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 5

1. Non-archimedean fields 5
2. Local fields 7
3. The different 11
4. Ramification filtration 16
5. Galois groups of local fields 25
6. Ramification in $\mathbf{Z}_p$-extensions 29

Chapter 2. Almost étale extensions 33

1. Norms and traces 33
2. Deeply ramified extensions 35

Bibliography 37

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 [**2**, 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

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

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 [**6**, 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 $f(X)=\sum\limits_{i\gg -\infty} a_iX^i$. *Note that* X *is a uniformizer of* K *and* $O_K\simeq k_K[[X]]$.

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

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

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

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

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

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

□

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

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

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*

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

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

PROOF. The proof is left as an exercise. □

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

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

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

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

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

which can be explicitly described as follows. Let k/k_K be a finite extension of k_K. Write $k=k_K(\alpha)$ and denote by $f(X)\in k_K[X]$ the minimal polynomial of α. Let $\widehat{f}(X)\in O_K[X]$ denote any lift of $f(X)$. Then we associate to k the extension $L=K(\widehat{\alpha})$, where $\widehat{\alpha}$ is the unique root of $\widehat{f}(X)$ whose reduction modulo $\mathfrak{m}_L$ is α.

An easy argument using Hensel's lemma shows that L doesn't depend on the choice of the lift $\widehat{f}(X)$.

Unramified extensions form distinguished classes of extensions in the sense of [**5**]. 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.

□

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[**6**, 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 [**5**, 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 $\det\left(t_{L/K}(\omega_i,\omega_j)_{1\leqslant i,j\leqslant n}\right)$ is non-zero. Therefore the form $t_{L/K}$ is non-degenarate.

□

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 $\omega_1, \ldots, \omega_n$ be a base of L/K and let $\omega_1', \ldots, \omega_n'$ 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 $a\omega_1, \ldots, a\omega_n$ are integral over A. Let M_1 denote the A-module generated by $a\omega_1, \ldots, a\omega_n$. 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 $x_1, \ldots, x_n$ be a basis of M_2 over A. Then there exists $b \in B$ such that $bx_1, \ldots, bx_n \in B$. 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 $(B')^{-1} \subset B$. $\square$

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. □

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,

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

and therefore

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

Now we prove the theorem using formula (3).

For any polynomial $g(X) = c_0 + c_1 X + \cdots + c_k X^k$ 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

$$\frac{f(X)}{X-\alpha} = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}.$$

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

$$\mathfrak{D}_{B/A}^{-1} = \frac{1}{f'(\alpha)}\,(b_0 A + b_1 A + \cdots + b_{n-1} A).$$

To complete the proof, we only need to show that

$$b_0 A + b_1 A + \cdots + b_{n-1} A = A[\alpha]. \tag{4}$$

Since $b_i \in B$ the inclusion

$$b_0 A + b_1 A + \cdots + b_{n-1} A \subset B$$

is clear. On the other hand from the identity

$$f(X) = (b_0 + b_1 X + \cdots + b_{n-1} X^{n-1})(X - \alpha)$$

we obtain, by induction that

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

Therefore $A[\alpha] \subseteq b_0 A + b_1 A + \cdots + b_{n-1} A$, 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 [**6**, 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). □

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

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

□

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

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

PROOF. We have

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

Since g acts trivially on Teichmüller lifts, this implies that

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

This implies the assertion. □

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

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

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 [**7**, Chapitre IV, Propositions 5-7]. □

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 $x = \sum_{k=0}^{n-1} a_k \alpha^k$ 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 $g_1, g_2 \in G$,

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

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

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

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

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

and we are done. □

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

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

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 $i_{L/K}(g) = v_L(g g_1^{-1}(\alpha) - g_1^{-1}(\alpha))$ for any $g \in G$. Hence

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

□

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

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

□

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

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

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 $f(X) = \prod_{h \in H} (X - h(\alpha))$ by any lift of s in G, we obtain

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

Therefore, $(sf)(\alpha) = \prod_{g \mapsto s} (\alpha - g(\alpha))$, 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 $e(L/F)i_{F/K}(s) = \sum_{g \mapsto s} i_{L/K}(g)$ 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

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

and $\text{RHS}(u) = \varphi_{L/K}(u)$ 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

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

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

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 $u \geqslant 0$*

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

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

PROOF. i) 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

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

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

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

Setting $x = \varphi_{L/K}(u)$, 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:

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

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 [**3**, 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

$$\begin{array}{ccc} \mathrm{Gal}(K_m/K) & \xrightarrow{\sim} & \mathbf{Z}/m\mathbf{Z} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_n/K) & \xrightarrow{\sim} & \mathbf{Z}/n\mathbf{Z} \end{array}$$

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:

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

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

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

Consider the exact sequence

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

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

$$\begin{tikzcd} K^* \arrow[r, "\theta_K"] \arrow[d, "v_K"] & G_K^{\mathrm{ab}} \arrow[d] \\ \widehat{\mathbf{Z}} \arrow[r] & \mathrm{Gal}(K^{\mathrm{ur}}/K), \end{tikzcd}$$

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* [**7**] *or* [**2**, 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 [**7**, 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, $0, 1, \dots$. 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 $v_0 < v_1 < v_2 < \dots$ 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 [**8**]). *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 $v_0, v_1, \ldots, v_{n-1}$, 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.

$\square$

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

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

It's clear that the rule

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

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

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

can be written as the trace $\mathrm{Tr}_{L/K}(x_n)$ of some $x_n \in \mathfrak{m}_L^{2n}$. From (18) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n) \in \mathfrak{m}_K^s$. The lemma is proved. □

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

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

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

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

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

It's clear that the rule

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

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

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

can be written as the trace $\mathrm{Tr}_{L/K}(x_n)$ of some $x_n \in \mathfrak{m}_L^{2n}$. From (18) and Lemma 1.1 it follows that $\mathrm{Tr}_{L/K}(x_n) \in \mathfrak{m}_K^s$. The lemma is proved. □

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

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

PROOF. From Lemmas 1.1 and 1.3 if follows that

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

and it's easy to see that

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

□

2. Deeply ramified extensions

2.0.1. In this section, we review the theory of deeply ramified extensions of Coates– Greenberg [**3**]. This theory goes back to the fundamental paper of Tate [**8**], 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 [**4**], 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 $x \in \mathfrak{D}_{L_m/K_m}^{-1}$ can be written as

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

Then

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

and we have:

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

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

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

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

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

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

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

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

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

Bibliography

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

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

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

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

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

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

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

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