SPÉCIALE MP* : CORRIGÉ DU DEVOIR LIBRE SUR LES ESPACES ULTRAMÉTRIQUES

Partie I

(1) Si $\mathrm{d}(x,z) < \mathrm{d}(z,y)$ alors $\mathrm{d}(x,y) \leqslant \sup\{\mathrm{d}(x,z),\mathrm{d}(z,y)\} \leqslant \mathrm{d}(z,y)$.
- Si $\mathrm{d}(x,y) > \mathrm{d}(z,x)$ alors $\mathrm{d}(z,y) \leqslant \sup\{\mathrm{d}(z,y),\mathrm{d}(x,y)\} \leqslant \mathrm{d}(x,y)$ d'où, par double inégalité, $\mathrm{d}(x,y) = \mathrm{d}(z,y)$.
- Si $\mathrm{d}(x,y) \leqslant \mathrm{d}(z,x)$ alors $\mathrm{d}(z,y) \leqslant \sup\{\mathrm{d}(z,x),\mathrm{d}(x,y)\} \leqslant \mathrm{d}(z,x)$ ce qui est contraire à l'hypothèse.

Conclusion : $\mathrm{d}(x,y) = \mathrm{d}(z,y)$.

(2) Si $\mathrm{d}(x,z) < r$ alors, comme $\mathrm{d}(y,z) \leqslant \sup\{\mathrm{d}(y,x),\mathrm{d}(x,z)\} < r$, on a $z \in B(y,r)$ donc $B(x,r) \subset B(y,r)$ et par symétrie ($\mathrm{d}(x,y) < r$), on a l'autre inclusion.
Conclusion : $B(x,r) = B(y,r)$.

(3) Soit $B(x,r)$ et $B(y,r')$ les deux boules en question, supposons $r \leqslant r'$.
S'il existe $z \in B(x,r) \cap B(y,r')$ alors $B(x,r) = B(z,r) \subset B(z,r') = B(y,r')$ sinon $B(x,r) \cap B(y,r') = \emptyset$.

Partie II

(1) (i) et (ii) sont immédiatement vérifiés. Prouvons que $\nu(x+y) \leqslant \sup\{\nu(x),\nu(y)\}$ (on écarte le cas où x ou y est nul).
- Si $\nu(x) < \nu(y)$ alors $x = p^r \dfrac{a'}{b'}$, $y = p^s \dfrac{c'}{d'}$ et $r > s$.
$$\begin{aligned} x + y &= p^s \left(\frac{p^{r-s} a'}{b'} + \frac{c'}{d'} \right) \\ &= p^s \frac{p^{r-s} a'd' + c'b'}{b'd'} \end{aligned}$$
et comme $c'b'$, $b'd'$ ne sont pas divisibles par p alors $\nu(x+y) = \nu(y)$.
- Si $\nu(x) = \nu(y)$ alors $x + y = p^s \dfrac{a'd' + b'c'}{b'd'}$ mais ici on ne sait pas si $a'd' + b'c'$ est ou non divisible par p donc $\nu(x+y) \leqslant \nu(x)$.

Conclusion : on a montré dans tous les cas que $\nu(x+y) \leqslant \sup\{\nu(x),\nu(y)\}$ ce qui s'écrit encore $\nu(x'-y') \leqslant \sup\{\nu(x'-z'),\nu(z'-y')\}$ en posant $x = x'-z'$, $y = z'-y'$.
Si $x = p^r \dfrac{a'}{b'}$ et $y = p^s \dfrac{c'}{d'}$ alors $xy = p^{r+s} \dfrac{a'c'}{b'd'}$. Or p ne divise ni $a'c'$ ni $b'd'$ donc $\nu(xy) = \alpha^{r+s} = \alpha^r \alpha^s = \nu(x)\nu(y)$.

(2) Tout d'abord, comme dans tout espace métrique, il y a unicité de la limite.
(i) Si $x = -1$ alors $u_n - x = 2^{n+1}$, donc $\nu(u_n - x) = \alpha^{n+1}$ et $\lim\limits_{n\to+\infty} u_n = -1$.
(ii) On a $v_n = \dfrac{1}{3} + \dfrac{2}{3} 4^{n+1}$ donc $\lim\limits_{n\to+\infty} v_n = \dfrac{1}{3}$.

(3) On sait que $\forall \varepsilon > 0$, $\exists N$, $\forall n \geqslant N$, $\nu(u_{n+1} - u_n) \leqslant \varepsilon$.
On a alors $\nu(u_{n+2} - u_n) \leqslant \sup\{\nu(u_{n+2} - u_{n+1}), \nu(u_{n+1} - u_n)\} \leqslant \varepsilon$ et par une récurrence immédiate $\nu(u_{n+p} - u_n) \leqslant \varepsilon$.

(4) a) On utilise la relation de Bézout avec $b \wedge p = 1$: $ub + vp = 1$, on multiplie par a cette relation puis on pose $x = au$ d'où $xb = a - avp$ donc il existe $x \in \mathbb{Z}$ tel que $bx \equiv a[p]$.

Il suffit alors de prendre pour x_0 le reste de la division par p de x : $x = pk + x_0$ avec $x_0 \in [\![0, p-1]\!]$. $bx_0 = bx - bpk \equiv a[p]$.
Si $x_1 \in [\![0, p-1]\!]$ et une autre solution alors $b(x_0 - x_1) \equiv 0[p]$ donc $p|b(x_0 - x_1)$ et comme $p \wedge b = 1$, $p|x_0 - x_1$ d'où $x_0 = x_1$ car $x_0 - x_1 \in [\![1-p, p-1]\!]$.
On pose alors $x_n = x_0 + py_{n-1}$ et on obtient

$$by_{n-1} = \frac{bx_n - bx_0}{p} = c + \frac{bx_n - a}{p} \equiv c[p^{n-1}].$$

b) On procède par récurrence sur n avec l'hypothèse suivante
$\forall n \in \mathbb{N}^*$, l'équation $bx \equiv a[p^n]$ admet une unique solution modulo p^n
$x = u_0 + u_1 p + \cdots + u_{n-1}p^{n-1} + X_n p^n$ où $u_i \in [\![0, p-1]\!]$ et ne dépend pas de n.

- Si $n = 1$ on reprend le résultat de la question de la question a.
- $P(n) \Rightarrow P(n+1)$: les solutions de $bx \equiv a[p^{n+1}]$ vérifient $\dfrac{x_{n+1} - u_0}{p}$ solution de $bx \equiv c[p^n]$ où $c = \dfrac{a - bu_0}{p}$ et, d'après l'hypothèse de récurrence, on sait que $\dfrac{x - u_0}{p} = u_1 + u_2 p + \cdots + u_n p^{n-1} + X_{n+1}p^n$ où $u_i \in [\![0, p-1]\!]$, indépendant de n.

On obtient alors $x = u_0 + u_1 p + \cdots + u_n p^n + X_{n+1}p^{n+1}$ où $u_i \in [\![0, p-1]\!]$.
Il reste à prouver l'unicité :

- Tout d'abord, si x et y vérifient $bx \equiv a[p^n]$ et $by \equiv a[p^n]$ alors $p^n|b(x-y)$ donc $p^n|x-y$.
- Ensuite si $\begin{cases} x &= u_0 + u_1 p + \cdots + u_{n-1}p^{n-1} + X_n p^n \\ y &= v_0 + v_1 p + \cdots + v_{n-1}p^{n-1} + Y_n p^n \end{cases}$ alors, compte tenu du premier point, $u_0 + u_1 p + \cdots + u_{n-1}p^{n-1} = v_0 + v_1 p + \cdots + v_{n-1}p^{n-1}$ d'où, par récurrence, $u_0 = v_0$ (reste de la division par p), on simplifie et on divise par p, $u_1 = v_1$ et, de la même façon, $u_i = v_i$.

c) On a $bx = b\left(u_0 + u_1 p + \cdots + u_{n-1}p^{n-1}\right) + bX_n p^n = a + K_n p^n$ d'où, en divisant par b,

$$\frac{a}{b} = u_0 + u_1 p + \cdots + u_{n-1}p^{n-1} + \frac{bX_n - K_n}{b}p^n.$$

Ce qui donne $\nu\left(\dfrac{a}{b} - (u_0 + u_1 p + \cdots + u_{n-1}p^{n-1})\right) = \alpha^n \to 0$ donc on peut écrire

$$\frac{a}{b} = \sum_{n=0}^{+\infty} u_n p^n.$$

Montrons maintenant que la suite est périodique à partir d'un certain rang.
D'après la question b on sait qu'il existe un unique $x_0 \in [\![0, p-1]\!]$ tel que $bx_0 \equiv a[p]$.
On a ainsi $a - bx_0 = pa_1$ (ici $a_1 = c$) donc $\dfrac{a}{b} = x_0 + p\dfrac{a_1}{b}$. On remarque que $x_0 = u_0$ et $|a_1| \leqslant \dfrac{|a|}{p} + |b|$. On résout alors l'équation $bx \equiv a_1[p]$ ce qui va donner $u_1 \in [\![0, p-1]\!]$ comme unique solution.
On utilise alors la récurrence suivante : on pose $a_{k+1} = \dfrac{a_k - bu_k}{p}$ et la résolution de $bx \equiv a_{k+1}[p]$ fournira u_{k+1} :
en effet on a $\dfrac{a}{b} = u_0 + p\dfrac{a_1}{b} = \ldots = u_0 + u_1 p + \cdots + u_k p^k + \dfrac{a_{k+1}}{b}p^{k+1}$.
On prouve ensuite la majoration suivante : $|a_k| \leqslant \dfrac{|a|}{p} + \dfrac{p|b|}{p-1}$ (immédiat lorsqu'on

connaît la majoration) : en fait on montre par récurrence que

$$|a_k| \leqslant \frac{|a|}{p} + |b|\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{k-1}}\right) \leqslant \frac{|a|}{p} + \frac{p|b|}{p-1}.$$

Les entiers relatifs a_k sont dans un ensemble fini donc il existe k et $h > k$ tels que $a_k = a_h$. Il est alors classique de prouver que $a_{k+m} = a_{h+m}$ par récurrence sur m ce qui entraîne $u_{k+m} = u_{h+m}$ et la périodicité de (u_k) à partir d'un certain rang.
Algorithme :

- On cherche $b' \in [\![1, p-1]\!]$ l'inverse de b dans $\mathbb{Z}/p\mathbb{Z}$, soit avec Bézout comme dans la question a, soit en calculant b^{p-1} et en utilisant le petit théorème de Fermat : $b^{p-1} \equiv 1[p]$.
- On effectue la division de $b'a$ par p, ce qui donne u_0.
- On effectue alors la boucle

```
n:=1;
a[0]:=a;
while n<=|a|/p+p*|b|/(p-1) do
  a[n]:=(a[n-1]-b*u[n-1])/p;
  u[n]:=b'*a mod p;
  print(u[n]);
  for i from 0 to n-1
    do if a[i]=a[n] then print(i,n); end;
    od;
  n:=n+1;
od
end;
```

(algorithme non vérifié) et on sait que cet algorithme se termine grâce à la périodicité de la suite (a_n).

d) On a vu que l'on pouvait écrire le rationnel $\dfrac{a}{b}$ sous la forme $p^r\dfrac{a'}{b'}$ avec $p \wedge a' = p \wedge b' = 1$. Il suffit alors d'appliquer la question précédente à la fraction $\dfrac{a'}{b'}$. $u_0 \neq 0$ sinon on pourrait mettre p en facteur dans a' ce qui a été écarté.

e) $a = 1$ et $b = 5$ on trouve la suite périodique (à partir du rang 1)

$$\frac{1}{5} = 1 + 2^2 + 2^3 + 2^6 + 2^7 + \cdots + 2^{2+4n} + 2^{3+4n} + \cdots$$

$a = 5$ et $b = 7$, là c'est un peu plus long mais on trouve

$$\frac{5}{7} = 2 + (2.3^2 + 3^3 + 2.3^4 + 3^6) + \cdots + (2.3^{6n+2} + 3^{6n+3} + 2.3^{6n+4} + 3^{6n+6}) + \cdots$$
$$= 2 - 9\frac{104}{728}.$$

Partie III

(1) On a $\nu(a/b) = \dfrac{\nu(a)}{\nu(b)}$, $\nu(x) = \nu(1)\nu(x) \Rightarrow \nu(1) = 1$ et $\nu(-1) = 1$. On utilise alors la décomposition de tout entier en produit de facteurs premiers :
si $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ alors $\nu(a) = \nu(p_1)^{\alpha_1} \ldots \nu(p_k)^{\alpha_k}$.
Conclusion : il suffit de connaître ν sur l'ensemble des nombres premiers pour connaître ν sur $\mathbb{Q}$.

(2) a) $p^a \wedge q^b = 1$ et on utilise l'égalité de Bézout.

b) On a $\nu(u) \leqslant 1$, $\nu(v) \leqslant 1$ d'où
$$\begin{aligned} 1 = \nu(up^a + vq^b) &\leqslant \nu(u)\nu(p^a) + \nu(v)\nu(q^b) \\ &\leqslant \nu(p)^a + \nu(q)^b. \end{aligned}$$
Si on fait tendre a et b vers $+\infty$, on obtient $1 \leqslant 0$ ce qui est contradictoire.

c) Conclusion : $\nu(p) < 1$ et $\forall q$ premier, $q \neq p$, $\nu(q) = 1$, ν est bien une distance p-adique car $\nu(a/b) = \alpha^r$ où $\dfrac{a}{b} = p^r \dfrac{a'}{b'}$ avec $a' \wedge p = b' \wedge b' = 1$.

(3) a) On a $\nu(x) \leqslant x\nu(1) = x$ par l'inégalité triangulaire et récurrence sur x.

b) On écrit que
$$\begin{aligned} \nu(x) &\leqslant x_0 + x_1 p^a + \cdots + x_n p^{na} \leqslant p(1 + p^a + \cdots + p^{na}) \\ &= p\frac{p^{(n+1)a} - 1}{p^a - 1} \leqslant \frac{p^{a+1}}{p^a - 1}(p^n)^a \end{aligned}$$
et comme $p^n \leqslant x$ alors $(p^n)^a \leqslant x^a$ d'où $\nu(x) \leqslant cx^a$ où $c = \dfrac{p^{a+1}}{p^a - 1}$.

c) $\nu(x) = [\nu(x^m)]^{1/m} \leqslant c^{1/m}[(x^m)^a]^{1/m}$ d'où, pour tout $m \in \mathbb{N}^*$, $\nu(x) \leqslant c^{1/m}x^a$ et en passant à la limite quand $n \to +\infty$, on obtient $\nu(x) \leqslant x^a$ car $\lim\limits_{m \to +\infty} c^{1/m} = 1$.

(4) a) $p^{n+1} = x + y$ donc, par inégalité triangulaire, $\nu(p^{n+1}) \leqslant \nu(x) + \nu(y)$ d'où $\nu(x) \geqslant \nu(p^{n+1}) - \nu(y)$ et comme $\nu(y) \leqslant y^a \leqslant (p^{n+1} - p^n)^a$ alors
$$\nu(x) \geqslant p^{a(n+1)} - (p^{n+1} - p^n)^a = p^{a(n+1)}b.$$

b) Comme $x < p^{n+1}$ alors $\nu(x) > x^a b$ et par le même raisonnement qu'au 3.c, on en déduit que $\nu(x) \geqslant x^a$.
Conclusion ; $\nu(x) = x^a$.
Remarque : comme $\nu(x) \leqslant x$ pour $x \in \mathbb{N}$ alors $x^a \leqslant x$ donc $0 < a \leqslant 1$.

c) On peut alors énoncer le théorème d'Ostrowski :
si l'on excepte la métrique discrète, il n'y a sur $\mathbb{Q}$ que les métriques p-adiques et la métrique classique (si $a < 1$, les distances associées aux métriques $|x|^a$ et $|x|$ sont topologiquement équivalentes).
Il reste quand même à s'assurer que $|x+y|^a \leqslant |x|^a + |y|^a$ pour tout couple $(x, y) \in \mathbb{R}$ et tout $a \in]0, 1]$.
Pour cela, on remarque que $|x + y|^a \leqslant (|x| + |y|)^a$ donc on se ramène au cas où x et y sont positifs. On étudie alors la fonction $g(x) = x^a + y^a - (x + y)^a$ sur $[0, +\infty[$.
$g'(x) = a\left(x^{a-1} - (x + y)^{a-1}\right) \geqslant 0$ (pour $x > 0$) et $g(0) = 0$ d'où le tableau de variation suivant

x	0	$+\infty$
$g'(x)$	—	$+$
$g(x)$	0 $\nearrow$	$+\infty$

donc $g(x) \geqslant 0$ ce qui prouve la relation et permet de conclure.