LES NOMBRES p-ADIQUES, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

1. Corps Normés

1.1. Normes

Définition 1.1. — Soit K un corps. Une norme sur K est une application $x \mapsto |x|$ de K dans $\mathbf{R}_+$ vérifiant les trois propriétés suivantes :

(i) $|x| = 0 \Leftrightarrow x = 0$;

(ii) $|xy| = |x||y|$;

(iii) $|x + y| \leqslant |x| + |y|$.

Une norme sur K est dite *ultramétrique*, si elle vérifie la condition

(iii′) $|x + y| \leqslant \sup(|x|, |y|)$,

qui est plus forte que la condition (iii).

Proposition 1.2. — *Si K est un corps et $|\ |$ est une norme sur K, les conditions suivantes sont équivalentes*

(i) $|\ |$ *est ultramétrique*

(ii) $|\ |$ *est bornée sur* $\mathbf{Z}$ (plus précisément sur l'image de $\mathbf{Z}$ dans K).

(iii) $|x| \leqslant 1$ *quel que soit* $x \in \mathbf{Z}$ (idem).

Démonstration. — On a (i)⇒(iii)⇒(ii) de manière évidente ; il suffit donc de prouver (ii)⇒(i). Si on suppose que $|m| \leqslant M$ quel que soit $m \in \mathbf{Z}$ et si $x, y \in K$ et $n \in \mathbf{N}$, alors

$$|x + y|^n = |(x + y)^n| = |\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}| \leqslant (n + 1)M \sup(|x|, |y|)^n.$$

On en déduit le résultat en prenant la racine n-ième des deux membres et en passant à la limite.

Corollaire 1.3. — *Si K est de caractéristique p, alors toute norme sur K est ultramétrique.*

1.2. Normes et topologie

Si K est un corps muni d'une norme $|\ |$, et x, y sont deux éléments de K, on pose $d(x, y) = |x - y|$. Les propriétés (i) et (iii) des normes assurent que d est une distance sur K et donc définit une topologie sur K.

Lemme 1.4. — *Si $|\ |$ est ultramétrique et $|x| \neq |y|$, alors $|x + y| = \sup(|x|, |y|)$.*

Démonstration. — Quitte à permuter x et y, on peut supposer $|x| > |y|$. On a alors

$$|x + y| \leqslant |x| = |(x + y) - y| \leqslant \sup(|x + y|, |y|)$$

et comme $|y| < |x|$, on en déduit l'égalité $\sup(|x + y|, |y|) = |x + y|$, ce qui permet de conclure.

Proposition 1.5. — *Si $|\ |$ est ultramétrique, alors*

(i) *Tout triangle est isocèle*

(ii) *Tout point d'une boule en est "le" centre*

(iii) *Deux boules sont soit disjointes soit l'une est contenue dans l'autre (comme des billes de mercure)*

(iv) *Les boules sont à la fois ouvertes et fermées.*
(v) *La topologie est totalement discontinue.*

Démonstration. — Le (i) est une conséquence immédiate du lemme 1.4. Si $x_1 \in B(x_0, r)$ (boule ouverte ou fermée), et si $y \in B(x_1, r)$, alors $d(x_0, y) \leqslant \sup(d(x_0, x_1), d(x_1, y)) \leqslant r$ (ou $< r$ si on parle de boules ouvertes), et donc $B(x_1, r) \subset B(x_0, r)$. L'inclusion dans l'autre sens s'obtient en échangeant les rôles de x_0 et x_1, ce qui permet de démontrer le (ii). D'après le (ii), si deux boules ont une intersection non vide, tout élément de l'intersection est le centre des deux boules ce qui démontre le (iii). Le (v) est une conséquence immédiate du (iv), et si B est une boule ouverte de rayon r, le complémentaire de B contient la boule ouverte de rayon r autour de chacun de ses points d'après le (iii), ce qui montre que ce complémentaire est ouvert et donc que B est fermée. Si B est une boule fermée de rayon non nul, alors B est un voisinage de chacun de ses points puisque ceux-ci en sont "le" centre.

Définition 1.6. — Deux normes sur un corps K sont dites équivalentes si elle définissent la même topologie.

Proposition 1.7. — *Deux normes $|\ |_1$ et $|\ |_2$ sont équivalentes si et seulement si il existe $s \in \mathbf{R}_+^*$ tel que l'on ait $|x|_1 = |x|_2^s$ quel que soit $x \in K^*$.*

Démonstration. — Si $|\ |$ est une norme sur un corps K, alors $|x| < 1$ si et seulement si la suite de terme général x^n tend vers 0 quand n tend vers $+\infty$. On en déduit le fait que si $|\ |_1$ et $|\ |_2$ sont équivalentes, alors $\{x \in K \mid |x|_1 < 1\} = \{x \in K \mid |x|_2 < 1\}$. Si ce dernier ensemble est réduit à $\{0\}$, on a $|x|_1 = |x|_2 = 1$ quel que soit $x \in K^*$. Sinon, soit $x \in K^*$ vérifiant $|x|_1 < 1$. Si $y \in K^*$, $a \in \mathbf{Z}$ et $b \in \mathbf{N}$, alors

$$|y^b x^{-a}|_1 < 1 \Leftrightarrow |y^b x^{-a}|_2 < 1.$$

On en déduit le fait que

$$\{r \in \mathbf{Q} \mid r < \frac{\log |y|_1}{\log |x|_1}\} = \{r \in \mathbf{Q} \mid r < \frac{\log |y|_2}{\log |x|_2}\}$$

et donc que les réels $\frac{\log |y|_1}{\log |x|_1}$ et $\frac{\log |y|_2}{\log |x|_2}$ définissent la même coupure de Dedekind et sont donc égaux, ce qui montre que la fonction $y \to \frac{\log |y|_1}{\log |y|_2}$ est constante sur K^* et permet de conclure.

1.3. Exemples

1.3.1. La norme triviale. — On peut munir n'importe quel corps K de la norme triviale définie par $|x| = 1$ si $x \neq 0$. La topologie associée est alors la topologie discrète sur K.

1.3.2. Norme induite. — Si L est un corps normé, et K est un sous-corps, on peut munir K de la norme obtenue par restriction de celle sur L. Par exemple, on peut munir tout sous-corps de $\mathbf{C}$ de la norme induite par l'application module $|x + iy| = \sqrt{x^2 + y^2}$ sur $\mathbf{C}$.

1.3.3. Normes sur $\mathbf{Q}$. — Comme $\mathbf{Q}$ est un sous-corps de $\mathbf{C}$, on peut le munir de la norme $|\ |_\infty$ usuelle. Par ailleurs, si p est un nombre premier, on peut munir $\mathbf{Q}$ de la norme p-adique $|\ |_p$ définie par $|\frac{a}{b}|_p = p^{v_p(b) - v_p(a)}$ où, si $n \in \mathbf{Z} - \{0\}$, $v_p(n)$ est le plus grand entier v tel que p^v divise n. La norme $|\ |_p$ est clairement multiplicative et vérifie l'inégalité ultramétrique car si $|z| \leqslant 1$, on peut écrire z sous la forme $\frac{a}{b}$ avec $(b, p) = 1$ ce qui implique $1 + z = \frac{a+b}{b}$ et $|1 + z| = p^{-v_p(a+b)} \leqslant 1$.

***Théorème 1.8* (Ostrowski).** — *Une norme non triviale sur* $\mathbf{Q}$ *est équivalente à la norme usuelle* $|\ |_\infty$ *ou à la norme p-adique pour un nombre premier p.*

Démonstration. — Commençons par supposer qu'il existe $k \in \mathbf{N}$ tel que $\|k\| > 1$. Comme $\|1\| = 1$, l'inégalité triangulaire implique $\|k\| \leqslant k$ et il existe $\alpha \in]0,1]$ tel que l'on ait $\|k\| = k^\alpha$. Soit $m \in \mathbf{N}$. On peut écrire m en base k sous la forme $m = \sum_{i=0}^n a_i k^i$ avec $a_i \in \{0, 1, \dots, k-1\}$ et $a_n \neq 0$ de telle sorte que l'on a $m \geqslant k^n$. Comme $\|a_i\| \leqslant a_i \leqslant k-1$ et $\|k^i\| = \|k\|^i$, on obtient la majoration

$$\|m\| \leqslant (k-1)\sum_{i=1}^{n} k^{i\alpha} = \frac{k-1}{k^\alpha - 1}(k^{(n+1)\alpha} - 1) \leqslant \frac{k^\alpha(k-1)}{k^\alpha - 1} k^{n\alpha} \leqslant C m^\alpha,$$

où $C = \frac{k^\alpha(k-1)}{k^\alpha - 1}$ est indépendant de m. On peut appliquer cette inégalité à m^n, ce qui nous donne $\|m\|^n \leqslant C m^{n\alpha}$ et, prenant la racine n-ième de cette égalité et passant à la limite, l'inégalité $\|m\| \leqslant m^\alpha$. On a donc $\frac{\log \|m\|}{\log m} \leqslant \frac{\log \|k\|}{\log k}$ quel que soit $m \in \mathbf{N}$. Par symétrie, on en déduit le fait que si $\|m\| > 1$, alors cette inégalité est une égalité. Dans le cas général, il existe $n \in \mathbf{N}$ tel que l'on ait $\|k^n m\| > 1$, ce qui montre que l'on a égalité quel que soit $m \in \mathbf{N}$ puis, utilisant la multiplicativité de la norme et le fait que $\|-1\| = 1$, que $\|x\| = |x|_\infty^\alpha$ quel que soit $x \in \mathbf{Q}$. On a donc montré que s'il existe $k \in \mathbf{N}$ tel que $\|k\| > 1$, alors $\|\ \|$ est équivalente à la norme usuelle.

Dans le cas contraire, on a $\|\ell\| \leqslant 1$ pour tout nombre premier ℓ. Comme on a supposé $\|\ \|$ non triviale, il existe au moins un nombre premier p tel que $\|p\| < 1$. Si il en existe un autre q, alors quel que soit $n \in \mathbf{N}$, on peut, d'après le théorème de Bezout, trouver $u_n, v_n \in \mathbf{Z}$ tels que l'on ait $u_n p^n + v_n q^n = 1$ On obtient donc

$$1 = \|1\| = \|u_n p^n + v_n q^n\| \leqslant \|u_n\| \cdot \|p\|^n + \|v_n\| \cdot \|q\|^n \leqslant \|p\|^n + \|q\|^n,$$

ce qui est impossible pour n assez grand. Il existe donc un et un seul nombre premier p tel que $\|p\| < 1$ et $\|\ \|$ est équivalente à la norme p-adique. Ceci termine la démonstration.

Le résultat suivant est une conséquence immédiate de l'unicité de la décomposition d'un entier en produit de facteurs premiers, mais est très important ; c'est ce qui justifie la normalisation utilisée pour $|\ |_p$.

***Théorème 1.9* (Formule du produit).** — *Si* $x \in \mathbf{Q}^*$, *alors*

$$|x|_\infty \cdot \prod_{p \text{ premier}} |x|_p = 1.$$

1.3.4. Normes sur $K(X)$. — Soit K un corps. L'exercice suivant a pour but de démontrer que $K(X)$ se comporte assez largement comme $\mathbf{Q}$ du point de vue des normes que l'on peut mettre dessus.

Exercice 1. — Soit a vérifiant $0 < a < 1$.

(i) Montrer que $f \mapsto |f|_\infty = a^{-\deg f}$ définit une norme ultramétrique sur $K(X)$.

(ii) Soit $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $K(X)$. Montrer que, si $P \in \mathscr{P}$, et si $f \in K(X)$ est non nul, il existe un unique $v_P(f) \in \mathbf{Z}$ tel que $P^{-v_P(f)} f = \frac{Q_1}{Q_2}$, avec Q_1 et Q_2 premiers à P. Montrer que $f \mapsto |f|_P = a^{\deg P \cdot v_P(f)}$ définit une norme ultramétrique sur $K(X)$, et que $|\ |_P$ n'est pas équivalente à $|\ |_\infty$.

(iii) Montrer que toute norme non triviale sur $K(X)$, qui est triviale sur K, est équivalente à $|\ |_\infty$ ou à $|\ |_P$ pour un unique $P \in \mathscr{P}$.

(iv) Montrer que $f \in K(X) - \{0\}$ vérifie la formule du produit

$$|f|_\infty \cdot \prod_{P \in \mathscr{P}} |f|_P = 1.$$

1.3.5. Norme de Gauss. — Si K un corps ultramétrique, et si $P(X) = \sum_{i=0}^n a_i X^i \in K(X)$, on définit la norme de Gauss $|P|_{\mathrm{G}}$ de P par $|P|_{\mathrm{G}} = \sup_i(|a_i|)$.

Lemme 1.10. — *Si P et Q sont deux éléments de $K(X)$, alors $|PQ|_{\mathrm{G}} = |P|_{\mathrm{G}}|Q|_{\mathrm{G}}$.*

Démonstration. — $|\ |$ étant ultramétrique, l'inégalité $|PQ|_{\mathrm{G}} \leqslant |P|_{\mathrm{G}}|Q|_{\mathrm{G}}$ est immédiate. Réciproquement, soit i_0 (resp. j_0) le plus petit entier i (resp. j) vérifiant $|a_i| = |P|_{\mathrm{G}}$ (resp. $|b_j| = |Q|_{\mathrm{G}}$). Soit $k_0 = i_0 + j_0$ et $PQ(X) = \sum_{k=0}^{n+m} c_k X^k$. Alors

$$c_{k_0} = a_{i_0} b_{j_0} + \sum_{i<i_0} a_i b_{k_0-i} + \sum_{j<j_0} a_{k_0-j} b_j$$

et par définition de i_0 et j_0, le seul terme de cette somme de norme $|P|_{\mathrm{G}}|Q|_{\mathrm{G}}$ est $a_{i_0}b_{j_0}$, les autres étant de norme strictement plus petite, ce qui permet, utilisant le lemme 1.4, de montrer que l'on a $|c_{k_0}| = |P|_{\mathrm{G}}|Q|_{\mathrm{G}}$, et permet de conclure.

Ce lemme permet de montrer que si $f = \frac{P}{Q}$ et si l'on pose $|f|_{\mathrm{G}} = \frac{|P|_{\mathrm{G}}}{|Q|_{\mathrm{G}}}$, cette expression ne dépend pas de l'écriture de f sous la forme $\frac{P}{Q}$ et définit donc une application $|\ |_{\mathrm{G}}$ de $K(X)$ dans $\mathbf{R}_+$ vérifant les propriétés (i) et (ii) des normes. D'autre part, si $f = \frac{P}{Q}$, on peut, quitte à diviser P et Q par un élément de K de norme $|Q|_{\mathrm{G}}$, supposer que $|Q|_{\mathrm{G}} = 1$ et $|f|_{\mathrm{G}} \leqslant 1$ est alors équivalent à $|P|_{\mathrm{G}} \leqslant 1$, et implique $|P+Q|_{\mathrm{G}} \leqslant 1$ de manière évidente. Ceci permet de montrer que $|\ |_{\mathrm{G}}$ est une norme ultramétrique sur $K(X)$.

Exercice 2. — Si K est un corps ultramétrique, on note $K[[X]]^b$ l'ensemble des séries $f = \sum_{n=0}^{+\infty} a_n X^n$ telles que la suite $(a_n)_{n\in\mathbf{N}}$ soit bornée dans K. On munit $K[[X]]^b$ de la norme de Gauss $|\ |_G$ définie par $\big|\sum_{n=0}^{+\infty} a_n X^n\big|_G = \sup_{n\in\mathbf{N}} |a_n|$.

(i) Montrer que, si $f, g \in K[[X]]^b$, alors $|fg|_G = |f|_G|g|_G$.

(ii) Montrer que $f = \sum_{n=0}^{+\infty} a_n X^n$ est inversible dans $K[[X]]^b$ si et seulement si $a_0 \neq 0$ et $|a_0| \geqslant |a_n|$ quel que soit $n \in \mathbf{N}$.

1.4. Complétion. — Si K est un corps normé, on note $\tilde{K}$ l'ensemble des suites de Cauchy à valeurs dans K [i.e. l'ensemble des suites $(a_n)_{n\in\mathbf{N}}$ telles que

$$\forall \varepsilon > 0,\ \exists N \in \mathbf{N} \text{ tel que } \forall n \geqslant N \text{ et } p \in \mathbf{N}, \quad |a_n - a_{n+p}| < \varepsilon].$$

Soit $I \subset \tilde{K}$ l'ensemble des suites tendant vers 0.

Lemme 1.11. — (i) *Si $(a_n)_{n\in\mathbf{N}} \in \tilde{K}$, alors la suite de terme général $|a_n|$ converge dans $\mathbf{R}_+$.*

(ii) *Si on suppose de plus que $|\ |$ est ultramétrique et que $a \notin I$, alors la suite de terme général $|a_n|$ est constante à partir d'un certain rang.*

(iii) *Si $a = (a_n)_{n\in\mathbf{N}}$ et $b = (b_n)_{n\in\mathbf{N}}$ sont deux éléments de $\tilde{K}$ différant par un élément de I, alors* $\lim_{n\to+\infty} |a_n| = \lim_{n\to+\infty} |b_n|$.

Démonstration. — L'inégalité triangulaire implique que l'on a $||a_{n+p}|-|a_n|| \leqslant |a_{n+p}-a_n|$ quels que soient n et p et donc que la suite de terme général $|a_n|$ est de Cauchy. On en déduit le (i).

D'autre part, si $a=(a_n)_{n\in\mathbf{N}} \in \tilde{K}-I$ il existe $\delta>0$ tel que l'on ait $|a_n| \geqslant \delta$ pour une infinité de n et la limite de la suite $|a_n|$ est donc supérieure ou égale à δ. Il existe donc $N\in\mathbf{N}$ tel que si $n\geqslant N$, alors $|a_n|>\frac{2}{3}\delta$ et $|a_{n+p}-a_n|<\frac{\delta}{2}$ quel que soit $p\in\mathbf{N}$. Ceci implique $|a_{n+p}-a_n|<|a_n|$ et donc, comme $|\ |$ est supposée ultramétrique, $|a_{n+p}|=|a_n|$ quel que soit $p\in\mathbf{N}$; d'où le (ii).

On a $||a_n|-|b_n|| \leqslant |a_n-b_n|$ et l'hypothèse implique que cette dernière suite tend vers 0 d'où le (iii).

Lemme 1.12. — *$\tilde{K}$ est un anneau et I est un idéal maximal de $\tilde{K}$.*

Démonstration. — Le fait que $\tilde{K}$ est un anneau et I un idéal est immédiat. L'élément unité de $\tilde{K}$ est la suite constante 1 dont tous les termes sont égaux à 1. Si $a=(a_n)_{n\in\mathbf{N}}\in\tilde{K}-I$, d'après ce qui précède, il existe $\delta>0$ et $N\in\mathbf{N}$ tels que l'on ait $|a_n|\geqslant\delta$ si $n\geqslant N$. La suite $b=(b_n)_{n\in\mathbf{N}}$ définie par $b_n=0$ si $n<N$ et $b_n=a_n^{-1}$ si $n\geqslant N$ est de Cauchy et $ab-1$ est élément de I, ce qui montre que a est inversible dans $\tilde{K}/I$ et permet de conclure au fait que I est maximal.

Il résulte du lemme précédent que $\widehat{K}=\tilde{K}/I$ est un corps et du lemme 1.11, que $|\ |$ s'étend à $\widehat{K}$.

Proposition 1.13. — *$|\ |$ est une norme sur $\widehat{K}$ et $\widehat{K}$ est complet pour cette norme et contient K comme sous-corps dense.*

Démonstration. — La multiplicativité de la norme et l'inégalité triangulaire (resp. ultramétrique) passent à la limite. D'autre part, $|a|=0 \Leftrightarrow \lim\limits_{n\to+\infty}|a_n|=0 \Leftrightarrow a\in I$ et donc $|\ |$ est une norme sur $\widehat{K}$ qui est ultramétrique si $|\ |$ est ultramétrique sur K.

Maintenant, si $a=(a_n)_{n\in\mathbf{N}}\in\tilde{K}$, alors $|a-a_n|\leqslant\sup_{p\geqslant1}|a_{n+p}-a_n|$ tend vers 0 quand n tend vers $+\infty$ puisque la suite $(a_n)_{n\in\mathbf{N}}$ est de Cauchy. On a donc $a=\lim_{n\to+\infty}a_n$ dans $\widehat{K}$ et donc que K est dense dans $\tilde{K}$.

Finalement, si $(a_n)_{n\in\mathbf{N}}$ est une suite de Cauchy dans $\widehat{K}$, comme K est dense dans $\widehat{K}$, on peut trouver pour chaque n un élément b_n de K tel que l'on ait $|a_n-b_n|\leqslant 2^{-n}$ et la suite b_n est de Cauchy dans K donc converge dans $\widehat{K}$ vers une limite qui est aussi celle de la suite $(a_n)_{n\in\mathbf{N}}$; ce qui prouve que $\widehat{K}$ est complet.

Définition 1.14. — Le corps $\widehat{K}$ (muni de la norme $|\ |$) s'appelle *le complété de K* pour la norme $|\ |$.

Exemple 1.15. — (i) $\mathbf{R}$ est le complété de $\mathbf{Q}$ pour la valeur absolue.

(ii) $\mathbf{C}$ est le complété de $\mathbf{Q}(i)$ pour la norme $|a+ib|=\sqrt{a^2+b^2}$.

(iii) De manière générale, si K est un corps normé complet, et L est un sous-corps dense de K, alors K est le complété de L pour la norme induite.

(iv) Le complété de $K(X)$ pour la norme $|\ |_X$ est $K((X))$.

Définition 1.16. — On note $\mathbf{Q}_p$, *corps des nombres p-adiques*, le complété de $\mathbf{Q}$ pour la norme $|\ |_p$.

1.5. Espaces vectoriels de dimension finie sur un corps normé complet

Proposition 1.17. — *Soit K un corps normé complet et V un espace vectoriel de dimension finie sur K, alors toutes les normes sur V (compatibles avec la norme sur K, i.e. vérifiant $\|\lambda x\| = |\lambda| \cdot \|x\|$ si $\lambda \in K$ et $x \in V$) sont équivalentes et V est complet pour n'importe laquelle d'entre elles.*

Démonstration. — Il suffit de prouver qu'elles sont toutes équivalentes à la norme du sup., ce qui se fait par récurrence sur la dimension de V. Si cette dimension est 1, il n'y a rien à faire. Sinon, soit $e_1, \dots, e_n$ une base de V ; on a

$$\|x_1 e_1 + \cdots + x_n e_n\| \leqslant (\|e_1\| + \cdots + \|e_n\|) \sup(|x_1|, \dots, |x_n|),$$

d'où l'une des deux inégalités à vérifier. Pour démontrer l'autre, raisonnons par l'absurde. Supposons qu'il existe une suite $x_1^{(k)} e_1 + \cdots + x_n^{(k)} e_n$ qui tende vers 0 pour la norme $\|\ \|$ mais pas pour la norme du sup. Il existe alors $C > 0$, $i \in \{1, \dots, n\}$ et une sous-suite infinie telle que l'on ait $|x_i^{(k)}| \geqslant C$ et donc la suite de terme général $v_k = \frac{x_1^{(k)}}{x_i^{(k)}} e_1 + \cdots + \frac{x_n^{(k)}}{x_i^{(k)}} e_n$ tend encore vers 0 pour $\|\ \|$. On en déduit le fait que e_i est dans l'adhérence de $W = \mathrm{Vect}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$ qui est complet d'après l'hypothèse de récurrence, ce qui implique $e_i \in W$ et est absurde puisque les e_i forment une base de V.

2. Corps ultramétriques

2.1. Normes ultramétriques et valuations

Définition 2.1. — Si K est un corps, une *valuation* v sur K est une application $x \mapsto v(x)$ de K dans $\mathbf{R} \cup \{+\infty\}$ vérifiant les trois conditions suivantes :

(i) $v(x) = +\infty \Leftrightarrow x = 0$.

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x + y) \geqslant \inf(v(x), v(y))$.

Remarque 2.2. — (i) Si K est un corps muni d'une norme ultramétrique $|\ |$ et si $\lambda < 0$, alors $v : K \to \mathbf{R}_+ \cup \{+\infty\}$ défini par $v(x) = \lambda \log |x|$ est une valuation sur K.

(ii) Réciproquement, si v est une valuation sur K et $0 < a < 1$, alors $|x| = a^{v(x)}$ est une norme ultramétrique sur K.

(iii) Il résulte du lemme 1.4 que l'on a $v(x + y) = \inf(v(x), v(y))$, si $v(x) \neq v(y)$.

On dit que la valuation est *discrète* si $v(K^*)$ est un sous-groupe discret de $\mathbf{R}$ (il est alors de la forme $a\mathbf{Z}$) et on dit qu'elle est *normalisée* si $v(K^*) = \mathbf{Z}$.

D'après la remarque précédente, il est équivalent de raisonner en termes de norme ultramétrique ou en termes de valuation, et on définit de manière évidente le complété $\widehat{K}$ d'un corps K muni d'une valuation v. Il faut toutefois faire attention au fait que les inégalités se trouvent renversées. Les formules étant en général nettement plus agréables en termes de valuations que de normes, nous ne parlerons plus que de valuations pour le reste de ce cours.

Remarque 2.3. — (i) Si K est muni d'une valuation v, il résulte du (ii) du lemme 1.11 que $v(\widehat{K}^*) = v(K^*)$, et donc que $v(\widehat{K}^*)$ est un sous-groupe additif de $\mathbf{R}$ qui n'a aucune raison d'être fermé.

(ii) Une suite est de Cauchy si et seulement si $v(u_{n+1} - u_n)$ tend vers $+\infty$. Donc, si K est complet, une suite converge si et seulement si $v(u_{n+1} - u_n)$ tend vers $+\infty$. De même, une série converge si et seulement si la valuation de son terme général tend vers $+\infty$.

Proposition 2.4. — *Si K est un corps muni d'une valuation v, alors $\mathscr{O}_K = \{x \in K \mid v(x) \geqslant 0\}$ est un anneau local d'idéal maximal $\mathfrak{m}_K = \{x \in K \mid v(x) > 0\}$.*

Démonstration. — Le fait que $\mathscr{O}_K$ soit un anneau et $\mathfrak{m}_K$ un idéal est une conséquence immédiate des propriétés d'une valuation. D'autre part, si x est un élément de $\mathscr{O}_K$ n'appartenant pas à $\mathfrak{m}_K$, alors $v(x) = 0$ et donc x^{-1} est un élément de K de valuation 0 donc appartient à $\mathscr{O}_K$, ce qui prouve que $\mathscr{O}_K - \mathfrak{m}_K$ n'est autre que le groupe des unités $\mathscr{O}_K^*$ de $\mathscr{O}_K$, et permet de conclure.

Définition 2.5. — L'anneau $\mathscr{O}_K$ s'appelle *l'anneau des entiers de K* et le corps $k_K = \mathscr{O}_K/\mathfrak{m}_K$ est *le corps résiduel de K*.

Exemple 2.6. — L'anneau des entiers de $K((X))$ est $K[[X]]$, et son corps résiduel est K.

Exercice 3. — Soit K un corps complet pour une valuation v. Soit $K\{\{X\}\}$ l'ensemble des séries de Laurent $f = \sum_{n\in\mathbf{Z}} a_n X^n$ telles que la suite $(a_n)_{n\in\mathbf{Z}}$ soit bornée dans K et tende vers 0 quand n tend vers $-\infty$ (autrement dit, il existe $C \in \mathbf{R}$ tel que $v(a_n) \geqslant C$ quel que soit $n \in \mathbf{Z}$, et $\lim_{n\to-\infty} v(a_n) = +\infty$). Si $f = \sum_{n\in\mathbf{Z}} a_n X^n \in K\{\{X\}\}$, on pose $v_G(f) = \inf_{n\in\mathbf{Z}} v(a_n)$.

(i) Montrer que, si $f, g \in K\{\{X\}\}$, alors $v_G(fg) = v_G(f) + v_G(g)$, que v_G est une valuation sur $K\{\{X\}\}$ et que $K\{\{X\}\}$ est complet pour v_G.

(ii) Montre que si v est une valuation discrète, alors $K\{\{X\}\}$ est un corps de valuation discrète, et que le corps résiduel de $K\{\{X\}\}$ est $k_K((X))$.

2.2. Le corps $\mathbf{Q}_p$ et l'anneau $\mathbf{Z}_p$

On note $\mathbf{Z}_p$ l'anneau des entiers de $\mathbf{Q}_p$ (que l'on voit comme complété de $\mathbf{Q}$ pour la valuation v_p). Son idéal maximal est $p\mathbf{Z}_p$ car $v_p(\mathbf{Q}_p^*) = v_p(\mathbf{Q}^*) = \mathbf{Z}$, et donc, si $v_p(x) > 0$, alors $v_p(x) \geqslant 1$. Il ressort de la discussion générale que $\mathbf{Q}_p$ est un corps ultramétrique complet et qu'une série $\sum_{i\in I} a_i$ converge dans $\mathbf{Q}_p$ si et seulement $v_p(a_i)$ tend vers $+\infty$ suivant le filtre des complémentaire des parties finies.

Lemme 2.7. — *L'application naturelle de $\mathbf{Z}/p^n\mathbf{Z}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$ est un isomorphisme.*

Démonstration. — Si x est un élément de $\mathbf{Z} \cap p^n\mathbf{Z}_p$, on a $v_p(x) \geqslant n$, ce qui signifie que x est divisible par p^n dans $\mathbf{Z}$. On en déduit l'injectivité. Prouvons la surjectivité. Soit $\overline{x} \in \mathbf{Z}_p/p^n\mathbf{Z}_p$ et $x \in \mathbf{Z}_p$ ayant pour image $\overline{x}$ modulo p^n. Comme $\mathbf{Q}$ est dense dans $\mathbf{Q}_p$, il existe $r \in \mathbf{Q}$ vérifiant $v_p(x - r) \geqslant n$; en particulier $v_p(r) \geqslant 0$. Écrivons r sous la forme $\frac{a}{b}$ avec $a, b \in \mathbf{Z}$. Comme $v_p(r) \geqslant 0$, on a $v_p(b) \leqslant v_p(a)$ et quitte à tout diviser par $p^{v_p(b)}$, on peut supposer $(b, p) = 1$. Soit $\overline{c}$ l'inverse de b dans $\mathbf{Z}/p^n\mathbf{Z}$ et $c \in \mathbf{Z}$ dont la réduction modulo p^n est $\overline{c}$. On a alors $v_p(r - ac) = v_p(a) + v_p(1 - bc) \geqslant n$ et donc $v_p(x - ac) \geqslant n$, ce qui prouve que ac a pour image $\overline{x}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$, et permet de conclure.

Corollaire 2.8. — *Le corps résiduel de $\mathbf{Q}_p$ est $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.*

On déduit de ce lemme une autre description, plus algébrique, de l'anneau $\mathbf{Z}_p$. On aurait d'ailleurs pu partir de cette construction, et rendre p inversible pour obtenir $\mathbf{Q}_p$; les deux approches ont leurs avantages.

Proposition 2.9. — *L'application qui à $x \in \mathbf{Z}_p$ associe la suite $(x_n)_{n\in\mathbf{N}}$ de ses images modulo p^n, $n \in \mathbf{N}$ induit un isomorphisme d'anneaux topologiques de $\mathbf{Z}_p$ sur la limite projective des $\mathbf{Z}/p^n\mathbf{Z}$* (l'ensemble des suites $(x_n)_{n\in\mathbf{N}}$, où $x_n \in \mathbf{Z}/p^n\mathbf{Z}$ et x_{n+1} a pour image x_n par l'application naturelle (de réduction modulo p^n) de $\mathbf{Z}/p^{n+1}\mathbf{Z}$ dans $\mathbf{Z}/p^n\mathbf{Z}$).

Démonstration. — Il suffit de vérifier la bijectivité de l'application $\iota : \mathbf{Z}_p \to \varprojlim \mathbf{Z}_p/p^n\mathbf{Z}_p$, qui à x, associe la suite de ses réductions modulo p^n, $n \in \mathbf{N}$. Si $\iota(x) = 0$, c'est que $v_p(x) \geqslant n$ quel que soit $n \in \mathbf{N}$, et donc $v_p(x) = +\infty$ et $x = 0$. On en déduit l'injectivité de ι. Maintenant, si $(\overline{x}_n)_{n\in\mathbf{N}} \in \varprojlim \mathbf{Z}_p/p^n\mathbf{Z}_p$, et si $x_n \in \mathbf{Z}_p$ est un relèvement quelconque de $\overline{x}_n$, alors $v_p(x_{n+k}-x_n) \geqslant n$ quels que soient $n, k \in \mathbf{N}$. La suite $(x_n)_n \in \mathbf{N}$ est donc de Cauchy dans $\mathbf{Q}_p$ et sa limite x vérifie, par passage à la limite, l'inégalité $v_p(x-x_n) \geqslant n$ quel que soit $n \in \mathbf{N}$. On a donc $\iota(x) = (\overline{x}_n)_{n\in\mathbf{N}}$, ce qui prouve la surjectivité de ι, et permet de conclure.

Théorème 2.10. — (i) *$\mathbf{Z}_p$ est compact et $\mathbf{Q}_p$ est localement compact.*

(ii) *Tout élément de $\mathbf{Z}_p$ peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} p^n a_n$ où $a_n \in \{0, 1, \ldots, p-1\}$.*

(iii) *$\mathbf{N}$ est dense dans $\mathbf{Z}_p$; plus généralement, si $b \in \mathbf{Z}$ est premier à p et $a \in \mathbf{Z}$, $a + b\mathbf{N}$ est dense dans $\mathbf{Z}_p$.*

Démonstration. — Le (i) suit de la proposition précédente : $\mathbf{Z}_p$ est un fermé d'un produit de compacts (et même d'ensembles finis) ; il est donc compact et les boules de $\mathbf{Q}_p$ sont isomorphes à $\mathbf{Z}_p$ donc compactes.

Il n'est pas difficile de voir que, si $x \in \mathbf{Z}_p$, et si x_n est l'unique élément de $\{0, \ldots, p^n - 1\}$ ayant même image que x dans $\mathbf{Z}/p^n\mathbf{Z}$, alors $\sum_{i=0}^{n} a_i p^i$ est le développement de x_n en base p (écrit dans le sens opposé à celui dont on a l'habitude...) ; on en déduit le (ii).

Le (iii) est une conséquence du (ii) (x est la limite de la suite de terme général $\sum_{i=0}^{n} p^i a_i$ dont tous les termes sont dans $\mathbf{N}$) et du fait que $x \to bx + a$ est une isométrie de $\mathbf{Z}_p$ si $(b, p) = 1$.

Exercice 4. — (i) Montrer que, si $x \in 1 + p\mathbf{Z}_p$, et si $n \in \mathbf{N}$ est premier à p, alors l'équation $y^n = x$ a une solution dans $\mathbf{Q}_p$.

(ii) Réciproquement, montrer que, si $x \in \mathbf{Q}_p - \{0\}$ est tel que l'équation $y^n = x$ a une solution dans $\mathbf{Q}_p$ pour tout $n \in \mathbf{N}$ premier à p, alors $x \in 1 + p\mathbf{Z}_p$.

(iii) Montrer que le groupe des automorphismes de corps de $\mathbf{Q}_p$ est réduit à l'identité.

2.3. Le lemme de Hensel. — Dans tout ce n° , K est un corps complet pour une valuation v, et $\mathscr{O}_K$ est l'anneau de ses entiers.

Si s est un entier, on note $\mathrm{P}_s(K)$ l'ensemble des polynômes de degré $\leqslant s-1$ à coefficients dans K muni de la base canonique $e_s = (1, X, \ldots, X^{s-1})$. Si $g \in K[X]$ est de degré $\leqslant n$ et $h \in K[X]$ est de degré $\leqslant m$, on note $\theta_{g,h}$ l'application de $\mathrm{P}_m \oplus \mathrm{P}_n$ dans P_{m+n} qui à (u, v) associe $ug + vh$ et on note $R_{m,n}(g, h)$ le déterminant de la matrice de $\theta_{g,h}$ exprimée dans les bases (e_m, e_n) et e_{m+n}.

Lemme 2.11. — *$R_{m,n}(g,h)=0$ si et seulement si on est dans un des deux cas (non exclusifs) suivants*

(i) $\deg g \leqslant n-1$ *et* $\deg h \leqslant m-1$

(ii) *g et h ne sont pas premiers entre eux.*

Démonstration. — Si $\deg g \leqslant n-1$ et $\deg h \leqslant m-1$, alors $\theta_{g,h}(\mathrm{P}_m \oplus \mathrm{P}_n) \subset \mathrm{P}_{n+m-1}$ et $\theta_{g,h}$ n'est pas bijective, ce qui implique $R_{m,n}(g,h)=0$. Si g et h sont divisibles par w avec $\deg w \geqslant 1$, on a $\theta_{g,h}(\frac{h}{w},-\frac{g}{w})=0$ et $\theta_{g,h}$ n'est pas injective, ce qui implique $R_{m,n}(g,h)=0$. Réciproquement, si g et h sont premiers entre eux, une solution de l'équation $gu+hv=0$ doit vérifier $g|v$ et $h|u$, ce qui, si $(u,v)\neq 0$, implique $\deg u \geqslant \deg h$ et $\deg v \geqslant \deg g$ et est impossible si $\deg g = n$ ou $\deg h = m$ et $(u,v)\in \mathrm{P}_m \oplus \mathrm{P}_n$. Ceci implique que $\theta_{g,h}$ est injective donc bijective et donc que $R_{m,n}(g,h)\neq 0$.

Si $f=\sum_{i=0}^n a_i X^i \in K[X]$, on définit $v_G(f)$ par la formule $v_G(f)=\inf_{0\leqslant i\leqslant n} v(a_i)$.

Théorème 2.12. — *(forme forte du lemme de Hensel) Soit $C>0$, et soient $f,g,h\in \mathscr{O}_K[X]$ vérifiant*

(i) $\deg g \leqslant n$, $\deg h \leqslant m$ *et* $\deg(f-gh)\leqslant n+m-1$

(ii) $v_G(f-gh)\geqslant C+2v(R_{m,n}(g,h))$,

alors il existe des polynômes $\tilde{g},\tilde{h}\in\mathscr{O}_K[X]$ uniques tels que l'on ait

(i) $\deg(\tilde{g}-g)\leqslant n-1$ *et* $\deg(\tilde{h}-h)\leqslant m-1$,

(ii) $v_G(\tilde{g}-g)\geqslant C+v(R_{m,n}(g,h))$ *et* $v_G(\tilde{h}-h)\geqslant C+v(R_{m,n}(g,h))$,

(iii) $f=\tilde{g}\tilde{h}$.

Démonstration. — On cherche $u\in\mathrm{P}_n$ et $v\in\mathrm{P}_m$ tels que l'on ait

$$f=(g+v)(h+u)\Leftrightarrow f-gh-uv=gu+hv\Leftrightarrow (u,v)=\theta_{g,h}^{-1}(f-gh-uv)$$

Soit $\varphi(u,v)=\theta_{g,h}^{-1}(f-gh-uv)$; on cherche un point fixe de φ. Soit

$$B=\{(u,v)\in \mathrm{P}_n\oplus\mathrm{P}_m,\ \inf(v_G(u),v_G(v))\geqslant C+v(R_{m,n}(g,h))\}.$$

Le théorème 2.12 est une conséquence immédiate du lemme suivant et de la complétude de K.

Lemme 2.13. — *φ est une application contractante de B dans elle-même.*

Démonstration. — Si $(u,v)\in B$, alors

$$\begin{aligned} v_G(f-gh-uv) &\geqslant \inf(v_G(f-gh),v_G(uv)) \\ &\geqslant \inf(C+2v(R_{m,n}(g,h)),2C+2v(R_{m,n}(g,h))) = C+2v(R_{m,n}(g,h).\end{aligned}$$

D'autre part, g et h étant à coefficients dans $\mathscr{O}_K$, $\theta_{g,h}$ a tous ses coefficients dans $\mathscr{O}_K$ et la matrice de $\theta_{g,h}^{-1}$ est donc à coefficients dans $\frac{1}{R_{m,n}(g,h)}\mathscr{O}_K$ et donc $v_G(\theta_{g,h}^{-1}(x))\geqslant v_G(x)-v(R_{m,n}(g,h))$. On en déduit le fait que φ envoie B dans B. Finalement, si (u,v) et (u',v') sont deux éléments de B,

$$\begin{aligned} v_G(\varphi(u,v)-\varphi(u',v')) =& v_G(\theta_{g,h}^{-1}(uv-u'v')) \\ \geqslant& v_G(u(v-v')+v'(u-u'))-v(R_{m,n}(g,h)) \\ \geqslant& \inf(v_G(u)+v_G(v-v'),v_G(v')+v_G(u-u')-v(R_{m,n}(g,h)) \\ \geqslant& C+\inf(v_G(u-u'),v_G(v-v')),\end{aligned}$$

ce qui prouve que φ est contractante sur B.

Corollaire 2.14. — *Soient $f, g, h \in \mathscr{O}_K[X]$ vérifiant les conditions suivantes : g est unitaire de degré n, $\deg h \leqslant m$, $\deg(f - gh) \leqslant n + m - 1$, Les réductions $\overline{g}$ et $\overline{h}$ de g et h modulo $\mathfrak{m}_K$ sont premières entre elles, et $v_G(f - gh) > 0$, alors il existe $\tilde{g}, \tilde{h} \in \mathscr{O}_K[X]$ uniques vérifiant $\deg(\tilde{g} - g) \leqslant n - 1$, $\deg(\tilde{h} - h) \leqslant m - 1$, $v_G(\tilde{g} - g) > 0$, $v_G(\tilde{h} - h) > 0$ et $\tilde{g}\tilde{h} = f$.*

Démonstration. — Comme $\overline{g}$ est de degré n et $\overline{g}$ et $\overline{h}$ sont premiers entre eux, on a $R_{m,n}(\overline{g}, \overline{h}) \neq 0$, ce qui implique $v(R_{m,n}(g, h)) = 0$. On est dans les conditions d'application du théorème pour n'importe quel $C \in \mathbf{R}$ vérifiant $v_G(f - gh) \geqslant C > 0$, et il suffit de faire tendre C vers 0 pour en déduire le résultat.

Un cas particulier intéressant est celui où g est de degré 1 : on obtient le résultat suivant permettant de localiser un zéro d'un polynôme connaissant un point où ce polynôme est « petit » C'est l'analogue ultramétrique du classique algorithme de Newton.

Proposition 2.15. — (lemme de Hensel) *Si $f \in \mathscr{O}_K[X]$ et $\alpha \in \mathscr{O}_K$ vérifie $v(f(\alpha)) > 2v(f'(\alpha))$, alors il existe $\tilde{\alpha} \in \mathscr{O}_K$ unique vérifiant les conditions $v(\tilde{\alpha} - \alpha) > v(f'(\alpha))$ et $f(\tilde{\alpha}) = 0$.*

Démonstration. — Soient d le degré de f et $C \in]0, v(f(\alpha)) - 2v(f'(\alpha))]$; cet intervalle est non vide par hypothèse. Soient g et h les éléments de $\mathscr{O}_K[X]$ donnés par les formules

$$g(X) = X - \alpha \quad \text{et} \quad h(X) = \frac{f(X) - f(\alpha)}{X - \alpha} = f^{[1]}(\alpha) + f^{[2]}(\alpha)(X - \alpha) + \cdots + f^{[d]}(\alpha)(X - \alpha)^{d-1},$$

où $f^{[i]}$ désigne la dérivée divisée i-ème de f (en caractéristique 0, on a $f^{[i]} = \frac{1}{i!} f^{(i)}$). La matrice de $\theta_{g,h} : K[X]_{d-2} \oplus K[X]_0 \to K[X]_{d-1}$ a comme coefficients (dans les bases constituées des puissances de $X - \alpha$ au lieu des puissances de X) des 1 en dessous de la diagonale, $(f^{[1]}(\alpha), \ldots, f^{[d]}(\alpha))$ sur la dernière colonne et des 0 partout ailleurs ; son déterminant est donc $\pm f^{[1]}(\alpha) = f'(\alpha)$. Le résultant $R_{d-1,1}(g, h)$ est donc de valuation $v(f'(\alpha))$. D'autre part, on a $v_G(f - gh) = v(f(\alpha)) \geqslant C + 2v(R_{d-1,1}(g, h))$ par définition de C, et $\deg f - gh \leqslant d - 1$. On est donc dans les conditions d'application du théorème 2.12 et il existe $\tilde{g}$ unique divisant f tel que $\deg(\tilde{g} - g) = 0$ et $v_G(\tilde{g} - g) \geqslant C + v(f'(\alpha))$. Il existe donc $\tilde{\alpha} \in \mathscr{O}_K$ unique tel que l'on ait $\tilde{g}(X) = X - \tilde{\alpha}$ [ce qui implique $f(\tilde{\alpha}) = 0$], et $v(\tilde{\alpha} - \alpha) \geqslant C + v(f'(\alpha))$. Il suffit alors de faire tendre C vers 0 pour en déduire le résultat.

Exercice 5. — Donner une démonstration de la prop. 2.15 utilisant l'algorithme de Newton ($x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, $x_0 = \alpha$).

Corollaire 2.16. — *Soit $f \in \mathscr{O}_K[X]$ un polynôme unitaire et soit $\overline{f}$ la réduction de f modulo $\mathfrak{m}_K$. Si $\overline{\alpha}$ est une racine simple de $\overline{f}$ dans k, alors il existe $\tilde{\alpha} \in \mathscr{O}_K$ unique, dont la réduction modulo $\mathfrak{m}_K$ est $\overline{\alpha}$ et qui vérifie $f(\tilde{\alpha}) = 0$*

Démonstration. — Soit $\alpha \in \mathscr{O}_K$ dont la réduction modulo $\mathfrak{m}_K$ est $\overline{\alpha}$. L'hypothèse selon laquelle $\overline{\alpha}$ est racine simple de $\overline{f}$ se traduit par le fait que $v(f(\alpha)) > 0$ et $v(f'(\alpha)) = 0$, ce qui permet d'utiliser la proposition 2.15 pour conclure.

Proposition 2.17. — *Soit $f \in K[X]$ un polynôme unitaire irréductible vérifiant $f(0) \in \mathscr{O}_K$. Alors tous les coefficients de f appartiennent à $\mathscr{O}_K$.*

Démonstration. — Supposons le contraire et soit i le plus grand entier tel que l'on ait $v(a_i) = v_G(f)$. Le polynôme $a_i^{-1}f$ est alors de la forme

$$b_nX^n + \cdots + b_{i+1}X^{i+1} + X^i + b_{i-1}X^{i-1} + \cdots b_0$$

où les b_k sont des éléments de $\mathscr{O}_K$ vérifiant $v(b_k) > 0$ quel que soit $k \in \{i+1, \ldots, n\}$. On peut donc appliquer le corollaire précédent à $g(X) = X^i + \cdots + b_0$ et $h = 1 + b_nX^{n-i}$ pour montrer qu'il existe des polynômes $\tilde{g}$ et $\tilde{h}$ de degrés respectifs i et j tels que l'on ait $f = a_i\tilde{g}\tilde{h}$, ce qui est en contradiction avec l'hypothèse f irréductible, et permet de conclure.

3. La clôture algébrique d'un corps valué complet

3.1. Extensions de valuations

Théorème 3.1. — *Soit K un corps complet pour une valuation v, et soit L une extension finie de K. Alors, il existe une unique manière de prolonger v en une valuation de L. De plus, si $x \in L$, alors*

$$v(x) = \frac{1}{[L:K]}v(\mathrm{N}_{L/K}(x)).$$

Démonstration. — On peut voir L comme un espace vectoriel de dimension finie $[L : K]$. Si v_1, v_2 sont deux valuations sur L prolongeant v, alors v_1 et v_2 définissent la même topologie sur L d'après la prop. 1.17. La proposition 1.7 montre alors qu'il existe $s \in \mathbf{R}_+^*$ tel que l'on ait $v_2(x) = s \cdot v_1(x)$ quel que soit $x \in L$, et comme $v_1(x) = v_2(x)$, si $x \in K$, on en déduit l'unicité d'une extension de v à L.

Pour conclure, il reste à montrer que la formule ci-dessus définit bien une valuation sur L, ou, autrement dit, que si $x \in L$ vérifie $v(\mathrm{N}_{L/K}(x)) \geqslant 0$, alors $v(\mathrm{N}_{L/K}(1+x)) \geqslant 0$.

Soit $f(X) = X^d + \cdots + a_0$, le polynôme minimal de x sur K. Ceci implique que d divise $[L : K]$ et $\mathrm{N}_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$ et donc $v(\mathrm{N}_{L/K}(x)) \geqslant 1$ implique $a_0 \in \mathscr{O}_K$ et l'irréductibilité de f implique que f est à coefficients dans $\mathscr{O}_K$ d'après la prop. 2.17. D'autre part, le polynôme minimal de $1 + x$ est $f(X - 1)$ et donc $\mathrm{N}_{L/K}(1 + x) = ((-1)^d f(-1))^{\frac{[L:K]}{d}} \in \mathscr{O}_K$, ce qui permet de conclure.

Corollaire 3.2. — *Si $\overline{K}$ est une clôture algébrique de K, il existe une unique manière de prolonger v à $\overline{K}$; de plus* $\mathrm{Aut}(\overline{K}/K)$ *agit sur $\overline{K}$ par des isométries.*

Démonstration. — L'unicité du prolongement est une conséquence directe du théorème précédent. Le reste de l'énoncé suit de ce que, si $x \in \overline{K}$, et si $\sigma \in \mathrm{Aut}(\overline{K}/K)$, alors $\mathrm{N}_{K(x)/K}(x) = \mathrm{N}_{K(\sigma(x))/K}(\sigma(x))$.

Corollaire 3.3. — *Si $P \in K[X]$ est irréductible, alors toutes ses racines dans $\overline{K}$ ont la même valuation.*

Démonstration. — Les racines d'un polynôme irréductible sont permutées transitivement par $\mathrm{Aut}(\overline{K}/K)$, et le corollaire précédent permet de conclure.

3.2. Polygones de Newton

Lemme 3.4. — *Soit $P(X) = a_nX^n + \cdots + a_0 \in K[X]$, un polynôme de degré n et soient $\alpha_1, \ldots, \alpha_n$, les racines (avec leur multiplicité) de P dans $\overline{K}$ rangées de telle sorte que l'on ait*

$$v(\alpha_1) \geqslant v(\alpha_2) \geqslant \cdots \geqslant v(\alpha_n).$$

Alors, si $i \in \{0, \ldots, n\}$, on a

$$v(a_i) \geqslant v(a_n) + \sum_{k=0}^{n-i-1} v(\alpha_{n-k}).$$

avec égalité si $v(\alpha_i) > v(\alpha_{i+1})$.

Démonstration. — L'inégalité est une conséquence du lien entre les coefficients de P et les fonctions symétriques des racines de P et le cas d'égalité vient de ce que, si $v(\alpha_i) > v(\alpha_{i+1})$, alors dans la fonction symétrique d'ordre $n-i$, tous les autres termes ont une valuation strictement plus grande que $\prod_{k=1}^{n-i-1} \alpha_{n-k}$.

Soit $u : [0, n[\to \mathbf{R} \cup \{+\infty\}$ la fonction définie par $u(x) = -v(\alpha_i)$ si $x \in [i-1, i[$ et $\mathrm{Newt}_P(x) = v(a_n) + \int_n^x u(t)dt$. La fonction $u(x)$ est croissante et en escalier et la fonction $\mathrm{Newt}_P(x)$ est donc convexe et affine par morceaux sur $[0, n]$. Le lemme précédent peut se traduire aussi par $v(a_i) \geqslant \mathrm{Newt}_P(i)$ avec égalité si $v(\alpha_i) > v(\alpha_{i+1})$, c'est-à-dire si les dérivées à droite et à gauche de la fonction Newt_P au point i sont différentes (autrement dit, si $(i, \mathrm{Newt}_P(i))$ est un *sommet* (du graphe) de Newt_P). L'ensemble $\{(x, y) \mid x \in [0, 1],\ y \geqslant \mathrm{Newt}_P(x)\}$ s'appelle le *polygone de Newton de P* ; c'est aussi l'enveloppe convexe de l'ensemble de $(i, v(a_i))$ et de $[0, n] \times \{+\infty\}$. On appelle *pente de* Newt_P ou *pente du polygône de Newton de P* un élément de $\mathrm{Newt}'_P([0, n])$ et, si λ est une pente de Newt_P, on appelle *segment de pente λ* de Newt_P l'ensemble $\{(x, \mathrm{Newt}_P(x)) \mid \mathrm{Newt}'_P(x) = \lambda\}$; la *longueur* de ce segment est, par définition, la longueur de sa projection sur l'axe des x.

Le théorème suivant est une traduction du lemme 3.4, en utilisant le langage des polygones de Newton.

Théorème 3.5. — *Il existe une racine de P de valuation λ si et seulement si $-\lambda$ est une pente de* Newt_P. *De plus, le nombre de racines de P (comptées avec multiplicité) de valuation λ est la longueur du segment de pente $-\lambda$ de* Newt_P.

Remarque 3.6. — Il résulte du cor. 3.3 que Newt_P n'a qu'une pente, si P est irréductible.

Exercice 6. — Soient $P, Q \in K[X]$. On suppose que Q divise P. Comment obtient-on le polygone de Newton de $\frac{P}{Q}$ en fonction de ceux de P et Q.

Proposition 3.7. — *Supposons que v est discrète et normalisée. Soit $P \in K[X]$.*

(i) Les pentes du polygone de Newton de P sont des nombres rationnels. De plus, si $\frac{a}{b}$, avec $(a, b) = 1$, est une pente de Newt_P, *alors la longueur du segment de pente λ est un multiple de b.*

(ii) Si Newt_P *n'a qu'une pente $\frac{a}{b}$, avec $(a, b) = 1$, et si $\deg P = b$, alors P est irréductible.*

Démonstration. — Si la la valuation de K est discrète et normalisée, les sommets du polygone de Newton de P sont à coordonnées entières. Le résultat s'en déduit (modulo le petit exercice de réfléxion ci-dessus).

Corollaire 3.8. — *(Critère d'Eisenstein) Si* $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ *vérifie* $v(a_i) \geqslant 1$ *quel que soit* $0 \leqslant i \leqslant n-1$ *et* $v(a_0) = 1$*, alors* P *est irréductible*

Démonstration. — Son polygône de Newton est un segment de longueur n et de pente $\frac{-1}{n}$.

3.3. Condensé de théorie de Galois. — Soit K un corps, et soit $\overline{K}$ une clôture algébrique de K. Si L est un sous-corps de $\overline{K}$ contenant K, on note L^{sep} la *clôture séparable* de L dans $\overline{K}$, c'est-à-dire l'ensemble des éléments de $\overline{K}$ dont le polynôme minimal sur L est séparable (i.e. n'a que des racines simples). Si K est de caractéristique 0 ou, plus généralement, si K est *parfait* (si K est de caractéristique p, cela signifie que $x \mapsto x^p$ est une surjection de K dans K), alors $L^{\mathrm{sep}} = \overline{K}$; dans le cas général, L^{sep} est un sous-corps de $\overline{K}$.

Si L est un sous-corps de $\overline{K}$ contenant K, on note L^{rad} la *clôture radicielle* de L dans $\overline{K}$, c'est-à-dire l'ensemble des éléments x de $\overline{K}$ tels qu'il existe $n \in \mathbf{N}$ (dépendant de x) tel que $x^{p^n} \in L$. C'est un sous-corps parfait de $\overline{K}$, et on a $L^{\mathrm{sep}} \cap L^{\mathrm{rad}} = L$ et $L^{\mathrm{sep}} \cdot L^{\mathrm{rad}} = \overline{K}$.

Soit $\mathrm{G}_K = \mathrm{Aut}(\overline{K}/K)$. Si L est une extension algébrique de K contenue dans $\overline{K}$, on note G_L le sous-groupe des éléments de G_K laissant fixe L. On a aussi $\mathrm{G}_L = \mathrm{Gal}(L^{\mathrm{sep}}/L)$. Si L est une extension finie de K, alors G_L est d'indice fini dans G_K et $|\mathrm{G}_K/\mathrm{G}_L| \leqslant [L:K]$, avec égalité si et seulement si l'exension L/K est séparable.

Le groupe G_K est muni d'une topologie de groupe profini : une base de voisinages de l'élément neutre est constituée des G_L, où L parcourt l'ensemble des extensions finie de K dans $\overline{K}$. En particulier, G_K est un groupe compact. Si H est un sous-groupe fermé de G_K, on note $\overline{K}^H$ le sous-corps de $\overline{K}$ fixé par H.

La théorie de Galois peut alors se condenser en l'énoncé suivant.

Théorème 3.9. — *(i) Si* H *est un sous-groupe fermé de* G_K*, alors* $(K^{\mathrm{sep}})^H$ *(resp.* $\overline{K}^H$*) est une extension séparable de* K *(resp. de* K^{rad}*), galoisienne si* H *est distingué dans* G_K*, et on a* $\mathrm{G}_{(K^{\mathrm{sep}})^H} = \mathrm{G}_{\overline{K}^H} = H$*.*

(ii) Si L *est une extension algébrique de* K*, alors* G_L *est un sous-groupe fermé de* G_K*, et on a* $(L \cdot K^{\mathrm{sep}})^{\mathrm{G}_L} = L$ *et* $\overline{K}^{\mathrm{G}_L} = L^{\mathrm{rad}}$*.*

3.4. Le complété d'un corps algébriquement clos. — D'après le cor. 3.2, il existe une unique manière de prolonger une valuation à la clôture algébrique d'un corps valué complet. Cette clôture algébrique n'a aucune raison d'être complète (et elle ne l'est, en général, pas), donc on peut la compléter, reprendre la clôture algébrique, recompléter... Le théorème suivant montre qu'en fait le procédé converge très vite.

Théorème 3.10. — *Si* K *est un corps algébriquement clos muni d'une valuation, son complété* $\widehat{K}$ *est algébriquement clos.*

Démonstration. — Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire irréductible de $\widehat{K}[X]$. Notre but est de prouver que P a une racine dans $\widehat{K}$. Quitte à P en $\alpha^n P(\frac{X}{\alpha})$, ce qui multiplie a_i par α^{n-i}, on peut supposer que P est à coefficients entiers. Commençons par supposer que P est séparable, c'est-à-dire que P et P' sont premiers entre eux. Il existe alors des polynômes U et V tels que l'on ait $UP + VP' = 1$.

Soit, comme d'habitude, v_G la valuation de Gauss sur $\widehat{K}[X]$. Soit $C > \sup(0, -v_G(U), -2v_G(V))$, et, si $0 \leqslant i \leqslant n-1$, soit $b_i \in K$ tels que l'on ait $v(b_i - a_i) \geqslant C$. Soit $x_0 \in K$ une racine du

polynôme $Q(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$. On a $v(x_0) \geqslant 0$ car Q est à coefficients entiers. Ceci implique $v(U(x_0)P(x_0)) \geqslant C + v_G(U) > 0$ et donc $v(P'(x_0)V(x_0)) = 0$, d'où l'on tire $v(P'(x_0)) \leqslant -v_G(V)$, et $v(P(x_0)) \geqslant C > 2v(P'(x_0))$. Le lemme de Hensel permet de conclure au fait que l'équation $P(x) = 0$ a une solution dans $\widehat{K}$.

Si P est irréductible mais pas séparable, on est en caractéristique $p \neq 0$, et il existe Q irréductible et séparable et $m \in \mathbf{N}$ tel que l'on ait $P(X) = Q(X^{p^m})$. Si x est une racine de Q et x_n une suite d'éléments de K tendant vers x dans $\widehat{K}$, alors $x_n^{p^{-m}}$ est une suite d'éléments de K tendant vers une racine P (elle est de cauchy car $v(x^{p^{-m}} - y^{p^{-m}}) = p^{-m}v(x-y)$).

Exercice 7. — Montrer que le résultat ci-dessus reste vrai pour un corps muni d'une norme pas nécessairement ultramétrique

3.5. Le corps résiduel d'un corps algébriquement clos

Lemme 3.11. — *Soient K un corps ultramétrique complet et L une extension finie de K, alors k_L est une extension algébrique de k_K de degré $\leqslant [L : K]$.*

Démonstration. — On a $\mathscr{O}_K \cap \mathfrak{m}_L = \mathfrak{m}_K$ et donc k_K s'injecte dans k_L. Soient $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ des éléments de k_L formant une famille libre sur k_K. Choisissons pour chaque $i \in \{1, \ldots, d\}$ un élément α_i de $\mathscr{O}_L$ dont l'image dans k_L est $\overline{\alpha}_i$. Supposons que les α_i forment une famille liée sur K et soit $(\lambda_1, \ldots, \lambda_d)$ une famille d'éléments non tous nuls de K tels que l'on ait $\lambda_1\alpha_1 + \cdots + \lambda_d\alpha_d = 0$. Quitte à diviser tous les λ_i par celui qui a la plus grande norme, on peut supposer qu'ils sont tous éléments de $\mathscr{O}_K$ et que l'un d'entre eux est égal à 1, ce qui conduit à une contradiction quand on réduit modulo $\mathfrak{m}_L$. Ceci permet de conclure.

Lemme 3.12. — *Si K est un corps ultramétrique algébriquement clos, alors k_K est algébriquement clos.*

Démonstration. — Soit $\overline{P}(X) \in k_K[X]$ unitaire de degré $n \geqslant 1$ et soit $P(X) \in \mathscr{O}_K[X]$ unitaire de degré n relevant $\overline{P}$. Soit $\alpha \in K$ une racine de P. On a $\alpha \in \mathscr{O}_K$ (les pentes du polygone de Newton de P sont négatives, donc ses racines ont des valuations $\geqslant 0$), et l'image de α dans k_K est une racine de $\overline{P}$, ce qui permet de conclure.

Lemme 3.13. — *Si K est un corps ultramétrique et $\widehat{K}$ dénote son complété, alors $k_K = k_{\widehat{K}}$.*

Démonstration. — $\mathscr{O}_K \cap \mathfrak{m}_{\widehat{K}} = \{x \in \mathscr{O}_K \mid v(x) > 0\} = \mathfrak{m}_K$ et donc l'application naturelle de k_K dans $k_{\widehat{K}}$ est injective. D'autre part, comme $\mathscr{O}_K$ est dense dans $\mathscr{O}_{\widehat{K}}$, cette application est surjective, ce qui permet de conclure.

Corollaire 3.14. — *Si K est un corps valué complet, alors le corps résiduel de $\widehat{\overline{K}}$ est une clôture algébrique de k_K.*

3.6. Le théorème d'Ax-Sen-Tate. — Soit K un corps complet pour une valuation. Comme on l'a vu, au cor. 3.2 la valuation sur K se prolonge de manière unique en une valuation sur $\overline{K}$ et $\sigma \in \mathrm{G}_K = \mathrm{Aut}(\overline{K}/K)$ agit par une isométrie ; on peut donc étendre l'action de G_K par continuité en une action sur $\widehat{\overline{K}}$ qui est un corps algébriquement clos d'après le théorème 3.10.

Théorème 3.15. — *Soit H un sous-groupe fermé de G_K ; alors $(\widehat{\overline{K}})^H$ est le complété de $\overline{K}^H$. Autrement dit, $(\overline{K})^H$ est dense dans $(\widehat{\overline{K}})^H$.*

Soit $L = \overline{K}^H$; c'est un sous-corps parfait de $\overline{K}$. Si $\alpha \in \overline{K}$, on définit le *diamètre* $\Delta_L(\alpha)$ de α par rapport à L par $\Delta_L(\alpha) = \inf_{\sigma\in H} v(\sigma(\alpha)-\alpha)$. Notons que $\alpha \in L$ si et seulement si $\Delta_L(\alpha) = +\infty$.

La démonstration du théorème 3.15 repose sur la proposition suivante.

Proposition 3.16 **(Ax)**. — *Il existe une constante C telle que si $\alpha \in \overline{K}$, alors il existe $a \in L$ vérifiant $v(\alpha - a) \geqslant \Delta_L(\alpha) - C$.*

Autrement dit, si α est presque fixe par H, alors $\alpha \in \overline{K}$ est proche d'un élément de L. Soit $x \in \widehat{\overline{K}}$ fixe par H. Si α_n est une suite d'éléments de $\overline{K}$ tendant vers x, alors $\Delta_L(\alpha_n)$ tend vers $+\infty$ car $v(\sigma(\alpha_n)-\alpha_n) = v(\sigma(\alpha_n)-\sigma(x)+x-\alpha_n) \geqslant \inf(v(\sigma(x-\alpha_n), v(x-\alpha_n)) = v(x-\alpha_n)$, et donc si a_n est un élément de L vérifiant $v(a_n-\alpha_n) \geqslant \Delta_L(\alpha_n) - C$, la suite a_n est une suite d'éléments de L tendant vers x, et $x \in \widehat{L}$, ce qu'il fallait démontrer pour déduire le th. 3.15 de la prop. 3.16.

Passons à la démonstration de la proposition 3.16. La démonstration est un peu différente suivant qu'on est en égale ou inégale caractéristique.

3.6.1. Le cas d'égale caractéristique. — Notons M le corps $L(\alpha)$; c'est une extension finie de L qui est séparable car L est parfait.

Le cas où K est de caractéristique 0 et son corps résiduel aussi est évident : on peut prendre $C = 0$, et poser $a = \mathrm{Tr}_{M/L}(y\alpha)$, avec $y = \frac{1}{[M:L]}$; on a alors $v(y) = 0$, et

$$a - \alpha = \sum_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} \big(\sigma(y\alpha) - y\alpha\big) = y \cdot \sum_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} (\sigma(\alpha)-\alpha))$$

a une valuation $\geqslant \inf_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} v(\sigma(\alpha)-\alpha) = \Delta_L(\alpha)$.

Si K est de caractéristique p, l'application trace $\mathrm{Tr}_{M/L}$ est surjective (car M/L est séparable comme nous l'avons remarqué), et il existe $x \in M$ tel que l'on ait $\mathrm{Tr}_{M/L}(x) = 1$. Mais alors $\mathrm{Tr}_{M/L}(x^{p^{-n}}) = 1$ quel que soit $n \in \mathbf{N}$; on en déduit le fait que quel que soit $\delta > 0$, il existe $y \in M$ vérifiant $\mathrm{Tr}_{M/L}(y) = 1$ et $v(y) > -\delta$. Maintenant, on a $a = \mathrm{Tr}_{M/L}(y\alpha) \in L$ et

$$a - \alpha = \sum_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} \big(\sigma(y\alpha) - \sigma(y)\alpha\big) = \sum_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} \sigma(y)(\sigma(\alpha)-\alpha))$$

a un valuation $\geqslant \inf_{\sigma\in\mathrm{Hom}_L(M,\overline{K})} v(\sigma(y)) + v(\sigma(\alpha)-\alpha) \geqslant -\delta + \Delta_L(\alpha)$. On peut donc prendre pour C n'importe quel nombre strictement positif.

3.6.2. Le cas d'inégale caractéristique. — Supposons maintenant que K est de caractéristique 0 et que son corps résiduel est de caractéristique p ; quitte à renormaliser v, on peut supposer que $v = v_p$ (i.e. que $v(p) = 1$). Nous aurons besoin du lemme suivant.

Lemme 3.17. — *Soit $P \in \overline{K}[X]$ unitaire de degré n dont toutes les racines vérifient $v_p(\alpha) \geqslant u$*

(i) *Si $n = p^k d$ avec $(d,k) = 1$ et $d > 0$ et si $q = p^k$, alors le polynôme $P^{(q)}$, dérivée q-ième de P, a au moins une racine β vérifiant $v_p(\beta) \geqslant u$.*

(ii) *Si $n = p^{k+1}$ et $q = p^k$, alors $P^{(q)}$ a au moins une racine β vérifiant $v_p(\beta) \geqslant u - \frac{1}{p^{k+1}-p^k}$.*

Démonstration. — On a $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, avec $v_p(a_{n-i}) \geqslant iu$ d'après la théorie des polygônes de Newton (ou, ce qui revient au même, par un développement brutal). On a $\frac{1}{q!}P^{(q)}(X) = \sum_{i=0}^{n-q}\binom{n-i}{q}a_{n-i}X^{n-i-q}$, et le produit des racines de $P^{(q)}$ est, au signe près, $\frac{a_q}{\binom{n}{q}}$. On a donc $\sum_\beta v_p(\beta) = v_p(a_q) - v_p(\binom{n}{q}) \geqslant (n-q)u - v_p(\binom{n}{q})$, et il existe β vérifiant $v_p(\beta) \geqslant u - \frac{1}{n-q}v_p(\binom{n}{q})$. D'autre part, on a $\binom{n}{q} = \frac{n}{q}\prod_{i=1}^{q-1}\frac{n-i}{i}$ et, comme $q = p^k$ et $v_p(n) \geqslant k$, on a $v_p(\frac{n-i}{i}) = 0$ et $v_p(\binom{n}{q}) = v_p(n) - v_p(q)$. On en déduit le résultat.

La proposition suivante montre que l'on peut prendre $C = \frac{p}{(p-1)^2}$.

Proposition 3.18. — *Si $[L(\alpha) : L] = n$ et $\ell(n)$ est le plus grand entier ℓ tel que $p^\ell \leqslant n$, il existe $a \in L$ vérifiant $v_p(a-\alpha) \geqslant \Delta_L(\alpha) - \sum_{i=1}^{\ell(n)}\frac{1}{p^i - p^{i-1}}$.*

Démonstration. — Par récurrence sur n, le cas $n = 1$ étant évident. On va appliquer le lemme précédent à $P = Q(X+\alpha)$, où Q est le polynôme minimal de α sur L. Remarquons que les racines de P sont les $\sigma(\alpha) - \alpha$, pour $\sigma \in H$, et donc que le u du lemme précédent peut être pris égal à $\Delta_L(\alpha)$. Il y a deux cas.

• Si n n'est pas une puissance de p, il existe $q \in \mathbf{N}$ tel que le polynôme $P^{(q)}$ ait une racine β vérifiant $v_p(\beta - \alpha) \geqslant \Delta_L(\alpha)$. D'autre part, si $\sigma \in H$, alors

$$v_p(\sigma(\beta) - \beta) = v_p(\sigma(\beta) - \sigma(\alpha) + \sigma(\alpha) - \alpha + \alpha - \beta) \geqslant \min(v_p(\sigma(\beta-\alpha), v_p(\sigma(\alpha)-\alpha), v_p(\beta-\alpha)),$$

et comme $v_p(\sigma(\beta-\alpha)) = v_p(\beta-\alpha) \geqslant \Delta_L(\alpha)$ et $v_p(\sigma(\alpha)-\alpha) \geqslant \Delta_L(\alpha)$ par définition, on en tire l'inégalité $\Delta_L(\beta) \geqslant \Delta_L(\alpha)$, et comme $[L(\beta) : L] < n$, cela permet de conclure en utilisant l'hypothèse de récurrence.

• Si $n = p^{k+1}$, on peut trouver une racine β de $P^{(p^k)}$ vérifiant $v_p(\beta-\alpha) \geqslant \Delta_L(\alpha) - \frac{v_p(p)}{p^{k+1}-p^k}$ et on obtient par le même raisonnement l'existence de $\beta \in \overline{K}$ vérifiant $\Delta_L(\beta) \geqslant \Delta_L(\alpha) - \frac{1}{p^{k+1}-p^k}$ et $[L(\beta) : L] < n = p^{k+1}$. On tire de l'hypothèse de récurrence l'existence de $a \in L$ vérifiant $v_p(\beta - a) \geqslant \Delta_L(\beta) - \sum_{i=1}^{k}\frac{1}{p^i-p^{i-1}} \geqslant \Delta_L(\alpha) - \sum_{i=1}^{k+1}\frac{1}{p^i-p^{i-1}}$ et comme $v_p(\alpha-\beta) \geqslant \Delta_L(\alpha) - \sum_{i=1}^{k+1}\frac{1}{p^i-p^{i-1}}$, cela permet de conclure.

4. Le corps $\mathbf{C}_p$

4.1. Propriétés algébriques

4.1.1. Définition. — Soit $\overline{\mathbf{Q}}_p$ une clôture algébrique de $\mathbf{Q}_p$. D'après la théorie générale, v_p se prolonge de manière unique en une valuation sur $\overline{\mathbf{Q}}_p$. On note $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}}_p$ pour v_p. C'est un corps algébriquement clos d'après le th. 3.10. Ce corps joue, pour beaucoup de questions, le rôle de $\mathbf{C}$ en p-adique. Il est abstraitement isomorphe à $\mathbf{C}$ pour des raisons de cardinal, mais Tate a démontré (voir plus tard), qu'il ne contenait pas d'analogue raisonnable de $2i\pi$.

Si $r \in \mathbf{R}$ et $a \in \mathbf{C}_p$, on note $D(a,r)$ la boule fermée $\{x \in \mathbf{C}_p,\ v_p(x-a) \geqslant r\}$, et $D(a,r^+)$ la boule ouverte $\{x \in \mathbf{C}_p,\ v_p(x-a) > r\}$. En particulier, $D(0,0) = \mathscr{O}_{\mathbf{C}_p}$, et $D(0,0^+) = \mathfrak{m}_{\mathbf{C}_p}$.

4.1.2. Représentants de Teichmüller. — Le corps résiduel de $\mathbf{C}_p$ est une clôture algébrique $\overline{\mathbf{F}}_p$ de $\mathbf{F}_p$, d'après le cor. 3.14. Nous allons exhiber un système de représentants privilégiés de $\overline{\mathbf{F}}_p$ dans $\mathscr{O}_{\mathbf{C}_p}$.

Proposition 4.1. — *Si $x \in \overline{\mathbf{F}}_p^*$, il existe dans $\mathscr{O}_{\mathbf{C}_p}$ une unique racine de l'unité $[x]$ d'ordre premier à p dont l'image dans $\overline{\mathbf{F}}_p$ est x.*

Démonstration. — Il existe n tel que x appartienne à $\mathbf{F}_{p^n}$. Les éléments de $\mathbf{F}_{p^n}^*$ sont solutions de l'équation $P(X) = X^{p^n-1} - 1 = 0$. Or le polynôme $X^{p^n-1} - 1$ a un discriminant premier à p [son discriminant est au signe près $\prod_{\eta^{p^n-1}=1} P'(\eta) = \pm(p^n-1)^{p^n-1}$], ce qui signifie que toutes les images de ses racines sont distinctes mod $\mathfrak{m}_{\mathbf{C}_p}$; on a donc une injection d'un ensemble à p^n-1 éléments dans un ensemble à p^n-1 éléments et donc la réduction mod $\mathfrak{m}_{\mathbf{C}_p}$ est une bijection, ce qui permet de conclure.

Remarque 4.2. — L'unicité de $[x]$ implique que $[xy] = [x]\cdot[y]$. En posant $[0] = 0$, on a fabriqué un système multiplicatif de représentants, appelés *représentants de Teichmüller*, de $\overline{\mathbf{F}}_p$ dans $\mathscr{O}_{\mathbf{C}_p}$.

Exercice 8. — Soit ζ une racine de l'unité.

(i) Montrer que, si ζ est primitive d'ordre p^n, $n \geqslant 1$, alors $v_p(\zeta - 1) = \frac{1}{(p-1)p^{n-1}}$.

(ii) Montrer que, si ζ n'est pas d'ordre une puissance de p, alors $v_p(\zeta - 1) = 0$.

4.1.3. Le groupe multiplicatif $\mathbf{C}_p^*$. — On a $v_p(\mathbf{C}_p^*) = v_p(\overline{\mathbf{Q}}_p^*) = \mathbf{Q}$. Choisissons un morphisme de groupes de $\mathbf{Q}$ dans $\mathbf{C}_p^*$ envoyant 1 sur p. On notera p^r l'image de $r \in \mathbf{Q}$ par ce morphisme. Si $x \in \mathscr{O}_{\mathbf{C}_p}^*$, on note $\omega(x)$ l'unique racine de l'unité d'ordre premier à p telle que $v_p(x - \omega(x)) > 0$. Si $\overline{x}$ désigne l'image de x dans $\overline{\mathbf{F}}_p$, on a $\omega(x) = [\overline{x}]$.

Proposition 4.3. — *Les applications*

$$x \to p^{v_p(x)}, \quad x \to \tilde{\omega}(x) = \omega(xp^{-v_p(x)}) \quad \text{et} \quad x \to \langle x\rangle = xp^{-v_p(x)}\tilde{\omega}(x)^{-1}$$

sont des morphismes de groupes de $\mathbf{C}_p^*$ dans, respectivement, $p^{\mathbf{Q}}$, le groupe des racines de l'unité d'ordre premier à p et $D(1, 0^+)$, et on a $x = p^{v_p(x)}\tilde{\omega}(x)\langle x\rangle$.

Démonstration. — évident.

4.2. Rudiments d'analyse p-adique

4.2.1. La fonction logarithme

Lemme 4.4. — *Si $v_p(x) > 0$, la série $\log(1+x) = -\sum_{n=1}^{+\infty} \frac{(-x)^n}{n}$ converge dans $\mathbf{C}_p$. De plus, si $v_p(x) > 0$ et $v_p(y) > 0$, alors $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$*

Démonstration. — On a $v_p(\frac{(-x)^n}{n}) = nv_p(x) - v_p(n) \geqslant nv_p(x) - \frac{\log n}{\log p}$, et donc $v_p(\frac{(-x)^n}{n})$ tend vers $+\infty$ quand n tend vers $+\infty$ si $v_p(x) > 0$. Ceci démontre la convergence de $\log(1+x)$ si $v_p(x) > 0$.

Maintenant, on a $\log((1+X)(1+Y)) = \log(1+X) + \log(1+Y)$ en tant que série formelle en X, Y (il suffit de dériver). Un développement brutal de $\log(1 + (X + Y + XY))$ montre que les deux séries ci-dessus sont aussi égales à

$$\sum_{i_1+i_2+i_3 \geqslant 1} \frac{(-1)^{i_1+i_2+i_3}(i_1+i_2+i_3)!}{(i_1+i_2+i_3)i_1!i_2!i_3!} X^{i_1+i_3}Y^{i_2+i_3}.$$

Maintenant, la série triple $\sum_{i_1+i_2+i_3 \geqslant 1} \frac{(-1)^{i_1+i_2+i_3}(i_1+i_2+i_3)!}{(i_1+i_2+i_3)i_1!i_2!i_3!} x^{i_1+i_3}y^{i_2+i_3}$ converge car le terme général tend vers 0 quand $i_1+i_2+i_3$ tend vers $+\infty$ et on peut réordonner les termes comme on veut, ce qui permet de conclure.

Remarque 4.5. — Si ζ est une racine de l'unité d'ordre une puissance de p, alors $v_p(\zeta-1)>0$ d'après l'exercice ci-dessus. On peut donc calculer $\log\zeta$ par la formule ci-dessus. Par ailleurs, on a $\log(1+x)^n = n\log(1+x)$ si $n\in\mathbf{N}$ et $x\in D(0,0^+)$. En prenant pour n une puissance de p suffisamment grande, on en déduit que $\log\zeta=0$ si ζ est une racine de l'unité d'ordre une puissance de p, ce qui est une des manifestations de la non existence de $2i\pi$ dans $\mathbf{C}_p$.

Lemme 4.6. — *Si $x\in D(1,0^+)$ vérifie $\log x=0$, alors x est une racine de l'unité d'ordre une puissance de p.*

Démonstration. — On a « $\log x=0$ »⇔« $x=1$ » si $v_p(x-1)>\frac{1}{p-1}$ car alors le seul terme de valuation maximale dans $\sum_{n=1}^{+\infty}\frac{(1-x)^n}{n}$ est le premier, et $v_p(\log x)=v_p(x-1)$.

Maintenant, on a $x^p-1=(x-1)^p+p(x-1)\sum_{i=1}^{p-1}p^{-1}\binom{p}{i}(x-1)^{i-1}$. On en déduit la minoration $v_p(x^p-1)\geqslant\inf(1+v_p(x-1),pv_p(x-1))$, ce qui permet de prouver que $v_p(x^{p^n}-1)>\frac{1}{p-1}$ si n est assez grand et $x\in D(1,0^+)$. Comme « $\log x=0$ »⇔« $\log x^{p^n}=0$ », cela permet de conclure.

Proposition 4.7. — *Si $\mathscr{L}\in\mathbf{C}_p$, La fonction* log *a un unique prolongement noté $\log_{\mathscr{L}}$ à $\mathbf{C}_p^*$ vérifiant les trois conditions suivantes.*

(i) $\log_{\mathscr{L}}(xy)=\log_{\mathscr{L}}(x)+\log_{\mathscr{L}}(y)$;

(ii) $\log_{\mathscr{L}}(x)=-\sum_{n=1}^{+\infty}\frac{(1-x)^n}{n}$, *si* $x\in D(1,0^+)$;

(iii) $\log_{\mathscr{L}}p=\mathscr{L}$.

Démonstration. — On a vu que si l'on se fixe un morphisme $r\to p^r$ de $\mathbf{Q}$ dans $\mathbf{C}_p^*$, on pouvait écrire tout élément de $\mathbf{C}_p^*$ de manière unique sous la forme $p^{v_p(x)}\omega u$, où ω est une racine de l'unité d'ordre premier à p et $u\in D(1,0^+)$; on doit donc avoir $\log_{\mathscr{L}}x=\log u+\mathscr{L}v_p(x)$, ce qui prouve l'unicité. L'existence résulte du fait que $x\mapsto u$ et $x\mapsto v_p(x)$ sont des morphismes de groupes.

Remarque 4.8. — Le choix de $\mathscr{L}$ revient à *fixer une branche du logarithme*. D'un point de vue arithmétique, imposer $\log p=0$ est naturel ; on obtient alors *le logarithme d'Iwasawa*.

4.2.2. La fonction exponentielle

Notons $[x]$ la partie entière de x si $x\in\mathbf{R}$ (ne pas confondre avec un représentant de Teichmüller !).

Proposition 4.9. — *Si $n\in\mathbf{N}$, alors*

$$v_p(n!)=\sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right]=\frac{n-S_p(n)}{p-1},$$

où $S_p(n)$ désigne la somme des chiffres de l'écriture de n en base p.

Démonstration. — Soit a_k (resp. b_k) le cardinal de l'ensemble des entiers i vérifiant $1\leqslant i\leqslant n$ et $v_p(i)=k$ (resp. $v_p(i)\geqslant k$). On a $b_k=\sum_{\ell\geqslant k}a_\ell$ et

$$v_p(n!)=\sum_{k=1}^{+\infty}ka_k=\sum_{k=1}^{+\infty}b_k=\sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right],$$

ce qui nous fournit la première égalité. La seconde est laissée en exercice.

Proposition 4.10. — *La série* $\exp x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$ *converge si et seulement si* $v_p(x) > \frac{1}{p-1}$, *et induit un isomorphisme de groupes de la boule ouverte* $D(0, (\frac{1}{p-1})^+)$ *munie de l'addition sur la boule ouverte* $D(1, (\frac{1}{p-1})^+)$ *munie de la multiplication, inverse de l'application* log.

Démonstration. — La détermination du rayon de convergence vient de ce qu'il y a une infinité de n tels que $S_p(n) = 1$ (à savoir, les puissances de p). Le reste de la proposition est laissé en exercice.

Soit π une solution de l'équation $\pi^{p-1} = -p$ (c'est le π de Dwork). Le but de l'exercice ci-dessous est de démontrer le résultat suivant, dû à Dwork, qui en a tiré des merveilles.

Proposition 4.11. — (i) *La série formelle* $E_\pi(X) = \exp(\pi(X - X^p))$ *appartient à* $1 + \pi X + \pi^2 X^2 \mathscr{O}_{\mathbf{C}_p}[[X]]$, *et il existe* $r < 0$ *tel que la série formelle* $E_\pi(X) = \exp(\pi(X - X^p))$ *converge sur* $D(0, r)$.

(ii) *Si* $\omega : \mathbf{F}_p \to \mathbf{Z}_p$ *désigne l'application « représentant de Teichmüller », alors* $x \mapsto E_\pi(\omega(x))$ *est un isomorphisme de groupes de* $\mathbf{F}_p$ *sur* $\boldsymbol{\mu}_p$.

Remarque 4.12. — Ce résultat est un petit peu surprenant car, $\omega(x) - \omega(x)^p$ étant nul, on a l'impression que l'on devrait avoir $E_\pi(\omega(x)) = 1$ quel que soit $x \in \mathbf{F}_p$. Le point est que la série $\exp(\pi x)$ ne converge pas si $v_p(x) = 0$.

Exercice 9. — Soit $\mu : \mathbf{N} - \{0\} \mapsto \{-1, 0, 1\}$ la fonction de Moebius. Par définition, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, et $\mu(n) = (-1)^r$ si $n = p_1 \cdots p_r$, avec $p_1, \dots, p_r$ premiers distincts.

(i) Montrer que

$$\sum_{n|m} \mu(n) = \begin{cases} 1 & \text{si } m = 1, \\ 0 & \text{sinon,} \end{cases} \quad \text{et} \quad \sum_{\substack{n|m \\ (n,p)=1}} \mu(n) = \begin{cases} 1 & \text{si } m \text{ est une puissance de } p, \\ 0 & \text{sinon.} \end{cases}$$

(ii) Soit $\exp_{\mathrm{AH}}(X) = \exp(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots)$ (exponentielle d'Artin-Hasse). Déduire du (i) l'identité

$$\exp_{\mathrm{AH}}(X) = \prod_{(n,p)=1} (1 - X^n)^{-\frac{\mu(n)}{n}},$$

ainsi que l'appartenance de $\exp_{\mathrm{AH}}(X)$ à $\mathbf{Z}_p[[X]]$.

(iii) Montrer que $E_\pi(X) = \exp_{\mathrm{AH}}(\pi X) \prod_{k=2}^{+\infty} \exp - \big(\frac{(\pi X)^{p^k}}{p^k}\big)$. En déduire le (i) de la proposition 4.11.

(iv) Montrer que $E_\pi(y)^p = \frac{\exp(p\pi y)}{\exp(p\pi y^p)}$ quel que soit $y \in D(0, r)$. En déduire que $E_\pi(\omega(x)) \in \boldsymbol{\mu}_p$ si $x \in \mathbf{F}_p$.

(v) En utilisant le fait que $v_p(\zeta - 1) = v_p(\pi)$ si $\zeta \in \boldsymbol{\mu}_p - \{1\}$, démontrer le (ii) de la proposition 4.11.
