An introduction to p-adic Hodge theory

Denis Benois

Institut de Mathématiques, Université de Bordeaux, 351, cours de la Libération 33405 Talence, France

Email address: denis.benois@math.u-bordeaux.fr

Contents

CHAPTER 1

Preliminaries

1. Non-archimedean fields

1.1. We recall basic definitions and facts about non-archimedean fields.

Definition. *A non-archimedean field is a field K equipped a non-archimedean absolute value that is, an absolute value $|\cdot|_K$ satisfying the ultrametric trinagle inequality*

$$|x+y|_K \leqslant \max\{|x|_K, |y|_K\}, \qquad \forall x, y \in K.$$

We will say that K is complete if it is complete for the topology induced by $|\cdot|_K$.

To any non-archimedean field K can associate its ring of integers

$$O_K = \{x \in K \mid |x|_K \leqslant 1\}.$$

The ring O_K is local, with the maximal ideal

$$\mathfrak{m}_K = \{x \in K \mid |x|_K < 1\}.$$

The group of units of O_K is

$$U_K = \{x \in K \mid |x|_K = 1\}.$$

The residue field of K is defined as

$$k_K = O_K / \mathfrak{m}_K.$$

Theorem 1.2. *Let K be a complete non-archimedean field and let L/K be a finite extension of degree $n = [L : K]$. Then the absolute value $|\cdot|_K$ has a unique continuation $|\cdot|_L$ to L, which is given by*

$$|x|_L = \left|N_{L/K}(x)\right|_K^{1/n},$$

where $N_{L/K}$ is the norm map.

Proof. See [**2**, Ch. 2, Thm 7]. Another proof (valid only for locally compact fields) can be found in [**5**, Chapter II, section 10]. □

This theorem allows to extend $|\cdot|_K$ to the algebraic closure of K. In particular, we have a unique extension of $|\cdot|_K$ to the separable closure $\overline{K}$ of K.

Proposition 1.3 (Krasner's lemma). *Let K be a complete non-archimedean field. Let $\alpha \in \overline{K}$ and let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ denote the conjugates of α over K. Set*

$$d_\alpha = \min\{|\alpha - \alpha_i|_K \mid 2 \leqslant i \leqslant n\}.$$

If $\beta \in \overline{K}$ is such that $|\alpha - \beta| < d_\alpha$, then $K(\alpha) \subset K(\beta)$.

Proof. We recall the proof (see, for example, [**24**, Proposition 8.1.6]). Assume that $\alpha \notin K(\beta)$. Then $K(\alpha,\beta)/K(\beta)$ is a non-trivial extension, and there exists an embedding $\sigma : K(\alpha,\beta)/K(\beta) \to \overline{K}/K(\beta)$ such that $\alpha_i := \sigma(\alpha) \neq \alpha$. Hence

$$|\beta-\alpha_i|_K = |\sigma(\beta-\alpha)|_K = |\beta-\alpha|_K < d_\alpha$$

and

$$|\alpha-\alpha_i|_K = |(\alpha-\beta)+(\beta-\alpha_i)|_K \leqslant \max\{|\alpha-\beta|_K, |\beta-\alpha_i|_K\} < d_\alpha.$$

This gives a contradiction. □

Proposition 1.4 (Hensel's lemma). *Let K be a complete non-archimedean field. Let $f(X) \in O_K[X]$ be a monic polynomial such that*

a) the reduction $\bar f(X) \in k_K[X]$ of $f(X)$ modulo $\mathfrak{m}_K$ has a root $\bar\alpha \in k_K$;

b) $\bar f'(\bar\alpha) \neq 0$.

Then there exists a unique $\alpha \in O_K$ such that $f(\alpha) = 0$ and $\bar\alpha = \alpha \pmod{\mathfrak{m}_K}$.

Proof. See, for example [**19**, Chapter 2, §2]. □

1.5. Recall that a valuation on K is a function $v_K : K \to \mathbf{R} \cup \{+\infty\}$ satisfying the following properties:

1) $v_K(xy) = v_K(x) + v_K(y), \qquad \forall x,y \in K^*$;
2) $v_K(x+y) \geqslant \min\{v_K(x), v_K(y)\}, \qquad \forall x,y \in K^*$;
3) $v_K(x) = \infty \Leftrightarrow x = 0$.

For any $\rho \in]0,1[$, the function $|x|_\rho = \rho^{v_K(x)}$ defines an ultrametric absolute value on K. Conversely, if $|\cdot|_K$ is an ultrametric absolute value, then for any c the function $v_c(x) = \log_c |x|_K$ is a valuation on K. This establishes a one to one correspondence between equivalence classes of non-archimedean absolute values and equivalence classes of valuations on K.

2. Local fields

2.1. In this section we review the basic theory of local fields.

Definition. *A discrete valuation field is a field K equipped with a valuation v_K such that $v_K(K^*)$ is a discrete subgroup of $\mathbf{R}$. Equivalently, K is a discrete valuation field if it is equipped with an absolute value $|\cdot|_K$ such that $|K^*|_K \subset \mathbf{R}_+$ is discrete.*

Let K be a discrete valuation field. In the equivalence class of discrete valuations on K we can choose the unique valuation v_K such that $v_K(K^*) = \mathbf{Z}$. An element $\pi_K \in K$ such that $v_K(\pi_K) = 1$ is called a uniformizer of K. Every $x \in K^*$ can be written in the form $x = \pi_K^{v_K(x)} u$ with $u \in U_K$, and one has:

$$K^* \simeq \langle \pi_K \rangle \times U_K, \qquad \mathfrak{m}_K = (\pi_K).$$

We adopt the following convention.

Definition. *A local field is a complete discrete valuation field K whose residue field k_K is finite.*

Note that many (but not all) results and constructions of the theory are valid under the weaker assumption that the residue field k_K is perfect.

We will always assume that the discrete valuation

$$v_K : K \to \mathbf{Z} \cup \{+\infty\}$$

is surjective.

Proposition 2.2. *Let K be a local field. Then the groups O_K, $\mathfrak{m}_K^n$ and U_K are compact.*

Proof. One can easily prove the sequential compacteness of O_K considering finite sets $O_K/\mathfrak{m}_K^n$. Since $\mathfrak{m}_K = \pi_K O_K$ and $U_K \subset O_K$ is closed, this proves the lemma. □

2.3. If L/K is a finite extension of local fields, we define the ramification index $e(L/K)$ and the inertia degree $f(L/K)$ of L/K by

$$e(L/K) = v_L(\pi_K), \qquad f(L/K) = [k_L : k_K].$$

Recall the fundamental formula

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

(see, for example, [**2**, Ch. 3, Thm 6]).

2.4. Let K be a local field, $q = |k_K|$.

Proposition 2.5. *i) For any $x \in k_K$ there exists a unique $[x]$ such that $x = [x]$* mod π_K *and $[x]^q = [x]$.*

ii) The multiplicative group of K contains the subgroup μ_{q-1} of $(q-1)$th roots of unity and the map

$$\begin{aligned}[\,\cdot\,] : k_K^* &\to \mu_{q-1},\\ x &\mapsto [x]\end{aligned}$$

is an isomorphism.

iii) If $\mathrm{char}(K) = p$, *then $[\,\cdot\,]$ gives an inclusion of fields $k_K \hookrightarrow K$.*

Proof. The statements i-ii) follow easily from Hensel's lemma, applied to the polynomial $X^q - X$.

iii) If $\mathrm{char}(K) = p$ then for any $x, y \in k_K$

$$([x] + [y])^q = [x]^q + [y]^q = [x] + [y]$$

(use binomial expansion). By unicity, this implies that $[x + y] = [x] + [y]$. □

Corollary 2.6. *Every $x \in O_K$ can be written by a unique way in the form*

$$x = \sum_{i=0}^{\infty} [a_i]\pi_K^i.$$

Exercise 1. Let $x \in k_K$ and let $\widehat{x} \in O_K$ be any lift of x under the map $O_K \to k_K$.

a) Show that the sequence $(\widehat{x}^{q^n})_{n\in\mathbf{N}}$ converges to an element of O_K which doesn't depend on the choice of $\widehat{x}$.

b) Show that $[x] = \lim_{n\to+\infty} \widehat{x}^{q^n}$.

THEOREM 2.7. *Let K be a local field and $p = \mathrm{char}(k_K)$.*

i) If $\mathrm{char}(K) = p$, then K is isomorphic to the field $k_K((X))$ of Laurent power series, where k_K is the residue field of K and X is transcendental over k. The discrete valuation on K is given by

$$v_K(f(X)) = \mathrm{ord}_X f(X).$$

Note that X is a uniformizer of K and $O_K \simeq k_K[[X]]$.

ii) If $\mathrm{char}(K) = 0$, then K is isomorphic to a finite extension of the field of p-adic numbers $\mathbf{Q}_p$. The absolute value on K is the extension of the p-adic absolute value

$$\left|\frac{a}{b}p^k\right|_p = p^{-k}, \qquad p \nmid a, b.$$

PROOF. i) Assume that $\mathrm{char}(K) = p$. By Corollary 2.6, we have a bijection

$$\begin{aligned} &K \to k_K((X)),\\ &x \mapsto x = \sum_{i=0}^{\infty} a_i X^i, \qquad \text{where } x = \sum_{i=0}^{\infty} [a_i]\pi_K^i. \end{aligned}$$

By Proposition 2.5 iv), this map is an isomorphism.

ii) Assume that $\mathrm{char}(K) = 0$. Then $\mathbf{Q} \subset K$. The absolute value $|\cdot|_K$ induces an absolute value on $\mathbf{Q}$. By Ostrowski theorem, any non archimedean absolute value on $\mathbf{Q}$ is equivalent to the p-adic absolute value for some prime p. Since K is complete, this implies that $\mathbf{Q}_p \subset K$. Since k_K is finite, $[k_K : \mathbf{F}_p] < +\infty$. Since v_K is discrete, $e(K/\mathbf{Q}_p) = v_K(p) < +\infty$. This implies that $[K : \mathbf{Q}_p] < +\infty$.

□

2.8. The group of units U_K is equipped with the exhaustive descending filtration

$$U_K^{(n)} = 1 + \pi_K^n O_K, \qquad n \geqslant 0.$$

PROPOSITION 2.9. *i) The map*

$$U_K \to k_K^*, \qquad x \mapsto \bar{x} := x \pmod{\pi_K}$$

induces an isomorphism $U_K/U_K^{(1)} \simeq k_K^*$.

ii) For any $n \geqslant 1$, the map

$$U_K^{(n)} \to k_K, \qquad 1 + \pi_K^n x \mapsto \bar{x}$$

induces an isomorphism $U_K^{(n)}/U_K^{(n+1)} \simeq k_K^+$.

PROOF. The proof is left as an exercise. □

DEFINITION 2.10. *One says that L/K is*

i) unramified if $e(L/K) = 1$ (and therefore $f(L/K) = [L : K]$);

ii) totally ramified if $e(L/K) = [L : K]$ (and therefore $f(L/K) = 1$).

2.10.1. The unramified extensions can be described entirely in terms of the residue field k_K. Namely, there exists a one-to-one correspondence

$$\{\text{finite extensions of } k_K\} \longleftrightarrow \{\text{finite unramified extensions of } K\}$$

which can be explicitly described as follows. Let k/k_K be a finite extension of k_K. Write $k = k_K(\alpha)$ and denote by $f(X) \in k_K[X]$ the minimal polynomial of α. Let $\widehat{f}(X) \in O_K[X]$ denote any lift of $f(X)$. Then we associate to k the extension $L = K(\widehat{\alpha})$, where $\widehat{\alpha}$ is the unique root of $\widehat{f}(X)$ whose reduction modulo $\mathfrak{m}_L$ is α. An easy argument using Hensel's lemma shows that L doesn't depend on the choice of the lift $\widehat{f}(X)$.

Unramified extensions form distinguished classes of extensions in the sense of [**21**]. In particular, for any finite extension L/K one can define its maximal unramified subextension L_{ur} as the compositum of all its unramified subextensions. Then one has

$$f(L/K) = [L_{\mathrm{ur}} : K], \qquad e(L/K) = [L : L_{\mathrm{ur}}].$$

The extension L/L_{ur} is totally ramified.

2.10.2. Assume that L/K is totally ramified of degree n. Let π_L be any uniformizer of L and let

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in O_K[X]$$

be the minimal polynomial of π_L. Then $f(X)$ is an Eisenstein polynomial, namely

$$v_K(a_i) \geqslant 1 \qquad \text{for } 0 \leqslant i \leqslant n-1, \text{ and } v_K(a_0) = 1.$$

Conversely, if α is a root of an Eisenstein polynomial of degree n over K, then $K(\alpha)/K$ is totally ramified of degree n, and α is an uniformizer of $K(\alpha)$.

Definition 2.11. *One says that an extension L/K is*
i) tamely ramified, if $e(L/K)$ is coprime to p.
ii) totally tamely ramified, if it is totally ramified and $e(L/K)$ is coprime to p.

Using Krasner's lemma, it is easy to give an explicit description of totally tamely ramified extensions.

Proposition 2.12. *If L/K is totally tamely ramified of degree n, then there exists a uniformizer $\pi_K \in K$ such that*

$$L = K(\pi_L), \qquad \pi_L^n = \pi_K.$$

Proof. Assume that L/K is totally tamely ramified of degree n. Let Π be a uniformizer of L and $f(X) = X^n + \cdots + a_1X + a_0$ its minimal polynomial. Then $f(X)$ is Eisenstein, and $\pi_K := -a_0$ is a uniformizer of K. Let $\alpha_i \in \overline{K}$ $(1 \leqslant i \leqslant n)$ denote the roots of $g(X) := X^n + a_0$. Then

$$|g(\Pi)|_K = |g(\Pi) - f(\Pi)|_K \leqslant \max_{1 \leqslant i \leqslant n-1} |a_i \Pi^i|_K < |\pi_K|_K$$

Since $|g(\Pi)|_K = \prod_{i=1}^{n} (\Pi - \alpha_i)$ and $\Pi = (-1)^n \prod_{i=1}^{n} \alpha_i$, we have

$$\prod_{i=1}^{n} |\Pi - \alpha_i|_K < \prod_{i=1}^{n} |\alpha_i|_K.$$

Therefore there exists i_0 such that

(1) $$|\Pi-\alpha_{i_0}|_K<|\alpha_{i_0}|_K.$$

Set $\pi_L=\alpha_{i_0}$. Then
$$\prod_{i\neq i_0}(\pi_L-\alpha_i)=g'(\pi_L)=n\pi_L^{n-1}.$$
Since $(n,p)=1$ and $|\pi_L-\alpha_i|_K\leqslant |\pi_L|_K$, the previous equality implies that
$$d_{\pi_L}:=\min_{i\neq i_0}|\pi_L-\alpha_i|_K=|\pi_L|_K.$$
Together with (1), this gives that
$$|\Pi-\alpha_{i_0}|_K<d_{\pi_L}.$$
Applying Krasner's lemma we find that $K(\pi_L)\subset L$. Since $[L:K]=[K(\pi_L):K]=n$, we obtain that $L=K(\pi_L)$, and the proposition is proved. □

Exercise 2. Show that $\mathbf{Q}_p(\sqrt[p-1]{-p})=\mathbf{Q}_p(\zeta_p)$, where ζ_p is a primitive pth root of unity.

Exercise 3. Let K be a local field and π_K and π'_K be two uniformizers of K. Show that
$$K^{\mathrm{ur}}(\sqrt[n]{\pi_K})=K^{\mathrm{ur}}(\sqrt[n]{\pi'_K}),\qquad \text{for any } (n,p)=1.$$
Deduce that the compositum of two tamely ramified extensions is tamely ramified.

2.13. The following useful proposition follows easily from Krasner's lemma.

Proposition 2.14. *Let K be a local field of characteristic* 0. *For any $n\geqslant 1$ there exists only a finite number of extensions of K of degree n.*

Proof. See [**19**, Chapter 2, Proposition 14]. Since there exists only one unramified extension of given degree, it is sufficient to prove that for each n there exists only a finite number of totally ramified extensions of degree n. Each such extension is generated by a root of an Eisenstein polynomial of degree n. The map
$$f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0\mapsto (a_{n-1},\dots,a_1,a_0)$$
defines a bijection
$$\{\text{Eisenstein polynomials of degree } n\}\longleftrightarrow \mathfrak{m}_K\times\cdots\times\mathfrak{m}_K\times U_K.$$
By Krasner's lemma, for each Eisenstein polynomial $f(X)$, there exists an open neighborhood V of $f(X)$ such that the roots of any $g(X)\in V$ generate the same extensions of K as the roots of $f(X)$. Now the proposition follows from compacteness of $\mathfrak{m}_K\times\cdots\times\mathfrak{m}_K\times U_K$. □

Remark 2.15. *A local field of characteristic p has infinitely many separable extensions of degree p. It could be proved using Artin–Schreier extensions (see for example* [**21**, Chapter VI,§6] *for basic results of Artin–Schreier theory).*

3. The different

3.1. Let L/K be a finite separable extension of local fields. Consider the bilinear form

$$t_{L/K}\,:\,L\times L\to K,\qquad t_{L/K}(x,y)=\mathrm{Tr}_{L/K}(xy), \tag{2}$$

where $\mathrm{Tr}_{L/K}$ is the trace map. It is well known that this form is non degenerate. The set

$$O_L':=\{x\in L\mid t_{L/K}(x,y)\in O_K,\quad \forall y\in O_L\}$$

is a fractional ideal, and

$$\mathfrak{D}_{L/K}:=O_L^{-1}:=\{x\in L\mid xO_L'\subset O_L\}$$

is an ideal of O_L.

Definition. *The ideal $\mathfrak{D}_{L/K}$ is called the different of L/K.*

If $K\subset L\subset M$ is a tower of separable extensions, then

$$\mathfrak{D}_{M/K}=\mathfrak{D}_{M/L}\mathfrak{D}_{L/K}. \tag{3}$$

(see, for example, [**19**, Chapter 3, Proposition 5]).

Set

$$v_L(\mathfrak{D}_{L/K})=\inf\{v_L(x)\mid x\in\mathfrak{D}_{L/K}\}.$$

Proposition 3.2. *Let L/K be a finite separable extension of local fields and $e=e(L/K)$ the ramification index. The following assertions hold true:*

i) If $O_L=O_K[\alpha]$, and $f(X)\in O_K[X]$ is the minimal polynomial of α, then $\mathfrak{D}_{L/K}=(f'(\alpha))$.

ii) $\mathfrak{D}_{L/K}=O_L$ if and only if L/K is unramified.

iii) $v_L(\mathfrak{D}_{L/K})\geqslant e-1$.

iv) $v_L(\mathfrak{D}_{L/K})=e-1$ if and only if L/K is tamely ramified.

Proof. The first statement holds in the more general setting of Dedekind rings (see, for example, [**19**, Chapter 3, Proposition 2]). We prove ii-iv) for reader's convenience (see [**19**, Chapter 3, Proposition 8] for more detail).

a) Let L/K be an unramified extension of degree n. Write $k_L=k_K(\bar\alpha)$ for some $\bar\alpha\in k_L$. Let $f(X)\in k_K[X]$ denote the minimal polynomial of $\bar\alpha$. Then $\deg(\bar f)=n$. Take any lift $f(X)\in O_K[X]$ of $\bar f(X)$ of degree n. By Proposition 1.4 (Hensel's lemma) there exists a unique root $\alpha\in O_L$ of $f(X)$ such that $\bar\alpha=\alpha \pmod{\mathfrak{m}_K}$. It's easy to see that $O_L=O_K[\alpha]$. Since $\bar f(X)$ is separable, $\bar f'(\bar\alpha)\neq 0$, and therefore $f'(\alpha)\in U_L$. Applying i), we obtain that

$$\mathfrak{D}_{L/K}=(f'(\alpha))=O_L.$$

Therefore $\mathfrak{D}_{L/K}=O_L$ if L/K is unramified.

b) Assume that L/K is totally ramified. Then $O_L=O_K[\pi_L]$, where π_L is any uniformizer of O_L. Let $f(X)=X^e+a_{e-1}X^{e-1}+\cdots+a_1X+a_0$ be the minimal polynomial of π_L. Then

$$f'(\pi_L)=e\pi_L^{e-1}+(e-1)a_{e-1}\pi_L^{e-2}+\cdots+a_1.$$

Since $f(X)$ is Eisenstein, $v_L(a_i) \geqslant e$, and an easy estimation shows that $v_L(f'(\pi_L)) \geqslant e-1$. Thus

$$v_L(\mathfrak{D}_{L/K}) = v_L(f'(\alpha)) \geqslant e-1.$$

This proves iii). Moreover, $v_L(f'(\alpha)) = e-1$ if and only if $(e,p)=1$ i.e. if and only if L/K is tamely ramified. This proves iv).

c) Assume that $\mathfrak{D}_{L/K} = O_L$. Then $v_L(\mathfrak{D}_{L/K}) = 0$. Let L_{ur} denote the maximal unramified subextension of L/K. By (3), a) and b) we have

$$v_L(\mathfrak{D}_{L/K}) = v_L(\mathfrak{D}_{L/L_{\mathrm{ur}}}) \geqslant e-1.$$

Thus $e=1$, and we showed that each extension L/K such that $\mathfrak{D}_{L/K} = O_L$ is unramified. Together with a), this proves i). □

Exercise 4. Let L/K be a finite extension of local fields. Show that $O_L = O_K[\alpha]$ for some $\alpha \in O_L$. Hint: take $\alpha = [\xi] + \pi_L$, where $k_L = k_K(\xi)$.

4. Ramification filtration

4.1. In this section, we determine Galois groups of unramified extensions.

Proposition 4.2. *Let L/K be a finite unramified extension. Then L/K is a Galois extension and the natural homomorphism*

$$r : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$$

is an isomorphism.

Proof. a) Write $k_L = k_K(\xi)$ and denote by $f(X)$ the minimal polynomial of ξ. Let $\widehat{f}(X) \in O_K[X]$ be a lift of $f(X)$. Then $O_L = O_K[\widehat{\xi}]$ where $\widehat{f}(\widehat{\xi}) = 0$ and $\xi = \widehat{\xi} \pmod{\pi_L}$ Since k_L/k_K is a Galois extension, all roots $\xi_1, \dots, \xi_n$ of $f(X)$ lie in k_L. By Hensel's lemma, there exists unique roots $\widehat{\xi}_1, \dots, \widehat{\xi}_n \in O_L$ of $\widehat{f}(X)$ such that $\xi_i = \widehat{\xi}_i \pmod{\pi_L}$. This shows that L/K is a Galois extension.

b) Let $g_i \in \mathrm{Gal}(L/K)$ be such that $g_i(\widehat{\xi}) = \widehat{\xi}_i$. Then $r(g_i)(\xi) = \xi_i$. This shows that r is an isomorphism. □

Recall that $\mathrm{Gal}(k_L/k_K)$ is the cyclic group generated by the automorphism of Frobenius:

$$\mathrm{f}_{k_L/k_K}(x) = x^q, \qquad \forall x \in k_L.$$

Definition. *We denote by $F_{L/K}$ and call the Frobenius automorphism of L/K the pre-image of f_{k_L/k_K} in* $\mathrm{Gal}(L/K)$. *Thus $F_{L/K}$ is the unique automorphism such that*

$$F_{L/K}(x) \equiv x^q \pmod{\pi_L}.$$

4.3. Let L/K be a arbitrary finite Galois extension, and let L_{ur} denote its maximal unramified subextension. Then we have an exact sequence

$$\{1\} \to I_{L/K} \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_{\mathrm{ur}}/K) \to \{1\}$$

The subgroup $I_{L/K} = \mathrm{Gal}(L/L_{\mathrm{ur}})$ is called the inertia subgroup of $\mathrm{Gal}(L/K)$.

4.4. Let L/K be a finite Galois extension of local fields. Set $G = \mathrm{Gal}(L/K)$. For any integer $i \geqslant -1$ define

$$G_i = \{g \in G \mid v_L(g(x) - x) \geqslant i + 1, \quad \forall x \in O_L\}.$$

Definition. *The subgroups G_i are called ramification subgroups.*

We have a descending chain

$$G = G_{-1} \supset G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

called the ramification filtration on G (in low numbering). Below we collect some basic properties of these subgroups.

1) $G_{-1} = G$ and $G_0 = I_{L/K}$.

Proof. We have

$$g \in G_0 \Leftrightarrow g(x) \equiv x \pmod{\pi_L} \Leftrightarrow g \in I_{L/K}.$$

□

2) G_i are normal subgroups of G.

Proof. Let $g \in G_i$ and $s \in G$. Then

$$v_L(s^{-1}gs(x) - x) = v_L(s^{-1}gs(x) - s^{-1}s(x)) = v_L(gs(x) - s(x)).$$

□

3) For each $i \geqslant 0$ one has

$$G_i = \left\{ g \in G \mid v_L\left(1 - \frac{g(\pi_L)}{\pi_L}\right) \geqslant i \right\}.$$

Proof. We have

$$g(\pi_L^k) - \pi_L^k = (g(\pi_L))^k - \pi_L^k = (g(\pi_L) - \pi_L)a, \qquad a \in O_L$$

Since g acts trivially on Teichmüller lifts, this implies that

$$g \in G_i \Leftrightarrow v_L(g(\pi_L) - \pi_L) \geqslant i + 1.$$

This implies the assertion. □

Proposition 4.5. *i) For all $i \geqslant 0$, the map*

$$s_i : G_i/G_{i+1} \to U_L^{(i)}/U_L^{(i+1)}, \tag{4}$$

which sends $\bar{g} = g \mod G_{i+1}$ to $s_i(\bar{g}) = \frac{g(\pi_L)}{\pi_L} \pmod{U_L^{(i+1)}}$, is a well defined monomorphism which doesn't depend on the choice of the uniformizer π_L of L.

ii) The composition of s_i with the maps (2.9) gives monomorphisms

$$\delta_0 : G_0/G_1 \to k^*, \qquad \delta_i : G_i/G_{i+1} \to k^+, \quad \textit{for all } i \geqslant 1. \tag{5}$$

Proof. The proof is straightforward. See [**28**, Chapitre IV, Propositions 5-7]. □

Corollary 4.6. *The Galois group G is solvable for any Galois extension.*

Corollary 4.7. *$L_{\mathrm{tr}} = L^{G_1}$ is the maximal tamely ramified subextension of L.*

To sup up, we have the tower of extensions

(6)
$$\begin{tikzcd}
L \arrow[d, dash, "G_1"] \arrow[dd, dash, bend right, "G_0"'] \\
L_{\mathrm{tr}} \arrow[d, dash, "G_0/G_1"] \\
L_{\mathrm{ur}} \arrow[d, dash, "G/G_0"] \\
K
\end{tikzcd}$$

Definition 4.8. *The group $P_{L/K} := G_1$ is called the wild inertia subgroup.*

4.9. The different $\mathfrak{D}_{L/K}$ of a finite Galois extension can be computed in terms of the ramification subgroups.

Proposition 4.10. *Let L/K be a finite Galois extension of local fields. Then*

(7)
$$v_L(\mathfrak{D}_{L/K}) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

Proof. Let $O_L = O_K[\alpha]$ and let $f(X)$ be the minimal polynomial of α. For any $g \in G$ set $i_{L/K}(g) = v_L(g(\alpha) - \alpha)$. From the definition of ramification subgroups it follows that $g \in G_i$ if and only if $i_{L/K}(g) \geqslant i + 1$. Since

$$f'(\alpha) = \prod_{g \neq 1}(\alpha - g(\alpha)),$$

we have

$$\begin{aligned}
v_L(\mathfrak{D}_{L/K}) = v_L(f'(\alpha)) = \sum_{g\neq 1} v_L(\alpha - g(\alpha)) = \sum_{g \neq 1} i_{L/K}(g) = \sum_{i=0}^{\infty}(i+1)(|G_i| - |G_{i+1}|) \\
= \sum_{i=0}^{\infty}(i+1)((|G_i| - 1) - (|G_{i+1}| - 1)) = \sum_{i=0}^{\infty}(|G_i| - 1).
\end{aligned}$$

□

5. The upper ramification

5.1. This section is an introduction to Herbrand's theory of upper ramification. It is convenient to define G_u for all *real* $u \geqslant -1$ setting

$$G_t = G_i, \quad \text{where } i \text{ is the smallest integer} \geqslant u.$$

For any finite Galois extension the Hasse–Herbrand functions are defined as follows

$$
\begin{aligned}
&\varphi_{L/K}(u) = \begin{cases} u & \text{if } -1 \leqslant u \leqslant 0, \\ \displaystyle\int_0^u \frac{dt}{(G_0 : G_t)}, \text{if } u \geqslant 0 \end{cases} \\
&\psi_{L/K}(v) = \varphi_{L/K}^{-1}(v).
\end{aligned} \tag{8}
$$

From definition it follows that they are inverse to each other.

5.2. Let $K \subset F \subset L$ be a tower of finite Galois extensions. Set $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/F)$. It is clear that

$$G_i \cap H = H_i, \qquad \forall i \geqslant -1.$$

We want to describe the image of G_i in G/H under the canonical projection $G \to G/H$.

THEOREM 5.3. *i)* (Herbrand). *For any $u \geqslant 0$*

$$G_u H/H \simeq (G/H)_{\varphi_{L/F}(u)}.$$

ii) $\varphi_{L/K} = \varphi_{F/K} \circ \varphi_{L/F}$ and $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$.

PROOF. i) See [**28**, Chapter IV, §3].
ii) We deduce ii) from i). We have

$$(\varphi_{F/K} \circ \varphi_{L/F})'(x) = \varphi'_{F/K}(\varphi_{L/F}(x))\varphi'_{L/F}(x) = \frac{1}{((G/H)_0 : (G/H)_{\varphi_{L/F}(x)}) \cdot (H_0 : H_x)}$$

and

$$(G/H)_{\varphi_{L/F}(x)} = G_x H/H = G_x/(H \cap G_x) = G_x/H_x.$$

This implies that

$$((G/H)_0 : (G/H)_{\varphi_{L/F}(x)}) = (G_0 : G_x)/(H_0 : H_x),$$

and therefore

$$(\varphi_{F/K} \circ \varphi_{L/F})'(x) = \frac{1}{(G : G_x)} = \varphi'_{L/K}(x).$$

This implies ii). □

DEFINITION. *The ramification subgroups in upper numbering are defined as follows:*

$$G^{(v)} = G_{\psi_{L/K}(v)}$$

or equivalently $G^{\varphi_{L/K}(u)} = G_u$.

THEOREM 5.4.

$$(G/H)^{(v)} = G^{(v)}/G^{(v)} \cap H, \qquad \forall v \geqslant 0.$$

Proof. We have $(G/H)^{(v)} = (G/H)_{\psi_{F/K}(v)}$ and

$$G^{(v)}/G^{(v)} \cap H = G_{\psi_{L/K}(v)}/G_{\psi_{L/K}(v)} \cap H.$$

Setting $x = \psi_{L/K}(v)$, we have

$$G^{(v)}/G^{(v)} \cap H = G_x/G_x \cap H$$

and $(G/H)^{(v)} = (G/H)_{\varphi_{L/F}(x)}$. Now we apply Theorem 5.3. □

Proposition 5.5. *One has*

$$\psi_{L/K}(v) = \begin{cases} v & \text{if } -1 \leqslant v \leqslant 0, \\ \displaystyle\int_0^v (G^{(0)} : G^{(t)})dt & \text{if } u \geqslant 0. \end{cases}$$

Proof. Since $\psi_{L/K}(v) = \varphi_{L/K}^{-1}(v)$, we have

$$\psi'_{L/K}(\varphi_{L/K}(u)) = \frac{1}{\varphi'_{L/K}(u)} = (G_0 : G_u) = (G^{(0)} : G^{(\varphi_{L/K}(u))}).$$

Setting $t = \varphi_{L/K}(u)$, we obtain that $\psi'_{L/K}(t) = (G^{(0)} : G^{(t)})$. This proves the proposition. □

5.6. Hebrand's theorem allows to define the ramification filtration for infinite Galois extensions. Namely, for any (finite or infinite) Galois extension of local fields M/K define

$$\mathrm{Gal}(M/K)^{(v)} = \varprojlim_{L/K \text{ finite}} \mathrm{Gal}(L/K)^{(v)}$$

In particular, we can consider the ramification filtration on the absolute Galois group G_K of K. This filtration contains fundamental information about the field K.

5.7. Formula (7) can be written in terms of upper ramification subgroups:

Theorem 5.8. *Let L/K be a finite Galois extension. Then*

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty} \left(1 - \frac{1}{|G^{(v)}|}\right) dv.$$

Proof. By (7), we have

$$v_K(\mathfrak{D}_{L/K}) = \frac{v_L(\mathfrak{D}_{L/K})}{e(L/K)} = \frac{1}{|G_0|} \int_{-1}^{\infty} (|G_u| - 1)du.$$

Setting $u = \psi_{L/K}(v)$ and taking into accout that $\psi'_{L/K}(v) = (G^{(0)} : G^{(v)})$ we can write:

$$\begin{aligned} v_K(\mathfrak{D}_{L/K}) &= \frac{1}{|G_0|} \int_{-1}^{\infty} (|G^{(v)}| - 1)\psi'_{L/K}(v)dv \\ &= \frac{1}{|G_0|} \int_{-1}^{\infty} (|G^{(v)}| - 1)(G^{(0)} : G^{(v)})dv = \int_{-1}^{\infty} \left(1 - \frac{1}{|G^{(v)}|}\right) dv. \end{aligned}$$

□

In this form, it can be generalized to arbitrary finite extensions as follows. For any $v \geqslant 0$ define

$$\overline{K}^{(v)} = \overline{K}^{G_K^{(v)}}.$$

Theorem 5.9. *For any finite extension L/K one has*

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty} \left(1 - \frac{1}{[L : L \cap \overline{K}^{(v)}]}\right) dv \tag{9}$$

Proof. See [**6**, Lemma 2.1]). □

Exercise 5. 1) Let ζ_{p^n} be a p^nth primitive root of unity. Set $K = \mathbf{Q}_p(\zeta_{p^n})$ and $G = \mathrm{Gal}(K/\mathbf{Q}_p)$. We have isomorphism

$$\chi_n : G \simeq (\mathbf{Z}/p^n\mathbf{Z})^*, \qquad g(\zeta_{p^n}) = \zeta_{p^n}^{\chi_n(g)}.$$

Set $\Gamma = (\mathbf{Z}/p^n\mathbf{Z})^*$. Let $\Gamma^{(m)} = \{\bar{a} \in (\mathbf{Z}/p^n\mathbf{Z})^* \mid a \equiv 1 \pmod{p^m}\}$ (in particular $\Gamma^{(0)} = (\mathbf{Z}/p^n\mathbf{Z})^*$ and $\Gamma^{(n)} = \{1\}$).

a) Show that

$$\chi_n(G_i) = \Gamma^{(m)}, \quad \text{where } m \text{ is the unique integer such that } p^{m-1} \leqslant i < p^m.$$

b) Give Hasse–Herbrand's functions $\phi_{K/\mathbf{Q}_p}$ and $\psi_{K/\mathbf{Q}_p}$.

c) Set

$$\Gamma^{(v)} = \Gamma^{(m)} \qquad \text{where } m \text{ is the smallest integer} \geqslant v.$$

Show that the upper ramifiation filtration on G is given by

$$\chi_n(G^{(v)}) = \Gamma^{(v)}.$$

2) Let $(\zeta_{p^n})_{n\geqslant 1}$ denote a system of p^nth primitive roots of unity such that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$. Set $K_n = \mathbf{Q}_p(\zeta_{p^n})$, $K_\infty = \underset{n\geqslant 1}{\cup} K_n$ and $G_\infty = \mathrm{Gal}(K_\infty/\mathbf{Q}_p)$. Let $U_{\mathbf{Q}_p} = \mathbf{Z}_p^*$ be the group of units of $\mathbf{Q}_p$. We have the isomorphism:

$$\chi : G \simeq U_{\mathbf{Q}_p}, \qquad g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}, \quad \forall n \geqslant 1.$$

For any $v \geqslant 0$ set

$$U_{\mathbf{Q}_p}^{(v)} = U_{\mathbf{Q}_p}^{(m)}, \qquad \text{where } m \text{ is the smallest integer} \geqslant v.$$

Show that

$$\chi(G^{(v)}) = U_{\mathbf{Q}_p}^{(v)}, \qquad \forall v \geqslant 0.$$

6. Galois groups of local fields

6.1. The maximal unramified extension. In this section, we review the structure of Galois groups of local fields. Let K be a local field. Fix a separable closure $\overline{K}$ of K and set $G_K = \mathrm{Gal}(\overline{K}/K)$. Since the compositum of two unramified (respectively tamely ramified) extensions of K is unramified (respectively tamely ramified) we have the well defined notions of the maximal unramified (respectively maximal tamely ramified) extension of K. We denote these extension by K^{ur} and K^{tr} respectively.

For each n there exists a unique unramified Galois extension K_n of degree n, and we have a canonical isomorphism $\mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/n\mathbf{Z}$ which sends the Frobenius automorphism $F_{K_n/K}$ onto $1 \mod n\mathbf{Z}$. If $n \mid m$, the diagram

$$\begin{tikzcd}
\mathrm{Gal}(K_m/K) \arrow[r, "\sim"] \arrow[d] & \mathbf{Z}/m\mathbf{Z} \arrow[d] \\
\mathrm{Gal}(K_n/K) \arrow[r, "\sim"] & \mathbf{Z}/n\mathbf{Z}
\end{tikzcd}$$

commutes. Passing to projective limits, we et

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) = \varprojlim_n \mathrm{Gal}(K_n/K) \xrightarrow{\sim} \widehat{\mathbf{Z}},$$

where $\widehat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/n\mathbf{Z}$. To sum up, the maximal unramified extension K^{ur} of K is procyclic and its Galois group is generated by the Frobenius automorphism F_K:

$$\begin{aligned}
\mathrm{Gal}(K^{\mathrm{ur}}/K) &\xrightarrow{\sim} \widehat{\mathbf{Z}}, \\
F_K &\longleftrightarrow 1. \\
F_K(x) &\equiv x^{q_K} \pmod{\pi_K}, \qquad \forall x \in O_{K^{\mathrm{ur}}}.
\end{aligned}$$

Exercises 6. 1) Let ℓ be a prime number. Show that $\varprojlim_k \mathbf{Z}/\ell^k\mathbf{Z} \simeq \mathbf{Z}_\ell$.

2) Show that $\widehat{\mathbf{Z}} \simeq \prod_\ell \mathbf{Z}_\ell$.

3) Let K be a local field with residue field of characteristic p. Show that

$$K^{\mathrm{ur}} = \bigcup_{(n,p)=1} K(\zeta_n).$$

6.2. The maximal tamely ramified extension. Passing to direct limit in the diagram (6), we have:

(10)
$$\begin{tikzcd}
\overline{K} \arrow[d, dash, "P_K"] \arrow[dd, dash, bend right=60, "I_K"'] \\
K^{\mathrm{tr}} \arrow[d, dash] \\
K^{\mathrm{ur}} \arrow[d, dash, "\widehat{\mathbf{Z}}"'] \\
K
\end{tikzcd}$$

Consider the exact sequence

(11) $$1 \to \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \to \mathrm{Gal}(K^{\mathrm{tr}}/K) \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \to 1.$$

Here $\mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \widehat{\mathbf{Z}}$. From the explicit description of tamely ramified extensions (see also Exercise 3), it follows that K^{tr} is generated over K^{ur} by the roots $\pi_K^{1/n}$, $(n,p) = 1$ of any uniformizer π_K of K. Since

$$\mathrm{Gal}(K^{\mathrm{ur}}(\pi_K^{1/n})/K^{\mathrm{ur}}) \simeq \mathbf{Z}/n\mathbf{Z} \quad \text{(not canonically)}$$

this immediately implies that

$$\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \simeq \widehat{\mathbf{Z}} \simeq \prod_{\ell \neq p} \mathbf{Z}_l. \tag{12}$$

For any $(n,p)=1$ set $L_n = K(\zeta_n, \pi_K^{1/n})$. It's easy to see that $\mathrm{Gal}(L_n/K)$ is generated by the automorphisms $\widehat{F}_n$ and τ_n such that

$$\begin{aligned} \widehat{F}_n|_{K(\zeta_n)} &= F_{K(\zeta_n)/K}, & \widehat{F}_n(\pi_K^{1/n}) &= \pi_K^{1/n}, \\ \tau_n|_{K(\zeta_n)} &= \mathrm{id}_{K(\zeta_n)}, & \tau_n(\pi_K^{1/n}) &= \zeta_n \pi_K^{1/n}. \end{aligned}$$

These automorphisms are related by the unique relation

$$\widehat{F}_n \tau_n = \tau_n^{q_K} \widehat{F}_n, \qquad q_K = |k_K|.$$

Passing to projective limit, we obtain:

Proposition 6.3 (Iwasawa). *The group* $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ *is topologically generated by two automorphisms* $\widehat{F}_K$ *and* τ_K *with the only relation*

$$\widehat{\mathrm{Fr}}_K \, \tau_K \, \widehat{\mathrm{Fr}}_K^{-1} = \tau_K^{q_K}. \tag{13}$$

Proof. See [**24**, Theorem 7.5.3] for more detail. □

6.4. Local class field theory. We say that a Galois extension L/K is abelian if $\mathrm{Gal}(L/K)$ is an abelian group. It's easy to see that the compositum of two abelian extensions is abelian. Denote by K^{ab} compositum of all abelian extensions of K. Then $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is canonically isomorphic to the abelianization $G_K^{\mathrm{ab}} = G_K/[G_K, G_K]$ of the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$. Local class field theory gives an explicit description of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ in terms of K.

Theorem 6.5. *here exists a canonical group homomorphism (called the reciprocity map) with dense image*

$$\theta_K \,:\, K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that

i) *For any finite abelian extension* L/K*, the homomorphism* θ_K *induces an isomorphism*

$$\theta_{L/K} \,:\, K^*/N_{L/K}(L^*) \xrightarrow{\sim} \mathrm{Gal}(L/K),$$

where $N_{L/K} : L \to K$ *is the norm map.*

ii) *If* L/K *is unramified, then for any uniformizer* $\pi_K \in K^*$ *the automorphism* $\theta_{L/K}(\pi)$ *coincides with the arithmetic Frobenius* $F_{L/K}$.

iii) *For any* $x \in K^*$*, the automorphism* $\theta_K(x)$ *acts on* K^{ur} *by*

$$\theta_K(x)|_{K^{\mathrm{ur}}} = F_K^{v_K(x)}.$$

Remark 6.6. *Local class field theory was developed by Hasse. The modern approach bases on the cohomology of finite groups (see* [**28**] *or* [**5**, Chapter VI]*, written by Serre).*

It can be shown, that the reciprocity map is compatible with the ramification filtration. Namely, for any real $v \geqslant 0$ set $U_K^{(v)} = U_K^{(n)}$, where n is the smallest integer $\geqslant v$. Then

$$\theta_K\left(U_K^{(v)}\right) = \mathrm{Gal}(K^{\mathrm{ab}}/K)^{(v)}, \qquad \forall v \geqslant 0. \tag{14}$$

For the classical proof of this result, see [**28**, Chapter XV].

6.7. Ramification jumps.

Definition. *Let L/K be a Galois extension of local fields (finite or infinite). We say that $v \geqslant -1$ is a ramification jump of L/K if*

$$\mathrm{Gal}(L/K)^{(v+\varepsilon)} \neq \mathrm{Gal}(L/K)^{(v)}, \qquad \forall \varepsilon > 0.$$

From (14) it follows that the ramification jumps of K^{ab}/K are the integers $v_{-1} = -1$, $v_0 = 0$, $v_1 = 1, \ldots$.

If L/K is an abelian extension with Galois group G, then by by Galois theory $G = G_K^{\mathrm{ab}}/H$ for some closed normal subgroup $H \subset G_K^{\mathrm{ab}}$. From Herbrand's theorem we have $G^{(v)} = (G_K^{\mathrm{ab}})^{(v)}/H \cap (G_K^{\mathrm{ab}})^{(v)}$. Therefore from (14) the jumps of the ramification filtration on G are integers (theorem of Hasse-Arf). Let denote them by $v_0 < v_1 < v_2 < \ldots$. Then from Proposition 4.5 i) it follows that the quotients $G^{(v_i)}/G^{(v_{i+1})}$ are p-elementary abelian groups (each non trivial element has order p).

6.8. Example: ramification in $\mathbf{Z}_p$-extensions. We illustrate this theorem on the following example.

Definition. *A $\mathbf{Z}_p$-extension is a Galois extension L/K with Galois group isomorphic to $\mathbf{Z}_p$.*

Let L/K be a $\mathbf{Z}_p$-extension. Set $\Gamma = \mathrm{Gal}(L/K)$. For any n, $p^n\mathbf{Z}_p$ is the unique open subgroup of $\mathbf{Z}_p$ of index p^n and we denote by $\Gamma(n)$ the corresponding subgroup of Γ. Set $K_n = L^{\Gamma(n)}$. Then K_n is the unique subextension of L/K of degree p^n over K. We have

$$L = K_\infty := \bigcup_{n \geqslant 1} K_n, \qquad \mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}.$$

Let $(v_i)_{i \geqslant 0}$ denote the increasing sequence of ramification jumps of L/K. Since $\Gamma \simeq \mathbf{Z}_p$ and all quotients $\Gamma^{(v_i)}/\Gamma^{(v_{i+1})}$ are p-elementary, we obtain that

$$\Gamma^{(v_i)} = p^i\mathbf{Z}_p, \qquad \forall i \geqslant 0.$$

Proposition 6.9 (Tate [**30**]). *Let K be a finite extension of $\mathbf{Q}_p$ and let K_∞/K be totally ramified $\mathbf{Z}_p$-extension. Let $(v_i)_{i \geqslant 1}$ denote the increasing sequence of ramification jumps of K_∞/K. Then*

i) There exists i_0 such that

$$v_{i+1} = v_i + e_K, \qquad \forall i \geqslant i_0.$$

ii) There exists a constant c such that for all $n \geqslant 1$

$$v_K(\mathfrak{D}_{K_n/K}) = e_K n + c + a_n p^{-n},$$

where $(a_n)_{n \geqslant 1}$ is bounded.

We first prove the following auxiliary lemma:

LEMMA 6.10. *Let $K/\mathbf{Q}_p$ be a finite extension and let $e_K = e(K : \mathbf{Q}_p)$. Then*
i) The series

$$\log(1+x) = \sum_{m=1}^{\infty} (-1)^{m+1} \frac{x^m}{m}$$

converges for all $x \in \mathfrak{m}_K$.
ii) The series

$$\exp(x) = \sum_{m=0}^{\infty} \frac{x^m}{m!}$$

converges for all x such that $v_K(x) > \frac{e_K}{p-1}$.
iii) For any integer $n > \frac{e_K}{p-1}$ we have isomorphisms

$$\log : U_K^{(n)} \to \mathfrak{m}_K^n, \qquad \exp : \mathfrak{m}_K^n \to U_K^{(n)}$$

which are inverse to each other.

PROOF. We have

$$v_K(m) \leqslant e_K \log_p(m),$$

and

$$v_K(m!) = e_K\left([m/p] + [m/p^2] + \cdots\right) \leqslant \frac{e_K m}{p-1}.$$

This implies the convergence of the series. Other assertions can be proved by routine computations. □

COROLLARY 6.11. *For any integer $n > \frac{e_K}{p-1}$*

$$\left(U_K^{(n)}\right)^p = U_K^{(n+e_K)}.$$

PROOF. $\left(U_K^{(n)}\right)^p$ and $U_K^{(n+e_K)}$ have the same image under log. □

PROOF OF PROPOSITION.
Step 1. Let $\Gamma = \mathrm{Gal}(L/K)$. By Galois theory, $\Gamma = G_K^{\mathrm{ab}}/H$, where H is a closed subgroup. Consider the exact sequence

$$\{1\} \to \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \to G_K^{\mathrm{ab}} \xrightarrow{s} \mathrm{Gal}(K^{\mathrm{ur}}/K) \to \{1\}$$

Since K_∞/K is totally ramified, $(K^{\mathrm{ab}})^H \cap K^{\mathrm{ur}} = K$, and $s(H) = \mathrm{Gal}(K^{\mathrm{ur}}/K)$. Therefore

$$\Gamma \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})/(H \cap \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})).$$

By local class field theory, $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \simeq U_K$, and there exists a closed subgroup $N \subset U_K$ such that

$$\Gamma \simeq U_K/N.$$

The order of $U_K/U_K^{(1)} \simeq k_K^*$ is coprime with p. Therefore the index of $U_K^{(1)}/(N \cap U_K^{(1)})$ in U_K/N is coprime with p. On the other hand, $U_K/N \simeq \Gamma$ is a pro-p group. Therefore

$$U_K^{(1)}/(N \cap U_K^{(1)}) = U_K/N.$$

and we have an isomorphism

$$\rho\,:\,\Gamma\simeq U_K^{(1)}/(N\cap U_K^{(1)}).$$

Step 2. To simplify notation, set

$$\mathscr{U}^{(v)}=U_K^{(v)}/(N\cap U_K^{(v)}),\qquad \forall v\geqslant 1.$$

By (14) and Theorem 5.4

$$\rho(\Gamma^{(v)})\simeq \mathscr{U}^{(v)},\qquad v\geqslant 1.$$

Let γ be a topological generator of Γ. Then $\gamma_n=\gamma^{p^n}$ is a topological generator of $\Gamma(n)$. Let i_0 be an integer such that

$$\rho(\gamma_{i_0})\in \mathscr{U}^{(m_0)},$$

with some integer $m_0>\frac{e_K}{p-1}$. Fix such i_0 and assume that, for this fixed i_0, m_0 is the biggest integer satisfying these conditions. Since γ_{i_0} generates $\Gamma(i_0)$, this means that

$$\rho(\Gamma(i_0))=\mathscr{U}^{(m_0)},\qquad \text{but}\qquad \rho(\Gamma(i_0))\neq \mathscr{U}^{(m_0+1)}.$$

Therefore m_0 is the i_0-th ramification jump for K_∞/K, *i.e.*

$$m_0=v_{i_0}.$$

We can write $\rho(\gamma_{i_0})=\overline{x}$, where $\overline{x}=x \pmod{(N\cap U_K^{(m_0)})}$ and $x\in U_K^{(m_0)}\setminus U_K^{(m_0+1)}$. By Corollary 6.11,

$$x^{p^n}\in U_K^{(m_0+e_Kn)}\setminus U_K^{(m_0+e_Kn+1)},\qquad \forall n\geqslant 0.$$

Since $\rho(\gamma_{i_0+n})=\overline{x}^{p^n}$ and γ_{i_0+n} generates $\Gamma(m_0+n)$, this implies that

$$\rho(\Gamma(i_0+n))=\mathscr{U}^{(m_0+ne_K)}\quad \text{but}\quad \rho(\Gamma(i_0+n))\neq \mathscr{U}^{(m_0+ne_K+1)}.$$

This shows that for each integer $n\geqslant 0$ the ramification filtration has a jump at m_0+ne_K and

$$\Gamma^{(m_0+ne_K)}=\Gamma(i_0+n).$$

In other terms, for any *real* $v\geqslant v_{i_0}=m_0$ we have

$$\Gamma^{(v)}=\Gamma(i_0+n+1)\qquad\text{if}\qquad v_{i_0}+ne_K<v\leqslant v_{i_0}+(n+1)e_K.$$

This shows that $v_{i_0+n}=v_{i_0}+e_Kn$ for all $n\geqslant 0$, and the assertion i) is proved.

Step 3. We prove ii) applying Theorem 5.8. For any $n>0$, set $G(n)=\Gamma/\Gamma(n)$. We have

$$v_K(\mathfrak{D}_{K_n/K})=\int_{-1}^{\infty}\left(1-\frac{1}{|G(n)^{(v)}|}\right)dv.$$

By Herbrand's theorem, $G(n)^{(v)}=\Gamma^{(v)}/(\Gamma(n)\cap\Gamma^{(v)})$. Since $\Gamma^{(v_n)}=\Gamma(n)$, the ramification jumps of $G(n)$ are $v_0,v_1,\dots,v_{n-1}$, and we have

$$|G(n)^{(v)}|=\begin{cases}p^{n-i}, & \text{if } v_{i-1}<v\leqslant v_i,\\ 1, & \text{if } v>v_{n-1}\end{cases}\tag{15}$$

(for $i = 0$ we set $v_{i-1} := 0$ to uniformize notation). Assume that $n > i_0$. Then

$$v_K(\mathfrak{D}_{K_n/K}) = A + \int_{v_{i_0}}^{v_{n-1}} \left(1 - \frac{1}{|G(n)^{(v)}|}\right) dv,$$

where $A = \int_{-1}^{v_{i_0}} \left(1 - \frac{1}{|G(n)^{(v)}|}\right) dv$. We evaluate the second integral

$$\int_{v_{i_0}}^{v_{n-1}} \left(1 - \frac{1}{|G(n)^{(v)}|}\right) dv =$$
$$\sum_{i=i_0+1}^{n-1} (v_i - v_{i-1}) \left(1 - \frac{1}{|G(n)^{(v)}|}\right) = \sum_{i=i_0+1}^{n-1} e_K \left(1 - \frac{1}{p^{n-i}}\right)$$

(here we use i) and (15). An easy computation gives

$$\sum_{i=i_0+1}^{n-1} e_K \left(1 - \frac{1}{p^{n-i}}\right) = e_K(n - i_0 - 1) + \frac{e_K}{p-1} \left(1 - \frac{1}{p^{n-i_0-1}}\right).$$

Setting $c = A - e_K(i_0 + 1) + \frac{e_K}{p-1}$, we see that for $n > i_0$

$$v_K(\mathfrak{D}_{K_n/K}) = c + e_K n - \frac{1}{(p-1)p^{n-i_0-1}}.$$

This implies the proposition.

□

6.12. The absolute Galois group. The structure of the absolute Galois group G_K of a local field of characteristic p case can be determined easily. One sees that the wild ramification subgroup P_K is pro-p-free with a countable number of generators. This allows to describe G_K as an explicit semidirect product of the tame Galois group $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ and P_K (see [**24**, Theorem 7.5.13]). The characteristic 0 case is much more difficult. If K is a finite extension of $\mathbf{Q}_p$, the structure of the G_K in terms of generators and relations was first described by Yakovlev [**32**] under additional assumption $p \neq 2$. A simpler description was found by Jannsen and Wingberg in [**18**].

The ramification filtration $(G_K^{(v)})$ on G_K has a highly nontrivial structure. Abrashkin [**1**] and Mochizuki [**23**] proved that a local field can be completely determined by its absolute Galois group together with the ramification filtration.

CHAPTER 2

Almost étale extensions

1. Norms and traces

1.0.1. The results proved in this section are technical by the nature, but they play a crucial role in our discussion of deeply ramified extensions and the field of norms functor. They can be seen as a first manifestation of a deep relation between characteristic 0 and characteristic p cases. In this section, we assume that L/K is a finite extension of local fields of characteristic 0.

LEMMA 1.1. *One has*

$$\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) = \mathfrak{m}_K^r,$$

where $r = \left[\frac{v_L(\mathfrak{D}_{L/K})+n}{e(L/K)} \right]$.

PROOF. From the definition of the different if follows immediately that $\mathfrak{D}_{L/K}^{-1}$ is the maximal fractional ideal such that

$$\mathrm{Tr}_{L/K}(\mathfrak{D}_{L/K}^{-1}) = O_K.$$

Set $\delta = v_L(\mathfrak{D}_{L/K})$ and $e = e(L/K)$. Then

$$\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n\mathfrak{m}_K^{-r}) = \mathrm{Tr}_{L/K}(\mathfrak{m}_L^n\mathfrak{m}_L^{-er}) \subset \mathrm{Tr}_{L/K}(\mathfrak{m}_L^{n-(\delta+n)}) = \mathrm{Tr}_{L/K}(\mathfrak{D}_{L/K}^{-1}) = O_K,$$

and therefore $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) \subset \mathfrak{m}_K^r$. Conversely, $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n)$ is an ideal of O_K, and we can write in in the form $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) = \mathfrak{m}_K^a$. Then $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n\mathfrak{m}_K^{-a}) = O_K$ and therefore $\mathfrak{m}_L^n\mathfrak{m}_K^{-a} \subset \mathfrak{D}_{L/K}^{-1}$. This implies that

$$n - ae \geqslant -\delta.$$

Therefore $a \leqslant \left[\frac{n+\delta}{e}\right] = r$ and $\mathfrak{m}_K^r \subset \mathrm{Tr}_{L/K}(\mathfrak{m}_L^n)$. The lemma is proved.

□

1.1.1. Assume that L/K is a totally ramified Galois extension of degree p. Set $G = \mathrm{Gal}(L/K)$ and denote by t the maximal natural number such that $G_t = G$ (and therefore $G_{t+1} = \{1\}$). Formula (7) reads:

$$v_L(\mathfrak{D}_{L/K}) = (p-1)(t+1). \tag{16}$$

LEMMA 1.2. *Then for any* $x \in \mathfrak{m}_L^n$

$$N_{L/K}(1+x) \equiv 1 + N_{L/K}(x) + \mathrm{Tr}_{L/K}(x) \pmod{\mathrm{m}_K^s},$$

where $s = \left[\frac{(p-1)(t+1)+2n}{p}\right]$.

Proof. Set $G = \mathrm{Gal}(L/K)$ and for each $1 \leqslant n \leqslant p$ denote by C_n the set of all n-subsets $\{g_1, \dots, g_n\}$ of G (note that $g_i \neq g_j$ if $i \neq j$). Then

$$N_{L/K}(1+x) = \prod_{g \in G}(1+g(x)) = 1 + N_{L/K}(x) + \mathrm{Tr}_{L/K}(x) + \sum_{\{g_1,g_2\} \in C_2} g_1(x)g_2(x) + \dots + \sum_{\{g_1,\dots g_{p-1}\} \in C_{p-1}} g_1(x) \cdots g_{p-1}(x).$$

It's clear that the rule

$$g \star \{g_1, \dots, g_n\} = \{gg_1, \dots, gg_n\}$$

defines an action of G on C_n. Moreover, from the fact that $|G| = p$ is a prime number, it's easy to see that all stabilizers are trivial, and therefore each orbit has p elements. This implies that each sum

$$\sum_{\{g_1,\dots g_n\} \in C_n} g_1(x) \cdots g_n(x), \qquad 2 \leqslant n \leqslant p-1$$

can be written as the trace $\mathrm{Tr}_{L/K}(x_n)$ of some $x_n \in \mathfrak{m}_L^{2n}$. From (16) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n) \in \mathfrak{m}_K^s$. The lemma is proved. □

Lemma 1.3. *For any* $x \in \mathfrak{m}_L^n$

$$N_{L/K}(1+x) \equiv 1 + N_{L/K}(x) + \mathrm{Tr}_{L/K}(x) \pmod{\mathfrak{m}_K^s},$$

where $s = \left[\frac{(p-1)(t+1)+2n}{p}\right]$.

Proof. Set $G = \mathrm{Gal}(L/K)$ and for each $1 \leqslant n \leqslant p$ denote by C_n the set of all n-subsets $\{g_1, \dots, g_n\}$ of G (note that $g_i \neq g_j$ if $i \neq j$). Then

$$N_{L/K}(1+x) = \prod_{g \in G}(1+g(x)) = 1 + N_{L/K}(x) + \mathrm{Tr}_{L/K}(x) + \sum_{\{g_1,g_2\} \in C_2} g_1(x)g_2(x) + \dots + \sum_{\{g_1,\dots g_{p-1}\} \in C_{p-1}} g_1(x) \cdots g_{p-1}(x).$$

It's clear that the rule

$$g \star \{g_1, \dots, g_n\} = \{gg_1, \dots, gg_n\}$$

defines an action of G on C_n. Moreover, from the fact that $|G| = p$ is a prime number, it's easy to see that all stabilizers are trivial, and therefore each orbit has p elements. This implies that each sum

$$\sum_{\{g_1,\dots g_n\} \in C_n} g_1(x) \cdots g_n(x), \qquad 2 \leqslant n \leqslant p-1$$

can be written as the trace $\mathrm{Tr}_{L/K}(x_n)$ of some $x_n \in \mathfrak{m}_L^{2n}$. From (16) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n) \in \mathfrak{m}_K^s$. The lemma is proved. □

Corollary 1.4. *Let* L/K *is a totally ramified Galois extension of degree* p. *Then*

$$v_K(N_{L/K}(1+x) - 1 - N_{L/K}(x)) \geqslant \frac{t(p-1)}{p}.$$

Proof. From Lemmas 1.1 and 1.3 if follows that

$$v_K(N_{L/K}(1+x)-1-N_{L/K}(x)) \geqslant \left[\frac{(p-1)(t+1)}{p}\right],$$

and it's easy to see that

$$\left[\frac{(p-1)(t+1)}{p}\right] = \left[\frac{(p-1)t}{p}+1-\frac{1}{p}\right] \geqslant \frac{t(p-1)}{p}.$$

□

2. Deeply ramified extensions

2.0.1. In this section, we review the theory of deeply ramified extensions of Coates– Greenberg [**6**]. This theory goes back to the fundamental paper of Tate [**30**], where the case of $\mathbf{Z}_p$-extensions was studied and applied to the proof of the Hodge–Tate decomposition for p-divisible groups.

Let K be a local field of characteristic 0. In this section, we consider an infinite algebraic extension K_∞/K. Since for each m the number of algebraic extensions of K of degree m is finite, we can always write K_∞ in the form

$$K_\infty = \overset{\infty}{\underset{n=0}{\cup}} K_n, \qquad K_0 = K, \qquad K_n \subset K_{n+1}, \qquad [K_n : K] < \infty.$$

Following [**15**], we define the different of K_∞/K as the intersection of differents of its finite subextensions.

Definition. *The different of K_∞/K is defined by*

$$\mathfrak{D}_{K_\infty/K} = \overset{\infty}{\underset{n=0}{\cap}} (\mathfrak{D}_{K_n/K} O_{K_\infty}).$$

Let L_∞ be a finite extension of K_∞. Then $L_\infty = K_\infty(\alpha)$, where α is a root of an irreducible polynomial $f(X) \in K_\infty[X]$. The coefficients of $f(X)$ lie in a finite extension K_f of K. Let

$$n_0 = \min\{n \in \mathbf{N} \mid f(X) \in K_n[X]\}.$$

Setting $L_n = K_n(\alpha)$ for all $n \geqslant n_0$, we can write

$$L_\infty = \overset{\infty}{\underset{n=n_0}{\cup}} L_n.$$

In what follows we will assume that $n_0 = 0$ without loss of generality. Note that $[L_n : K_n] = \deg(f)$ doesn't depend on $n \geqslant 0$.

Proposition 2.1. *i) If $m \geqslant n$, then*

$$\mathfrak{D}_{L_n/K_n} O_{L_m} \subset \mathfrak{D}_{L_m/K_m}.$$

ii) One has

$$\mathfrak{D}_{L_\infty/K_\infty} = \overset{\infty}{\underset{n=0}{\cup}} (\mathfrak{D}_{L_n/K_n} O_{L_\infty}).$$

PROOF. i) We consider the trace duality (2):

$$t_{L_n/K_n}\,:\, L_n\times L_n \to K_n, \qquad t_{L_n/K_n}(x,y)=\mathrm{Tr}_{L_n/K_n}(xy).$$

Let $\{e_k\}_{k=1}^s$ be a basis of O_{L_n} over O_{K_n}, and let $\{e_k^*\}_{k=1}^s$ denote the dual basis. Then

$$\mathfrak{D}_{L_n/K_n}=O_{L_n}e_1^*+\cdots+O_{L_n}e_s^*.$$

Since $\{e_k\}_{k=1}^s$ is also a basis of L_m over K_m, any $x\in \mathfrak{D}_{L_m/K_m}^{-1}$ can be written as

$$x=\sum_{k=1}^s a_k e_k^*.$$

Then

$$a_k=t_{L_m/K_m}(x,e_k)\in O_{K_m}, \qquad \forall 1\leqslant k\leqslant s,$$

and we have:

$$x\in O_{K_m}e_1^*+\cdots+O_{K_m}e_s^*\subset \mathfrak{D}_{L_n/K_n}^{-1}O_{L_m}.$$

Therefore $\mathfrak{D}_{L_m/K_m}^{-1}\subset \mathfrak{D}_{L_n/K_n}^{-1}O_{L_m}$, and, by consequence, $\mathfrak{D}_{L_n/K_n}O_{L_m}\subset \mathfrak{D}_{L_m/K_m}$.

ii) With the same argument as in the proof of i), we have

$$\bigcup_{n=0}^{\infty}(\mathfrak{D}_{L_n/K_n}O_{L_\infty})\subset \mathfrak{D}_{L_\infty/K_\infty}.$$

We need to prove that $\mathfrak{D}_{L_\infty/K_\infty}\subset \bigcup_{n=0}^{\infty}(\mathfrak{D}_{L_n/K_n}O_{L_\infty})$ or equivalently that

$$\bigcap_{n=0}^{\infty}(\mathfrak{D}_{L_n/K_n}^{-1}O_{L_\infty})\subset \mathfrak{D}_{L_\infty/K_\infty}^{-1}.$$

Let $x\in \bigcap_{n=0}^{\infty}(\mathfrak{D}_{L_n/K_n}^{-1}O_{L_\infty})$ and $y\in O_{L_\infty}$. Choosing n such that $x\in\mathfrak{D}_{L_n/K_n}^{-1}$ and $y\in O_{L_n}$, we have

$$t_{L_\infty/K_\infty}(x,y)=t_{L_n/K_n}(x,y)\in O_{K_n}\subset O_{K_\infty}.$$

The proposition is proved. □

DEFINITION. *i) For any algebraic extension of local fields M/K (finite or infinite) we set*

$$v_K(\mathfrak{D}_{M/K})=\inf\{v_K(x)\mid x\in\mathfrak{D}_{M/K}\}.$$

ii) We say that M/K has finite conductor if there exists $v\geqslant 0$ such that $M\subset \overline{K}^{(v)}$. If that is the case, we call the conductor of M the number

$$c(M)=\inf\{v\mid M\subset \overline{K}^{(v-1)}\}.$$

THEOREM 2.2 (Coates–Greenberg). *Let K_∞/K be an algebraic extension of local fields. Then the following assertions are equivalent:*

i) $v_K(\mathfrak{D}_{K_\infty/K})=+\infty$;

ii) K_∞/K doesn't have finite conductor;

iii) For any finite extension L_∞/K_∞ one has

$$v_K(\mathfrak{D}_{L_\infty/K_\infty})=0;$$

iv) For any finite extension L_∞/K_∞ one has

$$\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})=\mathfrak{m}_{K_\infty}.$$

Below we prove that

$$i) \Leftrightarrow ii) \Rightarrow iii) \Rightarrow iv).$$

For further detail, see [**6**]. We start with an auxiliary lemma.

LEMMA 2.3. *For any finite extension M/K, one has*

$$\frac{c(M)}{2} \leqslant v_K(\mathfrak{D}_{M/K}) \leqslant c(M).$$

PROOF. We have

$$[M : M \cap \overline{K}^{(v)}] = 1, \quad \text{for any } v > c(M) - 1,$$

$$[M : M \cap \overline{K}^{(v)}] \geqslant 2, \quad \text{if } -1 \leqslant v < c(M) - 1.$$

Therefore

$$v_K(\mathfrak{D}_{M/K}) = \int_{-1}^{\infty} \left(1 - \frac{1}{[M : M \cap \overline{K}^{(v)}]}\right) dv \leqslant \int_{-1}^{c(M)-1} dv = c(M),$$

and

$$v_K(\mathfrak{D}_{M/K}) = \int_{-1}^{\infty} \left(1 - \frac{1}{[M : M \cap \overline{K}^{(v)}]}\right) dv \geqslant \frac{1}{2} \int_{-1}^{c(M)-1} dv = \frac{c(M)}{2}.$$

The lemma is proved. □

2.3.1. We prove that *i*) $\Leftrightarrow$ *ii*). First assume that $v_K(\mathfrak{D}_{K_\infty/K}) = +\infty$. For any $c > 0$, there exists $K \subset M \subset K_\infty$ such that $v_K(\mathfrak{D}_{M/K}) \geqslant c$. By Lemma 2.3, $c(M) \geqslant c$. This shows that K_∞/K doesn't have finite conductor.

Conversely, assume that K_∞/K doesn't have finite conductor. Then for each $c > 0$ there exists a nonzero element $\beta \in K_\infty$ such that $\beta \notin \overline{K}^{(c)}$. Let $M = K(\beta)$. Then $c(M) > c$ and $v_K(\mathfrak{D}_{M/K}) \geqslant \frac{c}{2}$ by Lemma 2.3. Therefore $v_K(\mathfrak{D}_{K_\infty/K}) = +\infty$.

LEMMA 2.4. *Assume that w is such that $L \subset \overline{K}^{(w)}$. Then for any $n \geqslant 0$*

$$[L_n : L_n \cap \overline{K}^{(w)}] = [K_n : K_n \cap \overline{K}^{(w)}].$$

PROOF. Since $\overline{K}^{(w)}/K$ is a Galois extension, K_n and $\overline{K}^{(w)}$ are linearly disjoint over $K_n \cap \overline{K}^{(w)}$. Therefore K_n and $\overline{K}^{(w)} \cap L_n$ are linearly disjoint over $K_n \cap \overline{K}^{(w)}$ (see exercise 7). We have

$$[K_n : K_n \cap \overline{K}^{(w)}] = [K_n \cdot (\overline{K}^{(w)} \cap L_n) : (\overline{K}^{(w)} \cap L_n)]. \tag{17}$$

Clearly $K_n \cdot (\overline{K}^{(w)} \cap L_n) \subset L_n$. On the other hand, since $L_n = K_n \cdot L$ and $L \subset \overline{K}^{(w)}$, we have $L_n \subset K_n \cdot (\overline{K}^{(w)} \cap L_n)$. Thus

$$L_n = K_n \cdot (\overline{K}^{(w)} \cap L_n)$$

Together with (17), this proves the lemma. □

Exercise 7. Show that K_n and $\overline{K}^{(w)} \cap L_n$ are linearly disjoint over $K_n \cap \overline{K}^{(w)}$.

2.4.1. We prove that *ii*) ⇒ *iii*). By the multiplicativity of the different, for any $n \geqslant 0$ we have

$$v_K(\mathfrak{D}_{L_n/K_n}) = v_K(\mathfrak{D}_{L_n/K}) - v_K(\mathfrak{D}_{K_n/K}).$$

Let w be such that $L \subset \overline{K}^{(w)}$. Using formula (9) and Lemma 2.4, we obtain that

$$v_K(\mathfrak{D}_{L_n/K_n}) = \int_{-1}^{\infty} \left(\frac{1}{[K_n : (K_n \cap \overline{K}^{(v)})]} - \frac{1}{[L_n : (L_n \cap \overline{K}^{(v)})]} \right) dv =$$
$$\int_{-1}^{w} \left(\frac{1}{[K_n : (K_i \cap \overline{K}^{(v)})]} - \frac{1}{[L_n : (L_n \cap \overline{K}^{(v)})]} \right) dv \leqslant \int_{-1}^{w} \frac{dv}{[K_n : (K_n \cap \overline{K}^{(v)})]}.$$

Since $[K_n : (K_i \cap \overline{K}^{(v)})] \geqslant [K_n : (K_n \cap \overline{K}^{(w)})]$ for any $v \leqslant w$, this gives the following estimate for the different:

$$v_K(\mathfrak{D}_{L_n/K_n}) \leqslant \frac{w+1}{[K_n : (K_n \cap \overline{K}^{(w)})]}.$$

Since K_∞/K doesn't have finite conductor, for any $c > 0$ there exists $n \geqslant 0$ such that $[K_n : (K_n \cap \overline{K}^{(w)})] > c$, and therefore $v_K(\mathfrak{D}_{L_n/K_n}) \leqslant (w+1)/c$ (see exercise 8 below). This proves that $v_K(\mathfrak{D}_{L_\infty/K_\infty}) = 0$.

Exercise 8. Assume that K_∞/K doesn't have a finite conductor. Show that for any fixed $w \geqslant -1$

$$[K_n : K_n \cap \overline{K}^{(w)}] \to +\infty \qquad \text{when } n \to +\infty.$$

Hint: proof by contradiction. Show that if $[K_n : K_n \cap \overline{K}^{(w)}]$ is bounded, then $K_n \subset F \cdot \overline{K}^{(w)}$ for some finite extension F/K. Show that in that case K_∞ has a finite conductor.

2.4.2. We prove that *iii*) ⇒ *iv*). We consider two cases.

a) First assume that the set $\{e(K_n/K) \mid n \geqslant 0\}$ is bounded. Then there exists n_0 such that $e(K_n/K_{n_0}) = 1$ for any $n \geqslant n_0$. Therefore $e(L_n/L_{n_0}) = 1$ for any $n \geqslant n_0$ and by the mutiplicativity of the different

$$\mathfrak{D}_{L_n/K_n} = \mathfrak{D}_{L_{n_0}/K_{n_0}} O_{L_n}, \qquad \forall n \geqslant n_0.$$

From Proposition 2.1 and assumption iii) it follows that $\mathfrak{D}_{L_n/K_n} = O_{L_n}$ for all $n \geqslant n_0$. Therefore L_n/K_n are unramified and Lemma 1.1 (or just the well known surjectivity of the trace map in unramified extensions) gives:

$$\mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n}) = \mathfrak{m}_{K_n}, \qquad \text{for all } n \geqslant n_0.$$

Thus $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty}) = \mathfrak{m}_{K_\infty}$.

b) Now assume that the set $\{e(K_n/K) \mid n \geqslant 0\}$ is unbounded. Let $x \in \mathfrak{m}_{K_\infty}$. Then there exists n such that $x \in \mathfrak{m}_{K_n}$. By Lemma 1.1,

$$\mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n}) = \mathfrak{m}_{K_n}^{r_n}, \qquad r_n = \left[\frac{v_{L_n}(\mathfrak{D}_{L_n/K_n}) + 1}{e(L_n/K_n)} \right].$$

From our assumptions and Proposition 2.1 it follows that we can choose n such that in addition

$$v_K(\mathfrak{D}_{L_n/K_n}) + \frac{1}{e(L_n/K)} \leqslant v_K(x).$$

Then

$$r_n \leqslant \frac{v_{L_n}(\mathfrak{D}_{L_n/K_n})+1}{e(L_n/K_n)} = \left(v_K(\mathfrak{D}_{L_n/K_n}) + \frac{1}{e(L_n/K)}\right) e(K_n/K) \leqslant v_{K_n}(x).$$

Since $\mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n})$ is an ideal in O_{K_n}, this implies that $x \in \mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n})$, and the inclusion $\mathfrak{m}_{K_\infty} \subset \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$ is proved. Since the converse inclusion is trivial, we have $\mathfrak{m}_{K_\infty} = \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$.

Exercise 9. i) Show that $G_K^{(0)} = I_K$ and that the wild ramification subgroup $\mathrm{Gal}(\overline{K}/K^{\mathrm{tr}})$ can be written as

$$\mathrm{Gal}(\overline{K}/K_{\mathrm{tr}}) = \overline{\underset{\varepsilon>0}{\cup} G_K^{(\varepsilon)}}$$

(topological closure of $\underset{\varepsilon>0}{\cup} G_K^{(\varepsilon)}$).

ii) Show that K^{tr}/K has finite conductor and determine it.

3. Almost étale extensions

3.1. Almost etale extensions.

3.1.1. We introduce, in our very particular setting, the notion of almost etale extension.

Definition. *A finite extension L/K of non archimedean fields is almost etale if and only if*

$$\mathrm{Tr}_{L/K}(\mathfrak{m}_L) = \mathfrak{m}_K.$$

It's clear that an unramified extension of local fields is almost etale. Below we give two other archetypical examples of almost etale extensions.

1) Assume that K is a perfect non archimedean field of characteristic p. Then any finite extension of K is almost etale.

Proof. Let L/K be a finite extension. It's clear that $\mathrm{Tr}_{L/K}(\mathfrak{m}_L) \subset \mathfrak{m}_K$. Moreover, $\mathrm{Tr}_{L/K}(\mathfrak{m}_L)$ is an ideal of O_K and for any $\alpha \in \mathfrak{m}_L$

$$\lim_{n\to+\infty} |\mathrm{Tr}_{L/K}\varphi^{-n}(\alpha)|_K = 0.$$

This implies that $\mathfrak{m}_K \subset \mathrm{Tr}_{L/K}(\mathfrak{m}_L)$, and the proposition is proved. □

2) Assume that K_∞ is a deeply ramified extension of a local field K of characteristic 0. Then any finite extension of K_∞ is almost etale. This was proved in Theorem 2.2.

3.1.2. Let K be a perfect complete non archimedean field. We denote by $\mathbf{C}_K$ the completion of $\overline{K}$.

Proposition 3.2. *The field $\mathbf{C}_K$ is algebraically closed.*

Proof. Proof by contradiction. Assume that there exists $\alpha \notin \mathbf{C}_K$ which is algebraic over $\mathbf{C}_K$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ denote the conjugates of α and let $d_\alpha = \min\limits_{2\leqslant i\leqslant n} |\alpha_i - \alpha|_K$. Take $\beta \in \overline{K}$ such that $|\beta - \alpha| < d_\alpha$. Then $\alpha \in \mathbf{C}_K(\beta) = \mathbf{C}_K$ by Krasner's lemma. □

Theorem 3.3. *Assume that F is an algebraic extension of K such that any finite extension of F is almost etale. Then*

$$\mathbf{C}_K^{G_F} = \widehat{F}.$$

We first prove the following lemma.

Lemma 3.4. *Let L/F be an almost etale Galois extension with Galois group G. Then for any $\alpha \in L$ and any $c > 1$ there exists $\beta \in F$ such that*

$$\left|\alpha - \beta\right|_F < c \cdot \max_{g\in G}\left|g(\alpha) - \alpha\right|_F.$$

Proof. Let $c > 1$. By Theorem 2.2 iv), there exists $x \in O_E$ such that $y = \mathrm{Tr}_{L/F}(x)$ satisfies

$$1/c < |y|_F \leqslant 1.$$

Set $\beta = \dfrac{1}{y}\sum\limits_{g\in G} g(\alpha x)$. Then

$$|\alpha-\beta|_F = \left|\frac{\alpha}{y}\sum_{g\in G} g(x) - \frac{1}{y}\sum_{g\in G} g(\alpha x)\right|_F = \left|\frac{1}{y}\sum_{g\in G} g(x)(\alpha - g(\alpha))\right|_F$$
$$\leqslant \frac{1}{|y|_F}\cdot \max_{g\in G}\left|g(\alpha)-\alpha\right|_F.$$

The lemma is proved. □

3.4.1. *Proof of Theorem 3.3.* Let $\alpha \in \mathbf{C}_K^{G_F}$. Choose a sequence $(\alpha_n)_{n\in\mathbf{N}}$ of elements $\alpha_n \in \overline{K}$ such that $|\alpha_n - \alpha|_K < p^{-n}$. Then

$$|g(\alpha_n) - \alpha_n|_K = |g(\alpha_n - \alpha) - (\alpha_n - \alpha)|_K < p^{-n}, \qquad \forall g \in G_F.$$

By Lemma 3.4, for each n there exists $\beta_n \in F$ such that $|\beta_n - \alpha_n|_K < p^{-n}$. Then

$$\alpha = \lim_{n\to+\infty} \beta_n \in \widehat{F}.$$

The theorem is proved.

□

4. The normalized trace

4.1. In this section, K_∞/K is a totally ramified $\mathbf{Z}_p$-extension. Fix a topological generator γ of Γ. For any $x \in K_n$ set

$$\mathrm{T}_{K_\infty/K}(x) = \frac{1}{p^n}\mathrm{Tr}_{K_n/K}(x).$$

It's clear that this definition doesn't depend on the choice of n. Therefore we have a well defined homomorphism

$$\mathrm{T}_{K_\infty/K} \,:\, K_\infty \to K.$$

Note that $\mathrm{T}_{K_\infty/K}(x) = x$ for $x \in K$. Our first goal is to prove that $\mathrm{T}_{K_\infty/K}$ is continuous.

Proposition 4.2 (Tate). *i) There exists a constant $c > 0$ such that*

$$|\mathrm{T}_{K_\infty/K}(x) - x|_K \leqslant c|\gamma(x) - x|_K, \qquad \forall x \in K_\infty.$$

ii) The map $\mathrm{T}_{K_\infty/K}$ is continuous and extends by continuity to $\widehat{K}_\infty$.

Proof. a) By Proposition 6.9, $v_K(\mathfrak{D}_{K_n/K_{n-1}}) = e_K + \alpha_n p^{-n}$, where α_n is bounded. Applying Lemma 1.1 to the extension K_n/K_{n-1}, we obtain that

$$|\mathrm{Tr}_{K_n/K_{n-1}}(x)|_K \leqslant |p|_K^{1-b/p^n}|x|_K, \qquad \forall x \in K_n \tag{18}$$

with some constant $b > 0$ which doesn't depend on n.

b) Set $\gamma_n = \gamma^{p^n}$. For any $x \in K_n$ we have

$$\mathrm{Tr}_{K_n/K_{n-1}}(x) = \sum_{k=0}^{p-1}\gamma_{n-1}^k(x).$$

Therefore

$$\mathrm{Tr}_{K_n/K_{n-1}}(x) - px = \sum_{k=0}^{p-1}(\gamma_{n-1}^k(x) - x) = \sum_{k=1}^{p-1}(1 + \gamma_{n-1} + \cdots \gamma_{n-1}^{k-1})(\gamma_{n-1}(x) - x).$$

and we obtain that

$$\left|\frac{1}{p}\mathrm{Tr}_{K_n/K_{n-1}}(x) - x\right|_K \leqslant |p|^{-1}\cdot|\gamma_{n-1}(x) - x|_K, \qquad \forall x \in K_n.$$

Since $\gamma_{n-1}(x) - x = (1 + \gamma + \cdots + \gamma^{p^{n-1}-1})(\gamma(x) - x)$, we also have

$$\left|\frac{1}{p}\mathrm{Tr}_{K_n/K_{n-1}}(x) - x\right|_K \leqslant |p|^{-1}\cdot|\gamma(x) - x|_K, \qquad \forall x \in K_n. \tag{19}$$

c) We prove by induction on n that

$$\left|\mathrm{T}_{K_\infty/K}(x) - x\right|_K \leqslant c_n\cdot|\gamma(x) - x|_K, \qquad \forall x \in K_n, \tag{20}$$

where $c_1 = |p|_K$ and $c_n = c_{n-1}\cdot|p|_K^{-b/p^n}$. For $n = 1$, this follows from (19). For $n \geqslant 2$ and $x \in K_n$, we write

$$\mathrm{T}_{K_\infty/K}(x) - x = \left(\frac{1}{p}\mathrm{Tr}_{K_n/K_{n-1}}(x) - x\right) + (\mathrm{T}_{K_\infty/K}(y) - y), \qquad y = \frac{1}{p}\mathrm{Tr}_{K_n/K_{n-1}}(x).$$

The first term can be bounded by (19). For the second term, we have

$$|\mathrm{T}_{K_\infty/K}(y)-y|_K \leqslant c_{n-1}|\gamma(y)-y|_K = c_{n-1}|p|_K^{-1}|\mathrm{Tr}_{K_n/K_{n-1}}(\gamma(x)-x)|_K \leqslant c_{n-1}|p|_K^{-b/p^n}|\gamma(x)-x|_K.$$

(Here the last inequality follows from (18)). This proves (20).

d) Set $c = c_1\prod_{n=1}^{\infty}|p|_K^{-b/p^n} = c_1|p|_K^{-b/(p-1)}$. Then $c_n < c$ for all $n \geqslant 1$, and from (20) we obtain that

$$\left|\mathrm{T}_{K_\infty/K}(x)-x\right|_K \leqslant c\cdot|\gamma(x)-x|_K, \qquad \forall x\in K_\infty,$$

This proves the first assertion of the proposition. The second assertion is immediate. □

Definition. *The map* $\mathrm{T}_{K_\infty/K}:\widehat{K}_\infty\to K$ *is called the normalized trace.*

4.2.1. Since $\mathrm{T}_{K_\infty/K}$ is an idempotent map, we have a decomposition

$$\widehat{K}_\infty = K\oplus\widehat{K}_\infty^\circ,$$

where $K_\infty^\circ = \ker(\mathrm{T}_{K_\infty/K})$.

Theorem 4.3. *i) The map* $\lambda-1$ *is bijective, with a continuous image, on* $\widehat{K}_\infty^\circ$.

ii) For any $\lambda\in U_K^{(1)}$ *which is not a root of unity, the map* $\gamma-\lambda$ *is bijective, with a continuous image, on* $\widehat{K}_\infty$.

Proof. a) Write $K_n = K\oplus K_n^\circ$, where $K_n^\circ = \ker(\mathrm{T}_{K_\infty/K})\cap K_n$. Since $\gamma-1$ is injective on K_n°, and K_n° has finite dimension over K, $\gamma-1$ is bijective on K_n° and on $K_\infty^\circ = \bigcup_{n\geqslant 0}K_n^\circ$. Let $\rho: K_\infty^\circ\to K_\infty^\circ$ denote its inverse. From Proposition 4.2 we have that

$$|x|_K \leqslant c|(\gamma-1)(x)|_K, \qquad \forall x\in K_\infty^\circ,$$

and therefore

$$|\rho(x)|_K\leqslant c|x|_K, \qquad \forall x\in K_\infty^\circ.$$

Thus ρ is continuous and extends to $\widehat{K}_\infty^\circ$. This proves the theorem for $\lambda=1$.

b) Assume that $\lambda\in U_K^{(1)}$ satisfies

$$|\lambda-1|_K < c^{-1}.$$

Then $\rho(\gamma-\lambda) = 1+(1-\lambda)\rho$ and the series

$$\theta = \sum_{i=0}^{\infty}(\lambda-1)^i\rho^i$$

converges to an operator θ such that $\rho\theta(\gamma-\lambda)=1$. Thus $\gamma-\lambda$ is invertible on $\widehat{K}_\infty^\circ$. Since $\lambda\neq 1$, it is also invertible on K and therefore invertible on $\widehat{K}_\infty$.

c) In the general case, we choose n such that $|\lambda^{p^n}-1|_K < c^{-1}$. Since $\lambda^{p^n}\neq 1$, then by part b), $\gamma^{p^n}-\lambda^{p^n}$ is invertible on $\widehat{K}_\infty$. Since

$$\gamma^{p^n}-\lambda^{p^n} = (\gamma-\lambda)\sum_{i=0}^{p^n-1}\gamma^{p^n-i-1}\lambda^i,$$

$\gamma - \lambda$ is invertible too. The theorem is proved. □

4.4. Let $\eta : \Gamma \to U_K^{(1)}$ be a continuous character. We denote by $\widehat{K}_\infty(\eta)$ the K-vector space $\widehat{K}_\infty$ equipped with the η-twisted action of Γ, namely

$$g \star x = \eta(\gamma) \cdot \gamma(x), \qquad \forall \gamma \in \Gamma, \quad x \in \widehat{K}_\infty(\eta).$$

We will also consider η as the character

$$G_K \to \Gamma \to U_K^{(1)}$$

and denote by $\mathbf{C}_K(\eta)$ the field $\mathbf{C}_K$ equipped with the η-twisted action of G_K.

Theorem 4.5 (Tate). *Let K_∞/K be a totally ramified Γ-extension. Then the following holds true:*

i) $\widehat{K}_\infty^\Gamma = K$ and $\mathbf{C}_K^{G_K} = K$.

ii) If $\eta : \Gamma \to U_K^{(1)}$ is a character with infinite image $\eta(\Gamma)$, then $\widehat{K}_\infty(\eta)^\Gamma = 0$ and $\mathbf{C}_K(\eta)^{G_K} = 0$.

Proof. We combine Theorems 3.3 and 4.3. Let γ be a topological generator of Γ. Since $\tau = \gamma - 1$ is bijective on $\widehat{K}_\infty^\circ$, we have $(\widehat{K}_\infty^\circ)^\Gamma = 0$ and

$$\widehat{K}_\infty^\Gamma = K^\Gamma \oplus (\widehat{K}_\infty^\circ)^\Gamma = K.$$

Moreover,

$$\mathbf{C}_K^{G_K} = \left(\mathbf{C}_K^{G_{K_\infty}}\right)^\Gamma = \widehat{K}_\infty^\Gamma = K.$$

If η is a nontrivial character, set $\lambda = \eta(\gamma)$. Then

$$\widehat{K}_\infty(\eta)^\Gamma = \{x \in \widehat{K}_\infty \mid \gamma(x) = \lambda^{-1} x\}$$

Again by Theorem 4.3, $\widehat{K}_\infty^\circ(\eta)^\Gamma = 0$. Since $\lambda \neq 1$, we also have $K(\eta)^\Gamma = 0$. Thus $\widehat{K}_\infty(\eta)^\Gamma = 0$. Finally

$$\mathbf{C}_K(\eta)^{G_K} = \left(\mathbf{C}_K(\eta)^{G_{K_\infty}}\right)^\Gamma = \left(\mathbf{C}_K^{G_{K_\infty}}(\eta)\right)^\Gamma = \widehat{K}_\infty(\eta)^\Gamma = 0.$$

□

CHAPTER 3

From characteristic 0 to characteristic p and vice versa I: perfectoid fields

1. Perfectoid fields

1.0.1. The notion of perfectoid field was introduced in Scholze's fundamental paper [**25**] as a far-reaching generalization of Fontaine's constructions [**10**], [**12**]. Fix a prime number p. Let E be a field equipped with a non-archimedean absolute value $|\cdot|_E : E \to \mathbf{R}_+$ such that $|p|_E < 1$. Note that we don't exclude the case of characteristic p, where the last condition holds automatically. We denote by O_E the ring of integers of E and by $\mathfrak{m}_E$ the maximal ideal of O_E.

Definition. *Let E be a field equipped with an absolute value $|\cdot|_E : E \to \mathbf{R}_+$ such that $|p|_E < 1$. One says that E is perfectoid if the following holds true:*
i) $|\cdot|_E$ is nondiscrete;
ii) E is complete for $|\cdot|_E$;
iii) The Frobenius map

$$\varphi : O_E/pO_E \to O_E/pO_E, \qquad \varphi(x) = x^p$$

is surjective.

We give first examples of perfectoid fields, which can be treated directly.

1) Let K be a non archimedean field. The completion $\mathbf{C}_K$ of its algebraic closure is a perfectoid field.
2) Let K be a local field. Fix a uniformizer π_K of K and set $\pi_n = \pi_K^{1/p^n}$. Then the completion of the Kummer extension $K(\pi_K^{1/p^\infty}) = \overset{\infty}{\underset{n=1}{\cup}} K(\pi_n)$ is a perfectoid field. This follows from the congruence
$$\left(\sum_{i=0}^m [a_i]\pi_n^m\right)^p \equiv \sum_{i=0}^m [a_i]^p \pi_{n-1}^m \pmod{p}.$$

The following important result is a particilar case of [**14**, Proposition 6.6.6].

Theorem 1.1 (Gabber–Ramero). *Let K be a local field of characteristic 0. A complete subfield $K \subset E \subset \mathbf{C}_K$ is a perfectoid field if and only if it is the completion of a deeply ramified extension of K.*

2. Tilting

2.0.1. In this section, we describe the tilting construction, which functorially associates to any perfectoid field of characteristic 0 a perfect field of characteristic

p. This construction first appeared in the pionnering papers of Fontaine [**9, 10**]. The tilting of so-called arithmetically profinite (APF) extensions is closely related to the field of norms functor of Fontaine–Wintenberger and will be studied in the next chapter. In the full generality, the tilting was defined in the famous paper of Scholze [**25**] for perfectoid algebras. This generalization is crucial for geometric application. However, in this introductory course, we will consider only the arithmetic case.

2.0.2. Let E be a perfectoid field. Consider the projective limit

$$O_{E^\flat} := \varprojlim_{\varphi} O_E/pO_E = \varprojlim (O_E/pO_E \xleftarrow{\varphi} O_E/pO_E \xleftarrow{\varphi} \cdots), \tag{21}$$

where $\varphi(x) = x^p$ is the absolute frobenius. It's clear that $O_{E^\flat}$ is equipped with a natural ring structure. An element x of $O_{E^\flat}$ is an infinite sequence $x = (x_n)_{n\in\mathbf{N}}$ of elements $x_n \in O_E/pO_E$ such that $x_{n+1}^p = x_n$. Below we summarize first properties of the ring $O_{E^\flat}$:

1) If we choose, for all $m \in \mathbf{N}$, a lift $\widehat{x}_m \in O_E$ of x_m, then for any fixed n the sequence $(\widehat{x}_{n+m}^{p^m})_{m\in\mathbb{N}}$ converges to an element

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

which does not depends on the choice of the lifts $\widehat{x}_m$. In addition, $\left(x^{(n)}\right)^p = x^{(n-1)}$ fol all $n \geqslant 1$.

Proof. Since $x_{m+n}^p = x_{m+n-1}$, we have $\widehat{x}_{m+n}^p \equiv \widehat{x}_{m+n-1} \pmod p$, and an easy induction shows that $\widehat{x}_{m+n}^{p^m} \equiv \widehat{x}_{m+n-1}^{p^{m-1}} \pmod{p^m}$. Therefore the sequence $(\widehat{x}_{n+m}^{p^m})_{m\in\mathbb{N}}$ converges. Assume that $\widetilde{x}_m \in O_E$ are another lifts of x_m, $m \in \mathbf{N}$. Then $\widetilde{x}_m \equiv \widehat{x}_m \pmod p$ and therefore $\widetilde{x}_{n+m}^{p^m} \equiv \widehat{x}_{n+m}^{p^m} \pmod{p^{m+1}}$. This implies that the limit doesn't depend on the choice of the lifts. □

2) For all $x, y \in O_{E^\flat}$ one has

$$(x+y)^{(n)} = \lim_{m\to+\infty} \left(x^{(n+m)} + y^{(n+m)}\right)^{p^m}, \qquad (xy)^{(n)} = x^{(n)}y^{(n)}. \tag{22}$$

Proof. It's easy to see that $x^{(n)} \in O_E$ is a lift of x_n. Therefore $x^{(n+m)} + y^{(n+m)}$ is a lift of $x_{n+m} + y_{n+m}$, and the first formula follows from the definition of $(x+y)^{(n)}$. The same argument proves the second formula. □

3) The map $x \mapsto (x^{(n)})_{n\geqslant 0}$ defines an isomorphism

$$O_{E^\flat} \simeq \varprojlim_{x^p \leftarrow x} O_E, \tag{23}$$

where the right hand side is equipped with the addition and multiplication defined by (22).

Proof. This follows from from 2). □

Define

$$
\begin{aligned}
&|\cdot|_{E^\flat}\,:\,O_{E^\flat}\to \mathbf{R}\cup\{+\infty\},\\
&|x|_{E^\flat}=|x^{(0)}|_E.
\end{aligned}
$$

PROPOSITION 2.1. *i) $|\cdot|_{E^\flat}$ is a non archimedean absolute value on $O_{E^\flat}$.*

ii) $O_{E^\flat}$ is a perfect complete valuation ring of characteristic p with maximal ideal $\mathfrak{m}_{E^\flat}=\{x\in O_{E^\flat}\mid v_{E^\flat}(x)>0\}$ and residue field k_E. It is integrally closed in its field of fractions.

iii) Let $E^\flat$ denote the field of fractions of $O_{E^\flat}$. Then $|E^\flat|_{E^\flat}=|E|_E$.

PROOF. i) Let $x,y\in O_{E^\flat}$. It's clear that

$$
|xy|_{E^\flat}=|(xy)^{(0)}|_E=|x^{(0)}y^{(0)}|_E=|x^{(0)}|\cdot|y^{(0)}|_E=|x|_{E^\flat}|y|_{E^\flat}.
$$

Also,

$$
\begin{aligned}
|x+y|_{E^\flat}&=|(x+y)^{(0)}|_E=|\lim_{m\to+\infty}(x^{(m)}+y^{(m)})^{p^m}|_E=\lim_{m\to+\infty}|x^{(m)}+y^{(m)}|_E^{p^m}\\
&\leqslant \lim_{m\to+\infty}\max\{|x^{(m)}|_E,|x^{(m)}|_E\}^{p^m}=\lim_{m\to+\infty}\max\{\left|(x^{(m)})^{p^m}\right|_E,\left|(x^{(m)})^{p^m}\right|_E\}\\
&\qquad\qquad=\max\{\left|(x^{(0)})\right|_E,\left|(x^{(0)})\right|_E\}=\max\{|x|_{E^\flat},|y|_{E^\flat}\}.
\end{aligned}
$$

This proves that $|\cdot|_{E^\flat}$ is an non archimedean absolute value.

ii) We prove the completeness of $O_{E^\flat}$ (other properties follow easily from i) and properties 1-3) above.

First remark that if $y=(y_0,y_1,\dots)\in O_{E^\flat}$, then

$$
y_n=0\quad\Leftrightarrow\quad |y|_{E^\flat}\leqslant |p|_E^{p^n}. \tag{24}
$$

Let $(x_n)_{n\in\mathbf{N}}$ be a Cauchy sequence in $O_{E^\flat}$. Then for any $M>0$ there exist N such that for all $n,m\geqslant N$

$$
|x_n-x_m|_{E^\flat}\leqslant |p|_E^{p^M}.
$$

Writing $x_n=(x_{n,0},x_{n,1},\dots), x_m=(x_{m,0},x_{m,1},\dots)$ and using (24), we obtain that for all $n,m\geqslant N$

$$
x_{n,i}=x_{m,i}\quad\text{for all}\quad 0\leqslant i\leqslant M.
$$

This shows that for each $i\geqslant 0$ the sequence $(x_{n,i})_{n\in\mathbf{N}}$ is stationary. Set $a_i=\lim_{n\to+\infty}x_{n,i}$. Then $a=(a_0,a_1,\dots)\in O_{E^\flat}$, and it's easy to check that $\lim_{n\to+\infty}x_n=a$. □

Exercise 10. Complete the proof of Proposition 2.1.

DEFINITION. *The field $E^\flat$ will be called the tilt of E.*

PROPOSITION 2.2. *A perfectoid field E is algebraically closed if and only if $E^\flat$ is.*

PROOF. The proposition can be proved by successive approximation. See [**7**, Proposition 2.1.11] for the proof that $E^\flat$ is algebraically closed and [**7**, Proposition 2.2.19, Corollary 3.1.10] for two different proofs of the converse statement. Scholze's original proof can be found in [**25**, Proposition 3.8]. See also Kedlaya's proof in [**3**].

□

3. Witt vectors

3.1. In this section, we review the theory of Witt vectors. Consider the sequence of polynomials $w_0(x_0), w_1(x_0,x_1),\dots$ defined by

$$
\begin{aligned}
&w_0(x_0) = x_0,\\
&w_1(x_0,x_1) = x_0^p + px_1,\\
&w_2(x_0,x_1,x_2) = x_0^{p^2} + px_1^p + p^2x_2,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&w_n(x_0,x_1,\dots x_n) = x_0^{p^n} + px_1^{p^{n-1}} + p^2x_2^{p^{n-2}} + \dots + p^nx_n,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned}
$$

PROPOSITION 3.2. *Let $F(x,y) \in \mathbf{Z}[x,y]$ be a polynomial with coefficients in $\mathbf{Z}$ such that $F(0,0) = 0$. Then there exists a unique sequence of polynomials*

$$
\begin{aligned}
&\Phi_0(x_0,y_0) \in \mathbf{Z}[x_0,y_0],\\
&\Phi_1(x_0,y_0,x_1,y_1) \in \mathbf{Z}[x_0,y_0,x_1,y_1],\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&\Phi_n(x_0,y_0,x_1,y_1,\dots,x_n,y_n) \in \mathbf{Z}[x_0,y_0,x_1,y_1,\dots,x_n,y_n],\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned}
$$

such that

(25)
$$w_n(\Phi_0,\Phi_1,\dots,\Phi_n) = F(w_n(x_0,x_1,\dots,x_n), w_n(y_0,y_1,\dots,y_n)), \qquad \text{for all } n \geqslant 0.$$

To prove this proposition, we need the following elementary lemma.

LEMMA 3.3. *Let $f \in \mathbf{Z}[x_0,\dots,x_n]$. Then*

$$f^{p^m}(x_0,\dots,x_n) \equiv f^{p^{m-1}}(x_0^p,\dots,x_n^p) \pmod{p^m}, \qquad \text{for all } m \geqslant 1.$$

PROOF. The proof is left to the reader. ☐

PROOF OF PROPOSITION 3.2. The proposition could be easily proved by induction on n. For $n = 0$ we have $\Phi_0(x_0,y_0) = F(x_0,y_0)$. Assume that $\Phi_0,\Phi_1,\dots,\Phi_{n-1}$ are constructed. From (25) it follows that

$$\Phi_n = \frac{1}{p^n}\Big(F(w_n(x_0,x_1,\dots,x_n), w_n(y_0,y_1,\dots,y_n)) - (\Phi_0^{p^n} + \dots + p^{n-1}\Phi_{n-1}^p)\Big). \tag{26}$$

This proves the uniqueness. It remains to prove that Φ_n has coefficients in $\mathbf{Z}$. Since

$$w_n(x_0,\dots,x_{n-1},x_n) \equiv w_{n-1}(x_0^p,\dots,x_{n-1}^p) \pmod{p^n},$$

we have:

$$
\begin{aligned}
&F(w_n(x_0,\dots,x_{n-1},x_n), w_n(y_0,\dots,y_{n-1},y_n))\\
&\qquad\qquad \equiv F(w_{n-1}(x_0^p,\dots,x_{n-1}^p), w_{n-1}(y_0^p,\dots,y_{n-1}^p)) \pmod{p^n}.
\end{aligned} \tag{27}
$$

On the other hand, applying Lemma 3.3 and the induction hypothesis we have

$$
\begin{aligned}
(28)\quad \Phi_0^{p^n}+\cdots+p^{n-1}\Phi_{n-1}^p &\equiv w_{n-1}\left(\Phi_0(x_0^p,y_0^p),\dots,\Phi_{n-1}(x_0^p,y_0^p,\dots,x_{n-1}^p,y_{n-1}^p)\right)\\
&\equiv F(w_{n-1}(x_0^p,\dots,x_{n-1}^p),w_{n-1}(y_0^p,\dots,y_{n-1}^p)) \pmod{p^n}.
\end{aligned}
$$

From (27) and (28) we obtain that

$$
F(w_n(x_0,\dots,x_{n-1},x_n),w_n(y_0,\dots,y_{n-1},y_n))\equiv \Phi_0^{p^n}+\cdots+p^{n-1}\Phi_{n-1}^p \pmod{p^n}.
$$

Together with (26), this shows that Φ_n has coeffiients in $\mathbf{Z}$. The proposition is proved. □

3.3.1. Let $(f_n)_{n\geqslant 0}$ denote the polynomials $(\Phi_n)_{n\geqslant 0}$ for $F(x,y)=x+y$ and $(g_n)_{n\geqslant 0}$ denote the polynomials $(\Phi_n)_{n\geqslant 0}$ for $F(x,y)=xy$. In particular,

$$
\begin{aligned}
&f_0(x_0,y_0)=x_0+y_0, \quad f_1(x_0,y_0,x_1,y_1)=x_1+y_1+\frac{x_0^p+y_0^p-(x_0+y_0)^p}{p},\\
&g_0(x_0,y_0)=x_0y_0, \qquad g_1(x_0,y_0,x_1,y_1)=x_0^py_1+x_1y_0^p+px_1y_1.
\end{aligned}
$$

3.4. For any commutative unitary ring A, we denote by $W(A)$ the set of infinite vectors $a=(a_0,a_1,\dots)\in A^{\mathbf{N}}$ equipped with the addition and multiplication defined by the formulas:

$$
\begin{aligned}
a+b&=(f_0(a_0,b_0),f_1(a_0,b_0,a_1,b_1),\dots),\\
a\cdot b&=(g_0(a_0,b_0),g_1(a_0,b_0,a_1,b_1),\dots).
\end{aligned}
$$

Theorem 3.5 (Witt). *With addition and multiplication defined as above, $W(A)$ is a commutative unitary ring with*

$$
1=(1,0,0,\dots).
$$

Proof. a) We show the associativity of addition. From construction it's clear that there exist polynomials with integer coefficients $(u_n)_{n\geqslant 0}$, and $(v_n)_{n\geqslant 0}$ such that $u_n,v_n\in\mathbf{Z}[x_0,y_0,z_0,\dots,x_n,y_n,z_n]$ and for any $a,b,c\in W(A)$

$$
\begin{aligned}
(a+b)+c&=(u_0(a_0,b_0,c_0),\dots,u_n(a_0,b_0,c_0,\dots,a_n,b_n,c_n),\dots),\\
a+(b+c)&=(v_0(a_0,b_0,c_0),\dots,v_n(a_0,b_0,c_0,\dots,a_n,b_n,c_n),\dots).
\end{aligned}
$$

Moreover

$$
\begin{aligned}
w_n(u_0,\dots,u_n)&=w_n(f_0(x_0,y_0),f_1(x_0,y_0,x_1,y_1),\dots)+w_n(z_0,\dots,z_n)\\
&=w_n(x_0,\dots,x_n)+w_n(y_0,\dots,y_n)+w_n(z_0,\dots,z_n)
\end{aligned}
$$

and

$$
\begin{aligned}
w_n(v_0,\dots,v_n)&=w_n(x_0,\dots,x_n)+w_n(f_0(y_0,z_0),f_1(y_0,z_0,y_1,z_1),\dots)\\
&=w_n(x_0,\dots,x_n)+w_n(y_0,\dots,y_n)+w_n(z_0,\dots,z_n).
\end{aligned}
$$

Therefore

$$
w_n(u_0,\dots,u_n)=w_n(v_0,\dots,v_n), \qquad \text{for all } n\geqslant 0,
$$

and an easy induction shows that $u_n=v_n$ for all n. This shows the associativity of addition.

b) We will show the formula

$$(x_0,x_1,x_2,\dots)\cdot(y_0,0,0,\dots)=(x_0y_0,x_1y_0^p,x_1y_0^{p^2},\dots) \tag{29}$$

In particular, it implies that $1=(1,0,0,\dots)$ is the unity of $W(A)$. We have

$$(x_0,x_1,x_2,\dots)\cdot(y_0,0,0,\dots)=(h_0,h_1,\dots),$$

where $h_0,h_1,\dots$ are some polynomials in $y_0,x_0,x_1\cdots$. We prove by induction that $h_n=x_ny_0^n$. For $n=0$ we have $h_0=g_0(x_0,y_0)=x_0y_0$. Assume that the formula is proved for all $i\leqslant n-1$. We have

$$w_n(h_0,h_1,\dots,h_n)=w_n(x_0,x_1,\dots,x_n)w_n(y_0,0,\dots,0x).$$

Thus

$$h_0^{p^n}+ph_1^{p^{n-1}}+\cdots+p^{n-1}h_1+p^nh_n=(x_0^{p^n}+px_1^{p^{n-1}}+\cdots+p^{n-1}x_1+p^nx_n)y_0^{p^n}.$$

By induction hypothesis, $h_i=x_iy_0^{p^i}$ for $0\leqslant i\leqslant n-1$. Then $h_n=x_ny_0^{p^n}$, and the statement is proved.

Other properties can be proved by the same method. □

3.6. We assemble below some properties of the ring $W(A)$:

1) Any morphism of rings $\psi: A\to B$ induces

$$W(A)\to W(B),\qquad \psi(a_0,a_1,\dots)=(\psi(a_0),\psi(a_1),\dots).$$

2) If p is invertible in A, then there exists an isomorphism of rings $W(A)\simeq A^{\mathbf{N}}$.

Proof. The map

$$w: W(A)\to A^{\mathbf{N}},\qquad w(a_0,a_1,\dots)=(w_0(a_0),w_1(a_0,a_1),w_2(a_0,a_1,a_2),\cdots)$$

is an homomorphism by the definition of the addition and multiplication in $W(A)$. If p is invertible, then for any $(b_0,b_1,b_2,\dots)$ the system of equations

$$w_0(x_0)=b_0,\quad w_1(x_0,x_1)=b_1,\quad w_2(x_0,x_1,x_2)=b_2,\dots$$

has a unique solution in A. Therefore w is an isomorphism. □

3) For any $a\in A$, define its Teichmüller lift $[a]\in W(A)$ by

$$[a]=(a,0,0,\dots).$$

Then $[ab]=[a][b]$ for all $a,b\in A$.

Proof. This follows from (29). □

4) The shift map (Verschiebung)

$$V: W(A)\to W(A),\qquad (a_0,a_1,0,\dots)\mapsto(0,a_0,a_1,\dots),$$

is additive, i.e. $V(a+b)=V(a)+V(b)$.

Proof. Can be proved by the same method. □

5) For any $n \geqslant 0$ define
$$I_n(A) = \{(a_0, a_1, \dots) \in W(A) \mid a_i = 0 \text{ for all } 0 \leqslant i \leqslant n\}.$$
It's easy to see that $(I_n(A))_{n\geqslant 0}$ is a descending chain of ideals which defines a separable filtration on $W(A)$. Set
$$W_n(A) := W(A)/I_n(A).$$
Then
$$W(A) = \varprojlim W(A)/I_n(A).$$
We equip $W(A)/I_n(A)$ with the discrete topology and define the standard topology on $W(A)$ as the topology of the projective limit. It is clearly Hausdorff. This topology coincides with the topology of the direct product on $W(A)$:
$$W(A) = A \times A \times A \times \cdots,$$
where each copy of A is equipped with the discrete topology. The ideals $I_n(A)$ form a neighborhood base at 0 (each open neighborhood of 0 contains $I_n(A)$ for some n).

6) For any $a = (a_0, a_1, \dots) \in W(A)$, one has
$$(a_0, a_1, a_2, \dots) = \sum_{n=0}^{\infty} V^n[a_n].$$

Proof. Can be proved by the standard method. □

Assume that A is a ring of characteristic p. Then A is equipped with the absolute Frobenius endomorphism
$$\varphi : A \to A, \qquad \varphi(x) = x^p.$$
In the remainder of this paper, will will only consider the Witt vectors with coefficients in semiperfect rings.

Definition. *Let A be a ring of charactersitic p. We say that A is perfect if φ is an isomorphism.*

7) If A is a ring of characteristic p, then the map (which we denote again by φ)
$$\varphi : W(A) \to W(A), \qquad (a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots),$$
is a ring endomomorphism. In addition
$$\varphi V = V\varphi = p.$$

Proof. We should show that
$$p(a_0, a_1, \dots) = (0, a_0^p, a_1^p, \dots).$$
By definition of Witt vectors, the multiplication by p is given by
$$p(a_0, a_1, \dots) = (\bar{h}_0(a_0), \bar{h}_1(a_0, a_1), \dots),$$

where $\overline{h}_n(x_0,x_1,\dots,x_n)$ is the reduction $\mod p$ of the polynomials defined by

$$w_n(h_0,h_1,\dots,h_n)=pw_n(x_0,x_1,\dots,x_n), \qquad n\geqslant 0.$$

An easy induction shows that $h_n\equiv x_{n-1}^p \pmod p$, and 4) is proved. □

Proposition 3.7. *Assume that A is an integral perfect ring of characteristic p. The following holds true:*

i) $p^{n+1}W(A)=I_n(A)$.

ii) The standard topology on $W(A)$ coincides with the p-adic topology.

iii) Each $a=(a_0,a_1,\dots)\in W(A)$ can be written as

$$(a_0,a_1,a_2,\dots)=\sum_{n=0}^{\infty}[a_n^{p^{-n}}]p^n.$$

Proof. i) Since φ is bijective on A (and therefore on $W(A)$), we can write

$$p^{n+1}W(A)=V^{n+1}\varphi^{-(n+1)}W(A)=V^{n+1}W(A)=I_n(A).$$

□

ii) Follows directly from i).

iii) One has

$$(a_0,a_1,a_2,\dots)=\sum_{n=0}^{\infty}V^n([a_n])=\sum_{n=0}^{\infty}p^n\varphi^{-n}([a_n])=\sum_{n=0}^{\infty}[a_n^{p^{-n}}]p^n.$$

Theorem 3.8. *i) Let A be an integral perfect ring of characteristic p. Then there exists a unique, up to an isomorphism, ring R such that*

a) R is integral of characteristic 0;

b) $R/pR\simeq A$;

c) R is complete for the p-adic topology, namely

$$R\simeq \varprojlim_n R/p^nR.$$

ii) The ring $W(A)$ satisfies properties a-c).

Proof. i) See [**28**, Chapitre II, Théorème 3].

ii) This follows from Proposition 3.7. □

3.9. Examples. 1) $W(\mathbf{F}_p)\simeq \mathbf{Z}_p$.

2) Let $\overline{\mathbf{F}}_p$ be the algebraic closure of $\mathbf{F}_p$. Then $W(\mathbf{F}_p)$ is isomorphic to the ring of integers of $\widehat{\mathbf{Q}}_p^{\mathrm{ur}}$.

4. The tilting equivalence

4.1. The ring $\mathbf{A}_{\mathrm{inf}}(E)$. Let E be a perfectoid field.

Definition. *The ring*

$$\mathbf{A}_{\mathrm{inf}}(E):=W(O_E^{\flat}).$$

is called the infinitesimal thickening of $O_{E^\flat}$.

Each element of $\mathbf{A}_{\mathrm{inf}}(E)$ is an infinite vector

$$a = (a_0, a_1, a_2, \dots), \qquad a_n \in O_E^\flat,$$

which also can be written in the form

$$a = \sum_{n=0}^{\infty} [a_n^{p^{-n}}] p^n.$$

Proposition 4.2 (Fontaine, Fargues–Fontaine). *i) The map*

$$\theta_E : \mathbf{A}_{\mathrm{inf}}(E) \to O_E$$

given by

$$\theta_E \left(\sum_{n=0}^{\infty} [a_n] p^n \right) = \sum_{n=0}^{\infty} a_n^{(0)} p^n$$

is a surjective ring homomorphism.

ii) $\ker(\theta_E)$ *is a principal ideal. An element* $\sum\limits_{n=0}^{\infty} [a_n] p^n \in \ker(\theta_E)$ *is a generator of* $\ker(\theta_E)$ *if and only if* $v_{E^\flat}(a_0) = v_E(p)$.

Proof. i) For any ring A set $W_n(A) = W(A)/I_n(A)$. Directly from the definition of Witt vectors it follows that for any $n \geqslant 0$ the map

$$w_n : W_n(O_E) \to O_E,$$
$$w_n(a_0, a_1, \dots, a_n) = a_0^{p^n} + p a_1^{p^{n-1}} + \dots + p^n a_n$$

is a ring homomorphism. Consider the map

$$\eta_n : W_n(O_E/pO_E) \to O_E/p^{n+1}O_E,$$
$$\eta_n(a_0, a_1, \dots, a_n) = \widehat{a}_0^{p^n} + p \widehat{a}_1^{p^{n-1}} + \dots + p^n \widehat{a}_n,$$

where $\widehat{a}_i$ denotes any lift of a_i in O_E. It's easy to see that the definition of η_n doesn't depend on the choice of these lifts. Moreover, the diagram

$$\begin{array}{ccc} W_n(O_E) & \xrightarrow{w_n} & O_E \\ \downarrow & & \downarrow \\ W_n(O_E/pO_E) & \xrightarrow{\eta_n} & O_E/p^{n+1}O_E \end{array}$$

commutes by the functoriality of the Witt vectors functor. This shows, that η_n is a ring homomorphism. Let $\theta_{E,n} : W_{n+1}(O_E^\flat) \to O_E/p^{n+1}O_E$ denote the reduction of θ_E modulo p^{n+1}.

Claim. *From the definitions of our maps, it follows that* $\theta_{E,n}$ *coincides with the composition*

$$W_n(O_E^\flat) \xrightarrow{\varphi^{-n}} W_n(O_E^\flat) \xrightarrow{\mathrm{pr}} W_n(O_E/pO_E) \xrightarrow{\eta_n} O_E/p^{n+1}O_E,$$

where the map pr *is induced by the projection*

$$O_E^\flat \to O_E/pO_E, \qquad (y_0, y_1, \dots) \mapsto y_0.$$

The proof is left as an exercise (see below).

The claim shows that $\theta_{E,n}$ is a ring homomorphism for all $n \geqslant 0$. Therefore θ_E is a ring homomorphism.

ii-iii) We omit the proof. See [**10**, Proposition 2.4] and [**7**, Proposition 3.1.9].

The surjectivity of θ_E follows from the surjectivity of the map

$$\theta_{E,0} : O_E^\flat \to O_E/pO_E.$$

$\square$

Exercise 11. 1) Let $y = (y_0, y_1, \dots) \in O_{E^\flat}$. Show that

$$(\varphi(y))^{(m)} = y^{(m-1)}, \qquad \forall m \geqslant 1.$$

2) Show that

$$(\varphi^{-n}(y))^{(0)} = y^{(n)}, \qquad \forall n \geqslant 0.$$

3) Let $a = (a_0, a_1, \dots) \in \mathbf{A}_{\mathrm{inf}}(E)$, $a_i \in O_{E^\flat}$. Show that the map $\eta_n \circ \mathrm{pr} \circ \varphi^{-n}$ sends a to

$$a_0^{(0)} + pa_1^{(1)} + \cdots + p^n a_n^{(n)}.$$

4) Deduce the claim from 3).

We continue to assume that E is a perfectoid field. Fix an algebraic closure $\overline{E}$ of E and denote by $\mathbf{C}_E$ its completion. By Proposition 2.2, $\mathbf{C}_E^\flat$ is algebraically closed and we denote by $\overline{E^\flat}$ the separable closure of $E^\flat$ in $\mathbf{C}_E^\flat$. Let $\widehat{\overline{E^\flat}}$ denote the p-adic completion of $\overline{E^\flat}$.

4.3. The untilt. We have the following picture

$$\begin{tikzcd}
\mathbf{C}_E \arrow[r, squiggly, "\flat"] \arrow[d, dash] & \mathbf{C}_E^\flat \arrow[d, dash] \\
E \arrow[r, squiggly, "\flat"] & E^\flat
\end{tikzcd}$$

Let $\mathfrak{F}$ be a complete intermediate field $E^\flat \subset \mathfrak{F} \subset \mathbf{C}_E^\flat$. Fix a generator ξ of $\ker(\theta_E)$. Consider the diagram, where $O_{\mathfrak{F}^\sharp} := \theta_{\mathbf{C}_E}(W(O_{\mathfrak{F}}))$:

$$\begin{tikzcd}
0 \arrow[r] & \xi\mathbf{A}_{\mathrm{inf}}(E) \arrow[r] \arrow[d, hook] & \mathbf{A}_{\mathrm{inf}}(E) \arrow[r, "\theta_E"] \arrow[d, hook] & O_E \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \xi W(O_{\mathfrak{F}}) \arrow[r] \arrow[d, hook] & W(O_{\mathfrak{F}}) \arrow[r] \arrow[d, hook] & O_{\mathfrak{F}^\sharp} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \xi\mathbf{A}_{\mathrm{inf}}(\mathbf{C}_E) \arrow[r] & \mathbf{A}_{\mathrm{inf}}(\mathbf{C}_E) \arrow[r, "\theta_{\mathbf{C}_E}"] & O_{\mathbf{C}_E} \arrow[r] & 0
\end{tikzcd}$$

We remark that

$$O_{\mathfrak{F}^\sharp} = W(O_{\mathfrak{F}})/\xi W(O_{\mathfrak{F}}).$$

Set $\mathfrak{F}^\sharp = O_{\mathfrak{F}^\sharp}[1/p]$ (field of fractions of $O_{\mathfrak{F}^\sharp}$).

Claim. $\mathfrak{F}^\sharp$ is a perfectoid field and $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$.

PROOF OF THE CLAIM. We admit that $\mathfrak{F}^\sharp$ is complete with ring of integers $O_{\mathfrak{F}^\sharp}$. If $\xi = \sum\limits_{n\geqslant 0} [a_n]p^n$, then from Proposition 4.2 ii) we have $a_0 \in \mathfrak{m}_{E^\flat}$. Thus

$$\xi \mod p = a_0 \in \mathfrak{m}_{E^\flat}.$$

Then

$$O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp} \simeq O_{\mathfrak{F}}/a_0O_{\mathfrak{F}}.$$

The exercise below shows that $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$. □

Exercise 12. Let $\mathfrak{F}$ be a perfect complete non-archimedean field of characteristic p. Let $\alpha \in \mathfrak{m}_{\mathfrak{F}}$. Then

$$\varprojlim_{\varphi} O_{\mathfrak{F}}/\alpha O_{\mathfrak{F}} \simeq O_{\mathfrak{F}}.$$

The isomorphism is given by the maps

$$\varprojlim_{\varphi} O_{\mathfrak{F}}/\alpha O_{\mathfrak{F}} \to O_{\mathfrak{F}}, \qquad (x_n)_{n\geqslant 0} \mapsto \lim_{n\to+\infty} \widehat{x}_n^{\,p^n},$$

$$O_{\mathfrak{F}} \to \varprojlim_{\varphi} O_{\mathfrak{F}}/\alpha O_{\mathfrak{F}}, \qquad x \mapsto (\varphi^{-n}(x) \mod \alpha O_{\mathfrak{F}})_{n\geqslant 0},$$

This exercise shows that

$$\varprojlim_{\varphi} O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp} = \varprojlim_{\varphi} O_{\mathfrak{F}}/a_0O_{\mathfrak{F}} \simeq O_{\mathfrak{F}},$$

i.e. that $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$.

PROPOSITION 4.4. *One has* $\mathbf{C}_E^\flat = \mathbf{C}_{E^\flat}$, *where* $\mathbf{C}_{E^\flat}$ *is the completion of* $\overline{E^\flat}$.

PROOF. Since $E^\flat \subset \mathbf{C}_E^\flat$ and $\mathbf{C}_E^\flat$ is complete and algebraically closed, we have $\mathbf{C}_{E^\flat} \subset \mathbf{C}_E^\flat$. Set $\mathfrak{F} := \mathbf{C}_{E^\flat}$. By the claim, $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$. Since $\mathfrak{F}$ is complete and algebraically closed, $\mathfrak{F}^\sharp$ is complete and algebraically closed by Proposition 2.2. Since $\mathfrak{F}^\sharp \subset \mathbf{C}_E$, we have $\mathfrak{F}^\sharp \subset \mathbf{C}_E$. Therefore

$$\mathfrak{F} = (\mathfrak{F}^\sharp)^\flat = \mathbf{C}_E^\flat.$$

The proposition is proved. □

Now we can prove the main results of this section.

THEOREM 4.5 (Scholze, Fargues–Fontaine). *Let E be a perfectoid field of characteristic* 0. *Then the following holds true:*

i) Each finite extension of E is a perfectoid field.

ii) The tilt functor $F \mapsto F^\flat$ induces an equivalence between the categories of finite extensions of E and $E^\flat$ respectively.

iii) The functor

$$\mathfrak{F} \mapsto \mathfrak{F}^\sharp, \qquad \mathfrak{F}^\sharp := (W(O_{\mathfrak{F}})/\xi W(O_{\mathfrak{F}}))[1/p]$$

is a quasi inverse to the tilt functor.

Proof. The proof below due to Fargues and Fontaine [**7**, Theorem 3.2.1].

a) The Galois group $G_E = \mathrm{Gal}(\overline{E}/E)$ acts on $\mathbf{C}_E$ and $\mathbf{C}_E^\flat$. Let $\mathbf{E} = \widehat{\overline{E^\flat}}$. By Proposition 4.4, $\mathbf{C}_E^\flat = \mathbf{E}$, and we have a map

$$G_E \to \mathrm{Aut}(\mathbf{C}_E^\flat/E^\flat) \xrightarrow{\sim} \mathrm{Aut}(\widehat{\overline{E^\flat}}/E^\flat) \xrightarrow{\sim} \mathrm{Aut}(\overline{E^\flat}/E^\flat) = G_{E^\flat}. \tag{30}$$

Conversely, again by Proposition 4.4, we have an isomorphism

$$W(O_{\mathbf{E}})/\xi W(O_{\mathbf{E}}) \simeq O_{\mathbf{C}_E}, \tag{31}$$

which induces a map

$$G_{E^\flat} \xrightarrow{\sim} \mathrm{Aut}(\mathbf{E}/E^\flat) \to \mathrm{Aut}(\mathbf{C}_E/E) \xrightarrow{\sim} G_E.$$

It's easy to see that the maps (30) and (31) are inverse to each other. Therefore

$$G_E \simeq G_{E^\flat},$$

and by Galois theory we have a one-to-one correspondence

$$\{\text{finite extensions of } E\} \leftrightarrow \{\text{finite extensions of } E^\flat\} \tag{32}$$

b) Let $\mathfrak{F}/E^\flat$ be a finite extension. Then

$$\mathfrak{F}^\sharp = (W(O_{\mathfrak{F}})/\xi W(O_{\mathfrak{F}}))[1/p)] \subset \mathbf{C}_E^{G_{\mathfrak{F}}}.$$

The following is admitted

$$\mathfrak{F}^\sharp = \mathbf{C}_E^{G_{\mathfrak{F}}}.$$

This shows that the Gaois correspondence

$$\{\text{finite extensions of } E^\flat\} \to \{\text{finite extensions of } E\} \tag{33}$$

is given by the untilting $\mathfrak{F} \mapsto \mathfrak{F}^\sharp$. Moreover, by the claim $\mathfrak{F}^\sharp$ is perfectoid and $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$.

c) Conversely, let F be a finite extension of E. Set $\mathfrak{F} = (\overline{E^\flat})^{G_F}$. Then tautologically $G_{\mathfrak{F}} = G_F$ and $F = \mathbf{C}_E^{G_{\mathfrak{F}}}$. From part b),

$$\mathbf{C}_E^{G_{\mathfrak{F}}} = \mathfrak{F}^\sharp,$$

and $\mathfrak{F}^\sharp$ is a perfectoid field. Therefore $F = \mathfrak{F}^\sharp$ is a perfectoid field. Moreover

$$F^\flat = \left(\mathfrak{F}^\sharp\right)^\flat = \mathfrak{F},$$

and

$$(F^\flat)^\sharp = \mathfrak{F}^\sharp = F.$$

This concludes the proof. $\square$

CHAPTER 4

From characteristic 0 to characteristic p and vice versa II: the field of norms

1. Arithmetically profinite extensions

1.1. In this chapter, we introduce the theory of the arithmetically profinite (APF) extensions and the field of norms construction of Fontaine–Wintenberger [**31**].

Definition. *An algebraic extension L/K is called arithmetically profinite (APF) if and only if*

$$(G_K : G_K^{(v)} G_L) < +\infty \qquad \forall v \geqslant -1.$$

If L/K is a Galois extension with $G = \mathrm{Gal}(L/K)$, then it is APF if and only if

$$(G : G^{(v)}) < +\infty \qquad \forall v \geqslant -1.$$

It is clear that any finite extension is APF. Below we give some basic properties and examples of APF extensions.

1) An infinite APF extension is deeply ramified.

Proof. We have $\overline{K}^{G_L G_K^{(v)}} = L^{G_K^{(v)}} = L \cap \overline{K}^{(v)}$. Therefore for each v

$$[L \cap \overline{K}^{(v)} : K] = (G_K : G_L G_K^{(v)}) < +\infty.$$

This shows that L doesn't have finite conductor. □

The converse of this statement is clearly wrong ($\overline{K}/K$ is deeply ramified but not APF). However Fesenko [**8**] proved that every deeply ramified extension L/K of finite residue degree and with discrete set of ramification jumps is APF.

2) Let $\mathcal{G} = \mathrm{GL}_N(\mathbf{Z}_p)$. This group is equipped with the natural descending filtration $\mathcal{G}[n] = \{A \in \mathrm{GL}_N(\mathbf{Z}_p) \mid A \equiv 1 \pmod{p^n}\}$. Let L/K be a totally ramified Galois extension of local fields of characteristic 0 with the Galois group G. Assume that there exists a continuous embedding of G in $\mathcal{G}$. Let $G[n]$ denote the filtration on G induced by this embedding, namely

$$G[n] = G \cap \mathcal{G}[n].$$

Then a theorem of Sen [**26**] says that there exists a constant c such that

$$G^{(ne+c)} \subset G[n] \subset G^{(ne-c)}, \qquad \forall n \in \mathbf{N}.$$

Here $e = e(K/\mathbf{Q}_p)$ denotes the ramification index. From this theorem it follows that

$$(G : G^{(ne-c)}) \leqslant (G : G[n]) \leqslant (\mathcal{G} : \mathcal{G}[n]) < +\infty.$$

Therefore L/K is APF.

3) Any totally ramified $\mathbf{Z}_p$-extension is APF. This remark applies to the p-cyclotomic extension $K(\zeta_{p^\infty})$. This follows from 2), but also from Proposition 6.9.

1.2. We analyze the ramification jumps of APF extensions. First we extend the definition of the ramification jumps to general (non necessarily Galois) extensions. Let K be a local field of characteristic 0.

Definition. *Let L/K be an algebraic extension. A real number $v \geqslant -1$ is a ramification jump of L/K if and only if*

$$G_K^{(v+\varepsilon)} G_L \neq G_K^{(v)} G_L \qquad \forall \varepsilon > 0.$$

Proposition 1.3. *Let L/K be an infinite APF extension and let B denote the set of ramification jumps of K. Then B is a countably infinite unbounded set.*

Proof. a) Let L/K be an APF extension. First we prove that B is discrete. Let $v_2 \geqslant v_1 \geqslant -1$ be two ramification jumps. Then

$$(G_K : G_K^{(v_1)} G_L) \leqslant (G_K : G_K^{(v_2)} G_L) < +\infty,$$

and

$$(G_K^{(v_1)} G_L : G_K^{(v_2)} G_L) < +\infty.$$

Therefore there exists only finitely many subgroups H such that

$$G_K^{(v_2)} G_L \subset H \subset G_K^{(v_1)} G_L.$$

This implies that there are only finitely many ramification jumps in the interval (v_1, v_2).

b) We prove that B is unbounded by contradiction. Assume that B is bounded above by a. Then $G_L G_K^{(a)} = \bigcap\limits_{t \geqslant 0} G_L G_K^{(a+t)}$. Let $g \in G_L G_K^{(a)}$. Then for any $n \geqslant 0$ we can write $g = x_n y_n$ with $x_n \in G_L$ and $y_n \in G_K^{(a+n)}$. Since G_L is compact, we can assume that $(x_n)_{n \geqslant 0}$ converges. In this case $(y_n)_{n \geqslant 0}$ converges to some $y \in \bigcap\limits_{n \geqslant 0} G_K^{(a+n)}$. From $\bigcap\limits_{n \geqslant 0} G_K^{(a+n)} = \{1\}$, we obtain that $g \in G_L$. Therefore $G_L G_K^{(a)} = G_L$, and

$$(G_K : G_L G_K^{(a)}) = (G_K : G_L) + \infty,$$

which is in contradiction with the definition of APF extensions. □

Let L/K be an infinite APF extension. We denote by $B^+ = (b_i)_{n \geqslant 1}$ the set of its strictly *positive* ramification jumps. For all $i \geqslant 1$ define

$$K_i = \overline{K}^{G_L G_K^{(b_i)}}.$$

PROPOSITION 1.4. *i)* $L = \bigcup_{i=1}^{\infty} K_i$;
ii) K_1 *is the maximal tamely ramified subextension of* L/K;
iii) For all $i \geqslant 1$, K_{i+1}/K_i *is a nontrivial finite* p*-extension.*
iv) Assume that L/K *is a Galois extension. Then for all* $i \geqslant 1$ *the group* $\mathrm{Gal}(K_{i+1}/K_i)$ *has a unique ramification jump. In particular,* $\mathrm{Gal}(K_{i+1}/K_i)$ *is a* p*-elementary abelian group.*

PROOF. ii) The maximal tamely ramified subextension of L/K is

$$L_{\mathrm{tr}} = \overline{K}^{G_L P_K},$$

where P_K is the wild ramification subgroup. From definitions, it is easy to see that P_K is the topological closure of $\bigcup_{v>0} G_K^{(v)}$ in G_K. This implies that $G_L P_K = G_L G_K^{(b_1)}$, and ii) is proved.

The assertions i), iii) and iv) are clear. □

1.5. We record some general properties of APF extension.

PROPOSITION 1.6. *Let* $K \subset F \subset L$ *be a tower of extensions.*
i) If F/K *is APF and* L/F *is finite, then* L/K *is APF.*
ii) If F/K *is finite and* L/F *is APF, then* L/K *is APF.*
iii) If L/K *is APF, then* F/K *is APF.*

PROOF. See [**31**, Proposition 1.2.3]. □

The definition of Hasse–Herbrand functions can be extended to APF extensions. Namely, for an APF extension L/K define

$$\psi_{L/K}(v) = \begin{cases} v, & \text{if } v \in [-1, 0], \\ \displaystyle\int_0^v (G_K^{(0)} : G_L^{(0)} G_K^{(t)}) dt, & \text{if } v \geqslant 0. \end{cases}$$
$$\varphi_{L/K}(u) = \psi_{L/K}^{-1}(u).$$

It is not difficult to check that if $K \subset F \subset L$ with $[F : K] < +\infty$, then

$$\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}, \qquad \varphi_{L/K} = \varphi_{F/K} \circ \varphi_{L/F}.$$

2. The field of norms

2.1. In this Section, we review the construction of the field of norms of an APF extension. Let $K_1 = L \cap K^{\mathrm{tr}}$ denote the maximal tamely ramified subextension of L/K. Note that by Proposition 1.4 K_1/K is finite. Denote by $\mathcal{E}(L/K)$ the directed set of finite extensions E/K such that of $K_1 \subset E \subset L$.

THEOREM 2.2 (Fontaine–Wintenberger). *Let* L/F *be an infinite APF extension. Set*

$$\mathcal{X}(L/K) = \varprojlim_{E \in \mathcal{E}(L/K)} E^* \cup \{0\}.$$

Then the following holds true.

i) Let $\alpha = (\alpha_E)_E$ and $\beta = (\beta_E)_E$. Then $\alpha\beta$ and $\alpha + \beta$ defined by the formulas

$$(\alpha\beta)_E := \alpha_E \beta_E,$$
$$(\alpha+\beta)_E := \lim_{E' \in \mathcal{E}(L/E)} N_{E'/E}(\alpha_{E'} + \beta_{E'})$$

are well defined elements of $\mathcal{X}(L/K)$.

ii) The above defined addition and multiplication equip $\mathcal{X}(L/K)$ with a structure of a local field of characteristic p with residue field k_L.

iii) The valuation on $\mathcal{X}(L/K)$ is given by

$$v(\alpha) = v_E(\alpha_E),$$

for any E.

iv) For any $\xi \in k_L$, let $[\xi]$ denote its Teichmüller lift. For any $K_1 \subset E \subset L$ set

$$\xi_E := [\xi]^{1/[E:K_1]}.$$

Then the map

$$k_L \to \mathcal{X}(L/K), \qquad \xi \mapsto (\xi_E)_E$$

is a canonical embedding.

Definition. *The field $\mathcal{X}(L/K)$ is called the field of norms of the APF extension L/K.*

2.3. Functorial properties.

2.3.1. In this section L/K denotes an infinite APF extension. Any finite extension M of L can be written as $M = L(\alpha)$, where α is a root of an irreducible polynomial $f(X) \in L[X]$. The coefficients of $f(X)$ lie in some finite subextension $F \in \mathcal{E}(L/K)$. For any $E \in \mathcal{E}(L/F)$,

$$F(\alpha) \cap E = F,$$

and we set $E' = E(\alpha)$. The system $(E')_{E \in \mathcal{E}(L/K)}$ is cofinal in $\mathcal{E}(M/K)$. Consider the map

$$j_{M/L} : \mathcal{X}(L/K) \to \mathcal{X}(M/K)$$

which sends any $\alpha = (\alpha_E)_E \in \mathcal{X}(L/K)$ to the element $\beta \in \mathcal{X}(M/K)$ defined by

$$\beta_{E'} = \alpha_E \text{ if } E' = E(\alpha) \text{ with } E \in \mathcal{E}(L/F).$$

The previous remarks show that $j_{M/L}$ is a well defined embedding.

Theorem 2.4 (Fontaine–Wintenberger). *i) Let M/L be a finite extension. Then $\mathcal{X}(M/K)/\mathcal{X}(L/K)$ is a separable extension of degree $[M : L]$. If M/L is a Galois extension, then the natural action of* $\mathrm{Gal}(M/L)$ *on $\mathcal{X}(M/L)$ induces an isomorphism*

$$\mathrm{Gal}(M/L) \simeq \mathrm{Gal}\left(\mathcal{X}(M/K)/\mathcal{X}(L/K)\right).$$

ii) The above construction establishes a one-to-one correspondence

$$\{\textit{finite extensions of } L\} \leftrightarrow \{\textit{finite separable extensions of } \mathcal{X}(L/K)\},$$

which is compatible with the Galois correspondence.

PROOF. We only explain how to associate to any finite separable extension $\mathcal{M}$ of $X(L/K)$ a canonical finite extension M of L of the same degree. Let $\mathcal{M} = X(L/K)(\alpha)$, where α is a root of some irreducible polynomial $f(X)$ with coefficients in the ring of integers of $X(L/K)$. We can write $f(X)$ as a sequence $f(X) = (f_E(X))_{E\in\mathcal{E}(L/K)}$ where $f_E(X) \in E[X]$. Then $M = L(\widehat{\alpha})$, where $\widehat{\alpha}$ is a root of $f_E(X)$, and E is of "sufficiently big" degree over K. See [**31**, Théorème 3..2] for a detailed proof. □

2.4.1. From this theorem it follows that the separable closure $\overline{X(L/K)}$ of $X(L/K)$ can de written as

$$\overline{X(L/K)} = \bigcup_{[M:L]<\infty} X(M/K).$$

COROLLARY 2.5. *The field of norms functor induces a canonical isomorphism of absolute Galois groups:*

$$G_{X(L/K)} \simeq G_L.$$

.

2.6. Comparision with the tilting equivalence.

2.6.1. Recall that an infinite APF extension if deeply ramified, and therefore its completion $\widehat{L}$ is a perfectoid field. We finish this section with comparing the field of norms with the tilting construction. A general result was proved by Fontaine and Wintenberger for APF extensions satisfying some additional condition.

DEFINITION. *A strictly APF extension is an APF extension satisfying the following property:*

$$\liminf_{v\to+\infty} \frac{\psi_{L/K}(v)}{(G_K^{(0)} : G_L^{(0)} G_K^{(v)})} > 0.$$

From Sen's theorem (see Section 1.1) it follows that if $\mathrm{Gal}(L/K)$ is a p-adic Lie group, then L/K is strictly APF.

2.6.2. Let L/K be an infinite strict APF extension. Recall that K_1 denotes the maximal tamely ramified subextension of E/K. Fot any $E \in \mathcal{E}(L/K)$ set $d(E) = [E : K_1]$. For any $n \geqslant 1$ let $\mathcal{E}_n$ denote the subset of extensions $E \in \mathcal{E}(L/K)$ such that p^n divides the degree $d(E)$. Let $\alpha = (\alpha_E)_E \in X(L/K)$. It can be proved (see [**31**, Proposition 4.2.1]) that for any $n \geqslant 1$ the family

$$\alpha_E^{d(E)p^{-n}}, \qquad E \in \mathcal{E}_n$$

converges to an element $x_n \in \widehat{L}$. Once the convergence is proved, it's clear that $x_n^p = x_{n-1}^p$ for all n, and therefore $x = (x_n)_{n\geqslant 1} \in \widehat{L}^\flat$. This defines an embedding

$$X(L/K) \hookrightarrow \widehat{L}^\flat.$$

THEOREM 2.7 (Fontaine–Wintenberger). *Let L/K be an infinite strict APF extension. Then*

$$X(\widehat{L/K})^{\mathrm{rad}} = \widehat{L}^\flat.$$

Here $X(\widehat{L/K})^{\mathrm{rad}}$ denotes the completion of the maximal purely inseparable extension of $X(L/K)$.

PROOF. See [**31**, Théorème 4.3.2 & Corollaire 4.3.4]. □

REMARK 2.8. *In* [**8**], *Fesenko gives an example of a deeply ramified extension which doesn't contain infinite APF extensions. In some sense, this shows that the theory of perfectoid fields doesn't reduce to the theory of APF extensions.*

3. The case of cyclotomic extensions

3.0.1. In this section, we consider cyclotomic extensions of local fields. Let F be an unramified extension of $\mathbf{Q}_p$. Set $F_n = F(\zeta_{p^n})$ and $F_\infty = \bigcup_{n\geqslant 1} F_n$. Let $\Gamma_F = \mathrm{Gal}(F_\infty/F)$. Then we have a canonical isomorphism

$$\chi_F\,:\,\Gamma_F \to \mathbf{Z}_p^*, \qquad \gamma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_F(\gamma)}, \qquad \gamma\in\Gamma_F.$$

The extension F_∞/F is totally ramified and F_∞/F_1 is a $\mathbf{Z}_p$-extension. Therefore F_∞/F is APF. Set $\pi_n = \zeta_{p^n}-1$. Then π_n is a uniformizer of F_n. From $(1+\pi_{n+1})^p = 1+\pi_n$ we have

$$f(\pi_{n+1}) = 0, \qquad X^p + pX^{p-1}+\cdots+pX-\pi_n. \tag{34}$$

Therefore (for $p\neq 2$)

$$N_{F_{n+1}/F_n}(\pi_{n+1}) = \pi_n \equiv \pi_{n+1}^p \pmod{p}. \tag{35}$$

For $p=2$, $N_{F_{n+1}/F_n}(\pi_{n+1}) = -\pi_n\equiv \pi_n \pmod{2}$ and the congruence holds again. From (34) and Proposition 3.2 we have for the different of F_{n+1}/F_n:

$$\mathscr{D}_{F_{n+1}/F_n} = pO_{F_{n+1}}.$$

Therefore

$$v_{F_{n+1}}(\mathscr{D}_{F_{n+1}/F_n}) = [F_{n+1}:F] = (p-1)(t+1), \qquad t:=p^n-1.$$

Applying Corollary 1.4, we obtain that for all $\alpha,\beta\in O_{F_{n+1}}$

$$v_{F_n}(N_{F_{n+1}/F_n}(\alpha+\beta)-N_{F_{n+1}/F_n}(\alpha)-N_{F_{n+1}/F_n}(\beta)) \geqslant \frac{(p-1)(p^n-1)}{p}.$$

Equivalently

$$\begin{aligned} v_F(N_{F_{n+1}/F_n}(\alpha+\beta)-N_{F_{n+1}/F_n}(\alpha)-N_{F_{n+1}/F_n}(\beta))& \\ \geqslant \frac{(p-1)(p^n-1)}{p(p-1)p^{n-1}} = 1-\frac{1}{p^n}\geqslant \frac{p-1}{p}&, \end{aligned} \tag{36}$$

for all $n\geqslant 1$. Set $\mathbf{C}_p := \mathbf{C}_{\mathbf{Q}_p}$.

Exercise 13. Let $a\in\mathfrak{m}_{\mathbf{C}_p^\flat}$ be such that $v(a)\leqslant v(p)$ (one can take $v:=v_F$, then the condition reads $v_F(p)\leqslant 1$). Show that

$$O_{\mathbf{C}_p^\flat} \simeq \varprojlim_{\varphi} O_{\mathbf{C}_p}/aO_{\mathbf{C}_p}.$$

Each element $x\in O_{F_{n+1}}$ can be written in the form

$$x=\sum_k [\xi_k]\pi_{n+1}^k,$$

where $[\xi_k]$ are Teichmüller lifts of $\xi_k \in k_F$. From (35) and (36) we have

$$v_F(N_{F_{n+1}/F_n}(x) - x^p) \geqslant \frac{p-1}{p}, \qquad \forall n \geqslant 1.$$

Choose $a \in F_1$ such that $0 < v_F(a) \leqslant \frac{p-1}{p}$ (if $p \neq 2$, one can take $a = \pi_1$). Therefore we have a commutative diagram, where N denotes the norm map:

$$\begin{tikzcd}
O_{F_1} \arrow[d] & O_{F_2} \arrow[l, "N"'] \arrow[d] & O_{F_3} \arrow[l, "N"'] \arrow[d] & \cdots \arrow[l] \\
O_{F_1}/(a) \arrow[d] & O_{F_2}/(a) \arrow[l, "\varphi"'] \arrow[d] & O_{F_3}/(a) \arrow[l, "\varphi"'] \arrow[d] & \cdots \arrow[l] \\
O_{\mathbf{C}_p}/(a) & O_{\mathbf{C}_p}/(a) \arrow[l, "\varphi"'] & O_{\mathbf{C}_p}/(a) \arrow[l, "\varphi"'] & \cdots \arrow[l]
\end{tikzcd}$$

The projective limit of the upper row is $\mathcal{X}(F) := \mathcal{X}(F_\infty/F)$. The projective limit of the bottom row is $O_{\mathbf{C}_p^\flat}$. Therefore this diagram gives an embedding

$$O_{\mathcal{X}(F)} \to O_{\mathbf{C}_p^\flat},$$

which agrees with the embedding constructed in Section 2.6. We can also replace $\mathbf{C}_p$ by the perfectoid field $\widehat{F}_\infty$ in the bottom row. This gives the embedding $O_{\mathcal{X}(F)} \to O_{\widehat{F}_\infty^\flat}$.

3.1. We denote by $\mathbf{E}_F$ the image of $\mathcal{X}(F)$ in $\mathbf{C}_p^\flat$. Since $\mathbf{C}_p^\flat$ is algebraically closed, we have an embedding $\overline{\mathcal{X}(F)}$ of the separable closure of $\mathcal{X}(F)$ in $\mathbf{C}_p^\flat$. We denote by $\mathbf{E} := \overline{\mathbf{E}}_F$ the image of $\overline{\mathcal{X}(F)}$ in $\mathbf{C}_p^\flat$. Then for the Galois groups we have:

$$G_{F_\infty} \simeq G_{\mathcal{X}(F)} \simeq G_{\mathbf{E}}.$$

Let now K be a finite totally ramified extension of F and let $K_\infty = K(\zeta_{p^\infty})$ be its cyclotomic expension. Then $[K_\infty : F_\infty] \leqslant [K : F] < +\infty$. Therefore $\mathcal{X}(K) := \mathcal{X}(K_\infty/K) = \mathcal{X}(K_\infty/F)$ is a finite extension of $\mathcal{X}(F)$, and corresponds to a unique intermediate field $\mathbf{E}_F \subset \mathbf{E}_K \subset \mathbf{E}$. We have

$$\mathbf{E}_K = \mathbf{E}^{G_{K_\infty}}.$$

CHAPTER 5

p-adic representations of local fields

1. ℓ-adic representationss

1.1. Let E be a field equipped with a Hausdorff topology and let V be a finite dimensional E-vector space. Each choice of a basis of V fixes topological isomorphisms $V \simeq E^n$ and $\mathrm{Aut}(V) \simeq \mathrm{GL}_n(E)$ where $n = \dim_L(E)$. Note that V is equipped with the induced topology.

Definition. *A representation of a topological group G on V is a continuous homomorphism*

$$\rho : G \to \mathrm{Aut}(V).$$

Fixing a basis of V we can view a representation of G as a continuous homomorphism $G \to \mathrm{GL}_n(E)$.

Let K be a field and let $\overline{K}$ be a separable closure of K. We denote by G_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K. Recall that G_K is equipped with the inverse limit topology and therefore is a compact and totally disconnected topological group.

1.2. Example. Equip E with the discrete topology. Let $\rho : G_K \to \mathrm{GL}_n(E)$ be a representation of G_K. Then $H := \rho^{-1}\{1\}$ is an open normal subgroup in G_K. Since any open subgroup of G_K has a finite index, $(G_K : H) < +\infty$. Set $L := \overline{K}^H$. Then L/K is a finite extension, $\mathrm{Gal}(L/K) = G_K/H$, and ρ factors through $\mathrm{Gal}(L/K)$:

$$\begin{tikzcd} G_K \arrow[r] \arrow[dr] & \mathrm{GL}_n(E) \\ & \mathrm{Gal}(L/K). \arrow[u] \end{tikzcd}$$

Definition. *Let ℓ be a prime number.*

i)An ℓ-adic Galois representation is a representation of G_K on a finite dimensional $\mathbf{Q}_\ell$-vector space.

ii) An $\mathbf{Z}_\ell$-adic representation is of G_K is a free $\mathbf{Z}_\ell$-module T of finite rank equipped with a continuous homomorphism $\rho : G_K \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T)$.

Sometimes it is convenient to consider representations with coefficients with a finite extension E of $\mathbf{Q}_\ell$.

If $\rho : G_K \to \mathrm{Aut}_{\mathbf{Q}_\ell}(V)$ is an ℓ-adic representation, we will write

$$g(x) := \rho(g)(x), \qquad \forall g \in G_K, x \in V.$$

1.3. A morphism of ℓ-adic representations is a linear map $f : V_1 \to V_2$ such that

$$f(g(x)) = gf(x), \qquad \forall g \in G_K, \quad x \in V_1.$$

We denote by $\mathbf{Rep}_{\mathbf{Q}_\ell}(G_K)$ the category of p-adic representations of the absolute Galois group of a field K. Below we assemble some basic properties of this category.

1.3.1. $\mathbf{Rep}_{\mathbf{Q}_\ell}(G_K)$ is an abelian category.

1.3.2. $\mathbf{Rep}_{\mathbf{Q}_\ell}(G_K)$ is equipped with the internal Hom:

$$\mathrm{Hom}_{\mathbf{Q}_\ell}(V_1, V_2).$$

Namely, $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_1, V_2)$ is the $\mathbf{Q}_\ell$-vector space of all $\mathbf{Q}_\ell$-linear maps $f : V_1 \to V_2$ equipped with the following linear action of G_K:

$$(gf)(x) := g(f(g^{-1}(x)), \qquad \forall g \in G_K, \quad x \in V_1.$$

This induces a structure of an ℓ-adic representation on $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_1, V_2)$.

1.3.3. For each V, we have the dual representation $V^* = \mathrm{Hom}_{\mathbf{Q}_\ell}(V, \mathbf{Q}_\ell)$. The action of G_K on V^* is given by $(gf)(x) = f(g^{-1}(x))$.

1.3.4. $\mathbf{Rep}_{\mathbf{Q}_\ell}(G_K)$ is equipped with $\otimes$. Namely, if V_1 and V_2 are ℓ-adic representations, the structure of an ℓ-adic representation on the tensor product $V_1 \otimes_E V_2$ is given by

$$g(x_1 \otimes x_2) = g(x_1) \otimes g(x_2), \qquad g \in G_K.$$

Proposition 1.4. *For any ℓ-adic representation V, there exists a $\mathbf{Z}_\ell$-lattice stable under the action of G_K.*

Remark 1.5. *The proposition shows that the functor*

$$\begin{aligned} &\mathbf{Rep}_{\mathbf{Z}_\ell}(G_K) \to \mathbf{Rep}_{\mathbf{Q}_\ell}(G_K), \\ &T \mapsto T \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \end{aligned}$$

is essentially surjective.

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis of V and

$$T' = \mathbf{Z}_\ell e_1 + \cdots + \mathbf{Z}_\ell e_n$$

the associated lattice. The group

$$U = \mathrm{Aut}_{\mathbf{Z}_\ell}(T') \simeq \mathrm{GL}_n(\mathbf{Z}_\ell) \subset \mathrm{GL}_n(\mathbf{Q}_\ell) \simeq \mathrm{Aut}_{\mathbf{Q}_\ell}(V)$$

is open in $\mathrm{Aut}_{\mathbf{Q}_\ell}(V)$. Therefore $H := \rho^{-1}(U) \subset G_K$ is open and $(G_K : H) < +\infty$. Replacing H by $\underset{g}{\cap} gHg^{-1}$, where g runs the representatives of left cosets of H, one can assume that H is normal in G. Write $G = \overset{m}{\underset{i=1}{\cup}} g_i H$ and set

$$T = g_1(T') + \cdots + g_m(T').$$

Then T is a lattice in V, which is stable under the action of G_K. □

Below we give some examples of ℓ-adic representations.

1.5.1. *Roots of unity.* Let $\ell \neq \mathrm{char}(K)$. The group G_K acts on the groups μ_{ℓ^n} of ℓ^n-th roots of unity *via* the cyclotomic character $\chi_\ell : G_K \to \mathbf{Z}_\ell^*$

$$g(\zeta) = \zeta^{\chi_\ell(g)}, \qquad \text{if } g \in G_K,\ \zeta \in \mu_{\ell^n}.$$

Set $\mathbf{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}$ and $\mathbf{Q}_\ell(1) = \mathbf{Z}_\ell(1) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. Then $\mathbf{Q}_\ell(1)$ is a one dimensional $\mathbf{Q}_\ell$-vector space equipped with a continuous action of G_K. The homomorphism $G_K \to \mathrm{Aut}(\mathbf{Q}_\ell(1)) \simeq \mathbf{Q}_\ell^*$ concides with χ_ℓ.

1.5.2. *Elliptic curves.* Let E be an elliptic curve over a field K of characteristic 0. The group $A[\ell^n]$ of ℓ^n-torsion points of $E(\overline{K})$ is a Galois module which is isomorphic (not canonically) to $(\mathbf{Z}/\ell^n\mathbf{Z})^{2d}$ as an abstract group. The ℓ-adic Tate module of A is defined as the projective limit

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

with respect to the multiplication-by-ℓ maps $E[\ell^{n+1}] \to E[\ell^n]$. This is a free $\mathbf{Z}_\ell$-module of rank d equipped with a continuous action of G_K. The associated vector space $V_\ell(A) = T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ gives rise to an ℓ-adic representation

$$\rho_{E,\ell} : G_K \to \mathrm{Aut}(V_\ell(E)).$$

Note that $T_\ell(E)$ is a canonical G_K -lattice of $V_\ell(E)$. The reduction of $T_\ell(E)$ modulo ℓ is isomorphic to $E[\ell]$.

1.6. ℓ-adic representations of local fields ($\ell \neq p$). From now on, we consider ℓ-adic representations of local fields. Let K be a local field with residue field k_K of characteristic p. To distinguish between the cases $\ell \neq p$ and $\ell = p$, we will use in the second case the term p-adic keeping ℓ-adic exclusively for the inequal characteristic case.

We consider the ℓ-adic case. Recall that for the tame quotient of the inertia subgroup we have an isomorphism

$$\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \simeq \prod_{q \text{ prime}} \mathbf{Z}_q$$

(see (12)). Let ψ_ℓ denote the projection

$$\psi_\ell : I_K \to \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \to \mathbf{Z}_\ell.$$

The following general result reflects the Frobenius structure on the tame Galois group.

Theorem 1.7 (Grothendieck ℓ-adic monodromy theorem). *Let*

$$\rho : G_K \to \mathrm{GL}(V)$$

be an ℓ-adic representation. Then the following holds true:

i) There exists an open subgroup H of the inertia group I_K such that the automorphism $\rho(g)$ is unipotent for all $g \in H$.

ii) More precisely, there exists a nilpotent operator $N : V \to V$ such that

$$\rho(g) = \exp(N\psi_\ell(g)), \qquad \forall g \in H.$$

iii) Let $\widehat{\mathrm{Fr}}_K \in G_K$ *be any lift of the arithmetic Frobenius* Fr_K*. Set* $F = \rho(\widehat{\mathrm{Fr}}_K)$*. Then*

$$FN = q_K NF,$$

where $q_K = |k_K|$*.*

Proof. See [**29**] for details.

a) By Proposition 1.4, ρ can be viewed as an homomorphism

$$\rho : G_K \to \mathrm{GL}_d(\mathbf{Z}_\ell).$$

Let $U = 1 + \ell^2 \mathrm{M}_d(\mathbf{Z}_\ell)$. Then U has finite index in $\mathrm{GL}_d(\mathbf{Z}_\ell)$, and there exists a finite extension K'/K such that $\rho(G_{K'}) \subset U$. Without loss of generality, we may (and will) assume that $K' = K$.

b) The wild ramification subgroup P_K is a pro-p-group. Since U is a pro-ℓ-group with $\ell \neq p$, we have $\rho(P_K) = \{1\}$, and ρ factors through the tame ramification group $\mathrm{Gal}(K^{\mathrm{tr}}/K)$. Since $\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \simeq \prod\limits_q \mathbf{Z}_q$, the same argument shows that ρ factors through the Galos group of the extension K_ℓ^{tr}/K, where

$$K_\ell^{\mathrm{tr}} = K^{\mathrm{ur}}(\pi_K^{1/\ell^\infty}).$$

Let τ_ℓ be the automorphism that maps to 1 under the isomorphism $\mathrm{Gal}(K_\ell^{\mathrm{tr}}/K^{\mathrm{ur}}) \simeq \mathbf{Z}_\ell$. By Proposition 6.3, $\mathrm{Gal}(K_\ell^{\mathrm{tr}}/K)$ is the pro-ℓ-group topologically generated by τ_ℓ and any lift f_ℓ of Frobenius with the single relation

$$f_\ell \tau_\ell f_\ell^{-1} = \tau_\ell^{q_K}. \tag{37}$$

c) Set $X = \rho(\tau_\ell) \in U$. The ℓ-adic logarithm map converges on U, and we define

$$N := \log(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(X-1)^n}{n}.$$

From definitions it follows that for any $g \in I_K$ we have

$$\rho(g) = \rho(\tau_\ell^{\psi_\ell(g)}) = \exp(N\psi_\ell(g)).$$

Moreover, applying the identity $\log(BAB^{-1}) = B\log(A)B^{-1}$ to (37) and setting $F = \rho(f_\ell)$, we obtain that

$$FNF^{-1} = q_K N.$$

d) It remains to show that N is nilpotent. From the last formula it follows that N and $q_K N$ have the same eigenvalues. Therefore they are all zero, and the theorem is proved. □

2. Formal groups

2.1. Formal groups.

2.1.1. In this section, we make first steps in studing p-adic representations arising from p-divisible groups.

DEFINITION. *Let A be an integral domain. A one-dimensional commutative formal group over A is a formal power series $\mathscr{F}(X,Y)\in A[[X,Y]]$ satisfying the following conditions:*
i) $\mathscr{F}(\mathscr{F}(X,Y),Z)=\mathscr{F}(X,\mathscr{F}(Y,Z))$;
ii) $\mathscr{F}(X,Y)=\mathscr{F}(Y,X)$;
iii) $F(X,0)=X$ *and* $F(0,Y)=Y$;
iv) There exists $i(X)\in XA[[X]]$ *such that* $\mathscr{F}(X,i(X))=0$.

It can be proved that ii) and iv) follow from i) and iii). We will often write $X+_{\mathscr{F}}Y$ instead $\mathscr{F}(X,Y)$.

2.1.2. **Examples.** 1) The additive formal group $\widehat{\mathbf{G}}_a(X,Y)=X+Y$. Here $i(X)=-X$.

2) The multiplicative formal group $\widehat{\mathbf{G}}_m(X,Y)=X+Y+XY$. Note that $\widehat{\mathbf{G}}_m(X,Y)=(1+X)(1+Y)-1$. Here $i(X)=-\dfrac{X}{1+X}$.

3) More generally, for each $a\in A$,

$$\mathscr{F}(X,Y)=X+Y+aXY$$

is a formal group over A. Here $i(X)=-\dfrac{X}{1+aX}$.

2.1.3. We introduce basic notions of the theory of formal groups. An homomorphism of formal groups $\mathscr{F}\to\mathcal{G}$ over A is a power series $f\in XA[[X]]$ such that $f\circ\mathscr{F}(X,Y)=\mathcal{G}(f(X),f(Y))$. The set $\mathrm{Hom}_A(\mathscr{F},\mathcal{G})$ of homomorphisms $\mathscr{F}\to\mathcal{G}$ is an abelian group with respect to the addition defined as

$$f\oplus g=\mathcal{G}(f(X),g(X)).$$

We set $\mathrm{End}_A(\mathscr{F})=\mathrm{Hom}_A(\mathscr{F},\mathscr{F})$. Then $\mathrm{End}_A(\mathscr{F})$ is a ring with respect to the addition defined above and the multiplication given by the composition of power series:

$$f\circ g(X)=f(g(X)).$$

2.1.4. The module $\Omega^1_{A[[X]]}$ of formal Kähler differentials of $A[[X]]$ over A is the free $A[[X]]$-module generated by dX.

DEFINITION. *We say that $\omega(X)=f(X)dX\in\Omega^1_{A[[X]]}$ is an invariant differential form on the formal group $\mathscr{F}$ if*

$$\omega(X+_{\mathscr{F}}Y)=\omega(X).$$

2.1.5. The next proposition describes invariant differential forms on one-dimensional formal groups. We will write $\mathscr{F}'_1(X,Y)$ (respectively $\mathscr{F}'_2(X,Y)$ the formal derivative of $\mathscr{F}(X,Y)$ with respect to the first (respectively second) variable.

PROPOSITION 2.2. *The space of invariant differential forms on a one-dimensional formal group $\mathscr{F}(X,Y)$ is the free A-module of rank one generated by*

$$\omega_{\mathscr{F}}(X)=\frac{dX}{\mathscr{F}'_1(0,X)}.$$

PROOF. (See, for example, [**17**, Section 1.1].) a) Since $\mathscr{F}(Y,X) = Y + X +$ (terms of degree $\geqslant 2$), the series $\mathscr{F}_1'(0,X)$ is invertible in $A[[X]]$, and

$$\omega(X) := \frac{dX}{\mathscr{F}_1'(0,X)} \in A[[X]].$$

Differentiating the identity

$$\mathscr{F}(Z,\mathscr{F}(X,Y)) = \mathscr{F}(\mathscr{F}(Z,X),Y)$$

with respect ot Z, we have

$$\mathscr{F}_1'(Z,\mathscr{F}(X,Y)) = \mathscr{F}_1'(\mathscr{F}(Z,X),Y)\cdot\mathscr{F}_1'(Z,X).$$

Taking $Z = 0$, we obtain that

$$\frac{\mathscr{F}_1'(X,Y)}{\mathscr{F}_1'(0,\mathscr{F}(X,Y))} = \frac{1}{\mathscr{F}_1'(0,X)},$$

or equivalently, that

$$\frac{d\mathscr{F}(X,Y)}{\mathscr{F}_1'(0,\mathscr{F}(X,Y))} = \frac{dX}{\mathscr{F}_1'(0,X)}.$$

This shows that $\omega(X)$ is invariant.

b) Conversely, assume that $\omega(X) = f(X)dX$ is invariant. Then

$$f(\mathscr{F}(X,Y))\mathscr{F}_1'(X,Y) = f(X),$$

and setting $X = 0$, we obtain that $f(Y) = \mathscr{F}_1'(0,Y)f(0)$. Therefore

$$\omega(X) = f(0)\omega_{\mathscr{F}}(X),$$

and the proposition is proved. □

REMARK 2.3. *We can write*

$$\omega_{\mathscr{F}}(X) = \left(\sum_{n=0}^{\infty} a_n X^n\right)dX, \qquad \text{where } a_n \in A \text{ and } a_0 \neq 0.$$

2.3.1. Let K denote the field of fractions of A. We say that a power series $\lambda(X) \in K[[X]]$ is a logarithm of $\mathscr{F}$, if

$$\lambda(X +_{\mathscr{F}} Y) = \lambda(X) + \lambda(Y).$$

PROPOSITION 2.4. *Assume that* $\mathrm{char}(K) = 0$. *Then the map*

$$\omega \mapsto \lambda_\omega(X) := \int_0^X \omega$$

establishes an isomorphism between the one-dimensional K-vector space generated by invariant differential forms on $\mathscr{F}$ and the K-vector space of logarithms of $\mathscr{F}$.

Proof. a) Let $\omega(X) = g(X)dX$ be a nonzero invariant differential form on $\mathscr{F}$. Set $g(X) = \sum_{n=0}^{\infty} b_n X^n$. Since $\mathrm{char}(K) = 0$, the series $f(X)$ has the formal primitive

$$\lambda_\omega(X) := \int_0^X \omega = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} X^n \in K[[X]].$$

The invariance of ω reads

$$g(\mathscr{F}(X,Y))\mathscr{F}_1'(X,Y) = g(X),$$

and taking the primitives, we obtain that

$$\lambda_\omega(X +_{\mathscr{F}} Y) = \lambda_\omega(X) + h(Y)$$

for some $h(Y) \in K[[Y]]$. Putting $X = 0$ in the last formula, we have $h(Y) = \lambda_\omega(Y)$, and $\lambda_\omega(X +_{\mathscr{F}} Y) = \lambda_\omega(X) + \lambda_\omega(Y)$. Therefore λ_ω is a logarithm of $\mathscr{F}$.

b) Conversely, let $\lambda(X)$ be a logarithm of $\mathscr{F}$. Differentiating the equality $\lambda(Y +_{\mathscr{F}} X) = \lambda(Y) + \lambda(X)$ with respect to Y and setting $Y = 0$ we obtain that

$$\lambda'(X) = \frac{\lambda'(0)}{\mathscr{F}_1(0,X)}.$$

Therefore $\omega = \lambda'(0)\omega_{\mathscr{F}}$, and the proposition is proved. □

Definition 2.5. *Let*

$$\lambda_{\mathscr{F}}(X) = \int_0^X \omega_{\mathscr{F}}.$$

Note that $\lambda_{\mathscr{F}}(X)$ is the unique logarithm of $\mathscr{F}$ such that

$$\lambda_{\mathscr{F}}(X) \equiv X \pmod{\deg 2}.$$

From Proposition 2.4 if follows that over a field of characteristic 0 all formal goups are isomorphic to the additive formal group. Indeed, $\lambda_{\mathscr{F}}$ is an isomorphism $\mathscr{F} \xrightarrow{\sim} \widehat{\mathbf{G}}_a$.

2.5.1. **Example.** For the multiplicative group we have

$$\omega_{\mathbf{G}_m}(X) = \frac{dX}{1+X}, \qquad \lambda_{\mathbf{G}_m}(X) = \log(1+X) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{X^n}{n}.$$

2.5.2. We consider formal groups over the ring of integers of a local field K of characteristic 0 and residue caracteristic p.

For each $n \in \mathbf{Z}$ we denote by $[n]$ the formal multiplication by n:

$$[n] = \begin{cases} \underbrace{X +_{\mathscr{F}} + X_{\mathscr{F}} +_{\mathscr{F}} \cdots + X}_{n}, & \text{if } n \geqslant 0, \\ \\ i([-n]), & \text{if } n < 0. \end{cases}$$

This defines an injection

$$[\ \ ] : \mathbf{Z} \to \mathrm{End}_{O_K}(\mathscr{F}), \qquad n \to [n](X) = nX + \cdots.$$

It can be easily checked that this map can be extended by continuity to an injective map

$$[\ ]: \mathbf{Z}_p \to \mathrm{End}_{O_K}(\mathscr{F}), \qquad a \to [a](X) = aX + \cdots.$$

PROPOSITION 2.6. *Let $\mathscr{F}$ be a formal group over O_K. Then either*

$$[p](X) \equiv 0 \pmod{\pi_K}$$

or there exists an integer $h \geqslant 1$ and a power series $g(X) = c_1X + \cdots$ such that $c_1 \not\equiv 0 \pmod{\pi_K}$ and

$$[p](X) \equiv g(X^{p^h}) \pmod{\pi_K}. \tag{38}$$

PROOF. The proof is not difficult. See, for example, [**16**, Chapter I, § 3, Theorem 2]. □

DEFINITION 2.7. *If $[p](X) \equiv 0 \pmod{\pi_K}$, we say that $\mathscr{F}$ has infinite height. Otherwise, we say that $\mathscr{F}$ is p-divisible and call the height of $\mathscr{F}$ the unique $h \geqslant 1$ satisfying the condition (38).*

2.7.1. Now we can explain the connection between formal groups and p-adic representations. Any formal group law $\mathscr{F}(X,Y)$ over O_K defines a structure of $\mathbf{Z}_p$-module on the maximal ideal $\mathfrak{m}_{\overline{K}}$ of $\overline{K}$:

$$\begin{aligned} &\alpha +_{\mathscr{F}} \beta := \mathscr{F}(\alpha,\beta), \quad \alpha,\beta \in \mathfrak{m}_{\overline{K}}, \\ &\mathbf{Z}_p \times \mathfrak{m}_{\overline{K}} \to \mathfrak{m}_{\overline{K}}, \qquad (a,\alpha) \mapsto [a](\alpha). \end{aligned}$$

We will denote by $\mathscr{F}(\mathfrak{m}_{\overline{K}})$ the ideal $\mathfrak{m}_{\overline{K}}$ equipped with this $\mathbf{Z}_p$-module structure. The analogious notation will be used for O_K-submodules of $\mathfrak{m}_{\overline{K}}$.

PROPOSITION 2.8. *Assume that $\mathscr{F}$ is a formal group of finite height h. Then*
i) The map $[p] : \mathscr{F}(\mathfrak{m}_{\overline{K}}) \to \mathscr{F}(\mathfrak{m}_{\overline{K}})$ is surjecive.
ii) The kernel $\ker([p])$ is a free $\mathbf{Z}/p\mathbf{Z}$-module of rank h.

PROOF. i) Consider the equation

$$[p](X) = \alpha, \qquad \alpha \in \mathscr{F}(\mathfrak{m}_{\overline{K}}).$$

A version of the Weierstrass preparation theorem (see, for example, the proof of [**20**, Theorem 4.2]) shows that this equation can be written in the form $f(X) = g(\alpha)$, where $f(X) \in O_K[X]$ is a polynomial of degree p^h such that $f(X) \equiv X^{p^h} \pmod{\pi_K}$, and $g \in O_K[[X]]$. Therefore the roots of this equation are in $\mathfrak{m}_{\overline{K}}$.

ii) To prove that $\ker([p])$ is a free $\mathbf{Z}/p\mathbf{Z}$-module of rank h we only need to show that the roots of the equation $[p](X) = 0$ are all of multiplicity one. Differentiating the identity

$$[p](\mathscr{F}(X,Y)) = \mathscr{F}([p](X),[p](Y))$$

with respect to Y and setting $Y = 0$, we get

$$[p]'(X) \cdot \mathscr{F}_2'(X,0) = \mathscr{F}_2'([p](X),0).$$

Let $[p](\xi) = 0$. Since $\mathscr{F}_2'(X,0)$ is invertible in $O_K[[X]]$ and $\xi \in \mathfrak{m}_{\overline{K}}$, we have $\mathscr{F}_2'(\xi,0) \neq 0$ and $[p]'(\xi) \neq 0$. Therefore ξ is a simple root. □

2.8.1. For $n \geqslant 1$, let $T_{\mathscr{F},n}$ denote the p^n-torsion subgroup of $\mathscr{F}(\overline{\mathfrak{m}}_K)$. From Proposition 2.8 it follows that as abelian group, it is isomorphic to $(\mathbf{Z}/p^n\mathbf{Z})^h$ and sits in the exact sequence

$$0 \to T_{\mathscr{F},n} \to \mathscr{F}(\mathfrak{m}_{\overline{K}}) \xrightarrow{[p^n]} \mathscr{F}(\mathfrak{m}_{\overline{K}}) \to 0.$$

As in the case of abelian varieties, the Tate module of $\mathscr{F}$ is defined as the projective limit

$$T(\mathscr{F}) = \varprojlim_n T_{\mathscr{F},n}$$

with respect to the multiplication by p maps. Since the series $[p^n](X)$ have coefficients in O_K, the Galois group G_K acts on $E_{\mathscr{F},n}$, and this action gives rise to a $\mathbf{Z}_p$-adic representation

$$\rho_{\mathscr{F}} : G_K \to \mathrm{Aut}_{\mathbf{Z}_p}(T(\mathscr{F})) \simeq \mathrm{GL}_h(\mathbf{Z}_p).$$

We will denote by $V(\mathscr{F}) = T(\mathscr{F}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ the associated p-adic representation.

3. Classification of p-adic representations: the case of characteristic p

3.1. In this section, we turn to p-adic representations. The main reference is [**11**]. It turns out, that it is possible to give a full classification of p-adic representations of the Galois group of *any* field K of characteristic p in terms of modules equipped with a semilinear operator. This is explained by the existence of the absolute Frobenius structure on K. To simplify the exposition we will work with the purely inseparable closure $F := K^{\mathrm{rad}}$ of K. It is a perfect field with $G_F = G_K$. However, it is not absolutely necessary. On the contrary, it is sometime preferable to work with non-perfect fields.

Consider the ring of Witt vectors

$$O_{\mathscr{F}} = W(F)$$

Recall that $O_{\mathscr{F}}$ is a complete discrete valuation ring of characteristic 0 with maximal ideal $(p) = pO_{\mathscr{F}}$ and residue field F. Its field of fractions $\mathscr{F} = O_{\mathscr{F}}[1/p]$ is an unramified discrete valuation field.

Definition. *Let $A = F, O_{\mathscr{F}}$ or $\mathscr{F}$.*

i) A φ-module over A is a finitely generated free A-module (respectively $\mathscr{F}$-vector space) D equipped with a semilinear injective operator $\varphi : D \to D$. Namely, φ satisifies the following properties:

$$\begin{aligned} &\varphi(x+y) = \varphi(x) + \varphi(y), && \forall x, y \in D, \\ &\varphi(ax) = \varphi(a)\varphi(x), && \forall a \in A, x \in D. \end{aligned}$$

ii) Assume that $A = F$ or $O_{\mathscr{F}}$. A φ-module D over A is étale if the matrix of the operator $\varphi : D \to D$ is invertible over A. This condition does not depend on the choice of the basis.

iii) An étale φ-module over $\mathscr{F}$ is a finitely generated free $\mathscr{F}$-module equipped with a semilinear operator φ and having an étale $O_{\mathscr{F}}$-lattice.

3.1.1. A morphism of φ-modules is an A-linear map $f : D_1 \to D_2$ such that

$$f(\varphi(x)) = \varphi(f(x)), \qquad \forall x \in D_1.$$

We denote by $\mathbf{M}_A^{\varphi,\text{ét}}$ the category of étale φ-modules over A.

Exercise 14. We consider A as an A-module via the Frobenius map $\varphi : A \to A$ (so $a \in A$ acts on $x \in A$ as the multiplication by $\varphi(a)$). For a φ-module D, let $D \otimes_{A,\varphi} A$ denote the tensor product of A-modules D and A. We consider $D \otimes_{A,\varphi} A$ as an A-module:

$$\lambda(d \otimes a) = d \otimes \lambda a, \qquad \lambda \in A \quad d \otimes a \in D \otimes_{A,\varphi} A.$$

i) Show that the map

$$\Phi : D \otimes_{A,\varphi} A \to D, \qquad d \otimes a \mapsto a\varphi(d)$$

is A-linear. Show that Φ is an isomorphism if and only if D is étale.

ii) Let D_1 and D_2 be two étale φ-modules. Denote by

$$\underline{\mathrm{Hom}}(D_1, D_2) := \mathrm{Hom}_A(D_1, D_2)$$

the A-module of all A-linear maps $f : D_1 \to D_2$ (so, in general, f is not compatible with the action of φ). Define the map $\varphi(f)$ as the composition:

$$\varphi(f) : D_1 \xrightarrow{\Phi^{-1}} D_1 \otimes_{A,\varphi} A \xrightarrow{f \otimes \mathrm{id}} D_2 \otimes_{A,\varphi} A \xrightarrow{\Phi} D_2.$$

Show that the following holds:

a) $\varphi(f)(\varphi(d)) = \varphi(f(d))$;

b) $\varphi(f) = f$ if and only if $f(\varphi(d)) = \varphi(f(d)), \quad \forall d \in D$;

c) $\underline{\mathrm{Hom}}(D_1, D_2)$ is an étale φ-module.

Exercise 15. Let D_1 and D_2 be two φ-modules. Equip $D_1 \otimes_A D_2$ with the diagonal action of φ :

$$\varphi(d_1 \otimes d_2) = \varphi(d_1) \otimes \varphi(d_2).$$

Show that if that D_1 and D_2 are étale, then $D_1 \otimes_A D_2$ is.

Proposition 3.2. *Let D be an étale φ-module over F of dimension n. Then* $\mathrm{Hom}_F(D, \overline{F})^{\varphi=1}$ *and* $(D \otimes_F \overline{F})^{\varphi=1}$ *are* $\mathbf{F}_p$*-vector spaces of dimension n.*

Proof. a) Fix a basis $\{e_1, \dots, e_n\}$ of D. Write:

$$\varphi(e_i) = \sum_{i=1}^{n} a_{ij} e_j, \qquad a_{ij} \in F, \qquad 1 \leqslant i \leqslant n.$$

Consider the $\mathbf{F}_p$-vector space $\mathrm{Hom}_F(D, \overline{F})^{\varphi=1}$. Let $f \in \mathrm{Hom}_F(D, \overline{F})$. Then $\varphi(f) = f$ if and only if $f(\varphi(d)) = \varphi(f(d))$ for all $d \in D$ (see Exercise 14). Taking $d = e_1, \dots, e_n$, we see that $\varphi(f) = f$ if and only if the vector $(f(e_1), \dots f(e_n)) \in \overline{F}^n$ is a solution of the system

$$X_i^p - \sum_{i=1}^{n} a_{ij} X_j = 0, \qquad 1 \leqslant i \leqslant n.$$

Claim: The solutions of the above system form a $\mathbf{F}_p$-vector space of dimension n.

COMMENTS ON THE CLAIM. The claim follows from standard results of commutative algebra (which are beyond the program of this course). Here are the details. Let $I \subset F[X_1,\dots,X_n]$ denote the ideal generated by

$$X_i^p - \sum_{i=1}^{n} a_{ij}X_j, \qquad 1 \leqslant i \leqslant n.$$

Consider the algebra $A := F[X_1,\dots,X_n]/I$. Therefore we have isomorphisms:

$$\mathrm{Hom}_F(D,\overline{F})^{\varphi=1} = \mathrm{Hom}_{F-\mathrm{alg}}(A,\overline{F}) = \mathrm{Spec}(A)(\overline{F}).$$

The algebra A is étale over F if and only if the matrix $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ is invertible if and only if D is an étale φ-module. On the other hand, if D is étale, then the cardinality of $\mathrm{Spec}(A)(\overline{F})$ is p^n, and $\mathrm{Hom}_F(D,\overline{F})^{\varphi=1}$ is a $\mathbf{F}_p$-vector space of dimension n (see, for example, [**22**, Chapter I, §3]). □

b) For the dual module D^*, we have a canonical isomorphisms:

$$D\otimes_F \overline{F} \simeq \mathrm{Hom}_F(D^*,F)\otimes_F \overline{F} \simeq \mathrm{Hom}_F(D^*,\overline{F}).$$

Then

$$(D\otimes_F \overline{F})^{\varphi=1} \simeq \mathrm{Hom}_F(D^*,\overline{F})^{\varphi=1},$$

and applying the previous remark to D^*, we see that $(D\otimes_F \overline{F})^{\varphi=1}$ is a $\mathbf{F}_p$-vector space of dimension n. The proposition is proved.

□

3.3. Following Fontaine [**11**], we construct a canonical equivalence between the category $\mathbf{Rep}_{\mathbf{F}_p}(G_K)$ of modular Galois representations of G_K and $\mathbf{M}_F^{\varphi,\text{ét}}$. For any $V \in \mathbf{Rep}_{\mathbf{F}_p}(G_K)$, set:

$$\mathbf{D}_F(V) = (V\otimes_{\mathbf{F}_p} \overline{F})^{G_K}.$$

Since G_K acts trivially on F, it is clear that $\mathbf{D}_F(V)$ is an F-module equipped with the diagonal action of φ (here φ acts trivially on V). For any $D \in \mathbf{M}_F^{\varphi,\text{ét}}$, set:

$$\mathbf{V}_F(D) = (D\otimes_F \overline{F})^{\varphi=1}.$$

Then $\mathbf{V}_F(D)$ is an $\mathbf{F}_p$-vector space equipped with the diagonal action of G_K (here G_K acts trivially on D).

THEOREM 3.4. *i) Let $V \in \mathbf{Rep}_{\mathbf{F}_p}(G_K)$ be a modular Galois representation of dimension n. Then $\mathbf{D}_F(V)$ is an étale φ-module of rank n over F.*

ii) Let $D \in \mathbf{M}_F^{\varphi,\text{ét}}$ be an étale φ-module of rank n over F. Then $\mathbf{V}_F(D)$ is a modular Galois representation of G_K of dimension n over $\mathbf{F}_p$.

iii) The functors $\mathbf{D}_F$ and $\mathbf{V}_F$ establish equivalences of tannakian categories

$$\mathbf{D}_F\,:\,\mathbf{Rep}_{\mathbf{F}_p}(G_K)\to \mathbf{M}_F^{\varphi,\text{ét}}, \qquad \mathbf{V}_F\,:\,\mathbf{M}_F^{\varphi,\text{ét}}\to \mathbf{Rep}_{\mathbf{F}_p}(G_K),$$

which are quasi-inverse to each other. Moreover, for all $T \in \mathbf{Rep}_{\mathbf{F}_p}(G_K)$ and $D \in \mathbf{M}_F^{\varphi,\text{ét}}$, we have canonical and functorial isomorphisms compatible with the actions *of G_K and φ on the both sides:*

$$\mathbf{D}_F(T)\otimes_F \overline{F} \simeq T\otimes_{\mathbf{F}_p} \overline{F},$$
$$\mathbf{V}_F(D)\otimes_{\mathbf{F}_p} \overline{F} \simeq D\otimes_F \overline{F}.$$

Th proof of this theorem uses the following result:

THEOREM 3.5. *[Hilbert's theorem 90] Let E be a field, and let X be a finite-dimensional vector space over the separable closure $\overline{E}$ of E. Assume that X is equipped with a continuous semi-linear action of $G_E := \mathrm{Gal}(\overline{E}/E)$:*

$$g(x+y) = g(x)+g(y), \qquad \forall g \in G_E, \quad x,y \in X,$$
$$g(\lambda x) = g(\lambda)g(x), \qquad \forall g \in G_E, \quad x \in X.$$

Then:

i) X has a basis fixed by G_E;

ii) The map

$$X^{G_E}\otimes_E \overline{E} \to X, \qquad x\otimes\lambda \mapsto \lambda x$$

is an isomorphism.

PROOF. In the course, we omit the proof of this theorem. It follows from the standard form of the non-abelian Hilbert's theorem 90. Here are some detail.

i) Let $\{e_1,\dots,e_n\}$ be a basis of X. For any $g \in \mathrm{Gal}(\overline{E}/E)$, let $A_g \in \mathrm{GL}_n(\overline{E})$ denote the unique matrix such that

$$g(e_1,\dots,e_n) = (e_1,\dots,e_n)A_g.$$

Then the map

$$f : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\overline{E}), \qquad f(g) = A_g$$

is a 1-cocyle, namely

$$f(g_1g_2) = f(g_1)(g_1f(g_2)), \qquad \forall g_1,g_2 \in G_E.$$

Hilbert's Theorem 90 (as stated, for example, in [**24**, Theorem 6.2.3]) says that there exists a matrix $B \in \mathrm{GL}_n(\overline{E})$ such that

$$f(g) = Bg(B)^{-1}, \qquad \forall g \in G_E.$$

It is easy to check that $(e_1,\dots,e_n)B$ is fixed by G_E. Therefore X has a basis fixed by G_E. This proves the first assertion.

ii) The second assertion follows from i). □

PROOF OF THEOREM 3.4. a) Let $V \in \mathbf{Rep}_{\mathbf{F}_p}(G_K)$ be a modular representation of dimension n. The Galois group G_F acts semi-linearly on $V\otimes_{\mathbf{F}_p}\overline{F}$. From Hilbert's Theorem 90, it follows that $\mathbf{D}_F(V) = (V\otimes_{\mathbf{F}_p}\overline{F})^{G_F}$ has dimension n over F, and that the multiplication in $\overline{F}$ induces an isomorphism

$$(V\otimes_{\mathbf{F}_p}\overline{F})^{G_F}\otimes_F \overline{F} \xrightarrow{\sim} V\otimes_{\mathbf{F}_p}\overline{F}.$$

Hence:

$$\mathbf{D}_F(V)\otimes_F \overline{F} \xrightarrow{\sim} V\otimes_{\mathbf{F}_p}\overline{F}.$$

This isomorphism shows that the matrix of φ is invertible in $\mathrm{GL}_n(\overline{F})$ and therefore in $\mathrm{GL}_n(F)$. This proves that $\mathbf{D}_F(V)$ is étale.

Taking the φ-invariants on the both sides, one has:

$$\mathbf{V}_F(\mathbf{D}_F(V)) = (\mathbf{D}_F(V)\otimes_F \overline{F})^{\varphi=1} \xrightarrow{\sim} (V\otimes_{\mathbf{F}_p} \overline{F})^{\varphi=1} = V. \tag{39}$$

b) Conversely, let $D \in \mathbf{M}_F^{\varphi,\text{ét}}$. By Proposition 3.2, $\mathbf{V}_F(D)$ is a $\mathbf{F}_p$-vector space of dimension n. Consider the map

$$\alpha : (D\otimes_F \overline{F})^{\varphi=1} \otimes_{\mathbf{F}_p} \overline{F} \to D\otimes_F \overline{F}, \tag{40}$$

induced by the multiplication in $\overline{F}$. We claim that this map is an isomorpism. Since the both sides have the same dimension over $\overline{F}$, it is sufficient to prove the injectivity. To do that, we use the following argument, known as Artin's trick. Assume that f is not surjective, and take a non-zero element $x \in \ker(\alpha)$ which has a shortest presentation in the form

$$x = \sum_{i=1}^{m} d_i \otimes a_i, \qquad d_i \in \mathbf{V}_F(D), \quad a_i \in \overline{F}.$$

Without loss of generality, we can assume that $a_m = 1$ (dividing by a_m). Note that $\varphi(x) - x \in \ker(\alpha)$. On the other hand, it can be written as:

$$\varphi(x) - x = \sum_{i=1}^{m} d_i \otimes (\varphi(a_i) - a_i) = \sum_{i=1}^{m-1} d_i \otimes (\varphi(a_i) - a_i).$$

By our choice of x, this implies that $\varphi(a_i) = a_i$, and therefore $a_i \in \mathbf{F}_p$ for all i. But in this case $x \in \mathbf{V}_F(D)$, and $x = \alpha(x) = 0$. This proves the injectivity of (40).

c) By part b), we have an isomorphism:

$$\mathbf{V}_F(D)\otimes_{\mathbf{F}_p} \overline{F} \to D\otimes_F \overline{F}.$$

Taking the Galois invariants on the both sides, we obtain:

$$\mathbf{D}_F(\mathbf{V}_F(D)) = (\mathbf{V}_F(D)\otimes_{\mathbf{F}_p} \overline{F})^{G_F} \xrightarrow{\sim} (D\otimes_F \overline{F})^{G_F} = D. \tag{41}$$

From (39) and (41), it follows that the functors $\mathbf{D}_F$ and $\mathbf{V}_E$ are quasi-inverse to each other. In particular, they are equivalences of categories. Other assertions can be checked easily. □

3.5.1. Now we turn to $\mathbf{Z}_p$-representations. For all $T \in \mathbf{Rep}_{\mathbf{Z}_p}(G_K)$ and $D \in \mathbf{M}_{O_{\mathscr{F}}}^{\varphi,\text{ét}}$, set:

$$\mathbf{D}_{O_{\mathscr{F}}}(T) = (T\otimes_{\mathbf{Z}_p} W(\overline{F}))^{G_K},$$
$$\mathbf{V}_{O_{\mathscr{F}}}(D) = (D\otimes_{O_{\mathscr{F}}} W(\overline{F}))^{\varphi=1}.$$

The following theorem can be deduced from Theorem 3.4 by devissage.

THEOREM 3.6 (Fontaine). *i) Let $T \in \mathbf{Rep}_{\mathbf{Z}_p}(G_K)$ be a $\mathbf{Z}_p$-representation. Then $\mathbf{D}_{O_{\mathscr{F}}}(T)$ is an étale φ-module over $O_{\mathscr{F}}$.*

ii) Let $D \in \mathbf{M}_{O_{\mathscr{F}}}^{\varphi,\text{ét}}$ be an étale φ-module over $O_{\mathscr{F}}$. Then $\mathbf{V}_{O_{\mathscr{F}}}(D)$ is a $\mathbf{Z}_p$-representation of G_K.

iii) The functors $\mathbf{D}_{O_{\mathscr{F}}}$ *and* $\mathbf{V}_{O_{\mathscr{F}}}$ *establish equivalences of categories*

$$\mathbf{D}_{O_{\mathscr{F}}}\,:\,\mathbf{Rep}_{\mathbf{Z}_p}(G_K)\to \mathbf{M}^{\varphi,\text{ét}}_{O_{\mathscr{F}}},\qquad \mathbf{V}_{O_{\mathscr{F}}}\,:\,\mathbf{M}^{\varphi,\text{ét}}_{O_{\mathscr{F}}}\to \mathbf{Rep}_{\mathbf{Z}_p}(G_K),$$

which are quasi-inverse to each other. Moreover, for all $T\in \mathbf{Rep}_{\mathbf{Z}_p}(G_K)$ *and* $D\in \mathbf{M}^{\varphi,\text{ét}}_{O_{\mathscr{F}}}$, *we have canonical and functorial isomorphisms compatible with the actions of* G_K *and* φ *on the both sides:*

$$\mathbf{D}_{O_{\mathscr{F}}}(T)\otimes_{O_{\mathscr{F}}} W(\overline{F})\simeq T\otimes_{\mathbf{Z}_p} W(\overline{F}),$$
$$\mathbf{V}_{O_{\mathscr{F}}}(D)\otimes_{\mathbf{Z}_p} W(\overline{F})\simeq D\otimes_{O_{\mathscr{F}}} W(\overline{F}).$$

3.7. For p-adic representations, we have the following theorem. Here $\widehat{\mathscr{F}}^{\mathrm{ur}}:=W(\overline{F})[1/p]$ is the completion of the maximal unramified extension of $\mathscr{F}$.

THEOREM 3.8. *i) Let V be a p-adic representation of G_K of dimension n. Then* $\mathbf{D}_{\mathscr{F}}(V)=(V\otimes_{\mathbf{Q}_p}\widehat{\mathscr{F}}^{\mathrm{ur}})^{G_K}$ *is an étale φ-module of dimension n over $\mathscr{F}$.*

ii) Let $D\in \mathbf{M}^{\varphi,\text{ét}}_{\mathscr{F}}$ *be an étale φ-module of dimension n over $\mathscr{F}$. Then* $\mathbf{V}_{\mathscr{F}}(D)=(D\otimes_{\mathbf{Q}_p}\widehat{\mathscr{F}}^{\mathrm{ur}})^{\varphi=1}$ *is a p-adic Galois representation of G_K of dimension n over* $\mathbf{Q}_p$.

iii) The functors

$$\mathbf{D}_{\mathscr{F}}\,:\,\mathbf{Rep}_{\mathbf{Q}_p}(G_K)\to \mathbf{M}^{\varphi,\text{ét}}_{\mathscr{F}},$$
$$\mathbf{V}_{\mathscr{F}}\,:\,\mathbf{M}^{\varphi,\text{ét}}_{\mathscr{F}}\to \mathbf{Rep}_{\mathbf{Q}_p}(G_K),$$

are equivalences of tannakian categories, which are quasi-inverse to each other. Moreover, for all $V\in\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$ *and* $D\in \mathbf{M}^{\varphi,\text{ét}}_{\mathscr{F}}$, *we have canonical and functorial isomorphisms compatible with the actions of* G_K *and* φ *on the both sides:*

$$\mathbf{D}_{\mathscr{F}}(V)\otimes_{\mathscr{F}}\widehat{\mathscr{F}}^{\mathrm{ur}}\simeq V\otimes_{\mathbf{Q}_p}\widehat{\mathscr{F}}^{\mathrm{ur}},$$
$$\mathbf{V}_{\mathscr{F}}(D)\otimes_{\mathbf{Q}_p}\widehat{\mathscr{F}}^{\mathrm{ur}}\simeq D\otimes_{\mathscr{F}}\widehat{\mathscr{F}}^{\mathrm{ur}}.$$

4. The case of characteristic 0

4.1. In this section, K is a local field of characteristic 0 with residual characteristic p. Let $K_\infty=K(\zeta_{p^\infty})$ denote the p-cyclotomic extension of K. Set $G_{K_\infty}=\mathrm{Gal}(\overline{K}/K_\infty)$ and $\Gamma_K=\mathrm{Gal}(K_\infty/K)$. Then K_∞/K is a deeply ramified (even an APF) extension, and we can consider the tilt of its completion:

$$F:=\widehat{K}^{\flat}_\infty.$$

The field F is perfect, of characteristic p, and we apply to F the contructions of Section 3. Namely, set $O_{\mathscr{F}}=W(F)$ and $\mathscr{F}=O_{\mathscr{F}}[1/p]$.

The ring of Witt vectors $W(F)$ is equipped with the p-adic (standard) topology. Now we equip it with a coarser topology, which will be called the *canonical topology*. It is defined as the topology of the infinite direct product

$$W(F)=F^{\mathbf{N}},$$

where each F is equipped with the topology induced by the absolute value $|\cdot|_F$. For any ideal $\mathfrak{a}\subset O_F$ and integer $n\geqslant 0$, the set

$$U_{\mathfrak{a},n}=\{x=(x_0,x_1,\dots)\in W(F)\mid x_i\in\mathfrak{a}\quad\text{for all } 0\leqslant i\leqslant n\}$$

is an ideal in $W(F)$. In the canonical topology, the family $(U_{\mathfrak{a},n})$ of these ideals form a base of the fundamental system of neighborhoods of $W(F)$.

4.2. By Proposition 4.4, the separable closure $\overline{F}$ of F is dense in $\mathbf{C}_K^\flat$ and we have a natural inclusion $W(\overline{F}) \subset W(\mathbf{C}_K^\flat)$. The Galois group G_K acts naturally on the maximal unramified extension $\mathscr{F}^{\mathrm{ur}}$ of $\mathscr{F}$ in $W(\mathbf{C}_K^\flat)[1/p]$ and on its p-adic completion $\widehat{\mathscr{F}}^{\mathrm{ur}} = W(\overline{F})[1/p]$. By Theorem 4.5, this action induces a canonical isomorphism:

$$G_{K_\infty} \simeq G_F (\simeq \mathrm{Gal}(\mathscr{F}^{\mathrm{ur}}/\mathscr{F})). \tag{42}$$

In particular, $(\widehat{\mathscr{F}}^{\mathrm{ur}})^{H_K} = \mathscr{F}$. The cyclotomic Galois group Γ_K acts on F and therefore on $O_{\mathscr{F}}$ and $\mathscr{F}$.

Definition. *Let $A = F, O_{\mathscr{F}}$, or $\mathscr{F}$. A (φ, Γ_K)-module over A is a φ-module over A equipped with a continuous semi-linear action of Γ_K commuting with φ. A (φ, Γ_K)-module is étale if it is étale as a φ-module.*

We denote by $\mathbf{M}_A^{\varphi,\Gamma,\text{ét}}$ the category of (φ, Γ_K)-modules over A. It can be easily seen that $\mathbf{M}_A^{\varphi,\Gamma,\text{ét}}$ is an abelian tensor category. Moreover, if $A = F$ or $\mathscr{F}$, it is neutral tannakian.

4.2.1. Now we are in position to introduce the main constructions of Fontaine's theory of (φ, Γ_K)-modules. Let T be a $\mathbf{Z}_p$-representation of G_K. Set:

$$\mathbf{D}_{O_{\mathscr{F}}}(T) = (T \otimes_{\mathbf{Z}_p} W(\overline{F}))^{G_{K_\infty}}.$$

Thanks to the isomorphism (42) and the results of Section 3, $\mathbf{D}_{O_{\mathscr{F}}}(T)$ is an étale φ-module. In addition, it is equipped with a natural action of Γ_K, and therefore we have a functor

$$\mathbf{D}_{O_{\mathscr{F}}} : \mathbf{Rep}_{\mathbf{Z}_p}(G_K) \to \mathbf{M}_{O_{\mathscr{F}}}^{\varphi,\Gamma,\text{ét}}.$$

Conversely, let D be an étale (φ, Γ_K)-module over $O_{\mathscr{F}}$. Set:

$$\mathbf{V}_{O_{\mathscr{F}}}(D) = (D \otimes_{\mathbf{Z}_p} W(\overline{F}))^{\varphi=1}.$$

By the results of Section 3, $\mathbf{V}_{O_{\mathscr{F}}}(D)$, is a free $\mathbf{Z}_p$-module of the same rank. Moreover, it is equipped with a natural action of G_K, and we have a functor

$$\mathbf{V}_{O_{\mathscr{F}}} : \mathbf{M}_{O_{\mathscr{F}}}^{\varphi,\Gamma,\text{ét}} \to \mathbf{Rep}_{\mathbf{Z}_p}(G_K).$$

Theorem 4.3 (Fontaine). *i) The functors $\mathbf{D}_{O_{\mathscr{F}}}$ and $\mathbf{V}_{O_{\mathscr{F}}}$ are equivalences of categories, which are quasi-inverse to each other.*

ii) For all $T \in \mathbf{Rep}_{\mathbf{Z}_p}(G_K)$ and $D \in \mathbf{M}_{O_{\mathscr{F}}}^{\varphi,\text{ét}}$, we have canonical and functorial isomorphisms compatible with the actions of G_K and φ on the both sides:

$$\begin{aligned} \mathbf{D}_{O_{\mathscr{F}}}(T) \otimes_{O_{\mathscr{F}}} W(\overline{F}) &\simeq T \otimes_{\mathbf{Z}_p} W(\overline{F}), \\ \mathbf{V}_{O_{\mathscr{F}}}(D) \otimes_{\mathbf{Z}_p} W(\overline{F}) &\simeq D \otimes_{O_{\mathscr{F}}} W(\overline{F}). \end{aligned} \tag{43}$$

Here G_K acts on (φ, Γ_K)-modules through Γ_K.

Proof. Theorem 3.6 provide us with the canonial and functorial isomorphisms (43), which are compatible with the action of φ and G_{K_∞}. From construction, it follows that they are compatible with the action of the whole Galois group G_K on the both sides. This implies that the functors $\mathbf{D}_{O_{\mathscr{F}}}$ and $\mathbf{V}_{O_{\mathscr{F}}}$ are quasi-inverse to each other, and the theorem is proved. □

Remark 4.4. *We invite the reader to formulate and prove the analogous statements for the categories* $\mathbf{Rep}_{\mathbf{F}_p}(G_K)$ *and* $\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$.

5. Admissible representations

5.1. General approach. The classification of all p-adic representations of local fields of characteristic 0 in terms of (φ,Γ_K)-modules is a powerful result. However, the representations arising in algebraic geometry have very special properties and form some natural subcategories of $\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$. Moreover, as was first observed by Grothendieck, it should be possible to classify them in terms of some objects of semi-linear algebra (φ-modules with filtration). We consider Fontaine's general approach to this problem.

In this section, K is a local field. As usual, we denote by $\overline{K}$ its separable closure and set $G_K = \mathrm{Gal}(\overline{K}/K)$. To simplify notation, in the remainder of this paper we will write $\mathbf{C}$ instead of $\mathbf{C}_K$ for the p-adic completion of $\overline{K}$. Since the field of complex numbers will appear only occasionally, this convention should not lead to confusion.

Let B be a commutative $\mathbf{Q}_p$-algebra without zero divisors, equipped with a $\mathbf{Q}_p$-linear action of G_K. Let C denote the field of fractions of B. Set $E = B^{G_K}$. We adopt the following definition of a regular algebra (provided by Brinon and Conrad in [**4**], which differs from the original definition in [**13**].

Definition. *The algebra B is G_K-regular if it satisfies the following conditions:*
i) $B^{G_K} = C^{G_K}$;
ii) Each non-zero $b \in B$ such that the line $\mathbf{Q}_p b$, is stable under the action of G_K, is invertible in B.

If B is a field, these conditions are satisfied automatically.

5.2. In the remainder of this section, we assume that B is G_K-regular. From the condition ii), it follows that E is a field. For any p-adic representation V of G_K we consider the E-module

$$\mathbf{D}_B(V) = (V \otimes_{\mathbf{Q}_p} B)^{G_K}.$$

The multiplication in B induces a natural map

$$\alpha_B : \mathbf{D}_B(V) \otimes_E B \to V \otimes_{\mathbf{Q}_p} B.$$

Proposition 5.3. *i) The map α_B is injective for all $V \in \mathbf{Rep}_{\mathbf{Q}_p}(G_K)$.*
ii) $\dim_E \mathbf{D}(V) \leqslant \dim_{\mathbf{Q}_p} V$.

PROOF. See [**4**, Theorem 5.2.1]. Set $\mathbf{D}_C(V) = (V \otimes_{\mathbf{Q}_p} C)^{G_K}$. Since $B^{G_K} = C^{G_K}$, $\mathbf{D}_C(V)$ is an E-vector space, and we have the following diagram with injective vertical maps:

$$\begin{array}{ccc} \mathbf{D}_B(V) & \xrightarrow{\alpha_B} & V \otimes_{\mathbf{Q}_p} B \\ \downarrow & & \downarrow \\ \mathbf{D}_C(V) & \xrightarrow{\alpha_C} & V \otimes_{\mathbf{Q}_p} B. \end{array}$$

Therefore it is sufficient to prove that α_C is injective. We prove it applying Artin's trick. Assume that $\ker(\alpha_C) \neq 0$ and choose a non-zero element

$$x = \sum_{i=1}^{m} d_i \otimes c_i \in \ker(\alpha_C)$$

of the shortest length m. It is clear that in this formula, $d_i \in \mathbf{D}_C(V)$ are linearly independent. Moreover, since C is a field, one can assume that $c_m = 1$. Then for all $g \in G_K$

$$g(x) - x = \sum_{i=1}^{m-1} d_i \otimes (g(c_i) - c_i) \in \ker(\alpha_C).$$

This shows that $g(x) = x$ for all $g \in G_K$, and therefore that $c_i \in C^{G_K} = E$ for all $1 \leqslant i \leqslant m$. Thus $x \in \mathbf{D}_C(V)$. From the definition of α_C, it follows that $\alpha_C(x) = x$, hence $x = 0$. □

DEFINITION. *A p-adic representation V is called B-admissible if*

$$\dim_E \mathbf{D}_B(V) = \dim_{\mathbf{Q}_p} V.$$

PROPOSITION 5.4. *If V is admissible, then the map α_B is an isomorphism.*

PROOF. See [**13**, Proposition 1.4.2]. Let $v = \{v_i\}_{i=1}^n$ and $d = \{d_i\}_{i=1}^n$ be arbitrary bases of V and $\mathbf{D}_B(V)$ respectively. Then $v = Ad$ for some matrix A with coefficients in B. The bases $x = \bigwedge_{i=1}^n d_i \in \bigwedge^n \mathbf{D}_B(V)$ and $y = \bigwedge_{i=1}^n v_i \in \bigwedge^n V$ are related by $x = \det(A)y$. Since G_K acts on $y \in \bigwedge^n V$ as multiplication by a character, the $\mathbf{Q}_p$-vector space generated by $\det(A)$ is stable under the action of G_K. This shows that A is invertible, and α_B is an isomorphism. □

5.4.1. We denote by $\mathbf{Rep}_B(G_K)$ the category of B-admissible representations. The following proposition summarizes some properties of this category.

PROPOSITION 5.5. *The following holds true:*
i) If in an exact sequence

$$0 \to V' \to V \to V'' \to 0$$

V is B-admissible, then V' and V'' are B-admissible.
ii) If V' and V'' are B admissible, then $V' \otimes_{\mathbf{Q}_p} V''$ and $\underline{\mathrm{Hom}}(V', V'') = \mathrm{Hom}_{\mathbf{Q}_p}(V', V'')$ *are B-admissible.*
iii) V is B-admissible if and only if the dual representation V^* is B-admissible, and in that case $\mathbf{D}_B(V^*) = \mathbf{D}_B(V)^*$.

iv) The functor

$$\mathbf{D}_B : \mathbf{Rep}_B(G_K) \to \mathbf{Vect}_E$$

to the category of finite dimensional E-vector spaces, is exact and faithful.

Proof. The proof is formal. See [**13**, Proposition 1.5.2]. □

5.5.1. We can also work with the contravariant version of the functor $\mathbf{D}_B$:

$$\mathbf{D}_B^*(V) = \mathrm{Hom}_{G_K}(V, B).$$

From definitions, it is clear that

$$\mathbf{D}_B^*(V) = \mathbf{D}_B(V^*).$$

In particular, if V (and therefore V^*) is admissible, then

$$\mathbf{D}_B^*(V) = \mathbf{D}_B(V)^* := \mathrm{Hom}_E(\mathbf{D}_B(V), E).$$

The last isomorphism shows that the covariant and contravariant theories are equivalent. For an admissible V, we have the canonical non-degenerate pairing

$$\langle\, ,\, \rangle : V \times \mathbf{D}^*(V) \to B, \qquad \langle v, f\rangle = f(v),$$

which can be seen as an abstract p-adic version of the canonical duality between singular homology and de Rham cohomology of a complex variety.

5.6. Examples.

5.6.1. *$B = \overline{K}$, where K is of characteristic* 0. One has $B^{G_K} = K$. The following proposition describes $\overline{K}$-admissible representations.

Proposition 5.7. *$\rho : G_K \to \mathrm{Aut}_{\mathbf{Q}_p} V$ is $\overline{K}$-admissible if and only if $\mathrm{Im}(\rho)$ is finite.*

Proof. a) Assume that $\mathrm{Im}(\rho)$ is finite. The group G_K acts semi-linearly on $\overline{K} \otimes_{\mathbf{Q}_p} V$:

$$g(a \otimes v) = g(a) \otimes g(v), \qquad g \in G_K.$$

Since $\mathrm{Im}(\rho)$ is finite, for each $x \in \overline{K} \otimes_{\mathbf{Q}_p} V$ there exists a subgroup $H \subset G_K$ of finite index such that H acts trivially on x. This implies that G_K acts on $\overline{K} \otimes_{\mathbf{Q}_p} V$ continuously (here $\overline{K} \otimes_{\mathbf{Q}_p} V$ is equipped with the *discrete* topology !). By Hilbert's theorem 90 (Theorem 3.5), one has:

$$\dim_K \mathbf{D}_B(V) := \dim_K (\overline{K} \otimes_{\mathbf{Q}_p} V)^{G_K} = \dim_{\mathbf{Q}_p} V.$$

Therefore V is $\overline{K}$-admissible.

b) Assume that V is $\overline{K}$-admissible. Fix a basis $\{v_j\}_{j=1}^n$ of V and a basis $\{d_i\}_{i=1}^n$ of $\mathbf{D}_B(V) = (\overline{K} \otimes_{\mathbf{Q}_p} V)^{G_K}$. Then:

$$d_i = \sum_{j=1}^n a_{ij} \otimes v_j, \qquad a_{ij} \in \overline{K}, \quad 1 \leqslant i \leqslant n.$$

There exists a finite extension L/K such that G_L acts trivially on all a_{ij}. Since G_L acts trivially on $\{d_i\}_{i=1}^n$, and $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ is invertible, G_L acts trivially on $\{v_j\}_{j=1}^n$. Therefore G_L acts trivially on V, and $\mathrm{Im}(\rho)$ is finite. □

5.7.1. *$B = \mathbf{C}_K$, where K is of characteristic* 0. One has $\mathbf{C}_K^{G_K} = K$ by Theorem 4.5.

THEOREM 5.8 (Sen). *ρ is $\mathbf{C}_K$-admissible if and only if $\rho(I_K)$ is finite.*

Exercise 16. Prove that if $\rho(I_K)$ is finite, then ρ is $\mathbf{C}_K$-admissible. Hint: use Hilbert's theorem 90.

The converse statement is difficult. See [**27**].

5.8.1. Take $V = \mathbf{Q}_p(1)$. Then

$$\mathbf{D}_{\mathbf{C}_K}(\mathbf{Q}_p(1)) = (\mathbf{C}_K \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(1))^{G_K} = (\mathbf{C}_K(\chi_K))^{G_K} = 0$$

by Theorem 4.5. Therefore $\mathbf{Q}_p(1)$ is not $\mathbf{C}_K$-admissible.

6. Hodge–Tate representations

6.1. We maintain notation and conventions of Section 5.1. The notion of a Hodge–Tate representation was introduced in Tate's paper [**30**]. We use the formalism of admissible representations. Let K be a local field of characteristic 0. Let

$$\mathbf{B}_{\mathrm{HT}} = \mathbf{C}_K[t, t^{-1}]$$

denote the ring of polynomials in the variable t with integer exponents and coefficients in $\mathbf{C}_K$. We equip $\mathbf{B}_{\mathrm{HT}}$ with the action of G_K given by

$$g\left(\sum a_i t^i\right) = \sum g(a_i)\chi_K^i(g)\, t^i, \qquad g \in G_K,$$

where χ_K denotes the cyclotomic character. Therefore G_K acts naturally on $\mathbf{C}_K$, and t can be viewed as the "p-adic $2\pi i$" – the p-adic period of the multiplicative group $\mathbb{G}_m$. For any p-adic representation V of G_K, we set:

$$\mathbf{D}_{\mathrm{HT}}(V) = (V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{HT}})^{G_K}.$$

PROPOSITION 6.2. *The ring $\mathbf{B}_{\mathrm{HT}}$ is G_K-regular and $\mathbf{B}_{\mathrm{HT}}^{G_K} = K$.*

PROOF. a) The field of fractions $\mathrm{Fr}(\mathbf{B}_{\mathrm{HT}})$ of $\mathbf{B}_{\mathrm{HT}}$ is isomorphic to the field of rational functions $\mathbf{C}_K(t)$. Embedding it in $\mathbf{C}_K((t))$, we have:

$$\mathbf{B}_{\mathrm{HT}}^{G_K} \subset \mathrm{Fr}(\mathbf{B}_{\mathrm{HT}})^{G_K} \subset \mathbf{C}_K((t))^{G_K}.$$

From Theorem 4.5, it follows that $(\mathbf{C}_K t^i)^{G_K} = K$ if $i = 0$, and $(\mathbf{C}_K t^i)^{G_K} = 0$ otherwise. Hence $\mathbf{B}_{\mathrm{HT}}^{G_K} = \mathbf{C}_K((t))^{G_K} = K$. Therefore

$$\mathrm{Fr}(\mathbf{B}_{\mathrm{HT}})^{G_K} = \mathbf{B}_{\mathrm{HT}}^{G_K} = K.$$

b) Let $b \in \mathbf{B}_{\mathrm{HT}} \setminus \{0\}$. Assume that $\mathbf{Q}_p b$ is stable under the action of G_K. This means that

$$g(b) = \eta(g)b, \qquad \forall g \in G_K \tag{44}$$

for some character $\eta : G_K \to \mathbf{Z}_p^*$. Write b in the form

$$b = \sum_i a_i t^i.$$

We will prove by contradiction that all, except one monomials in this sum are zero. From formula (44), if follows that for all i one has:

$$g(a_i)\chi_K^i(g) = a_i\eta(g), \qquad g \in G_K.$$

Assume that a_i and a_j are both non-zero for some $i \neq j$. Then

$$\frac{g(a_i)\chi_K^i(g)}{a_i} = \frac{g(a_j)\chi_K^j(g)}{a_j}, \qquad \forall g \in G_K.$$

Set $c = a_i/a_j$ and $m = i - j \neq 0$. Then c is a non-zero element of $\mathbf{C}_K$ such that

$$g(c)\chi_K^m(g) = c, \qquad \forall g \in G_K.$$

This is in contradiction with the fact that $\mathbf{C}_K(\chi_K^m)^{G_K} = 0$ if $m \neq 0$.

Therefore $b = a_i t^i$ for some $i \in \mathbf{Z}$ and $a_i \neq 0$. This implies that b is invertible in $\mathbf{B}_{\mathrm{HT}}$. The proposition is proved. □

6.2.1. Let $\mathbf{Grad}_K$ denote the category of finite-dimensional graded K-vector spaces. The morphisms in this category are linear maps preserving the grading. We remark that $\mathbf{D}_{\mathrm{HT}}(V)$ has a natural structure of a graded K-vector space:

$$\mathbf{D}_{\mathrm{HT}}(V) = \bigoplus_{i\in\mathbf{Z}} \mathrm{gr}^i\mathbf{D}_{\mathrm{HT}}(V), \qquad \mathrm{gr}^i\mathbf{D}_{\mathrm{HT}}(V) = \left(V \otimes_{\mathbf{Q}_p} \mathbf{C}_K t^i\right)^{G_K}.$$

Therefore we have a functor

$$\mathbf{D}_{\mathrm{HT}} : \mathbf{Rep}_{\mathbf{Q}_p}(G_K) \to \mathbf{Grad}_K.$$

Note that this functor is clearly left exact but not right exact.

Definition. *A p-adic representation V is a Hodge–Tate representation if it is $\mathbf{B}_{\mathrm{HT}}$-admissible.*

We denote by $\mathbf{Rep}_{\mathrm{HT}}(G_K)$ the category of Hodge–Tate representations. From the general formalism of B-admissible representations, it follows that the restriction of $\mathbf{D}_{\mathrm{HT}}$ on $\mathbf{Rep}_{\mathrm{HT}}(G_K)$ is exact and faithful.

6.3. Set:

$$V^{(i)} = \{x \in V \otimes_{\mathbf{Q}_p} \mathbf{C}_K \mid g(x) = \chi_K(g)^i x, \quad \forall g \in G_K\}, \qquad i \in \mathbf{Z},$$

$$V\{i\} = V^{(i)} \otimes_K \mathbf{C}_K.$$

It is clear that

$$V^{(i)} \simeq \mathrm{gr}^{-i}\mathbf{D}_{\mathrm{HT}}(V), \qquad x \leftrightarrow xt^{-i}$$

is an isomorphism of K-vector spaces. Therefore

$$V^{(i)} \simeq \mathrm{gr}^{-i}\mathbf{D}_{\mathrm{HT}}(V) \otimes_K Kt^i, \qquad x \leftrightarrow (xt^{-i}) \otimes t^i$$

is an isomorphism of G_K-modules (G_K acts on the both sides as the multiplication by χ_K^i). Set:

$$V\{i\} := V^{(i)} \otimes_K \mathbf{C}_K.$$

From the above isomorphism, it follows that

$$V\{i\} \simeq \mathrm{gr}^{-i}\mathbf{D}_{\mathrm{HT}}(V) \otimes_K \mathbf{C}_K t^i, \qquad i \in \mathbf{Z}.$$

Set:

$$\mathrm{gr}^0\left(\mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{B}_{\mathrm{HT}}\right)=\bigoplus_{i\in\mathbf{Z}}\left(\mathrm{gr}^{-i}\mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{C}_K t^i\right)\subset \mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{B}_{\mathrm{HT}}.$$

We have a commutative diagram

$$\begin{tikzcd}
\bigoplus_{i\in\mathbf{Z}} V\{i\} \arrow[r] \arrow[d, "\simeq"] & V\otimes_{\mathbf{Q}_p}\mathbf{C}_K \arrow[d, "="] \\
\mathrm{gr}^0\left(\mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{B}_{\mathrm{HT}}\right) \arrow[r] \arrow[d, hook] & V\otimes_{\mathbf{Q}_p}\mathbf{C}_K \arrow[d, hook] \\
\mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{B}_{\mathrm{HT}} \arrow[r, "\alpha_{\mathrm{HT}}"] & V\otimes_{\mathbf{Q}_p}\mathbf{B}_{\mathrm{HT}}.
\end{tikzcd}$$

The upper map in this diagram

$$\bigoplus_{i\in\mathbf{Z}} V\{i\}\to V\otimes_{\mathbf{Q}_p}\mathbf{C}_K \tag{45}$$

is induced by the maps:

$$V\{i\}=V^{(i)}\otimes_K \mathbf{C}_K\to V\otimes_{\mathbf{Q}_p}\mathbf{C}_K,$$
$$\left(\sum_k v_k\otimes a_k\right)\otimes\lambda\mapsto \sum_k v_k\otimes a_k\lambda,$$

where $\sum_k v_k\otimes a_k\in V^{(i)}$, $\lambda\in\mathbf{C}_K$.

The following proposition shows that our definition of a Hodge–Tate representation coincides with Tate's original definition:

Proposition 6.4. *i) For any representation V, the map (45) is injective.*
ii) V is a Hodge–Tate if and only if (45) is an isomorphism.

Proof. i) By Proposition 5.3, for *any* p-adic representation V, the map

$$\alpha_{\mathrm{HT}}:\mathbf{D}_{\mathrm{HT}}(V)\otimes_K \mathbf{B}_{\mathrm{HT}}\to V\otimes_{\mathbf{Q}_p}\mathbf{B}_{\mathrm{HT}}$$

is injective. The restriction of α_{HT} on the homogeneous subspaces of degree 0 coincides with the map (45). Therefore (45) is injective.

ii) By Proposition 5.4, V is a Hodge–Tate if and only if α_{HT} is an isomorphism. We remark that α_{HT} is an isomorphism if and only if the map (45) is. Now ii) follows from the above diagram (exercise). This proves the proposition. □

Definition. *Let V be a Hodge–Tate representation. The isomorphism*

$$V\otimes_{\mathbf{Q}_p}\mathbf{C}_K\simeq\bigoplus_{i\in\mathbf{Z}} V\{i\}$$

is called the Hodge–Tate decomposition of V. If $V\{i\}\neq 0$, one says that the integer i is a Hodge–Tate weight of V, and that $d_i=\dim_{\mathbf{C}_K} V\{i\}$ is the multiplicity of i.

We will use the standard notation $\mathbf{C}_K(i) = \mathbf{C}_K(\chi_K^i)$ for the cyclotomic twists of $\mathbf{C}_K$. Then $V\{i\} = \mathbf{C}_K(i)^{d_i}$ as a Galois module. The Hodge–Tate decomposition of V can be written in the following form:

$$V \otimes_{\mathbf{Q}_p} \mathbf{C}_K = \underset{i \in \mathbf{Z}}{\oplus} \mathbf{C}_K(i)^{d_i}.$$

6.5. Example. If $\mathscr{F}$ is a (one-dimensional) formal group of height h, then $V(\mathscr{F})$ is a Hodge–Tate representation. Namely

$$V(\mathscr{F}) \otimes_{\mathbf{Q}_p} \mathbf{C}_K \simeq \mathbf{C}_K(1) \oplus \mathbf{C}_K^{h-1}.$$

The Hodge–Tate weights of $V(\mathscr{F})$ are 0 (of multiplicity $h-1$) and 1 (of multiplicity one). It was first proved by Tate [**30**].

7. De Rham representations

7.1. The field $\mathbf{B}_{\mathrm{dR}}$. In this section, we define Fontaine's field of p-adic periods $\mathbf{B}_{\mathrm{dR}}$. For proofs and more detail, we refer the reader to [**10**] and [**12**].

Let K be a local field of characteristic 0. Recall that the ring of integers of the tilt $\mathbf{C}_K^\flat$ of $\mathbf{C}_K$ was defined as the projective limit

$$O_{\mathbf{C}_K}^\flat = \varprojlim_{\varphi} O_{\mathbf{C}_K}/p\,O_{\mathbf{C}_K}, \qquad \varphi(x) = x^p$$

(see Section 2). By Propositions 2.1 and 2.2, $O_{\mathbf{C}_K}^\flat$ is a complete perfect valuation ring of characteristic p with residue field $\bar{k}_K$. The field $\mathbf{C}_K^\flat$ is a complete algebraically closed field of characteristic p.

7.1.1. We will denote by $\mathbf{A}_{\mathrm{inf}}$ the ring of Witt vectors

$$\mathbf{A}_{\mathrm{inf}}(\mathbf{C}_K) = W(O_{\mathbf{C}_K}^\flat).$$

Recall that $\mathbf{A}_{\mathrm{inf}}$ is equipped with the surjective ring homomorphism $\theta : \mathbf{A}_{\mathrm{inf}} \to O_{\mathbf{C}_K}$ (see Proposition 4.2, where it is denoted by θ_E). The kernel of θ is the principal ideal generated by any element $\xi = \sum_{n=0}^{\infty} [a_n] p^n \in \ker(\theta)$ such that a_1 is a unit in $O_{\mathbf{C}_K}^\flat$. Useful canonical choices are:

- $\xi = [\tilde{p}] - p$, where $\tilde{p} = (p^{1/p^n})_{n \geqslant 0}$;
- $\omega = \sum_{i=0}^{p-1} [\varepsilon]^{i/p}$, where $\varepsilon = (\zeta_{p^n})_{n \geqslant 0}$.

Let K_0 denote the maximal unramified subextension of K. Then $O_{K_0} = W(k_K) \subset \mathbf{A}_{\mathrm{inf}}$, and we set $\mathbf{A}_{\mathrm{inf},K} = \mathbf{A}_{\mathrm{inf}} \otimes_{O_{K_0}} K$. Then θ extends by linearity to a sujective homomorphism

$$\theta \otimes \mathrm{id}_K \ : \ \mathbf{A}_{\mathrm{inf}}(\mathbf{C}_K) \otimes_{O_{K_0}} K \to \mathbf{C}_K.$$

Again, the kernel $J_K := \ker(\theta \otimes \mathrm{id}_K)$ is a principal ideal. It is generated, for example, by $[\tilde{\pi}_K] - \pi_K$, where π_K is any uniformizer of K and $\tilde{\pi}_K = (\pi_K^{1/p^n})_{n \geqslant 0}$. The action of G_K extends naturally to $\mathbf{A}_{\mathrm{inf},K}$, and it's easy to see that J_K is stable under this action. Let $\mathbf{B}_{\mathrm{dR},K}^+$ denote the completion of $\mathbf{A}_{\mathrm{inf},K}$ for the J_K-adic topology:

$$\mathbf{B}_{\mathrm{dR},K}^+ = \varprojlim_{n} \mathbf{A}_{\mathrm{inf},K}/J_K^n.$$

The action of G_K extends to $\mathbf{B}^+_{\mathrm{dR},K}$. The main properties of $\mathbf{B}^+_{\mathrm{dR},K}$ are summarized in the following proposition:

Proposition 7.2. *i)* $\mathbf{B}^+_{\mathrm{dR},K}$ *is a discrete valuation ring with maximal ideal*

$$\mathfrak{m}_{\mathrm{dR},K} = J_K\mathbf{B}^+_{\mathrm{dR},K}.$$

The residue field $\mathbf{B}^+_{\mathrm{dR},K}/\mathfrak{m}_{\mathrm{dR},K}$ *is isomorphic to* $\mathbf{C}_K$ *as a Galois module.*

ii) The series

$$t = \log([\varepsilon]) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{([\varepsilon]-1)^n}{n}$$

converges in the J_K*-adic topology to a uniformizer of* $\mathbf{B}^+_{\mathrm{dR},K}$*, and the Galois group acts on* t *as follows:*

$$g(t) = \chi_K(g)t, \qquad g \in G_K.$$

iii) If L/K *is a finite extension, then the natural map* $\mathbf{B}^+_{\mathrm{dR},K} \to \mathbf{B}^+_{\mathrm{dR},L}$ *is an isomorphism. In particular,* $\mathbf{B}^+_{\mathrm{dR},K}$ *depends only on the algebraic closure* $\overline{K}$ *of* K*.*

iv) There exists a natural G_K*-equivariant embedding of* $\overline{K}$ *in* $\mathbf{B}^+_{\mathrm{dR},K}$*, and*

$$\left(\mathbf{B}^+_{\mathrm{dR},K}\right)^{G_K} = K.$$

7.2.1. We refer the reader to [**10**] and [**12**] for detailed proofs of these properties. Note that if L is a finite extension of K, then one checks first that $\mathbf{B}^+_{\mathrm{dR},K} \subset \mathbf{B}^+_{\mathrm{dR},L}$. From assertions i) and ii), it follows that this is an unramified extension of discrete valuation rings with the same residue field. This implies that $\mathbf{B}^+_{\mathrm{dR},K} = \mathbf{B}^+_{\mathrm{dR},L}$. Since $L \subset \mathbf{B}^+_{\mathrm{dR},L}$ for all L/K, this proves that $\overline{K} \subset \mathbf{B}^+_{\mathrm{dR},K}$.

7.2.2. The above proposition shows that $\mathbf{B}^+_{\mathrm{dR},K}$ depends only on the residual characteristic of the local field K. By this reason, we will omit K from notation and write $\mathbf{B}^+_{\mathrm{dR}} := \mathbf{B}^+_{\mathrm{dR},K}$.

Definition. *The field of* p*-adic periods* $\mathbf{B}_{\mathrm{dR}}$ *is defined to be the field of fractions of* $\mathbf{B}^+_{\mathrm{dR}}$*.*

7.2.3. The field $\mathbf{B}_{\mathrm{dR}}$ is equipped with the canonical filtration induced by the discrete valuation, namely

$$\mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}} = t^i\mathbf{B}^+_{\mathrm{dR}}, \qquad i \in \mathbf{Z}.$$

In particular, $\mathrm{Fil}^0\mathbf{B}_{\mathrm{dR}} = \mathbf{B}^+_{\mathrm{dR}}$ and $\mathrm{Fil}^1\mathbf{B}_{\mathrm{dR}} = \mathfrak{m}_{\mathrm{dR}}$. From Proposition 7.2, it follows that

$$\mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}}/\mathrm{Fil}^{i+1}\mathbf{B}_{\mathrm{dR}} \simeq \mathbf{C}_K(i), \qquad \mathbf{C}_K(i) := \mathbf{C}_K(\chi_K^i).$$

Therefore for the associated graded module we have

$$\mathrm{gr}^\bullet(\mathbf{B}_{\mathrm{dR}}) \simeq \mathbf{B}_{\mathrm{HT}}.$$

Note that from this isomorphism it follows that $\mathbf{B}_{\mathrm{dR}}^{G_K} = K$ as claimed in Proposition 7.2, iii).

7.3. Filtered vector spaces.

DEFINITION. *A filtered vector space over K is a finite dimensional K-vector space Δ equipped with an exhaustive separated decreasing filtration by K-subspaces $(\mathrm{Fil}^i\Delta)_{i\in\mathbf{Z}}$:*

$$\ldots \supset \mathrm{Fil}^{i-1}\Delta \supset F^i\Delta \supset F^{i+1}\Delta \supset \ldots, \qquad \bigcap_{i\in\mathbf{Z}} \mathrm{Fil}^i\Delta = \{0\}, \quad \bigcup_{i\in\mathbf{Z}} \mathrm{Fil}^i\Delta = \Delta.$$

A morphism of filtered spaces is a linear map $f : \Delta' \to \Delta''$ which is compatible with filtrations:

$$f(\mathrm{Fil}^i\Delta') \subset \mathrm{Fil}^i\Delta'', \qquad \forall i \in \mathbf{Z}.$$

If Δ' and Δ'' are two filtered spaces, one defines the filtered space $\Delta' \otimes_K \Delta''$ as the tensor product of Δ' and Δ'' equipped with the filtration

$$\mathrm{Fil}^i(\Delta' \otimes_K \Delta'') = \sum_{i'+i''=i} \mathrm{Fil}^{i'}\Delta' \otimes_K \mathrm{Fil}^{i''}\Delta''.$$

The one-dimensional vector space $\mathbf{1}_K = K$ with the filtration

$$\mathrm{Fil}^i\mathbf{1}_K = \begin{cases} K & \text{if } i \leqslant 0 \\ 0 & \text{if } i > 0 \end{cases}$$

is a unit object with respect to the tensor product defined above, namely

$$\Delta \otimes_K \mathbf{1}_K \simeq \Delta \qquad \text{for any filtered module } \Delta.$$

One defines the internal Hom in the category of filtered vector spaces as the vector space $\underline{\mathrm{Hom}}_K(\Delta', \Delta'')$ of K-linear maps $f : \Delta' \to \Delta''$ equipped with the filtration

$$\mathrm{Fil}^i\left(\underline{\mathrm{Hom}}_K(\Delta', \Delta'')\right) = \{f \in \underline{\mathrm{Hom}}_K(\Delta', \Delta'') \mid f(\mathrm{Fil}^j\Delta') \subset \mathrm{Fil}^{j+i}(\Delta'') \quad \forall j \in \mathbf{Z}\}.$$

In particular, we consider the dual space $\Delta^* = \underline{\mathrm{Hom}}_K(\Delta, \mathbf{1}_K)$ as a filtered vector space.

We denote by $\mathbf{MF}_K$ the category of filtered K-vector spaces. It is easy to check that the category $\mathbf{MF}_K$ is an additive tensor category with kernels and cokernels, but it is not abelian.

7.4. De Rham representations. Since $\mathbf{B}_{\mathrm{dR}}$ is a field, it is G_K-regular. To any p-adic representation V of G_K we associate the finite-dimensional K-vector space

$$\mathbf{D}_{\mathrm{dR}}(V) = (V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{dR}})^{G_K}.$$

We equip it with the filtration induced from $\mathbf{B}_{\mathrm{dR}}$:

$$\mathrm{Fil}^i\mathbf{D}_{\mathrm{dR}}(V) = (V \otimes_{\mathbf{Q}_p} \mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}})^{G_K}.$$

The mapping which assigns $\mathbf{D}_{\mathrm{dR}}(V)$ to each V defines a functor of tensor categories

$$\mathbf{D}_{\mathrm{dR}} : \mathbf{Rep}_{\mathbf{Q}_p}(G_K) \to \mathbf{MF}_K.$$

DEFINITION. *A p-adic representation V is called de Rham if it is $\mathbf{B}_{\mathrm{dR}}$-admissible, i.e. if*

$$\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \dim_{\mathbf{Q}_p}(V).$$

We denote by $\mathbf{Rep}_{\mathrm{dR}}(G_K)$ the category of de Rham representations. By Proposition 5.5, the restriction of $\mathbf{D}_{\mathrm{dR}}$ on $\mathbf{Rep}_{\mathrm{dR}}(G_K)$ is exact and faithful.

PROPOSITION 7.5. *Each de Rham representation is Hodge–Tate.*

PROOF. Recall that we have exact sequences

$$0 \to \mathrm{Fil}^{i+1}\mathbf{B}_{\mathrm{dR}} \to \mathrm{Fil}^{i}\mathbf{B}_{\mathrm{dR}} \to \mathbf{C}_K t^i \to 0.$$

Tensoring with V and taking Galois invariants we have

$$\dim_K\left(\mathrm{gr}^i\mathbf{D}_{\mathrm{dR}}(V)\right) \leqslant \dim_K(V \otimes_{\mathbf{Q}_p} \mathbf{C}_K t^i).$$

From $\mathbf{B}_{\mathrm{HT}} = \bigoplus_{i\in\mathbf{Z}} \mathbf{C}_K t^i$ it follows that

$$\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \sum_{\imath\in\mathbb{Z}} \dim_K\left(\mathrm{gr}^i\mathbf{D}_{\mathrm{dR}}(V)\right) \leqslant \dim_K \mathbf{D}_{\mathrm{HT}}(V) \leqslant \dim_{\mathbf{Q}_p}(V).$$

The proposition is proved. □

REMARK 7.6. *1) The functor $\mathbf{D}_{\mathrm{dR}}$ is not fully faithful. A p-adic representation cannot be recovered from its filtered module.*

Recall that $\mathbf{A}_{\mathrm{inf}}$ is equipped with the canonical Frobenius operator φ. One has:

$$\varphi(\xi) = [\widetilde{p}]^p - p, \qquad \theta(\xi) = p^p - p \neq 0.$$

From this formula it follows that $\ker(\theta)$ is not stable under the action of φ, and therefore φ can not be naturally extended to $\mathbf{B}_{\mathrm{dR}}$.

8. Crystalline representations

8.0.1. We define the ring $\mathbf{B}_{\mathrm{cris}}$ of crystalline p-adic periods, which is a subring of $\mathbf{B}_{\mathrm{dR}}$ equipped with a natural Frobenius structure. Set:

$$\mathbf{A}^+_{\mathrm{cris}} = \left\{ \sum_{n=0}^{\infty} a_n \frac{\xi^n}{n!} \mid a_n \in \mathbf{A}_{\mathrm{inf}}, \quad \lim_{n\to+\infty} a_n = 0 \right\} \subset \mathbf{B}^+_{\mathrm{dR}}.$$

In this definition, $a_n \to 0$ in the *p-adic topology* of $\mathbf{A}_{\mathrm{inf}}$. From the formula

$$\frac{\xi^n}{n!}\frac{\xi^m}{m!} = \binom{n+m}{n}\frac{\xi^{n+m}}{(n+m)!}, \qquad \binom{n+m}{n} \in \mathbf{Z},$$

PROPOSITION 8.1. *i) $\mathbf{A}^+_{\mathrm{cris}}$ is stable under the action of G_K.*
ii) The action of φ on $\mathbf{A}_{\mathrm{inf}}$ extends to an injective map $\varphi : \mathbf{A}^+_{\mathrm{cris}} \to \mathbf{A}^+_{\mathrm{cris}}$.

PROOF. The verification of the both properties is straightforward, but we omit the details. □

The element $t = \log[\varepsilon]$ belongs to $\mathbf{A}^+_{\mathrm{cris}}$, and one has:

$$\varphi(t) = pt.$$

DEFINITION. *Set $\mathbf{B}^+_{\mathrm{cris}} = \mathbf{A}^+_{cris}[1/p]$ and $\mathbf{B}_{\mathrm{cris}} = \mathbf{B}^+_{\mathrm{cris}}[1/t]$. The ring $\mathbf{B}_{\mathrm{cris}}$ is called the ring of crystalline periods.*

It is easy to see that the rings $\mathbf{B}_{\mathrm{cris}}^{+}$ and $\mathbf{B}_{\mathrm{cris}}$ are stable under the action of G_K. The actions of G_K and φ on $\mathbf{B}_{\mathrm{cris}}$ commute to each other. The inclusion $\mathbf{B}_{\mathrm{cris}} \subset \mathbf{B}_{\mathrm{dR}}$ induces a filtration on $\mathbf{B}_{\mathrm{cris}}$ which we denote by $\mathrm{Fil}^i\mathbf{B}_{\mathrm{cris}}$. Note that $\mathbf{B}_{\mathrm{cris}}^{+} \subset \mathrm{Fil}^0\mathbf{B}_{\mathrm{cris}}$ but the latter space is much bigger. Also the action of φ on $\mathbf{B}_{\mathrm{cris}}$ is not compatible with filtration i.e. $\varphi(\mathrm{Fil}^i\mathbf{B}_{\mathrm{cris}}) \not\subset \mathrm{Fil}^i\mathbf{B}_{\mathrm{cris}}$. We summarize some properties of $\mathbf{B}_{\mathrm{cris}}$ in the following proposition.

Proposition 8.2. *The following holds true:*
i) The map

$$K \otimes_{K_0} \mathbf{B}_{\mathrm{cris}} \to \mathbf{B}_{\mathrm{dR}}, \qquad a \otimes x \to ax$$

is injective.
ii) $\mathbf{B}_{\mathrm{cris}}^{G_K} = K_0$.
iii) $\mathrm{Fil}^0\mathbf{B}_{\mathrm{cris}}^{\varphi=1} = \mathbf{Q}_p$.
iv) $\mathbf{B}_{\mathrm{cris}}$ *is* G_K*-regular.*

Proof. See [**12**], especially Theorems 4.2.4 and 5.3.7. □

8.3. Filtered φ-modules. Let K be a local field of characteristic 0 with residue field k of characteristic p, and let K_0 denote the maximal unramified subfield of K. A φ-module over K_0 is a finite-dimensional K_0-vector space D equipped with a φ-semininear bijective operator $\varphi : D \to D$:

$$\varphi(x+y) = \varphi(x) + \varphi(y), \qquad \forall x, y \in D,$$
$$\varphi(\lambda x) = \varphi(\lambda)\varphi(x), \qquad \forall \lambda \in K_0, x \in D.$$

Definition. *i) A filtered φ-module over K is a φ-module D over K_0 together with a structure of filtered K-vector space on $D_K := D \otimes_{K_0} K$.*

A morphism of filtered φ-modules is a K_0-linear map $f : D' \to D''$ such that the induced linear map

$$f_K : D'_K := D' \otimes_{K_0} K \to D''_K := D'' \otimes_{K_0} K,$$
$$f_K(d' \otimes \lambda) = f(d') \otimes \lambda, \qquad \forall d' \in D', \quad \lambda \in K$$

is a morphism of filtered modules, namely $f_K(\mathrm{Fil}^i D'_K) \subset \mathrm{Fil}^i D''_K$ for all $i \in \mathbf{Z}$.

Filtered φ-modules form an additive tensor category which we denote by $\mathbf{MF}_K^{\varphi}$. Note that this category is not abelian.

8.4. Crystalline representations.

8.4.1. Recall that $\mathbf{B}_{\mathrm{cris}}$ is G_K-regular with $\mathbf{B}_{\mathrm{cris}}^{G_K} = K_0$. Therefore for each p-adic representation V, the K_0-vector space

$$\mathbf{D}_{\mathrm{cris}}(V) = (V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{cris}})^{G_K}$$

is finite-dimensional with $\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) \leqslant \dim_{\mathbf{Q}_p}(V)$. The action on φ on $\mathbf{B}_{\mathrm{cris}}$ induces a semi-linear operator on $\mathbf{D}_{\mathrm{cris}}(V)$, which we denote again by φ. Since φ is injective on $\mathbf{B}_{\mathrm{cris}}$, it is bijective on the finite-dimensional vector space $\mathbf{D}_{\mathrm{cris}}(V)$. The embedding $K \otimes_{K_0} \mathbf{B}_{\mathrm{cris}} \hookrightarrow \mathbf{B}_{\mathrm{dR}}$ induces an inclusion

$$K \otimes_{K_0} \mathbf{D}_{\mathrm{cris}}(V) \hookrightarrow \mathbf{D}_{\mathrm{dR}}(V).$$

This equips $\mathbf{D}_{\mathrm{cris}}(V)_K := K \otimes_{K_0} \mathbf{D}_{\mathrm{cris}}(V)$ with the induced filtration:

$$\mathrm{Fil}^i \mathbf{D}_{\mathrm{cris}}(V)_K = \mathbf{D}_{\mathrm{cris}}(V)_K \cap \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V).$$

Thereore $\mathbf{D}_{\mathrm{cris}}$ can be viewed as a functor

$$\mathbf{D}_{\mathrm{cris}} : \mathbf{Rep}_{\mathbf{Q}_p}(G_K) \to \mathbf{MF}_K^{\varphi}.$$

Definition. *A p-adic representation V is crystalline if it is $\mathbf{B}_{\mathrm{cris}}$-admissible, i.e. if*

$$\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) = \dim_{\mathbf{Q}_p} V.$$

By Proposition 5.4, V is crystalline if and only if the map

$$\alpha_{\mathrm{cris}} : \mathbf{D}_{\mathrm{cris}}(V) \otimes_{K_0} \mathbf{B}_{\mathrm{cris}} \to V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{cris}} \tag{46}$$

is an isomorphism. We denote by $\mathbf{Rep}_{\mathrm{cris}}(G_K)$ the category of crystalline representations.

8.4.2. **Example.** Let $V = \mathbf{Q}_p(m)$, $m \in \mathbf{Z}$. Let $v_m \in \mathbf{Q}_p(m)$ be a basis of $\mathbf{Q}_p(m)$. Then $g(v_m) = \chi_K^m(g) v_m$ for all $g \in \mathrm{Gal}_K$. Set $d_m = v_m \otimes t^{-m} \in V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{cris}}$. It is clear that d_m is G_K-invariant, and therefore $d_m \in \mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(m))$. Since $\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(m)) \leqslant \dim_{\mathbf{Q}_p} V = 1$, we obtain that $\mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(m))$ is the one-dimensional K_0-vector space generated by d_m. In particular, $\mathbf{Q}_p(m)$ is crystalline, and

$$\mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(m)) = \mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(m))_K = K d_m.$$

The action of φ on $\mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(m))$ is given by

$$\varphi(d_m) = v_m \otimes \varphi(t)^{-m} = p^{-m} d_m.$$

Moreover, since $t^{-m} \in \mathrm{Fil}^{-m} \mathbf{B}_{\mathrm{dR}}$, one has

$$\mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(m)) = \begin{cases} \mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(m)), & \text{if } i \leqslant -m, \\ 0, & \text{if } i > -m. \end{cases}$$

Proposition 8.5. *Let V be a crystalline representation. Then*

$$V \simeq \mathrm{Fil}^0 (\mathbf{D}_{\mathrm{cris}}(V) \otimes_{K_0} \mathbf{B}_{\mathrm{cris}})^{\varphi=1}.$$

In other words, one can recover V from $\mathbf{D}_{\mathrm{cris}}(V)$.

Proof. This follows from the formula

$$\mathrm{Fil}^0 (\mathbf{B}_{\mathrm{cris}})^{\varphi=1} = \mathbf{Q}_p.$$

Namely, assume that V is crystalline. Then using (46), we have

$$\mathrm{Fil}^0 (\mathbf{D}_{\mathrm{cris}}(V) \otimes_{K_0} \mathbf{B}_{\mathrm{cris}})^{\varphi=1} = \mathrm{Fil}^0 (V \otimes_{\mathbf{Q}_p} \mathbf{B}_{\mathrm{cris}})^{\varphi=1} = V.$$

□

We constructed subcategories

$$\mathbf{Rep}_{\mathrm{cris}}(G_K) \subset \mathbf{Rep}_{\mathrm{dR}}(G_K) \subset \mathbf{Rep}_{\mathrm{HT}}(G_K) \subset \mathbf{Rep}_{\mathbf{Q}_p}(G_K).$$

8.6. Example. Let $V(\mathscr{F})$ be the representation associated to to a formal group $\mathscr{F}$ of finite height. Then $V(\mathscr{F})$ is crystalline. This is a particular case of a theorem of Fontaine [**9**], [**10**].

Bibliography

[1] V.A. Abrashkin, *A local analogue of the Grothendieck conjecture*, Int. J. of Math. **11** (2000), pp. 3-43.

[2] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967, 349 pp.

[3] B. Bhatt, *Lecture notes for a class on perfectoid spaces* `http://www-personal.umich.edu/~bhattb/teaching/mat679w17/lectures.pdf`

[4] O. Brinon and B. Conrad, *CMI summer school notes on p-adic Hodge theory*, `http://math.stanford.edu/~conrad/papers/notes.pdf`

[5] J.W. C. Cassels and A. Fröhlich (eds) *Algebraic Number Theory*, Thompson Book Company, 1967, 366 pages.

[6] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), pp. 129-174.

[7] L. Fargues, J.-M. Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, Astérisque **406** (2018), 382 pages.

[8] I. Fesenko, *On deeply ramified extensions*, J. London Math. Soc. **57** (1998), 325-335.

[9] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque **47-48** (1977), 264 pages.

[10] J.-M. Fontaine, *Sur certaines types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Ann. of Math. **115** (1982), 529-577.

[11] J.-M. Fontaine, *Représentations p-adiques des corps locaux*, in: "The Grothendieck Festschrift" (P. Cartier, L. Illusie, N. M. Katz, G. Laumon Y.I. Manin, K. A. Ribet eds.), vol. II, Progress in Math. **87**, Birkhäuser, Boston 1991, pp. 249-309.

[12] J.-M. Fontaine, *Le corps des périodes p-adiques*, Astérisque **223** (1994), pp. 59-102.

[13] J.-M. Fontaine, *Représentations p-adiques semistables*, Astérisque **223** (1994), pp. 113-184.

[14] O. Gabber and L. Ramero, *Almost Ring Theory*, Lecture Notes in Math. **1800** (2003), 307 pages.

[15] J. Fresnel and M. Matignon, *Produit tensoriel topologique de corps valués*, Can. J. Math., **35**, no. 2, (1983), pp. 218-273.

[16] A. Fröhlich, *Formal groups*, Lecture Notes in Math. **74**, 1968, 140 pages.

[17] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213-246.

[18] U.Jannsen, K.Wingberg, *Die Struktur der absoluten Galoisgruppep-adischer Zahlkörper*, Invent. math. **70** (1982), pp. 71-98.

[19] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, 1986, 354 pp.

[20] S. Lang, *Introduction to Modular forms*, Grundlehren der mathematischen Wissenschaften **222**, 1976, 265 pages.

[21] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, 2002

[22] J. Milne, *Étale cohomology*, Princeton Univ. Press 1980, 344 pages.

[23] Sh. Mochizuki, *A version of the Grothendieck conjecture for p-adic local fields*, Int. Journal of Math. **8** (1997), pp. 499-506.

[24] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften Bd. **323**, Springer, 2013.

[25] P. Scholze, *Perfectoid spaces*, Publ. math. de l'IHÉS **116** (2012), no. 1, pp. 245-313.

[26] S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17** (1972), pp. 44-50.

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

[28] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968.

[29] J.-P. Serre and J. Tate, *Good Reduction of Abelian varieties*, Ann. of Math. **88** (1968), pp. 492-517.

[30] J. Tate, *p-divisible groups*, in Proc. Conf. Local Fields, Driebergen, 1966, Springer T.A. ed., Springer, 1967, pp. 158-183.

[31] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. Sc. ENS **16** (1983), pp.59-89.

[32] A. V. Yakovlev, *The Galois group of the algebraic closure of a local field*, Math. USSR Izv. 2 (1968), 1231-1269.