# LOCAL FIELDS

*by*

Laurent Berger

**Contents**

## 1. $p$-adic numbers

The field $\mathbf{R}$ of real numbers is the completion of $\mathbf{Q}$ for the usual absolute value $|\cdot|$. This absolute value (norm) is not the only one that can be defined on $\mathbf{Q}$. Let $p$ be a prime number. We have the $p$-adic valuation $\mathrm{val}_p(\cdot)$ and the $p$-adic norm $|\cdot|_p$ on $\mathbf{Q}$. The completion of $\mathbf{Q}$ for $|\cdot|_p$ is the space $\mathbf{Q}_p$ of $p$-adic numbers. It is a complete normed field which contains $\mathbf{Q}$ as a dense subset. If $x$, $y \in \mathbf{Q}_p$ then $|x+y|_p \leq \max(|x|_p, |y|_p)$. The set $\mathbf{Z}_p = \{x \in \mathbf{Q}_p \text{ such that } |x|_p \leq 1\}$ of integers of $\mathbf{Q}_p$ is therefore a ring, and $\mathbf{Q}_p = \mathbf{Z}_p[1/p]$.

***Proposition 1.1***. — *The ring $\mathbf{Z}_p$ is the completion of $\mathbf{Z}$ for $|\cdot|_p$.*

*Proof.* — Take $x \in \mathbf{Z}_p$, $x = \lim x_n$ with $x_n \in \mathbf{Q}$. Assume that $|x - x_n|_p \leq p^{-n}$ for $n \geq 1$. We have $|x_n|_p \leq 1$ for $n \geq 1$ so that $x_n = a_n/b_n$ with $p \nmid b_n$. Let $c_n \in \mathbf{Z}$ be such that $b_n c_n \equiv 1 \bmod p^n$. We have $|x - a_n c_n|_p \leq p^{-n}$. □

The ring $\mathbf{Z}_p$ contains $\mathbf{Z}$, as well as any rational number $a/b$ with $p \nmid b$. If $n \in \mathbf{Z}$ and $k \geq 1$, we have $\binom{n}{k} \in \mathbf{Z}$ and $n \mapsto \binom{n}{k}$ is uniformly continuous (it is a polynomial) hence it extends to a map $a \mapsto \binom{a}{k}$ from $\mathbf{Z}_p \to \mathbf{Z}_p$. If $z \in p\mathbf{Z}_p$, then the function $a \mapsto (1+z)^a = \sum_{k \geq 0} \binom{a}{k} z^k$ is continuous and $(1+z)^a \cdot (1+z)^b = (1+z)^{a+b}$. For example, if $p \nmid 2$, then $(1+z)^{1/2}$ is the unique square root of $1+z$ that is congruent to 1 mod $p$. For example, $\sqrt{-5} \in \mathbf{Z}_3$.

The field $\mathbf{Q}_p$ is an example of a complete normed field. We will study the general properties of these objects. Before we do that, let us mention the following result of Ostrowski. We say that a norm is ultrametric if $|x+y| \leq \max(|x|, |y|)$.

***Theorem 1.2***. — *If $|\cdot|$ is a nontrivial ultrametric norm on $\mathbf{Q}$, then $|\cdot|$ is equivalent to $|\cdot|_p$ for some prime number $p$.*

*Proof.* — By induction, we see that $|m| \leq 1$ for all $m \in \mathbf{Z}$. If the norm is nontrivial, there is a prime number $p$ such that $|p| < 1$. If $m \wedge p = 1$, then we can write $px + my = 1$ and hence $|m| = 1$. This implies that $|p^n m_0| = |p|^n$ if $p \nmid m_0$, so that there exists $c$ such that $|\cdot| = |\cdot|_p^c$. □

## 2. Complete normed fields

Let $K$ be a field and let $|\cdot|$ be a nontrivial ultrametric norm on $K$, for which $K$ is complete. If $a > 1$ and if we let $\mathrm{val}(x) = -\log_a |x|$, then $\mathrm{val}(\cdot)$ is a valuation on $K$, so we can talk interchangeably about either norms or valuations. Given such a field $K$, note that (1) if $x = x_1 + \cdots + x_n$ and $|x_i| \neq |x_j|$ whenever $i \neq j$, then $|x| = \max |x_i|$, (2) if

$x \neq 0$ and $x = \lim x_n$, then $|x_n| = |x|$ for $n \gg 0$, (3) a series $\sum_{n\geq 1} x_n$ converges if and only if $x_n \to 0$,

Let $\mathcal{O}_K = \{x \in K \text{ such that } |x| \leq 1\}$ be the ring of integers of $K$, and let $\mathfrak{m}_K = \{x \in K \text{ such that } |x| < 1\}$. If $|x| = 1$, then $|x^{-1}| = 1$ so that $\mathcal{O}_K = \mathcal{O}_K^\times \sqcup \mathfrak{m}_K$ and therefore $\mathcal{O}_K$ is a local ring whose maximal ideal is $\mathfrak{m}_K$. Let $k_K = \mathcal{O}_K/\mathfrak{m}_K$ be the residue field of $K$.

There exists $\pi \in \mathfrak{m}_K$ such that $\mathfrak{m}_K = \pi\mathcal{O}_K$ if and only if $\mathrm{val}(K^\times)$ is a discrete subgroup of $\mathbf{R}$, ie if $\mathrm{val}(K^\times) = c \cdot \mathbf{Z}$. We can then take for $\pi$ any $\pi$ such that $\mathrm{val}(\pi) = c$. Such an element is called a uniformizer of $\mathcal{O}_K$. We then let $\mathrm{val}_K$ be normalized by $\mathrm{val}_K(\pi) = 1$.

We say that a complete discretely valued field is a local field. For example if $K = \mathbf{Q}_p$ we can take $\pi = p$; in this case, $\mathfrak{m}_{\mathbf{Q}_p} = p\mathbf{Z}_p$ and $k_{\mathbf{Q}_p} = \mathbf{Z}/p\mathbf{Z}$. If $k$ is any field and $K = k(\!(X)\!)$ and $\mathrm{val} = \mathrm{val}_X$, we can take $\pi = X$. If $K = \cup_{n\geq 1}\mathbf{C}(\!(X^{1/n!})\!)$ (Puiseux series), and $\mathrm{val} = \mathrm{val}_X$, then $K$ is not discretely valued.

***Proposition 2.1***. — *If $K$ is a local field, then $\mathcal{O}_K$ is a PID. Actually, any nontrivial ideal of $\mathcal{O}_K$ is of the form $\mathfrak{m}_K^n$ for some $n \geq 1$.*

***Proposition 2.2***. — *Let $K$ be a local field, let $S$ be a system of representatives of $k$ in $\mathcal{O}_K$ and let $\{\pi_n\}_{n\geq 0}$ be a sequence of elements of $\mathcal{O}_K$ with $\mathrm{val}_K(\pi_n) = n$. Every $x \in \mathcal{O}_K$ can be written as $x = \sum_{n\geq 0} x_n\pi_n$ with $x_n \in S$, in one and only one way.*

*Proof.* — Let $s : \mathcal{O}_K \to S$ be the map such that $\overline{s(x)} = \overline{x}$. Let $x_0 = s(x/\pi_0)$. We have $x = x_0\pi_0 + y_1\pi_1$. Assume that we can write $x = x_0\pi_0 + \cdots + x_n\pi_n + y_{n+1}\pi_{n+1}$. We can take $x_{n+1} = s(y_{n+1})$ and then $x = \sum_{n\geq 0} x_n\pi_n$. At each step, $x_n$ is determined. □

Every element of $\mathbf{Z}_p$ can therefore be written as $\sum_{n\geq 0} x_n p^n$ with $x_n \in \{0, \ldots, p-1\}$.

***Proposition 2.3***. — *The map $\mathcal{O}_K \to \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ is an isomorphism.*

*Proof.* — It is injective because if $x \mapsto 0$, then $|x| = 0$. If $(\overline{x_n})_{n\geq 1} \in \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ and $x_n \in \mathcal{O}_K$ lifts $\overline{x_n}$, then $(x_n)_{n\geq 1}$ is Cauchy, and hence converges to $x \in \mathcal{O}_K$, which lifts $(\overline{x_n})_{n\geq 1}$. □

***Corollary 2.4***. — *If $K$ is a local field and $k$ is finite, then $\mathcal{O}_K$ is compact.*

This is the case for $K = \mathbf{Q}_p$ and for $K = k(\!(X)\!)$ if $k$ is finite. In general, $K$ is a totally disconnected topological space.

## 3. Hensel's lemma

Let $A$ be a ring and consider $P(X) = a_d X^d + \cdots + a_0 \in A[X]$. For $i \geq 0$, let

$$P^{[i]}(X) = \binom{d}{i} a_d X^{d-i} + \cdots + \binom{i}{i} a_i \in A[X].$$

The following formula holds

$$P(X+Y) = P(X) + Y \cdot P^{[1]}(X) + Y^2 \cdot P^{[2]}(X) + \cdots + Y^d \cdot P^{[d]}(X).$$

Note that if $i!$ is invertible in $A$, then $P^{[i]}(X) = P^{(i)}(X)/i!$. Let $K$ be a complete normed field. The following result is (one of many results) known as Hensel's lemma.

***Theorem 3.1***. — *If $P(X) \in \mathcal{O}_K[X]$ and $\lambda < 1$ and $\alpha_0 \in \mathcal{O}_K$ is such that $|P(\alpha_0)| \leq \lambda |P'(\alpha_0)|^2$, there exists a unique $\alpha \in \mathcal{O}_K$ such that $P(\alpha) = 0$ and $|\alpha - \alpha_0| \leq \lambda |P'(\alpha_0)|$.*

*Proof.* — Let $C = \{x \text{ such that } |x - \alpha_0| \leq \lambda |P'(\alpha_0)|\}$. We have $P'(\alpha_0 + h) \in P'(\alpha_0) + h\mathcal{O}_K$ so that $|P'(x)| = |P'(\alpha_0)|$ if $x \in C$. Define a sequence $\{\alpha_n\}_{n \geq 0}$ by $\alpha_{n+1} = \alpha_n - P(\alpha_n)/P'(\alpha_n)$. We claim that $|P(\alpha_n)| \leq \lambda^{2^n} |P'(\alpha_0)|^2$. It is true for $n = 0$ and

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

which implies the claim. This implies that $\{\alpha_n\}_{n \geq 1}$ is a Cauchy sequence in $C$ and its limit $\alpha$ has the required properties.

If $\alpha$, $\beta$ satisfy the conclusion of the theorem, then $P(\beta) = P(\alpha) + (\beta - \alpha) P'(\alpha) + (\beta - \alpha)^2 h$ with $h \in \mathcal{O}_K$ so that if $\alpha \neq \beta$, then $P'(\alpha) \in (\beta - \alpha)\mathcal{O}_K \subset (\alpha - \alpha_0)\mathcal{O}_K$, contradiction. □

The theorem applies in particular when $|P'(\alpha_0)| = 1$, ie when $\overline{\alpha_0}$ is a simple root of $\overline{P(X)}$ in $k_K[X]$. For instance $P(X) = X^{p-1} - 1$ has $p-1$ simple roots in $\mathbf{F}_p$ so that it has $p-1$ roots in $\mathbf{Z}_p$. We therefore have $\mu_{p-1} \subset \mathbf{Z}_p$.

***Theorem 3.2***. — *If $K$ is a local field of characteristic $p$ with uniformizer $\pi$ and finite residue field $k$, then $K = k(\!(\pi)\!)$.*

*Proof.* — Let $q = \mathrm{card}(k)$. By theorem 3.1, $X^q - X = 0$ has $q$ solutions in $\mathcal{O}_K$ so that the map $\mathcal{O}_K \to k$ has a canonical section and $k \subset \mathcal{O}_L$. The theorem now follows from proposition 2.2. □

If $K$ is of mixed characteristic and $k$ is finite, then in proposition 2.2 we can take for $S$ the solutions of $X^q - X$, but the addition laws are very complicated.

## 4. Extending the norm

Let $K$ be a complete normed field. If $|\cdot|_1$ and $|\cdot|_2$ are two norms on $K$, we say that they are equivalent if they define the same topology on $K$.

***Proposition 4.1***. — *If $|\cdot|_1$ and $|\cdot|_2$ are two norms on $K$, they are equivalent if and only if there exists $\alpha > 0$ such that $|\cdot|_2 = |\cdot|_1^\alpha$.*

*Proof.* — If there is $\alpha > 0$ such that $|\cdot|_2 = |\cdot|_1^\alpha$, then $|\cdot|_1$ and $|\cdot|_2$ are clearly equivalent. Assume that $|\cdot|_1$ and $|\cdot|_2$ are equivalent. If $y \in K$, then $y^n \to 0$ if and only if $|y| < 1$ and hence $|y|_1 < 1$ if and only if $|y|_2 < 1$. Fix $y \in K$ such that $|y|_1 \neq 1$; if $x \in K$, then $|x^m y^{-n}|_1 < 1$ if and only if $|x^m y^{-n}|_2 < 1$ and hence $|x|_1 < |y|_1^{n/m}$ if and only if $|x|_2 < |y|_2^{n/m}$. We find that if $s \in \mathbf{R}$, then $|x|_1 = |y|_1^s$ if and only if $|x|_2 = |y|_2^s$ so that if $|y|_2 = |y|_1^\alpha$, then $|x|_2 = |x|_1^\alpha$ for all $x \in K$. □

***Theorem 4.2***. — *If $V$ is a finite dimensional $K$-vector space, then all norms on $V$ are equivalent, and $V$ is complete for any of them.*

*Proof.* — Let $e_1, \ldots, e_d$ be a basis of $V$ and let $\|\cdot\|_\infty$ be the corresponding sup norm (for which $V$ is indeed complete). We'll show by induction on $\dim(V)$ that any norm $\|\cdot\|$ on $V$ is equivalent to $\|\cdot\|_\infty$. If $d = 1$, this is obvious. We also have $\|x_1 e_1 + \cdots + x_d e_d\| \leq \sup|x_i| \cdot \sup\|e_i\|$ so that $\|x\| \leq C\|x\|_\infty$ with $C = \sup\|e_i\|$.

Let us show that there exists $D$ such that $\|x\|_\infty \leq D\|x\|$ for all $x$. If not, there is a sequence $\{u_n\}_{n\geq 1}$ with $\|u_n\|_\infty \geq 1$ but $\|u_n\| \to 0$. Write $u_n = x_1^{(n)} e_1 + \cdots + x_d^{(n)} e_d$. For each $n$, one of the $|x_i^{(n)}|$ is $\geq 1$ and we can assume that $|x_1^{(n)}| \geq 1$ for all $n$. Let $v_n = u_n / x_1^{(n)} = e_1 + \cdots$ and let $W = \mathrm{Span}(e_2, \ldots, e_d)$. We have $\|v_n\| \to 0$ so that the sequence $\{v_n - e_1\}_{n\geq 1}$ is Cauchy in $W$. By induction, $W$ is complete for $\|\cdot\|$, so there exists $w \in W$ such that $v_n \to e_1 + w$, so that $e_1 \in W$, impossible. □

***Corollary 4.3***. — *If $K$ is a complete normed field, and $L$ is a finite extension of $K$, then the norm on $K$ has at most one extension to $L$.*

*Proof.* — Let $|\cdot|$ be one such norm. The field $L$ is a finite dimensional $K$-vector space, so by theorem 4.2 all the norms on $L$ are equivalent to $|\cdot|$. By proposition 4.1 applied to $L$, they are of the form $|\cdot|^\alpha$ and since they coincide on $K$, they are equal. □

***Theorem 4.4***. — *If $K$ is a local field and $L/K$ is a finite extension, the norm on $K$ extends to a norm on $L$. The normed field $L$ is also a local field.*

*Proof.* — Assume first that $L/K$ is separable. Let $A$ be the integral closure of $\mathcal{O}_K$ in $L$. By the same reasoning as in the number field case, $A$ is a finite $\mathcal{O}_K$-module, hence a Dedekind domain. Let $\pi$ be a uniformizer of $\mathcal{O}_K$. The ideal $\pi A$ is a product $P_1^{e_1} \cdots P_r^{e_r}$. Let $\mathrm{val}_K$ denote the valuation normalized by $\mathrm{val}_K(\pi) = 1$. For each $i$, let $\mathrm{val}_i(\cdot)$ be the function on $A$ defined by: $\mathrm{val}_i(x)$ is the exponent of $P_i$ in the decomposition of $xA$. The function $\mathrm{val}_i(\cdot)/e_i$ extends $\mathrm{val}_K$. Since $\mathrm{Frac}(A) = L$, this gives an extension of $\mathrm{val}_K$ to $L$.

If $L/K$ is purely inseparable, then there exists $q$ such that if $x \in L$, then $x^q \in K$ and then we can set $|x| = |x^q|^{1/q}$. This finishes the extension of the norm.

The field $L$ is complete by theorem 4.2. □

***Corollary 4.5***. — *If $L/K$ is finite Galois and $g \in \mathrm{Gal}(L/K)$, then $g$ is an isometry.*

If $K^{\mathrm{alg}}$ denotes an algebraic closure of $K$, the norm on $K$ extends uniquely to $K^{\mathrm{alg}}$.

## 5. Finite extensions

By the preceding section, if $K$ is a local field and $L/K$ is a finite extension of degree $d$, then $L$ is also a complete normed field. If $x \in L^\times$, then $\mathrm{N}_{L/K}(x) \in K^\times$ and $|\mathrm{N}_{L/K}(x)| = |x|^d$ so that $e = e(L/K) = [\mathrm{val}(L^\times) : \mathrm{val}(K^\times)]$ divides $d$, and $L$ is a local field.

If $x_1, \ldots, x_g$ are elements of $\mathcal{O}_L$ whose images in $k_L$ are linearly independent over $k_K$, then $x_1, \ldots, x_g$ are linearly independent over $K$ in $L$, and hence $k_L$ is a finite extension of $k_K$. Let $f = f(L/K) = [k_L : k_K]$.

***Theorem 5.1***. — *Let $\{u_i\}_{1 \leq i \leq f}$ be elements of $\mathcal{O}_L$ whose images give a basis of $k_L$ over $k_K$ and let $\pi$ be a uniformizer of $\mathcal{O}_L$. We have $\mathcal{O}_L = \oplus_{1 \leq i \leq f, 0 \leq j \leq e-1} u_i \pi^j \cdot \mathcal{O}_K$.*

*Proof.* — Let $S_K$ be a set of representatives of $k_K$ in $\mathcal{O}_K$ and let $S_L = \sqcup_{1 \leq i \leq f} u_i S_K$, which is a set of representatives of $k_L$ in $\mathcal{O}_L$. Let $\pi_K$ be a uniformizer of $\mathcal{O}_K$. If $n \geq 0$, write $n = q(n)e + r(n)$. The theorem follows from applying proposition 2.2 with $\pi_n = \pi^{r(n)} \pi_K^{q(n)}$. □

***Corollary 5.2***. — *We have $ef = d$, and $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $d$.*

*Proof.* — By the theorem, $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $ef$, so that $[L : K] = d$. □

Note that $e(L/F) = e(L/K)e(K/F)$ and $f(L/F) = f(L/K)f(K/F)$.

***Corollary 5.3***. — *If $k_K$ is finite, then there exists $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$.*

*Proof.* — Note that if $x \in \mathcal{O}_L$, then $\mathcal{O}_K[x]$ is closed in $\mathcal{O}_L$. Let $q = \mathrm{card}(k_L)$. Take $y \in \mathcal{O}_L$ whose image is a primitive element for $k_L/k_K$ and such that $y^q = y$. Theorem

5.1 implies that $\mathcal{O}_L = \mathcal{O}_K[y, \pi_L]$. Let $x = y + \pi_L$. We have $x^{q^n} \to y$ so that $y \in \mathcal{O}_K[x]$ and therefore $\pi_L \in \mathcal{O}_K[x]$ as well. □

We say that $L/K$ is unramified if $e(L/K) = 1$, and totally ramified if $f(L/K) = 1$.

***Proposition 5.4***. — *If $L/K$ is totally ramified and $\pi_L$ is a uniformizer of $\mathcal{O}_L$, then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ and $\pi_L$ satisfies an Eisenstein polynomial over $\mathcal{O}_K$.*

*Proof.* — If $L/K$ is totally ramified, then $k_L = k_K$ and theorem 5.1 implies that $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Let $\mathrm{val} = \mathrm{val}_K$ so that $\mathrm{val}(\pi_L) = 1/e$. If $x = a_0 + a_1\pi_L + \cdots + a_{e-1}\pi_L^{e-1}$, then $\mathrm{val}(x) = \min \mathrm{val}(a_i\pi_L^i)$ as the vals are pairwise distinct. Hence if $\pi_L^e = a_0 + a_1\pi_L + \cdots + a_{e-1}\pi_L^{e-1}$, then $\mathrm{val}(a_0) = \mathrm{val}(\pi_L^e) = \mathrm{val}(\pi_K)$ so that $\pi_L$ satisfies an Eisenstein equation. □

Conversely, if $P(X) \in \mathcal{O}_K[X]$ is an Eisenstein polynomial, and $P(\pi_L) = 0$, then $\pi_L$ is a uniformizer of $L = K(\pi_L)$, which is totally ramified over $K$.

***Proposition 5.5***. — *If $k_L/k_K$ is separable, there exists a unique subextension $L_0$ such that $L_0/K$ is unramified and $L/L_0$ is totally ramified.*

*Proof.* — Take $\overline{y}$ such that $k_L = k_K(\overline{y})$, and let $P(X) \in \mathcal{O}_K[X]$ be a monic lift of its minimal polynomial. By Hensel's lemma, there is a $y \in \mathcal{O}_L$ that lifts $\overline{y}$ with $P(y) = 0$. The extension $K(y)/K$ is of degree $\leq \deg(P)$ and $[k_{K(y)} : k_K] = \deg(P)$ so that $K(y)/K$ is unramified, and $L/K(y)$ is totally ramified. We can take $L_0 = K(y)$.

If $L_0'$ is another such subextension, then the above contruction of $y$ shows that $y \in L_0'$ so that $L_0' = L_0$. □

***Proposition 5.6***. — *If $k_K$ is finite and $q = \mathrm{card}(k_K)$ and $f \geq 1$, then $K$ has exactly one unramified extension of degree $f$, namely $K(\mu_{q^f-1})$.*

*Proof.* — If $L/K$ is unramified of degree $f$, then $[k_L : k_K] = f$ so that $k_L = \mathbf{F}_{q^f}$ and $L = K(\mu_{q^f-1})$ by Hensel's lemma. □

## 6. Newton polygons

The theory of Newton polygons allows us to compute the valuations of the roots of a polynomial from the valuations of its coefficients. Let $K$ be a local field, and choose a valuation $\mathrm{val}(\cdot)$, which then extends to $K^{\mathrm{alg}}$.

If $P(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$, then the Newton polygon $\mathrm{NP}(P)$ is the lower convex hull of the points $(0, \mathrm{val}(a_0))$, $(1, \mathrm{val}(a_1))$, …, $(d, \mathrm{val}(a_d))$. The Newton polygon $\mathrm{NP}(P)$ is therefore a finite union of segments of increasing slopes, starting at $(0, \mathrm{val}(a_0))$

and finishing at $(d, \mathrm{val}(a_d))$. The first segment can possibly be of slope $-\infty$ (if $a_0 = 0$). A slope of $\mathrm{NP}(P)$ is the slope of one of these segments, and the length of a segment is the length of its component along the $x$-axis.

***Theorem 6.1***. — *If $P(X) \in K[X]$, then the number of roots of $P$ in $K^{\mathrm{alg}}$ with valuation $\lambda$ is equal to the length of the segment of $\mathrm{NP}(P)$ with slope $-\lambda$.*

*Proof.* — We can divide $P(X)$ by $a_d$ and assume that $P(X)$ is monic. Assume that $P$ has $d_1$ roots of valuation $\lambda_1$ and $d_2$ roots of valuation $\lambda_2$, etc, $d_k$ roots of valuation $\lambda_k$ with $\lambda_1 > \cdots > \lambda_k$. The coefficient $a_i$ is $\pm$ the sum of all possible products of $d-i$ roots. In particular, $a_{d_1+\cdots+d_{s-1}}$ is the sum of a term of valuation $d_s\lambda_s + \cdots + d_k\lambda_k$ and of terms which are all of valuation $> d_s\lambda_s + \cdots + d_k\lambda_k$ so that

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

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

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

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

***Proposition 6.2***. — *If $P(X) \in K[X]$ is irreducible, then all its roots have the same valuation.*

*Proof.* — Let $P$ be irreducible and let $L = K[X]/P$. This is a field, which can be embedded in $K^{\mathrm{alg}}$ by $X \mapsto \alpha$ for each root $\alpha$ of $P$. If two roots had different norms, this would give two different norms on $L$, which would contradict corollary 4.3. □

***Corollary 6.3***. — *If $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ is irreducible and $a_0 \in \mathcal{O}_K$, then $a_i \in \mathcal{O}_K$ for all $i$.*

***Proposition 6.4***. — *Assume that $\mathrm{val}(K^\times) \subset \mathbf{Z}$. If $\mathrm{NP}(P)$ has only one slope, $a/b$ in lowest terms, then $b$ divides $\deg(P)$ and if $b = \deg(P)$, then $P$ is irreducible.*

*Proof.* — We have $\lambda = \mathrm{val}(P(0))/\deg(P)$ so that $b \mid \deg(P)$. If $P = QR$ is reducible, all the roots of $Q$ and $R$ have the same valuation so $\mathrm{NP}(Q)$ has one slope $\mathrm{val}(Q(0))/\deg(Q)$, hence $\deg(Q) = \deg(P)$. □

***Corollary 6.5***. — *An Eisenstein polynomial is irreducible.*

## 7. The field $\mathbf{C}_p$

Let $\overline{\mathbf{Q}}_p$ denote an algebraic closure of $\mathbf{Q}_p$.

***Theorem 7.1***. — *If $d \geq 1$, then $\mathbf{Q}_p$ has only finitely many extensions of degree $d$.*

For example, if $d = 2$, then every quadratic extension of $\mathbf{Q}_p$ is of the form $\mathbf{Q}_p(\sqrt{y})$ and we need to show that $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ is finite, which is easy, given the following result.

***Lemma 7.2***. — *If $p \neq 2$, then $\mathbf{Q}_p^\times = p^{\mathbf{Z}} \times \mu_{p-1} \times (1 + p\mathbf{Z}_p)$; for $p = 2$, $\mathbf{Q}_2^\times = 2^{\mathbf{Z}} \times \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$.*

The result below is known as Krasner's lemma.

***Theorem 7.3***. — *If $F$ is a finite extension of $\mathbf{Q}_p$ and if $\alpha$, $\beta \in \overline{\mathbf{Q}}_p$ are such $|\alpha - \beta| < |\alpha - \alpha_i|$ for $i = 2, \ldots, n$ where the $\alpha_i$ are the conjugates of $\alpha$ over $F$ (with $\alpha_1 = \alpha$), then $F(\alpha) \subset F(\beta)$.*

*Proof.* — Let $K$ be a finite Galois extension of $F$ containing $\alpha$ and $\beta$, and take $\sigma \in \mathrm{Gal}(K/F(\beta))$. We have $|\sigma(\alpha) - \alpha| \leq \max(|\sigma(\alpha) - \sigma(\beta)|, |\alpha - \beta|) = |\alpha - \beta|$. If $\sigma(\alpha) \neq \alpha$, then $|\alpha - \beta| < |\sigma(\alpha) - \alpha|$, a contradiction. Hence $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(K/F(\beta))$ and so $\alpha \in F(\beta)$. □

If $P(X) = a_0 + \cdots + a_d X^d \in F[X]$, let $|P|_G = \max |a_i|$. The lemma below follows from the continuity of the roots of a polynomial in terms of the coefficients.

***Lemma 7.4***. — *If $P(X) \in F[X]$ is monic of degree $d$ with no double root and $\varepsilon > 0$, then there exists $\delta > 0$ such that : if $Q(X) \in F[X]$ is monic of degree $d$ with $|P - Q|_G < \delta$, then for each root $x$ of $P$ in $\overline{\mathbf{Q}}_p$ there exists a root $y$ of $Q$ such that $|x - y| < \varepsilon$.*

*Proof of theorem 7.1.* — If $K$ is an extension of $\mathbf{Q}_p$ of degree $d$ and $K_0$ is the maximal unramified subextension of $K$, then $K_0 = \mathbf{Q}_p(\mu_{p^f-1})$ with $f \mid d$ and so it is enough to prove that if $F$ is a finite extension of $\mathbf{Q}_p$ and $e \geq 1$, then $F$ has only finitely many totally ramified extensions of degree $e$.

Given an $e$-tuple $a = \{a_0, \ldots, a_{e-1}\} \in \Pi = (\mathfrak{m}_F \setminus \mathfrak{m}_F^2) \times \mathfrak{m}_F^{e-1}$, one can attach to it the $e$ extensions of $F$ generated by the $e$ roots of the Eisenstein polynomial $P(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$, and by proposition 5.4, all totally ramified extensions of $F$ arise this way.

An Eisenstein polynomial is irreducible, and so has no double roots. We can therefore apply lemma 7.4 with $\varepsilon < \min(\alpha_i - \alpha_j)$ where the $\{\alpha_i\}$ are the roots of $P(X)$. If $b \in \Pi$ is another $e$-tuple such that $|a_i - b_i| < \delta$, then the polynomial $Q(X)$ attached to $b$ has

$e$ roots $\{\beta_i\}$ that we can reorder so that $|\beta_i - \alpha_i| < \varepsilon$. Theorem 7.3 now implies that $F(\beta_i) = F(\alpha_i)$ and therefore that in an open neighborhood of $a \in \Pi$, the $e$ extensions of $F$ attached to $b$ are the same. Since $\Pi$ is compact, the theorem follows. □

***Corollary 7.5***. — *The field $\overline{\mathbf{Q}}_p$ is not complete.*

*Proof.* — The theorem implies that $\overline{\mathbf{Q}}_p$ is an extension of $\mathbf{Q}_p$ of countable degree, and so cannot be complete by Baire's theorem. □

We let $\mathbf{C}_p$ denote the $p$-adic completion of $\overline{\mathbf{Q}}_p$.

***Theorem 7.6***. — *The field $\mathbf{C}_p$ is algebraically closed.*

*Proof.* — Let $P(X) \in \mathbf{C}_p[X]$ be a monic polynomial of degree $d$. We can replace $P(X)$ by $p^{kd}P(p^{-k}X)$ for $k \gg 0$, and assume that the coefficients of $P(X)$ have norm $\leq 1$. For $n \geq 1$, let $P_n(X) \in \overline{\mathbf{Q}}_p[X]$ be a monic polynomial of degree $d$ such that $|P - P_n|_p \leq p^{-n}$. The coefficients of $P_n(X)$ are all of norm $\leq 1$, and the theory of Newton polygons implies that the roots of $P_n(X)$ are all of norm $\leq 1$.

Define by induction a sequence $(a_n)$ of $\overline{\mathbf{Q}}_p$: $a_0$ is any root of $P_0(X)$ and if $a_n$ is a root of $P_n(X)$, define $a_{n+1}$ as follows. We have $|P_{n+1}(a_n)|_p = |(P_{n+1} - P_n)(a_n)|_p \leq p^{-n}$ (as $|a_n|_p \leq 1$). There is therefore at least one root $a_{n+1}$ of $P_{n+1}(X)$ such that $|a_n - a_{n+1}|_p \leq p^{-n/d}$. The sequence $(a_n)$ thus defined is Cauchy in $\overline{\mathbf{Q}}_p$ and converges to some $a$ in $\mathbf{C}_p$. As $P(a_n) \to 0$, we have $P(a) = 0$. □

The field $\mathbf{C}_p$ is the smallest complete and algebraically closed field containing $\mathbf{Q}_p$. It is known as the field of $p$-adic complex numbers. We have $\mathrm{val}_p(\mathbf{C}_p^\times) = \mathbf{Q}$. The ring $\mathcal{O}_{\mathbf{C}_p}$ is the $p$-adic unit disk, $\mathfrak{m}_{\mathbf{C}_p}$ is the $p$-adic open unit disk, and $\mathcal{O}_{\mathbf{C}_p}/\mathfrak{m}_{\mathbf{C}_p} = \overline{\mathbf{F}}_p$.

## 8. The ramification filtration

In this section, $L/K$ is a finite Galois extension of local fields, with $k_K$ of characteristic $p$ and $k_L/k_K$ separable (and hence Galois), and $\mathrm{val}_L$ is the valuation on $L^\times$ normalized by $\mathrm{val}_L(L^\times) = \mathbf{Z}$. If $g \in \mathrm{Gal}(L/K)$, let $i_L(g) = \inf_{a \in \mathcal{O}_L} \mathrm{val}_L(g(a) - a)$. Note that if $x \in \mathcal{O}_L$ is such that $\mathcal{O}_L = \mathcal{O}_K[x]$, then $i_L(g) = \mathrm{val}_L(g(x) - x)$.

***Proposition 8.1***. — *If $g$, $h \in \mathrm{Gal}(L/K)$, then*

1. $i_L(ghg^{-1}) = i_L(h)$;
2. $i_L(gh) \geq \min(i_L(g), i_L(h))$ *with equality if* $i_L(g) \neq i_L(h)$;
3. $i_L(g) = i_L(g^{-1})$.

*Proof.* — If $\mathcal{O}_L = \mathcal{O}_K[x]$, then $\mathcal{O}_L = \mathcal{O}_K[g^{-1}(x)]$ and hence

$$i_L(ghg^{-1}) = \mathrm{val}_L(ghg^{-1}(x) - x) = \mathrm{val}_L(hg^{-1}(x) - g^{-1}(x)) = i_L(h)$$

which shows (1). Next, $i_L(gh) = \mathrm{val}_L(gh(x) - x) = \mathrm{val}_L(gh(x) - h(x) + h(x) - x)$ which implies (2), and (3) is clear. □

If $G = \mathrm{Gal}(L/K)$ and $u \geq -1$, let $G_u = \{g \in G \text{ such that } i_L(g) \geq u+1\}$. Proposition 8.1 implies that $G_u$ is a normal subgroup of $G$. We have $G_{-1} = G$ and if $u \geq \max_{g \neq 1} i_L(g)$, then $G_u = \{1\}$. Let $L_0$ be the maximal unramified subsextension of $L/K$ as in prop 5.5.

***Lemma 8.2***. — *The group $G_0$ is the inertia subgroup $I(L/K)$ of $G$, and $L_0 = L^{G_0}$.*

*Proof.* — By definition, $I(L/K) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K))$ and it is therefore the set of $g \in G$ such that $g(a) - a \in \mathfrak{m}_L$ for all $a \in \mathcal{O}_L$, that is $G_0$.

In the notation of the proof of proposition 5.5, we have $L_0 = K(y)$ where $y$ is the unique root of $P$ lifting $\overline{y}$. If $g \in G_0$, then $g(y)$ is also a root of $P$ lifting $\overline{y}$, so that $g(y) = y$ and $L_0 \subset L^{G_0}$. By comparing degrees, we get $L_0 = L^{G_0}$. □

If $\pi_L$ is a uniformizer of $L$, then $L = L_0[\pi_L]$ so that $i_L(g) = \mathrm{val}_L(g(\pi_L)/\pi_L - 1) + 1$ if $g \in G_0$. Hence if $u \geq 0$, then $G_u = \{g \in G_0 \text{ such that } \mathrm{val}_L(g(\pi_L)/\pi_L - 1) \geq u\}$.

***Lemma 8.3***. — *If $u \in \mathbf{Z}_{\geq -1}$ then $G_u^p \subset G_{u+1}$.*

*Proof.* — If $g \in G_u$ then we can write $g(\pi_L)/\pi_L = 1 + \alpha$ with $\alpha \in \mathfrak{m}_L^u$ and

$$\frac{g^p(\pi_L)}{\pi_L} = \frac{g(\pi_L)}{\pi_L}\frac{g^2(\pi_L)}{g(\pi_L)} \cdots \frac{g^p(\pi_L)}{g^{p-1}(\pi_L)} = (1+\alpha)(1+g(\alpha)) \cdots (1+g^{p-1}(\alpha))$$

Since $g \in G_u$ we have $g(\alpha) - \alpha \in \mathfrak{m}_L^{u+1}$ and hence $g^p(\pi_L)/\pi_L \equiv 1 + p\alpha \equiv 1 \bmod \mathfrak{m}_L^{u+1}$ so that $g^p \in G_{u+1}$. □

***Proposition 8.4***. — *The group $G_1$ is the unique $p$-Sylow subgroup of $G_0$.*

*Proof.* — Lemma 8.3 above shows that $G_1^{p^n} \subset G_{1+n}$ and hence that $G_1^{p^n} = \{1\}$ if $n \gg 0$ which shows that $G_1$ is a $p$-group. We now show that for each $g \in G_0$ such that $g^p \in G_1$, we have $g \in G_1$ so that every element whose order is a power of $p$ is in $G_1$.

If $g$ is such an element, we can write $g(\pi_L)/\pi_L = \alpha \in \mathcal{O}_L^\times$ and since $G_0$ is the inertia subgroup of $G$, we have $g(\alpha) \equiv \alpha \bmod \mathfrak{m}_L$. This implies that $g^p(\pi_L)/\pi_L \equiv 1 \bmod \mathfrak{m}_L$ if and only if $\alpha^p \equiv 1 \bmod \mathfrak{m}_L$, that is if and only if $\alpha \equiv 1 \bmod \mathfrak{m}_L$. □

If $L/K$ is a totally ramified extension, we say that it is tamely ramified if $p \nmid e(L/K)$.

***Proposition 8.5***. — *If $L/K$ is a totally ramified Galois extension, and if we write $e = e(L/K) = p^k n$ with $p \nmid n$, then there is a unique subextension $L_1$ such that $[L_1 : K] = n$.*

*Proof.* — By Galois theory, we have $L_1 = L^{G_1}$. □

More generally, the ramification filtration on $\mathrm{Gal}(L/K)$ gives a tower of subextensions $K \subset L_0 \subset L_1 \subset \cdots \subset L$ where ramification becomes increasingly complicated.

***Proposition 8.6***. — *If $u \in \mathbf{Z}_{\geq 0}$, then the map $g \mapsto g(\pi_L)/\pi_L$ induces an injective group homomorphism $G_u/G_{u+1} \to 1 + \mathfrak{m}_L^u/1 + \mathfrak{m}_L^{u+1}$.*

*Proof.* — If $g(\pi_L)/\pi_L = 1 + \alpha_g$ and $h(\pi_L)/\pi_L = 1 + \alpha_h$, with $\alpha_g$, $\alpha_h \in \mathfrak{m}_L^u$, then $g(\alpha_h) = \alpha_h \bmod \mathfrak{m}_L^{u+1}$, so that:

$$\frac{gh(\pi_L)}{\pi_L} = (1 + g(\alpha_h))(1 + \alpha_g) = (1 + \alpha_g)(1 + \alpha_h) \bmod \mathfrak{m}_L^{u+1}.$$

Hence the map is indeed a group homomorphism. It is clearly injective. □

***Corollary 8.7***. — *The group $G_0$ is hyper-solvable.*

*Proof.* — The group $G_0/G_1$ injects into $\mathcal{O}_L^\times/1 + \mathfrak{m}_L \simeq k_L^\times$ by proposition 8.6, and if $u \in \mathbf{Z}_{\geq -1}$, then $1 + \mathfrak{m}_L^u/1 + \mathfrak{m}_L^{u+1} \simeq k_L$ so that $G_u/G_{u+1}$ is a finite dimensional $\mathbf{F}_p$-vector space. □

***Example 8.8***. — Let $K = \mathbf{Q}_p$ and $K_n = \mathbf{Q}_p(\mu_{p^n})$ with $n \geq 1$. This is a totally ramified extension of $K$, of degree $p^{n-1}(p-1)$, with uniformizer $1 - \zeta_{p^n}$.

If $1 \leq j \leq n$ and $p^{j-1} \leq u \leq p^j - 1$, then $\mathrm{Gal}(K_n/K)_u = \mathrm{Gal}(K_n/K_j)$.

The ramification filtration is compatible with subgroups: if $F$ is a subextension of $L/K$, then $\mathrm{Gal}(L/F)_u = \mathrm{Gal}(L/K)_u \cap \mathrm{Gal}(L/F)$. In practice, we would prefer to fix $K$ and vary $L$. However, the filtration is not compatible with quotients in general. In order to remedy this, we have the following results of Herbrand. Define a function $\varphi_{L/K} : \mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$ by $\varphi_{L/K}(u) = \int_0^u [G_0 : G_t]^{-1} dt$.

***Lemma 8.9***. — *The function $\varphi_{L/K} : \mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$ is piecewise linear, continuous, increasing, concave, and a homeomorphism $\mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$.*

Let $\psi_{L/K} : \mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$ be the composition inverse of $\varphi_{L/K}$, and let $G^u = G_{\psi_{L/K}(u)}$. This is the upper ramification filtration of $G$. For example, if $K = \mathbf{Q}_p$ and $K_n = \mathbf{Q}_p(\mu_{p^n})$ with $n \geq 1$ and $i \geq 1$, then $G^i = \mathrm{Gal}(K_n/K_i)$. The following is Herbrand's theorem.

***Theorem 8.10***. — *If $G = \mathrm{Gal}(L/K)$ and $H$ is a distinguished subgroup of $G$, then $(G/H)^u = G^u H/H$.*

## 9. Infinite Galois extensions

Let $K$ be a field and let $L$ be an algebraic extension. We say that $L/K$ is Galois if and only if it is the union of finite Galois extensions of $K$. If $\sigma$ is a $K$-automorphism of $L$ and $E$ is a finite Galois extension of $K$ contained in $L$, then $\sigma(E) = E$. Conversely, if $L$ is a union of Galois extensions $E/K$ and $\{\sigma_E\}$ is a compatible family of automorphisms, then it gives rise to an automorphism $\sigma$ of $L$. If $\mathrm{Gal}(L/K)$ denotes the group of $K$-automorphisms of $L$, we therefore have an isomorphism $\mathrm{Gal}(L/K) \simeq \varprojlim \mathrm{Gal}(E/K)$. We give $\mathrm{Gal}(L/K)$ the product topology, so that it is a compact topological group. Galois theory extends to a bijection between closed subgroups of $\mathrm{Gal}(L/K)$ and algebraic extensions of $K$ contained in $L$, given by $H \leftrightarrow L^H$. The extension $L^H/K$ is then finite if and only if $H$ is an open subgroup of $\mathrm{Gal}(L/K)$. For example, we can consider $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, which is a large compact group.

For example, if $K = \mathbf{Q}_p$ and $K_n = \mathbf{Q}_p(\mu_{p^n})$ then $K^{\mathrm{cyc}} = \cup_{n\geq 1} K_n$ is the cyclotomic extension of $\mathbf{Q}_p$, and $\mathrm{Gal}(K^{\mathrm{cyc}}/K) = \mathbf{Z}_p^\times$ via the cyclotomic character. If $K$ is a finite extension of $\mathbf{Q}_p$, then every unramified extension of $K$ is of the form $K(\mu_{q^f-1})$ for some $f \geq 1$. The union of these extensions is the maximal unramified extension $K^{\mathrm{unr}}$ of $K$. We have $\mathrm{Gal}(K(\mu_{q^f-1})/K) = \mathbf{Z}/f\mathbf{Z}$ so that $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \widehat{\mathbf{Z}}$. The compositum of the extensions $K^{\mathrm{cyc}}$ and $K^{\mathrm{unr}}$ is an abelian extension of $K$. When $K = \mathbf{Q}_p$, it is the maximal abelian extension of $\mathbf{Q}_p$, by a $p$-adic analogue of the Kronecker-Weber theorem. We'll see later on how to construct the maximal abelian extension of a finite extension of $\mathbf{Q}_p$.

The upper ramification filtration is compatible with quotients by theorem 8.10 and can therefore be extended to the Galois groups of infinite extensions. If $K = \mathbf{Q}_p$ and $K_n = \mathbf{Q}_p(\mu_{p^n})$, then $\mathrm{Gal}(K^{\mathrm{cyc}}/K) \simeq \mathbf{Z}_p^\times$ and $\mathrm{Gal}(K^{\mathrm{cyc}}/K)^i = \mathrm{Gal}(K^{\mathrm{cyc}}/K_i) \simeq 1 + p^i\mathbf{Z}_p$.

## 10. Power series and the Weierstrass preparation theorem

Let $K$ be a finite extension of $\mathbf{Q}_p$, let $\pi$ be a uniformizer of $\mathcal{O}_K$. Given a power series $f(X) = \sum_{i\geq 0} a_i X^i \in K[\![X]\!]$, we can evaluate $f(X)$ at $z \in \mathbf{C}_p$ if and only if $a_i z^i \to 0$, that is iff $|a_i|\rho^i \to 0$ where $\rho = |z|$. Let $\rho(f) = \sup\{\rho \in \mathbf{R} \text{ such that } |a_i|\rho^i \to 0\}$ be the radius of convergence of $f$. If $\rho < \rho(f)$ and $|z| = \rho$, then $f(z)$ converges and if $\rho > \rho(f)$ and $|z| = \rho$, then $f(z)$ diverges.

Let $\mathrm{H}_K = \{f(X) \in K[\![X]\!] \text{ such that } \rho(f) \geq 1\} = \{f(X) \in K[\![X]\!] \text{ such that } |a_i|\rho^i \to 0 \text{ for all } \rho < 1\} = \{f(X) \in K[\![X]\!] \text{ such that } f(z) \text{ converges for all } z \in \mathfrak{m}_{\mathbf{C}_p}\}$. For example, $K \otimes \mathcal{O}_K[\![X]\!] \subset \mathrm{H}_K$ but also $\log(1+X) \in \mathrm{H}_K$.

Take $f(X) \in \mathrm{H}_K$ and $\rho \in \mathbf{R}$ such that there exists $z \in \mathfrak{m}_{\mathbf{C}_p}$ with $|z| = \rho$. Let $|f|_\rho = \sup_{|z|=\rho} |f(z)|$.

***Theorem 10.1***. — *If $f$ and $\rho$ are as above, then $\sup_{i\geq 0} |a_i|\rho^i$ is a* max *and $|f|_\rho = \sup_{i\geq 0} |a_i|\rho^i$.*

*Proof.* — We have $|a_i|\rho^i \to 0$ so that the sup is a max. Note that $|f|_\rho \leq \sup_{i\geq 0} |a_i|\rho^i$, and we prove that equality holds. Let $L$ be a finite extension of $K$ such that there exists $\alpha \in L$ with $|\alpha| = \rho$ and let $\beta = a_j\alpha^j$ where $a_j\alpha^j = \max |a_i|\rho^i$. Let $g(X) = f(\alpha X)/\beta = \sum_{i\geq 0} g_i X^i$. We have $|g_i| \leq 1$ and $|g_j| = 1$ and $g_i \to 0$. In particular, $\overline{g}(X)$ belongs to $k_L[X]$ and is a nonzero polynomial. Hence there exists $w \in \overline{\mathbf{F}}_p$ such that $\overline{g}(w) \neq 0$. Let $y \in \mathcal{O}_{\mathbf{C}_p}$ be a lift of $w$. We have $|g(y)| = 1$ and hence $|f(\alpha y)| = \sup_{i\geq 0} |a_i|\rho^i$ with $|\alpha y| = \rho$. □

The theorem implies that $|f|_\sigma \leq |f|_\rho$ if $\sigma \leq \rho$. The maximum modulus principle holds: $|f|_\rho = \sup_{|z|\leq\rho} |f(z)|$. In addition, the (proof of the) theorem implies that $|fg|_\rho = |f|_\rho \cdot |g|_\rho$.

The theorem also implies that $f \in \mathrm{H}_K$ is bounded if and only if $f \in K \otimes \mathcal{O}_K[\![X]\!]$ and that $f$ is bounded by 1 iff $f \in \mathcal{O}_K[\![X]\!]$. If $f(X) = f_0 + f_1 X + \cdots \in \mathcal{O}_K[\![X]\!]$, let $\mathrm{wideg}(f)$ be the smallest $i$ such that $f_i \in \mathcal{O}_K^\times$, so that $\mathrm{wideg}(f) = +\infty$ if and only if $f(X) \in \pi \cdot \mathcal{O}_K[\![X]\!]$. A function $f(X) \in \mathcal{O}_K[\![X]\!]$ is a unit if and only if $f_0 \in \mathcal{O}_K^\times$, ie if and only if $\mathrm{wideg}(f) = 0$. We also have $\mathrm{wideg}(fg) = \mathrm{wideg}(f) + \mathrm{wideg}(g)$.

***Proposition 10.2***. — *Take $f(X) \in \mathcal{O}_K[\![X]\!]$ such that $\mathrm{wideg}(f) = n$ is finite. If $g(X) \in \mathcal{O}_K[\![X]\!]$, then there exists a series $q(X) \in \mathcal{O}_K[\![X]\!]$ and a polynomial $r(X) \in \mathcal{O}_K[X]$ of degree $\leq n-1$, such that $g(X) = f(X)q(X)+r(X)$, and $q$ and $r$ are uniquely determined.*

*Proof.* — In $k[\![X]\!]$, we have $\overline{f}(X) = X^n f_0(X)$ with $f_0(X) \in k[\![X]\!]^\times$. If $h(X) = \sum_{i=0}^{+\infty} h_i X^i \in k[\![X]\!]$, then $h(X) = r(X) + X^n s(X)$ with $r(X) = h_0 + h_1 X + \cdots + h_{n-1}X^{n-1}$ and $s(X) = \sum_{i=n}^{+\infty} h_i X^{i-n}$. We then have $h = r + q\overline{f}$ with $q(X) = s(X)\overline{f}_0^{-1}(X)$.

If $g(X) \in \mathcal{O}_K[\![X]\!]$, we can then write $g = r_0 + q_0 f + \pi g_1$ with $q_0$ and $r_0$ as above, and then $g = r_0 + q_0 f + \pi(r_1 + q_1 f) + \pi^2 g_2$, ... We can then take $r = \sum_{i\geq 0} \pi^i r_i$ and $q = \sum_{i\geq 0} \pi^i q_i$.

We now prove unicity. If $qf + r = 0$, then reducing mod $\pi$, we get that $X^n$ divides $\overline{r}$ so that $\overline{r} = 0$ and then $\overline{q} = 0$. This implies that $\pi$ divides $r$ and $q$. By dividing by $\pi$ and iterating, this shows that $q = r = 0$. □

***Corollary 10.3***. — *If $\alpha \in \mathfrak{m}_K$, then $f(X) = (X-\alpha)q(X) + f(\alpha)$ with $q(X) \in \mathcal{O}_K[\![X]\!]$.*

A polynomial $P(X) \in \mathcal{O}_K[X]$ is called distinguished if $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_i \in \mathfrak{m}_K$ for all $0 \leq i \leq n-1$. By the theory of Newton polygons, a distinguished polynomial has exactly $\deg(P)$ roots in $\mathfrak{m}_{\overline{\mathbf{Q}}_p} \subset \mathfrak{m}_{\mathbf{C}_p}$.

***Theorem 10.4***. — *If $f(X) \in \mathcal{O}_K[\![X]\!]$ and $n = \mathrm{wideg}(f)$ is finite, there exists a unique distinguished polynomial $p$ of degree $n$ such that $f(X) = p(X)u(X)$ where $u \in \mathcal{O}_K[\![X]\!]^\times$.*

*Proof.* — If we apply proposition 10.2 to $g(X) = X^n$, we find $q$ and $r$ such that $X^n = f(X)q(X) + r(X)$. We see that $r \equiv 0 \mod \pi$, so that $p(X) = X^n - r(X)$ is distinguished, and $f(X)q(X) = p(X)$. We have $\mathrm{wideg}(q) = 0$ so that $q$ is a unit and $f(X) = p(X)u(X)$ with $u(X) = q(X)^{-1}$.

The series $f$ therefore has precisely $\mathrm{wideg}(f)$ roots in $\mathfrak{m}_{\mathbf{C}_p}$. If $f = p_1u_1 = p_2u_2$, then $p_1$ and $p_2$ are distinguished and have the same roots, so that they are equal. □

***Corollary 10.5***. — *If $f(X) \neq 0 \in \mathcal{O}_K[\![X]\!]$, then*

1. *we can write $f(X) = \pi^\mu p(X)u(X)$ where $p$ is distinguished, $u$ is a unit, and $\mu \geq 0$;*
2. *$f(X)$ has finitely many (namely $\mathrm{wideg}(\pi^{-\mu}f)$) zeroes in $\mathfrak{m}_{\mathbf{C}_p}$.*

Furthermore, the theory of Newton polygons extends to $K \otimes \mathcal{O}_K[\![X]\!]$.

***Theorem 10.6***. — *The ring $K \otimes \mathcal{O}_K[\![X]\!]$ is a PID.*

*Proof.* — If $I = (\{f_i\}_i)$, we can write $f_i = \pi^{\mu_i}p_iu_i$ and $I = (\{p_i\}_i)$. The ring $K[X]$ is a PID, and therefore $(\{p_i\}_i) = (p)$ in $K[X]$. This implies that $I = (p)$ in $K \otimes \mathcal{O}_K[\![X]\!]$. □

Likewise, one can prove that $\mathcal{O}_K[\![X]\!]$ is a noetherian local ring, with maximal ideal $(\pi, X)$, whose other prime ideals are $(0)$, $(\pi)$, and $(p(X))$ with $p$ a distinguished and irreducible polynomial.

***Theorem 10.7***. — *If $f(X) \in \mathrm{H}_K$ and $\rho \in p^{\mathbf{Q}<0}$, then $f(X)$ has only finitely many zeroes in $B(0, \rho)$. In addition, all these zeroes are in $\mathfrak{m}_{\overline{\mathbf{Q}}_p}$.*

*Proof.* — Let $L$ be a finite extension of $K$ and $\alpha \in \mathfrak{m}_L$ be such that $|\alpha| = \rho$. The function $f(\alpha X)$ belongs to $L \otimes \mathcal{O}_L[\![X]\!]$. It therefore has only finitely many zeroes in $\mathfrak{m}_{\mathbf{C}_p}$ by corollary 10.5 and all these zeroes are in $\mathfrak{m}_{\overline{\mathbf{Q}}_p}$ by ibid. □

***Theorem 10.8***. — *If $f(X) \in \mathrm{H}_K$, then $f$ is bounded if and only if $f$ has finitely many zeroes in $\mathfrak{m}_{\mathbf{C}_p}$.*

*Proof.* — If $f$ is bounded, then it belongs to $K \otimes \mathcal{O}_K[\![X]\!]$ and therefore has only finitely many zeroes in $\mathfrak{m}_{\mathbf{C}_p}$ by corollary 10.5. Conversely, take $\rho \in p^{\mathbf{Q}<0}$ and $\alpha \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$ such that $|\alpha| = \rho$. The number of zeroes of $f$ in $B(0, \rho)$ is the wideg of $f(\alpha X)/\beta$, where $|\beta| = |f|_\rho$,

which is equal to $\min\{j \text{ such that } |a_j|\rho^j = \max |a_i|\rho^i\}$. If $f$ has $n$ zeroes in $\mathfrak{m}_{\mathbf{C}_p}$ then this min is $\leq n$ and therefore for all $k$, we have $|a_k|\rho^k \leq \max_{j=0}^n |a_j|\rho^j$. By letting $\rho \to 1$, we get that $|a_k| \leq \max_{j=0}^n |a_j|$, which implies that $f$ is bounded. □

Note that there exist nonzero power series $f(X) \in \mathcal{O}_{\mathbf{C}_p}[\![X]\!]$ that have an infinite number of zeroes in $\mathfrak{m}_{\mathbf{C}_p}$.

## 11. $p$-adic Banach spaces

Let $K$ be a finite extension of $\mathbf{Q}_p$, with residue field $k$. A $p$-adic Banach space is a topological $K$-vector space $E$ whose topology comes from an ultrametric norm $\|\cdot\| : E \to \mathbf{R}$, for which it is complete. We say that $E$ satisfies condition (N) if $\|E\| = |K|$. If $E$ does not satisfy condition (N), then the norm $\|\cdot\|'$ defined by $\|x\|' = |\pi|^{-\lfloor \mathrm{val}_\pi(\|x\|)\rfloor}$ is equivalent to $\|\cdot\|$ and satisfies condition (N). The unit ball $\mathcal{O}_E$ of $E$ is an $\mathcal{O}_K$-module, and $k_E = \mathcal{O}_E/\mathfrak{m}_E$ is a $k$-vector space.

The following are $p$-adic Banach spaces:

1. any finite dimensional $K$-vector space;
2. $\mathbf{C}_p$, for which $k_{\mathbf{C}_p} = \overline{\mathbf{F}}_p$;
3. $C^0(X, E)$, where $X$ is a compact metric space and $E$ is a Banach space;
4. If $I$ is a set and $\ell^0_\infty(I) = \{a_i\}_{i\in I}$ where $a_i \in K$ and for every $\varepsilon > 0$, the set of $i$ such that $|a_i| > \varepsilon$ is finite, then $\ell^0_\infty(I)$ is a Banach space with $\|a\| = \sup_{i\in I} |a_i|$.

If $E$ is a Banach space and $\{e_i\}_{i\in I}$ is a bounded family of elements, then there is a continuous map $s : \ell^0_\infty(I) \to E$ given by $a \mapsto \sum_{i\in I} a_i e_i$. We say that $\{e_i\}_{i\in I}$ is a Banach basis if $s$ is an isometry. If $s$ is merely an isomorphism of Banach spaces, we say that $\{e_i\}_{i\in I}$ is a pseudo Banach basis.

***Proposition 11.1***. — *If $E$ satisfies condition (N), then a family $\{e_i\}_{i\in I}$ of $\mathcal{O}_E$ is a Banach basis if and only if $\{\overline{e}_i\}_{i\in I}$ is a basis of the $k$-vector space $k_E$.*

*Proof.* — One implication is clear, so take a family $\{e_i\}_{i\in I}$ that gives a basis of the $k$-vector space $k_E$. The map $s : \mathcal{O}_{\ell^0_\infty(I)} \to \mathcal{O}_E$ given by $a \mapsto \sum_{i\in I} a_i e_i$ is surjective modulo $\pi$, so by lemma **??**, it is surjective. If $s(a) = 0$, then $\pi$ divides $a_i$ for all $i$, and by iterating this, we get $a = 0$. If $\|a\| = 1$, then $\overline{s(a)} \neq 0$, so that $\|s(a)\| = 1$. This shows that $s$ is an isometry, since $E$ satisfies condition (N). □

***Example 11.2***. — The set $\{\binom{x}{n}\}_{n\geq 0}$ is a Banach basis of the Banach space $C^0(\mathbf{Z}_p, \mathbf{Q}_p)$.

This result is known as Mahler's theorem, and we now prove it. If $(a_n)$ is a sequence of $\mathbf{Z}_p$ that goes to 0, then $x \mapsto \sum_{n\geq 0} a_n \binom{x}{n}$ is a continuous function on $\mathbf{Z}_p$.

***Proposition 11.3***. — *If $f \in C^0(\mathbf{Z}_p, \mathbf{Z}_p)$ can be written as $x \mapsto \sum_{n\geq 0} a_n \binom{x}{n}$ where $(a_n)$ is a sequence of $\mathbf{Z}_p$ that goes to 0, then $a_n = \sum_{i=0}^n f(i)(-1)^{n-i}\binom{n}{i}$ and $\|f\|_\infty = \max |a_n|_p$.*

*Proof.* — We have $f(0) = a_0$, $f(1) = a_0 + a_1$, $\ldots$, $f(n) = \sum_{i=0}^n a_i \binom{n}{i}$ and hence $a_n = \sum_{k=0}^n (-1)^{n-k}\binom{n}{k} f(k)$. We therefore have $|a_n|_p \leq \|f\|_\infty$ for all $n$. Since $\|f\|_\infty \leq \max |a_n|_p$, we have $\|f\|_\infty = \max |a_n|_p$. □

***Theorem 11.4***. — *Every function $f \in C^0(\mathbf{Z}_p, \mathbf{Z}_p)$ can be written in one and only one way as $x \mapsto \sum_{n\geq 0} a_n \binom{x}{n}$ where $(a_n)$ is a sequence of $\mathbf{Z}_p$ that goes to 0.*

*Proof.* — It is enough to show that if we let $a_n = \sum_{k=0}^n (-1)^{n-k}\binom{n}{k} f(k)$, then $a_n \to 0$. In this case, the function $x \mapsto \sum_{n\geq 0} a_n \binom{x}{n}$ is a continuous function on $\mathbf{Z}_p$, that coincides with $f$ on $\mathbf{Z}_{\geq 0}$ and hence on $\mathbf{Z}_p$ by density.

It is a combinatorics exercise to show that for all $m, n \geq 0$, we have

$$\sum_{j=0}^{m} \binom{m}{j} a_{n+j} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+m). \tag{1}$$

Take $s \geq 1$. Since $f$ is uniformly continuous, there exists $t \geq 1$ such that $f(x) - f(y) \in p^s\mathbf{Z}_p$ if $x - y \in p^t\mathbf{Z}_p$. Equation (1) applied to $m = p^t$ and the definition of $a_n$ imply that

$$a_{n+p^t} = -\sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j} + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \big(f(k+p^t) - f(k)\big) \tag{2}$$

The RHS belongs to $p^s\mathbf{Z}_p$. Furthermore, $\binom{p^t}{j} = \frac{p^t}{j}\binom{p^t-1}{j-1} \in p\mathbf{Z}_p$ for all $1 \leq j \leq p^t - 1$. This implies that $a_{n+p^t} \in p\mathbf{Z}_p$ for all $n \geq 0$. By plugging this back into (2), we find that $a_{n+2p^t} \in p^2\mathbf{Z}_p$ for all $n \geq 0$, and then by induction that $a_{n+sp^t} \in p^s\mathbf{Z}_p$ for all $n \geq 0$. We then have $a_n \in p^s\mathbf{Z}_p$ if $n \geq sp^t$. This implies that $a_n \to 0$. □

The following properties of (real and complex) Banach spaces also hold for $p$-adic Banach spaces: the open mapping theorem (a continuous bijection between two Banach spaces is a homeomorphism) and the Banach-Steinhaus theorem. The next two results are specific to the $p$-adic situation.

***Proposition 11.5***. — *If $F$ is a closed subspace of a $p$-adic Banach space $E$, then $F$ has a closed complement.*

*Proof.* — We can change the norm so that it satisfies condition (N). In this case, $k_E$ has basis of the form $B_F \sqcup C$, where $B_F$ gives rise to a Banach basis of $F$. The set $C$ then gives rise to a Banach basis of a closed complement of $F$ in $E$. □

***Corollary 11.6***. — *If $f : E \to F$ is a continuous and surjective map of Banach spaces, then it has a continuous splitting $s : F \to E$.*

*Proof.* — Let $S$ be a closed complement of $\ker(f)$. The map $f : S \to F$ is a continuous bijection, hence a homeomorphism. Its inverse $s : F \to S \subset E$ is a splitting of $f$. □

## 12. Formal groups

Let $R$ be a ring, such as $k$ or $\mathcal{O}_K$ or $K$ where $K$ is a finite extension of $\mathbf{Q}_p$. A formal group (law) over $R$ is a power series $F(X,Y) \in R[\![X,Y]\!]$ such that

1. $F(X,Y) = X + Y + \deg \geq 2$;
2. $F(X,F(Y,Z)) = F(F(X,Y),Z)$;
3. $F(X,Y) = F(Y,X)$;
4. there exists $i(X) \in R[\![X]\!]$ such that $F(X,i(X)) = 0$.

A formal group law over $\mathcal{O}_K$ can be used to define a new commutative group structure over $\mathfrak{m}_L$ for any extension $L$ of $K$, by $x \oplus y = F(x,y)$. Examples of formal groups are $\mathbf{G}_a$ given by $F(X,Y) = X + Y$ and $\mathbf{G}_m$ given by $F(X,Y) = X + Y + XY$. Other examples include $F(X,Y) = (X+Y)/(1+XY)$ as well as

$$F(X,Y) = \frac{X\sqrt{1-Y^4} + Y\sqrt{1-X^4}}{1+X^2Y^2}.$$

***Lemma 12.1***. — *Item (4) follows from (1), and $i(X)$ is unique.*

*Proof.* — If $i_1(X) = -X$, then $F(X,i_1(X)) = \mathrm{O}(X^2)$ by (1). Assume that we have $i_n(X)$ such that $F(X,i_n(X)) = cX^{n+1} + \mathrm{O}(X^{n+2})$. We have $F(X,i_n(X) - cX^{n+1}) = F(X,i_n(X)) - cX^{n+1}F_Y(X,i_n(X)) + \mathrm{O}(X^{2(n+1)}) = \mathrm{O}(X^{n+2})$. Take $i(X) = \lim i_n(X)$. The proof also shows that $i(X)$ is uniquely determined. □

***Lemma 12.2***. — *If $f(X) \in X \cdot R[\![X]\!]$ and $f'(0) \in R^\times$, then there exists $g(X) \in X \cdot R[\![X]\!]$ such that $f \circ g(X) = g \circ f(X) = X$.*

Items (1) and (2) imply that $F(X,0) = X$ and $F(0,Y) = Y$: if $A(X) = F(X,0)$, then $A(X) = X + \mathrm{O}(X^2)$ by (1) and $A(A(X)) = A(X)$ so that $A(X) = X$ by lemma 12.2.

A homomorphism $h : F \to G$ between two formal groups is a power series $h(X) \in X \cdot R[\![X]\!]$ such that $h(F(X,Y)) = G(h(X),h(Y))$. By lemma 12.2, it is an isomorphism

if and only if $h'(0) \in R^\times$. For example, let $F$ be a formal group and let $[n](X)$ be defined by $[1](X) = X$ and $[n+1](X) = F(X, [n](X))$ for $n \geq 1$ and $[-1](X) = i(X)$ and $[n-1](X) = F(i(X), [n](X))$ for $n \leq -1$. These are endomorphisms of $F$.

A differential form on $F$ is an element $\omega(X) = p(X)dX$ of $R[\![X]\!]dX$. If $f(X) \in XR[\![X]\!]$, then $\omega(f(X)) = p(f(X))f'(X)dX$. It is invariant if $\omega \circ f = \omega$ where $f(X) = F(X, Y)$ with $Y$ seen as a constant, ie if $p(F(X,Y)) \cdot F_X(X,Y) = p(X)$. By setting $X = 0$, we get $p(Y) = p(0)/F_X(0, Y)$ so that if $\omega$ is invariant, then $\omega(X) = a \cdot dX/F_X(0, X)$.

***Lemma 12.3***. — *The form $dX/F_X(0, X)$ is invariant.*

*Proof.* — Write $F(Z, F(X, Y)) = F(F(Z, X), Y)$, take the derivative with respect to $Z$, and evaluate at $Z = 0$ □

Let $\omega_F(X) = dX/F_X(0, X)$ be the normalized invariant differential form. If $F$ are $G$ formal groups and $h \in \mathrm{Hom}(F, G)$, then $\omega_G \circ h = h'(0) \cdot \omega_F$. If $R = K$, let $\log_F(X) = \int \omega_F(X)$ (with $\log_F(0) = 0$). This is the logarithm of $F$. Note that $\log_F(X) \in \mathrm{H}_K$.

***Proposition 12.4***. — *We have $\log_F(F(X, Y)) = \log_F(X) + \log_F(Y)$, so that $\log_F : F \to \mathbf{G}_a$ is an isomorphism over $K$.*

*Proof.* — Let $E(X) = \log_F(F(X, Y)) - \log_F(X)$. We have $dE(X) = \omega_F \circ F - \omega_F = 0$ since $\omega_F$ is invariant, so that $E(X) = E(0) = \log_F(Y)$. □

For example, $\log_{\mathbf{G}_m} = \log(1 + X)$. Over $K$, any two formal groups are therefore isomorphic. Over $\mathcal{O}_K$, this is not the case. For example, $\mathfrak{m}_{\mathbf{C}_p}$ with the law coming from $\mathbf{G}_a$ is torsion free, but not $\mathfrak{m}_{\mathbf{C}_p}$ with the law coming from $\mathbf{G}_m$.

## 13. The Tate module

Let $k$ be a field of characteristic $p$, and let $F$, $G$ be formal groups over $k$. If $f \in \mathrm{Hom}(F, G)$, then the height $\mathrm{ht}(f)$ of $f$ is the largest integer $h$ such that $f(X) = g(X^{p^h})$.

***Proposition 13.1***. — *If $f(X) = g(X^{p^h})$ with $h = \mathrm{ht}(f)$, then $g'(0) \neq 0$.*

*Proof.* — We first show that if $f \in \mathrm{Hom}(F, G)$ and $f'(0) = 0$, then $f(X)$ is of the form $g(X^p)$. We have $0 = f'(0) \cdot \omega_F = \omega_G \circ f = f'(X)dX/G_X(0, X)$ so that $f'(X) = 0$. Since $k$ is of char $p$, this implies that $f(X) = g(X^p)$.

Write $F(X, Y) = \sum a_{ij} X^i Y^j$ and let $F^{(h)}(X, Y) = \sum a_{ij}^{p^h} X^i Y^j$. This is a new formal group, since $x \mapsto x^p$ is a ring homomorphism of $k$, and if $f \in \mathrm{Hom}(F, G)$ and $f(X) = g(X^{p^h})$, then $g \in \mathrm{Hom}(F^{(h)}, G)$. The proposition now follows from the above claim. □

Let $K$ be a finite extension of $\mathbf{Q}_p$ and let $F$ be a formal group over $\mathcal{O}_K$. The height of $F$ is the height of $[p](X) \in \mathrm{Hom}(\overline{F}, \overline{F})$. If $F$ comes from an elliptic curve, then it is of height 1 or 2. If $h = \mathrm{ht}(F)$ is finite, then $\mathrm{wideg}([p](X)) = p^h$ by proposition 13.1. If $y \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$, the equation $[p](z) = y$ then has $p^h$ solutions. Since $\omega_F \circ [p] = p \cdot \omega_F$, we have $[p](X)' = p(1 + \mathrm{O}(X))$, and the roots of $[p](z) - y$ are simple.

Let $M[p^n] = \{z \in \mathfrak{m}_{\overline{\mathbf{Q}}_p}$ such that $[p^n](z) = 0\}$. This set has $p^{hn}$ elements, it is a $\mathbf{Z}/p^n\mathbf{Z}$-module, and $[p] : M[p^{n+1}] \to M[p^n]$ is surjective. Let $M = \varprojlim_n M[p^n] = \{(z_1, z_2, \ldots)$ with $[p](z_1) = 0$ and $[p](z_{n+1}) = z_n\}$. This is a $\mathbf{Z}_p$-module. If $z = (z_1, z_2, \ldots) \in M$, then $pz = (0, z_1, z_2, \ldots)$. For instance, $pz = 0$ implies $z = 0$. We have a map $M/p^nM \to M[p^n]$ given by $z \mapsto z_n$ and this map is a bijection. Let $m_1, \ldots, m_h \in M$ be elements whose images are a basis of the $\mathbf{F}_p$-vector space $M/pM$. We easily see that $M = \oplus_{i=1}^h \mathbf{Z}_p m_i$, so that $M$ is free of rank $h$ over $\mathbf{Z}_p$.

This is the Tate module of $F$, also denoted by $T_pF$. Let $V_pF = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pF$. This is a $\mathbf{Q}_p$-vector space of dimension $h$. The group $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$ acts on $V_pF$ : this is the $p$-adic representation attached to $F$. If we choose a basis of $T_pF$, we get a map $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \to \mathrm{GL}_h(\mathbf{Z}_p)$. For example, if $F = \mathbf{G}_m$, then $\mathrm{ht}(F) = 1$ and the resulting map $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathbf{Z}_p^\times$ is the cyclotomic character.

## 14. Lubin-Tate theory

Let $K$ be a finite extension of $\mathbf{Q}_p$, with residue field $k$ of cardinality $q$. A formal $\mathcal{O}_K$-module is a formal group $F$ over $\mathcal{O}_K$ along with a ring homomorphism $\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$, $a \mapsto [a](X)$, such that $[a](X) = aX + \mathrm{O}(X^2)$. The space $\mathfrak{m}_{\mathbf{C}_p}$ is then equipped with an $\mathcal{O}_K$-module structure. Fix a uniformizer $\pi$ of $\mathcal{O}_K$ and let $\mathcal{L}_\pi$ be the set of power series $\varphi(X)$ such that $\varphi(X) = \pi X + \mathrm{O}(X^2)$ and $\varphi(X) \equiv X^q \bmod \pi$.

***Theorem 14.1***. — *If $\varphi \in \mathcal{L}_\pi$, then there exists a formal $\mathcal{O}_K$-module $F$ such that $[\pi](X) = \varphi(X)$. The isomorphism class of $F$ only depends on $\pi$, not on $\varphi \in \mathcal{L}_\pi$.*

For example, if $K = \mathbf{Q}_p$ and $\pi = p$ and $\varphi(X) = (1 + X)^p - 1$, then $F = \mathbf{G}_m$. In order to prove the theorem, we need a general lemma.

***Lemma 14.2***. — *If $\varphi$, $\psi \in \mathcal{L}_\pi$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K^n$, then there exists a unique $H_\alpha^{\varphi,\psi} \in \mathcal{O}_K[\![X_1, \ldots, X_n]\!]$ such that*

1. $H_\alpha^{\varphi,\psi}(X_1, \ldots, X_n) = \alpha_1 X_1 + \cdots + \alpha_n X_n + \deg \geq 2$;
2. $\varphi \circ H_\alpha^{\varphi,\psi}(X_1, \ldots, X_n) = H_\alpha^{\varphi,\psi}(\psi(X_1), \ldots, \psi(X_n))$.

*Proof.* — Take any $H_1(X_1,\dots,X_n) \equiv \alpha_1 X_1 + \cdots + \alpha_n X_n + \mathrm{O}(X^2)$. Note that $\varphi \circ H_1 - H_1 \circ \psi$ only has terms of degree $\geq 2$. We construct a sequence $\{H_i\}_i$ of power series with coefficients in $\mathcal{O}_K$ such that $\varphi \circ H_i - H_i \circ \psi$ only has terms of degree $\geq i+1$ and such that $H_i \equiv H_{i+1}$ modulo terms of degree $\geq i+1$. Suppose that we have $H_i$. We want $H_{i+1} = H_i + R_i$ where $R_i$ only has terms of degree $\geq i+1$. In this case,

$$\varphi(H_{i+1}) = \varphi(H_i + R_i) = \varphi(H_i) + \varphi'(H_i)R_i + \deg \geq i+2 = \varphi(H_i) + \pi R_i + \deg \geq i+2$$

and likewise $H_{i+1}(\psi) = H_i(\psi) + R_i(\psi) = H_i(\psi) + \pi^{i+1}R_i + \deg \geq i+2$.

Therefore, we need to have $R_i = (\varphi \circ H_i - H_i \circ \psi)/(\pi^{i+1} - \pi) \bmod \deg \geq i+2$. We have $\varphi \circ H_i - H_i \circ \psi \equiv H_i(X_1,\dots,X_n)^q - H_i(X_1^q,\dots,X_n^q) \equiv 0 \bmod \pi$, so that we can take $R_i = (\varphi \circ H_i - H_i \circ \psi)/(\pi^{i+1} - \pi)$. The power series $\{H_i\}_i$ then converge to a series $H_\alpha^{\varphi,\psi}$ satisying (1) and (2). The proof also shows that if we have two power series satisfying (1) and (2) that coincide in degree $\leq i$, then they have to coincide in degree $\leq i+1$. This implies unicity by induction. □

*Proof of theorem 14.1.* — Let $F(X,Y) = H_{1,1}^{\varphi,\varphi}(X,Y)$. It is easy to check (1)–(4) in the definition of a formal group. For instance, $F(X,F(Y,Z)) = H_{1,1,1}^{\varphi,\varphi} = F(F(X,Y),Z)$ and $i(X) = H_{-1}^{\varphi,\varphi}(X)$. For $a \in \mathcal{O}_K$ let $[a](X) = H_a^{\varphi,\varphi}(X)$. We show the same way that they are endomorphisms of $F$. Finally if $\varphi$, $\psi \in \mathcal{L}_\pi$, then $H_1^{\varphi,\psi}$ gives an isomorphism between $F_\varphi$ and $F_\psi$. □

***Remark 14.3***. — The group $F$ is of height $[K : \mathbf{Q}_p]$.

We are interested in the field $K_n^\varphi$ generated by the $\pi^n$-torsion points of $F_\varphi$. Note that if $z \in F_\varphi[\pi^n]$, then $H_1^{\varphi,\psi}(z) \in F_\psi[\pi^n]$. The field $K_n^\varphi$ is therefore independent of the choice of $\varphi$, so we can take $\varphi(X) = \pi X + X^q$. Note that $\varphi'(X) = qX^{q-1} + \pi$ so that if $z \in \mathfrak{m}_{\mathbf{C}_p}$, the roots of $\varphi(X) - z$ are all simple. The set $F[\pi^n]$ is a finite subgroup of $(\mathfrak{m}_{\mathbf{C}_p}, \oplus)$. Since $[\pi](X) = \varphi(X)$, the theory of Newton polygons tells us that $F[\pi^n]$ has $q^n$ elements. Let $K_n = K(F[\pi^n])$ and $K_\infty = \cup_{n \geq 0} K_n$.

***Theorem 14.4***. — *The extension $K_\infty/K$ is totally ramified, and there is a character $\chi_\pi : \mathrm{Gal}(K_\infty/K) \simeq \mathcal{O}_K^\times$.*

*Proof.* — Let $\Lambda_0 = \{0\}$ and for $n \geq 1$, let $\Lambda_n$ be the set of $z \in \mathfrak{m}_{\mathbf{C}_p}$ such that $[\pi^n](z) = 0$ and $[\pi^{n-1}](z) \neq 0$. We have $F[\pi^n] = \Lambda_0 \sqcup \cdots \sqcup \Lambda_n$, and $\Lambda_n$ has $q^{n-1}(q-1)$ elements. If $y \in \Lambda_k$ and $[\pi](z) = y$, then $z \in \Lambda_{k+1}$, so that $K_n = K(\Lambda_n)$.

The group $\mathcal{O}_K^\times$ acts on $\Lambda_n$ by $\alpha \cdot z = [\alpha](z)$. We have $\alpha \cdot z = z$ if and only if $[\alpha - 1](z) = 0$, that is if $\alpha \in 1 + \pi^n \mathcal{O}_K$. Since $\mathcal{O}_K^\times / 1 + \pi^n \mathcal{O}_K$ has $q^{n-1}(q-1)$ elements, it acts freely and transitively on $\Lambda_n$. Hence $K_n = K(z)$ for any $z \in \Lambda_n$. Let $Q(X) = X^{q-1} + \pi$. An

element $z \in \Lambda_n$ is a root of $Q \circ \varphi^{\circ(n-1)}(X)$, which is an Eisenstein polynomial of degree $q^{n-1}(q-1)$, so that $K_n$ is totally ramified, $z$ is a uniformizer of $\mathcal{O}_{K_n}$, $K_n/K$ is Galois, and $\mathrm{Gal}(K_n/K) \simeq \mathcal{O}_K^\times/1+\pi^n\mathcal{O}_K$ via the map $g \mapsto \chi_\pi^{(n)}(g)$ determined by $g(z) = [\chi_\pi^{(n)}(g)](z)$.

The extension $K_\infty/K$ is therefore totally ramified, and $\mathrm{Gal}(K_\infty/K) \simeq \mathcal{O}_K^\times$, via the map $g \mapsto \chi_\pi(g)$ determined by $g(z) = [\chi_\pi(g)](z)$ for all $z \in F[\pi^\infty]$. □

The character $\chi_\pi$ constructed above is the Lubin-Tate character attached to the uniformizer $\pi$. It is independent of the choice of $\varphi \in \mathcal{L}_\pi$.

***Remark 14.5***. — The Tate module $T_pF$ is isomorphic to $\varprojlim_n F[\pi^n]$, and the corresponding Galois representation is given by $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \xrightarrow{\chi_\pi} \mathcal{O}_K^\times \hookrightarrow \mathrm{GL}_{[K:\mathbf{Q}_p]}(\mathbf{Z}_p)$.

***Remark 14.6***. — An element $z \in \Lambda_n$ as above is a root of $Q \circ \varphi^{\circ(n-1)}(X)$ whose constant coefficient is $\pi$, so that $\pi$ is the norm of an element of $K_n$ for all $n \geq 1$. We can show that $\cap_{n\geq 1} \mathrm{N}_{K_n/K}(K_n^\times) = \pi^{\mathbf{Z}}$.

***Remark 14.7***. — If $1 \leq j \leq n$ and $q^{j-1} \leq u \leq q^j-1$, then $\mathrm{Gal}(K_n/K)_u = \mathrm{Gal}(K_n/K_j)$. If $n \geq 0$, then $\mathrm{Gal}(K_\infty/K)^n = 1 + \pi^n\mathcal{O}_K$.

## 15. Local class field theory

Let $K_\infty^\pi$ denote the extension of $K$ constructed above. It is an abelian totally ramified extension of $K$. The extension $K^{\mathrm{unr}}/K$ is also abelian, with $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathrm{Gal}(\overline{\mathbf{F}}_p/k)$ We have $\mathrm{Gal}(\overline{\mathbf{F}}_p/k) = \widehat{\mathbf{Z}}$, generated by $\mathrm{Fr}_q : x \mapsto x^q$. Let $\mathrm{Fr}_q$ denote the corresponding element of $\mathrm{Gal}(K^{\mathrm{unr}}/K)$.

Let $\mathrm{Art} : K^\times \to \mathrm{Gal}(K_\infty^\pi \cdot K^{\mathrm{unr}}/K) = \mathrm{Gal}(K_\infty^\pi/K) \times \mathrm{Gal}(K^{\mathrm{unr}}/K)$ be the map given by $\pi \mapsto \mathrm{Fr}_q$ and $u \mapsto \chi_\pi^{-1}(u^{-1})$ where $\chi_\pi : \mathrm{Gal}(K_\infty^\pi/K) \to \mathcal{O}_K^\times$ is the above isomorphism.

***Theorem 15.1***. — 1. *The extension $K_\infty^\pi \cdot K^{\mathrm{unr}}$ is the maximal abelian extension $K^{\mathrm{ab}}$ of $K$, and the map* $\mathrm{Art} : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ *is independent of all the choices.*

2. *If $L/K$ is a finite abelian extension, then* Art *gives rise to an isomorphism between* $\mathrm{Gal}(L/K)$ *and* $K^\times/\mathrm{N}_{L/K}(L^\times)$.

3. *This gives a bijection between the set of closed (resp. open) subgroups of $K^\times$ and the set of all (resp. all finite) abelian extensions of $K$.*

4. *If $L/K$ is any finite extension, then the following diagram commutes*

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{Art}_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K). \end{array}$$

***Corollary 15.2.*** — *There is an unramified character $\eta : G_K \to \mathbf{Z}_p^\times$ such that if $g \in G_K$, then $\mathrm{N}_{K/\mathbf{Q}_p}(\chi_\pi(g)) = \chi_{\mathrm{cyc}}(g)\eta(g)$.*

*Proof.* — Take $g \in G_K$ such that $n(g) \in \mathbf{Z}$ (where $g = \mathrm{Fr}_q^{n(g)}$ on $\overline{\mathbf{F}}_p$). Write $q = p^f$. We have $\mathrm{Art}_K^{-1}(g) = \pi^{n(g)}\chi_\pi(g)^{-1}$ and $\mathrm{Art}_{\mathbf{Q}_p}^{-1}(g) = p^{fn(g)}\chi_{\mathrm{cyc}}(g)^{-1}$. The commutative diagram in theorem 15.1 implies that $\mathrm{N}_{K/\mathbf{Q}_p}(\chi_\pi(g)) = \chi_{\mathrm{cyc}}(g) \cdot (\mathrm{N}_{K/\mathbf{Q}_p}(\pi)/p^f)^{n(g)}$. □

## 16. Galois cohomology

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

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

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

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

Other examples are: if $M$ is abelian and $G$ acts trivially on $M$, then $H^1(G, M) = \mathrm{Hom}(G, M)$. If $G$ is finite cyclic generated by $g$ and $M$ is abelian, then $H^1(G, M) =$

$\ker(\mathrm{N})/(1-g)M$ where $\mathrm{N}(x) = \sum_g g(x)$. If $G$ is infinite topologically generated by $g$, and $M$ is abelian and finite, then $H^1(G,M) = M/(1-g)M$.

If $0 \to X \to E \to Y \to 0$ is an exact sequence of $R$-modules with a continuous action of $G$, then we have a long exact sequence $0 \to X^G \to E^G \to Y^G \xrightarrow{\delta} H^1(G,X) \to H^1(G,E) \to H^1(G,Y)$, where the map $\delta : Y^G \to H^1(G,X)$ is defined as follows : if $y \in Y^G$ is the image of $e \in E$, then $\delta(y)(g) = e - g(e)$.

Finally, note that if $M$ is an abelian group, we can define cohomology groups $H^i(G,M)$ for all $i \geq 0$. They are spaces of cocycles, which are certain maps $c : G^i \to M$, modulo an equivalence relation.

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

***Theorem 16.1***. — *If $G$, $M$ and $H$ are as above, then :*

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

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

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

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

***Theorem 16.2***. — *If $L/K$ is a finite Galois extension and $G = \mathrm{Gal}(L/K)$, then :*

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

***Lemma 16.3***. — *If $L$ is an infinite field and if $\sigma_1, \ldots, \sigma_n$ are the elements of a finite group of automorphisms of $L$, then $\sigma_1, \ldots, \sigma_n$ are algebraically independant over $L$.*

*Proof.* — This is Artin's theorem on the algebraic independance of characters. See for instance Lang's Algebra, chapter VI, theorem 12.2 for a proof. □

*Proof of theorem 16.2.* — Choose some $U \in H^1(G, \mathrm{GL}_d(L))$. For $\alpha \in L$, define $P(\alpha) = \sum_{h\in G} h(\alpha)U(h)$. The cocyle relation gives us $U(g) \cdot g(P(\alpha)) = P(\alpha)$ so that in order to prove (1), it is enough to show that there exists some $\alpha \in L$ such that $P(\alpha)$ is invertible.

We do this in the case when $L$ is infinite (the case of a finite field is an exercise). Let $\{X_g\}_{g\in G}$ be a set of variables indexed by the elements of $G$, and consider the multivariable polynomial $Q(\{X_g\}_{g\in G}) = \det(\sum_{g\in G} X_g U(g))$. This polynomial is nonzero because the $U(g)$'s are invertible, and lemma 16.3 then gives us the existence of an $\alpha \in L$ such that $Q(\{g(\alpha)\}_{g\in G}) \neq 0$ so that $P(\alpha)$ is invertible, which proves (1).

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

***Corollary 16.4***. — *Let $L/K$ be a Galois extension with $G = \mathrm{Gal}(L/K)$ and give $L$ the discrete topology. If we consider only continuous cocycles, then $H^1(G, \mathrm{GL}_d(L)) = \{1\}$ and $H^1(G, L) = \{0\}$.*

*Proof.* — In both cases, such a cocyle factors through a finite quotient $\mathrm{Gal}(M/K)$ of $\mathrm{Gal}(L/K)$ and the field generated over $K$ by all the possible values of the cocycle is also a finite extension of $K$ so that we are in the situation of theorem 16.2. □

***Example 16.5***. — Let $L = K^{\mathrm{alg}}$ and $G = \mathrm{Gal}(L/K)$. We have an exact sequence $0 \to \mu_n \to L^\times \xrightarrow{x\mapsto x^n} L^\times \to 0$. The resulting long exact sequence and theorem 16.2 give us $H^1(G, \mu_n) = K^\times/(K^\times)^n$.

## 17. Periods of unramified characters of $G_K$

Let $\eta : G_K \to \mathbf{Z}_p^\times$ be a character. A period (in $\mathbf{C}_p$) for $\eta$ is an element $\alpha$ of $\mathbf{C}_p^\times$ such that $\eta(g) = g(\alpha)/\alpha$ for all $g \in G_K$. Which characters have periods in $\mathbf{C}_p$?

We say that $\eta$ is unramified if $\eta$ is trivial on $I_K$. In this case, $\eta$ factors through $\mathrm{Gal}(K^{\mathrm{unr}}/K)$.

***Theorem 17.1***. — *If $\eta : G_K \to \mathbf{Z}_p^\times$ is an unramified character, then there exists $\alpha \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^\times$ such that $g(\alpha) = \eta(g) \cdot \alpha$ for all $g \in G_K$.*

*Proof.* — We have $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_q)$, which is topologically generated by $\varphi_q$. It is therefore enough to prove that if $x \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^{\times}$, then there exists $y \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^{\times}$ such that $x = \varphi_q(y)/y$ (and apply this to $x = \eta(\varphi_q) \in \mathbf{Z}_p^{\times}$).

Since $x \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^{\times}$ we have $\overline{x} \in \overline{\mathbf{F}}_p^{\times}$ and $\overline{x}$ is of the form $z^{q-1}$ for some $z \in \overline{\mathbf{F}}_p^{\times}$. Take $y_1 \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^{\times}$ whose image is $z$. We then have $x = \varphi_q(y_1)/y_1 \cdot (1 + \pi x_1)$ with $x_1 \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$.

Assume that we have $x = \varphi_q(y_i)/y_i \cdot (1 + \pi^i x_i)$ with $x_i \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^{\times}$. We have $\overline{x}_i \in \overline{\mathbf{F}}_p$ and $\overline{x}_i$ is of the form $z_i^q - z_i$ for some $z_i \in \overline{\mathbf{F}}_p$. Take $v_i \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$ whose image is $z_i$. We have $x = \varphi_q(y_i(1+\pi^i v_i))/y_i(1+\pi^i v_i) \cdot (1+\pi^{i+1} x_{i+1})$ with $x_{i+1} \in \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$. We can therefore take $y_{i+1} = y_i(1 + \pi^i v_i)$ and $y = \lim y_i$. □

## 18. Periods of Lubin-Tate characters

Let $K$ be a finite extension of $\mathbf{Q}_p$ and let $\pi$ be a uniformizer of $K$ and let $\chi_\pi : G_K \to \mathcal{O}_K^{\times}$ be the Lubin-Tate character constructed in §14. Assume for simplicity that $K/\mathbf{Q}_p$ is unramified of degree $h$, so that it is Galois over $\mathbf{Q}_p$ and $\mathrm{Gal}(K/\mathbf{Q}_p) = \mathbf{Z}/h\mathbf{Z}$, generated by the arithmetic Frobenius map $\sigma$. We then have $\pi = pu$ with $u \in \mathcal{O}_K^{\times}$. Let $q = p^h$.

***Theorem 18.1***. — *If $1 \leq k \leq h-1$, then there exists $x_k \in \mathbf{C}_p^{\times}$ such that $g(x_k) = \sigma^k(\chi_\pi(g)) \cdot x_k$ for all $g \in G_K$.*

If $f(X) = \sum_{i \geq 0} f_i X^i \in K[\![X]\!]$ and $g \in \mathrm{Gal}(K/\mathbf{Q}_p)$, let $f^g(X) = \sum_{i \geq 0} g(f_i) X^i$. Let $F$ be the Lubin-Tate group such that $[\pi](X) = \pi X + X^q$. Let $\{z_1, z_2, \ldots\}$ be a sequence of elements of $\mathfrak{m}_{\mathbf{C}_p}$ such that $z_1 \neq 0$, $[\pi](z_1) = 0$, and $[\pi](z_{n+1}) = z_n$ for $n \geq 1$.

***Lemma 18.2***. — *If $x, y \in \mathfrak{m}_{\mathbf{C}_p}$ and $x \equiv y \bmod p^n$, then $[\pi]^g(x) \equiv [\pi]^g(y) \bmod p^{n+1}$.*

*Proof.* — Immediate. □

***Lemma 18.3***. — *The sequence $\{[\pi^n]^{\sigma^k}(z_n^{p^k})\}_{n \geq 1}$ converges in $\mathfrak{m}_{\mathbf{C}_p}$.*

*Proof.* — We have $[\pi]^{\sigma^k}(z_{n+1}^{p^k}) \equiv z_{n+1}^{qp^k} \equiv z_n^{p^k} \bmod p$. By applying lemma 18.2 $n$ times, we get $[\pi^{n+1}]^{\sigma^k}(z_{n+1}^{p^k}) \equiv [\pi^n]^{\sigma^k}(z_n^{p^k}) \bmod p^{n+1}$. This implies the result. □

Let $y_k$ be the limit of the sequence in lemma 18.3.

***Lemma 18.4***. — *We have $\mathrm{val}_p(y_k) = 1 + p^k/(q-1)$.*

*Proof.* — We prove that $\mathrm{val}_p([\pi^n]^{\sigma^k}(z_n^{p^k})) = 1 + p^k/(q-1)$ for all $n \geq 1$.

We have $[\pi^n]^{\sigma^k}(z_n^{p^k}) = \prod_{[\pi^n]^{\sigma^k}(w)=0}(z_n^{p^k} - w)$. The roots of $[\pi^n]^{\sigma^k}(X)$ are either those of $[\pi^{n-1}]^{\sigma^k}(X)$, whose valuations are $>$ to that of $z_n^{p^k}$, or $q^{n-1}(q-1)$ roots of valuation $1/q^{n-1}(q-1) < \mathrm{val}_p(z_n^{p^k})$. The lemma follows. □

***Lemma 18.5***. — *If $g \in G_K$, then $g(y_k) = [\chi_\pi(g)]^{\sigma^k}(y_k)$.*

*Proof.* — We have $g(z_n) = [\chi_\pi(g)](z_n)$. By raising to the $p^k$th power, we get $g(z_n^{p^k}) \equiv [\chi_\pi(g)]^{\sigma^k}(z_n^{p^k}) \bmod p$. Applying $[\pi^n]^{\sigma^k}$ to both sides and using lemma 18.2, we get $g([\pi^n]^{\sigma^k}(z_n^{p^k})) \equiv [\chi_\pi(g)]^{\sigma^k}[\pi^n]^{\sigma^k}(z_n^{p^k}) \bmod p^{n+1}$. This implies the lemma. □

*Proof of theorem 18.1.* — Take $x_k = \log_F^{\sigma^k}(y_k)$. Lemma 18.5 and the fact that $\log_F \circ [a] = a \cdot \log_F$ imply that $g(x_k) = \sigma^k(\chi_\pi(g)) \cdot x_k$ if $g \in G_K$. We need to check that $x_k \neq 0$. In fact $\log_F = \int \omega_F = X + \sum_{j\geq 2} a_j X^j/j$ with $a_j \in \mathcal{O}_K$. Since $\mathrm{val}_p(y_k) > 1$, we have $\mathrm{val}_p(\sigma^k(a_j) y_k^j/j) > \mathrm{val}_p(y_k)$ for all $j \geq 2$. This implies that $\mathrm{val}_p(x_k) = \mathrm{val}_p(y_k)$. □

One motivating question for what follows is: is there a period in $\mathbf{C}_p$ for the cyclotomic character $\chi_{\mathrm{cyc}} : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathbf{Z}_p^\times$? And more generally for $\chi_\pi : \mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \to \mathcal{O}_K^\times$?

## 19. The Ax-Sen-Tate theorem

Let $K$ be an extension of $\mathbf{Q}_p$ contained in $\overline{\mathbf{Q}}_p$, and let $G_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$. By Galois theory, we have $K = \overline{\mathbf{Q}}_p^{G_K}$. What can we say about $\mathbf{C}_p^{G_K}$?

***Theorem 19.1***. — *We have $\mathbf{C}_p^{G_K} = \widehat{K}$.*

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

***Lemma 19.2***. — *Let $P(X) \in \overline{\mathbf{Q}}_p[X]$ be a monic polynomial of degree $n$, all of whose roots satisfy $\mathrm{val}_p(\alpha) \geq c$ for some constant $c$.*

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

*Proof.* — If we write $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ then $\mathrm{val}_p(a_i) \geq (n-i)\cdot c$ and $1/q! \cdot P^{(q)}(X) = \sum_{i=0}^{n-q} \binom{n-i}{q} a_{n-i} X^{n-i-q}$. The product of the roots of $P^{(q)}(X)$ is then $\pm a_q / \binom{n}{q}$ so that there is at least one root $\beta$ satisfying
$$\mathrm{val}_p(\beta) \geq \frac{1}{n-q}\left((n-q)c - \mathrm{val}_p\binom{n}{q}\right).$$
The lemma follows from the fact that in case (1), we have $\mathrm{val}_p(\binom{n}{q}) = 0$ while in case (2), we have $\mathrm{val}_p(\binom{n}{q}) = 1$. □

If $\alpha \in \overline{\mathbf{Q}}_p$, let $\Delta_K(\alpha) = \inf_{g\in G_K} \mathrm{val}_p(g(\alpha) - \alpha)$.

***Lemma 19.3***. — *If $\alpha \in \overline{\mathbf{Q}}_p$, then there exists $\delta \in K$ such that* $\mathrm{val}_p(\alpha-\delta) \geq \Delta_K(\alpha) - p/(p-1)^2$.

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

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

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

Let $Q(X)$ be the minimal polynomial of $\alpha$ over $K$ and let $P(X) = Q(X+\alpha)$. The roots of $P(X)$ are the $g(\alpha)-\alpha$ with $g \in G_K$. Lemma 19.2 applied to $P(X)$ gives us an element $\beta$ such that $\mathrm{val}_p(\beta) \geq c$ or $\mathrm{val}_p(\beta) \geq c - 1/p^m(p-1)$ depending on the nature of $n$. Let $\alpha' = \beta + \alpha$, which is a root of $Q^{(q)}(X)$. We then have $[K(\alpha') : K] < [K(\alpha) : K]$ while $g(\alpha') - \alpha' = g(\alpha'-\alpha) + g(\alpha) - \alpha + \alpha - \alpha'$, so that either $\Delta_K(\alpha') \geq \Delta_K(\alpha)$ or $\Delta_K(\alpha') \geq \Delta_K(\alpha) - 1/p^m(p-1)$. This allows us to finish the proof by induction. □

*Proof of theorem 19.1*. — If $\alpha \in \mathbf{C}_p$ then we can write $\alpha = \lim \alpha_n$ with $\alpha_n \in \overline{\mathbf{Q}}_p$. We then have $\Delta_K(\alpha_n) \to +\infty$ and lemma 19.3 gives us a sequence $\{\delta_n\}_{n\geq 1}$ with $\delta_n \in K$ and $\mathrm{val}_p(\alpha_n - \delta_n) \to +\infty$ so that $\alpha$ is a limit of elements of $K$. □

## 20. Tate's normalized traces

Let $F = \mathbf{Q}_p$ and $F_n = \mathbf{Q}_p(\mu_{p^n})$ and $F_\infty = \cup_{n\geq 1} F_n$. If $x \in F_\infty$ and $n \geq 1$, then $x \in F_{n+k}$ for $k \gg 0$ and $R_n(x) = p^{-k} \mathrm{Tr}_{F_{n+k}/F_n}(x)$ does not depend on such a $k$. This defines a $F_n$-linear projection $R_n : F_\infty \to F_n$ which commutes with the action of $G_F$. Note also that $R_n \circ R_m = R_{\min(m,n)}$.

***Lemma 20.1***. — *If $k \geq 0$ and $n \geq 1$, then*

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

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

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

***Corollary 20.2***. — *If $x \in F_\infty$ then* $\mathrm{val}_p(R_n(x)) > \mathrm{val}_p(x) - \mathrm{val}_p(\zeta_{p^n} - 1)$.

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

***Theorem 20.3***. — *If $\psi : \mathrm{Gal}(F_\infty/F) \to \mathbf{Z}_p^\times$ is of infinite order, and if $x \in \mathbf{C}_p$ is such that $g(x) = \psi(g) \cdot x$ for all $g \in G_F$, then $x = 0$.*

*Proof.* — If $h \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/F_\infty)$, then $h(x) = x$, so that $x \in \mathbf{C}_p^{\mathrm{Gal}(\overline{\mathbf{Q}}_p/F_\infty)}$. By theorem 19.1, this implies that $x \in \hat{F}_\infty$. If $g \in G_F$, then $g(x) = \psi(g) \cdot x$ so that if $n \geq 1$, then $g(R_n(x)) = \psi(g) \cdot R_n(x)$. If $R_n(x) \neq 0$, then $\psi$ is trivial on $G_{F_n}$. Since $\psi$ is of infinite order, we have $R_n(x) = 0$ for all $n \geq 0$ and hence $x = \lim R_n(x) = 0$. □

We now extend these constructions to the cyclotomic extension of $K$, where $K$ is a finite extension of $\mathbf{Q}_p$. We know that $F_n$ is a totally ramified extension of $F$ of degree $p^{n-1}(p-1)$ and that $\mathcal{O}_{F_n} = \mathbf{Z}_p[\zeta_{p^n}]$. If $K$ is a finite extension of $\mathbf{Q}_p$ and $K_n = K(\zeta_{p^n})$ for $n \geq 1$, the above properties are no longer necessarily true.

***Proposition 20.4***. — *If $K$ is a finite extension of $\mathbf{Q}_p$, there exists $n(K) \geq 1$ such that if $n \geq n(K)$, then*

1. *$[K_{n+1} : F_{n+1}] = [K_n : F_n]$;*
2. *$K_{n+1}/K_n$ is totally ramified of degree $p$;*
3. *$\chi_{\mathrm{cyc}} : \mathrm{Gal}(K_\infty/K_n) \to 1 + p^n\mathbf{Z}_p$ is an isomorphism.*

*Proof.* — Since $K_{n+1} = K_nF_{n+1}$, the sequence $\{[K_n : F_n]\}_{n\geq 1}$ is decreasing, and therefore equal to $d = [K_\infty : F_\infty]$ for $n \geq n_0(K)$. Since $F_n \subset K_n$, we have $f(K_n/F) = f(K_n/F_n) \leq [K_n : F_n]$, so that $f(K_n/F) \leq d$ and $f(K_n/F)$ is equal to $f(K_\infty/F)$ for $n \geq n_1(K)$.

Take $n \geq \max(n_0(K), n_1(K))$. We have $[K_{n+1} : F_{n+1}] = [K_n : F_n]$ so that $[K_{n+1} : K_n] = [F_{n+1} : F_n] = p$. In addition, $f(K_{n+1}/K_n) = f(K_{n+1}/F)/f(K_n/F) = 1$ so that $K_{n+1}/K_n$ is totally ramified. The extension $K_\infty/F_n$ is then the compositum of the disjoint extensions $F_\infty/F_n$ and $K_n/F_n$ so that $\mathrm{Gal}(K_\infty/K_n) = \mathrm{Gal}(F_\infty/F_n)$. □

Take $n = n(K)$ and $m \geq n$. If $e_1, \ldots, e_d$ is a basis of $K_n$ over $F_n$, then it is also a basis of $K_{n+k}$ over $F_{n+k}$ for all $k \geq 1$ and of $K_\infty$ over $F_\infty$. Let $e_1^*, \ldots, e_d^*$ denotes the dual basis (for the pairing $(x, y) \mapsto \mathrm{Tr}_{K_n/F_n}(xy)$). If $x \in K_{n+k}$ then we can write $x = \sum_{i=1}^d x_i e_i^*$ where $x_i = \mathrm{Tr}_{K_{n+k}/F_{n+k}}(xe_i) \in F_{n+k}$. We then define $R_m(x) = \sum_{i=1}^d R_m(x_i)e_i^*$ which gives a projection $R_m : K_{n+k} \to K_m$ and $R_m : K_\infty \to K_m$ as before.

Note that $R_m$ is independent of the choice of $e_1, \ldots, e_d$.

***Proposition 20.5***. — *There exists $C$ such that $\mathrm{val}_p(R_m(x)) \geq \mathrm{val}_p(x) - C$ if $x \in K_\infty$.*

*Proof.* — Take $\ell$ such that all the $e_i$ and $e_i^*$ are in $p^{-\ell}\mathcal{O}_{K_n}$. If $x \in \mathcal{O}_{K_{n+k}}$, then $x_i = \mathrm{Tr}_{K_{n+k}/F_{n+k}}(xe_i) \in p^{-\ell}\mathcal{O}_{F_{n+k}}$. We have $R_m(x_i) \in p^{-\ell-1}\mathcal{O}_{F_m}$ by corollary 20.2 and hence $R_m(x) \in p^{-2\ell-1}\mathcal{O}_{K_m}$. This implies the proposition with $C = 2\ell + 2$. □

The maps $R_m$ therefore extend to $\hat{K}_\infty$ and satisfy the properties (1) $x = \lim_m R_m(x)$ (2) $g \circ R_m = R_m \circ g$ if $g \in \mathrm{Gal}(K_\infty/K_{n(K)})$. This way we get the following extension of theorem 20.3.

***Corollary 20.6***. — *If $\psi : \mathrm{Gal}(K_\infty/K) \to \mathbf{Z}_p^\times$ is of infinite order, and if $x \in \mathbf{C}_p$ is such that $g(x) = \psi(g) \cdot x$ for all $g \in G_K$, then $x = 0$.*

***Corollary 20.7***. — *Let $K$ be a finite unramified extension of $\mathbf{Q}_p$ and let $\pi$ be a uniformizer of $K$. If $x \in \mathbf{C}_p$ is such that $g(x) = \chi_\pi(g) \cdot x$ for all $g \in G_K$, then $x = 0$.*

*Proof.* — By theorem 18.1, $\tau \circ \chi_\pi$ has a period in $\mathbf{C}_p$ for all $\tau \neq \mathrm{Id} \in \mathrm{Gal}(K/\mathbf{Q}_p)$. By corollary 15.2, $\mathrm{N}_{K/\mathbf{Q}_p}(\chi_\pi) = \chi_{\mathrm{cyc}}\eta$ where $\eta : G_K \to \mathbf{Z}_p^\times$ is unramified, and therefore has a period by theorem 17.1. If $\chi_\pi$ had a period, then so would $\chi_{\mathrm{cyc}}$, a contradiction with corollary 20.6. □

## 21. Rings of periods and admissible representations

Let $\mu : G_K \to \mathbf{Z}_p^\times$ be a character, let $\mathbf{Q}_p(\mu)$ be the one dimensional representation of $G_K$ on which $G_K$ acts by $\mu$, let $\mathbf{C}_p(\mu) = \mathbf{C}_p \otimes \mathbf{Q}_p(\mu)$, a semilinear $\mathbf{C}_p$-representation of $G_K$. The space $\mathbf{C}_p(\mu)^{G_K}$ is a $K$-vector space of dimension 1 or 0 depending on whether $\mu$ has a period in $\mathbf{C}_p$ or not.

If $V$ is a $p$-adic representation of $G_K$ of dimension $d$, then $\mathbf{C}_p \otimes V$ is a semilinear $\mathbf{C}_p$-representation of $G_K$ of dimension $d$, and $(\mathbf{C}_p \otimes V)^{G_K}$ is a $K$-vector space. We have a map $\alpha : \mathbf{C}_p \otimes_K (\mathbf{C}_p \otimes V)^{G_K} \to \mathbf{C}_p \otimes V$.

***Proposition 21.1***. — *The map $\alpha$ is injective.*

*Proof.* — Suppose that it is not injective, and take $x \neq 0 \in \ker \alpha$. We can write $x = x_1 \otimes d_1 + \cdots + x_r \otimes d_r$ with $x_i \in \mathbf{C}_p$ and $d_i \in (\mathbf{C}_p \otimes V)^{G_K}$ and we can assume that $r$ is minimal, in particular that $x_i \neq 0$. We can also divide $x$ by $x_1$ and assume that $x_1 = 1$.

If $g \in G_K$, then $g(x) = 1 \otimes d_1 + g(x_2) \otimes d_2 + \cdots + g(x_r) \otimes d_r$ and $g(x) - x \in \ker \alpha$ is a tensor of rank $\leq r - 1$, so that $g(x) - x = 0$ by minimality of $r$. If $g(x_i) - x_i \neq 0$ for some $g$ and some $i$, then $1 \otimes d_i$ is a linear combination of the other $1 \otimes d_j$ which would contradict the minimality of $r$. Hence $x_i \in \mathbf{C}_p^{G_K} = K$ for all $i$ and hence $r = 1$. □

This implies that $(\mathbf{C}_p \otimes V)^{G_K}$ is a $K$-vector space of dimension at most $d$. We say that $V$ is $\mathbf{C}_p$-admissible if the dimension is equal to $d$, ie if $\alpha$ is an isomorphism.

More generally, we can study rings of periods. These are $\mathbf{Q}_p$-algebras $B$ with an action of $G_K$. Given a $\mathbf{Q}_p$-representation $V$ of $G_K$, we say that $V$ is $B$-admissible if

the semilinear $B$-representation $B \otimes V$ is trivial (ie isomorphic to $B^d$ as a semilinear $B$-representation). In order for the theory to work well, we assume that (Per1) $B$ is a domain (Per2) $(\operatorname{Frac} B)^{G_K} = B^{G_K}$ (Per3) if $\delta \in B$ is such that $g(\mathbf{Q}_p\delta) = \mathbf{Q}_p\delta$ for all $g \in G_K$, then $\delta \in B^\times$. Given $B$ and $V$, let $D_B(V) = (B \otimes V)^{G_K}$. We have a map

$$\alpha : B \otimes_{B^{G_K}} D_B(V) \to B \otimes V.$$

***Proposition 21.2***. — *The map $\alpha$ is injective. Furthermore, the following are equivalent*

1. *$V$ is $B$-admissible;*
2. *$\alpha$ is an isomorphism;*
3. $\dim_{B^{G_K}} D_B(V) = \dim V$.

*Proof.* — The proof that $\alpha$ is injective is similar to the proof of proposition 21.1: if $x = x_1 \otimes d_1 + \cdots + x_r \otimes d_r \in \ker \alpha$ and $g \in G_K$ then $x_1 g(x) - g(x_1)x \in \ker \alpha$ so that by minimality, $x/x_1 \in (\operatorname{Frac} B \otimes_{B^{G_K}} D_B(V))^{G_K} = D_B(V)$ by (Per2).

The implications (1) implies (2) and (3), and (2) implies (1) and (3) are easy. Let us prove that (3) implies (1). Choose bases of $V$ over $\mathbf{Q}_p$ and of $D_B(V)$ over $B^{G_K}$ and let $\delta = \det \operatorname{Mat}(\alpha)$. Since $\alpha$ is injective, we have $\delta \neq 0$. If $g \in G_K$, then $g(\delta) = \det \operatorname{Mat}(g|V)\delta$, so that by (Per3), $\delta \in B^\times$ and $\alpha$ is an isomorphism. □

As an exercise, prove that $V$ is $\overline{\mathbf{Q}}_p$-admissible if and only if there exists a finite extension $L/K$ such that $V|_{G_L}$ is trivial. It is much more difficult to prove the following theorem of Sen: $V$ is $\mathbf{C}_p$-admissible if and only if there exists a finite extension $L/K$ such that $V|_{I_L}$ is trivial.

## 22. The ring $\mathbf{B}_{\mathrm{HT}}$

Let $\mathbf{B}_{\mathrm{HT}} = \mathbf{C}_p[t, t^{-1}]$, with the action of $G_K$ given by $g(\sum a_i t^i) = \sum g(a_i)\chi_{\mathrm{cyc}}(g)^i t^i$. This ring contains a period for the cyclotomic character. The fraction field of $\mathbf{B}_{\mathrm{HT}}$ is included in the field $\mathbf{C}_p[\![t]\!][t^{-1}]$.

***Proposition 22.1***. — *The ring $\mathbf{B}_{\mathrm{HT}}$ satisfies conditions (Per1-3).*

*Proof.* — The ring $\mathbf{B}_{\mathrm{HT}}$ is clearly a domain. The action of $G_K$ on $\mathbf{C}_p[\![t]\!][t^{-1}]$ is still given by $g(\sum a_i t^i) = \sum g(a_i)\chi_{\mathrm{cyc}}(g)^i t^i$ and hence $(\mathbf{C}_p[\![t]\!][t^{-1}])^{G_K} = K$. Take $x \in \mathbf{B}_{\mathrm{HT}}$ such that $g(x) = \mu(g)x \in \mathbf{Q}_p^\times \cdot x$, with $x = \sum x_i t^i$. We have $g(x_i)\chi(g)^i = \mu(g)x_i$ for all $i$. If $x_i$ and $x_j$ are $\neq 0$ for $i \neq j$, then $g(x_i/x_j) = \chi(g)^{j-i}(x_i/x_j)$ for $g \in G_K$, not possible. Hence $x = x_i t^i \in \mathbf{B}_{\mathrm{HT}}^\times$. □

If $V$ is a $p$-adic representation of $G_K$, we let $\mathbf{D}_{\mathrm{HT}}(V) = (\mathbf{B}_{\mathrm{HT}} \otimes V)^{G_K}$. This is a $K$-vector space of dimension $\leq \dim V$, and we say that $V$ is Hodge-Tate if there is equality.

For example, recall that every $x \in \mathbf{Z}_p^\times$ can be written as $\omega(x)\langle x \rangle$. If $r \in \mathbf{Z}/(p-1)\mathbf{Z}$ and $s \in \mathbf{Z}_p$, we have the character $g \mapsto \omega(\chi_{\mathrm{cyc}}(g))^r \langle \chi_{\mathrm{cyc}}(g) \rangle^s$. This character is Hodge-Tate if and only if $s \in \mathbf{Z}$. Let $\mathbf{C}_p(h)$ denote the representation $\mathbf{C}_p(\chi_{\mathrm{cyc}}^h)$.

***Proposition 22.2.*** — *A $p$-adic representation $V$ is Hodge-Tate if and only if there exists $h_1, \dots, h_d \in \mathbf{Z}$ such that $\mathbf{C}_p \otimes V = \oplus_{i=1}^d \mathbf{C}_p(h_i)$.*

*Proof.* — It is clear that if $\mathbf{C}_p \otimes V = \oplus_{i=1}^d \mathbf{C}_p(h_i)$, then $V$ is Hodge-Tate. Conversely, if $x \in \mathbf{B}_{\mathrm{HT}} \otimes V$, then we can write $x = \sum x_i t^i$ with $x_i \in \mathbf{C}_p \otimes V$, and $g(x) = \sum g(x_i) \chi_{\mathrm{cyc}}(g)^i t^i$. We have $x \in (\mathbf{B}_{\mathrm{HT}} \otimes V)^{G_K}$ if and only if $g(x_i)\chi_{\mathrm{cyc}}(g)^i = x_i$, that is if $x_i \in (\mathbf{C}_p(i) \otimes V)^{G_K}$. We deduce that $(\mathbf{B}_{\mathrm{HT}} \otimes V)^{G_K} \simeq \oplus (\mathbf{C}_p(i) \otimes V)^{G_K}$.

The map $\alpha$ gives rise to an injection $\mathbf{C}_p(-i) \otimes_K (\mathbf{C}_p(i) \otimes V)^{G_K} \to \mathbf{C}_p \otimes V$, so that if $\dim_K (\mathbf{C}_p(i) \otimes V)^{G_K} = d_i$, then $\mathbf{C}_p \otimes V$ contains $\mathbf{C}_p(-i)^{d_i}$. The proposition follows. □

The integers $h_1, \dots, h_d$ are called the Hodge-Tate weights of $V$. For example, the Hodge-Tate weight of $\chi_{\mathrm{cyc}}$ is 1.

***Theorem 22.3.*** — *Let $K$ be the unramified extension of $\mathbf{Q}_p$ of dimension $h$, let $\pi$ be a uniformizer of $K$, and let $\chi_\pi$ be the corresponding Lubin-Tate character and $V$ the $h$-dimensional representation of $G_K$ coming from $\chi_\pi : G_K \to \mathcal{O}_K^\times \subset \mathrm{GL}_h(\mathbf{Z}_p)$.*

*The representation $V$ is Hodge-Tate with weights $1, 0 \dots, 0$.*

*Proof.* — Recall that $\mathbf{C}_p \otimes K$ can be computed by writing $K = \mathbf{Q}_p(\alpha) = \mathbf{Q}_p[X]/P_{\min,\alpha}(X)$ and

$$\mathbf{C}_p \otimes K = \mathbf{C}_p \otimes \mathbf{Q}_p[X]/P_{\min,\alpha}(X) = \mathbf{C}_p[X]/P_{\min,\alpha}(X) = \prod_{\tau \in \mathrm{Gal}(K/\mathbf{Q}_p)} \mathbf{C}_p$$

with the last map sending $X$ to $(\tau(\alpha))_\tau$. We get $\mathbf{C}_p \otimes K = \prod_\tau \mathbf{C}_p$ via the map $x \otimes k \mapsto (x\tau(k))_\tau$. This implies that $\mathbf{C}_p \otimes K(\chi_\pi) = \prod_\tau \mathbf{C}_p(\tau \circ \chi_\pi)$.

For $\tau \neq \mathrm{Id}$, the character $\tau \circ \chi_\pi$ has a period in $\mathbf{C}_p$, so that $\mathbf{C}_p(\tau \circ \chi_\pi) = \mathbf{C}_p(0)$. We have also seen that $\chi_\pi/\chi_{\mathrm{cyc}}$ has a period in $\mathbf{C}_p$, so that $\mathbf{C}_p(\chi_\pi) = \mathbf{C}_p(1)$. □

More generally, one can prove that if $F$ is a formal group over $\mathcal{O}_K$ of height $h$, then $V = V_p F$ is Hodge-Tate with weights $1, 0 \dots, 0$.

## 23. The different

Let $K$ be a finite extension of $\mathbf{Q}_p$ and let $L$ be a finite extension of $K$. The bilinear form $L \times L \to K$ given by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerate and if $I$ is a fractional

ideal of $L$, we set $\check{I} = \{y \in L \text{ such that } \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } x \in I\}$. The different of the extension $L/K$ is the ideal $\mathfrak{d}_{L/K} = (\check{\mathcal{O}}_L)^{-1}$. Note that $\check{\mathcal{O}}_L$ contains $\mathcal{O}_L$, so that $\mathfrak{d}_{L/K}$ is an ideal of $\mathcal{O}_L$. Let $\mathrm{val}_K(\cdot)$ and $\mathrm{val}_L(\cdot)$ denote the normalized valuations on $K$ and $L$.

***Proposition 23.1***. — 1. *If $I$ is an ideal of $\mathcal{O}_L$, then $\check{I} = I^{-1}\mathfrak{d}_{L/K}^{-1}$;*
2. *If $I_K$ and $I_L$ are ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$, then $\mathrm{Tr}_{L/K}(I_L) \subset I_K$ iff $I_L \subset I_K\mathfrak{d}_{L/K}^{-1}$;*
3. $\mathrm{val}_K(\mathrm{Tr}_{L/K}(I)) = \lfloor \mathrm{val}_K(I \cdot \mathfrak{d}_{L/K})\rfloor$.

*Proof.* — If $I = \pi_L^r\mathcal{O}_L$, then $\check{I} = \pi_L^{-r}\check{\mathcal{O}}_L = I^{-1}\check{\mathcal{O}}_L$. This proves (1). We have $\mathrm{Tr}_{L/K}(I_L) \subset I_K$ iff $\mathrm{Tr}_{L/K}(I_K^{-1}I_L) \subset \mathcal{O}_K$ iff $I_K^{-1}I_L \subset \mathfrak{d}_{L/K}^{-1}$, which proves (2). In particular, $\mathrm{Tr}_{L/K}(I)$ is the smallest ideal $J$ of $\mathcal{O}_K$ such that $J \cdot \mathcal{O}_L$ contains $I \cdot \mathfrak{d}_{L/K}$, which implies (3). □

Item (3) implies that if $I = \pi_L^n\mathcal{O}_L$ and $\mathfrak{d}_{L/K} = \pi_L^m$, then $\mathrm{Tr}_{L/K}(I) = \pi_K^{\lfloor (m+n)/e(L/K)\rfloor}\mathcal{O}_K$.

***Corollary 23.2***. — *If $L/K/F$ is a tower of extensions, then $\mathfrak{d}_{L/F} = \mathfrak{d}_{L/K} \cdot \mathfrak{d}_{K/F}$.*

*Proof.* — If $x \in \mathcal{O}_L$, then $x \in \mathfrak{d}_{L/F}^{-1}$ iff $\mathrm{Tr}_{L/F}(x\mathcal{O}_L) \subset \mathcal{O}_F$ iff $\mathrm{Tr}_{K/F}\,\mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_F$ iff $\mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathfrak{d}_{K/F}^{-1}$ iff $x\mathcal{O}_L \subset \mathfrak{d}_{L/K}^{-1}\mathfrak{d}_{K/F}^{-1}$. □

***Theorem 23.3***. — *If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $\mathfrak{d}_{L/K} = P'_{\min,\alpha}(\alpha) \cdot \mathcal{O}_L$.*

*Proof.* — Let $P = P_{\min,\alpha}$ and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be the roots of $P$. We first prove that $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 0$ if $k = 1, \ldots, d-1$ and $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 1$ if $k = d$ and $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) \in \mathcal{O}_K$ for all $k \geq 1$. We have

$$\frac{1}{P(T)} = \sum_{i=1}^{d} \frac{1}{P'(\alpha_i)(T-\alpha_i)}.$$

Write $P(T) = T^d + p_{d-1}T^{d-1} + \cdots + p_0 = T^d(1 + p_{d-1}/T + \cdots + p_0/T^d)$. We have

$$\frac{1}{P(T)} = \frac{1}{T^d(1 + p_{d-1}/T + \cdots + p_0/T^d)} = \frac{1}{T^d}(1 - \frac{p_{d-1}}{T} + \cdots) \in \mathcal{O}_K[\![\frac{1}{T}]\!],$$

so that

$$\sum_{i=1}^{d} \frac{1}{P'(\alpha_i)T(1-\alpha_i/T)} = \sum_{k\geq 1} \frac{1}{T^k} \sum_{i=1}^{d} \frac{\alpha_i^{k-1}}{P'(\alpha_i)}$$
$$= \sum_{k\geq 1} \frac{1}{T^k}\,\mathrm{Tr}_{L/K}\left(\frac{\alpha^{k-1}}{P'(\alpha)}\right) = \frac{1}{T^d}(1 - \frac{p_{d-1}}{T} + \cdots) \in \mathcal{O}_K[\![\frac{1}{T}]\!].$$

This tells us that $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 0$ if $k = 1, \ldots, d-1$ and $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 1$ if $k = d$ and $\mathrm{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) \in \mathcal{O}_K$ for all $k \geq 1$, so that $P'(\alpha)^{-1}\mathcal{O}_L \subset \check{\mathcal{O}}_L$.

Take $y \in \check{\mathcal{O}}_L$ and write $y = y_0/P'(\alpha) + y_1\alpha/P'(\alpha) + \cdots + y_{d-1}\alpha^{d-1}/P'(\alpha)$ with $y_i \in K$. We have $\mathrm{Tr}_{L/K}(y) = y_{d-1}$ so that $y_{d-1} \in \mathcal{O}_K$, and then $\mathrm{Tr}_{L/K}(\alpha y) = y_{d-2} +$

$\mathrm{Tr}_{L/K}(y_{d-1}\alpha^d/P'(\alpha))$ so that $y_{d-2} \in \mathcal{O}_K$, and by induction $y_i \in \mathcal{O}_K$ for all $i$. This shows that $\check{\mathcal{O}}_L \subset P'(\alpha)^{-1}\mathcal{O}_L$. □

***Corollary 23.4***. — *If $L/K$ is a Galois extension and $G = \mathrm{Gal}(L/K)$, then $\mathrm{val}_L(\mathfrak{d}_{L/K}) = \sum_{g\neq 1\in G} i_L(g) = \int_{-1}^{\infty}(|G_t|-1)dt$.*

*Proof.* — We have $\mathrm{val}_L(\mathfrak{d}_{L/K}) = \mathrm{val}_L(P'(\alpha)) = \sum_{g\neq 1\in G}\mathrm{val}_L(g(\alpha)-\alpha) = \sum_{g\neq 1\in G} i_L(g)$. Next, note that $i_L(g) = i+1$ if and only if $g \in G_i \setminus G_{i+1}$, and the second formula follows, by integrating by parts. □

***Corollary 23.5***. — *We have $\mathrm{val}_K(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(1-1/|G^u|)du$.*

*Proof.* — By the previous corollary, $\mathrm{val}_L(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(|G_t|-1)dt$. Let $t = \psi_{L/K}(u)$ where $\psi_{L/K}$ is the function defined after proposition 8.9. We have $\psi'_{L/K}(u) = [G^0 : G^u]$, so that $\mathrm{val}_L(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(|G^u|-1)|G^0|/|G^u|du$. The corollary follows, since $|G^0| = e(L/K)$ and $\mathrm{val}_L(\cdot) = e(L/K)\,\mathrm{val}_K(\cdot)$. □

If $L/K$ is a Galois extension, let $L^u = L^{\mathrm{Gal}(L/K)^u}$. If $L/K$ is not Galois, and $L$ is contained in some Galois extension $M$ of $K$, then $L^u = M^u \cap L$ does not depend on $M$ by Herbrand's theorem.

***Theorem 23.6***. — *If $L/K$ is a finite (not necessarily Galois) extension, then*

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

*Proof.* — If $L/K$ is Galois, this follows from the above corollaries. In general, the proof requires a bit more work. □

## 24. Ramification in cyclotomic extensions

Recall that $K_n = K(\mu_{p^n})$.

***Theorem 24.1***. — *If $K$ is a finite extension of $F = \mathbf{Q}_p$, then $\{p^n \mathrm{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n\geq 1}$ is bounded.*

*Proof.* — Applying theorem 23.6, we get (the upper numbering is with respect to $F$)

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

By subtracting, we get

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

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

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

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

***Proposition 24.2.*** — *If $L/K$ is a finite extension, then* $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty}) = \mathfrak{m}_{K_\infty}$.

*Proof.* — Take $n \geq \max(n(K), n(L))$. Proposition 23.1 implies that $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n}) = \mathfrak{m}_{K_n}^{c_n}$ where $c_n = \lfloor \operatorname{val}_{K_n}(\mathfrak{m}_{L_n} \cdot \mathfrak{d}_{L_n/K_n}) \rfloor$ and theorem 24.1 implies that the sequence $\{\operatorname{val}_{K_n}(\mathfrak{d}_{L_n/K_n})\}_{n \geq 1}$ is bounded. This shows that there exists some constant $c$ such that $c_n \leq c$ for all $n$ and hence that $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n}) \supset \mathfrak{m}_{K_n}^c$ for all $n \gg 0$.

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

## References


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

[FV02] I. B. Fesenko & S. V. Vostokov – *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002, With a foreword by I. R. Shafarevich.

[Gou97] F. Q. Gouvêa – *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction.

[Kob84] N. Koblitz – *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.

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

[Neu99] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rob00] A. M. Robert – *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.

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

[Sil09] J. H. Silverman – *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[ST115] *Correspondance Serre-Tate. Vol. I* – Documents Mathématiques (Paris) [Mathematical Documents (Paris)], vol. 13, Société Mathématique de France, Paris, 2015, Edited, and with notes and commentaries by Pierre Colmez and Jean-Pierre Serre.

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

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