Université Joseph Fourier
Institut Fourier, UFR de Mathématiques
Année universitaire 2009/2010
Licence de 3ème année

Exercices de préparation-1 (Corrections, indications, réponses)

Analyse p–adique et applications

A.A.Pantchichkine, 1 semestre

(1) Soit $U_{a,r} = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\}$.
(a) Montrer que pour tout $a, a' \in \mathbb{Q}_p$, et $r, r' \in \mathbb{R}$ soit
(i) $U_{a,r} \subseteq U_{a',r'}$, soit
(ii) $U_{a,r} \supseteq U_{a',r'}$, soit
(iii) $U_{a,r} \cap U_{a',r'} = \emptyset$.
Correction. Si $U_{a,r} \cap U_{a',r'} \neq \emptyset$, il existe $z \in U_{a,r} \cap U_{a',r'}$, $|z-a| < r, |z-a'| < r'$ => $|a-a'| < \max\{r, r'\}$.
Si $\max\{r, r'\} = r$, alors $U_{a,r} = U_{z,r}$, $U_{a',r'} = U_{z,r'}$, donc $U_{a,r} \supseteq U_{a',r'}$
(b) Trouver $U_{2,1/5} \cap U_{11,1/7}$ dans $\mathbb{Q}_3$.
Correction. On a $11 \in U_{2,1/5}$, car $|11-2|_3 = 1/9$ donc $11 \in U_{2,1/5}$, $U_{2,1/5} = U_{11,1/5}$ => $U_{11,1/7} \subset U_{2,1/5}$ => $U_{2,1/5} \cap U_{11,1/7} = U_{11,1/7}$.

(2) Évaluer

(i) $\mathrm{ord}_3 54$	(ii) $\mathrm{ord}_2 128$	(iii) $\mathrm{ord}_3 57$
(iv) $\mathrm{ord}_7(-700/197)$	(v) $\mathrm{ord}_2(128/7)$	(vi) $\mathrm{ord}_3(7/9)$
(vii) $\mathrm{ord}_5(-0.0625)$	(viii) $\mathrm{ord}_3(109)$	(ix) $\mathrm{ord}_3(-13.23)$
(x) $\mathrm{ord}_7(-13.23)$	(xi) $\mathrm{ord}_5(-13.23)$	(xii) $\mathrm{ord}_{11}(-13.23)$
(xiii) $\mathrm{ord}_{13}(-26/169)$	(xiv) $\mathrm{ord}_{103}(-1/309)$	(xv) $\mathrm{ord}_3(9!)$

Correction. On a $54 = 2 \cdot 3^3$=> $\mathrm{ord}_3 54 = 3$, etc.

(3) Évaluer les distances p-adiques $|a-b|_p$, où

(i) $a = 1, b = 26, p = 5$	(ii) $a = 1, b = 26, p = \infty$
(iii) $a = 1, b = 26, p = 3$	(iv) $a = 1/9, b = -1/16, p = 5$
(v) $a = 1, b = 244, p = 3$	(vi) $a = 1, b = 1/244, p = 3$
(vii) $a = 1, b = 1/243, p = 3$	(viii) $a = 1, b = 183, p = 13$
(ix) $a = 1, b = 183, p = 7$	(x) $a = 1, b = 183, p = 2$
(xi) $a = 1, b = 183, p = \infty$	(xii) $a = 9!, b = 0, p = 3$
(xiii) $a = (9!)^2/3^9, b = 0, p = 3$	(xiv) $a = 2^{2^N}/2^N, b = 0, p = 2$
(xv) $a = 2^{2^N}/(2^N)!, b = 0, p = 2,$	

Correction. On a $26 - 1 = 25 = 5^2$=> $|26-1|_5 = 1/25$ etc.

(4) Soit $n \geq 1$ un nombre naturel.
(a) Montrer que

$$\mathrm{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots .$$

(b) En déduire que

$$\text{ord}_p(p^m!) = p^{m-1} + p^{m-2} + \cdots + 1.$$

(c) En déduire $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_s p^s$ est écrit en base p, avec $0 \le a_j \le p-1$, et si on pose $S_n = \sum_j a_j$ (la somme de chiffres en base p), alors on a la formule:

$$\text{ord}_p(n!) = \frac{n - S_n}{p-1}.$$

(d)Trouver $\text{ord}_3(100!)$
(e)Trouver $\text{ord}_5(\binom{100}{25})$.
Indication. (a) Il suffit d'utiliser la définition $n! = 1 \cdot 2 \cdot \cdots \cdot (n-1)n$. Le nombre de termes divisibles par p^s est $\left[\frac{n}{p^s}\right]$, est le nombre de termes divisibles par p^{s+1} est $\left[\frac{n}{p^{s+1}}\right]$.

(b) Utiliser (a) directement; (c) Utiliser (a) en ecrivant

$$\begin{aligned}
&\text{ord}_p(a_0 + a_1 p + a_2 p^2 + \cdots + a_s p^s)! = \\
&\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \\
&\left[\frac{n}{p}\right] = \frac{(n-a_0)}{p}, \left[\frac{n}{p^2}\right] = \frac{(n-a_0-a_1p)}{p^2}, \cdots \\
&\left[\frac{n}{p^s}\right] = \frac{(n-a_0-a_1p-\cdots-a_{s-1}p^{s-1})}{p^s}
\end{aligned}$$

d'où la formule (par la sommation sur s de 1 à ∞, vu que

$$\frac{n}{p} + \frac{n}{p^2} + \cdots = \frac{n}{p-1}).$$

(d) Utiliser $100 = 1 + 2 \cdot 3^2 + 3^4$; (e) Utiliser (c) et $100 = 4 \cdot 5^2, 75 = 3 \cdot 5^2$.

(5) Pour $x \in \mathbb{Q}$, montrer que $\lim_{i\to\infty} |x^i/i!|_p = 0$ si et seulement si $\text{ord}_p x \ge 1$ si $p \ne 2$, $\text{ord}_2 x \ge 2$ si $p = 2$. *Indication.* Utiliser l'exercice précédente.

(6) Montrer que pour tout nombre premier p, et pour toute suite des nombres entiers il existe une sous-suite de Cauchy par rapport à la norme $|\cdot|_p$.
Indication. Utiliser le compact $\mathbb{Z}_p \supset \mathbb{Z}$.

(7) Soit $a \in \mathbb{Q}_p$ de dévelopement p-adique

$$a = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + \cdots + a_s p^s.$$

quel est le dévelopement de $-a$?
Correction.
$-a = 0 - a = (p - a_{-m})p^{-m} + (p - 1 - a_{-m+1})p^{-m+1} +$

$\cdots + (p-1-a_0) + (p-1-a_1)p + \cdots + (p-1-a_s)p^s + (p-1)p^{s+1} + \cdots$,

(8) Trouver tous les 4 racines quatrièmes de 1 dans $\mathbb{Q}_p$ avec quatre chiffres p-adiques pour $p = 5$. Montrer que $\mathbb{Q}_p$ contiens toujours p solutions $a_0, a_1, ..., a_{p-l}$ de l'equation $x^p - x = 0$, oú $a_i \equiv i(\text{mod}p)$. Ces p nombres sont dit les "représentants de Teichmüller" de {0, 1, 2, ... , $p-1$ }.
Réponse. $1; 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + O(5^5)$;
$2+5+2\cdot 5^2+5^3+3\cdot 5^4+O(5^5); 3+3\cdot 5+2\cdot 5^2+3\cdot 5^3+5^4+O(5^5)$.
Indication. Utiliser le Lemme d'Hensel.

(9) Montrer le "critère d'Eisenstein" pour un polynôme $f(x) = a_0 + a_1x + \cdots + a_nx^n$ à coefficients $a_i \in \mathbb{Z}_p$: si $a_i \equiv 0(\text{mod}p)$ pour $i = 0, 1, 2, ..., n-1$, $a_n \not\equiv 0(\text{mod}p)$, et si $a_0 \not\equiv 0(\text{mod}p^2)$, alors $f(x)$ est irréductible sur $\mathbb{Q}_p$, c'est-à-dire, on ne peut pas l'écrire comme produit de deux polynômes de degré inférieur à coefficients dans $\mathbb{Q}_p$.
Indication. Utiliser le lemme de Gauss pour l'anneau factoriel $\mathbb{Z}_p$.

(10) Démontrer que si m et p sont premiers entre eux, toute unite p-adique ε telle que $\varepsilon \equiv 1 \bmod p$ est une puissance m ième dans $\mathbb{Q}_p$.

(11) Soit $m = p^\delta m_0$, $(m_0, p) = 1$ et soit ε une unite p-adique telle que $\varepsilon \equiv 1 \bmod p^{\delta+1}$. Montrer que ε est une puissance m ième dans $\mathbb{Q}_p$.
Indication. Utiliser le Lemme d'Hensel.

(12) Démontrer que, pour $p \neq 2$, la résolubilité de la congruence $\alpha x^p \equiv \beta \bmod p^2$ par des entiers p-adiques α et β non divisibles par p entraîne la resolubilite de l'équation $\alpha x^p = \beta$ dans le corps $\mathbb{Q}_p$.
Indication. Utiliser le Lemme d'Hensel.

(13) Posant $x_n = 1 + p + \cdots + p^{n-1}$, montrer que dans le corps des nombres p-adiques, la suite $\{x_n\}$ converge vers $\dfrac{1}{1-p}$.

(14) Soient $p \neq 2$ et c un résidu quadratique modulo p. Montrer qu'il existe deux nombres p-adiques distincts dont les carres sont egaux a c.

(15) Soit c un entier rationnel non divisible par p. Montrer que la suite $\{c^{p^n}\}$ est convergente dans l'anneau $\mathbb{Z}_p$. Soit y la limite de cette suite; montrer que $\gamma \equiv c(\text{mod}p)$ et $\gamma^{p-1} = 1$.

(16) Utilisant 1'exercice precedent, montrer que le polynôme $t^{p-1}-1$ se decompose en facteurs linéaires dans le corps $\mathbb{Q}_p$.

(17) Dans le corps des nombres p-adiques, ecrire le nombre -2 comme somme d'une série du type

$$a = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1p + \cdots ,$$

avec $0 \leq a_j \leq p-1$.

(18) Montrer qu'il existe des extensions finies de degré quelconque du corps $\mathbb{Q}_p$.

(19) Démontrer, que pour des nombres premiers p et q distincts, les corps $\mathbb{Q}_p$ et $\mathbb{Q}_q$ ne sont pas isomorphes. Démontrer egalement qu'aucun des corps $\mathbb{Q}_p$ n'est pas ismorphe au corps des nombres reels.

(20) Démontrer que le seul automorphisme du corps des nombres p-adiques estl'identite (c'est également vrai pour le corps des nombres réels).

(21) Soit $r, s \in \mathbb{N}$.

(a) Montrer que pour tout $r, s \in \mathbb{N}$ on a $\left|\binom{r}{s}\right|_p \leq \left|\frac{r}{s}\right|_p$.

(b) Calculer $\mathrm{ord}_p\binom{r}{s}$.

(22) Soit $f : \mathbb{Z}_p \to \mathbb{Q}_p$ définie par $f(x) = \begin{cases} 1, & \text{si } x \equiv 1 (\mathrm{mod} p) \\ 0, & \text{sinon,} \end{cases}$, et

soit $f(x) = \displaystyle\sum_{n=0}^{\infty} a_n \binom{x}{n}$ sa série de Mahler.

(a) Trouver les coefficients a_n en utilisant

$$a_{n+p} = -\sum_{j=1}^{p-1} \binom{p}{j} a_{n+j} + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} (f(k+p) - f(k)) \qquad (*)$$

(b) Démontrer l'égalité (*)

Indication. Utiliser la fomule du cours $a_m = \displaystyle\sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} f(j)$.

(23) Soit $f(X) = X^{11} - 10X^9 + 25X^2 - 30 \in \mathbb{Z}_5[X]$.

(a) Montrer que f est irréductible dans $\mathbb{Q}_5[X]$

(b) Trouver l'indice de ramification e de l'extension K de $\mathbb{Q}_5$ engendrée par une racine du polynôme

$$f(X) = X^{11} - 10X^9 + 25X^2 - 30.$$

Indication. (a) Utiliser le "critère d'Eisenstein" ci-dessus.

(b) *Réponse*: Pour toute racine α de f on a $\mathrm{ord}_5(\alpha) = 1$. En utilisant la norme algébrique, on trouve $\mathrm{ord}_p(K^*) = \dfrac{1}{11}\mathbb{Z}$ puisque le degré de f est 11, donc $e = 11$.

(24) Trouver toutes les solutions de la congruence

$$X^3 \equiv 2 (\mathrm{mod} 5^3).$$

Indication. Utiliser le Lemme d'Hensel.

(25) On considère les extenstions du corps des nombres p-adiques $\mathbb{Q}_p$;

(a) Trouver le polynôme minimal d'une racine p^m-ème ζ_{p^m} de 1 sur le corps $\mathbb{Q}_p$;

(b) Trouver le degré $[\mathbb{Q}_p(\zeta_{p^m}) : \mathbb{Q}_p]$.

Indication. (a) Utiliser le "critère d'Eisenstein" ci-dessus pour le polynôme

$$f(X) = (X+1)^{(p-1)p^{m-1}} + (X+1)^{(p-2)p^{m-1}} + \cdots (X+1)^{p^{m-1}} + 1$$

et déduire que $f(X)$ est le polynôme minimal de $\zeta_{p^m} - 1$ sur $\mathbb{Q}_p$, donc $f(X-1)$ est le polynôme minimal de ζ_{p^m} sur $\mathbb{Q}_p$

(b) On a $\mathbb{Q}_p(\zeta_{p^m}) = \mathbb{Q}_p(\zeta_{p^m} - 1)$, et

$$[\mathbb{Q}_p(\zeta_{p^m}) : \mathbb{Q}_p] = (p-1)p^{m-1} = \deg(f).$$