Nombres p-Adiques

Cours de Laurent Berger
Notes de Alexis Marchand

ENS de Lyon
S2 2017-2018
Niveau L3

Table des matières

1 Valuation p-adique, écriture en base p, et congruences

1.1 Définitions

Notation 1.1.1. *Dans tout le cours, p est un nombre premier fixé.*

Définition 1.1.2 (Valuation p-adique)**.** *Pour tout $a \in \mathbb{Z}\backslash\{0\}$, il existe un unique $n \in \mathbb{N}$ et un unique $a_0 \in \mathbb{Z}$ avec $p \nmid a_0$ t.q. $a = p^n a_0$. L'entier n est appelé* valuation p-adique *de a est noté $v_p(a)$. On adopte de plus la convention $v_p(0) = +\infty$.*

Proposition 1.1.3. *Soit $(a, b) \in \mathbb{Z}^2$.*

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) $v_p(a + b) \geqslant \min(v_p(a), v_p(b))$.

Définition 1.1.4 (Écriture en base p)**.** *Soit $a \in \mathbb{N}$. Il existe $k \in \mathbb{N}$ et $(a_i)_{0\leqslant i\leqslant k} \in \{0, \dots, p-1\}^{k+1}$ t.q. $a = \sum_{i=0}^{k} a_i p^i$. Les $(a_i)_{0\leqslant i\leqslant k}$ sont uniquement déterminés pour un k donné ; ils sont appelés les* chiffres *de a en base p. On note alors :*

$$a = (a_k \cdots a_0)_p .$$

1.2 Valuations p-adiques des factorielles et des coefficients binomiaux

Notation 1.2.1. *Soit $a \in \mathbb{N}$, qu'on écrit en base p : $a = (a_k \cdots a_0)_p$. On pose :*

$$s_p(a) = \sum_{i=0}^{k} a_i.$$

Proposition 1.2.2. *Pour $n \in \mathbb{N}^*$, on a :*

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Démonstration. Utiliser le fait que $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ puis écrire n en base p. Alternativement, on peut raisonner par récurrence sur n. □

Proposition 1.2.3. *Pour tout $k \in \{1, \dots, p-1\}$, $\binom{p}{k}$ est divisible par p.*

Proposition 1.2.4. *Pour $(a, b) \in \mathbb{N}^2$, $v_p\left(\binom{a+b}{a}\right)$ est le nombre de retenues effectuées lors de l'addition de a et b.*

Proposition 1.2.5. *Soit $(m, n, k) \in \mathbb{N}^3$. Alors :*

$$\binom{m+n}{k} = \sum_{i+j=k} \binom{m}{i}\binom{n}{j}.$$

Démonstration. Écrire $(1+X)^{m+n} = (1+X)^m (1+X)^n$, développer les deux membres de l'égalité et comparer les coefficients de X^k. □

Proposition 1.2.6. *Soit $(m, n) \in \mathbb{N}^2$, qu'on écrit en base p : $m = (m_k \cdots m_0)_p$ et $n = (n_k \cdots n_0)_p$. Alors :*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod p.$$

Démonstration. Noter d'abord que selon la proposition 1.2.3, on a $(1+X)^p \equiv 1 + X^p \mod p$. On en déduit que $(1+X)^{p^2} = ((1+X)^p)^p \equiv 1 + X^{p^2} \mod p$, puis par récurrence :

$$\forall i \in \mathbb{N},\ (1+X)^{p^i} \equiv 1 + X^{p^i} \mod p.$$

On écrit alors $m = \sum_{i=0}^{k} m_i p^i$, d'où $(1+X)^m = \prod_{i=0}^{k} (1+X)^{m_i p^i} \equiv \prod_{i=0}^{k} \left(1 + X^{p^i}\right)^{m_i} \mod p$. Or, dans ce produit, l'unique manière d'obtenir X^n est sous la forme $X^n = X^{n_0} \cdots X^{n_k}$. Le coefficient de X^n est donc $\binom{m_0}{n_0} \cdots \binom{m_k}{n_k}$. Le résultat suit. □

1.3 Le corps $\mathbb{F}_p$ et les anneaux $\mathbb{Z}/p^n\mathbb{Z}$

Proposition 1.3.1. *Pour tout $n \geqslant 1$, $\mathbb{Z}/p^n\mathbb{Z}$ est un anneau. Pour $n = 1$, $\mathbb{Z}/p\mathbb{Z}$ est un corps que l'on note $\mathbb{F}_p$.*

Proposition 1.3.2. *Soit $n \geqslant 1$. Les inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ sont les classes des entiers premiers avec p. Ainsi :*

$$\left|(\mathbb{Z}/p^n\mathbb{Z})^\times\right| = p^{n-1}(p-1).$$

Proposition 1.3.3. *Soit $(x, y) \in \mathbb{Z}^2$. Pour $n \geqslant 1$, on a :*

$$x \equiv y \mod p^n \Longrightarrow x^p \equiv y^p \mod p^{n+1}.$$

Démonstration. Écrire $x = y + p^n z$, avec $z \in \mathbb{Z}$, puis développer $x^p = (y + p^n z)^p$. □

Proposition 1.3.4. *Soit $y \in \mathbb{Z}$. On suppose que $p \neq 2$. Alors pour $n \geqslant 1$:*

$$(1 + p^n y)^p \equiv 1 + p^{n+1} y \mod p^{n+2}.$$

Lemme 1.3.5. *Soit K un corps. Alors tout sous-groupe fini de $(K^\times, \times)$ est cyclique.*

Démonstration. Soit G un sous-groupe fini de $K^\times$ de cardinal N. Pour $n \in \mathbb{N}^*$, on note $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ l'indicatrice d'Euler de n ; c'est le nombre d'éléments d'ordre n de $(\mathbb{Z}/n\mathbb{Z}, +)$. On note de plus $\psi(n)$ le nombre d'éléments d'ordre n de $(G, \times)$. On veut prouver que $\psi(N) \neq 0$. Soit $n \in \mathbb{N}^*$ t.q. $\psi(n) \neq 0$ (cela implique $n \mid N$). Il existe donc $x \in G$ d'ordre n. Considérons :

$$\vartheta_x : \left| \begin{array}{c} \mathbb{Z}/n\mathbb{Z} \longrightarrow G \\ a \longmapsto x^a \end{array} \right. .$$

Alors ϑ_x est un morphisme injectif de groupes. De plus, $\operatorname{Im} \vartheta_x$ est inclus dans l'ensemble des racines de $(X^n - 1)$ dans K. Comme cet ensemble est de cardinal au plus n, $\operatorname{Im} \vartheta_x$ est exactement l'ensemble des racines de $(X^n - 1)$ dans K. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au sous-groupe de G constitué des éléments d'ordre divisant n. Ceci prouve que, si $\psi(n) \neq 0$, alors $\psi(d) = \varphi(d)$ pour tout $d \mid n$. En particulier, pour tout $n \mid N$, $\psi(n) \in \{0, \varphi(n)\}$. Ainsi :

$$N = \sum_{n|N} \psi(n) \leqslant \sum_{n|N} \varphi(n) = N.$$

On a égalité, donc pour tout $n \mid N$, $\psi(n) = \varphi(n)$. En particulier, $\psi(N) = \varphi(N) \neq 0$. □

Théorème 1.3.6.

(i) *Le groupe $\left(\mathbb{F}_p^\times, \times\right)$ est cyclique.*

(ii) *On suppose que $p \neq 2$. Alors pour tout $n \geqslant 1$, le groupe $\left((\mathbb{Z}/p^n\mathbb{Z})^\times, \times\right)$ est cyclique.*

Démonstration. (i) C'est un corollaire du lemme 1.3.5. (ii) Le résultat est déjà prouvé pour $n = 1$. *Étape 1* : $n = 2$. Notons que $(\mathbb{Z}/p^2\mathbb{Z})^\times$ est un groupe de cardinal $p(p-1)$. Et on a un morphisme surjectif de groupes :

$$s : \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times \to (\mathbb{Z}/p\mathbb{Z})^\times .$$

Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, soit $x \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ t.q. $s(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors le groupe $\langle x \rangle$ engendré par x a une image de cardinal $(p-1)$, donc $|\langle x \rangle|$ est multiple de $(p-1)$. De plus, $|\langle x \rangle|$ divise $p(p-1)$, donc $|\langle x \rangle| \in \{(p-1), p(p-1)\}$. Si $|\langle x \rangle| = p(p-1)$, alors $\langle x \rangle = (\mathbb{Z}/p^2\mathbb{Z})^\times$ et on a terminé. Sinon, on a $x^{p-1} = 1$. On considère $y = x(1+p)$. Alors $s(y)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ et $y^{p-1} \not\equiv 1 \mod p^2$. Ainsi, $\langle y \rangle = (\mathbb{Z}/p^2\mathbb{Z})^\times$. *Étape 2* : $n \geqslant 3$. On a un morphisme surjectif de groupes :

$$s : (\mathbb{Z}/p^n\mathbb{Z})^\times \to \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times .$$

Comme $(\mathbb{Z}/p^2\mathbb{Z})^\times$ est cyclique, soit $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ t.q. $s(x)$ engendre $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Ainsi, $|\langle x\rangle|$ divise $p^{n-1}(p-1)$ et est multiple de $p(p-1)$. De plus, il existe $y \not\equiv 0 \mod p$ t.q.

$$x^{p-1} \equiv 1 + py \mod p^2.$$

On a donc, selon la proposition 1.3.3, $x^{p(p-1)} \equiv (1+py)^p \mod p^3$ puis, selon la proposition 1.3.4 (car $p \neq 2$), $x^{p(p-1)} \equiv 1+p^2y \mod p^3$. Par récurrence, il vient $x^{p^{n-2}(p-1)} \equiv 1+p^{n-1}y \not\equiv 1 \mod p^n$. Ainsi, $|\langle x\rangle| = p^{n-1}(p-1)$, d'où $\langle x\rangle = (\mathbb{Z}/p^n\mathbb{Z})^\times$. □

Remarque 1.3.7. *Le point* (ii) *du théorème 1.3.6 est faux si $p = 2$. On peut en fait montrer que, pour $n \geqslant 2$:*

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/2^{n-2}\mathbb{Z}\right).$$

2 Complétion de $\mathbb{Q}$, construction de $\mathbb{Q}_p$ et $\mathbb{Z}_p$

2.1 Distance p-adique

Définition 2.1.1 (Valuation p-adique des rationnels)**.** *Pour tout $a \in \mathbb{Q}\backslash\{0\}$, il existe $n \in \mathbb{Z}$, $(c,d) \in \mathbb{Z} \times \mathbb{N}^*$ t.q. $p \nmid c$, $p \nmid d$ et $a = p^n \frac{c}{d}$. L'entier n est uniquement déterminé ; il est appelé* valuation p-adique *de a est noté $v_p(a)$.*

Proposition 2.1.2. *Soit $(a,b) \in \mathbb{Q}^2$.*

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$.

Définition 2.1.3 (Distance p-adique)**.**

(i) *On définit $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ en posant :*

$$\forall a \in \mathbb{Q},\ |a|_p = p^{-v_p(a)}.$$

(ii) *On définit $d_p : \mathbb{Q}^2 \to \mathbb{R}_+$ en posant :*

$$\forall (a,b) \in \mathbb{Q}^2,\ d_p(a,b) = |a-b|_p.$$

Définition 2.1.4 (Distance ultramétrique)**.** *Une distance d sur un ensemble X est dite* ultramétrique *lorsque :*

$$\forall (a,b,c) \in X^3,\ d(a,b) \leqslant \max(d(a,c), d(c,b)).$$

Cette propriété est plus forte que l'inégalité triangulaire.

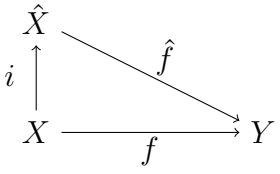
Proposition 2.1.5. *Soit (X,d) un espace ultramétrique. Alors :*

$$\forall (a,b,c) \in X^3,\ d(a,c) \neq d(c,b) \Longrightarrow d(a,b) = \max(d(a,c), d(c,b)).$$

Proposition 2.1.6. *d_p est une distance ultramétrique sur $\mathbb{Q}$.*

2.2 Complétion d'un espace métrique

Théorème 2.2.1. *Si (X,d) est un espace métrique, alors il existe un espace métrique complet $\left(\hat{X}, \hat{d}\right)$ et une isométrie $i : X \to \hat{X}$ d'image dense. L'espace $\left(\hat{X}, \hat{d}\right)$ est unique à isométrie bijective près. De plus, il vérifie la propriété universelle suivante : si Y est un espace métrique complet et si $f : X \to Y$ est une application uniformément continue, alors il existe une application uniformément continue $\hat{f} : \hat{X} \to Y$ faisant commuter le diagramme suivant :*



Comme $\left(\hat{X}, \hat{d}\right)$ est unique à isométrie bijective près, on l'appelle le complété *de (X,d).*

2.3 L'espace $\mathbb{Q}_p$

Définition 2.3.1 ($\mathbb{Q}_p$)**.** *On note $(\mathbb{Q}_p, d_p)$ le complété de $(\mathbb{Q}, d_p)$. C'est un espace métrique complet et $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$. On définit $+$ et $\times$ comme suit :*

(i) *Si $(a,b) \in \mathbb{Q}_p^2$, il existe $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ t.q. $a_n \xrightarrow[n\to+\infty]{} a$ et $b_n \xrightarrow[n\to+\infty]{} b$. Alors la suite $(a_n + b_n)_{n\in\mathbb{N}}$ est de Cauchy et sa limite (qui ne dépend pas du choix de $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$) est notée $a + b$.*

(ii) *Si $(a,b) \in \mathbb{Q}_p^2$, il existe $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ t.q. $a_n \xrightarrow[n\to+\infty]{} a$ et $b_n \xrightarrow[n\to+\infty]{} b$. Alors la suite $(a_n b_n)_{n\in\mathbb{N}}$ est de Cauchy et sa limite (qui ne dépend pas du choix de $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$) est notée ab.*

Ceci définit une structure de corps sur $\mathbb{Q}_p$ qui étend celle de $\mathbb{Q}$. De plus, les opérations $+$, $-$, $\times$ et $\cdot^{-1}$ sont continues.

Proposition 2.3.2. $\forall (x,y) \in \mathbb{Q}_p^2,\ x \neq y \Longrightarrow d_p(x,y) \in p^{\mathbb{Z}} = \{p^n,\ n \in \mathbb{Z}\}$.

Proposition 2.3.3. *La distance d_p est ultramétrique.*

Notation 2.3.4. *Soit (X,d) un espace métrique. Pour $a \in X$ et $r > 0$, on note :*

(i) $B(a,r) = \{x \in X,\ d(x,a) < r\}$,

(ii) $BF(a,r) = \{x \in X,\ d(a,x) \leqslant r\}$.

Corollaire 2.3.5.

(i) *Tout triangle dans $\mathbb{Q}_p$ est isocèle.*

(ii) *Soit $a \in \mathbb{Q}_p$ et $r > 0$. Alors :*

$$\forall x \in B(a,r),\ B(a,r) = B(x,r).$$

(iii) *Soit $a \in \mathbb{Q}_p$ et $r > 0$. Alors :*

$$\operatorname{diam} B(a,r) \leqslant r.$$

(iv) *Soit $(a,b) \in \mathbb{Q}_p^2$ et $r,s > 0$. Si $B(a,r) \cap B(b,s) \neq \varnothing$, alors $B(a,r) \subset B(b,s)$ ou $B(a,r) \supset B(b,s)$.*

(v) *Soit $a \in \mathbb{Q}_p$ et $r > 0$. Alors $B(a,r)$ est ouverte et fermée.*

(vi) *Une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}_p^{\mathbb{N}}$ est de Cauchy* ssi $d_p(a_n, a_{n+1}) \xrightarrow[n\to+\infty]{} 0$.

(vii) *Une série $\sum a_n$ converge* ssi $a_n \xrightarrow[n\to+\infty]{} 0$.

Proposition 2.3.6. *La fonction $v_p : \mathbb{Q} \to \mathbb{Z}$ se prolonge en une fonction $v_p : \mathbb{Q}_p \to \mathbb{Z}$, par exemple en posant :*

$$\forall x \in \mathbb{Q}_p^\times,\ v_p(x) = -\log_p |x|_p .$$

Ainsi, v_p a les propriétés suivantes :

(i) *v_p est continue sur $\mathbb{Q}_p$.*

(ii) *v_p est localement constante sur $\mathbb{Q}_p^\times$.*

(iii) $\forall (x,y) \in \mathbb{Q}_p^2,\ v_p(xy) = v_p(x) + v_p(y)$.

(iv) $\forall (x,y) \in \mathbb{Q}_p^2,\ v_p(x+y) \geqslant \min(v_p(x), v_p(y))$.

(v) *Si une suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}_p^{\mathbb{N}}$ converge vers $a \in \mathbb{Q}_p$, alors $(v_p(a_n))_{n\in\mathbb{N}}$ stationne en $v_p(a)$.*

2.4 L'espace $\mathbb{Z}_p$

Définition 2.4.1 ($\mathbb{Z}_p$). *On note $\mathbb{Z}_p$ le complété de $\mathbb{Z}$ pour d_p ; autrement dit, $\mathbb{Z}_p$ est l'adhérence de $\mathbb{Z}$ en tant que partie de $\mathbb{Q}_p$. Ainsi, $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}_p$.*

Proposition 2.4.2. $\mathbb{Z}_p = BF(0,1) = \{x \in \mathbb{Q}_p,\ v_p(x) \geqslant 0\}$.

Démonstration. ($\subset$) On a $\mathbb{Z} \subset BF(0,1)$, et $BF(0,1)$ est un fermé de $\mathbb{Q}_p$, donc $\mathbb{Z}_p = \overline{\mathbb{Z}} \subset BF(0,1)$. ($\supset$) Soit $a \in BF(0,1)$. On peut supposer que $a \neq 0$. Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ t.q. $a_n \xrightarrow[n\to+\infty]{} a$. Quitte à extraire, on peut supposer que $\forall n \in \mathbb{N},\ d_p(a, a_n) \leqslant p^{-n}$. Ainsi :

$$\forall n \in \mathbb{N},\ v_p(a_n) \geqslant \min\left(v_p(a), v_p(a_n - a)\right) \geqslant 0.$$

Pour $n \in \mathbb{N}$, on peut donc écrire $a_n = \frac{c_n}{d_n}$, avec $(c_n, d_n) \in \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ et $p \nmid d_n$. Comme $p \nmid d_n$, il existe $e_n \in \mathbb{Z}$ t.q. $e_n d_n \equiv 1 \mod p^n$. Ainsi :

$$\begin{aligned}\forall n \in \mathbb{N},\ v_p(a_n - c_n e_n) &= v_p(d_n) + v_p(a_n - c_n e_n) = v_p(c_n) + v_p(1 - e_n d_n)\\ &= v_p(a_n) + v_p(1 - e_n d_n) \geqslant n.\end{aligned}$$

Donc $a_n - c_n e_n \xrightarrow[n\to+\infty]{} 0$, d'où $a = \lim_{n\to+\infty} a_n = \lim_{n\to+\infty} c_n e_n \in \overline{\mathbb{Z}} = \mathbb{Z}_p$. □

Proposition 2.4.3. *$\mathbb{Z}_p$ est compact.*

Démonstration. Comme $\mathbb{Z}_p$ est complet, il suffit de montrer que $\mathbb{Z}_p$ est précompact (i.e. pour tout $\varepsilon > 0$, $\mathbb{Z}_p$ peut être recouvert par un nombre fini de boules de rayon ε). Soit donc $\varepsilon > 0$. Soit $n \in \mathbb{N}^*$ t.q. $p^{-n} < \varepsilon$. Pour $a \in \mathbb{Z}_p$, il existe $b \in \mathbb{Z}$ t.q. $d_p(a,b) \leqslant p^{-n}$. On se donne $b' \in \{0, 1, \ldots, p^n - 1\}$ t.q. $b \equiv b' \mod p^n$. Ainsi, $d(a, b') \leqslant p^{-n}$, donc $a \in BF(b', p^{-n})$. On a prouvé que :

$$\mathbb{Z}_p \subset \bigcup_{b'\in\{0,1,\ldots,p^n-1\}} BF\left(b', p^{-n}\right) \subset \bigcup_{b'\in\{0,1,\ldots,p^n-1\}} B(b', \varepsilon).$$

Donc $\mathbb{Z}_p$ est précompact complet, donc compact. □

Remarque 2.4.4. *Pour $n \in \mathbb{N}^*$, on a prouvé que $\mathbb{Z}_p = \bigcup_{b\in\{0,1,\ldots,p^n-1\}} BF(b, p^{-n})$. Comme les boules $(BF(b, p^{-n}))_{0\leqslant b\leqslant p^n-1}$ sont à la fois ouvertes et fermées, on en déduit que $\mathbb{Z}_p$ est homéomorphe à l'espace de Cantor $\{0,1\}^{\mathbb{N}}$.*

Proposition 2.4.5. *On a :*

$$\mathbb{Q}_p = \bigcup_{n\in\mathbb{N}} p^{-n}\mathbb{Z}_p.$$

2.5 Propriétés algébriques de $\mathbb{Z}_p$

Proposition 2.5.1. *$\mathbb{Z}_p$ est un sous-anneau du corps $\mathbb{Q}_p$.*

Proposition 2.5.2. $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p,\ v_p(a) = 0\}$.

Proposition 2.5.3. *Le groupe additif $\mathbb{Z}_p$ est* topologiquement cyclique *: c'est l'adhérence du groupe cyclique $\mathbb{Z}$.*

Proposition 2.5.4. *Les sous-groupes fermés non triviaux du groupe additif $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$ pour $n \in \mathbb{N}$.*

Démonstration. Soit G un sous-groupe fermé non trivial de $\mathbb{Z}_p$. Soit $a \in G$ t.q. $v_p(a) = \min_{b\in G} v_p(b)$. On note $n = v_p(a)$. On a $G \subset p^n\mathbb{Z}_p$ (car $\forall b \in G,\ v_p(p^{-n}b) = v_p(b) - n \geqslant 0$ donc $p^{-n}b \in \mathbb{Z}_p$). Notons de plus que l'adhérence de $a\mathbb{Z}$ dans $\mathbb{Z}_p$ est $a\mathbb{Z}_p$. Or G est fermé et $a\mathbb{Z} \subset G$ (car $a \in G$), donc $a\mathbb{Z}_p \subset G$. Mais si $a_0 = p^{-n}a$, alors $v_p(a_0) = 0$, donc $a_0 \in \mathbb{Z}_p^\times$. Donc $p^n\mathbb{Z}_p = aa_0^{-1}\mathbb{Z}_p = a\mathbb{Z}_p \subset G$, d'où $G = p^n\mathbb{Z}_p$. □

Proposition 2.5.5. *Les idéaux non triviaux de l'anneau $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$ pour $n \in \mathbb{N}$.*

2.6 Écriture en base p

Définition 2.6.1 (Réduction modulo p^n)**.** *Soit $n \in \mathbb{N}^*$. Alors pour tout $a \in \mathbb{Z}_p$, il existe $a_1 \in \mathbb{Z}$ t.q. $|a - a_1|_p \leqslant p^{-n}$, autrement dit il existe $b \in \mathbb{Z}_p$ t.q. $a = a_1 + p^n b$. Ainsi, la classe de a_1 dans $\mathbb{Z}/p^n\mathbb{Z}$ ne dépend que de a et on la note $\overline{a}$. On définit donc un morphisme d'anneaux :*

$$\left| \begin{array}{l} \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ a \longmapsto \overline{a} \end{array} \right. .$$

On notera parfois $a \mod p^n$ plutôt que $\overline{a}$.

Proposition 2.6.2. *Soit $n \in \mathbb{N}^*$. Alors $\overline{a} = 0$ dans $\mathbb{Z}/p^n\mathbb{Z}$* ssi *$a \in p^n\mathbb{Z}_p$.*

Corollaire 2.6.3. *Pour $n \in \mathbb{N}^*$, on a :*

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Théorème 2.6.4. *Pour tout $a \in \mathbb{Z}_p$, il existe une unique suite $(a_n)_{n\in\mathbb{N}} \in \{0, 1, \ldots, p-1\}^{\mathbb{N}}$ t.q. $a = \sum_{n=0}^{\infty} a_n p^n$. Cette suite est appelée* écriture en base p *de a ; on note :*

$$a = (\cdots a_n \cdots a_2 a_1 a_0)_p .$$

Démonstration. *Unicité.* Soit $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \{0, 1, \ldots, p-1\}^{\mathbb{N}}$ t.q. $(a_n)_{n\in\mathbb{N}} \neq (b_n)_{n\in\mathbb{N}}$. Si $n_0 = \min\{n \in \mathbb{N},\ a_n \neq b_n\}$, alors :

$$v_p\left(\sum_{n=0}^{\infty} a_n p^n - \sum_{n\in\mathbb{N}} b_n p^n\right) = n_0 < +\infty,$$

d'où $\sum_{n=0}^{\infty} a_n p^n \neq \sum_{n=0}^{\infty} b_n p^n$. *Existence.* On définit $(s_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ et $(a_n)_{n\in\mathbb{N}} \in \{0, 1, \ldots, p-1\}^{\mathbb{N}}$ par récurrence en posant $s_0 = a$, puis après avoir construit $s_0, a_0, \ldots, s_{n-1}, a_{n-1}, s_n$, on pose a_n l'unique élément de $\{0, 1, \ldots, p-1\}$ t.q. $\overline{s_n} = \overline{a_n}$ et $s_{n+1} = \frac{1}{p}(s_n - a_n)$. On a alors :

$$\forall n \in \mathbb{N},\ a = a_0 + pa_1 + \cdots + p^n a_n + p^{n+1} s_{n+1}.$$

Ainsi, $a = \sum_{n=0}^{\infty} a_n p^n$. □

2.7 Une autre réalisation algébrique de $\mathbb{Z}_p$

Proposition 2.7.1. *On considère :*

$$\mathfrak{B} = \left\{ (b_n)_{n\in\mathbb{N}^*} \in \prod_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z},\ \forall n \in \mathbb{N}^*,\ b_{n+1} \equiv b_n \mod p^n \right\}.$$

On munit $\prod_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$ de la topologie produit, ce qui en fait un espace compact selon le théorème de Tykhonov, et on munit $\mathfrak{B}$ de la topologie induite. On considère l'application :

$$\left| \begin{array}{l} \mathbb{Z}_p \longrightarrow \mathfrak{B} \\ b \longmapsto (b \mod p^n)_{n\in\mathbb{N}^*} \end{array} \right. .$$

Alors cette application est un homéomorphisme et un isomorphisme d'anneaux.

Démonstration. *Surjectivité.* Soit $(b_n)_{n\in\mathbb{N}^*} \in \mathfrak{B}$. Pour $n \in \mathbb{N}^*$, il existe $\hat{b}_n \in \mathbb{Z}_p$ qui relève b_n modulo p^n. La suite $\left(\hat{b}_n\right)_{n\in\mathbb{N}^*}$ est alors de Cauchy, donc converge vers $b \in \mathbb{Z}_p$. Et on vérifie que $\forall n \in \mathbb{N}^*$, $b_n \equiv b \mod p^n$. □

Proposition 2.7.2. *Soit $Q \in \mathbb{Z}[X_1, \ldots, X_d]$. S'équivalent :*

(i) *Q a une racine dans $\mathbb{Z}_p^d$.*

(ii) *$\forall n \in \mathbb{N}^*$, Q a une racine dans $(\mathbb{Z}/p^n\mathbb{Z})^d$.*

Démonstration. (i) $\Rightarrow$ (ii) Clair. (ii) $\Rightarrow$ (i) Pour $n \in \mathbb{N}^*$, soit $\left(\widetilde{x}_1^{(n)}, \ldots, \widetilde{x}_d^{(n)}\right) \in (\mathbb{Z}/p^n\mathbb{Z})^d$ t.q. $Q\left(\widetilde{x}_1^{(n)}, \ldots, \widetilde{x}_d^{(n)}\right) = 0$. Soit $\left(x_1^{(n)}, \ldots, x_d^{(n)}\right) \in \mathbb{Z}_p^d$ relevant $\left(\widetilde{x}_1^{(n)}, \ldots, \widetilde{x}_d^{(n)}\right)$ modulo p^n. Alors la suite $\left(\left(x_1^{(n)}, \ldots, x_d^{(n)}\right)\right)_{n\in\mathbb{N}^*}$ est à valeurs dans le compact $\mathbb{Z}_p^d$, donc admet une sous-suite convergeant vers un $(x_1, \ldots, x_d) \in \mathbb{Z}_p^d$. Et on a $Q(x_1, \ldots, x_d) = 0$. □

3 Lemme de Hensel

3.1 Une version du lemme de Hensel

Remarque 3.1.1. *Si $Q \in \mathbb{Z}_p[X]$ admet une racine dans $\mathbb{Z}_p$ alors pour tout $n \in \mathbb{N}^*$, Q admet une racine dans $\mathbb{Z}/p^n\mathbb{Z}$.*

Notation 3.1.2 (Dérivée de Hasse)**.** *Soit A un anneau commutatif. Pour $Q = \sum_{k=0}^d q_k X^k \in A[X]$ et $i \in \mathbb{N}$, on pose :*

$$Q^{[i]} = \sum_{k=0}^{d-i} \binom{i+k}{i} q_{i+k} X^k \in A[X].$$

On dit que $Q^{[i]}$ est la i-ième dérivée de Hasse *de Q. Dans le cas où $i!$ est inversible dans A, on a :*

$$Q^{[i]} = \frac{Q^{(i)}}{i!}.$$

Proposition 3.1.3. *Soit A un anneau commutatif. Pour $Q = \sum_{k=0}^d q_k X^k \in A[X]$, on a :*

$$Q(X+Y) = \sum_{k=0}^{d} Y^k Q^{[k]}(X).$$

Théorème 3.1.4 (Lemme de Hensel)**.** *Soit $Q \in \mathbb{Z}_p[X]$. On suppose qu'il existe $a_0 \in \mathbb{Z}_p$ t.q.*

$$Q(a_0) \in p\mathbb{Z}_p \qquad \text{et} \qquad Q'(a_0) \in \mathbb{Z}_p^\times.$$

Autrement dit, Q admet une racine simple dans $\mathbb{Z}/p\mathbb{Z}$. Alors il existe un unique $a \in \mathbb{Z}_p$ t.q. $Q(a) = 0$ et $(a - a_0) \in p\mathbb{Z}_p$.

Démonstration. *Existence* : *méthode de Newton.* On pose $\mathfrak{C} = a_0 + p\mathbb{Z}_p = BF(a_0, p^{-1})$. Si $x \in \mathfrak{C}$, il existe un $h \in \mathbb{Z}_p$ t.q. $x = a_0 + ph$. Donc :

$$Q'(x) = Q'(a_0 + ph) = Q'(a_0) + ph \sum_{k=1}^{d} (ph)^{k-1} (Q')^{[k]}(a_0) \in \mathbb{Z}_p^\times,$$

où $d = \deg Q$. Par le même argument, on a $\forall x \in \mathfrak{C}$, $Q(x) \in p\mathbb{Z}_p$. On définit donc à bon droit :

$$\varphi : \left| \begin{array}{l} \mathfrak{C} \longrightarrow \mathfrak{C} \\ x \longmapsto x - \dfrac{Q(x)}{Q'(x)} \end{array} \right. .$$

À partir de a_0, on définit par récurrence une suite $(a_n)_{n\in\mathbb{N}} \in \mathfrak{C}^{\mathbb{N}}$ en posant :

$$\forall n \in \mathbb{N},\ a_{n+1} = \varphi(a_n).$$

On montre par récurrence sur n que $\forall n \in \mathbb{N}$, $Q(a_n) \in p^{2^n}\mathbb{Z}_p$. Ceci prouve d'une part que $(a_n)_{n\in\mathbb{N}}$ est de Cauchy (donc converge vers $a \in \mathfrak{C}$, car $\mathfrak{C}$ est un fermé de l'espace complet $\mathbb{Z}_p$), d'autre part que $Q(a_n) \xrightarrow[n\to+\infty]{} 0$. Ainsi, $Q(a) = 0$. *Unicité.* Si a et a' sont deux racines distinctes de Q dans $a_0 + p\mathbb{Z}_p$, alors $(X-a)(X-a')$ divise Q. En réduisant modulo p, $(X - \overline{a_0})^2$ divise Q dans $\mathbb{Z}/p\mathbb{Z}[X]$, ce qui contredit l'hypothèse $Q'(a_0) \in \mathbb{Z}_p^\times$. □

Exemple 3.1.5. *Le polynôme $X^{p-1}-1$ a $(p-1)$ racines simples dans $\mathbb{Z}/p\mathbb{Z}$. Le lemme de Hensel assure que chacune de ces racines se relève dans $\mathbb{Z}_p$ en une unique racine de $X^{p-1}-1$. Pour tout $a \in \mathbb{Z}_p^\times$, il y a donc dans $\mathbb{Z}_p^\times$ une unique racine $(p-1)$-ième de l'unité qui est congrue à a modulo p ; on la note $\omega(a)$ et on pose $\langle a \rangle = a\omega(a)^{-1} \in 1+p\mathbb{Z}_p$. Ainsi :*

(i) *$\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ est un morphisme de groupes.*

(ii) *$\forall a \in \mathbb{Z}_p^\times$, $a = \omega(a)\langle a \rangle$ avec $\omega(a)^{p-1} = 1$ et $\langle a \rangle \in 1+p\mathbb{Z}_p$.*

(iii) *$\mathbb{Z}_p^\times = \mu_{p-1} \times (1+p\mathbb{Z}_p)$, où μ_{p-1} est l'ensemble des racines $(p-1)$-ièmes de l'unité.*

Exemple 3.1.6. *Supposons $p \neq 2$. Si $c \in \mathbb{Z}$ est un carré non nul modulo p, alors $\sqrt{c} \in \mathbb{Z}_p$.*

3.2 Première généralisation

Lemme 3.2.1. *Soit K un corps, $(P,Q) \in K[X]^2$. On suppose que P et Q sont premiers entre eux. Alors pour tout $R \in K[X]$, il existe $(A,B) \in K[X]^2$ t.q.*

$$R = AP + BQ \qquad \text{et} \qquad \deg A < \deg Q.$$

Démonstration. L'égalité de Bézout fournit l'existence de $\left(\widetilde{A}, \widetilde{B}\right) \in K[X]^2$ t.q. $R = \widetilde{A}P + \widetilde{B}Q$. On a alors $\forall C \in K[X]$, $R = \left(\widetilde{A} - CQ\right)P + \left(\widetilde{B} + CP\right)Q$. En prenant C le quotient de la division euclidienne de $\widetilde{A}$ par Q, le couple $(A,B) = \left(\widetilde{A} - CQ, \widetilde{B} + CP\right)$ convient. □

Proposition 3.2.2. *Soit $F \in \mathbb{Z}_p[X]$. Soit $(G_1, H_1) \in \mathbb{Z}_p[X]^2$ vérifiant :*

(i) *$F \equiv G_1 H_1 \mod p$.*

(ii) *Les réduits modulo p $\overline{G_1}$ et $\overline{H_1}$ sont premiers entre eux dans $\mathbb{Z}/p\mathbb{Z}[X]$.*

(iii) *G_1 est unitaire.*

Alors il existe $(G,H) \in \mathbb{Z}_p[X]^2$ t.q. $F = GH$, G est unitaire, $G \equiv G_1 \mod p$ et $H \equiv H_1 \mod p$.

Démonstration. On note $d = \deg F$ et $m = \deg G_1$. On a $\deg \overline{F} \leqslant d$ et $\deg \overline{G_1} = m$ (car G_1 est unitaire). On peut de plus supposer que $\deg \overline{H_1} = d - m$ quitte à enlever les termes divisibles par p. On va construire deux suites $(Y_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}_p[X]^{\mathbb{N}^*}$ et $(Z_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}_p[X]^{\mathbb{N}^*}$ avec $\forall n \in \mathbb{N}^*$, $\deg Y_n < m$ et $\deg Z_n \leqslant d-m$ t.q. si $G = G_1 + \sum_{n=1}^{\infty} p^n Y_n$ et $H = H_1 + \sum_{n=1}^{\infty} p^n Z_n$, alors $F = GH$. Soit $n \in \mathbb{N}^*$ tel qu'on ait construit $(Y_1, \ldots, Y_{n-1})$ et $(Z_1, \ldots, Z_{n-1})$. On pose :

$$G_n = G_1 + \sum_{k=1}^{n-1} p^k Y_k \qquad \text{et} \qquad H_n = H_1 + \sum_{k=1}^{n-1} p^k Z_k.$$

On suppose que $F \equiv G_n H_n \mod p^n$ (c'est vrai pour $n=1$, et on s'assurera que la propriété est vérifiée au rang $(n+1)$ pour que la récurrence se propage). Il existe alors $F_n \in \mathbb{Z}_p[X]$ t.q. $F = G_n H_n + p^n F_n$. Et on cherche $(Y_n, Z_n) \in \mathbb{Z}_p[X]^2$ t.q.

$$F \equiv (G_n + p^n Y_n)(H_n + p^n Z_n) \equiv F + p^n (Y_n H_n + Z_n G_n - F_n) \mod p^{n+1},$$

i.e. $Y_n H_n + Z_n G_n \equiv F_n \mod p$. On remarque que $G_n \equiv G_1 \mod p$ et $H_n \equiv H_1 \mod p$ donc $\overline{G_n} \wedge \overline{H_n} = 1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On applique donc le lemme 3.2.1 dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour obtenir $(Y_n, Z_n) \in \mathbb{Z}_p[X]^2$ t.q. $Y_n H_n + Z_n G_n \equiv F_n \mod p$, avec $\deg Y_n < m$ (et $\deg Z_n \leqslant d-m$). La récurrence se propage et les polynômes $G = G_1 + \sum_{n=1}^{\infty} p^n Y_n$ et $H = H_1 + \sum_{n=1}^{\infty} p^n Z_n$ conviennent. □

3.3 Seconde généralisation

Proposition 3.3.1. *Soit $Q \in \mathbb{Z}_p[X]$. On suppose qu'il existe $a_0 \in \mathbb{Z}_p$ et $k \in \mathbb{N}^*$ t.q.*

$$Q(a_0) \in p^k Q'(a_0)^2 \mathbb{Z}_p.$$

Alors il existe un unique $a \in \mathbb{Z}_p$ t.q. $Q(a) = 0$ et $(a - a_0) \in p^k Q'(a_0)\mathbb{Z}_p$.

Démonstration. Même démonstration que le théorème 3.1.4 (méthode de Newton). □

4 Fonctions continues sur $\mathbb{Z}_p$

4.1 Espace des fonctions continues sur $\mathbb{Z}_p$

Définition 4.1.1 (Norme de $\mathbb{Q}_p$-espace vectoriel)**.** *Soit V un $\mathbb{Q}_p$-espace vectoriel. On appelle* norme *sur V toute norme ultramétrique $\|\cdot\|$ vérifiant :*

$$\forall \lambda \in \mathbb{Q}_p,\ \forall v \in V,\ \|\lambda v\| = |\lambda|_p \|v\|.$$

Notation 4.1.2. *On munit $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ de la norme $\|\cdot\|_\infty$.*

Proposition 4.1.3. *$(\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p), \|\cdot\|_\infty)$ est un $\mathbb{Q}_p$-espace vectoriel normé complet.*

Proposition 4.1.4. *Les fonctions localement constantes sont denses dans $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.*

Démonstration. Remarquer que :

$$\forall n \in \mathbb{N},\ \mathbb{Z}_p = \bigsqcup_{a \in \{0,\dots,p^n-1\}} BF\left(a, p^{-n}\right).$$

Utiliser cette égalité pour approcher une fonction $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ par des fonctions localement constantes, en utilisant l'uniforme continuité de f (car $\mathbb{Z}_p$ est compact). □

4.2 Coefficients binomiaux, fonctions puissances

Notation 4.2.1. *Pour $k \in \mathbb{N}$, on pose :*

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!} \in \mathbb{Q}_p[X].$$

Proposition 4.2.2. $\forall x \in \mathbb{Z}_p,\ \forall k \in \mathbb{N},\ \binom{x}{k} \in \mathbb{Z}_p$.

Démonstration. On fixe $k \in \mathbb{N}$ et on considère $f : x \in \mathbb{Z}_p \longmapsto \binom{x}{k}$. On a $f(\mathbb{Z}_{\geqslant k}) \subset \mathbb{Z} \subset \mathbb{Z}_p$ et $\mathbb{Z}_{\geqslant k}$ est dense dans $\mathbb{Z}_p$, donc $f(\mathbb{Z}_p) = f\left(\overline{\mathbb{Z}_{\geqslant k}}\right) \subset \overline{f(\mathbb{Z}_{\geqslant k})} \subset \mathbb{Z}_p$. □

Notation 4.2.3. *Pour $a \in \mathbb{Z}_p$ et $z \in p\mathbb{Z}_p$, on note :*

$$(1+z)^a = \sum_{k=0}^{\infty} \binom{a}{k} z^k \in \mathbb{Z}_p.$$

Remarque 4.2.4. *Soit $z \in p\mathbb{Z}_p$. Avec la notation 4.2.3, on a $\forall a \in \mathbb{N},\ (1+z)^a = \underbrace{(1+z)\cdots(1+z)}_{a \text{ fois}}$.*

Lemme 4.2.5. $\forall (x,y) \in \mathbb{Z}_p^2,\ \forall k \in \mathbb{N},\ \binom{x+y}{k} = \sum_{i=0}^{k} \binom{x}{i}\binom{y}{k-i}$.

Proposition 4.2.6. *Soit $z \in p\mathbb{Z}_p$.*

(i) *La fonction $a \in \mathbb{Z}_p \longmapsto (1+z)^a \in \mathbb{Z}_p$ est continue.*

(ii) $\forall (a,b) \in \mathbb{Z}_p^2,\ (1+z)^a(1+z)^b = (1+z)^{a+b}$.

Exemple 4.2.7. *Supposons $p \neq 2$. Alors $\frac{1}{2} \in \mathbb{Z}_p$. Ainsi, pour $z \in p\mathbb{Z}_p$, $(1+z)^{\frac{1}{2}}$ est une racine carrée de $(1+z)$ dans $\mathbb{Z}_p$. D'après le lemme de Hensel (théorème 3.1.4), c'est en fait la seule racine carrée de $(1+z)$ qui est congrue à 1 modulo p. Par exemple, dans $\mathbb{Z}_5$: $16^{\frac{1}{2}} = -4$.*

Proposition 4.2.8. *On suppose que $p \neq 2$. On considère :*

$$\varphi : \left| \begin{array}{l} \mathbb{Z}_p \longrightarrow 1 + p\mathbb{Z}_p \\ a \longmapsto (1+p)^a \end{array} \right. .$$

Alors φ est un isomorphisme de groupes entre $(\mathbb{Z}_p, +)$ et $(1+p\mathbb{Z}_p, \times)$ et c'est aussi un homéomorphisme.

Démonstration. *Morphisme de groupes.* Voir proposition 4.2.6. *Injectivité.* Soit $a \in \mathbb{Z}_p \backslash \{0\}$. Écrivons $a = a_0 p^n$, avec $a_0 \in \mathbb{Z}_p^\times$ et $n = v_p(a)$. Alors :

$$\varphi(a) = (1+p)^a = 1 + a_0 p^{n+1} + \sum_{k=2}^{\infty} \frac{a_0 p^n}{k} \binom{a_0 p^n - 1}{k-1} p^k.$$

Or, comme $p \neq 2$, on a $v_p\left(\frac{p^k}{k}\right) \geqslant 2$ pour tout $k \geqslant 2$. Donc $v_p\left(\sum_{k=2}^{\infty} \frac{a_0 p^n}{k}\binom{a_0 p^n - 1}{k-1} p^k\right) \geqslant n+2 > n+1 = v_p\left(a_0 p^{n+1}\right)$. Ainsi, $v_p\left(\varphi(a) - 1\right) = n+1 < +\infty$ donc $a \notin \operatorname{Ker} \varphi$. *Surjectivité.* On se donne $x \in \mathbb{Z}_p$ et on cherche $a \in \mathbb{Z}_p$ t.q. $(1+p)^a = 1 + px$. Construisons par récurrence deux suites $(a_n)_{n \in \mathbb{N}^*} \in \mathbb{Z}_p^{\mathbb{N}^*}$ et $(y_n)_{n \in \mathbb{N}^*} \in \mathbb{Z}_p^{\mathbb{N}^*}$ t.q.

$$\forall n \in \mathbb{N}^*,\ (1+p)^{a_n} = 1 + px + p^n y_n.$$

On prend $(a_1, y_1) = (0, -x)$. Supposons avoir construit $(a_1, \ldots, a_n)$ et $(y_1, \ldots, y_n)$. On vérifie que si $a_{n+1} = a_n - p^{n-1} y_n$, alors $(1+p)^{a_{n+1}} \equiv 1 + px \mod p^{n+1}$. La récurrence se propage. La suite $(a_n)_{n \in \mathbb{N}^*}$ ainsi construite et alors de Cauchy car $|a_{n+1} - a_n|_p \leqslant p^{-(n-1)} \xrightarrow[n \to +\infty]{} 0$. Et si $a = \lim_{n \to +\infty} a_n$, alors $(1+p)^a = 1 + px$. □

Corollaire 4.2.9. *On suppose que $p \neq 2$. Alors le groupe $1 + p\mathbb{Z}_p$ est topologiquement cyclique (c'est l'adhérence d'un groupe cyclique) et ses sous-groupes fermés non triviaux sont les $1 + p^n \mathbb{Z}_p$ pour $n \geqslant 1$.*

Corollaire 4.2.10. *Si $p \neq 2$, alors :*

$$\mathbb{Z}_p^\times \simeq \mu_{p-1} \times \mathbb{Z}_p,$$

où μ_{p-1} est l'ensemble des racines $(p-1)$-ièmes de l'unité dans $\mathbb{Z}_p$.

Démonstration. Voir exemple 3.1.5. □

Exemple 4.2.11. $1 + 4\mathbb{Z}_2 \simeq \mathbb{Z}_2$.

4.3 Théorème de Mahler

Remarque 4.3.1. *Soit $(a_n)_{n \in \mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ t.q. $a_n \xrightarrow[n \to +\infty]{} 0$. Alors $x \longmapsto \sum_{n=0}^{\infty} \binom{x}{n} a_n$ définit une fonction continue $\mathbb{Z}_p \to \mathbb{Z}_p$.*

Proposition 4.3.2. *Soit $(a_n)_{n \in \mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ t.q. $a_n \xrightarrow[n \to +\infty]{} 0$. On pose :*

$$f : x \in \mathbb{Z}_p \longmapsto \sum_{n=0}^{\infty} \binom{x}{n} a_n \in \mathbb{Z}_p.$$

Alors :

(i) $\forall n \in \mathbb{N},\ a_n = \sum_{i=0}^{n} f(i)(-1)^{n-i}\binom{n}{i}$.

(ii) $\|f\|_\infty = \max_{n \in \mathbb{N}} |a_n|_p$.

Démonstration. (i) Montrer d'abord que, pour tout $n \in \mathbb{N}$:

$$\begin{pmatrix} f(0) \\ \vdots \\ f(n) \end{pmatrix} = M \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}, \qquad \text{avec } M = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & \ddots & \vdots \\ 1 & 2 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & n & \binom{n}{2} & \cdots & 1 \end{pmatrix} = \left(\binom{i}{j}\right)_{0 \leqslant i,j \leqslant n}.$$

Prouver que $M^{-1} = \left((-1)^{i-j}\binom{i}{j}\right)_{0\leqslant i,j\leqslant n}$ et en déduire le résultat. (ii) On a :

$$\forall x \in \mathbb{Z}_p,\ |f(x)|_p = \left|\sum_{n=0}^{\infty}\binom{x}{n}a_n\right|_p \leqslant \max_{n\in\mathbb{N}}\left(\left|\binom{x}{n}\right|_p |a_n|_p\right) \leqslant \max_{n\in\mathbb{N}}|a_n|_p\,.$$

Donc $\|f\|_\infty \leqslant \max_{n\in\mathbb{N}}|a_n|_p$. Réciproquement, à partir du résultat du (i), on a $\forall n \in \mathbb{N},\ |a_n|_p \leqslant \|f\|_\infty$, donc $\max_{n\in\mathbb{N}}|a_n|_p \leqslant \|f\|_\infty$. □

Lemme 4.3.3. *Soit $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$. Pour $n \in \mathbb{N}$, soit $a_n = \sum_{i=0}^{n} f(i)(-1)^{n-i}\binom{n}{i}$. Alors :*

$$\forall (m,n) \in \mathbb{N}^2,\ \sum_{j=0}^{m}\binom{m}{j}a_{n+j} = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k+m).$$

Théorème 4.3.4 (Théorème de Mahler)**.** *Soit $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$. Alors il existe une unique suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ de limite nulle t.q.*

$$\forall x \in \mathbb{Z}_p,\ f(x) = \sum_{n=0}^{\infty}\binom{x}{n}a_n.$$

Démonstration. *Unicité.* C'est une conséquence de la proposition 4.3.2. *Existence.* Pour $n \in \mathbb{N}$, on pose :

$$a_n = \sum_{i=0}^{n} f(i)(-1)^{n-i}\binom{n}{i}.$$

Il suffit de montrer que $a_n \xrightarrow[n\to+\infty]{} 0$. En effet, on pourra alors considérer $\hat{f} : x \in \mathbb{Z}_p \longmapsto \sum_{n=0}^{\infty}\binom{x}{n}a_n \in \mathbb{Z}_p$, et on aura $f_{|\mathbb{N}} = \hat{f}_{|\mathbb{N}}$, ce qui permettra de conclure par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$. Montrons donc que $a_n \xrightarrow[n\to+\infty]{} 0$. Soit $\varepsilon > 0$. Soit $s \in \mathbb{N}$ t.q. $p^{-s} \leqslant \varepsilon$. Comme f est continue sur le compact $\mathbb{Z}_p$, f est uniformément continue : il existe $t \in \mathbb{N}$ t.q.

$$\forall (x,y) \in \mathbb{Z}_p^2,\ (x-y) \in p^t\mathbb{Z}_p \Longrightarrow (f(x)-f(y)) \in p^s\mathbb{Z}_p.$$

En appliquant le lemme 4.3.3 avec $m = p^t$, on a :

$$\forall n \in \mathbb{N},\ a_{n+p^t} + \sum_{j=1}^{p^t-1}\binom{p^t}{j}a_{n+j} + a_n = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f\left(k+p^t\right).$$

En soustrayant à cette égalité la définition de a_n, on a :

$$\forall n \in \mathbb{N},\ a_{n+p^t} = -\sum_{j=1}^{p^t-1}\underbrace{\binom{p^t}{j}}_{\in p\mathbb{Z}_p}a_{n+j} + \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\underbrace{\left(f\left(k+p^t\right)-f\left(k\right)\right)}_{\in p^s\mathbb{Z}_p}. \qquad (*)$$

Ainsi, $\forall n \in \mathbb{N},\ a_{n+p^t} \in p\mathbb{Z}_p$. En réinjectant ceci dans $(*)$, on obtient $\forall n \in \mathbb{N},\ a_{n+2p^t} \in p^2\mathbb{Z}_p$, puis en itérant :

$$\forall n \in \mathbb{N},\ a_{n+sp^t} \in p^s\mathbb{Z}_p.$$

Autrement dit : $\forall n \geqslant sp^t,\ |a_n|_p \leqslant p^{-s} \leqslant \varepsilon$. Donc $a_n \xrightarrow[n\to+\infty]{} 0$. □

Remarque 4.3.5. *Si $\ell^0(\mathbb{N}) = \left\{(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}},\ a_n \xrightarrow[n\to+\infty]{} 0\right\}$, qu'on munit de $\|\cdot\|_\infty$, alors on a une bijection isométrique linéaire :*

$$\left|\begin{array}{c} \ell^0(\mathbb{N}) \longrightarrow \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p) \\ (a_n)_{n\in\mathbb{N}} \longmapsto \left(x \longmapsto \sum_{n=0}^{\infty}\binom{x}{n}a_n\right) \end{array}\right..$$

On dit que $\left(\binom{X}{n}\right)_{n\in\mathbb{N}}$ est une base de Banach *de l'espace de Banach $(\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p), \|\cdot\|_\infty)$.*

4.4 Fonctions différentiables

Définition 4.4.1 (Fonction différentiable)**.** *Une fonction $f : \mathbb{Z}_p \to \mathbb{Q}_p$ est dite* différentiable *en un point $a \in \mathbb{Z}_p$ s'il existe un $f'(a) \in \mathbb{Q}_p$ t.q.*

$$f(x) = f(a) + (x-a)f'(a) + o_a(x-a).$$

On dit de plus que f est $\mathcal{C}^1$ sur un ouvert $\mathcal{U}$ de $\mathbb{Z}_p$ lorsque f est différentiable en tout point de $\mathcal{U}$ et l'application $f' : \mathcal{U} \to \mathbb{Q}_p$ est continue. On définit de même la notion de fonction $\mathcal{C}^k$ (pour $1 \leqslant k \leqslant +\infty$) sur un ouvert de $\mathbb{Z}_p$.

Exemple 4.4.2.

(i) *Les polynômes de $\mathbb{Q}_p[X]$ sont $\mathcal{C}^\infty$ sur $\mathbb{Z}_p$.*

(ii) *Les fonctions localement constantes sont $\mathcal{C}^\infty$ sur $\mathbb{Z}_p$, de dérivée nulle.*

Exemple 4.4.3. *On considère :*

$$f : \left| \begin{array}{l} \mathbb{Z}_p \longrightarrow \mathbb{Q}_p \\ x \longmapsto \begin{cases} p^{2v_p(x)} & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases} \end{array} \right. .$$

Alors f est $\mathcal{C}^1$, de dérivée nulle sur $\mathbb{Z}_p$, mais f n'est pas localement constante (elle n'est pas constante au voisinage de 0).

Remarque 4.4.4. *Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ t.q. $a_n \xrightarrow[n\to+\infty]{} 0$ et $f : x \in \mathbb{Z}_p \longmapsto \sum_{n=0}^{\infty} \binom{x}{n} a_n \in \mathbb{Z}_p$. Alors on a les résultats (admis) suivants :*

(i) $f \in \mathcal{C}^1(\mathbb{Z}_p, \mathbb{Q}_p) \iff |a_n|_p = o\left(\frac{1}{n}\right)$.

(ii) $f \in \mathcal{C}^r(\mathbb{Z}_p, \mathbb{Q}_p) \iff |a_n|_p = o\left(\frac{1}{n^r}\right)$.

(iii) *f est lipschitzienne* $\iff |a_n|_p = \mathcal{O}\left(\frac{1}{n}\right)$.

5 Extensions finies de $\mathbb{Q}_p$

5.1 Théorème d'Ostrowski

Définition 5.1.1 (Norme de corps)**.** *Soit K un corps. On appelle* norme de corps *sur K toute application $|\cdot| : K \to \mathbb{R}_+$ vérifiant :*

(i) $\forall (x,y) \in K^2,\ |x+y| \leqslant |x| + |y|$,

(ii) $\forall (x,y) \in K^2,\ |xy| = |x| \cdot |y|$,

(iii) $|1_K| = 1$.

Définition 5.1.2 (Norme ultramétrique, archimédienne)**.** *Soit $|\cdot|$ une norme de corps sur $\mathbb{Q}$.*

(i) *On dit que $|\cdot|$ est* ultramétrique *lorsque :*

$$\forall (x,y) \in \mathbb{Q}^2,\ |x+y| \leqslant \max(|x|, |y|).$$

(ii) *On dit que $|\cdot|$ est* archimédienne *lorsque :*

$$\exists n \in \mathbb{Z},\ |n| > 1.$$

Proposition 5.1.3. *Une norme de corps $|\cdot|$ sur $\mathbb{Q}$ est ultramétrique* ssi *elle est non archimédienne.*

Démonstration. ($\Rightarrow$) Clair. ($\Leftarrow$) Supposons que $|\cdot|$ est non archimédienne. Soit $(x,y) \in \mathbb{Q}^2$, avec $|x| \geqslant |y|$. Alors :

$$\forall k \in \mathbb{N}^*,\ |x+y|^k = \left|(x+y)^k\right| = \left|\sum_{j=0}^{k} \binom{k}{j} x^{k-j} y^j\right| \leqslant (k+1)x^k.$$

Donc $\forall k \in \mathbb{N}^*,\ |x+y| \leqslant (k+1)^{\frac{1}{k}} |x|$. En faisant tendre $k \to +\infty$, on a $|x+y| \leqslant |x| = \max(|x|, |y|)$. Donc $|\cdot|$ est ultramétrique. □

Définition 5.1.4 (Norme triviale)**.** *On appelle* norme triviale *sur $\mathbb{Q}$ la norme de corps $|\cdot|$ donnée par :*

$$\forall x \in \mathbb{Q},\ |x| = \begin{cases} 1 & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases}.$$

Théorème 5.1.5 (Théorème d'Ostrowski)**.** *Soit $|\cdot|$ une norme de corps non triviale sur $\mathbb{Q}$.*

(i) *Si $|\cdot|$ est non archimédienne, alors il existe un nombre premier p et un $c \in \mathbb{R}_+^*$ t.q. $|\cdot| = |\cdot|_p^c$.*

(ii) *Si $|\cdot|$ est archimédienne, alors il existe un $c \in \mathbb{R}_+^*$ t.q. $|\cdot| = |\cdot|_\infty^c$, où $|\cdot|_\infty$ est la norme de corps usuelle sur $\mathbb{Q}$.*

5.2 $\mathbb{Q}_p$-espaces vectoriels normés

Définition 5.2.1 (Norme de $\mathbb{Q}_p$-espace vectoriel)**.** *Soit V un $\mathbb{Q}_p$-espace vectoriel. On appelle* norme *sur V toute norme ultramétrique $\|\cdot\|$ vérifiant :*

$$\forall \lambda \in \mathbb{Q}_p,\ \forall v \in V,\ \|\lambda v\| = |\lambda|_p \|v\|.$$

Théorème 5.2.2. *Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension finie. Alors toutes les normes sur V sont équivalentes, et V est complet pour n'importe laquelle.*

Démonstration. Même démonstration que sur $\mathbb{R}$ (on utilise le fait que $\Sigma = \{x \in V,\ \|x\|_\infty = 1\}$ est compacte pour $\|\cdot\|_\infty$, où $\|\cdot\|_\infty$ est la norme sup associée à une base quelconque de V). □

5.3 Prolongement de la norme p-adique aux extensions de $\mathbb{Q}_p$

5.3.1 Existence

Lemme 5.3.1. *Soit $Q \in \mathbb{Q}_p[X]$. Si $Q(0) \in \mathbb{Z}_p$ et Q est irréductible, alors $Q \in \mathbb{Z}_p[X]$.*

Démonstration. Soit $m \in \mathbb{N}$ le plus petit entier t.q. $F = p^m Q \in \mathbb{Z}_p[X]$. On suppose par l'absurde $m \geqslant 1$. Alors l'image de F dans $\mathbb{F}_p$ est divisible par X (car $v_p(F(0)) \geqslant m \geqslant 1$ comme $Q(0) \in \mathbb{Z}_p$). Soit donc $r \in \mathbb{N}^*$ la plus grande puissance de X divisant F dans $\mathbb{F}_p$, et soit $H_1 \in \mathbb{Z}_p[X]$ t.q.

$$F \equiv X^r H_1 \mod p.$$

Selon la proposition 3.2.2, il existe $(G,H) \in \mathbb{Z}_p[X]^2$ t.q. $F = GH$, $G \equiv X^r \mod p$ et $H \equiv H_1 \mod p$. En particulier, G et H sont non constants, ce qui contredit l'irréductibilité de F, donc de Q. □

Lemme 5.3.2. *Soit K une extension finie de $\mathbb{Q}_p$. Soit $N : K \to \mathbb{R}_+$ une application vérifiant $N(0) = 0$, $N(1) = 1$ et $\forall (x,y) \in K^2,\ N(xy) = N(x)N(y)$. Sont équivalentes :*

(i) $\forall (x,y) \in K^2,\ N(x+y) \leqslant \max(N(x), N(y))$.

(ii) $\forall z \in K,\ N(z) \leqslant 1 \Longrightarrow N(1+z) \leqslant 1$.

Proposition 5.3.3. *Soit K une extension finie de $\mathbb{Q}_p$, dont on note d le degré. Pour $x \in K$, on pose $m_x : y \in K \longmapsto xy \in K$. On définit :*

$$N : x \in K \longmapsto |\det m_x|_p^{1/d}.$$

Alors N est une norme de corps ultramétrique sur K qui prolonge $|\cdot|_p$.

Démonstration. Notons d'abord que $\forall x \in \mathbb{Q}_p$, $m_x = x \cdot id_K$, donc N prolonge bien $|\cdot|_p$. De plus, il est clair que $N(0) = 0$, $N(1) = 1$ et $\forall (x, y) \in K^2$, $N(xy) = N(x)N(y)$. Selon le lemme 5.3.2, il suffit donc de montrer que $\forall z \in K$, $N(z) \leqslant 1 \Longrightarrow N(1 + z) \leqslant 1$. Autrement dit, il suffit de montrer que :

$$\forall z \in K,\ \det m_z \in \mathbb{Z}_p \Longrightarrow \det m_{1+z} \in \mathbb{Z}_p.$$

Soit donc $z \in K$ t.q. $\det m_z \in \mathbb{Z}_p$. On pose $F = \mathbb{Q}_p(z)$, et on note $f = [F : \mathbb{Q}_p]$. Si $(k_1, \ldots, k_e)$ est une F-base de K, chaque $F \cdot k_i$ est stable par m_z et m_{1+z}, d'où on déduit :

$$\det m_z = (\det \hat{m}_z)^e \qquad \text{et} \qquad \det m_{1+z} = (\det \hat{m}_{1+z})^e,$$

où $\hat{m}_z$ et $\hat{m}_{1+z}$ sont les endomorphismes de F induits respectivement par m_z et m_{1+z}. On se ramène ainsi au cas où $K = F = \mathbb{Q}_p(z)$. On note maintenant $Q \in \mathbb{Q}_p[X]$ le polynôme minimal de z sur $\mathbb{Q}_p$; il est irréductible et de degré f. De plus :

$$\forall P \in \mathbb{Q}_p[X],\ P(m_z) = m_{P(z)}.$$

Ceci implique que Q est le polynôme minimal de m_z. Or F est de dimension $f = \deg Q$ sur $\mathbb{Q}_p[X]$, donc Q est aussi le polynôme caractéristique de m_z sur F. Il vient :

$$Q(0) = (-1)^f \det m_z \in \mathbb{Z}_p.$$

Selon le lemme 5.3.1, il vient $Q \in \mathbb{Z}_p[X]$. Donc $\det m_{1+z} = \det(id_K + m_z) = (-1)^f Q(-1) \in \mathbb{Z}_p$. □

5.3.2 Unicité

Lemme 5.3.4. *Soit F un corps ; $|\cdot|_1$ et $|\cdot|_2$ deux normes de corps non triviales sur F induisant la même topologie. Alors il existe $\alpha > 0$ t.q. $|\cdot|_2 = |\cdot|_1^\alpha$.*

Démonstration. Notons que :

$$\forall z \in F,\ |z|_1 < 1 \Longleftrightarrow z^n \xrightarrow[n\to+\infty]{|\cdot|_1} 0 \Longleftrightarrow z^n \xrightarrow[n\to+\infty]{|\cdot|_2} 0 \Longleftrightarrow |z|_2 < 1.$$

On fixe maintenant $y \in F$ avec $|y|_1 < 1$ (car $|\cdot|_1$ est non triviale). Pour $x \in F$, on a alors $\forall (m, n) \in \mathbb{Z} \times \mathbb{N}^*$, $|x|_1 < |y|_1^{m/n} \Longleftrightarrow |x|_2 < |y|_2^{m/n}$. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il vient $\forall s \in \mathbb{R}$, $|x|_1 = |y|_1^s \Longleftrightarrow |x|_2 = |y|_2^s$. Si on choisit maintenant $\alpha \in \mathbb{R}_+^*$ t.q. $|y|_2 = |y|_1^\alpha$, on a bien $|\cdot|_2 = |\cdot|_1^\alpha$. □

Théorème 5.3.5. *Soit K une extension finie de $\mathbb{Q}_p$. Alors il existe une unique norme de corps ultramétrique notée $|\cdot|_p$ sur K prolongeant la norme p-adique sur $\mathbb{Q}_p$.*

Démonstration. *Existence.* Voir proposition 5.3.3. *Unicité.* Si N_1 et N_2 sont deux normes de corps ultramétriques prolongeant $|\cdot|_p$ sur K, alors ce sont en particulier des normes de $\mathbb{Q}_p$-espace vectoriel, donc elles sont équivalentes selon le théorème 5.2.2. Selon le lemme 5.3.4, il existe donc $\alpha > 0$ t.q. $N_2 = N_1^\alpha$. Or $N_{1|\mathbb{Q}_p} = N_{2|\mathbb{Q}_p}$ donc $\alpha = 1$ et $N_1 = N_2$. □

Corollaire 5.3.6. *Si K est une extension finie de $\mathbb{Q}_p$, alors $\left(K, |\cdot|_p\right)$ est un corps normé complet.*

Remarque 5.3.7. *Le théorème 5.3.5 reste vrai pour les extensions algébriques de $\mathbb{Q}_p$.*

5.3.3 Quelques exemples

Notation 5.3.8. *Si K est une extension algébrique de $\mathbb{Q}_p$, on prolonge la valuation p-adique à K en posant :*

$$\forall x \in K,\ v_p(x) = -\log_p |x|_p .$$

Proposition 5.3.9. *Si K est une extension finie de $\mathbb{Q}_p$ de degré d, alors :*

$$\forall x \in K,\ v_p(x) \in \frac{1}{d}\mathbb{Z}.$$

Exemple 5.3.10. *On considère $K = \mathbb{Q}_p\left(\sqrt[d]{p}\right)$, qui est une extension finie de $\mathbb{Q}_p$ de degré d. Alors $\left(1, \sqrt[d]{p}, \ldots, \left(\sqrt[d]{p}\right)^{d-1}\right)$ est une $\mathbb{Q}_p$-base de K, et on a :*

$$\forall (a_0, \ldots, a_{d-1}) \in \mathbb{Q}_p^d,\ v_p\left(\sum_{i=0}^{d} a_i \left(\sqrt[d]{p}\right)^i\right) = \min_{0 \leqslant i \leqslant d-1} \left(v_p(a_i) + \frac{i}{d}\right).$$

Proposition 5.3.11. *Si K est une extension galoisienne (finie) de $\mathbb{Q}_p$, alors tout $g \in \mathrm{Gal}(K/\mathbb{Q}_p)$ est une isométrie de $\left(K, |\cdot|_p\right)$.*

5.4 Polygones de Newton

Notation 5.4.1. *On note $\overline{\mathbb{Q}}_p$ la clôture algébrique de $\mathbb{Q}_p$.*

Définition 5.4.2 (Polygone de Newton)**.** *Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Q}_p[X]\backslash\{0\}$, avec $a_d \neq 0$. Le* polygone de Newton *de P, noté $NP(P)$, est l'enveloppe convexe inférieure des points $(k, v_p(a_k))_{0 \leqslant k \leqslant d}$ dans $\mathbb{R}^2$. Dans le cas où les premiers termes sont nuls, par exemple $a_0 = \cdots = a_{i-1} = 0 \neq a_i$, le polygone de Newton est constitué d'une demi-droite verticale vers le haut de base $(a_i, v_p(a_i))$, suivie de l'enveloppe convexe des points suivants.*

- *Une* pente *de $NP(P)$ est la pente d'un des segments ($-\infty$ dans le cas d'une demi-droite verticale).*
- *Une* longueur *de $NP(P)$ est la longueur de la composante d'un segment le long de l'axe des abscisses (i dans le cas d'une demi-droite verticale basée en $(i, v_p(a_i))$).*

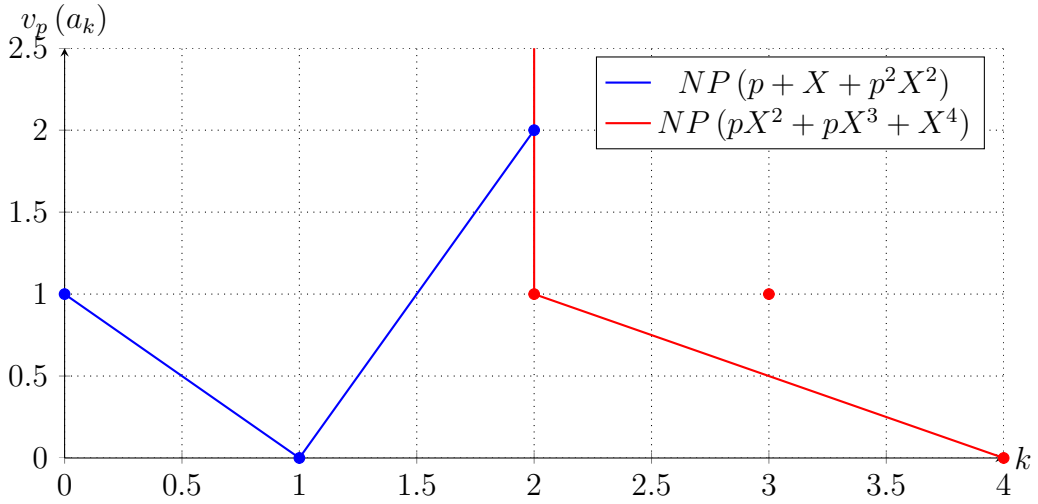


FIGURE 1 – Exemples de polygones de Newton

Théorème 5.4.3. *Soit $P \in \mathbb{Q}_p[X]$. Alors le nombre de racines de P dans $\overline{\mathbb{Q}}_p$ de valuation λ est égal à la longueur du segment de $NP(P)$ de pente $-\lambda$.*

Remarque 5.4.4. *Multiplier un polynôme de $\mathbb{Q}_p[X]$ par une constante non nulle revient à translater son polygone de Newton verticalement, ce qui ne change pas les pentes.*

Corollaire 5.4.5 (Critère d'Eisenstein)**.** *Soit $P = X^d + \sum_{k=0}^{d-1} a_k X^k \in \mathbb{Z}_p[X]$. On suppose que :*

(i) $\forall i \in \{0, \dots, d-1\}$, $a_i \in p\mathbb{Z}_p$.

(ii) $a_0 \in p\mathbb{Z}_p^\times$.

Alors p est irréductible sur $\mathbb{Q}_p$.

Démonstration. Le polygone de Newton $NP(P)$ a ici un seul segment, de longueur d et de pente $\left(-\frac{1}{d}\right)$. Selon le théorème 5.4.3, toutes les racines de P sont de valuation $\frac{1}{d}$. Soit maintenant $z \in \overline{\mathbb{Q}}_p$ une racine de P. Alors les éléments $1, z, \dots, z^{d-1}$ sont de valuations respectives $0, \frac{1}{d}, \dots, \frac{d-1}{d}$; ils sont donc linéairement indépendants. D'où :

$$d \leqslant [\mathbb{Q}_p(z) : \mathbb{Q}_p] \leqslant \deg P = d.$$

Donc P est le polynôme minimal de z sur $\mathbb{Q}_p$; il est donc irréductible. □

Proposition 5.4.6. *Si $P \in \mathbb{Q}_p[X]$ est irréductible, alors toutes ses racines dans $\overline{\mathbb{Q}}_p$ sont de même valuation.*

Démonstration. Soit K le corps de décomposition de P sur $\mathbb{Q}_p$. Comme P est irréductible, le groupe de Galois $\mathrm{Gal}\,(K/\mathbb{Q}_p)$ agit transitivement sur l'ensemble des racines de P. Si α et β sont deux racines de P, il existe donc $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q}_p)$ t.q. $\sigma(\alpha) = \beta$. Or, d'après la proposition 5.3.11, σ est une isométrie, donc :

$$|\beta|_p = |\sigma(\alpha)|_p = |\alpha|_p ,$$

d'où $v_p(\beta) = v_p(\alpha)$. □

Corollaire 5.4.7. *Si $P \in \mathbb{Q}_p[X]$ est irréductible, alors son polygone de Newton $NP(P)$ n'a qu'un seul segment.*

Remarque 5.4.8. *Le corollaire 5.4.7 donne une autre démonstration du fait que si $P \in \mathbb{Q}_p[X]$ est irréductible et vérifie $P(0) \in \mathbb{Z}_p$, alors $P \in \mathbb{Z}_p[X]$ (lemme 5.3.1).*

Remarque 5.4.9. *La théorie des polygones de Newton fonctionne sans modification pour des polynômes à coefficients dans une extension finie de $\mathbb{Q}_p$.*

6 Analyse p-adique

6.1 Le corps $\mathbb{C}_p$

Proposition 6.1.1. *Le corps normé $\left(\overline{\mathbb{Q}}_p, |\cdot|_p\right)$ n'est pas complet.*

Démonstration. On va montrer que $\left(\overline{\mathbb{Q}}_p, |\cdot|_p\right)$ n'est pas un espace de Baire, donc pas un espace métrique complet. Pour $d \in \mathbb{N}^*$, on note X_d l'ensemble des $x \in \overline{\mathbb{Q}}_p$ de degré d'algébricité sur $\mathbb{Q}_p$ inférieur ou égal à d. Soit $d \in \mathbb{N}^*$. *Étape 1* : X_d est fermé. Soit en effet $(x_n)_{n\in\mathbb{N}} \in X_d^{\mathbb{N}}$ t.q. $x_n \xrightarrow[n\to+\infty]{} x \in \overline{\mathbb{Q}}_p$. Pour $n \in \mathbb{N}$, soit $P_n \in \mathbb{Q}_p[X]\backslash\{0\}$ t.q. $P_n(x_n) = 0$ et $\deg P_n \leqslant d$. On peut supposer que chaque P_n appartient à l'ensemble K des polynômes de $\mathbb{Z}_p[X]$ de degré au plus d et dont au moins un des coefficients est dans $\mathbb{Z}_p^\times$. Or K est compact. Donc $(P_n)_{n\in\mathbb{N}}$ admet une valeur d'adhérence $P \in K \subset \mathbb{Z}_p[X]\backslash\{0\}$. On a donc $\deg P \leqslant d$ et on montre que $P(x) = 0$. *Étape 2* : X_d est d'intérieur vide. En effet, si ce n'est pas le cas, il existe $a \in X_d$ et $r > 0$ t.q. $B(a, r) \subset X_d$. Soit alors $x \in \overline{\mathbb{Q}}_p$. Pour k suffisamment grand, $b = a + p^k x \in B(a, r)$, donc $a \in X_d$ et $b \in X_d$. Ainsi $x = p^{-k}(b - a)$ est de degré d'algébricité au plus d^2. Ceci prouve que tout élément de $\overline{\mathbb{Q}}_p$ est de degré d'algébricité au plus d^2, ce qui est absurde, car pour tout $s \in \mathbb{N}^*$, le polynôme $X^s - p$ est irréductible

sur $\mathbb{Q}_p$ d'après le critère d'Eisenstein (corollaire 5.4.5) donc ses racines dans $\overline{\mathbb{Q}}_p$ sont de degré s. *Conclusion.* $(X_d)_{d\in\mathbb{N}^*}$ est une famille de fermés de $\overline{\mathbb{Q}}_p$ d'intérieur vide, et de réunion égale à $\overline{\mathbb{Q}}_p$. $\overline{\mathbb{Q}}_p$ n'est donc pas un espace de Baire (donc pas un espace métrique complet), car il n'est pas d'intérieur vide. □

Définition 6.1.2 ($\mathbb{C}_p$)**.** *On note $\mathbb{C}_p$, appelé ensemble des* complexes p-adiques*, le complété de $\overline{\mathbb{Q}}_p$ pour $|\cdot|_p$. Muni de $|\cdot|_p$, c'est un corps normé complet.*

Proposition 6.1.3. $v_p(\mathbb{C}_p) = \mathbb{Q}$.

Théorème 6.1.4. *$\mathbb{C}_p$ est algébriquement clos.*

Démonstration. On se donne $P \in \mathbb{C}_p[X]$ un polynôme unitaire de degré $d \geqslant 1$. Montrons que P a une racine dans $\mathbb{C}_p$. Quitte à remplacer P par $p^{kd}P\left(p^{-k}X\right)$ pour k suffisamment grand, on peut supposer que les coefficients de P sont de norme inférieure ou égale à 1. Pour $n \in \mathbb{N}$, on se donne alors $P_n \in \overline{\mathbb{Q}}_p[X]$ unitaire de degré d t.q. $\|P - P_n\| \leqslant p^{-n}$, où $\mathbb{C}_p[X]$ est muni de la norme $\|\cdot\|$ définie par $\left\|\sum_{k=0}^{\delta} a_k X^k\right\| = \max_{0\leqslant k\leqslant\delta} |a_k|_p$. Ainsi, les coefficients de chaque P_n sont tous de norme inférieure ou égale à 1. La théorie des polygones de Newton permet alors de montrer que les racines de chaque P_n sont de valuation positive, donc de norme inférieure ou égale à 1. Définissons maintenant une suite $(a_n)_{n\in\mathbb{N}}$ par récurrence. On pose a_0 une racine de P_0, puis après avoir construit $a_0, \ldots, a_n$ avec a_i racine de P_i pour tout $i \in \{0, \ldots, n\}$, on remarque que $|P_{n+1}(a_n)|_p = |(P_{n+1} - P_n)(a_n)|_p \leqslant p^{-n}$. Or, si $\mathcal{R}$ est l'ensemble des racines de P_{n+1}, on a $P_{n+1} = \prod_{z\in\mathcal{R}}(X - z)$; il existe donc $a_{n+1} \in \mathcal{R}$ t.q. $|a_{n+1} - a_n|_p \leqslant p^{-\frac{n}{d}}$. La suite $(a_n)_{n\in\mathbb{N}}$ ainsi construite est de Cauchy dans $\overline{\mathbb{Q}}_p$, donc converge vers un $a \in \mathbb{C}_p$. Et on vérifie que $P(a) = 0$. □

6.2 Séries formelles

Définition 6.2.1 (Séries formelles)**.** *Si A est un anneau, on note $A[[X]]$ l'anneau des* séries formelles *à coefficients dans A, c'est-à-dire des séries $\sum_{n=0}^{\infty} a_n X^n$, avec $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$. $A[[X]]$ est un anneau, muni du produit $\times$ défini par :*

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty}\left(\sum_{p+q=n} a_p b_q\right) X^n.$$

Proposition 6.2.2. *Soit A un anneau. Soit $f = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$. Alors $S \in A[[X]]^\times$* ssi *$a_0 \in A^\times$.*

Définition 6.2.3 (Degré de Weierstraß)**.** *Soit A un anneau. Si $f = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$, on définit le* degré de Weierstraß *de S par :*

$$\operatorname{wideg} f = \inf\left\{n \in \mathbb{N},\ a_n \in A^\times\right\} \in \mathbb{N} \cup \{\infty\}.$$

Corollaire 6.2.4. *Soit A un anneau. Pour $f \in A[[X]]$, on a :*

$$f \in A[[X]]^\times \iff \operatorname{wideg} f = 0.$$

Proposition 6.2.5. *Soit A un anneau. On a :*

$$\forall (f, g) \in A[[X]]^2,\ \operatorname{wideg}(fg) = \operatorname{wideg} f + \operatorname{wideg} g.$$

Proposition 6.2.6. *Soit K un corps. Soit $(f, g) \in K[[X]]^2$, avec* $\operatorname{wideg} f = n \in \mathbb{N}$*. Alors :*

$$\exists q \in K[[X]],\ \exists r \in K[X],\ (g = qf + r \text{ et } \deg r < n).$$

6.3 Théorème de préparation de Weierstraß

Notation 6.3.1. *On note* $\mathcal{D} = \left\{ z \in \mathbb{C}_p,\ |z|_p < 1 \right\}$ *le disque unité ouvert p-adique.*

Définition 6.3.2. *Soit* $f = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}_p[[X]]$. *Alors pour tout* $z \in \mathcal{D}$, *la série* $\sum_{n=0}^{\infty} a_n z^n$ *converge dans* $\mathbb{C}_p$ *; sa somme est notée* $f(z)$.

Proposition 6.3.3. *Soit* $(f, g) \in \mathbb{Z}_p[[X]]^2$, *avec* $\operatorname{wideg} f = n \in \mathbb{N}$. *Alors :*

$$\exists q \in \mathbb{Z}_p[[X]],\ \exists r \in \mathbb{Z}_p[X],\ (g = qf + r \text{ et } \deg r < n)\,.$$

Démonstration. On va utiliser la proposition 6.2.6 dans $\mathbb{F}_p$. Supposons avoir construit $q_k \in \mathbb{Z}_p[[X]]$ et $r_k \in \mathbb{Z}_p[X]$ t.q.

$$g \equiv q_k f + r_k \mod p^k \quad \text{et} \quad \deg r_k < n.$$

Il existe donc $h_k \in \mathbb{Z}_p[[X]]$ t.q. $g = q_k f + r_k - p^k h_k$. Selon la proposition 6.2.6 appliquée dans $\mathbb{F}_p$ aux réductions respectives $\overline{h_k}$ et $\overline{f}$ de h_k et f modulo p, il existe $s_k \in \mathbb{Z}_p[[X]]$ et $t_k \in \mathbb{Z}_p[X]$ t.q.

$$h_k \equiv f s_k + t_k \mod p \quad \text{et} \quad \deg t_k < n.$$

Ainsi, $g \equiv \left(q_k - p^k s_k\right) f + \left(r_k - p^k t_k\right) \mod p^{k+1}$; on pose donc $q_{k+1} = q_k - p^k s_k$ et $r_{k+1} = r_k - p^k t_k$. La construction se propage par récurrence ; on note finalement $q = \lim_{k \to +\infty} q_k$ et $r = \lim_{k \to +\infty} r_k$. □

Théorème 6.3.4 (Théorème de préparation de Weierstraß)**.** *Soit* $f \in \mathbb{Z}_p[[X]]$. *On suppose que* $\operatorname{wideg} f = n < +\infty$. *Alors il existe un polynôme unitaire* $s = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{Z}_p[X]$ *avec* $\forall k \in \{0, \ldots, n-1\}$, $a_k \in p\mathbb{Z}_p$, *et une série formelle inversible* $u \in \mathbb{Z}_p[[X]]^\times$ *t.q.*

$$f = su.$$

Démonstration. D'après la proposition 6.3.3, il existe $q \in \mathbb{Z}_p[[X]]$ et $r \in \mathbb{Z}_p[X]$ t.q.

$$X^n = fq + r \quad \text{et} \quad \deg r < n.$$

Il vient $fq = X^n - r$, d'où :

$$n \leqslant n + \operatorname{wideg} q = \operatorname{wideg}(fq) = \operatorname{wideg}\left(X^n - r\right) \leqslant n.$$

Donc $\operatorname{wideg} q = 0$. Ainsi $q \in \mathbb{Z}_p[[X]]^\times$. On pose donc $s = X^n - r$ et $u = q^{-1}$. □

Corollaire 6.3.5. *Soit* $f \in \mathbb{Z}_p[[X]]$. *Si* $\operatorname{wideg} f = n < +\infty$, *alors* f *admet exactement* n *zéros (comptés avec leurs multiplicités) dans* $\mathcal{D}$.

Démonstration. D'après le théorème 6.3.4, il existe $s = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{Z}_p[X]$ avec $\forall k \in \{0, \ldots, n-1\}$, $a_k \in p\mathbb{Z}_p$ et $u \in \mathbb{Z}_p[[X]]^\times$ t.q. $f = su$. Comme u est inversible, elle n'admet pas de zéro dans $\mathcal{D}$, donc les zéros de f sont exactement ceux de s. Or s est de degré n, donc admet exactement n zéros (comptés avec leurs multiplicités) dans $\overline{\mathbb{Q}}_p$. La théorie des polygones de Newton montre alors que ces zéros sont de valuation supérieure ou égale à $\frac{1}{n}$, donc sont dans $\mathcal{D}$. □

Corollaire 6.3.6. *Si* $f \in \mathbb{Z}_p[[X]] \backslash \{0\}$, *alors* f *n'a qu'un nombre fini de zéros dans* $\mathcal{D}$.