Polygones de Newton ; Corps $\overline{\mathbb{Q}}_p$ et $\mathbb{C}_p$

Dans toute la suite, p désignera un nombre premier. Pour tout polynôme $P \in \mathbb{Q}_p[X]$, on notera $\mathrm{NP}(P)$ son polygone de Newton.

Exercice 1. Pour chacun des polynômes de $\mathbb{Q}_p[X]$ suivants, déterminer son polygone de Newton, dire s'il est irréductible et déterminer le nombre de racines de valuation donnée dans $\overline{\mathbb{Q}_p}$.

— $P_1 = 1 + X^2 + (p + p^3)X^4 + p^3X^6$;
— $P_2 = X^3 + 3pX + 3p^2X^2 + p^3$;
— $P_3 = X^3 + 3p^3X + 3p^2X^2 + p$;
— $P_4 = \prod_{i=1}^{p^2}(1 - iX)$.

Exercice 2. Soit $P \in \mathbb{Q}_p[X]$.

1. Soit $\lambda \in \mathbb{Q}_p^\times$. Décrire $\mathrm{NP}(\lambda P)$ en fonction de $\mathrm{NP}(P)$.
2. On écrit $P = \lambda \prod_{i=1}^{n} \prod_{j=1}^{m_i} (X - r_{i,j})$ où les $r_{i,j}$ sont les racines de P dans $\overline{\mathbb{Q}_p}$ de valuation v_i avec $v_1 < v_2 < \cdots < v_n$. Décrire le polygone de Newton de P.
3. Montrer que pour tout i, le polynôme $P_i = \prod_{j=1}^{m_i} (X - r_{i,j})$ est à coefficients dans $\mathbb{Q}_p$.

Exercice 3. (Polynômes irréductibles – Examen 2018)
Soit $P \in \mathbb{Q}_p[X]$ un polynôme unitaire de degré d tel que $P(0) \neq 0$. On suppose que $\mathrm{NP}(P)$ n'a qu'une seule pente λ.

1. Montrer qu'on peut écrire $\lambda = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ premiers entre eux, avec b divisant d.
2. Montrer que si $b = d$, alors P est irréductible.
3. Inversement, si P est irréductible, il a été vu en cours que $\mathrm{NP}(P)$ n'a qu'une seule pente, qu'on peut donc écrire $\frac{a}{d}$. L'entier $a \in \mathbb{Z}$ est-il nécessairement premier à d ?

Exercice 4. (Principe de continuité des racines)

1. Soit $a \in \overline{\mathbb{Q}_p}$, soit P le polynôme minimal de a sur $\mathbb{Q}_p$ et G le groupe de Galois de P sur $\mathbb{Q}_p$. On pose $r = \inf\left\{|\sigma(a) - a|_p\,,\ \sigma \in G \text{ et } \sigma(a) \neq a\right\}$.
   (a) Justifier que $r = +\infty$ si, et seulement si, $a \in \mathbb{Q}_p$.
   (b) Soit $b \in \overline{\mathbb{Q}_p}$. On suppose que $a \notin \mathbb{Q}_p(b)$. Montrer que $|b - a|_p \geqslant r$.
   (c) En déduire que pour tout $b \in B_{\overline{\mathbb{Q}_p}}(a, r) = \{x \in \overline{\mathbb{Q}_p},\ |x - a|_p < r\}$, le corps $\mathbb{Q}_p(b)$ est une extension de $\mathbb{Q}_p(a)$.
2. On définit sur l'ensemble des polynômes à coefficients dans $\overline{\mathbb{Q}_p}$ de degré inférieur à d une norme par $\left\|\sum_{i=0}^{d} a_i X^i\right\| = \max\{|a_i|_p,\ 0 \leqslant i \leqslant d\}$. Soit a un élément algébrique de degré d sur $\mathbb{Q}_p$ et P son polynôme minimal.
   (a) Soit $Q \in \mathbb{Q}_p[X]$ un polynôme de degré d et $b_1, \ldots, b_d$ ses racines dans $\overline{\mathbb{Q}_p}$. On pose $M = \max\{|a|_p^i,\ 0 \leqslant i \leqslant d\}$. Montrer qu'il existe i tel que $|a - b_i|_p^n \leqslant \|P - Q\|M$.
   (b) En déduire qu'il existe $\varepsilon > 0$ tel que pour tout $Q \in \mathbb{Q}_p[X]$ de degré d tel que $\|P - Q\| \leqslant \varepsilon$ il existe une racine b de Q telle que $\mathbb{Q}_p(a) = \mathbb{Q}_p(b)$.
   (c) En déduire qu'il existe une suite de polynômes unitaire Q_i de degré d, à coefficients dans $\mathbb{Q}$ qui converge coefficient par coefficient vers P, et une suite d'éléments $x_i \in \mathbb{Q}_p(a)$, racines des Q_i, qui converge vers a.
3. Montrer que l'espace métrique $\overline{\mathbb{Q}_p}$ est séparable.

Exercice 5. (Le corps $\mathbb{C}_p$ n'est pas sphériquement complet)

Le but de cet exercice est de montrer qu'il existe une suite décroissante de boules de $\mathbb{C}_p$ d'intersection vide. On considère une suite strictement décroissante de réels positifs $(r_n)_{n\in\mathbb{N}}$ de limite $\lim\limits_{n\to\infty} r_n = r_\infty$ et on se propose de construire une suite de boules fermées de $\mathbb{C}_p$, qu'on notera $B_n = B(z_n, r_n) = \{z \in \mathbb{C}_p,\ |z - z_n|_p \leqslant r_n\}$ avec $z_n \in \mathbb{C}_p$ telles que $B_0 \supset B_1 \supset B_2 \supset \cdots$.

1. Montrer que l'espace métrique complet $\mathbb{C}_p$ est séparable.
   Indication : on pourra utiliser l'exercice précédent.
2. Montrer que si $r_\infty = 0$, alors $\bigcap\limits_{n\in\mathbb{N}} B_n$ est un singleton de $\mathbb{C}_p$.

On suppose désormais $r_\infty > 0$.

3. Soient $r, s \in \mathbb{R}_+^*$ avec $r > s$. Montrer que dans toute boule fermée de $\mathbb{C}_p$ de rayon r, on peut trouver deux boules fermées, disjointes l'une de l'autre, de même rayon s.
4. Construire pour tout $n \in \mathbb{N}$ une famille de boules fermées $\left(B_{i_1,\ldots,i_n}\right)_{i_1,\ldots,i_n\in\{0,1\}}$ de rayon r_n telles que pour tout $1 \leqslant m \leqslant n-1$, tout $i_1, \ldots, i_m \in \{0,1\}$, on ait $B_{i_1,\ldots,i_m,0} \subset B_{i_1,\ldots,i_m}$ et $B_{i_1,\ldots,i_m,1} \subset B_{i_1,\ldots,i_m}$ et $B_{i_1,\ldots,i_m,0} \cap B_{i_1,\ldots,i_m,1} = \emptyset$.
5. Montrer que pour toute suite $i = (i_n)_{n\in\mathbb{N}^*}$ d'éléments $i_n \in \{0,1\}$, l'intersection $B_{(i)} = \bigcap\limits_{m\in\mathbb{N}^*} B_{i_1,\ldots,i_m}$ est soit vide, soit une boule de rayon r_∞.
6. On suppose qu'aucune des $B_{(i)}$ n'est vide. Montrer que les $B_{(i)}$ forment une famille non dénombrable d'ouverts deux à deux disjoints de $\mathbb{C}_p$.
7. Conclure.

Exercice 6.(Sous-groupes additifs et multiplicatifs dans $\mathbb{C}_p$)

Pour $r \in \mathbb{R}_+$ et $z \in \mathbb{C}_p$, on notera $D(a, r) = \{z \in \mathbb{C}_p,\ |z - a|_p \leqslant r\}$.

1. Montrer que pour $r > 0$, l'ensemble $D(0, r)$ est un sous-groupe de $(\mathbb{C}_p, +)$, puis que, pour tout $0 < s < r$, le sous-groupe $D(0, r)$ n'est pas le produit direct de $D(0, s)$ avec un autre sous-groupe de $(\mathbb{C}_p, +)$, autrement dit que la suite exacte de groupes abéliens
$$0 \to D(0, s) \to D(0, r) \to D(0, r)/D(0, s) \to 0$$
n'est pas scindée.
Indication : $\lim\limits_{n\to\infty} p^n x = 0$ *pour tout* $x \in D(0, s)$.
2. Montrer que pour $r > 0$, l'ensemble $D(1, r)$ est un sous-groupe de $(\mathbb{C}_p^*, \times)$, puis que, pour tout $0 < s < r$, le sous-groupe $D(0, r)$ n'est pas le produit direct de $D(0, s)$ avec un autre sous-groupe de $(\mathbb{C}_p^*, \times)$, autrement dit que la suite exacte de groupes abéliens
$$1 \to D(1, s) \to D(1, r) \to D(1, r)/D(1, s) \to 1$$
n'est pas scindée.
Indication : $\lim\limits_{n\to\infty} (1 + x)^{p^n} = 1$ *si* $|x|_p < 1$.
3. Montrer que si $0 < s^2 \leqslant r < s < 1$, alors il existe un isomorphisme de groupes canonique :
$$D(1, s)/D(1, r) \xrightarrow{\simeq} D(0, s)/D(0, r)$$
Indication : Considérer le morphisme de groupes $x \mapsto (x - 1) \mod D(0, r)$.