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-bordeaux1.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 [**1**, Ch. 2, Thm 7]. Another proof (valid only for locally compact fields) can be found in [**4**, 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. 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. □

We give an application of Krasner's lemma. Let $\overline{K}$ be an algebraic closure of K. By Theorem 1.2, the absolute value $|\cdot|_K$ extends in a unique way to an absolute value on $\overline{K}$, which we will again denote by $|\cdot|_K$. Let $\mathbf{C}_K$ denote the completion of $\overline{K}$ with respect to $|\cdot|_K$.

PROPOSITION 1.4. *Assume that K is a complete non-archimedean field of characteristic* 0. *Then the field $\mathbf{C}_K$ is algebraically closed.*

PROOF. Proof by contradiction. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in O_{\mathbf{C}_K}[X]$ be an irreducible monic polynomial of degree $\geqslant 2$, and let C denotes its splitting field. By Theorem 1.2, the absolute value $|\cdot|_K$ extends to C. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $f(X)$ in C. Set

$$d := \min_{1 \leqslant i \neq j \leqslant n} |\alpha_i - \alpha_j|_K > 0.$$

Choose a monic polynomial $g(X) := X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in \overline{K}[X]$ such that

$$|b_i - a_i|_K < d^n, \qquad \text{for all} \quad 0 \leqslant i \leqslant n-1.$$

Let $\beta \in \overline{K}$ be a root of $g(X)$. Since

$$f(X) - g(X) = \sum_{i=0}^{n-1} (a_i - b_i) X^i,$$

and $\beta \in O_{\overline{K}}$, we have:

$$|f(\beta)|_K = |f(\beta) - g(\beta)|_K \leqslant \max_{0 \leqslant i \leqslant n-1} |b_i - a_i|_K < d^n.$$

On the other hand, $f(\beta) = \prod_{i=1}^{n} (\beta - \alpha_i)$. Hence

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

Therefore, there exists i_0 such that $|\beta - \alpha_{i_0}|_K < d$. Taking into account the definition of d, we obtain that

$$|\beta - \alpha_{i_0}|_K < \min_{i \neq i_0} |\alpha_i - \alpha_{i_0}|_K$$

By Krasner's lemma, this implies that $\mathbf{C}_K(\alpha_{i_0}) \subset \mathbf{C}_K(\beta) = \mathbf{C}_K$. Therefore $\alpha_{i_0} \in \mathbf{C}_K$, and we conclude that $f(X)$ has a root in $\mathbf{C}_K$. This contradicts the irreductibility of $f(X)$. □

PROPOSITION 1.5 (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 [**13**, Chapter 2, §2]. □

1.6. 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.

Exercise 1. Let K be a field of characteristic p with algebraically closed residue field. Consider the polynomial $f(X) := X^p - X - c$. Show that if $c \in O_K$, then $f(X)$ splits in 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. $\square$

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, [**1**, 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 $[x+y] = [x] + [y]$. $\square$

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 2. 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

$$v_K(f(X)) = \mathrm{ord}_X f(X) := \min\{i \in \mathbf{Z} \mid a_i \neq 0\},$$

where $f(X) = \sum_{i \gg -\infty} a_i X^i$. *Note that* X *is a uniformizer of* K *and* $O_K \simeq k_K[[X]]$.

ii) If $\operatorname{char}(K) = 0$, *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*

$$\left| \frac{a}{b} p^k \right|_p = p^{-k}, \qquad p \not| a, b.$$

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

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

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

ii) Assume that $\operatorname{char}(K) = 0$. 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 $[K : \mathbf{Q}_p] < +\infty$.

$\square$

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. $\square$

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 [**12**]. 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

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

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.

$\square$

Exercise 3. 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 4. 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.

Exercise 5. (See[**13**, Chapter 2, Proposition 14]). Let K be a local field of characteristic 0. Show that for any $n\geqslant 1$ there exists only a finite number of extensions of K of degree n.

Exercise 6. Show that a local field of characteristic p has infinitely many separable extensions of degree p. This could be proved using Artin–Schreier extensions (see for example [**12**, Chapter VI,§6] for basic results of Artin–Schreier theory).

3. The different

3.1. The Dedekind different. In this subsection, A denotes a Dedekind ring with fraction field K. Let L/K be a finite separable extention and B the integral closure of A in L. We consider the map
$$t_{L/K}\,:\,L\times L\to K,$$
$$t_{L/K}(x,y)=\mathrm{Tr}_{L/K}(xy).$$

PROPOSITION 3.2. *$t_{L/K}$ is a non-degenerate symmetric K-bilinear form on L.*

PROOF. We have:
$$t_{L/K}(x_1+x_2,y)=\mathrm{Tr}_{L/K}((x_1+x_2)y)=\mathrm{Tr}_{L/K}(x_1y+x_2y)=$$
$$\mathrm{Tr}_{L/K}(x_1y)+\mathrm{Tr}_{L/K}(x_2y)=t_{L/K}(x_1,y)+t_{L/K}(x_2,y).$$
If $a\in K$, then for any $z\in L$ on has $\mathrm{Tr}_{L/K}(az)=a\mathrm{Tr}_{L/K}(z)$, and therefore
$$\langle ax,y\rangle=\mathrm{Tr}_{L/K}(axy)=a\mathrm{Tr}_{L/K}(xy)=a\langle x,y\rangle.$$
This shows that $t_{L/K}$ is a K-bilinear form. Moreover, it is clear that it is symmetric. From the general theory of field extensions, it is known that the separability of L/K implies that for any basis $\{\omega_i\}_{i=1}^n$ of L over K, the determinant $\det\big(t_{L/K}(\omega_i,\omega_j)_{1\leqslant i,j\leqslant n}\big)$ is non-zero. Therefore the form $t_{L/K}$ is non-degenarate.

$\square$

If $M \subseteq L$ is a finitely generated A-module, we define its complementary module M' as

$$M' = \{x \in L \,|\, t_{L/K}(x,y) \in A \text{ for all } y \in M\}.$$

It is easy to see that M' is an A-module and that $M \subseteq N$ implies $N' \subseteq M'$.

Let $\omega_1, \dots, \omega_n$ be a base of L/K and let $\omega_1', \dots, \omega_n'$ denote the dual base, i.e.

$$t_{L/K}(\omega_i, \omega_j') = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

If $M = A\omega_1 + \ldots + A\omega_n$, then $M' = A\omega_1' + \cdots + A\omega_n'$.

We study the complementary module B' of the Dedekind ring B. Note that, in general, B is not free over A.

PROPOSITION 3.3. *i) There exist free A-modules $M_1, M_2 \subset L$ such that*

$$M_1 \subseteq B \subseteq M_2.$$

ii) B' is a fractional ideal of B and $B \subset B'$.

iii) The inverse $(B')^{-1}$ of B' is an ideal of B.

PROOF. i) Let $\{\omega_i\}_{i=1}^n$ be a basis of L/K. There exists $a \in A$ such that $a\omega_1, \dots, a\omega_n$ are integral over A. Let M_1 denote the A-module generated by $a\omega_1, \dots, a\omega_n$. Then M_1 is A-free, and $M_1 \subseteq B$.

ii) By definition, B' is an A-module. If $x, y \in B$, then

$$t_{L/K}(x,y) = \mathrm{Tr}_{L/K}(xy) \in A.$$

Hence $B \subset B'$. To show that B' is a fractional ideal, we only should find $b \neq 0$ such that $bB' \subseteq B$. Let $x_1, \dots, x_n$ be a basis of M_2 over A. Then there exists $b \in B$ such that $bx_1, \dots, bx_n \in B$. Hence $bB' \subset bM_2 \in B$.

iii) By definition, the inverse $(B')^{-1}$ of B' is the fractional ideal defined by

$$(B')^{-1} = \{x \in L \,|\, xB' \subset B\}$$

Let $x \in (B')^{-1}$. Since $B \subseteq B'$, we have $x \in xB \subset xB' \subset B$. This proves that $(B')^{-1} \subset B$. □

DEFINITION. *The ideal $\mathfrak{D}_{B/A} := (B')^{-1}$ is called the different of B over A.*

THEOREM 3.4. *Let $K \subset L \subset M$ be a tower of separable extensions. Let B and C denote the integral closure of A in L and M respectively. Then*

$$\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}.$$

Here $\mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$ denotes the ideal of C generated by the products xy, $x \in \mathfrak{D}_{C/B}$, $y \in \mathfrak{D}_{B/A}$.

PROOF. We will prove the theorem in the equivalent form

$$\mathfrak{D}_{C/A}^{-1} = \mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1}.$$

First prove that

$$\mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1} \subset \mathfrak{D}_{C/A}^{-1}. \tag{2}$$

The ideal $\mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1}$ is generated by the products xy $x \in \mathfrak{D}_{C/B}^{-1}$, $y \in \mathfrak{D}_{B/A}^{-1}$. Let $z \in C$. Then $\mathrm{Tr}_{M/L}(xz) \in B$, and

$$\mathrm{Tr}_{M/K}((xy)z) = \mathrm{Tr}_{L/K}(y\mathrm{Tr}_{M/L}(xz)) \in A.$$

therefore $xy \in \mathfrak{D}_{C/A}^{-1}$, and the inclusion (2) is proved.

Now assume that $x \in \mathfrak{D}_{C/A}^{-1}$. Then for all $y \in C$ one has

$$\mathrm{Tr}_{M/K}(xy) \in A.$$

Since $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$, we obtain that for all $b \in B$

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(xy)b) = \mathrm{Tr}_{M/K}(x(yb)) \in A.$$

Hence, $\mathrm{Tr}_{M/L}(xy) \in \mathfrak{D}_{B/A}^{-1}$. This implies that for all $z \in \mathfrak{D}_{B/A}$ one has

$$\mathrm{Tr}_{M/L}((xz)y) = z\mathrm{Tr}_{M/L}(xy) \in B,$$

and we obtain that $xz \in \mathfrak{D}_{C/B}^{-1}$. Therefore we proved that

$$\mathfrak{D}_{C/A}^{-1}\mathfrak{D}_{B/A} \subset \mathfrak{D}_{C/B}^{-1},$$

i.e. that

$$\mathfrak{D}_{C/A}^{-1} \subset \mathfrak{D}_{B/A}^{-1}\mathfrak{D}_{C/B}^{-1}.$$

Together with (2), this gives the theorem. $\square$

Now we compute the different in the important case of simple extensions of Dedekind rings.

THEOREM 3.5. *Assume that $B = A[\alpha]$, where α is some element integral over A. Then $\mathfrak{D}_{B/A}$ coincides with the principal ideal generated by $f'(\alpha)$:*

$$\mathfrak{D}_{B/A} = (f'(\alpha)).$$

PROOF. Let $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in A[X]$ denote the minimal monic polynomial of α over K. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of B over A. In particular, B is free of rank n over A.

Let $\alpha_1, \ldots, \alpha_n$ denote the roots of $f(X)$ in some algebraic closure of K containing B. We claim that

$$\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)} = X^r \tag{3}$$

for all $r = 0, 1, \ldots, n-1$. To prove this formula, it is sufficient to remark that X^r and $\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}$ are both polynomials of degree $\leqslant n-1$ taking the same values at $\alpha_1, \ldots \alpha_n$. Namely,

$$\left.\left(\frac{f(X)}{X-\alpha_i}\right)\right|_{X=\alpha_j} = \begin{cases} 0, & \text{if } i \neq j, \\ f'(\alpha_j), & \text{if } i = j. \end{cases}$$

and therefore

$$\sum_{i=1}^{n} \left.\left(\frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}\right)\right|_{X=\alpha_j} = f'(\alpha_j) \cdot \frac{\alpha_j^r}{f'(\alpha_j)} = f'(\alpha_j).$$

Now we prove the theorem using formula (3).

For any polynomial $g(X) = c_0 + c_1X + \cdots + c_kX^k$ with coefficients in L, define:

$$\mathrm{Tr}_{L/K}(g(X)) = \sum_{i=1}^{k} \mathrm{Tr}_{L/K}(c_i)X^i.$$

Then formula (3) reads:

$$\mathrm{Tr}_{L/K}\left(\frac{f(X)}{X-\alpha}\frac{\alpha^r}{f'(\alpha)}\right) = X^r.$$

Set

$$\frac{f(X)}{X-\alpha} = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}.$$

From the Euclidean division, it follows that all $b_i \in B$. We have:

$$\mathrm{Tr}_{L/K}\left(\frac{b_i}{f'(\alpha)}\,\alpha^r\right) = \begin{cases} 0, & \text{if } i \neq r, \\ 1, & \text{if } i = r. \end{cases}$$

Therefore the elements $b_i/f'(\alpha)$, $0 \leqslant i \leqslant n-1$ form the dual basis of the basis $1, \alpha, \ldots, \alpha^{n-1}$. Hence

$$\mathfrak{D}_{B/A}^{-1} = \frac{1}{f'(\alpha)}\,(b_0A + b_1A + \cdots + b_{n-1}A).$$

To complete the proof, we only need to show that

$$b_0A + b_1A + \cdots + b_{n-1}A = A[\alpha]. \tag{4}$$

Since $b_i \in B$ the inclusion

$$b_0A + b_1A + \cdots + b_{n-1}A \subset B$$

is clear. On the other hand from the identity

$$f(X) = (b_0 + b_1X + \cdots + b_{n-1}X^{n-1})(X-\alpha)$$

we obtain, by induction that

$$\begin{aligned}
&b_{n-1} = 1 \quad \Rightarrow \quad A = b_{n-1}A\\
&b_{n-2} - \alpha = a_{n-1} \quad \Rightarrow \quad \alpha = b_{n-2} - a_{n-1} \in A + b_{n-2}A,\\
&b_{n-3} - \alpha b_{n-2} = a_{n-2} \quad \Rightarrow \quad \alpha^2 \in A + b_{n-2}A + b_{n-3}A,\\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

Therefore $A[\alpha] \subseteq b_0A + b_1A + \cdots + b_{n-1}A$, and (4) is proved. It implies that $\mathfrak{D}_{B/A}^{-1} = f'(\alpha)^{-1}B$, and we are done. $\square$

3.6. The case of local fields. Let L/K be a finite separable extension of local fields. In that case, $\mathfrak{D}_{L/K}$ is a principal ideal and therefore $\mathfrak{D}_{L/K} = \mathfrak{m}_L^s$ for some $s \geqslant 0$. Set

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

PROPOSITION 3.7. *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 is a particular case of Theorem 3.5. We prove ii-iv) (see also [**13**, 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 1.5 (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 ${}_pi_L$. 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 (**??**), 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). $\square$

Exercise 7. 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:

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

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

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

$\square$

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. $\square$

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

$$s_i\,:\, G_i/G_{i+1} \to U_L^{(i)}/U_L^{(i+1)}, \tag{5}$$

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

$$\delta_0\,:\, G_0/G_1 \to k^*, \qquad \delta_i\,:\, G_i/G_{i+1} \to k^+, \quad \textit{for all } i \geqslant 1. \tag{6}$$

PROOF. The proof is straightforward. See [**16**, Chapitre IV, Propositions 5-7]. $\square$

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

4.7. For our study of the ramification filtration, it is convenient to introduce the function

$$i_{L/K}\,:\, G \to \mathbf{Z} \cup \{+\infty\}, \qquad i_{L/K}(g) = \min\{g(x)-x \mid x \in O_L\}.$$

Below, we summarize basic properties of this function:

1) If $O_L = O_K[\alpha]$, then

$$i_{L/K}(g) = v_L(g(\alpha)-\alpha).$$

Note that for any finite extension of local fields L/K, there exists $\alpha \in L$ such that $O_L = O_K[\alpha]$ (see Exercise 7).

PROOF. We only need to show that for any $x \in O_L$,

$$v_L(g(x)-x) \geqslant v_L(g(\alpha)-\alpha).$$

Since $x = \sum\limits_{k=0}^{n-1} a_k\alpha^k$ for some $a_k \in O_K$, this follows from the computation

$$g(\alpha)-\alpha = \sum_{k=0}^{n-1} a_k g(\alpha^k) - \sum_{k=0}^{n-1} a_k\alpha^k = \sum_{k=1}^{n-1} a_k(g(\alpha)^k - \alpha^k)$$

and the identity

$$g(\alpha)^k - \alpha^k = (g(\alpha)-\alpha)\cdot\left(\sum_{j=0}^{k-1} g(\alpha)^{k-j-1}\alpha^k\right).$$

□

2) For all $g_1, g_2 \in G$,

$$i_{L/K}(g_1g_2) \geqslant \min\{i_{L/K}(g_1), i_{L/K}(g_2)\}.$$

PROOF. For any $x \in O_L$, one has

$$g_1g_2(x) - x = g_1(g_2(x)-x) + (g_1(x)-x).$$

Since $v_L(g(y)) = v_L(y)$ for any $y \in L$ and $g \in G$, we obtain that

$$\begin{aligned} v_L(g_1g_2(x)-x) \geqslant \min\{&v_L(g_1(g_2(x)-x)), v_L(g_1(x)-x)\} \\ &= \min\{v_L(g_2(x)-x), v_L(g_1(x)-x)\}, \end{aligned}$$

and we are done. □

3) For all $g_1, g_2 \in G$,

$$i_{L/K}(g_1^{-1}g_2g_1) = i_{L/K}(g_2).$$

PROOF. Let $O_L = O_K[\alpha]$. Since $g_1 : O_L \to O_L$ is a bijection, one has $O_L = O_K[g_1^{-1}(\alpha)]$ and $i_{L/K}(g) = v_L(gg_1^{-1}(\alpha) - g_1^{-1}(\alpha))$ for any $g \in G$. Hence

$$\begin{aligned} i_{L/K}(g_1^{-1}g_2g_1) &= v_L(g_1^{-1}g_2g_1(g_1^{-1}(\alpha) - g_1^{-1}(\alpha))) = v_L(g_1^{-1}g_2(\alpha) - g_1^{-1}(\alpha)) \\ &= v_L(g_1^{-1}(g_2(\alpha)-\alpha)) = v_L(g_2(\alpha)-\alpha) = i_{L/K}(g_2). \end{aligned}$$

□

4) For any $g \in G$,

$$i_{L/K}(g^{-1}) = i_{L/K}(g).$$

PROOF. This property follows immediately from the following computation:

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

□

5) $g \in G_i$ if and only if $i_{L/K}(g) \geqslant i+1$.

PROOF. This property is clear. □

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

PROPOSITION 4.9. *Let L/K be a finite Galois extension of local fields. Then*

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

PROOF. Let $O_L = O_K[\alpha]$ and let $f(X)$ be the minimal polynomial of α. Since

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

we have

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

$\square$

4.10. Our next goal is to understand the behavior of the ramification filtration in towers of local fields. We will consider a tower

$$\begin{tikzcd} L \arrow[d, dash, "H"] \arrow[dd, dash, bend right=60, "G"'] \\ F \arrow[d, dash] \\ K \end{tikzcd} \tag{7}$$

where $G := \mathrm{Gal}(L/K)$ and $H := \mathrm{Gal}(L/F)$. From the definition of the ramifiaction subgroups it follows immediately that

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

COROLLARY 4.11. *One has*

$$e(L/F)\, v_F(\mathfrak{D}_{F/K}) = \sum_{g\in G\setminus H} i_{L/K}(g).$$

PROOF. Write Proposition 4.9 for the extension L/F:

$$v_L(\mathfrak{D}_{L/F}) = \sum_{h\in H\setminus\{e\}} i_{L/F}(h)$$

Taking into account that $i_{L/F}(h) = i_{L/K}(h)$ and $G = (G\setminus H)\cup H$, we have

$$v_L(\mathfrak{D}_{L/K}) - v_L(\mathfrak{D}_{L/F}) = \sum_{g\in G\setminus H} i_{L/F}(g). \tag{8}$$

On the other hand, from Theorem 3.4, we have

$$v_L(\mathfrak{D}_{L/K}) = v_L(\mathfrak{D}_{L/F}) + v_L(\mathfrak{D}_{F/K}) = v_L(\mathfrak{D}_{L/F}) + e(L/F) v_F(\mathfrak{D}_{F/K}). \tag{9}$$

(Here we use the formula $v_L(x) = e(L/F)v_F(x)$ for $x \in F$.) Comparing formulas (8) and (9), we obtain the corollary. $\square$

From now one, we assume that F/K is a Galois extension. Note that in that case $\mathrm{Gal}(F/K) = G/H$. If $g \in G$ and $s \in G/H$, we will write $g \mapsto s$ if s is the image of g under the canonical projection $G \to G/H$.

PROPOSITION 4.12. *For all $s \in G/H$,*

$$e(L/F)i_{F/K}(s) = \sum_{g \mapsto s} i_{L/K}(g).$$

PROOF. If $s = e$, the both sides of the formula are equal to $+\infty$. Assume that $s \neq e$. Write $O_L = O_F[\alpha]$ and denote by $f(X) \in O_F[X]$ the minimal polynomial of α over F. Let $sf(X) \in O_F[X]$ denote the polynomial obtained acting s on the coefficients of $f(X)$ (so, s acts trivially on the variable X). Directly from the definition of $i_{F/K}$, one has

$$sf(X) - f(X) \equiv 0 \pmod{\mathfrak{m}_F^{i_{F/K}(s)}}.$$

Hence $(sf)(\alpha) \equiv 0 \pmod{\mathfrak{m}_F^{i_{F/K}(s)}}$. On the other hand, acting on the both sides of the formula $f(X) = \prod\limits_{h \in H}(X - h(\alpha))$ by any lift of s in G, we obtain

$$sf(X) = \prod_{g \mapsto s}(X - g(\alpha)).$$

Therefore, $(sf)(\alpha) = \prod\limits_{g \mapsto s}(\alpha - g(\alpha))$, and

$$\prod_{g \mapsto s}(\alpha - g(\alpha)) \equiv 0 \pmod{\mathfrak{m}_F^{i_{F/K}(s)}}.$$

Taking the valuations of the both sides, we obtain the inequality

$$\sum_{g \mapsto s} i_{L/K}(g) \geqslant e(L/F)i_{F/K}(s).$$

To show that this inequality is in fact equality, we take the sum over all $s \neq e$ and use Corollary 4.11:

$$e(L/F)\sum_{s \neq e} i_{F/K}(s) \geqslant \sum_{s \neq e}\sum_{g \mapsto s} i_{L/K}(g) = \sum_{g \in G \setminus H} i_{L/K}(g) = e(L/F)\sum_{s \neq e} i_{F/K}(s).$$

Therefore $e(L/F)i_{F/K}(s) = \sum\limits_{g \mapsto s} i_{L/K}(g)$ for all s, and the proposition is proved. $\square$

For any $s \in G/H$, define

$$j(s) := \max\{i_{L/K}(g) \mid g \mapsto s\}.$$

Then there exists $\tilde{g} \mapsto s$ such that $j(s) = i_{L/K}(\tilde{g})$. Then any g such that $g \mapsto s$ can be written in the form $g = \tilde{g}h$ for some $h \in H$. Hence

$$i_{L/K}(g) \geqslant \min\{i_{L/K}(\tilde{g}), i_{L/K}(h)\}.$$

On the other hand, writing $h = \tilde{g}^{-1}g$ we have

$$i_{L/K}(h) \geqslant \min\{i_{L/K}(\tilde{g}^{-1}), i_{L/K}(g)\} = \min\{i_{L/K}(\tilde{g}), i_{L/K}(g)\} = i_{L/K}(g).$$

Therefore

$$i_{L/K}(g)=\min\{i_{L/K}(\tilde g),i_{L/K}(h)\},$$

and we can write Proposition 4.12 in the following form:

COROLLARY 4.13. *For all $s\in G/H$,*

$$e(L/F)i_{F/K}(s)=\sum_{h\in H}\min\{j(s),i_{L/K}(h)\}.$$

4.14. Let L/K en a finite Galois extension of local fields. For any real $x\geqslant -1$ set $G_x:=G_m$, where m is the unique integer such that $m\leqslant x<m+1$. The Hasse–Herbrand function $varphi_{L/K}$ is defined as follows

$$\varphi_{L/K}(u)=\begin{cases} u & \text{if } -1\leqslant u\leqslant 0,\\ \displaystyle\int_0^u \frac{dx}{(G_0:G_x)}, \text{if } u\geqslant 0 \end{cases} \tag{10}$$

From definition it follows that $\varphi_{L/K}$ is a continuous strictly increasing piecewise linear function. More explicitly, if we set $g_m:=|G_m|$ for all integer $m\geqslant -1$, then

$$\varphi_{L/K}(u)=\frac{1}{g_0}(g_1+\ldots+g_m+(u-m)g_{m+1}),\qquad \text{if}\quad m<u\leqslant m+1.$$

In particular $\varphi_{L/K}:[-1,+\infty[\to[-1,+\infty[$ is a bijection, and we denote by $\psi_{L/K}$ its inverse function:

$$\psi_{L/K}(v):=\varphi_{L/K}^{-1}(v).$$

LEMMA 4.15. *The following formula holds true:*

$$\varphi_{L/K}(u)=\frac{1}{g_0}\sum_{g\neq e}\min\{i_{L/K}(g),u+1\}-1.$$

PROOF. a) The both sides of this formula are continuous functions. In addition, because $i_{L/K}(g)\geqslant 0$, for any $u\in[-1,0]$ one has

$$\min\{i_{L/K}(g),u+1\}=\begin{cases}0, & \text{if } g\notin G_0,\\ u+1, & \text{if } g\in G_0.\end{cases}$$

Therefore, if $u\in[-1,0]$, then

$$\mathrm{RHS}(u)=\frac{1}{g_0}\sum_{g\neq e}\min\{i_{L/K}(g),u+1\}-1=\frac{g_0(u+1)}{g_0}-1=u,$$

and $\mathrm{RHS}(u)=\varphi_{L/K}(u)$ on $[-1.0]$.

b) Assume that $m<u<m+1$ for some integer $m\geqslant 0$. Then

$$\min\{i_{L/K}(g),u+1\}=\begin{cases}i_{L/K}(g), & \text{if } g\notin G_{m+1},\\ u+1, & \text{if } g\in G_{m+1},\end{cases}$$

and therefore

$$\mathrm{RHS}'(u)=\frac{g_{m+1}}{g_0}=\varphi'_{L/K}(u).$$

This implies that $\mathrm{RHS}'(u)=\varphi'_{L/K}(u)$ if $u\notin\mathbf{Z}$. Hence $\mathrm{RHS}(u)=\varphi_{L/K}(u)$, and the lemma is proved. $\square$

LEMMA 4.16. *Let $K \subset F \subset L$ be a tower of finite Galois extensions. We keep notation of diagram* (7). *Then*

$$i_{F/K}(s) = \varphi_{L/F}(j(s)-1)+1, \qquad s \in G/H.$$

PROOF. From Lemma 4.15 it follows that

$$\varphi_{L/F}(j(s)-1)+1 = \frac{1}{|H_0|}\sum_{h\neq e}\min\{i_{L/K}(h), j(s)\}.$$

On the other hand, Corollary 4.13 can be written in the form

$$i_{F/K}(s) = \frac{1}{|H_0|}\sum_{h\in H}\min\{j(s), i_{L/K}(h)\}.$$

Here we remark that $e(L/F) = |H_0|$. These formulas imply the lemma. □

We are now in position to prove the central results of the ramification theory of Hasse-Herbrand.

THEOREM 4.17. *i) For any $u \geqslant 0$*

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

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

PROOF. i) The first statement follows from the equivalences

$$\begin{aligned} s \in (G/H)_{\varphi_{L/F}(u)} \Leftrightarrow i_{F/K}(s) \geqslant \varphi_{L/F}(u)+1 &\overset{\text{lemma 4.16}}{\Leftrightarrow} \varphi_{L/F}(j(s)-1) \geqslant \varphi_{L/F}(u) \\ &\Leftrightarrow j(s) \geqslant u+1 \Leftrightarrow \exists g \mapsto s, \text{ such that } g \in G_u. \end{aligned}$$

ii) We deduce ii) from i). We have

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

and

$$(G/H)_{\varphi_{L/F}(u)} = G_uH/H = G_u/(H\cap G_u) = G_u/H_u.$$

This implies that

$$((G/H)_0 : (G/H)_{\varphi_{L/F}(u)}) = (G_0 : G_u)/(H_0 : H_u),$$

and therefore

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

This implies ii). □

4.18. In order to define the ramification filtration for infinite extensions, we introduce the so-called upper numbering of ramification subgroups.

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 4.19.

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

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 $(G/H)^{(v)} = (G/H)_{\varphi_{L/F}(x)}$. By Theorem 4.17, $(G/H)_{\varphi_{L/F}(x)} = G_x/G_x \cap H$, and we are done. $\square$

PROPOSITION 4.20. *One has*

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

PROOF. Since $\psi_{L/K}(v) = \varphi^{-1}_{L/K}(v)$, 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 $x = \varphi_{L/K}(u)$, we obtain that $\psi'_{L/K}(x) = (G^{(0)} : G^{(x)})$. This proves the proposition. $\square$

4.21. Hasse-Hebrand theory 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.

Exercise 8. 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 the 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

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

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

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

4.22. Formula (4.9) can be written in terms of upper ramification subgroups:

THEOREM 4.23. *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. We start with the computation of the derivative of $\psi_{L/K}$. From the identity $\psi_{L/K} \circ \varphi_{L/K}(u) = u$, we have $\psi_{L/K}'(\varphi_{L/K}(u))\, \varphi_{L/K}'(u) = 1$. Since $\varphi_{L/K}'(u) = 1/(G_0 : G_u)$, this implies that

$$\psi_{L/K}'(\varphi_{L/K}(u)) = (G_0 : G_u).$$

Setting $v = \varphi_{L/K}(u)$, we obtain the formula

$$\psi_{L/K}'(v) = (G_0 : G_{\psi_{L/K}(v)}) = (G_0 : G^{(v)}) = (G^{(0)} : G^{(v)}).$$

We pass to the proof of the theorem. By (4.9), 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:

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

The theorem is proved. □

The above theorem can be generalized to arbitrary (not necessarily Galois) finite extensions as follows. For any $v \geqslant 0$ define

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

THEOREM 4.24. *For any finite extension L/K one has*

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty}\left(1-\frac{1}{[L : L\cap \overline{K}^{(v)}]}\right)dv \tag{11}$$

PROOF. See [**5**, Lemma 2.1]). □

5. Galois groups of local fields

5.1. 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 $\mathrm{Fr}_{K_n/K}$ 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 obtain an isomorphism

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

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 Fr_K:

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

Exercise 9. 1) Let ℓ be a prime number. Show that $\varprojlim_k \mathbf{Z}/\ell^k\mathbf{Z} \simeq \mathbf{Z}_\ell$.
2) Show that $\widehat{\mathbf{Z}} \simeq \prod\limits_{\ell} \mathbf{Z}_\ell$.

Exercise 10. Let K be a local field with residue field of characteristic p. Show that

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

5.2. The maximal tamely ramified extension. Let L/K be a finite Galois extension with the Galois group G. Recall that G_0 coincides with the inertia subgroup $I_{L/K}$ of G and $L_0 := L^{G_0}$ is the maximal unramified subextension of L/K. Set $L_1 := L^{G_1}$. Then $\mathrm{Gal}(L_1/L_0) \simeq G_0/G_1$ and $\mathrm{Gal}(L/L_1) = G_1$. From Propositions 4.5 and 2.9 it follows that L_1 is the maximal tamely ramified subextension L_{tr} of L/K. To sup up, we have the tower of extensions

(12)
$$\begin{tikzcd}
L \arrow[d, dash, "G_1"] \arrow[dd, dash, bend right=60, "G_0"'] \\
L_{\mathrm{tr}} \arrow[d, dash, "G_0/G_1"] \\
L_{\mathrm{ur}} \arrow[d, dash, "G/G_0"] \\
K
\end{tikzcd}$$

DEFINITION 5.3. *The group $P_{L/K} := G_1$ is called the wild inertia subgroup.*

We remark that $P_{L/K}$ is a p-group (its order is a power of p).
Passing to direct limit in the above diagram (12), we have:

(13)
$$\begin{tikzcd}
\overline{K} \arrow[d, dash, "P_K"] \arrow[dd, dash, bend right=60, "I_K"'] \\
K^{\mathrm{tr}} \arrow[d, dash] \\
K^{\mathrm{ur}} \arrow[d, dash, "\widehat{\mathbf{Z}}"'] \\
K
\end{tikzcd}$$

Consider the exact sequence

$$1 \to \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \to \mathrm{Gal}(K^{\mathrm{tr}}/K) \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \to 1. \tag{14}$$

Here $\mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \widehat{\mathbf{Z}}$. From the explicit description of tamely ramified extensions (see also Exercise 4), 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

$$\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}}) \simeq \varprojlim_{(n,p)=1} \mathbf{Z}/n\mathbf{Z} \simeq \prod_{\ell\neq p} \mathbf{Z}_l.$$

REMARK 5.4. *It is not difficult to discribe the group* $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ *in terms of generators and relations.*

5.5. 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} the compositum of all abelian extensions of K and by $G_K^{\mathrm{ab}} := \mathrm{Gal}(K^{\mathrm{ab}}/K)$ its Galois group. Local class field theory gives an explicit description of G_K^{ab} in terms of K.

THEOREM 5.6. *There exists a canonical group homomorphism (called the reciprocity map) with dense image*

$$\theta_K\,:\,K^*\to G_K^{\mathrm{ab}}$$

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 K^{ur}/K is the maximal unramified extension of K, then for any uniformizer $\pi_K\in K^*$ the restriction of the automorphism $\theta_K(\pi_K)$ on K^{ur} coincides with the Frobenius* $\mathrm{Fr}_{L/K}$, *and we have a commutative diagram*

$$\begin{array}{ccc} K^* & \xrightarrow{\theta_K} & G_K^{\mathrm{ab}} \\ \downarrow{\scriptstyle v_K} & & \downarrow \\ \widehat{\mathbf{Z}} & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ur}}/K), \end{array}$$

where the bottom map sends 1 to Fr_K. *Equivalently, for any $x\in K^*$, the automorphism $\theta_K(x)$ acts on K^{ur} by*

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

REMARK 5.7. *Local class field theory was developed by Hasse. The modern approach is based on the cohomology of finite groups (see* [**16**] *or* [**4**, Chapter VI]*, written by Serre).*

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

$$\theta_K\left(U_K^{(v)}\right) = (G_K^{\mathrm{ab}})^{(v)}, \qquad \forall v\geqslant 0. \tag{15}$$

For the classical proof of this result, see [**16**, Chapter XV].

5.8. 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 (15) it follows that the ramification jumps of K^{ab}/K are the integers -1, $0, 1, \ldots$. Under the reciprocity map, the inertia subgroup $I_{K^{\mathrm{ab}}/K}$ of G_K^{ab} is isomorphic to U_K and the wild ramification subgroup $P_{K^{\mathrm{ab}}/K}$ of $I_{K^{\mathrm{ab}}/K}$ is isomorphic to $U_K^{(1)}$. Therefore, for the maximal abelian tamely ramified extension $K^{\mathrm{ab,tr}}$ we have

$$\mathrm{Gal}(K^{\mathrm{ab,tr}}/K^{\mathrm{ur}}) \simeq U_K/U_K^{(1)} \simeq k_K^*.$$

If L/K is an abelian extension with Galois group G, then by Galois theory, $G = G_K^{\mathrm{ab}}/H$ for some closed 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 (15) it follows that the jumps of the ramification filtration on G are integers (theorem of Hasse-Arf). Assume, in addition, that L/K is wildly ramified i.e. totally ramified of degree power of p. The canonical projection of G_K^{ab} onto G induces a diagram

$$\begin{tikzcd}
0 \arrow[r] & P_{K^{\mathrm{ab}}/K} \arrow[r] \arrow[d] & G_K^{\mathrm{ab}} \arrow[r] \arrow[d] & \mathrm{Gal}(K^{\mathrm{ab,tr}}/K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_{L/K} \arrow[r] & G \arrow[r] & G/P_{L/K} \arrow[r] & 0.
\end{tikzcd}$$

Since L/K is wildly ramified, $G = P_{L/K}$, and one has

$$G \simeq P_{K^{\mathrm{ab}}/K}/(H \cap P_{K^{\mathrm{ab}}/K}).$$

Therefore

$$G^{(v)} \simeq P^{(v)}_{K^{\mathrm{ab}}/K}/(H \cap P^{(v)}_{K^{\mathrm{ab}}/K}), \qquad v \geqslant 1.$$

We can write this property in terms of the group of units U_K. Namely, let N denote the subgroup of $U_K^{(1)}$ that corresponds to $H \cap P_{K^{\mathrm{ab}}/K}$ under the isomorphism $P_{K^{\mathrm{ab}}/K} \simeq U_K^{(1)}$. Then we have an isomorphism

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

From the description of the ramification in terms of the reciprocity map (15), we obtain that

$$\rho\left(G^{(v)}\right) \simeq U_K^{(v)}/(N \cap U_K^{(v)}), \qquad v \geqslant 1. \tag{16}$$

Let denote by $v_0 < v_1 < v_2 < \ldots$ the ramification jumps of L/K. Since the quotients $U_K^{(i)}/U_K^{(i)}$ are p-elementary abelian groups (each non trivial element has order p), we conclude that all quotients $G^{(v_i)}/G^{(v_{i+1})}$ are p-elementary. This also can be proved directly using Proposition 4.5 without any reference to the reciprocity map θ_K.

6. Ramification in $\mathbf{Z}_p$-extensions

We illustrate the ramification theory of infinite extensions on the example of $\mathbf{Z}_p$-extensions.

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

In this section, we assume that K_∞/K is a totally ramified $\mathbf{Z}_p$-extension of local fields *of characteristic* 0 and set $\Gamma = \mathrm{Gal}(K_\infty/K)$. 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 K_∞/K of degree p^n over K. We have

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

Note that K_∞/K is abelian by definition. 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

$$\Gamma^{(v_i)} = p^i\mathbf{Z}_p, \qquad \forall i \geqslant 1.$$

THEOREM 6.1 (Tate [**17**]). *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 6.2. *Let $K/\mathbf{Q}_p$ be a finite extension and let $e_K = e(K/\mathbf{Q}_p)$. Then the following holds true:*

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 6.3. *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 THE THEOREM.

i) We apply the arguments of Section 5.8 to our setting with $L = K_\infty$ and $G = \Gamma$. Write $\Gamma = G_K^{\mathrm{ab}}/H$ with some closed subgroup H of G_K^{ab}. Let N denote the subgroup of $U_K^{(1)}$ that corresponds to $P_{K^{\mathrm{ab}}/K} \cap H$ under the reciprocity map. Set

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

Then the isomorphism (16) reads

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

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 $\rho(\gamma_{i_0}) = \bar{x}$, where $\bar{x} = x \pmod{(N \cap U_K^{(m_0)})}$ and $x \in U_K^{(m_0)} \setminus U_K^{(m_0+1)}$. By Corollary 6.3,

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

Since $\rho(\gamma_{i_0+n}) = \bar{x}^{p^n}$ 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 $v_{i_0+n} = v_{i_0} + e_K n$ for all $n \geqslant 0$, and the assertion i) is proved.

ii) We prove ii) applying Theorem 4.23. 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

$$|G(n)^{(v)}| = \begin{cases} p^{n-i}, & \text{if } v_{i-1} < v \leqslant v_i, \\ 1, & \text{if } v > v_{n-1} \end{cases} \tag{17}$$

(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 (17). 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 $n > i_0$

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

The theorem is proved.

□

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 for the different from Proposition 4.9 reads in our case:

$$v_L(\mathfrak{D}_{L/K}) = (p-1)(t+1). \tag{18}$$

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

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

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

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

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 (18) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n)\in\mathfrak{m}_K^s$. The lemma is proved. $\square$

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

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

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 (18) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n)\in\mathfrak{m}_K^s$. The lemma is proved. $\square$

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 [**5**]. This theory goes back to the fundamental paper of Tate [**17**], 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

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

Following [**6**], 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*

$$\mathfrak{D}_{K_\infty/K} = \bigcap_{n=0}^{\infty} (\mathfrak{D}_{K_n/K} O_{K_\infty}),$$

where $\mathfrak{D}_{K_n/K} O_{K_\infty}$ denotes the ideal in O_{K_∞} generated by $\mathfrak{D}_{K_n/K}$.

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

$$L_\infty = \bigcup_{n=n_0}^{\infty} L_n.$$

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

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

PROOF. i) We consider the bilinear form provided by the trace map (see Chapter I, Section 3) :

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

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 $x \in \mathfrak{D}^{-1}_{L_m/K_m}$ 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:

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

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

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

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

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

Hence $x \in \mathfrak{D}^{-1}_{L_\infty/K_\infty}$, and the inclusion $\bigcap_{n=0}^{\infty}(\mathfrak{D}^{-1}_{L_n/K_n}O_{L_\infty}) \subset \mathfrak{D}^{-1}_{L_\infty/K_\infty}$ is proved. $\square$

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 [**5**]. 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 $v_K(\mathfrak{D}_{K_\infty/K}) = +\infty$.

2.3.2. For any algebraic extension M/K, set $M^{(v)} := M^{G_K^{(v)}} = M \cap \overline{K}^{(v)}$.

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

$$[L_n : L_n^{(w)}] = [K_n : K_n^{(w)}].$$

PROOF. Recall that if M/F is a Galois extension and E/F is an arbitrary extension such that $M \cap E = F$, then M and E are linearly disjoint over F.

Since $G_K^{(w)}$ is a normal subgroup of K_K, the extension $\overline{K}^{(w)}/K$ is Galois. Hence $\overline{K}^{(w)}/K_n \cap \overline{K}^{(w)}$ is also a Galois extension, and the fields $\overline{K}^{(w)}$ an K_n are linearly disjoint over $K_n^{(w)} = K_n \cap \overline{K}^{(w)}$. Since $L_n^{(w)} = \overline{K}^{(w)} \cap L_n$ is a subfield of $\overline{K}^{(w)}$, we conclude that $L_n^{(w)}$ and K_n are linearly disjoint over $K_n^{(w)}$. Therefore

$$[K_n : K_n^{(w)}] = [K_n L_n^{(w)} : L_n^{(w)}]. \tag{19}$$

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

$$L_n = K_nL_n^{(w)}.$$

Together with (19), this proves the lemma. $\square$

2.4.1. We prove that *ii*) $\Rightarrow$ *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 (11) and Lemma 2.4, we obtain that

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

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

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

It's clear that the sequence $[K_n\overline{K}^{(w)} : \overline{K}^{(w)}]$ is increasing when $n \to +\infty$, and we only need to show that it goes to infinity. We prove this by contradiction. Assume that $[K_n\overline{K}^{(w)} : \overline{K}^{(w)}]$ is bounded above. Then there exists n_0 such that $[K_n\overline{K}^{(w)} : \overline{K}^{(w)}]$ is constant for $n \geqslant n_0$. Hence $K_n\overline{K}^{(w)} = K_{n_0}\overline{K}^{(w)}$ for $n \geqslant n_0$ and we conclude that $K_\infty\overline{K}^{(w)} = K_{n_0}\overline{K}^{(w)}$. Since K_{n_0}/K is finite, there exists $v \geqslant w$ such that $K_{n_0} \subset \overline{K}^{(v)}$. Then $K_\infty \subset K_{n_0}\overline{K}^{(w)} \subset \overline{K}^{(v)}$. Therefore K_∞/K has finite conductor, contrary to our assumption.

2.4.2. We prove that *iii*) $\Rightarrow$ *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 $\mathfrak{m}_{K_\infty} = \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$.

DEFINITION. *We say that an extension F/K of a local field K of characteristic* 0 *is deeply ramified if it satisfies the equivalent conditions of Theorem 2.2.*

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. 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*

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

Examples. 1) An unramified extension of local fields is almost etale.

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.

3.1.1.

THEOREM 3.2. *Assume that F is a deeply ramified extension of a local field K of characteristic* 0. *Then*

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

Fix an absolute value $|\cdot|_K$ on K. Recall (see Section 1) that $|\cdot|_K$ extends in a unique way to an absolute value on $\mathbf{C}_K$, which we denote again by $|\cdot|_K$.

We first prove the following lemma.

LEMMA 3.3. *Let L/F be a finite Galois extension of the deeply ramified extension F, and let $G = \mathrm{Gal}(L/F)$. Then for any $\alpha \in L$ and any $c > 1$ there exists $\beta \in F$ such that*

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

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

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

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

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

The lemma is proved. □

3.3.1. *Proof of Theorem 3.2.* 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 3.3, 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.

In this section, we denote by $|\cdot|_K$ the absolute value on K normalized as follows

$$|x|_K = \frac{1}{q^{v_K(x)}}, \qquad x \in K,$$

where $q = |k_K|$. In particular, $|p|_K = 1/q^{e_K}$, where $e_K = e(K/\mathbf{Q}_p)$. We extend this absolute value to $\mathbf{C}_K$.

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. First, we prove that $i) \Rightarrow ii)$. Let $x \in K_\infty$. Then

$$|T_{K_\infty/K}(x)|_K = |(T_{K_\infty/K}(x) - x) + x|_K \leqslant \max\{|T_{K_\infty/K}(x) - x|_K, |x|_K\}.$$

If we assume i), then

$$|T_{K_\infty/K}(x) - x|_K \leqslant c|\gamma(x) - x|_K \leqslant c \max\{|\gamma(x)|_K, |x|_K\} = c|x|_K,$$

and we obtain that

$$|T_{K_\infty/K}(x)|_K \leqslant A|x|_K, \qquad A = \max\{1, c\}.$$

Since $T_{K_\infty/K}$ is a K-linear map, this inequality implies that $T_{K_\infty/K}$ is continuous.

Now we prove i). We split the proof in several steps.

a) By Proposition 6.1, $v_K(\mathfrak{D}_{K_n/K}) = e_K n + a_n/p^n$, where the sequence a_n is bounded. Therefore

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

where α_n is bounded. Lemma 1.1 for the extension K_n/K_{n-1} can be written in the form

$$v_{K_{n-1}}(\mathrm{Tr}_{K_n/K_{n-1}}(x)) \geqslant \left[\frac{v_{K_n}(x) + v_{K_n}(\mathfrak{D}_{K_n/K_{n-1}})}{e(K_n/K_{n-1})}\right] \geqslant \frac{v_{K_n}(x) + v_{K_n}(\mathfrak{D}_{K_n/K_{n-1}})}{e(K_n/K_{n-1})} - 1.$$

Since $v_{K_n}(\cdot) = p^n v_K(\cdot)$ and $e(K_n/K_{n-1}) = p$, we have:

$$v_K(\mathrm{Tr}_{K_n/K_{n-1}}(x)) \geqslant v_K(x) + v_K(\mathfrak{D}_{K_n/K_{n-1}}) - \frac{1}{p^{n-1}}.$$

Taking into account the formula for the different, we obtain that

$$v_K(\mathrm{Tr}_{K_n/K_{n-1}}(x)) \geqslant v_K(x) + e_K(1 - b_n/p^{n-1})$$

for some bounded sequence b_n. Choose $b > 0$ such that $b_n < b$ for all n. Then

$$v_K(\mathrm{Tr}_{K_n/K_{n-1}}(x)) \geqslant v_K(x) + e_K(1 - b/p^{n-1}).$$

Passing to absolute values, we can write this formula in the following form:

$$|\mathrm{Tr}_{K_n/K_{n-1}}(x)|_K \leqslant |p|_K^{1-b/p^{n-1}} |x|_K, \qquad \forall x \in K_n. \tag{20}$$

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

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

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

$$\left|\frac{1}{p}\mathrm{Tr}_{K_n/K_{n-1}}(x)-x\right|_K \leqslant |p|_K^{-1}\cdot|\gamma(x)-x|_K, \qquad \forall x\in K_n. \tag{21}$$

c) We prove by induction on n that

$$\left|\mathrm{T}_{K_\infty/K}(x)-x\right|_K \leqslant c_n\cdot|\gamma(x)-x|_K, \qquad \forall x\in K_n, \tag{22}$$

where $c_1=|p|_K$ and $c_n=c_{n-1}\cdot|p|_K^{-b/p^{n-1}}$. For $n=1$, this follows from (21). 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 (21). For the second term, we have

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

(Here the last inequality follows from (20)). This proves (22).

d) Set $c=c_1\prod_{n=2}^{\infty}|p|_K^{-b/p^{n-1}}=c_1|p|_K^{-b/(p-1)}$. Then $c_n<c$ for all $n\geqslant 1$, and from (22) 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 inverse, 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 inverse, 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 3.2 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

Perfectoid fields

1. Perfectoid fields

1.0.1. The notion of perfectoid field was introduced in Scholze's fundamental paper [**15**] as a far-reaching generalization of Fontaine's constructions [**8**], [**9**]. 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.

Example 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

$$\left(\sum_{i=0}^{m} [a_i]\pi_n^m\right)^p \equiv \sum_{i=0}^{m} [a_i]^p \pi_{n-1}^m \pmod{p}.$$

3) Let $K_n = \mathbf{Q}_p[\zeta_{p^n}]$, where ζ_{p^n} is a primitive root of unity, and $K_\infty = \underset{n\geqslant 1}{\cup} K_n$. By the same method, it is not difficult to show that the completion of K_∞ is a perfectoid field.

The following important result is a particilar case of [**11**, 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 paper of Fontaine [**8**].

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

$$O_{E^\flat} := \varprojlim_{\varphi} O_E/pO_E = \varprojlim (O_E/pO_E \xleftarrow{\varphi} O_E/pO_E \xleftarrow{\varphi} \cdots), \tag{23}$$

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. $\square$

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

$$(x+y)^{(n)} = \lim_{m\to+\infty} \left(x^{(n+m)} + y^{(n+m)}\right)^{p^m}, \qquad (xy)^{(n)} = x^{(n)}y^{(n)}. \tag{24}$$

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. $\square$

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

$$O_{E^\flat} \simeq \varprojlim_{x^p \leftarrow x} O_E, \tag{25}$$

where the right hand side is equipped with the addition and multiplication defined by (24).

PROOF. This follows from from 2). $\square$

Define

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

Exercise 10. Let $y=(y_0,y_1,\dots)\in O_{E^\flat}$. Show that

$$y_n=0 \quad \Leftrightarrow \quad |y|_{E^\flat}\leqslant |p|_E^{p^n}. \tag{26}$$

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.

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,

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

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

ii) We prove the completeness of $O_{E^\flat}$. 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 (26), 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 $\lim_{n\to+\infty}x_n=a$.

We prove the perfectness of $O_{E^\flat}$. Set $A:=\varprojlim_{x^p\leftarrow x}O_E$. Then we have a commutative diagram

$$\begin{array}{ccc} O_{E^\flat} & \xrightarrow{\sim} & A \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} \\ O_{E^\flat} & \xrightarrow{\sim} & A, \end{array} \tag{27}$$

where the horizontal maps are the isomorphisms (25), and the map ψ is given by

$$\psi(a_0,a_1,a_2,\dots)=(a_0^p,a_1^p,a_2^p,\dots).$$

It's clear that $\ker(\psi)=\{0\}$, and therefore ψ is injective. From the formula

$$\psi(a_1,a_2,a_3,\dots)=\psi(a_0,a_1,a_2,\dots)$$

it follows that ψ is surjective. Therefore φ is an isomorphism.

The proof of the other assertions is left as an exercise.

□

Exercise 11. 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 [**15**, Proposition 3.8]. See also Kedlaya's proof in [**2**]. $\square$

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*

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

such that

$$w_n(\Phi_0,\Phi_1,\dots,\Phi_n)=F(w_n(x_0,x_1,\dots,x_n),w_n(y_0,y_1,\dots,y_n)),\qquad \textit{for all } n\geqslant 0. \tag{28}$$

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

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

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

PROOF. The proof is left to the reader. $\square$

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 (28) it follows that

$$\Phi_n=\frac{1}{p^n}\left(F(w_n(x_0,x_1,\dots,x_n),w_n(y_0,y_1,\dots,y_n))-(\Phi_0^{p^n}+\dots+p^{n-1}\Phi_{n-1}^p)\right). \tag{29}$$

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:

$$\begin{aligned}(30)\quad & F(w_n(x_0,\dots,x_{n-1},x_n), w_n(y_0,\dots,y_{n-1},y_n)) \\ &\qquad \equiv F(w_{n-1}(x_0^p,\dots,x_{n-1}^p), w_{n-1}(y_0^p,\dots,y_{n-1}^p)) \pmod{p^n}.\end{aligned}$$

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

$$\begin{aligned}(31)\quad \Phi_0^{p^n}+\cdots+p^{n-1}\Phi_{n-1}^p &\equiv w_{n-1}\left(\Phi_0(x_0^p,y_0^p),\dots,\Phi_{n-1}(x_0^p,y_0^p,\dots,x_{n-1}^p,y_{n-1}^p)\right) \\ &\equiv F(w_{n-1}(x_0^p,\dots,x_{n-1}^p), w_{n-1}(y_0^p,\dots,y_{n-1}^p)) \pmod{p^n}.\end{aligned}$$

From (30) and (31) 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 (29), 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

$$w_n(v_0,\dots,v_n) = w_n(x_0,\dots,x_n) + w_n(f_0(y_0,z_0), f_1(y_0,z_0,y_1,z_1),\dots)$$
$$= w_n(x_0,\dots,x_n) + w_n(y_0,\dots,y_n) + w_n(z_0,\dots,z_n).$$

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

$$(x_0,x_1,x_2,\dots)\cdot(y_0,0,0,\dots) = (x_0y_0, x_1y_0^p, x_1y_0^{p^2},\dots) \tag{32}$$

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 (32). □

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 method used in the proof of Theorem 3.5. □

5) For any $n \geqslant 0$ define

$$I_n(A) = \big\{(a_0, a_1, \dots) \in W(A) \mid a_i = 0 \text{ for all } 0 \leqslant i \leqslant n\big\}.$$

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 base of neighborhoods 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 method used in the proof of Theorem 3.5. □

Assume that A is a ring of characteristic p, i.e. that $p \cdot 1_A = 0_A$ in A. Then A is equipped with the absolute Frobenius endomorphism

$$\varphi : A \to A, \qquad \varphi(x) = x^p.$$

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 $\bar{h}_n(x_0,x_1,\dots,x_n)$ 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. □

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

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). Namely, the p-adic topology is determined by the property that $(p^nW(A))_{n\geqslant 0}$ is asystem of neighborhoods at 0.
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 a perfect integral domain (i.e. has no nonzero zero divisors) 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 [**16**, 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

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

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

$$\begin{tikzcd} W_n(O_E) \arrow[r, "w_n"] \arrow[d] & O_E \arrow[d] \\ W_n(O_E/pO_E) \arrow[r, "\eta_n"] & O_E/p^{n+1}O_E \end{tikzcd}$$

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) We omit the proof. See [**8**, Proposition 2.4] and [**7**, Proposition 3.1.9].

The surjectivity of θ_E follows from the surjectivity of the map

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

□

Exercise 12. 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

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

4) Deduce the claim from 3).

Example. Let $E = \mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$. Take a compatible system p^{1/p^m} of p^mth roots of p, i.e. such that $(p^{1/p^m})^p = p^{1/p^{m-1}}$ and set $a_m = p^{1/p^m} \mod p$. Then $a = (a_m)_{m \geqslant 0} \in O_{\mathbf{C}_p}^\flat$ and $a^{(0)} = p$. By Proposition 4.2, the element $\xi = [a] - p$ is a generator of $\ker(\theta_{\mathbf{C}_p})$.

4.3. The untilt. 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 $\mathbf{C}_{E^\flat} := \widehat{\overline{E^\flat}}$ denote the p-adic completion of $\overline{E^\flat}$. By construction, $\mathbf{C}_{E^\flat} \subset \mathbf{C}_E^\flat$. In proposition 4.5 below we will prove that $\mathbf{C}_{E^\flat} \subset \mathbf{C}_E^\flat$.

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 perfect 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 $O_{\mathfrak{F}^\sharp}$).

PROPOSITION 4.4. *$\mathfrak{F}^\sharp$ is a perfectoid field and $(\mathfrak{F}^\sharp)^\flat = \mathfrak{F}$.*

PROOF. We omit the proof that $\mathfrak{F}^\sharp$ is complete with the ring of integers $O_{\mathfrak{F}^\sharp}$. If $\xi = \sum_{n\geqslant 0} [a_n]p^n$, 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

$$O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp} \simeq O_{\mathfrak{F}}/a_0 O_{\mathfrak{F}}.$$

Since $O_{\mathfrak{F}}$ is perfect, the Frobenius map in surjective on $O_{\mathfrak{F}}/a_0O_{\mathfrak{F}}$ Therefore φ : $O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp} \to O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp}$ is surjective, and we proved that $\mathfrak{F}^\sharp$ is a perfectoid field.

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

Exercise 13. 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

$$\varprojlim_{\varphi} O_{\mathfrak{F}^\sharp}/pO_{\mathfrak{F}^\sharp} = \varprojlim_{\varphi} O_{\mathfrak{F}}/a_0 O_{\mathfrak{F}} \simeq O_{\mathfrak{F}},$$

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

PROPOSITION 4.5. *One has $\mathbf{C}_E^\flat = \mathbf{C}_{E^\flat}$.*

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 result of this section.

THEOREM 4.6 (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. (See Fargues–Fontaine [**7**, Theorem 3.2.1].)

a) Let $\mathrm{Aut}(\mathbf{C}_E/E)$ denote the group of continuous automorphisms of $\mathbf{C}_E/E$. The Galois group $G_E = \mathrm{Gal}(\overline{E}/E)$ acts on $\overline{E}$ continuously. Therefore it acts on $\mathbf{C}_E$, and $G_E = \mathrm{Aut}(\mathbf{C}_E/E)$. The same argument shows that $G_{E^\flat} = \mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$, where $G_{E^\flat} = \mathrm{Gal}(\overline{E}^\flat/E^\flat)$ and $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$ denotes the group of continuous automorphisms of $\mathbf{C}_{E^\flat}/E^\flat$.

By Proposition 4.5, $\mathbf{C}_E^\flat = \mathbf{C}_{E^\flat}$. The action of $\mathrm{Aut}(\mathbf{C}_E/E)$ on $O_{\mathbf{C}_E}$ induces an action of G_E on $O_{\mathbf{C}_E}/pO_{\mathbf{C}_E}$ and, therefore, on $O_{\mathbf{C}_E}^\flat := \varprojlim O_{\mathbf{C}_E}/pO_{\mathbf{C}_E}$. This provides a natural morphism of groups $\mathrm{Aut}(\mathbf{C}_E/E) \to \mathrm{Aut}(\mathbf{C}_E^\flat/E^\flat)$. Hence, we have a chain of morphisms:

$$G_E \to \mathrm{Aut}(\mathbf{C}_E^\flat/E^\flat) \xrightarrow{\sim} \mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat) \xrightarrow{\sim} G_{E^\flat}. \tag{33}$$

Conversely, again by Proposition 4.5, we have an isomorphism

$$W(O_{\mathbf{C}_{E^\flat}})/\xi W(O_{\mathbf{C}_{E^\flat}}) \simeq O_{\mathbf{C}_E}. \tag{34}$$

The action of $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$ on $\mathbf{C}_{E^\flat}$ induces an action of $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$ on $W(O_{\mathbf{C}_{E^\flat}})$. Since $\xi \in W(O_{E^\flat})$, the group $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$ acts trivially on ξ, and the above isomorphism defines a continuous action of $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat)$ on $O_{\mathbf{C}_E}$. This provides a morphism $\mathrm{Aut}(\mathbf{C}_{E^\flat}/E^\flat) \to \mathrm{Aut}(\mathbf{C}_E/E)$. Therefore, we have a chain of morphisms

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

It's easy to see that the maps (33) and (34) are inverse to each other. Therefore

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

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

$$\big\{\text{finite extensions of } E\big\} \leftrightarrow \big\{\text{finite extensions of } E^\flat\big\} \tag{35}$$

b) Using the isomorphism $G_E \simeq G_{E^\flat}$, we can consider subgroups of $G_{E^\flat}$ as subgroups of G_E and vice-versa. Let $\mathfrak{F}/E^\flat$ be a finite extension. Since $E^\flat$ is perfect, $\mathfrak{F}$ is also perfect. Then

$$\mathfrak{F}^\sharp = (W(O_{\mathfrak{F}})/\xi W(O_{\mathfrak{F}}))\,[1/p)] \subset \mathbf{C}_E^{G_{\mathfrak{F}}}. \tag{36}$$

We omit the proof that the above inclusion is, in fact, an equality:

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

This shows that the Galois correspondence

$$\left\{\text{finite extensions of } E^\flat\right\} \to \left\{\text{finite extensions of } E\right\} \tag{37}$$

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) We will use the fact that $\mathbf{C}_E^{G_F} = F$ for any finite extension F/E. Below, we give a proof only in the case $E \subset \mathbf{C}_K$, where K is a local field of characteristic 0. By Theorem 1.1, $E = \widehat{L}$, where L/K is deeply ramified. Write $F = E[\alpha]$, where α is a root of an irreducible polynomial with coefficients in E. From Krasner's lemma it follows that there exists an algebraic element β over L such that $E[\alpha] = E[\beta]$. Therefore $F = \widehat{M}$, where $M = K[\beta]$. Since the Galois group $G_M = \mathrm{Gal}(\overline{K}/M)$ acts continuously, we have $G_M = \mathrm{Aut}(\mathbf{C}_E/\widehat{M}) = G_F$. Since $\mathbf{C}_E = \mathbf{C}_K$, we have

$$\mathbf{C}_E^{G_F} = \mathbf{C}_K^{G_M} = \widehat{M} = F$$

(here we used Theorem 3.2 of Chapter 2!).

d) Let F be a finite extension of E. Set $\mathfrak{F} = \left(\overline{E^\flat}\right)^{G_F}$. Then $G_{\mathfrak{F}} = G_F$ and $F = \mathbf{C}_E^{G_{\mathfrak{F}}}$ by part c). From part b), we have

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

By Proposition 4.4, $\mathfrak{F}^\sharp$ is a perfectoid field. Therefore $F = \mathfrak{F}^\sharp$ is a perfectoid field, and the assertion i) is proved.

e) We have

$$F^\flat = \left(\mathfrak{F}^\sharp\right)^\flat = \mathfrak{F} = \left(\overline{E^\flat}\right)^{G_F}. \tag{38}$$

Formulas (38) shows that the inverse of the correspondence (37) is given by $F \mapsto F^\flat$. The theorem is proved. $\square$

CHAPTER 4

p-adic representations of local fields

1. p-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*

$$\mathbf{Rep}_{\mathbf{Z}_\ell}(G_K) \to \mathbf{Rep}_{\mathbf{Q}_\ell}(G_K),$$
$$T \mapsto T \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$$

is essentially surjective.

PROOF. Let $\{e_1, \dots, e_n\}$ 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 $\bigcap_g gHg^{-1}$, where g runs the representatives of left cosets of H, one can assume that H is normal in G. Write $G = \bigcup_{i=1}^{m} g_i H$ 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 $E[\ell]$.

2. Admissible representations

2.1. General approach. p-adic representations arising in algebraic geometry have very special properties and form some natural subcategories of $\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$. As was first observed by Grothendieck, it should be possible to classify them in terms of some objects of semi-linear algebra. We review 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 $G_K = \mathrm{Gal}(\overline{K}/K)$.

Let B be a commutative $\mathbf{Q}_p$-algebra without zero divisors, equipped with a $\mathbf{Q}_p$-linear action of G_K, namely

- $g(b_1 + b_2) = g(b_1) + g(b_2), \qquad g \in G_K, \quad b_1, b_2 \in B;$
- $g(b_1 b_2) = g(b_1) g(b_2), \qquad g \in G_K, \quad b_1, b_2 \in B;$
- $g(\lambda b) = \lambda g(b), \qquad g \in G_K, \quad \lambda \in \mathbf{Q}_p, \quad b \in B.$

Let C denote the field of fractions of B. the action of G_K extends to C by the formula $g(b_1/b_2) = g(b_1)/g(b_2)$. Set $E = B^{G_K} := \{b \in B \mid g(b) = b, \forall g \in G_K\}$.

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.

2.2. 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

$$\mathbf{D}_B(V) = (V \otimes_{\mathbf{Q}_p} B)^{G_K}.$$

Consider the map

$$(V \otimes_{\mathbf{Q}_p} B) \otimes_E B \to V \otimes_{\mathbf{Q}_p} B, \qquad (v \otimes b_1) \otimes b_2 \mapsto v \otimes b_1 b_2.$$

Since $\mathbf{D}_B(V) \subset V \otimes_{\mathbf{Q}_p} B$, it induces a map

$$\alpha_B : \mathbf{D}_B(V) \otimes_E B \to V \otimes_{\mathbf{Q}_p} B.$$

PROPOSITION 2.3. *i) The map α_B is injective for all $V \in \mathbf{Rep}_{\mathbf{Q}_p}(G_K)$.*
ii) $\dim_E \mathbf{D}_B(V) \leqslant \dim_{\mathbf{Q}_p} V$.

PROOF. See [**3**, 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 $x = 0$. $\square$

DEFINITION. *A p-adic representation V is called B-admissible if*

$$\dim_E \mathbf{D}_B(V) = \dim_{\mathbf{Q}_p} V.$$

PROPOSITION 2.4. *If V is admissible, then the map α_B is an isomorphism.*

PROOF. See [**10**, 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 $\bigwedge^n V$ is one dimensional, G_K acts on it by $g(y) = \eta(g) y$, where $\eta : G_K \to \mathbf{Z}_p^*$ is a character. Taking into account that x is stable under the action of the Galois group, we obtain that $g(\det(A)g(y) = \det(A)y$ and therefore that $g(\det(A)) = \eta(g)^{-1}\det(A)$. Hence the $\mathbf{Q}_p$-vector space generated by $\det(A)$ is stable under the action of G_K. Hence $\det(A) \in B$ is invertible, the matrix A is invertible, and α_B is an isomorphism. $\square$

2.4.1. We denote by $\mathbf{Rep}_B(G_K)$ the category of B-admissible representations. The following proposition summarizes some properties of this category.

PROPOSITION 2.5. *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. See [**10**, Proposition 1.5.2]. i) Since V, V' and V'' are $\mathbf{Q}_p$-vector spaces, the sequence

$$0 \to V' \otimes_{\mathbf{Q}_p} B \to V \otimes_{\mathbf{Q}_p} B \to V'' \otimes_{\mathbf{Q}_p} B \to 0$$

is an exact sequence of G_K-modules. Passing to Galois invariants, we obtain that

$$0 \to (V' \otimes_{\mathbf{Q}_p} B)^{G_K} \to (V \otimes_{\mathbf{Q}_p} B)^{G_K} \to (V'' \otimes_{\mathbf{Q}_p} B)^{G_K}$$

is exact. Tautologically, the last exact sequence reads:

$$0 \to \mathbf{D}_B(V') \to \mathbf{D}_B(V) \to \mathbf{D}_B(V'').$$

From the exact sequence we have that

$$\dim_E \mathbf{D}_B(V) \leqslant \dim_E \mathbf{D}_B(V') + \dim_E \mathbf{D}_B(V'').$$

Moreover $\dim_E \mathbf{D}_B(V') \leqslant \dim_{\mathbf{Q}_p}(V')$, $\dim_E \mathbf{D}_B(V) \leqslant \dim_{\mathbf{Q}_p}(V)$ and $\dim_E \mathbf{D}_B(V'') \leqslant \dim_{\mathbf{Q}_p}(V'')$ by Proposition 2.3. If V is B-admissible, $\dim_E \mathbf{D}_B(V) = \dim_{\mathbf{Q}_p}(V)$, and we obtain that

$$\dim_{\mathbf{Q}_p}(V) = \dim_{\mathbf{Q}_p}(V') + \dim_{\mathbf{Q}_p}(V'') \leqslant \dim_E \mathbf{D}_B(V') + \dim_E \mathbf{D}_B(V'').$$

Therefore $\dim_E \mathbf{D}_B(V') = \dim_{\mathbf{Q}_p}(V')$, $\dim_E \mathbf{D}_B(V'') \leqslant \dim_{\mathbf{Q}_p}(V'')$, and we proved that V' and V'' are B-admissible. In addition, in that case the sequence

$$0 \to \mathbf{D}_B(V') \to \mathbf{D}_B(V) \to \mathbf{D}_B(V'') \to 0$$

is exact.

ii) Assume that V' and V'' are B-admissible. Then we have isomorphisms

$$\mathbf{D}_B(V') \otimes_E B \to V' \otimes_{\mathbf{Q}_p} B, \qquad \mathbf{D}_B(V'') \otimes_E B \to V'' \otimes_{\mathbf{Q}_p} B.$$

Taking the tensor product of these isomorphisms over B, we obtain

$$(\mathbf{D}_B(V')\otimes_E B)\otimes_B(\mathbf{D}_B(V'')\otimes_E B)\simeq(V'\otimes_{\mathbf{Q}_p}B)\otimes_B(V''\otimes_{\mathbf{Q}_p}B).$$

Since

$$(\mathbf{D}_B(V')\otimes_E B)\otimes_B(\mathbf{D}_B(V'')\otimes_E B)\simeq(\mathbf{D}_B(V')\otimes_E\mathbf{D}_B(V''))\otimes_E B$$

and

$$(V'\otimes_{\mathbf{Q}_p}B)\otimes_B(V''\otimes_{\mathbf{Q}_p}B)\simeq(V'\otimes_{\mathbf{Q}_p}V'')\otimes_{\mathbf{Q}_p}B,$$

we have

$$(\mathbf{D}_B(V')\otimes_E\mathbf{D}_B(V''))\otimes_E B\simeq(V'\otimes_{\mathbf{Q}_p}V'')\otimes_{\mathbf{Q}_p}B.$$

Taking Galois invariants in the both sides, we obtain

$$\mathbf{D}_B(V')\otimes_E\mathbf{D}_B(V'')\simeq\mathbf{D}_B(V'\otimes_{\mathbf{Q}_p}V'').$$

In particular,

$$\begin{aligned}\dim_E\mathbf{D}_B(V'\otimes_{\mathbf{Q}_p}V'')&=\dim_E\mathbf{D}_B(V')\cdot\dim_E\mathbf{D}_B(V'')\\&=\dim_{\mathbf{Q}_p}(V')\cdot\dim_{\mathbf{Q}_p}(V'')=\dim_{\mathbf{Q}_p}(V'\otimes_{\mathbf{Q}_p}V'').\end{aligned}$$

This shows that $V'\otimes_{\mathbf{Q}_p}V''$ is B-admissible. In addition, in that case

$$\mathbf{D}_B(V'\otimes_{\mathbf{Q}_p}V'')\simeq\mathbf{D}_B(V')\otimes_E\mathbf{D}_B(V'').$$

iii) We prove that the dual V^* of an admissible representation V is admissible. This follows from the following isomorphisms:

$$\begin{aligned}\mathbf{D}_B(V^*)&=(\mathrm{Hom}_{\mathbf{Q}_p}(V,\mathbf{Q}_p)\otimes_{\mathbf{Q}_p}B)^{G_K}\simeq\mathrm{Hom}_{\mathbf{Q}_p}(V,B)^{G_K}\simeq\mathrm{Hom}_B(V\otimes_{\mathbf{Q}_p}B,B)^{G_K}\\&\simeq\mathrm{Hom}(\mathbf{D}_B(V)\otimes_E B,B)^{G_K}\simeq\mathrm{Hom}_E(\mathbf{D}_B(V),B)^{G_K}\simeq\mathrm{Hom}_E(\mathbf{D}_B(V),E).\end{aligned}$$

Therefore $\dim_E\mathbf{D}_B(V^*)=\dim_E\mathrm{Hom}_E(\mathbf{D}_B(V),E)=\dim_E\mathbf{D}_B(V)=\dim_{\mathbf{Q}_p}(V)$. This implies that V^* is admissible. In addition, in that case

$$\mathbf{D}_B(V^*)\simeq\mathrm{Hom}_E(\mathbf{D}_B(V),E).$$

Assume now that V' and V'' are B-admissible, Since

$$\mathrm{Hom}_{\mathbf{Q}_p}(V',V'')\simeq\mathrm{Hom}_{\mathbf{Q}_p}(V',\mathbf{Q}_p)\otimes_{\mathbf{Q}_p}V'',$$

the admissibility of $\mathrm{Hom}_{\mathbf{Q}_p}(V',V'')$ follows from the admissibility of the dual representation and the tensor product.

iv) Let $\mathrm{Hom}_{G_K}(V',V'')$ denote the vector space of morphisms $V'\to V''$.

$$\begin{aligned}\mathrm{Hom}_{G_K}(V',V'')&\hookrightarrow\mathrm{Hom}_{G_K}(V'\otimes_{\mathbf{Q}_p}B,V''\otimes_{\mathbf{Q}_p}B)\\&\simeq\mathrm{Hom}_{G_K}(\mathbf{D}_B(V')\otimes_E B,\mathbf{D}_B(V'')\otimes_E B)\simeq\mathrm{Hom}_E(\mathbf{D}_B(V'),\mathbf{D}_B(V'')).\end{aligned}$$

Therefore the map $\mathrm{Hom}_{G_K}(V',V'')\to\mathrm{Hom}_E(\mathbf{D}_B(V'),\mathbf{D}_B(V''))$ is injective, and the functor $\mathbf{D}_B$ is faithful. $\square$

2.5.1. 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

$$\langle\, ,\rangle \,:\, V \times \mathbf{D}^*_B(V) \to B, \qquad \langle v, f\rangle = f(v),$$

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.

2.6. Examples.

2.6.1. *$B = \overline{K}$, where K is of characteristic* 0. One has $B^{G_K} = K$. The following proposition describes $\overline{K}$-admissible representations.

PROPOSITION 2.7. *$\rho \,:\, G_K \to \mathrm{Aut}_{\mathbf{Q}_p}V$ 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 !).

THEOREM 2.8 (Hilbert's theorem 90). *Let W be a finite dimensional $\overline{K}$-vector space of dimension n equipped with a semilinear action of G_K, namely*

- $g(w_1 + w_2) = g(w_1) + g(w_2), \qquad g \in G_K, \quad w_1, w_2 \in W;$
- $g(\lambda w) = g(\lambda) g(w), \qquad g \in G_K, \quad \lambda \in \overline{K}, \quad w \in W.$

Assume that this action is continuous in the discrete topology on W. Then $W^{G_K} := \{w \in W \mid g(w) = w, \forall g \in G_K\}$ is an n-dimensional K-vector space and the natural map

$$\overline{K} \otimes_K W^{G_K} \to W, \qquad \lambda \otimes w \mapsto \lambda w$$

is an isomorphism.

PROOF. The proof is omitted. See, for example, [**14**, Chapter 2, §2]. □

By Hilbert's theorem 90, 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. □

2.8.1. *$B = \mathbf{C}_K$, where K is of characteristic* 0. One has $\mathbf{C}_K^{G_K} = K$ by Theorem 4.5, Chapter II.

THEOREM 2.9 (Sen). *ρ is $\mathbf{C}_K$-admissible if and only if $\rho(I_K)$ is finite.*

Example. Take $V = \mathbf{Q}_p(1)$. Then

$$\mathbf{D}_{\mathbf{C}_K}(\mathbf{Q}_p(1)) = (\mathbf{C}_K \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(1))^{G_K} = (\mathbf{C}_K(\chi_K))^{G_K} = 0$$

again by Theorem 4.5, Chapter II. Therefore $\mathbf{Q}_p(1)$ is not $\mathbf{C}_K$-admissible.

3. Hodge–Tate representations

3.1. We maintain notation and conventions of Section 2.1. The notion of a Hodge–Tate representation was introduced in Tate's paper [**?**]. 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 3.2. *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 the field of Laurent power series $\mathbf{C}_K((t))$, 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, Chapter II, 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

$$g(b) = \eta(g) b, \qquad \forall g \in G_K \tag{39}$$

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 (39), 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. □

3.2.1. A graded vector space over K is a K-vector space D equipped with a decomposition into a direct sum of subspaces D^i, $i \in \mathbf{Z}$:

$$G = \bigoplus_{i \in \mathbf{Z}} D^i.$$

We will often write $\mathrm{gr}^i(D) := D^i$ and $G = \bigoplus_{i \in \mathbf{Z}} \mathrm{gr}^i(D)$. A morphism of graded spaces $f : D' \to D''$ is a K-linear map preserving the grading :

$$f(\mathrm{gr}^i(D')) \subset \mathrm{gr}^i(D''), \qquad \forall i \in \mathbf{Z}.$$

Let $\mathbf{Grad}_K$ denote the category of finite-dimensional graded K-vector spaces. We remark that $\mathbf{D}_{\mathrm{HT}}(V)$ has a natural structure of a graded K-vector space:

$$\mathbf{D}_{\mathrm{HT}}(V) = \underset{i \in \mathbf{Z}}{\oplus} \mathrm{gr}^i \mathbf{D}_{\mathrm{HT}}(V), \qquad \mathrm{gr}^i \mathbf{D}_{\mathrm{HT}}(V) = \left(V \otimes_{\mathbf{Q}_p} \mathbf{C}_K t^i\right)^{G_K}.$$

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.

3.3. 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

$$V^{(i)} \simeq \mathrm{gr}^{-i}\mathbf{D}_{\mathrm{HT}}(V) \otimes_K Kt^i, \qquad\qquad x \leftrightarrow (xt^{-i}) \otimes t^i$$

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

$$\bigoplus_{i\in\mathbf{Z}} V\{i\} \to V \otimes_{\mathbf{Q}_p} \mathbf{C}_K \tag{40}$$

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 $\sum\limits_k v_k \otimes a_k \in V^{(i)}$, $\lambda \in \mathbf{C}_K$.

The following proposition shows that our definition of a Hodge–Tate representation coincides with Tate's original definition:

PROPOSITION 3.4. *i) For any representation V, the map (40) is injective.*
ii) V is a Hodge–Tate if and only if (40) is an isomorphism.

PROOF. i) By Proposition 2.3, 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 (40). Therefore (40) is injective.

ii) By Proposition 2.4, 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 (40) is. Now ii) follows from the above diagram (exercise). This proves the proposition. $\square$

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 $m_i=\dim_{\mathbf{C}_K}V\{i\}$ 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 $V\{i\}=\mathbf{C}_K(i)^{m_i}$ as a Galois module. The Hodge–Tate decomposition of V can be written in the following form:

$$V\otimes_{\mathbf{Q}_p}\mathbf{C}_K=\bigoplus_{i\in\mathbf{Z}}\mathbf{C}_K(i)^{m_i}.$$

Bibliography

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967, 349 pp.

[2] B. Bhatt, *Lecture notes for a class on perfectoid spaces* `http://www-personal.umich.edu/~bhattb/teaching/mat679w17/lectures.pdf`

[3] O. Brinon and B. Conrad, *CMI summer school notes on p-adic Hodge theory*, `http://math.stanford.edu/~conrad/papers/notes.pdf`.

[4] J.W. C. Cassels and A. Fröhlich (eds) *Algebraic Number Theory*, Thompson Book Company, 1967, 366 pages.

[5] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), pp. 129-174.

[6] J. Fresnel and M. Matignon, *Produit tensoriel topologique de corps valués*, Can. J. Math., **35**, no. 2, (1983), pp. 218-273.

[7] L. Fargues, J.-M. Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, Astérisque **406** (2018), 382 pages.

[8] 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.

[9] J.-M. Fontaine, *Le corps des périodes p-adiques*, Astérisque **223** (1994), pp. 59-102.

[10] J.-M. Fontaine, *Représentations p-adiques semistables*, Astérisque **223** (1994), pp. 113-184.

[11] O. Gabber and L. Ramero, *Almost Ring Theory*, Lecture Notes in Math. **1800** (2003), 307 pages.

[12] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, 2002

[13] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, 1986, 354 pp.

[14] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundlehren der mathematischen Wissenschaften Bd. 323, Springer, 2013.

[15] P. Scholze, *Perfectoid spaces*, Publ. math. de l'IHÉS **116** (2012), no. 1, pp. 245-313.

[16] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968.

[17] J. Tate *p-divisible groups*, Proc. Conf. Local Fields, Driebergen, 1967, pp. 158-183.