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 valation $\mathrm{val}_p(\cdot)$ 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 $\mathbf{Z}_p = \{x \in \mathbf{Q}_p$ 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 $p \nmid d$, $a = 1/d$ and $1 + px \in 1 + p\mathbf{Z}_p$, then $\sum_{k \geq 0} \binom{a}{k}(px)^k$ converges in $\mathbf{Z}_p$, to the unique dth root of $1 + px$ 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 a space endowed with an ultrametric norm, 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) if the space is moreover complete, then a series $\sum_{n \geq 1} x_n$ converges if and only if $x_n \to 0$,

Let $\mathcal{O}_K = \{x \in K$ such that $|x| \leq 1\}$ be the ring of integers of K, and let $\mathfrak{m}_K = \{x \in K$ 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 π any π such that $\mathrm{val}(\pi) = c$. Such an element is called a uniformizer of $\mathcal{O}_K$. We then let 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 $K = k(\!(X)\!)$ 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. — *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 2.2. — *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 2.3. — *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 α has the required properties.

If α, β 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 $P(X) = X^p - X$ has p simple roots in $\mathbf{F}_p$ so that it has p 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 π and finite residue field k, then $K = k(\!(\pi)\!)$.*

Proof. — Let $q = \operatorname{card}(k)$. 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 lift. The theorem now follows from proposition 2.1. □

If K is of mixed characteristic and k is finite, then in proposition 2.1 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 $\|x_1e_1 + \cdots + x_de_d\| \leq \sup |x_i| \cdot (\sum \|e_i\|)$ so that $\|x\| \leq C\|x\|_\infty$ with $C = \sum \|e_i\|$.

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 ≥ 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 π be a uniformizer of $\mathcal{O}_K$. The ideal πA is a product $P_1^{e_1} \cdots P_r^{e_r}$. Let 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 $xA = P_1^{\mathrm{val}_1(x)} \cdots P_r^{\mathrm{val}_r(x)}$. The function $\mathrm{val}_i(\cdot)/e_i$ extends val_K.

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

5. Finite extensions

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

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

Proof. — Let S_K be a set of representatives of k_K in $\mathcal{O}_K$ and let $S_L = \sqcup_{i \in I} u_i S_K$, which is a set of representatives of k_L in $\mathcal{O}_L$. Let π_K be a uniformizer of $\mathcal{O}_K$. If $n \geq 0$, write $n = qe + r$. The theorem follows from applying proposition 2.1 with $\pi_n = \pi^r \pi_K^q$. □

Let $f(L/K) = [k_L : k_K]$.

Corollary 5.2. — *We have $e(L/K) f(L/K) = [L : K]$.*

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. — 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 π_L is a uniformizer of $\mathcal{O}_L$, then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ and π_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 π_L satisfies an Eisenstein equation. □

Conversely, if $P(X) \in \mathcal{O}_K[X]$ is an Eisenstein polynomial, and $P(\pi_L) = 0$, then π_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 complete normed field, and choose a valuation $\mathrm{val}(\cdot)$.

If $P(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$, then the Newton polygon $\mathrm{NP}(P)$ is the lower convex hull of the points $(0, \mathrm{val}(a_0))$, $(1, \mathrm{val}(a_1))$, $\ldots$, $(d, \mathrm{val}(a_d))$. 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^{alg} with valuation λ is equal to the length of the segment of $\mathrm{NP}(P)$ with slope $-\lambda$.*

Proof. — We can divide $P(X)$ by a_d and assume that $P(X)$ is monic. Assume that P has d_1 roots of valuation λ_1 and d_2 roots of valuation λ_2, etc, d_k roots of valuation λ_k with $\lambda_1 > \cdots > \lambda_k$. The coefficient a_i is $\pm$ the sum of all possible products of $d-i$ roots.

In particular, $a_{d_1+\cdots+d_{s-1}}$ is the sum of a term of valuation $d_s\lambda_s + \cdots + d_k\lambda_k$ and of terms which are all of valuation $> d_s\lambda_s + \cdots + d_k\lambda_k$ so that

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

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 if $i = d_s$ 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^{alg} by $X \mapsto \alpha$ for each root α 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 $\lambda = \mathrm{val}(a_0)/\deg(P)$ 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 α, $\beta \in \overline{\mathbf{Q}}_p$ are such $|\alpha-\beta| < |\alpha-\alpha_i|$ for $i=2,\dots,n$ where the α_i are the conjugates of α over F (with $\alpha_1=\alpha$), then $F(\alpha)\subset F(\beta)$.*

Proof. — Let K be a finite Galois extension of F containing α and β, 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 $P(X) = a_0+\cdots+a_dX^d \in K[X]$, 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 $a=\{a_0,\dots,a_{e-1}\}\in\Pi=(\mathfrak{m}_F\setminus\mathfrak{m}_F^2)\times\mathfrak{m}_F^{e-1}$, 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 of them 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 Π 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. — We prove by induction on $\deg(P)$ that every polynomial $P(X) \in \mathbf{C}_p[X]$ of degree ≥ 1 has a root. We may assume that $P(X) \in \mathcal{O}_{\mathbf{C}_p}[X]$ is monic. Write $P(X) = \lim P_n(X)$ with $P_n(X) \in \overline{\mathbf{Q}}_p[X]$, and let $\alpha_n \in \overline{\mathbf{Q}}_p$ be a root of $P_n(X)$ so that $P(\alpha_n) \to 0$.

If $P'(\alpha_n)$ does not converge to 0, then Hensel's lemma implies that for $n \gg 0$, α_n gives rise to a root of $P(X)$. If $P'(\alpha_n) \to 0$, then by induction $P'(X)$ decomposes in $\mathbf{C}_p[X]$ and then α_n converges to one of its roots, which is then also a root of $P(X)$. □

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 and $\mathfrak{m}_{\mathbf{C}_p}$ is the p-adic open unit disk.

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 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 $u \in \mathbf{Z}_{\geq -1}$, then 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 subextension of L/K as in proposition 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 π_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 $u \geq 1$ 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 $g \in G_1$. 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 see 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 $u \geq 0$, 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:

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

so that 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 $u \geq 1$, 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 $n \geq 1$, which 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 $\mathrm{Gal}(K_n/K)_u = \mathrm{Gal}(K_n/K_j)$.

Define a function $\varphi_{L/K} : \mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$ by $\varphi_{L/K}(u) = \int_0^u [G_0 : G_t]^{-1} dt$.

Proposition 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 $\psi_{L/K} : \mathbf{R}_{\geq -1} \to \mathbf{R}_{\geq -1}$ denote the 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 $n \geq 1$, 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 σ 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 σ of L. If $\mathrm{Gal}(L/K)$ denotes the group of K-automorphisms of L, then we therefore have an isomorphism $\mathrm{Gal}(L/K) \simeq \varprojlim \mathrm{Gal}(E/K)$. We give $\mathrm{Gal}(L/K)$ the group topology, so that it is a compact topological group. Galois theory extends to a bijection between closed subgroups of $\mathrm{Gal}(L/K)$ and Galois 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^{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^{cyc} and K^{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. The Weierstrass preparation theorem

Let K be a finite extension of $\mathbf{Q}_p$, let π be a uniformizer of $\mathcal{O}_K$, and let $\mathcal{O}_K[\![X]\!]$ denote the set of power series with coefficients in $\mathcal{O}_K$. If $f(X) \in \mathcal{O}_K[\![X]\!]$ and $z \in \mathfrak{m}_{\mathbf{C}_p}$, we can evaluate $f(X)$ at z. What can we say about the zeroes of $f(X)$?

If $f(X) = f_0 + f_1X + \cdots$, 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 10.1. — *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.*

We prove the existence of q and r by applying a standard method, summarized in the lemma below, whose variants are known as "Nakayama's lemma".

Lemma 10.2. — *Let M and N be two $\mathcal{O}_K$-modules, such that*

1. *M is complete for the π-adic topology (ie $\sum_{k\geq 0} \pi^k m_k$ always converges in M)*
2. *N is separated for the π-adic topology (ie $\cap_{k\geq 0}\pi^k N = \{0\}$).*

If $f \in \mathrm{Hom}_{\mathcal{O}_K}(M, N)$ is such that $f : M \to N/\pi N$ is surjective, then f is surjective.

Proof. — Take $n \in N$. There exists $m_0 \in M$ and $n_1 \in N$ such that $n = f(m_0) + \pi n_1$. We prove by induction that there exists $m_k \in M$ and $n_k \in N$ such that $n = f(m_0 + \pi m_1 + \cdots + \pi^k m_k) + \pi^{k+1} n_{k+1}$. This is true for $k = 0$ and the case $k + 1$ follows from k by writing $n_{k+1} = f(m_{k+1}) + \pi n_{k+2}$.

Let $m = \sum_{k\geq 0} \pi^k m_k$. We have $n - f(m) \in \cap_{k\geq 0}\pi^k N = \{0\}$ so that $n = f(m)$. □

Proof of proposition 10.1. — Let $M = \mathcal{O}_K[\![X]\!] \times \mathcal{O}_K[X]_{\deg \leq n-1}$ and $N = \mathcal{O}_K[\![X]\!]$ and consider the map $(q, r) \mapsto qf + r$. By lemma 10.2, it is enough to prove that this map is surjective mod π. Take $g(X) \in k[\![X]\!]$. We can write $g(X) = g_0 + \cdots + g_{n-1}X^{n-1} + X^n h(X)$

and $\overline{f}(X) = X^n \times u(X)$ where u is a unit so that we can write $g = \overline{f}q + r$ with $r = g_0 + \cdots + g_{n-1}X^{n-1}$.

We now prove unicity. If $qf + r = 0$, then reducing mod π, we get that π divides r and hence q. By induction, this shows that $q = r = 0$. □

Corollary 10.3. — *If $\alpha \in \mathfrak{m}_K$ and $f(\alpha) = 0$, then $f(X) = (X - \alpha)q(X)$ 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 theorem 6.1, a distinguished polynomial has exactly $\deg(P)$ roots in $\mathfrak{m}_{\mathbf{C}_p}$.

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

Proof. — If we apply proposition 10.1 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 $\operatorname{wideg}(q) = 0$ 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 $\operatorname{wideg}(f)$ 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 $f(X) \in \mathcal{O}_K[\![X]\!]$, then*

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

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

Theorem 10.6. — *The ring $\mathcal{O}_K[\![X]\!]$ is a noetherian local ring, with maximal ideal (π, X), whose other prime ideals are (0), (π), and $(p(X))$ with p distinguished and irreducible.*

Proof. — Let us prove that $\mathcal{O}_K[\![X]\!]$ is noetherian. If $I = (\{f_i\}_i)$, we can write $f_i = \pi^{\mu_i}p_iu_i$ and $I = (\{\pi^{\mu_i}p_i\}_i)$. The ring $\mathcal{O}_K[X]$ is noetherian, and therefore so is $\mathcal{O}_K[\![X]\!]$.

Let I be a prime ideal and take $f = \pi^\mu pu \in I$ with p of least degree. Since I is prime, either $\pi \in I$ or $p \in I$. If both are in I, then $I = (\pi, p) = (\pi, X^n)$ so that $I = (\pi, X)$.

If $\pi \in I$ and $I \neq (\pi)$, then by the above $I = (\pi, X)$. If $p \in I$ and $\pi \notin I$ and $g = \pi^\nu qv \in I$, then $q \in I$, and $q \in (p)$ by euclidean division so that $I = (p)$. □

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 π, so by lemma 10.2, it is surjective. If $s(a) = 0$, then π 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 $C^0(\mathbf{Z}_p, K)$.

Proof. — We show that $\{\binom{x}{n}\}_{n\geq 0}$ is a basis of $C^0(\mathbf{Z}_p, k)$. If $f(x) = a_0\binom{x}{0} + \cdots + a_n\binom{x}{n} = 0$, then $f(0) = a_0 = 0$, and then $f(1) = a_1 = 0, \ldots, f(n) = a_n = 0$. Hence the set $\{\binom{x}{n}\}_{n\geq 0}$ is linearly independent over k.

We now show that the $\{\binom{x}{n}\}_{n\geq 0}$ generate $C^0(\mathbf{Z}_p, k)$ over k. If $f \in C^0(\mathbf{Z}_p, k)$, then f is locally constant so that there exists $m \geq 1$ such that $f(x) = \sum_{a=0}^{p^m-1} f(a)\,\mathrm{Id}_{a+p^m\mathbf{Z}_p}(x)$. It is therefore enough to show that if $a \in \mathbf{Z}_p$ and $m \geq 1$, then in $C^0(\mathbf{Z}_p, \mathbf{Z}_p)$, we can write $\mathrm{Id}_{a+p^m\mathbf{Z}_p}(x) = \sum_{n\geq 0} a_n\binom{x}{n}$ with $a_n \in \mathbf{Z}$ and $a_n \to 0$. Let us work in $L = \mathbf{Q}_p(\mu_{p^m})$.

If $x \in \mathbf{Z}_p$, then $\sum_{\eta^{p^m}=1} \eta^x = p^m$ if $p^m \mid x$ and 0 otherwise. Therefore,

$$\begin{aligned}\mathrm{Id}_{a+p^m\mathbf{Z}_p}(x) &= \frac{1}{p^m}\sum_\eta \eta^{x-a} = \frac{1}{p^m}\sum_\eta \eta^{-a}(1+(\eta-1))^x \\ &= \frac{1}{p^m}\sum_\eta \eta^{-a}\sum_{n\geq 0}\binom{x}{n}(\eta-1)^n = \sum_{n\geq 0}\binom{x}{n}\frac{1}{p^m}\sum_\eta \eta^{-a}(\eta-1)^n.\end{aligned}$$

It remains to check that $p^{-m}\sum_\eta \eta^{-a}(\eta-1)^n$ belongs to $\mathbf{Z}$ and $\to 0$ as $n \to +\infty$. □

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 11.3. — *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 11.4. — *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 $F(X,Y) = X+Y+XY$.

Lemma 12.1. — *Item (4) follows from (1).*

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 $F(X, i_n(X) - cX^{n+1}) = F(X, i_n(X)) - cX^{n+1}F_Y(X, i_n(X)) + \mathrm{O}(X^{2(n+1)}) = \mathrm{O}(X^{n+2})$ and $i(X) = \lim i_n(X)$. □

Note that (1) and (2) imply that $F(X,0) = X$ and $F(0,Y) = Y$. Indeed 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 below.

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 $f \circ g(X) = g \circ f(X) = X$.*

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 ω is invariant, then $\omega(X) = a \cdot dX/F_X(0,X)$. 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.

Proposition 12.3. — *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 $d/dX(E(X)) = 0$ since ω_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 $\omega_G \circ f = f'(0)\cdot\omega_F = 0$ so that $f'(X)=0$. Since k is of char p, this implies that $f(X)=g(X^p)$.

Write $F(X,Y)=\sum a_{ij}X^iY^j$ and let $F^{(h)}(X,Y)=\sum a_{ij}^{p^h}X^iY^j$. 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 $\mathrm{wideg}([p](X))=p^h$. If $y\in\mathfrak{m}_{\mathbf{C}_p}$, 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 solutions of $[p](z)=y$ are distinct.

Let $M_n=\{z\in\mathfrak{m}_{\mathbf{C}_p}$ such that $[p^n](z)=0\}$. This set has p^{hn} elements, it is a $\mathbf{Z}/p^n\mathbf{Z}$-module, and $[p]: M_{n+1}\to M_n$ is surjective. Let $M=\varprojlim_n M_n$. This is a $\mathbf{Z}_p$-module, and since $M\to M_1$ is onto, M is generated by h elements. We have $M/p^nM=M_n$ for all $n\geq 1$, 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 π 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 π, 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 φ, $\psi\in\mathcal{L}_\pi$ and $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathcal{O}_K^n$, then there exists a unique $H_\alpha^{\varphi,\psi}\in\mathcal{O}_K[\![X_1,\dots,X_n]\!]$ such that*

1. *$H_\alpha^{\varphi,\psi}(X_1,\dots,X_n)=\alpha_1X_1+\cdots+\alpha_nX_n+\deg\geq 2$;*

2. $\varphi \circ H_\alpha^{\varphi,\psi}(X_1, \dots, X_n) = H_\alpha^{\varphi,\psi}(\psi(X_1), \dots, \psi(X_n))$.

Proof. — Take any $H_1(X_1, \dots, X_n) \equiv \alpha_1 X_1 + \dots + \alpha_n X_n + \mathrm{O}(X^2)$. Note that $\varphi \circ H_1 - H_1 \circ \psi$ only has terms of degree ≥ 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 $\geq i+1$. Given H_i, let

$$H_{i+1} = H_i + \frac{1}{\pi^{i+1} - \pi} \left(\varphi \circ H_i - H_i \circ \psi \right).$$

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 H_{i+1} has coefficients in $\mathcal{O}_K$. Write $\varphi \circ H_i - H_i \circ \psi = cX^{i+1}$. We have

$$\begin{aligned} \varphi \circ H_{i+1} - H_{i+1} \circ \psi &= \varphi \left(H_i + \frac{cX^{i+1}}{\pi^{i+1} - \pi} \right) - H_i \circ \psi - \frac{c\psi^{i+1}}{\pi^{i+1} - \pi} + \mathrm{O}(X^{i+2}) \\ &= \varphi \circ H_i + \pi \frac{cX^{i+1}}{\pi^{i+1} - \pi} - H_i \circ \psi - \pi^{i+1} \frac{cX^{i+1}}{\pi^{i+1} - \pi} + \mathrm{O}(X^{i+2}) \\ &= \mathrm{O}(X^{i+2}). \end{aligned}$$

The power series $\{H_i\}_i$ then converge to a series $H_\alpha^{\varphi,\psi}$ satisying (1) and (2). Furthermore, $H_{i+1} \bmod X^{i+2}$ is uniquely determined by $H_i \bmod X^{i+1}$, so that $H_\alpha^{\varphi,\psi}$ is unique. □

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 φ, $\psi \in \mathcal{L}_\pi$, then $H_{1,1}^{\varphi,\psi}$ gives an isomorphism between F_φ and F_ψ. □

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

We are interested in the field K_n^φ generated by the π^n-torsion points of F_φ. Note that if $z \in F_\varphi[\pi^n]$, then $H_1^{\varphi,\psi}(z) \in F_\psi[\pi^n]$. The field K_n^φ is therefore independent of the choice of φ, 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_∞/K is totally ramified, and* $\mathrm{Gal}(K_\infty/K) \simeq \mathcal{O}_K^\times$.

Proof. — Let $\Lambda_0 = \{0\}$ and for $n \geq 1$, let Λ_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 $F[\pi^n] = \Lambda_0 \sqcup \dots \sqcup \Lambda_n$, and Λ_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 Λ_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 Λ_n. Hence $K_n = K(z)$ for any $z \in \Lambda_n$. Let $Q(X) = X^{q-1}+\pi$. The element z 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 $\mathcal{O}_{K_n}$, and $\mathrm{Gal}(K_n/K) \simeq \mathcal{O}_K^\times/1+\pi^n\mathcal{O}_K$ via the map $g \mapsto \chi_\pi(g)$ determined by $g(z) = [\chi_\pi(g)](z)$.

The extension K_∞/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 $z \in F[\pi^\infty]$. □

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. — The element z above is a root of $Q \circ \varphi^{\circ(n-1)}(X)$ whose constant coefficient is π, so that π is the norm of an element of K_n for all $n \geq 1$.

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_∞^π denote the extension of K constructed above. It is an abelian totally ramified extension of K. The extension K^{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 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^{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 (resp. finite) abelian extensions of* K.
4. *If* L/K *is any finite extension, then the following diagram commutes*

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

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 $e = \{e_1, \ldots, e_d\}$ is a basis of X. If we denote by $\mathrm{Mat}_e(g)$ the matrix of $g \in G$ in the basis e, then $g \mapsto \mathrm{Mat}_e(g)$ is a cocyle on G with values in $\mathrm{GL}_d(R)$. Furthermore, if f is another basis of X and if 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 $\inf : H^1(G/H, M^H) \to H^1(G,M)$ defined by $\inf(c)(g) = c(\overline{g})$. 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* $c \in \inf(H^1(G/H, M^H))$*;*
3. *if* $\inf(c) = 0$*, then* $c = 0$*.*

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

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

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 $(\mathrm{res} \circ \inf)(c)(h) = c(1) = 1$ so that $\mathrm{res} \circ \inf = 0$, 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 $c \in \inf(H^1(G/H, M^H))$. □

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 $H^1(G, \mu_n) = K^\times/(K^\times)^n$.

Let K be a finite extension of $\mathbf{Q}_p$, with uniformizer π, and let $G = \mathrm{Gal}(K^{\mathrm{unr}}/K)$. Recall that $G = \mathrm{Gal}(\overline{\mathbf{F}}_p/k)$. Let $\widehat{K}^{\mathrm{unr}}$ denote the p-adic completion of K^{unr}, so that $\widehat{K}^{\mathrm{unr}} \subset \mathbf{C}_p$. The group G acts on $\widehat{K}^{\mathrm{unr}}$ by continuous automorphisms. Let $H^1(G, \mathrm{GL}_d(\mathcal{O}_{\widehat{K}^{\mathrm{unr}}}))$ denote the set of continuous cocycles modulo equivalence.

Proposition 16.6. — *The set $H^1(G, \mathrm{GL}_d(\mathcal{O}_{\widehat{K}^{\mathrm{unr}}}))$ is trivial.*

Proof. — Let $A = \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$ so that there is a map $x \mapsto \overline{x}$ from A to $\overline{\mathbf{F}}_p$. Since $\overline{\mathbf{F}}_p$ is a field, $\mathrm{GL}_d(\overline{\mathbf{F}}_p)$ is generated by transvections and diagonal matrices, so that the map $\mathrm{GL}_d(A) \to \mathrm{GL}_d(\overline{\mathbf{F}}_p)$ is surjective. If $U \in H^1(G, \mathrm{GL}_d(A))$ then $\overline{U} \in H^1(G, \mathrm{GL}_d(\overline{\mathbf{F}}_p))$ so that by the triviality of $H^1(G, \mathrm{GL}_d(\overline{\mathbf{F}}_p))$ and the surjectivity of the map $\mathrm{GL}_d(A) \to \mathrm{GL}_d(\overline{\mathbf{F}}_p)$, there exists a matrix $M_0 \in \mathrm{GL}_d(A)$ with $M_0^{-1} \cdot U(g) \cdot g(M_0) \in \mathrm{Id} + \pi \, \mathrm{M}_d(A)$. Assume that we have constructed matrices $M_0, \ldots, M_{k-1}$ with $M_j \in \mathrm{Id} + \pi^j \, \mathrm{M}_d(A)$ such that

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

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

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

and the triviality of $H^1(G,\overline{\mathbf{F}}_p)$ allows us to find R_k such that

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

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

Corollary 16.7. — *If $\eta : \mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \to \mathbf{Z}_p^\times$ is an unramified character, then there exists $x\in\mathcal{O}_{\widehat{K}^{\mathrm{unr}}}^\times$ such that $g(x)=\eta(g)\cdot x$ for all $g\in\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$.*

Such an element is called a period of the character η. One motivating question for what follows is: is there a period in $\mathbf{C}_p$ for the cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)\to\mathbf{Z}_p^\times$?

17. 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 17.1. — *We have $\mathbf{C}_p^{G_K}=\widehat{K}$.*

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

Lemma 17.2. — *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 β satisfying $\mathrm{val}_p(\beta)\geq c$.*
2. *If $n=p^{k+1}$ and $q=p^k$, then $P^{(q)}(X)$ has a root β 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 β 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 17.3. — *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 δ 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 α over K. Lemma 17.2 applied to $P(X) = Q(X+\alpha)$ gives us an element $\alpha' = \beta + \alpha$ such that $\mathrm{val}_p(\alpha' - \alpha) \geq c$ or $\mathrm{val}_p(\alpha' - \alpha) \geq c - 1/p^k(p-1)$ depending on the nature of n. We then have $[K(\alpha') : K] < [K(\alpha) : K]$ while either $\Delta_K(\alpha') \geq \Delta_K(\alpha)$ or $\Delta_K(\alpha') \geq \Delta_K(\alpha) - 1/p^k(p-1)$. This allows us to finish the proof by induction. □

Proof of theorem 17.1. — 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 17.3 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 α is a limit of elements of K. □

18. 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 18.1. — *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 18.2. — *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 18.3. — *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 17.1, 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 ψ is trivial on G_{F_n}. Since ψ is of infinite order, we have $R_n(x) = 0$ for all $n \geq 0$ and hence $x = \lim R_n(x) = 0$. □

19. 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 19.1. — 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). □

Corollary 19.2. — *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 19.3. — *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 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

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

This tells us that $\operatorname{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 0$ if $k = 1, \ldots, d-1$ and $\operatorname{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) = 1$ if $k = d$ and $\operatorname{Tr}_{L/K}(\alpha^{k-1}/P'(\alpha)) \in \mathcal{O}_K$ 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 $\operatorname{Tr}_{L/K}(y) = y_{d-1}$ so that $y_{d-1} \in \mathcal{O}_K$, and then $\operatorname{Tr}_{L/K}(\alpha y) = y_{d-2} + \operatorname{Tr}_{L/K}(y_{d-1}\alpha^d/P'(\alpha))$ 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 19.4. — *If L/K is a Galois extension and $G = \operatorname{Gal}(L/K)$, then $\operatorname{val}_L(\mathfrak{d}_{L/K}) = \sum_{g\neq 1\in G} i_L(g) = \int_{-1}^{\infty}(|G_t|-1)dt$.*

Proof. — We have $\operatorname{val}_L(\mathfrak{d}_{L/K}) = \operatorname{val}_L(P'(\alpha)) = \sum_{g\neq 1\in G} \operatorname{val}_L(g(\alpha)-\alpha) = \sum_{g\neq 1\in G} i_L(g)$. 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 19.5. — *We have $\operatorname{val}_K(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(1-1/|G^u|)du$.*

Proof. — By the previous corollary, $\operatorname{val}_L(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(|G_t|-1)dt$. 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 $\operatorname{val}_L(\mathfrak{d}_{L/K}) = \int_{-1}^{\infty}(|G^u|-1)|G^0|/|G^u|du$. The corollary follows, since $|G^0| = e(L/K)$ and $\operatorname{val}_L(\cdot) = e(L/K)\operatorname{val}_K(\cdot)$. □

If L/K is a Galois extension, let $L^u = L^{\operatorname{Gal}(L/K)^u}$. 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. Corollaries 19.2 and 19.5 then imply the following.

Theorem 19.6. — *We have*

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

20. Ramification in cyclotomic extensions

Let $F = \mathbf{Q}_p$ and $F_n = \mathbf{Q}_p(\zeta_{p^n})$ for $n \geq 1$. We know that F_n is a totally ramified extension of F of degree $p^{n-1}(p-1)$ and that $\mathcal{O}_{F_n} = \mathbf{Z}_p[\zeta_{p^n}]$. 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 20.1. — *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. $\chi : \mathrm{Gal}(K_\infty/K_n) \to 1 + p^n\mathbf{Z}_p$ *is an isomorphism.*

Proof. — Since $K_{n+1} = K_n F_{n+1}$, 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_∞/F_n is then the compositum of the disjoint extensions F_∞/F_n and K_n/F_n so that $\mathrm{Gal}(K_\infty/K_n) = \mathrm{Gal}(F_\infty/F_n)$. □

Theorem 20.2. — *If K is a finite extension of $F = \mathbf{Q}_p$, then $\{p^n \operatorname{val}_p(\mathfrak{d}_{K_n/F_n})\}_{n\geq 1}$ is bounded.*

Proof. — Applying theorem 19.6, we get

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

By subtracting, we get

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

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 20.3. — *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 19.1 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 20.2 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 $x \in \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n})$. □

Let $H_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$. This result allows us to compute $H^1(H_K, \mathbf{C}_p)$.

Corollary 20.4. — *If $f : H_K \to p^n \mathcal{O}_{\mathbf{C}_p}$ is a continuous cocycle, then there exists $x \in p^{n-1}\mathcal{O}_{\mathbf{C}_p}$ such that the cohomologous cocyle $g \mapsto f(g) - (x - g(x))$ has values in $p^{n+1}\mathcal{O}_{\mathbf{C}_p}$.*

Proof. — Let L/K be a finite extension such that $f(H_L) \subset p^{n+2}\mathcal{O}_{\mathbf{C}_p}$. Lemma 20.3 gives us $y \in p^{-1}\mathcal{O}_{L_\infty}$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(y) = 1$. Let Q be a set of representatives of H_K/H_L and let $x_Q = \sum_{h \in Q} h(y) f(h)$ so that if $g \in H_K$ then $g(x_Q) = x_{g(Q)} - f(g)$ and hence $f(g) - (x_Q - g(x_Q)) = x_{g(Q)} - x_Q$. The cocyle relation and the choice of L tells us that $x_{g(Q)} - x_Q \in p^{n+1}\mathcal{O}_{\mathbf{C}_p}$ so that we can take $x = x_Q$. □

Theorem 20.5. — *We have $H^1(H_K, \mathbf{C}_p) = \{0\}$.*

Proof. — Let $f : H_K \to \mathbf{C}_p$ be a cocycle, and let $k \in \mathbf{Z}$ be such that $f(H_K) \subset p^k\mathcal{O}_{\mathbf{C}_p}$. Set $f_0 = f$ so that $f_j(H_K) \subset p^{k+j}\mathcal{O}_{\mathbf{C}_p}$ for $j = 0$. If $j \geq 0$, lemma 20.4 gives us $x_j \in p^{k+j-1}\mathcal{O}_{\mathbf{C}_p}$ such that if we set $f_{j+1}(g) = f_j(g) - (x_j - g(x_j))$, then $f_{j+1}(H_K) \subset p^{k+j+1}\mathcal{O}_{\mathbf{C}_p}$. We then have $f(g) = \sum_{j \geq 0} x_j - g(\sum_{j \geq 0} x_j)$. □

We finish by extending the construction of section 18 to $\hat{K}_\infty$. If $n \geq n(K)$, then $[K_n : F_n] = d = [K_\infty : F_\infty]$. If $e_1, \dots, e_d$ is a basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, then it is also a basis of K_{n+k} over F_{n+k}. Furthermore if $e_1^*, \dots, e_d^*$ denotes the dual basis, then $e_i^* \in \mathfrak{d}_{K_n/F_n}^{-1}$ so that if $\delta > 0$ is given and $n \gg 0$ then $\mathrm{val}_p(e_i^*) \geq -\delta$. If $x \in \mathcal{O}_{K_{n+k}}$ then we can write $x = \sum_{i=1}^d x_i e_i^*$ where $x_i = \mathrm{Tr}_{K_{n+k}/F_{n+k}}(x e_i) \in \mathcal{O}_{F_{n+k}}$.

We then define $R_n(x) = \sum_{i=1}^d R_n(x_i) e_i^*$ which gives a projection $R_n : \hat{K}_\infty \to K_n$.

Proposition 20.6. — *If $\varepsilon > 0$, there exists $n(\varepsilon)$ such that if $n \geq n(\varepsilon)$, then the maps $R_n : \hat{K}_\infty \to K_n$ defined above satisfy $\mathrm{val}_p(R_n(x)) \geq \mathrm{val}_p(x) - \varepsilon$.*

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

$$\mathrm{val}_p(x_i) > \mathrm{val}_p(x) - \mathrm{val}_p(\zeta_{p^{n+k}} - 1) \text{ by } F_{n+k}\text{-linearity},$$

$$\mathrm{val}_p(R_n(x_i)) > \mathrm{val}_p(x_i) - \mathrm{val}_p(\zeta_{p^n} - 1) \text{ by corollary 18.2},$$

$$\mathrm{val}_p(e_i^*) \geq -\delta \text{ if } \delta > 0 \text{ and } n \gg 0.$$

The proposition follows. □

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