Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices X

Exercice 1 Soit p un nombre premier. On désigne par $\mathbb{Q}_p$ le corps p-adique et par $|\cdot|_p$ la valeur absolue p-adique sur $\mathbb{Q}_p$. On fixe en outre une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$.

1) Montrer que la valeur absolue $|\cdot|_p$ s'étend de façon unique sur $\overline{\mathbb{Q}}_p$.

Pour tout entier $n \geqslant 1$, soit ζ_n une racine n-ième de l'unité qui est primitive. Soit $k : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ l'application telle que

$$k(n) = \begin{cases} n, & (p,n) = 1, \\ 1, & p \nmid n. \end{cases}$$

Pour tout entier $n \geqslant 1$, soit

$$\alpha_n = \sum_{1 \leqslant m \leqslant n} \zeta_{k(m)} p^m.$$

2) Montrer que $(\alpha_n)_{n \geqslant 1}$ est une suite de Cauchy dans $\overline{\mathbb{Q}}_p$.
3) Soit $n \geqslant 1$ un entier qui n'est pas divisible par p. Montrer que, si $\zeta \in \overline{\mathbb{Q}}_p$ est une racine n-ième de l'unité qui est différent de ζ_n, alors il existe un élément $a \in \mathbb{Z}_p$ tel que $a(\zeta - \zeta_n) - 1 \in p\mathbb{Z}_p$.
4) On suppose que la suite $(\alpha_n)_{n \geqslant 1}$ converge dans $\overline{\mathbb{Q}}_p$ vers un élément α et on note $K = \mathbb{Q}_p(\alpha)$. On suppose que $m \geqslant 2$ est un entier non-divisible par p et tel que $\{\zeta_{k(1)}, \ldots, \zeta_{k(m-1)}\} \subset K$.
   (i) Soit $\beta_m = \alpha - \alpha_{m-1}$. Montrer que $\beta_m \in K$.
   (ii) Montrer que la réduction de β_m^m modulo p est 1.
   (iii) En déduire qu'il existe $\zeta \in K$ tel que $\zeta^m = 1$ et que $\zeta \equiv \zeta_m$ modulo p.
   (iv) En déduire que $\zeta_m \in K$.
5) Montrer que $\overline{\mathbb{Q}}_p$ n'est pas complet.

Dans la suite, on désigne par $\mathbb{C}_p$ le complété de $\overline{\mathbb{Q}}_p$. Pour tout polynôme $F = \sum_i a_i X^i$ dans $\mathbb{C}_p[X]$, on note $\|F\| := \max_i |a_i|_p$. On fixe un polyôme unitaire P à coefficient dans $\mathbb{C}_p$. Soit d le degré de P, supposé être $\geqslant 1$.

6) Montrer qu'il existe une suite $(P_n)_{n \geqslant 1}$ de polynômes unitaires de degré d dans $\overline{\mathbb{Q}}_p[X]$ telle que la suite $(\|P_n - P\|)_{n \geqslant 1}$ soit contenue dans $[0, 1[$ et converge vers 0.
7) Soit x_n une racine de P_n dans $\overline{\mathbb{Q}}_p$.
   (i) Soient $(x_{n+1,i})_{i=1}^d$ les d racines de P_{n+1} (en comptant les multiplicités). Montrer que
   $$\prod_{i=1}^{d} |x_n - x_{n+1,i}|_p \leqslant \|P_{n+1} - P_n\| \max(1, |x_n|_p^d).$$
   (ii) En déduire qu'il existe une racine x_{n+1} de P_{n+1} telle que
   $$(*) \qquad |x_n - x_{n+1}| \leqslant \|P_{n+1} - P_n\|^{1/d} \max(1, |x_n|_p).$$

8) Soit $(x_n)_{n\geqslant 1}$ une suite dans $\overline{\mathbb{Q}}_p$ telle que, pour tout entier $n \geqslant 1$, x_n soit une racine de P_n, et la relation $(*)$ soit vérifiée. Montrer que la suite $(x_n)_{n\geqslant 1}$ est bornée.
9) En déduire que $(x_n)_{n\geqslant 1}$ est une suite de Cauchy.
10) Soit x la limite de la suite $(x_n)_{n\geqslant 1}$. Montrer que x est une racine du polynôme P.
11) En déduire que $\mathbb{C}_p$ est algébriquement clos.

Exercice 2 Pour tout entier strictement positif n et tout nombre premier p, on désigne par $v_p(n)$ l'exposant de p dans la décomposition canonique de n en produit de puissances de nombres premiers. On désigne par Ω la classe des entier strictement positif n qui vérifie la condition suivante :

$$\forall \text{ nombre premier } p, \quad p \equiv 3 \pmod 4 \Longrightarrow v_p(n) \text{ est pair.}$$

Le but de cet exercice est de montrer que l'ensemble Ω s'identifie à la classe des entiers exprimables comme la somme de deux carrés. Dans la suite, on désigne par h la fonction indicatrice de l'ensemble des sommes de deux carrés.

1) Soient a, b, c et d quatre entiers. En exprimant $(a^2+b^2)(c^2+d^2)$ comme la somme de deux carrés, montrer que la fonction h vérifie $h(mn) \geqslant h(m)h(n)$ $(m, n \in \mathbb{N}_*)$.
2) En déduire que, pour tout $n \in \Omega$, on a $h(n) = 1$.
3) Soit $n = a^2 + b^2$ un entier strictement positif avec $a, b \in \mathbb{Z}$. On suppose que p soit un nombre premier tel que $v_p(n) = 2s+1$, $s \in \mathbb{N}$.
   (i) Montrer que, $\min(v_p(a), v_p(b)) \leqslant s$.
   (ii) On suppose que $t = v_p(a) \leqslant s$. Montrer que $v_p(b) = t$.
   (iii) En déduire qu'il existe deux entiers α et β tels que $p \mid \alpha^2 + \beta^2$ et que $p \nmid \alpha\beta$.
   (iv) En déduire que $p \equiv 1 \pmod 4$.
4) Conclure.