring of $\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ for every $r>0$, which is stable under the frobenius φ of $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ and under the action of $G_{\mathbf{Q}_p}$ and on which φ is bijective.

Lemma 27.3. — *If $r>0$, then $\cap_{n\geqslant 1}\tilde{\mathbf{A}}^+ + p^{n-1}\tilde{\mathbf{A}}_{[0;r]}=\tilde{\mathbf{A}}^+$.*

Proof. — Suppose that $y = y_n + p^{n-1}z_n$ with $y_n \in \tilde{\mathbf{A}}^+$ and $z_n \in \tilde{\mathbf{A}}_{[0;r]}$ for all $n \geqslant 1$. We then have $y_{n+1} - y_n \in p^{n-1}\tilde{\mathbf{A}}_{[0;r]}$ so that $\mathrm{V}(y_{n+1} - y_n, r) \to \infty$. This implies that for each k, we have $w_k(y_{n+1} - y_n) \to \infty$ and hence $\{y_n\}_{n\geqslant 0}$ is Cauchy for the weak topology. Since $\tilde{\mathbf{A}}^+$ is complete for that topology, we have $y \in \tilde{\mathbf{A}}^+$. □

Lemma 27.4. — *We have* $(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})^{\varphi=1} = \mathbf{Q}_p$ *while* $(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})^{\varphi=p^{-n}} = \{0\}$ *if* $n \geqslant 1$.

Proof. — If $y \in \tilde{\mathbf{A}}_{[0;r_0]}$, then lemma 27.2 shows that we can write $y = \sum_{j\geqslant 0} a_j([\tilde{p}]/p)^j$ and if $y = \varphi^n(y)$, then $y = \sum_{j\geqslant 0} \varphi^n(a_j)([\tilde{p}^{p^n}]/p)^j$ so that $y \in \tilde{\mathbf{A}}^+ + p^m\tilde{\mathbf{A}}_{[0;r_0]}$ for all $m \geqslant 0$ and $y \in \tilde{\mathbf{A}}^+$ by lemma 27.3. This shows that $\tilde{\mathbf{A}}^{\varphi=1}_{[0;r_0]} = (\tilde{\mathbf{A}}^+)^{\varphi=1} = \mathbf{Z}_p$ which proves that $(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})^{\varphi=1} = \mathbf{Q}_p$.

If $y \in (\tilde{\mathbf{A}}_{[0;r_0]})^{\varphi=p^{-n}}$ then $y = p^{kn}\varphi^k(y) \in p^{kn}\tilde{\mathbf{A}}_{[0;r_0]}$ for all $k \geqslant 0$ so that $y = 0$. □

A much more general statement is proved in exercise 2.

Exercises

1. Suppose that $s \geqslant r$ and that $x \in \widetilde{\mathbf{B}}^{\dagger;r}_{\mathrm{rig}}$ and let $0 \leqslant \lambda \leqslant 1$. Prove the analogue of Hadamard's "three circles theorem": $\mathrm{V}(x, \lambda r + (1-\lambda)s) \geqslant \lambda \mathrm{V}(x,r) + (1-\lambda)\mathrm{V}(x,s)$.
2. Prove that if $r > 0$ and $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ is such that $\mathrm{V}(\varphi^{-n}(y), r) \geqslant 0$ for all $n \geqslant 0$, then $y \in \widetilde{\mathbf{B}}^+$.
3. Prove that if $t = \log(1+\pi)$, then $\mathrm{V}(t,r) \sim -r\log r$.

28. Embeddings into $\mathbf{B}_{\mathrm{dR}}$

Reference: [**Ber02**] and [**Col02**]. If $x \neq 0 \in \widetilde{\mathbf{E}}^+$ then $[x] \in \mathbf{B}^+_{\mathrm{dR}}$ and $\theta([x]) \neq 0$ so that $[x]$ is invertible in $\mathbf{B}^+_{\mathrm{dR}}$ and hence if $y \neq 0 \in \widetilde{\mathbf{E}}$, then $[y]$ makes sense in $\mathbf{B}^+_{\mathrm{dR}}$. If $x = \sum_{k\gg -\infty} p^k[x_k] \in \widetilde{\mathbf{B}}$, the latter series does not necessarily converge in $\mathbf{B}^+_{\mathrm{dR}}$ but it does so if the x_k's do not grow too fast.

Proposition 28.1. — *If* $\{x_k\}_{k\gg-\infty}$ *is a sequence of elements of* $\widetilde{\mathbf{E}}$*, then the series* $\sum_{k\gg-\infty} p^k[x_k]$ *converges in* $\mathbf{B}^+_{\mathrm{dR}}$ *if and only if* $\mathrm{val}_{\mathbf{E}}(x_k) + k \to \infty$ *as* $k \to \infty$*. The resulting map* $\iota_0 : \widetilde{\mathbf{B}}^{\dagger,r_0} \to \mathbf{B}^+_{\mathrm{dR}}$ *is uniformly continuous for the* $\mathrm{V}(\cdot, r_0)$*-adic topology.*

Proof. — If the series $\sum_{k\gg-\infty} p^k[x_k]$ converges in $\mathbf{B}^+_{\mathrm{dR}}$ then the series $\sum_{k\gg-\infty} p^k\theta([x_k])$ converges in $\mathbf{C}_p$ so that $k + \mathrm{val}_p(x_k^{(0)}) \to \infty$ as $k \to \infty$ and the first implication results from the fact that $\mathrm{val}_p(x_k^{(0)}) = \mathrm{val}_{\mathbf{E}}(x_k)$.

Conversely if $\ell \in \mathbf{Z}$, then in $\mathbf{B}_h$ we have

$$\begin{aligned}\left(\frac{p}{[\tilde{p}]}\right)^{\ell} &= \left(1+\left(\frac{[\tilde{p}]}{p}-1\right)\right)^{-\ell}\\ &= 1+\binom{-\ell}{1}\left(\frac{[\tilde{p}]}{p}-1\right)+\cdots+\binom{-\ell}{h-1}\left(\frac{[\tilde{p}]}{p}-1\right)^{h-1}\\ &\in p^{-(h-1)}\tilde{\mathbf{A}}^{+},\end{aligned}$$

so that if $\mathrm{val}_{\mathbf{E}}(x_k)+k \to \infty$ as $k \to \infty$, then $p^k[x_k] \to 0$ in $\mathbf{B}_h$ for all $h \geqslant 1$ and hence the series converges in $\mathbf{B}_{\mathrm{dR}}^{+}$. This also shows that the integers of $\widetilde{\mathbf{B}}^{\dagger,r_0}$ for $\mathrm{V}(\cdot,r_0)$ are mapped to $p^{-(h-1)}\tilde{\mathbf{A}}^{+} \subset \mathbf{B}_h$ which implies that the resulting map is uniformly continuous. □

Let K be a finite extension of $\mathbf{Q}_p$. We first extend the map $\theta : \widetilde{\mathbf{B}}^{+} \to \mathbf{C}_p$ to a map $\theta : K \otimes_{K_0} \widetilde{\mathbf{B}}^{+} \to \mathbf{C}_p$ in the natural way. Note that if π_K is a uniformizer of K, then every element of $\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+}$ can be written as $\sum_{i\geqslant 0} \pi_K^i[x_i]$ in a unique way. By mimicking the proof of proposition 26.1, we see that the kernel of $\theta : \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+} \to \mathcal{O}_{\mathbf{C}_p}$ is generated by any element y such that $\theta(y)=0$ and $\mathrm{val}_{\mathbf{E}}(\overline{y}) = \mathrm{val}_p(\pi_K)$, in particular $y = [\tilde{\pi}_K]-\pi_K$. Since $K \subset \mathbf{B}_{\mathrm{dR}}^{+}$ we have an map $K \otimes_{K_0} \widetilde{\mathbf{B}}^{+} \to \mathbf{B}_{\mathrm{dR}}^{+}$.

Lemma 28.2. — *The natural map $K \otimes_{K_0} \widetilde{\mathbf{B}}^{+} \to \mathbf{B}_{\mathrm{dR}}^{+}$ in injective.*

Proof. — It is enough to prove that the natural map $\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+} \to \mathbf{B}_{\mathrm{dR}}^{+}$ in injective. This map is given by gluing all the maps $\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+} \to \mathbf{B}_h$ and by the above discussion its kernel is $\cap_{h\geqslant 1}([\tilde{\pi}_K]-\pi_K)^h \cdot \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+} = \{0\}$. □

Since the map $\theta : K \otimes_{K_0} \widetilde{\mathbf{B}}^{+} \subset \mathbf{B}_{\mathrm{dR}}^{+} \to \mathbf{C}_p$ is a continuous surjective map between Banach spaces over K, there exists a K-linear continuous section $s : \mathbf{C}_p \to K \otimes_{K_0} \widetilde{\mathbf{B}}^{+}$ of θ such that $s(\mathcal{O}_{\mathbf{C}_p}) \subset \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+}$.

Proposition 28.3. — *If y is a generator of $\ker(\theta : \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+} \to \mathcal{O}_{\mathbf{C}_p})$, then the map $S_y : \sum_{n\geqslant 0} x_n T^n \mapsto \sum_{n\geqslant 0} s(x_n)y^n$ gives rise to isomorphisms of topological $K[\![T]\!]$-modules (but not of rings!) $\mathbf{C}_p[\![T]\!] \simeq \mathbf{B}_{\mathrm{dR}}^{+}$. In addition, $S_y(\mathcal{O}_{\mathbf{C}_p}[\![T]\!]) = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+}$.*

Proof. — If $x \in \mathbf{B}_{\mathrm{dR}}^{+}$ then we define two sequences $\{x_n\}_{n\geqslant 0}$ of $\mathbf{C}_p$ and $\{a_n\}_{n\geqslant 0}$ of $\mathbf{B}_{\mathrm{dR}}^{+}$ by $a_0 = x$ and $x_n = \theta(a_n)$ and $a_{n+1} = (a_n - s(x_n))/y$ so that we have $x = \sum_{n\geqslant 0} s(x_n)y^n$ and therefore the map S_y is surjective. If $S_y(\sum_{n\geqslant 0} x_n T^n) = 0$, then by induction we see that $s(x_n) \in \ker(\theta)$ so that $x_n = 0$ and therefore S_y is injective. The map $S_y : \mathbf{C}_p[\![T]\!]/T^h \to \mathbf{B}_h$ is a continuous isomorphism and hence an homeomorphism by the open mapping theorem, which implies that $S_y : \mathbf{C}_p[\![T]\!] \to \mathbf{B}_{\mathrm{dR}}^{+}$ is also an homeomorphism. Finally, we see that $x \in \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+}$ if and only if $x_n \in \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^{+}$ which implies the second assertion. □

Lemma 28.4. — *If* $\mathrm{val}_p(\pi) > 0$, *then*

$$\mathcal{O}_{\mathbf{C}_p}[\![\pi T]\!][1+T, \frac{1}{1+T}] \cap \pi \cdot \mathcal{O}_{\mathbf{C}_p}[\![T]\!] = \pi \cdot \mathcal{O}_{\mathbf{C}_p}[\![\pi T]\!][1+T, \frac{1}{1+T}].$$

Proof. — If $f(T) = \sum_{j=-e}^{d} f_j(T)(1+T)^j \in \mathcal{O}_{\mathbf{C}_p}[\![\pi T]\!][1+T, (1+T)^{-1}] \cap \pi \cdot \mathcal{O}_{\mathbf{C}_p}[\![T]\!]$, then $f(T) \in \sum_{j=-e}^{d} f_j(0)(1+T)^j + \pi T \mathcal{O}_{\mathbf{C}_p}[\![\pi T]\!][1+T, (1+T)^{-1}]$ and $f_j(0)$ is divisible by π so that $f(T) \in \pi \cdot \mathcal{O}_{\mathbf{C}_p}[\![\pi T]\!][1+T, (1+T)^{-1}]$ as claimed. □

By proposition 28.1, the map $\iota_0 : \widetilde{\mathbf{B}}^{\dagger, r_0} \to \mathbf{B}_{\mathrm{dR}}^+$ given by "summing the series" extends by uniform continuity to a map $\iota_0 : \widetilde{\mathbf{B}}_{[r_0;r_0]} \to \mathbf{B}_{\mathrm{dR}}^+$.

Theorem 28.5. — *If* K *is finite over* $\mathbf{Q}_p$, *then the map* $K \otimes_{K_0} \iota_0(\widetilde{\mathbf{B}}_{[r_0;r_0]}) \to \mathbf{B}_{\mathrm{dR}}^+$ *is injective.*

Proof. — Let π_K be a uniformizer of K. Proposition 28.3 applied with $y = [\tilde{\pi}_K] - \pi_K$ shows that if $Y = [\tilde{\pi}_K]/\pi_K - 1$, then the map S_y gives rise to a topological isomorphim $\mathbf{C}_p \otimes_{\mathcal{O}_{\mathbf{C}_p}} \mathcal{O}_{\mathbf{C}_p}[\![\pi_K Y]\!] \simeq K \otimes_{K_0} \widetilde{\mathbf{B}}^+$ and lemma 28.4 combined with proposition 32.6 implies that the injective map $(\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^+)[[\tilde{\pi}_K]/\pi_K, \pi_K/[\tilde{\pi}_K]] \to \mathbf{B}_{\mathrm{dR}}^+$ extends to an injective map from the p-adic completion of $(\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^+)[[\tilde{\pi}_K]/\pi_K, \pi_K/[\tilde{\pi}_K]]$ to $\mathbf{B}_{\mathrm{dR}}^+$.

If $e = e(K/\mathbf{Q}_p)$, then p/π_K^e is a unit and therefore $[\tilde{p}]/p$ and $([\tilde{\pi}_K]/\pi_K)^e$ differ by a unit of $\mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \tilde{\mathbf{A}}^+$ so that

$$(K \otimes_{K_0} \widetilde{\mathbf{B}}^+) \left[\frac{[\tilde{\pi}_K]}{\pi_K}, \frac{\pi_K}{[\tilde{\pi}_K]} \right] = K \otimes_{K_0} \widetilde{\mathbf{B}}^+ \left[\frac{[\tilde{p}]}{p}, \frac{p}{[\tilde{p}]} \right].$$

Lemma 27.2 implies that $\tilde{\mathbf{A}}_{[r_0;r_0]}$ is the p-adic completion of $\tilde{\mathbf{A}}^+[p/[\tilde{p}], [\tilde{p}]/p]$ so that the above reasoning proves that the map $K \otimes_{K_0} \iota_0(\widetilde{\mathbf{B}}_{[r_0;r_0]}) \to \mathbf{B}_{\mathrm{dR}}^+$ is injective. □

Corollary 28.6. — *If* K *is finite over* $\mathbf{Q}_p$, *then the map* $K \otimes_{K_0} \iota_0(\mathbf{B}_{\max}^+) \to \mathbf{B}_{\mathrm{dR}}^+$ *is injective.*

Corollary 28.7. — *If* K *is a finite extension of* $\mathbf{Q}_p$ *then* $\mathrm{Frac}(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger})^{G_K} = K_0$ *and* $\mathrm{Frac}(\mathbf{B}_{\max})^{G_K} = K_0$.

Proof. — If $a/b \in \mathrm{Frac}(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger})$ then $a, b \in \widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger, r}$ for $r \gg 0$ and then $\varphi^{-n}(a)/\varphi^{-n}(b) \in \mathrm{Frac}(\widetilde{\mathbf{B}}_{[r_0;r_0]})$ if $n \gg 0$. If $\varphi^{-n}(a)/\varphi^{-n}(b) = k \in K$ then $1 \otimes \varphi^{-n}(a) - k \otimes \varphi^{-n}(b)$ is in the kernel of the map $K \otimes_{K_0} \widetilde{\mathbf{B}}_{[r_0;r_0]} \to \mathbf{B}_{\mathrm{dR}}^+$ so that $1 \otimes \varphi^{-n}(a) = k \otimes \varphi^{-n}(b)$ and $k \in K_0$ The second statement follows from the fact that $\mathbf{B}_{\max}^+ \subset \widetilde{\mathbf{B}}_{[r_0;r_0]}$. □

If π_K is a uniformizer of K, then $\theta([\tilde{\pi}_K]/\pi_K - 1) = 0$ and therefore the series $\sum_{n \geqslant 1} (-1)^{n-1}([\tilde{\pi}_K]/\pi_K - 1)^n/n$ converges in $\mathbf{B}_{\mathrm{dR}}^+$ to an element which we denote by

$\log([\tilde\pi_K]/\pi_K)$. If we choose the branch of the p-adic logarithm $\log_p : \mathbf{C}_p^\times \to \mathbf{C}_p$ given by $\log_p(p)=0$ then we can define $\log([\tilde\pi_K]) \in \mathbf{B}_{\mathrm{dR}}^+$ by $\log([\tilde\pi_K]) = \log([\tilde\pi_K]/\pi_K) + \log_p(\pi_K)$.

If $x \in \tilde{\mathbf{A}}^+$ satisfies $\theta(x) \equiv 1 \bmod p$, then one can write $x-1 = pa + ([\tilde p]-p)b$ with $a,b \in \tilde{\mathbf{A}}^+$ so that the series

$$\sum_{n\geqslant 1} (-1)^{n-1} \frac{(x-1)^n}{n}$$

converges in $\mathbf{B}_{\max}^+$.

Proposition 28.8. — *There is a unique map* $\log([\cdot]) : (\widetilde{\mathbf{E}}^+)^\times \to \mathbf{B}_{\max}$ *such that* $\log([xy]) = \log([x]) + \log([y])$ *and* $\log([x]) = \sum_{n\geqslant 1}(-1)^{n-1}(x-1)^n/n$ *if* $\theta(x) \equiv 1 \bmod p$.

Proof. — Every $x \in (\widetilde{\mathbf{E}}^+)^\times$ can be written as $x = u(1+z)$ in a unique way where $u \in \overline{\mathbf{F}}_p$ and $z \in \mathfrak{m}_{\widetilde{\mathbf{E}}}$. Since $u \in \overline{\mathbf{F}}_p$, there exists $m \geqslant 1$ such that $u^m = 1$ and since $z \in \mathfrak{m}_{\widetilde{\mathbf{E}}}$ there exists $n \geqslant 1$ such that $(1+z)^{p^n} = 1 + z^{p^n}$ satisifes $\mathrm{val}_{\mathbf{E}}((1+z)^{p^n}-1) \geqslant 1$. This shows that $\log([\cdot])$ is uniquely determined by the conditions of the proposition and that we have $\log([x]) = p^{-n}\log([1+z^{p^n}])$ if u, z and n are as above. □

If $g \in G_{\mathbf{Q}_p}$ then $g(\tilde p)^{(0)} = p$ so that there exists $a(g) \in \mathbf{Z}_p$ with $g(\tilde p) = \tilde p \varepsilon^{a(g)}$. The map $a : G_{\mathbf{Q}_p} \to \mathbf{Z}_p$ thus defined satisifes the relation $a(gh) = a(g) + \chi(g)a(h)$ and therefore $a \in H^1(G_{\mathbf{Q}_p}, \mathbf{Z}_p(1))$. We then adjoin to the rings $\widetilde{\mathbf{B}}_{[r;s]}$ above a variable u which we think of as $\log([\tilde p])$. In particular, we extend φ and the action of $G_{\mathbf{Q}_p}$ to $\mathbf{B}_{\mathrm{st}}$ by setting $\varphi(u) = pu$ and $g(u) = u + a(g)t$ if $g \in G_{\mathbf{Q}_p}$. We also define a monodromy map N by $N = -d/du$ so that N commutes with the action of $G_{\mathbf{Q}_p}$ and satisfies $N\varphi = p\varphi N$.

The map ι_0 extends to a $G_{\mathbf{Q}_p}$-equivariant map $\iota_0 : \widetilde{\mathbf{B}}_{[r_0;r_0]}[u] \to \mathbf{B}_{\mathrm{dR}}^+$ by $\iota_0(u) = \log([\tilde p])$.

Theorem 28.9. — *If K is finite over $\mathbf{Q}_p$ then the map $K \otimes_{K_0} \iota_0(\widetilde{\mathbf{B}}_{[r_0;r_0]}[u]) \to \mathbf{B}_{\mathrm{dR}}^+$ is injective.*

Proof. — In the notation of the proof of theorem 28.5, the image of $\iota_0 : \widetilde{\mathbf{B}}_{[r_0;r_0]} \to \mathbf{B}_{\mathrm{dR}}^+$ is contained in $\mathbf{C}_p\{Y\}$. The elements $\log([\tilde p])$ and $e\cdot\log([\pi_K]/\pi_K)$ differ by an element of $K \otimes_{K_0} \widetilde{\mathbf{B}}^+$ so that $K \otimes_{K_0} \widetilde{\mathbf{B}}_{[r_0;r_0]}[u] \subset \mathbf{C}_p\{Y\}[\log(1+Y)]$ and in order to prove the theorem, we need to show that the natural map $\mathbf{C}_p\{Y\}[\log(1+Y)] \to \mathbf{C}_p[\![Y]\!]$ is injective.

Assume therefore that we have $a_0(Y) + a_1(Y)\log(1+Y) + \cdots + a_d(Y)\log(1+Y)^d = 0$ in $\mathbf{C}_p[\![Y]\!]$ and hence in the ring of holomorphic functions on the open unit disk. For every $n \geqslant 0$ and every p^n-th root of unity ζ, the function $\log(1+Y)$ has a zero at $\zeta - 1$ so that $a_0(\zeta-1) = 0$ also and corollary 3.3 implies that $a_0(Y) = 0$. This allows us to get a relation of smaller degree, and we are done by induction. □

We let $\mathbf{B}_{\mathrm{st}}^+ = \mathbf{B}_{\max}^+[u]$.

Corollary 28.10. — *If K is a finite extension of $\mathbf{Q}_p$ then the map $K \otimes_{K_0} \mathbf{B}_{\mathrm{st}}^{+} \to \mathbf{B}_{\mathrm{dR}}^{+}$ is injective.*

Corollary 28.11. — *If K is a finite extension of $\mathbf{Q}_p$ then $\mathrm{Frac}(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}[u])^{G_K} = K_0$ and $\mathrm{Frac}(\mathbf{B}_{\mathrm{st}})^{G_K} = K_0$.*

If $n \in \mathbf{Z}$, let $r_n = p^{n-1}(p-1)$ so that $\varphi^n : \widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger, r_0} \to \widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger, r_n}$ is a bijection.

Corollary 28.12. — *If $n \geqslant 0$ and $r_n \in [r; s]$, then the map $\iota_n = \iota_0 \circ \varphi^{-n} : \widetilde{\mathbf{B}}_{[r;s]}[u] \to \mathbf{B}_{\mathrm{dR}}^{+}$ is injective.*

Let u be the variable introduced above and let $\log(\pi)$ be the element of $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}[u]$ given by $\log(\pi) = p/(p-1) \cdot u + \log(\pi/[\tilde{p}^{p/(p-1)}])$ where the latter series converges in $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}$. We adjoin $\log(\pi)$ to $\mathbf{B}_{\mathrm{rig},K}^{\dagger}$ and the resulting ring is stable under the action of Γ since it is given by $\gamma(\log(\pi)) = \log(\pi) + \log(\gamma(\pi)/\pi)$, where the latter series converges in $\mathbf{B}_{\mathrm{rig},\mathbf{Q}_p}^{\dagger}$ and it is also stable under φ since $\varphi(\log(\pi)) = p\log(\pi) + \log(\varphi(\pi)/\pi^p)$ where again the latter series converges in $\mathbf{B}_{\mathrm{rig},\mathbf{Q}_p}^{\dagger}$. Finally, we define a monodromy operator N on $\mathbf{B}_{\mathrm{rig},K}^{\dagger}[\log(\pi)]$ by $N = -p/(p-1) \cdot d/d\log(\pi)$.

Corollary 28.13. — *If $r \geqslant r(K)$ and $n \geqslant n(r)$, then $K \otimes_{K_0} \iota_n(\mathbf{B}_{\mathrm{rig},K}^{\dagger,r}[\log(\pi)]) \to \mathbf{B}_{\mathrm{dR}}^{+}$ is injective, and furthermore $\mathrm{Frac}(\mathbf{B}_{\mathrm{rig},K}^{\dagger,r}[\log(\pi)])^{\Gamma_K} = K_0$.*

Exercises

1. Check that if $a \in \mathbf{Z}_p$, then ε^a makes sense in $\widetilde{\mathbf{E}}^{+}$ and that in $\tilde{\mathbf{A}}^{+}$ we have
$$[\varepsilon^a] = (1 + ([\varepsilon] - 1))^a = \sum_{j \geqslant 0} \binom{a}{j} ([\varepsilon] - 1)^a.$$
2. Prove that $\mathbf{A}_{\max}/p\mathbf{A}_{\max} \simeq (\mathcal{O}_{\mathbf{C}_p}/p\mathcal{O}_{\mathbf{C}_p})[T]$.
3. * Prove that there is no $G_{\mathbf{Q}_p}$-equivariant map $\mathbf{C}_p \to \mathbf{B}_2$ which is a section of θ.

29. Regularization of p-adic periods

Lemma 29.1. — *If $x \in \widetilde{\mathbf{B}}_{\mathrm{rig}}^{+}$ and $u \geqslant r$, then $\mathrm{V}(x, r) \geqslant r/u \cdot \mathrm{V}(x, u)$.*

Proof. — By continuity, it's enough to prove the lemma for $x = \sum_{k \gg -\infty} p^k [x_k] \in \widetilde{\mathbf{B}}^{+}$. We then have
$$\mathrm{V}(x, r) = \min(\mathrm{val}_{\mathbf{E}}(x_k) + ks(r)) = \min\left(\frac{r}{u}(\mathrm{val}_{\mathbf{E}}(x_k) + ks(u)) + (1 - \frac{r}{u})\mathrm{val}_{\mathbf{E}}(x_k)\right),$$
which is $\geqslant r/u \cdot \mathrm{V}(x, u)$ since $\mathrm{val}_{\mathbf{E}}(x_k) \geqslant 0$ for all k. □

The following result is an analogue of lemma 21.4 and can also be seen as "taking a power series and splitting it into its + and − parts".

Proposition 29.2. — *If $x \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ satisfies $\mathrm{V}(x,r) \geqslant 0$ then we can write $x = x^+ + x^-$ with $x^+ \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$ and $x^- \in \tilde{\mathbf{A}}^{\dagger,r}$ and $\mathrm{V}(x^{\pm},u) \geqslant \mathrm{V}(x,u)$ for all $u \geqslant r$.*

Proof. — If $x \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ and $\mathrm{V}(x,r) \geqslant 0$ then by definition we can write $x = \sum_{k\geqslant 0} x_k$ where $x_k \in \widetilde{\mathbf{B}}^{\dagger,r}$ and $\mathrm{V}(x_k,r) \geqslant 0$ and $\mathrm{V}(x_k,u) \to \infty$ for all $u \geqslant r$. Lemma 21.4 applied to x_k shows that we may write $x_k = x_k^+ + x_k^-$ with $x_k^+ \in \widetilde{\mathbf{B}}^{+}$ and $x_k^- \in \tilde{\mathbf{A}}^{\dagger,r}$ and $x_k^{\pm}$ converging to 0 for the Fréchet topology so that $x = x^+ + x^-$ with $x^+ \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$ and $x^- \in \tilde{\mathbf{A}}^{\dagger,r}$. In addition, lemma 21.4 again shows that $\mathrm{V}(x^{\pm},u) \geqslant \mathrm{V}(x,u)$ for all $u \geqslant r$. □

Corollary 29.3. — *Inside $\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ we have $\widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} + \widetilde{\mathbf{B}}^{\dagger,r} = \widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$ and $\widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} \cap \widetilde{\mathbf{B}}^{\dagger,r} = \widetilde{\mathbf{B}}^{+}$.*

Proof. — The first assertion follows from proposition 29.2 above. For the second one, note that if $x = \sum_{k\geqslant 0} p^k[x_k] \in \tilde{\mathbf{A}}^{\dagger,r}$ then $\mathrm{V}(x,r) \geqslant 0$ and if $x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$ then $\mathrm{V}(x,s) \geqslant 0$ for all $s \leqslant r$ so that $\mathrm{val}_{\mathbf{E}}(x_k) \geqslant 0$ and $x \in \tilde{\mathbf{A}}^{+}$. □

Lemma 29.4. — *If $x \in \widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}}$ and there exists a sequence $\{r_k\}_{k\geqslant 1}$ with $r_k \to 0$ and $x \in \widetilde{\mathbf{B}}^{\dagger,r_k}_{\mathrm{rig}}$ and $\mathrm{V}(x,r_k) \geqslant 0$, then $x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$.*

Proof. — For every $k \geqslant 1$, we can write $x = x_k^+ + x_k^-$ with $x_k^+ \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$ and $x_k^- \in \tilde{\mathbf{A}}^{\dagger,r_k}$. If $k \geqslant 1$, then $x_1^- - x_k^- = x_k^+ - x_1^+ \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} \cap \tilde{\mathbf{A}}^{\dagger,r_k} = \tilde{\mathbf{A}}^{+}$ so that $x_1^- \in \tilde{\mathbf{A}}^{\dagger,r_k}$ for all $k \geqslant 1$ and since $\cap_{s>0}\tilde{\mathbf{A}}^{\dagger,s} = \tilde{\mathbf{A}}^{+}$ we have $x_1^- \in \tilde{\mathbf{A}}^{+}$ which implies that $x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$. □

Proposition 29.5. — *If $x \in \widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}}$ and there exists a sequence $\{r_k\}_{k\geqslant 1}$ with $r_k \to 0$ and $x \in \widetilde{\mathbf{B}}^{\dagger,r_k}_{\mathrm{rig}}$ and $\liminf \mathrm{V}(x,r_k) \geqslant 0$, then $x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$.*

Proof. — We have $\mathrm{V}([\tilde{p}]x,r_k) = 1 + \mathrm{V}(x,r_k) \geqslant 0$ for $k \gg 0$ so that by lemma 29.4, we have $[\tilde{p}]x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$. By proposition 29.2, we can write $x = x^+ + x^-$ with $x^+ \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$ and $x^- \in \widetilde{\mathbf{B}}^{\dagger,r}$ for some $r > 0$ and we then have $[\tilde{p}]x^- \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} \cap \widetilde{\mathbf{B}}^{\dagger,r} = \widetilde{\mathbf{B}}^{+}$ by corollary 29.3. Finally, we have $V([\tilde{p}]x,0) \geqslant 1$ as well as $V([\tilde{p}]x^+,0) \geqslant 1$ so that $V([\tilde{p}]x^-,0) \geqslant 1$ which implies that $[\tilde{p}]x^- \in [\tilde{p}]\widetilde{\mathbf{B}}^{+}$ and therefore, $x \in \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}}$. □

Theorem 29.6. — *If $M \in \mathrm{M}_{m\times n}(\widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}})$ and $X \in \mathrm{M}_m(\widetilde{\mathbf{B}}^{+}_{\mathrm{rig}})$ and $Y \in \mathrm{M}_n(\widetilde{\mathbf{B}}^{+}_{\mathrm{rig}})$ are such that $\varphi(M) = XMY$, then $M \in \mathrm{M}_{m\times n}(\widetilde{\mathbf{B}}^{+}_{\mathrm{rig}})$.*

Proof. — Choose some $r > 0$ such that $M \in \mathrm{M}_{m\times n}(\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}})$. There exist some positive constants h_X and h_Y and c such that $\mathrm{V}(x_{ij},r) \geqslant -h_X$ and $\mathrm{V}(y_{ij},r) \geqslant -h_Y$ and $\mathrm{V}(m_{ij},r) \geqslant -c$. The equation $\varphi(M) = XMY$ implies that $\varphi(m_{ij}) = \sum_{k,\ell} x_{ik}m_{k\ell}y_{\ell j}$ so that if $M \in \mathrm{M}_{m\times n}(\widetilde{\mathbf{B}}^{\dagger,s}_{\mathrm{rig}})$ for some s then $\varphi(m_{ij}) \in \widetilde{\mathbf{B}}^{\dagger,s}_{\mathrm{rig}}$ and therefore $m_{ij} \in \widetilde{\mathbf{B}}^{\dagger,s/p}_{\mathrm{rig}}$.

Furthermore, in this case we have $\mathrm{V}(\varphi(M),s) \geqslant \mathrm{V}(X,s)+\mathrm{V}(M,s)+\mathrm{V}(Y,s)$. This and the fact that $\mathrm{V}(\varphi(m),s) = p\mathrm{V}(m,s/p)$ allows us to show by induction on $k \geqslant 0$ that $\mathrm{V}(M,r/p^k) \geqslant -(kh+c)/p^k$ where $h = h_X + h_Y$.

The theorem now results from proposition 29.5. □

Theorem 29.7. — *If $M \in \mathrm{M}_{m\times n}(\mathbf{B}^+_{\max})$ and $X \in \mathrm{M}_m(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})$ and $Y \in \mathrm{M}_n(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})$ are such that $M = X\varphi(M)Y$, then $M \in \mathrm{M}_{m\times n}(\widetilde{\mathbf{B}}^+_{\mathrm{rig}})$.*

Proof. — The relation $M = X^{-1}\varphi(M)Y^{-1}$ implies by induction on $n \geqslant 0$ that M has coefficients in $\varphi^n(\mathbf{B}^+_{\max})$ and the theorem follows from $\cap_{n\geqslant 0}\varphi^n(\mathbf{B}^+_{\max}) = \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$. □

We now explain how to recover $\widetilde{\mathbf{B}}^\dagger$ inside $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$.

Lemma 29.8. — *If $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$, then $\mathrm{V}(y,r) \geqslant 0$ for all $r \gg 0$ if and only if $y \in \tilde{\mathbf{A}}^+$.*

Proof. — If $y \in \tilde{\mathbf{A}}^+$, then $\mathrm{V}(y,r) \geqslant 0$ for all $r \geqslant 0$. Conversely, if $\mathrm{V}(y,r) \geqslant 0$ for all $r \gg 0$, then $\mathrm{V}(y,r) \geqslant 0$ for all $r \geqslant 0$ by the maximum modulus principle and we have $y \in \tilde{\mathbf{A}}_{[0;nr_0]}$ for all $n \geqslant 1$ so that we have

$$y \in \tilde{\mathbf{A}}^+\{\frac{[\tilde{p}]^n}{p}\} = \tilde{\mathbf{A}}^+ + \frac{[\tilde{p}]^n}{p}\tilde{\mathbf{A}}^+\{\frac{[\tilde{p}]^n}{p}\} \subset \tilde{\mathbf{A}}^+ + p^{n-1}\left(\frac{[\tilde{p}]}{p}\right)^n \tilde{\mathbf{A}}^+\{\frac{[\tilde{p}]}{p}\} \subset \tilde{\mathbf{A}}^+ + p^{n-1}\mathbf{A}_{\max},$$

and lemma 27.3 now implies that $y \in \tilde{\mathbf{A}}^+$. □

Corollary 29.9. — *If $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$, then there exists $C \geqslant 0$ such that $\mathrm{V}(y,r) \geqslant -Cr$ for all $r \gg 0$ if and only if $y \in \widetilde{\mathbf{B}}^+$.*

Proof. — Since $\mathrm{V}(p^n y,r) = \mathrm{V}(y,r) + ns(r)$, the result follows from lemma 29.8. □

Theorem 29.10. — *If $y \in \widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$, then $y \in \widetilde{\mathbf{B}}^{\dagger,r}$ if and only if there exists $C \geqslant 0$ such that $\mathrm{V}(y,s) \geqslant -Cs$ for all $s \gg 0$.*

Proof. — If $y \in \tilde{\mathbf{A}}^{\dagger,r}$, then $\mathrm{V}(y,s) \geqslant 0$ for all $s \geqslant r$ so that if $y \in \widetilde{\mathbf{B}}^{\dagger,r}$, then there exists $C \geqslant 0$ such that $\mathrm{V}(y,s) \geqslant -Cs$ for all $s \geqslant r$.

Conversely, if there exists $C \geqslant 0$ such that $\mathrm{V}(y,s) \geqslant -Cs$ for all $s \gg 0$ then we may replace y by $p^n y$ for $n \gg 0$ and assume that $\mathrm{V}(y,r) \geqslant 0$. By proposition 29.2, we can then write $y = y^+ + y^-$ where $y^- \in \tilde{\mathbf{A}}^{\dagger,r}$ and $y^+ \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ satisfies $\mathrm{V}(y^+,s) \geqslant \mathrm{V}(y,s)$ for all $s \geqslant r$. The theorem now follwos from corollary 29.9. □

Corollary 29.11. — *If $y \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$, then y is invertible if and only if $y \in \widetilde{\mathbf{B}}^\dagger$.*

Proof. — The ring $\widetilde{\mathbf{B}}^\dagger$ is a field by lemma 21.10 which proves one implication. Assume now that $yz = 1$ for some $y,z \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$. The function $s \mapsto \mathrm{V}(y,s)$ is convex by exercise 1 and $0 = \mathrm{V}(yz,s) = \mathrm{V}(y,s) + \mathrm{V}(z,s)$ so that one of $\mathrm{V}(y,s)$ and $\mathrm{V}(z,s)$ is eventually

positive. Theorem 29.10 then implies that either y or z is in $\widetilde{\mathbf{B}}^{\dagger}$ and therefore both are. □

Corollary 29.12. — *If $M \in \mathrm{M}_d(\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}})$ and if $X, Y \in \mathrm{GL}_d(\tilde{\mathbf{A}}^{\dagger,r})$ are such that $\varphi(M) = XMY$, then $M \in \mathrm{M}_d(\widetilde{\mathbf{B}}^{\dagger,r})$.*

Recall that we have constructed a surjective map $\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$ and computed its kernel.

Lemma 29.13. — *If $x \in \tilde{\mathbf{A}}^+$, then $\theta \circ \varphi^n(x) = 0$ for all $n \geqslant 0$ if and only if $x \in \pi\tilde{\mathbf{A}}^+$.*

Proof. — If $x \in \pi\tilde{\mathbf{A}}^+$, then $\theta \circ \varphi^n(x) = 0$ for all $n \geqslant 0$. Let $\omega = \pi/\varphi^{-1}(\pi)$ so that ω is a generator of $\ker(\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p})$ by proposition 26.1 and $\theta \circ \varphi^{-k}(\omega) \neq 0$ for all $k \neq 0$. This implies that if $\theta \circ \varphi^n(x) = 0$ for all $k \geqslant n \geqslant 0$, then $x \in \pi/\varphi^{-k}(\pi)\tilde{\mathbf{A}}^+$.

Let I be the ideal of elements of $\tilde{\mathbf{A}}^+$ such that $\theta \circ \varphi^n(x) = 0$ for all $n \geqslant 0$ so that $I = \cap_{k\geqslant 0}\pi/\varphi^{-k}(\pi)\tilde{\mathbf{A}}^+$. In $\widetilde{\mathbf{E}}^+$ we have $\overline{I} = \overline{\pi}\widetilde{\mathbf{E}}^+$ so that $I = \pi\tilde{\mathbf{A}}^+ + p(\tilde{\mathbf{A}}^+ \cap I)$ and therefore $I = \pi\tilde{\mathbf{A}}^+$. □

Theorem 29.14. — *If $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ is such that $\varphi^n(y) \in t\mathbf{B}^+_{\mathrm{dR}}$ for all $n \in \mathbf{Z}$, then $y \in t\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$.*

Proof. — If $y \in \tilde{\mathbf{A}}_{[0;r_0]}$ then by lemma 27.2, we can write $y = \sum_{j\geqslant 0} a_j([\tilde{p}]/p)^j$ where $a_j \in \tilde{\mathbf{A}}^+$ and $a_j \to 0$. Let $\omega = \pi/\varphi^{-1}(\pi)$ so that by proposition 26.1, ω is a generator of $\ker(\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p})$. The element $\omega/([\tilde{p}] - p)$ is then a unit of $\tilde{\mathbf{A}}^+$ and y can be written as $y = \sum_{j\geqslant 0} y_j(\omega/p - 1)^j$ where $y_j \to 0$ (to do this, we twice use the fact that $A\{X\} = A\{X - 1\}$). If $Q(\pi) = ((1+\pi)^p - 1)/\pi = \varphi(\omega)$, then $\varphi(y) = \sum_{j\geqslant 0} \varphi(y_j)(Q(\pi)/p - 1)^j$ in $\tilde{\mathbf{A}}_{[0;r_1]}$. Since $Q(\pi)/p - 1$ is a multiple of π, this means that we have $\varphi(y) = \varphi(y_0) + \pi z$ in $\widetilde{\mathbf{B}}_{[0;r_1]}$ with $y_0 \in \tilde{\mathbf{A}}^+$. If $\theta \circ \varphi^n(y) = 0$ for all $n \geqslant 1$, then lemma 29.13 implies that $\varphi(y_0) \in \pi\tilde{\mathbf{A}}^+$ and hence that $\varphi(y) \in \pi\widetilde{\mathbf{B}}_{[0;r_1]}$ so that $y \in \varphi^{-1}(\pi)\widetilde{\mathbf{B}}_{[0;r_0]}$. If in addition $\theta(y) = 0$, then $y \in \pi\widetilde{\mathbf{B}}_{[0;r_0]}$. Since t/π is a unit of $\widetilde{\mathbf{B}}_{[0;r_0]}$ (at least if $p \neq 2$, see exercise 1), we have $y \in t\widetilde{\mathbf{B}}_{[0;r_0]}$.

Since $\varphi^k : \widetilde{\mathbf{B}}_{[0;r_0]} \to \widetilde{\mathbf{B}}_{[0;r_k]}$ is a bijection for $n \geqslant 0$, we see that if $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ and $\theta \circ \varphi^n(y) = 0$ for all $n \geqslant -k$, then $y = t \cdot z_k$ with $z_k \in \widetilde{\mathbf{B}}_{[0;r_k]}$. The sequence $\{z_k\}_{k\geqslant 0}$ defines an element z of $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ which then satisfies $y = tz$ and this proves the theorem. □

Corollary 29.15. — *We have $\mathbf{B}^{\varphi=1}_{\max} \cap \mathrm{Fil}^0\mathbf{B}_{\mathrm{dR}} = \mathbf{Q}_p$.*

Proof. — If $y \in \mathbf{B}^{\varphi=1}_{\max}$ then theorem 29.7 implies that $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}[1/t]$. Choose $y \in \mathbf{B}^{\varphi=1}_{\max} \cap \mathrm{Fil}^0\mathbf{B}_{\mathrm{dR}}$ and let $k \geqslant 1$ be such that $y \in t^{-k}\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$. We have $\varphi^n(t^k y) = p^{-kn}t^k y \in t\mathbf{B}^+_{\mathrm{dR}}$ so that by theorem 29.14 above, we have $t^k y \in t\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ so that by induction, we get $y \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ and the corollary follows from lemma 27.4. □

We have $\hat{\mathbf{Q}}_p^{\mathrm{nr}} = W(\overline{\mathbf{F}}_p)[1/p] \subset \widetilde{\mathbf{B}}^+ \subset \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$. If $\lambda_0 \in W(\overline{\mathbf{F}}_p)^\times$ then by corollary 8.7, there exists $\mu \in W(\overline{\mathbf{F}}_p)^\times$ such that $\lambda_0 = \mu/\varphi(\mu)$. Every $\lambda \in \hat{\mathbf{Q}}_p^{\mathrm{nr}}$ can then be written as $\lambda = p^n\mu/\varphi(\mu)$. The map $\mathbf{B}_{\max}^{\varphi=\lambda} \to \mathbf{B}_{\max}^{\varphi=p^n}$ given $y \mapsto \mu y$ is then a bijection which respects the filtration induced by $\mathbf{B}_{\mathrm{dR}}$.

Proposition 29.16. — *If $\lambda \in \hat{\mathbf{Q}}_p^{\mathrm{nr}}$ and $n = \mathrm{val}_p(\lambda)$, then $\mathbf{B}_{\max}^{\varphi=\lambda} \cap \mathrm{Fil}^{n+1}\mathbf{B}_{\mathrm{dR}} = \{0\}$.*

Proof. — If $y \in \mathbf{B}_{\max}^{\varphi=\lambda} \cap \mathrm{Fil}^{n+1}\mathbf{B}_{\mathrm{dR}}$ and μ is as above, then $t^{-n}\mu y \in \mathbf{B}_{\max}^{\varphi=1} \cap \mathrm{Fil}^1\mathbf{B}_{\mathrm{dR}}$ so that $t^{-n}\mu y = 0$ by corollary 29.15. □

30. Filtered (φ, N)-modules

Reference: [**Fon94b**]. Let K be a finite extension of $\mathbf{Q}_p$ and let $K_0 = K \cap \mathbf{Q}_p^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbf{Q}_p$ in K. A φ-module D over K is a K_0-vector space with an invertible σ-semi-linear frobenius $\varphi : D \to D$. If D is of dimension 1, then we set $t_N(D) = \mathrm{val}_p(\mathrm{Mat}(\varphi))$ and if $\dim(D) \geqslant 1$, then we set $t_N(D) = t_N(\det D)$. Using theorem 8.9 (the Dieudonné-Manin theorem), one can construct the Newton polygon of a φ-module D. The terminal point is then $(\dim(D), t_N(D))$. A (φ, N)-module D over K is a φ-module with a K_0-linear map $N : D \to D$ which satisfies the equation $N\varphi = p\varphi N$. Since φ is invertible, N is necessarily nilpotent. Finally, a $(\varphi, N, \mathrm{Gal}(L/K))$-module D over K is a (φ, N)-module D over K with an action of $\mathrm{Gal}(L/K)$ and commuting with φ and N.

A filtered module D over K is a K-vector space with a filtration $\mathrm{Fil}^j D$ by sub-K-vector spaces which is decreasing ($\mathrm{Fil}^{j+1}D \subset \mathrm{Fil}^j D$), exhaustive ($\mathrm{Fil}^j D = D$ if $j \ll 0$) and separated ($\mathrm{Fil}^j D = \{0\}$ if $j \gg 0$). If D is of dimension 1, then there exists a well-defined $h \in \mathbf{Z}$ such that $\mathrm{Fil}^h D = D$ and $\mathrm{Fil}^{h+1} D = \{0\}$ and we set $t_H(D) = h$. If $\dim(D) \geqslant 1$, then we set $t_H(D) = t_H(\det D)$. One can also construct a polygon (the Hodge polygon) out of the filtration and its terminal point is then $(\dim(D), t_H(D))$.

A filtered (φ, N)-module D over K is a filtered (φ, N)-module D along with the structure of a filtered module on $D_K = K \otimes_{K_0} D$. A filtered (φ, N, G_K)-module D over K is a filtered $(\varphi, N, \mathrm{Gal}(L/K))$-module D along with the structure of a filtered module on $D_L = L \otimes_{K_0} D$ such that the filtration is stable under $\mathrm{Gal}(L/K)$ (or equivalently the structure of a filtered module on $D_K = (L \otimes_{K_0} D)^{\mathrm{Gal}(L/K)}$).

Definition 30.1. — We say that a filtered (φ, N)-module D over K is admissible if it satisfies the conditions:

1. $t_H(D) = t_N(D)$;

2. $t_H(D') \leqslant t_N(D')$ for every sub-object D' of D.

The category of admissible filtered (φ, N)-modules over K is an abelian category.

31. Crystalline and semistable representations

Reference: [**Fon94b**]. 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 $\mathrm{D}_{\mathrm{st}}(V) = (\mathbf{B}_{\mathrm{st}} \otimes_{\mathbf{Q}_p} V)^{G_K}$. Since $\mathrm{Frac}(\mathbf{B}_{\max})^{G_K} = K_0$ by corollary 28.7 and $\mathrm{Frac}(\mathbf{B}_{\mathrm{st}})^{G_K} = K_0$ by corollary 28.11, proposition 32.4 shows that $\mathrm{D}_{\mathrm{cris}}(V)$ and $\mathrm{D}_{\mathrm{st}}(V)$ are K_0-vector spaces of dimension $\leqslant \dim(V)$. We say that V is a crystalline (or semi-stable) representation if we have equality of dimensions. The space $\mathrm{D}_{\mathrm{st}}(V)$ is a (φ, N)-module and since $\mathbf{B}_{\max} = \mathbf{B}_{\mathrm{st}}^{N=0}$, we have $\mathrm{D}_{\mathrm{cris}}(V) = \mathrm{D}_{\mathrm{st}}(V)^{N=0}$; in particular, any crystalline representation is semi-stable.

Likewise, $\mathrm{D}_{\mathrm{dR}}(V) = (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ is a K-vector space of dimension $\leqslant \dim(V)$ which is a filtered K-vector space. We say that V is a de Rham representation if we have equality of dimensions.

By corollaries 28.6 and 28.10, the maps $K \otimes_{K_0} \mathrm{D}_{\mathrm{cris}}(V) \to \mathrm{D}_{\mathrm{dR}}(V)$ and $K \otimes_{K_0} \mathrm{D}_{\mathrm{st}}(V) \to \mathrm{D}_{\mathrm{dR}}(V)$ are injective, so that $\mathrm{D}_{\mathrm{cris}}(V)$ is a filtered φ-module over K and $\mathrm{D}_{\mathrm{st}}(V)$ is a filtered (φ, N)-module over K.

Proposition 31.1. — *The functors $V \mapsto \mathrm{D}_{\mathrm{cris}}(V)$ and $V \mapsto \mathrm{D}_{\mathrm{st}}(V)$ are fully faithful from the categories of crystalline and semi-stable representations to the categories of φ-modules over K and filtered (φ, N)-modules over K.*

Proof. — Corollary 29.15 shows that $\mathbf{B}_{\max}^{\varphi=1} \cap \mathrm{Fil}^0 \mathbf{B}_{\mathrm{dR}} = \mathbf{Q}_p$ so that if V is crystalline, then $V = \mathrm{Fil}^0(\mathbf{B}_{\mathrm{dR}} \otimes_K \mathrm{D}_{\mathrm{dR}}(V)) \cap (\mathbf{B}_{\max} \otimes_{K_0} \mathrm{D}_{\mathrm{cris}}(V))^{\varphi=1}$. Likewise if V is semi-stable, then $V = \mathrm{Fil}^0(\mathbf{B}_{\mathrm{dR}} \otimes_K \mathrm{D}_{\mathrm{dR}}(V)) \cap (\mathbf{B}_{\mathrm{st}} \otimes_{K_0} \mathrm{D}_{\mathrm{st}}(V))^{N=0,\varphi=1}$. In both cases, one can recover V from either $\mathrm{D}_{\mathrm{cris}}(V)$ or $\mathrm{D}_{\mathrm{st}}(V)$ and the corresponding functors are therefore fully faithful. □

Proposition 31.2. — *The categories of crystalline and semi-stable representations are stable under sub-objects, quotients, direct sums, tensor products (and hence symmetric and exterior powers) and duals. The functors $\mathrm{D}_{\mathrm{cris}}(\cdot)$ and $\mathrm{D}_{\mathrm{st}}(\cdot)$ behave in the expected way with respect to these operations.*

Proof. — The only assertion which may not be clear is the one concerning duals; it results from the case of characters which is itself a consequence of theorem 31.4 below. Indeed, this theorem implies that if a character is crystalline or semi-stable, then so is its inverse. □

If $\eta : G_K \to \mathbf{Z}_p^\times$ is a character, then we say that η is crystalline (or semi-stable, or de Rham) if the associated representation is. This is the case if and only if there exists $y \in \mathbf{B}_{\max}$ (or $y \in \mathbf{B}_{\mathrm{st}}$ or $y \in \mathbf{B}_{\mathrm{dR}}$) such that $\eta(g) = y/g(y)$.

Theorem 31.3. — *If $\eta : G_K \to \mathbf{Z}_p^\times$ is a character, then η is de Rham if and only if $\eta = \mu \cdot \chi^h$ where μ is potentially unramified and $h \in \mathbf{Z}$.*

Proof. — The character η is de Rham if and only if there exists $y \in \mathbf{B}_{\mathrm{dR}}^\times$ such that $\eta(g) = y/g(y)$. Let h be such that $y = y_0 t^{-h}$ where $y_0 \in (\mathbf{B}_{\mathrm{dR}}^+)^\times$. The character $\mu = \chi^{-h}\eta$ then satisfies $\mu(g) = \theta(y_0)/g(\theta(y_0))$ and is then potentially unramified by corollary 13.7. □

Theorem 31.4. — *If $\eta : G_K \to \mathbf{Z}_p^\times$ is a character, then η is crystalline if and only if it is semi-stable, and this occurs if only if $\eta = \mu \cdot \chi^h$ where μ is unramified and $h \in \mathbf{Z}$.*

Proof. — If η is semi-stable and V denotes the associated representation, then $\mathrm{D}_{\mathrm{st}}(V)$ is of dimension 1 so that $N = 0$ and therefore $\mathrm{D}_{\mathrm{st}}(V) = \mathrm{D}_{\mathrm{cris}}(V)$ and η is crystalline.

Let us prove that characters of the form $\mu \cdot \chi^h$ where μ is unramified and $h \in \mathbf{Z}$ are indeed crystalline. By corollary 8.7, there exists $y_0 \in W(\overline{\mathbf{F}}_p)^\times$ such that $y_0/\varphi(y_0) = \mu(\mathrm{Frob}_p)$ and then we have $\eta(g) = y/g(y)$ if $y = y_0 t^{-h}$ so that η is crystalline.

Assume now that η is crystalline; it is then de Rham and theorem 31.3 shows that $\eta = \mu \cdot \chi^h$ where μ is potentially unramified. Let L be a finite extension of K such that $\mu|_L$ is unramified, so that as above there exists $\lambda_0 \in W(\overline{\mathbf{F}}_p)^\times$ satisfying $\mu(g) = \lambda_0/g(\lambda_0)$ if $g \in G_L$. Since μ is crystalline, there exists $y_0 \in \mathbf{B}_{\max}$ such that $\mu(g) = y_0/g(y_0)$ if $g \in G_K$ and then $y_0/\lambda_0 \in \mathbf{B}_{\max}^{G_L} = L_0$ so that μ is unramified. □

Proposition 31.5. — *If V is a semi-stable representation, then $\mathrm{D}_{\mathrm{st}}(V)$ is an admissible filtered (φ, N)-module over K.*

Proof. — Then the fact that $t_H(\mathrm{D}_{\mathrm{st}}(V)) = t_N(\mathrm{D}_{\mathrm{st}}(V))$ results from theorem 31.4 applied to $\det(V)$. If D' is a sub-object of rank r of $\mathrm{D}_{\mathrm{st}}(V)$ then we can replace V by $\Lambda^r V$ so that D' is of dimension 1. In this case, $N = 0$ on D' and $D' \subset \mathrm{D}_{\mathrm{cris}}(V)$ is a line so that $D' \subset (\mathbf{B}_{\max} \otimes_{\mathbf{Q}_p} V)^{\varphi=\lambda}$ where $t_N(D) = \mathrm{val}_p(\lambda)$ and the proposition now results from proposition 29.16. □

Exercises

1. Prove that t/π is a unit of $\widetilde{\mathbf{B}}_{[0;r_0]}$ if $p \neq 2$. If $p = 2$, prove that $t/(\varphi(\pi)/2)$ is a unit of $\widetilde{\mathbf{B}}_{[0;r_0]}$ and use this to prove theorem 29.14.

2. Show that if V is a de Rham representation, then V is Hodge-Tate and the Hodge-Tate weights of V are the integers h such that $\mathrm{Fil}^{-h}\mathrm{D}_{\mathrm{dR}}(V) \neq \mathrm{Fil}^{-h+1}\mathrm{D}_{\mathrm{dR}}(V)$.
3. What can you say about $\hat{\mathbf{Q}}_p^{\mathrm{tame}}$-admissible representations?
4. Prove that if V is a Hodge-Tate representation, then $\mathrm{D}_{\mathrm{dR}}(V) \neq 0$.
5. Prove that if V is a de Rham representation, then $(V/V^{I_K})^{I_K} = 0$.
6. Prove that if V is a crystalline representation and $V = V^{H_K}$, then V is a direct sum of representations of the form $\mathbf{Q}_p(h)$ with $h \in \mathbf{Z}$.

32. Some useful results

This section contains various useful results that are used in the notes.

***Theorem 32.1* (Artin's lemma).** — *If K is a field and G is a finite group of automorphisms of K, then K is a finite Galois extension of K^G and $\mathrm{Gal}(K/K^G) \simeq G$.*

***Theorem 32.2* (Algebraic independance of characters)**

If K is an infinite field and if $\sigma_1, \ldots, \sigma_n$ are elements of a finite group of automorphisms of K, then $\sigma_1, \ldots, \sigma_n$ are algebraically independant over K.

Proposition 32.3. — *Let A be a domain and let f and g be two elements of A such that $A[1/f] \cap A[1/g] = A$ inside the fraction field of A.*

The map $P(X) \mapsto P(f/g)$ from $A[X]$ to $A[f/g]$ or from $A[X, 1/X]$ to $A[f/g, g/f]$ is then surjective and its kernel is $(gX - f)$ or $(gX - f, f/X - g)$.

Proof. — The surjectivity of the map is tautological. Let us show the assertion concerning the second kernel (the first one is analogous and simpler). If $P(f/g) = 0$ then in $A[1/fg][X]$ we can write $P(X) = P(X) - P(f/g)$ so that $P(X) = (gX - f)Q(X) + (f/X - g)R(1/X)$ where Q and R are two polynomials with coefficients $\{q_i\}$ and $\{r_j\}$ in $A[1/g]$ and $A[1/f]$ respectively. We have $fq_0 + gr_0 \in A$ so that $q_0 \in A[1/g] \cap A[1/f] = A$, and likewise for r_0. A straightforward induction then shows that $q_i \in A$ and $r_j \in A$ for all i and j. □

Proposition 32.4. — *Let M be a torsion-free module over a domain B, let S denote a set of maps each $s : M \to M$ of which is semilinear with respect to a ring homomorphism of B also denoted by s (that is, $s(bm) = s(b)s(m)$ for some $s : B \to B$). If $(\mathrm{Frac}B)^S = B^S$ then the map : $\alpha : B \otimes_{B^S} M^S \to M$ is injective.*

Proof. — If $\ker(\alpha) \neq \{0\}$, then there exists an element $b_1 \otimes m_1 + \cdots + b_k \otimes m_k$ in it for which k is minimal. Suppose that $k \geqslant 2$. If $s \in S$, then $s(b_1) \otimes m_1 + \cdots + s(b_k) \otimes m_k \in \ker(\alpha)$ so that by minimality, we have $b_1 s(b_j) - s(b_1)b_j = 0$ for all $1 \leqslant j \leqslant k$. This implies that $b_j/b_1 \in (\mathrm{Frac}B)^S$ and therefore that there exists $c_j \in B^S$ such that $b_j = b_1 c_j$. This

way we can reduce to the case where $k = 1$, but since M is torsion-free there is no such non-trivial relation. □

Proposition 32.5. — *If $M \subset N$ are two modules and M is complete for the p-adic topology and the map $M \to N/pN$ is surjective, then $M = N$.*

Let N be a torsion free $\mathbf{Z}_p$-module which is separated and complete for the p-adic topology and let $M \subset N$. If $\hat{M}$ denotes the completion of M for the p-adic topology, then the inclusion map $M \to N$ extends to a map $\hat{M} \to N$ whose image is the closure of M in N.

Proposition 32.6. — *If there exists $i \geqslant 1$ such that $p^i N \cap M \subset pM$, then the map above is injective.*

Proof. — Every element of $\hat{M}$ can be written as $m = \sum_{n \geqslant 0} p^{in} m_n$ with $m_n \in M$ and if $m \in \ker(\hat{M} \to N)$ then $m_0 \in p^i N \cap M \subset pM$ so that $\ker(\hat{M} \to N) \subset p \ker(\hat{M} \to N)$. By iterating this, we get that $\ker(\hat{M} \to N) \subset \cap_{k \geqslant 0} p^k \hat{M} = 0$. □

Exercises

1. Let $N = \mathbf{Z}_p[\![T]\!]$ and $M = \mathbf{Z}_p \cdot pT \oplus (\oplus_{n \geqslant 1} \mathbf{Z}_p \cdot (pT^{n+1} + T^n))$ so that M is a submodule of N, and let $x = pT - p(pT^2 + T) + p^2(pT^3 + T^2) - \cdots$. Prove that $x \neq 0$ in the p-adic completion of M but that the image of x in N is 0.
2. In proposition 32.6, prove that $p^{i+k} N \cap M \subset p^{k+1} M$ and use this to give an alternative proof.

References

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

[BC08] L. Berger & P. Colmez – "Familles de représentations de de Rham et monodromie p-adique", *Astérisque* (2008), no. 319, p. 303–337.

[Ber02] L. Berger – "Représentations p-adiques et équations différentielles", *Invent. Math.* **148** (2002), no. 2, p. 219–284.

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

[Ber11] ———, "A p-adic family of dihedral (φ, Γ)-modules", *Int. J. Number Theory* **7** (2011), no. 7, p. 1825–1834.

[BLZ04] L. Berger, H. Li & H. J. Zhu – "Construction of some families of 2-dimensional crystalline representations", *Math. Ann.* **329** (2004), no. 2, p. 365–377.

[CC98] F. Cherbonnier & P. Colmez – "Représentations p-adiques surconvergentes", *Invent. Math.* **133** (1998), no. 3, p. 581–611.

[CF00] P. Colmez & J.-M. Fontaine – "Construction des représentations p-adiques semistables", *Invent. Math.* **140** (2000), no. 1, p. 1–43.

[Che96] F. Cherbonnier – "Représentations p-adiques surconvergentes", Ph.D. Thesis, Université d'Orsay, 1996.

[Col99] P. Colmez – "Représentations cristallines et représentations de hauteur finie", *J. Reine Angew. Math.* **514** (1999), p. 119–143.

[Col02] ———, "Espaces de Banach de dimension finie", *J. Inst. Math. Jussieu* **1** (2002), no. 3, p. 331–439.

[Col03] ———, "Les conjectures de monodromie p-adiques", *Astérisque* (2003), no. 290, p. Exp. No. 897, vii, 53–101, Séminaire Bourbaki. Vol. 2001/2002.

[Col08] ———, "Espaces Vectoriels de dimension finie et représentations de de Rham", *Astérisque* (2008), no. 319, p. 117–186.

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

[Fon77] J.-M. Fontaine – *Groupes p-divisibles sur les corps locaux*, Société Mathématique de France, Paris, 1977, Astérisque, No. 47-48.

[Fon90] ———, "Représentations p-adiques des corps locaux. I", in *The Grothendieck Festschrift, Vol. II*, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, p. 249–309.

[Fon94a] ———, "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] ———, "Représentations p-adiques semi-stables", *Astérisque* (1994), no. 223, p. 113–184, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Fon04] ———, "Arithmétique des représentations galoisiennes p-adiques", *Astérisque* (2004), no. 295, p. xi, 1–115, Cohomologies p-adiques et applications arithmétiques. III.

[Fou09] L. Fourquaux – "Applications $\mathbf{Q}_p$-linéaires, continues et Galois-équivariantes de $\mathbf{C}_p$ dans lui-même", *J. Number Theory* **129** (2009), no. 6, p. 1246–1255.

[Laz62] M. Lazard – "Les zéros des fonctions analytiques d'une variable sur un corps valué complet", *Inst. Hautes Études Sci. Publ. Math.* (1962), no. 14, p. 47–75.

[LB10] J. Le Borgne – "Optimisation du théorème d'Ax-Sen-Tate et application à un calcul de cohomologie galoisienne p-adique", *Ann. Inst. Fourier (Grenoble)* **60** (2010), no. 3, p. 1105–1123.

[LT65] J. Lubin & J. Tate – "Formal complex multiplication in local fields", *Ann. of Math. (2)* **81** (1965), p. 380–387.

[Neu99] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[PS98] G. Pólya & G. Szegő – *Problems and theorems in analysis. I*, Classics in Mathematics, Springer-Verlag, Berlin, 1998, Series, integral calculus, theory of functions, Reprint of the 1978 English translation.

[Sch02] P. Schneider – *Nonarchimedean functional analysis*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[Sen73] S. Sen – "Lie algebras of Galois groups arising from Hodge-Tate modules", *Ann. of Math. (2)* **97** (1973), p. 160–170.

[Sen81] ———, "Continuous cohomology and p-adic Galois representations", *Invent. Math.* **62** (1980/81), no. 1, p. 89–116.

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

[Ser72] ———, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259–331.

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

[Zin84] T. Zink – *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte zur Mathematik, vol. 68, BSB B. G. Teubner Verlagsgesellschaft, Leipzig, 1984.

January – March 2010 (revised March 18, 2016)

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