<- Sommaire Site AP

Retour vers le sommaire de la page sur les nombres décadiques

8-Lien entre entiers, nombres décadiques et entiers, nombres 2-adiques et 5-adiques

Avant de pouvoir faire ce lien, quelques résultats sur les nombres p-adiques (p1er) sont nécessaires : je les donnerai sans démonstration (on les trouvera dans tout ouvrage relatif à la question).

Dans tout ce qui suit p sera un nombre 1er.

P8.1->**On note Q_p le corps (commutatif) des nombres p-adiques** : on peut le munir d'une norme ou valeur absolue, notée $| |_p$ avec les propritétés suivantes :
pour tout x et y dans Q_p on a :

- $|x|_p \geq 0$ et $|x|_p=0 \Leftrightarrow x=0$
- $|x+y|_p \leq \max(|x|_p,|y|_p) \leq |x|_p+|y|_p$
- elle est multiplicative : $|xy|_p=|x|_p|y|_p$
- elle définit une distance sur Q_p : $d_p(x,y)=|x-y|_p$

P8.2->**Z_p est le sous-anneau (unitaire, commutatif) de Q_p constitué des nombres p-adiques de norme ≤ 1 : ce sont les entiers p-adiques**.

P8.3->**Les limites étant prises au sens d_p**, pour n tendant vers $+\infty$, et notées $\lim_p$, on a :

- tout élément e de Z_p s'écrit $\lim_p e_0+e_1p+...+e_np^n$, avec $e_i \in \{0;1;...;p-1\}$, les e_i étant uniques
  - et e est inversible dans $Z_p \Leftrightarrow |e|_p=1 \Leftrightarrow e_0 \neq 0$
- tout élément x de Q_p s'écrit $\lim_p x_{-r}p^{-r}+...+x_{-1}p^{-1}+x_0+x_1p+...+x_np^n$, avec $x_i \in \{0;1;...;p-1\}$, les x_i étant uniques.

P8.4->**Tout élément de Z peut être identifié à un élément de Z_p** : $Z \subset Z_p$
et pour e dans Z, $|e|_p=1/(p^{val(e)})$, avec val(e)=exposant de p dans la décomposition en nombres 1er de e.
Donc $\lim_p p^n=0$.

P8.5->Et enfin une propriété qui va beaucoup servir ci-après :

> Toute suite $(k_n)_{(n\geq 1)}$ d'éléments de Z tels que pour tout $n\geq 1$ on a $0\leq k_n \leq p^n-1$ et $k_{n+1} \equiv k_n$ (p^n), est une suite (**appelée suite cohérente**) qui converge (au sens d_p)
> vers un entier p-adique $e=\lim_p e_0+e_1p+...+e_np^n$ avec $e_0=k_1$ et pour $n\geq 1$, $e_n=(k_{n+1}-k_n)/p^n$.
> (On peut vérifier que tous ces e_i sont bien dans $\{0;1;...;p-1\}$).
>
> Réciproquement, tout entier p-adique est la limite d'une **unique** suite cohérente.

(note perso : $p40_{6/1}$)

Le lien annoncé est le fait que les anneaux EN(10) et $Z_2 \times Z_5$ sont isomorphes ainsi que les anneaux NB(10) et $Q_2 \times Q_5$.
Avant de le prouver (compte-tenu de ce qui vient d'étre rappelé sur les p-adiques), je rappelle la notion de produit d'anneaux.
Rappelons, par exemple, que $Z_2 \times Z_5$ est l'ensemble des couples (a,b) avec a dans Z_2 et b dans Z_5, ensemble structuré par (a,b)+(a'+b')=(a+a',b+b') et (a,b)×(a',b')=(aa',bb') : on vérifie facilement qu'ainsi, le produit de deux anneaux reste un anneau, (0,0) étant le neutre pour l'addition et (1,1) le neutre pour la multiplication. Par contre le produit de deux corps ne sera pas un corps mais seulement un anneau, car ce produit admet des diviseurs de 0 (dont on a vu qu'ils n'admettent pas d'inverse : voir exercice 5 du chapitre 2) : (0,1) et (1,0) sont deux éléments non nuls de $Q_2 \times Q_5$ et leur produit est (0,0)=0, le neutre de l'addition. P8.6->
1) Dans $Z_2 \times Z_5$, comme dans $Q_2 \times Q_5$, les diviseurs de 0 sont (a,b) avec (a=0 et b≠0) ou (a≠0 et b=0)

2) Dans $Q_2 \times Q_5$, les éléments inversibles sont (a,b) avec a et b non nuls

3) Le résultat 2) n'est plus vrai dans $Z_2 \times Z_5$. On a uniquement :
si $(a,b) \in Z_2 \times Z_5$, (a,b) est inversible (dans $Z_2 \times Z_5$) ⇔ a est inversible dans Z_2 et b inversible dans Z_5.
Voir P8.3 pour la caractérisation d'un élément de Z_p inversible dans Z_p.

4) Dans $Q_2 \times Q_5$, x non inversible ⇔ x=(a,b) avec a=0 ou b=0⇔ x=0 ou x diviseur de 0

5) Ce résultat 4) n'est plus vrai dans $Z_2 \times Z_5$.

Exercice 1 : prouver P8.6.

P8.7->**Attention : dans tout l'énoncé ci-dessous de P8.7, p est soit toujours égal à 2, soit toujours égal à 5**.
Soit $x \in EN(10)$: pour tout $n \geq 1$ on définit un unique entier naturel k_n par $k_n \equiv [x]_{n-1}$ (p^n) avec $0 \leq k_n \leq p^n - 1$.
Cette suite $(k_n)_{n\geq 1}$ est une suite cohérente qui converge, dans Q_p au sens de la distance d_p, vers un élément $x^{(p)}$ de Z_p.
En notant f_p l'application de EN(10) dans Z_p qui à x dans EN(10) associe $f_p(x)=x^{(p)}$ (projeté de x sur Z_p), alors
f_p est un homomorphisme surjectif (d'anneau), c'est-à-dire pour tous les entiers décadiques x et y, on a :

$$f_p(x+y)=f_p(x)+f_p(y) \ ; \ f_p(-x)=-f_p(x) \ ; \ f_p(xy)=f_p(x)f_p(y) \ ;$$
et pour tout s dans Z_p il existe x dans EN(10) tel que $f_p(x)=s$

Pour tout x dans Z on a $f_p(x)=x$
Pour tout x dans EN(10), $f_p(x)=0$ ⇔ pour tout $n \geq 1$ p^n divise $[x]_{n-1}$; il existe effectivement x dans NB(10) non nul tel que $f_p(x)=0$. Donc f_p n'est pas injective, donc n'est pas un isomorphisme.

Soit g_p l'application de NB(10) dans Q_p qui à x dans NB(10) associe $g_p(x)=10^{-r}f_p(10^r x)$ où r est un entier naturel quelconque tel que $10^r x$ soit dans EN(10) : **g_p est aussi un homomorphisme surjectif**.

Bien sûr cette définition ne dépend pas du choix de r et **si x est entier décadique alors $g_p(x)=f_p(x)$** (on peut prendre r=0).

Exercice 2 : prouver P8.7

P8.8->Soit f l'application de EN(10) dans $Z_2 \times Z_5$ définie par $f(x)=(f_2(x),f_5(x))$: **f est un isomorphisme d'anneaux** (homomorphisme et bijectif).
De même si g est l'application de NB(10) dans $Q_2 \times Q_5$ définie par $g(x)=(g_2(x),g_5(x))$, alors **g est aussi un isomorphisme d'anneaux**.

Exercice 3 : prouver P8.8

P8.9->
1) Soit $x \in$NB(10) :

x inversible $\Leftrightarrow$ g(x) inversible
x diviseur de 0 $\Leftrightarrow$ g(x) diviseur de 0

2) Soit $x \in$EN(10) :

x inversible $\Leftrightarrow$ f(x) inversible
x diviseur de 0 $\Leftrightarrow$ f(x) diviseur de 0

3) **Soit $x \in$NB(10) : x non inversible $\Leftrightarrow$ x=0 ou x diviseur de 0**

4) **Attention** : si x est dans EN(10) et si x n'est pas inversible dans EN(10) alors, on n'a pas cette fois obligatoirement x=0 ou x diviseur de zéro.

Exemple : d'après P4.2, 70 n'est pas inversible dans EN(10), mais il a un inverse dans NB(10), et pourtant $70 \neq 0$ et 70 n'est pas un diviseur de 0 (puisqu'il est inversible dans NB(10)).

5) $x \in$EN(10) est un diviseur de $0 \Leftrightarrow (f_2(x)=0$ et $f_5(x) \neq 0)$ ou $(f_2(x) \neq 0$ et $f_5(x)=0)$

6) $x \in$NB(10) est un diviseur de $0 \Leftrightarrow (g_2(x)=0$ et $g_5(x) \neq 0)$ ou $(g_2(x) \neq 0$ et $g_5(x)=0)$

7) $x \in$EN(10) est un diviseur de $0 \Leftrightarrow$ $x \neq 0$ et (pour tout $n \in N^*$, 2^n divise $[x]_{n-1}$ ou pour tout $n \in N^*$, 5^n divise $[x]_{n-1}$)

Remarque 1 : le ou est exclusif.

Remarque 2 : tout diviseur de 0 se termine par un chiffre pair ou par 5, la terminaison 0 étant à exclure s'il s'agit d'un nombre décadique ayant effectivement des chiffres après la virgule.

8) **Soient x et y deux entiers décadiques (ou brenoms entiers) non nuls :**

xy=0 (cad x et y sont deux diviseurs de 0 associés)
$$\Leftrightarrow$$
$$(\forall n \in N,\ 2^{n+1} \text{ divise } [x]_n \text{ et } 5^{n+1} \text{ divise } [y]_n) \text{ ou } (\forall n \in N,\ 5^{n+1} \text{ divise } [x]_n \text{ et } 2^{n+1} \text{ divise } [y]_n)$$

Remarque : le ou est exclusif.

On retrouve donc P5.2.

9) Soient α et β deux nombres décadiques diviseurs de 0 associés (α et β non nuls, $\alpha\beta=0$).
Alors pour tout x nombre décadique diviseur de 0 on a $\alpha x=0$ ou (exclusif) $\beta x=0$.

Soient x et y deux diviseurs de 0 quelconques, alors ils sont associés ou (exclusif) ils sont associés chacun à un même 3ième.

Exercice 4 : prouver P8.9

Exercice 5 : en utilisant P8.9, P8.7, P8.5, P8.3 **retrouver P4.3, c'est-à-dire : un entier décadique a un inverse entier décadique ⇔ il se termine par 1 ou 3 ou 7 ou 9**.

P8.10->**Soit P un polynôme à coefficients dans NB(10) de degré n.**
On note, pour p=2 ou p=5, $g_p(P)$ le polynôme obtenu en remplacant les coefficients de P par leurs images par g_p : ainsi $g_p(P)$ est un polynôme à coefficients dans Q_p qui est de degré $\leq$n.
Soit x un nombre décadique (ou brenom) :
x est racine de P ⇔ $g_2(x)$ est racine de $g_2(P)$ et $g_5(x)$ est racine de $g_5(P)$

P a au plus n^2 racines dans NB(10).

Exemple :
c'est celui du chapitre 6) : le polynôme $P(X)=X^2-X$ a quatre racines 0, 1 et a et b entiers décadiques caractérisés par f(a)=(1,0) et f(b)=(0,1) ; a et b vérifient a+b=1, ab=0.

Exercice 6 : prouver P8.10

Exercice 7 : on a vu au chapitre 6 une méthode pour trouver des valeurs approchées de a et b, les racines non triviales de X^2-X.
Trouver deux autres méthodes :

l'une s'inspirant de la preuve de la surjectivité de f_p
l'autre utilisant le théorème des restes chinoix (rappelé lors de la preuve de la surjectivité de f).

Quelle est parmi ces trois méthodes permettant d'obtenir des valeurs approchées de a et b, celle qui semble la plus intéressante pour une programmation?

Solution des exercices du chapitre 8

Exercice 1 : preuve de P8.6
1) Un diviseur de 0=(0,0) de $Z_2\times Z_5$ est tel (a,b) non nul tel qu'il existe (a',b'), non nul, dans $Z_2\times Z_5$ avec (a,b)×(a',b')=(0,0), soit aa'=0 et bb'=0 ; quoique Z_2 et Z_5 ne soient pas des corps, ils sont inclus dans des corps (Q_2 et Q_5), et donc aa'=0 et bb'=0 ⇔ (a=0 ou a'=0) et (b=0 ou b'=0) ; mais comme a et b ne sont pas tous les deux nuls, ainsi que a' et b' , c'est qu'on (a=0 et b≠0 et a'≠0 et b'=0) ou (a≠0 et b=0 et a'=0 et b'≠0) ; donc nécessairement on a (a=0 et b≠0) ou (a≠0 et b=0). Réciproquement si on a cette condition, on peut effectivement trouver (a',b') non nul tel que (a,b)×(a',b')=0.

Même raisonnement pour les diviseurs de 0 dans $Q_2\times Q_5$.

2) Un élément (a,b) de $Q_2\times Q_5$ est inversible signifie qu'il existe (a',b') dans dans $Q_2\times Q_5$ avec (a,b)×(a',b')=(1,1), ce qui équivaut à aa'=1 et bb'=1, donc à a et b inversibles (respectivement dans Q_2 et Q_5) ; mais Q_2 et Q_5 sont des corps, et cette dernière condition équivaut à a et b non nuls.

3) Par le même raisonnement que celui fait au 2), on voit qu'un élément de $Z_2\times Z_5$ est inversible dans $Z_2\times Z_5$ équivaut à a inversible dans Z_2 et b inversible dans Z_5, mais là on ne peut dire que cela équivaut à a et b non nuls car Z_2 et Z_5 ne sont pas des corps.

4) Cf le 2) un élément (a,b) de $Q_2\times Q_5$ est non inversible équivaut à a=0 ou b=0, donc soit a=b=0, et x=0, soit (a=0 et b≠0) ou (a≠0 et b=0), et x est diviseur de 0 cf le 2ième résultat ci-dessus.

5) Ce résultat 4) n'est plus vrai si on remplace $Q_2\times Q_5$ par $Z_2\times Z_5$ à cause du 3).

<u>Exercice 2</u> : preuve de P8.7

Soit $x \in EN(10)$: pour $n \geq 1$ on pose $k_n \equiv [x]_{n-1}$ (p^n) avec $0 \leq k_n \leq p^n-1$.

Il s'agit de montrer que cette suite converge, dans Q_p au sens de la distance d_p, vers un élément $x^{(p)}$ de Z_p.

On a $k_{n+1} \equiv [x]_n$ (p^{n+1}) et ainsi $k_n=[x]_{n-1}+Kp^n$ et $k_{n+1}=[x]_n+K'p^{n+1}$ avec K et K' dans Z ; comme on a $[x]_n=x_n10^n+[x]_{n-1}$, $k_{n+1}-k_n=x_n10^n+K'p^{n+1}-Kp^n$.

Comme p=2 ou p=5, $10 \equiv 0$ (p) et $10^n \equiv 0$ (p^n) et ainsi $k_{n+1}-k_n \equiv 0$ (p^n).

Cette suite k_n vérifie les hypothèses de P8.5 : **c'est donc une suite cohérente** et elle converge donc, au sens d_p, vers un élément $x^{(p)}=f_p(x)$ de Z_p.

Montrons que f_p est surjectif.

Soit s dans Z_p : donc $s=\lim_p k_n$, avec k_n suite cohérente.

Il s'agit de montrer qu'il existe (au moins) un entier décadique x tel que $f_p(x)=s$.

Par définition, $f_p(x)=\lim_p k'_n$ avec, pour tout $n \geq 1$, $k'_n \equiv [x]_{n-1}$ (p^n) et $0 \leq k'_n \leq p^n-1$; et, on vient de le voir, cette suite k'_n est une suite cohérente.

Dire que $f_p(x)=s$, c'est dire que les deux suites cohérentes k_n et k'_n ont la même limite, d'où, cf l'unicité (voir P8.5), ceci est équivalent à ce que pour tout $n \geq 1$, on a $k_n=k'_n$, soit $[x]_{n-1} \equiv k_n$ (p^n), car $k_n=k'_n \Leftrightarrow k_n \equiv k'_n$ (p^n), puisque ces deux entiers sont dans $\{0;1;...;p^n-1\}$.

Il s'agit donc de voir, les k_n étant donnés, si on peut trouver x dans NB(10) tel que pour tout $n \geq 1$ on ait $[x]_{n-1} \equiv k_n$ (p^n).

> n=1 donne $x_0 \equiv k_1$ (p) : donc il y a une solution x_0 dans $\{0;1;...;p-1\}$ (rappel p=2 ou 5, donc cet x_0 est bien dans $\{0;1;...;9\}$; il y a une autre solution x_0+p, qui reste dans $\{0;1;...;9\}$).
>
> Pour $n \geq 1$, supposons $x_0,...,x_{n-1}$ obtenus de telle sorte que $"x_{i-1}...x_0" \equiv k_i$ (p^i) soient vérifiées pour i=1,2,...n.
>
> ($"x_{i-1}...x_0"$ désigne l'entier naturel dont les chiffres sont, à partir de la gauche, $x_{i-1},...,x_0$)
>
> Cherchons x_n tel que $"x_n...x_0" \equiv k_{n+1}$ (p^{n+1}), soit :
>
> $10^nx_n+"x_{n-1}...x_0" \equiv k_{n+1}$ (p^{n+1}), soit
>
> $10^nx_n \equiv k_n-"x_{n-1}...x_0"+k_{n+1}-k_n$ (p^{n+1})
>
> mais p^n divise $k_{n+1}-k_n$, cf suite cohérente, et divise $k_n-"x_{n-1}...x_0"$, cf hypothèse de récurrence, et enfin il divise aussi 10^n ; d'où en notant q_n le membre de droite divisé par p^n, x_n est caractérisé par $(10/p)^nx_n \equiv q_n$ (p) ; comme 10/p est 1er avec p (si p=2, 10/p=5 et si p=5, 10/p=2), $(10/p)^n$ a un inverse modulo p et il existe une unique solution x_n dans $\{0;1;...;p-1\}$, solution qui est dans $\{0;1;...;9\}$; mais dans $\{0;1;...;9\}$ il y a d'autres possibilités que cet x_n : si p=5 il y a x_n+5, si p=2 il y a x_n+2, x_n+4, x_n+6, x_n+8.
>
> Donc par récurrence, on montré que pour tout $n \geq 1$, il existe $x_0,...,x_{n-1}$ tels que $"x_{i-1}...x_0" \equiv k_i$ (p^i) soient vérifiées pour i=1,2,...n.

Donc en notant x l'entier décadique x dont les chiffres sont ces x_i, on a pour tout $n \geq 1$, $[x]_{n-1} \equiv k_n$ (p^n), soit $f_p(x)=s$.

Montrons tout de suite que pour tout x dans Z on a $f_p(x)=x$.

1er cas : x dans N

Pour n assez grand, $[x]_{n-1}=x$ et ainsi $k_n \equiv x$ (p^n) ; mais pour n assez grand on aura aussi $0 \leq x \leq p^n-1$ et donc, à partir d'un certain rang on a toujours $k_n=x$, donc $\lim_p k_n=x$ (suite constante à partir d'un certain rang), soit $f_p(x)=x$.

2ième cas : -x dans N

Posons y=-x ; $[x]_{n-1}=[-y]_{n-1} \equiv -[y]_{n-1}$ (10^n), d'après P2.4.

Comme pour n assez grand $[y]_{n-1}=y$ on a $[x]_{n-1} \equiv x$ (10^n), soit $[x]_{n-1}=x+K10^n$, avec K dans Z. Mais on a vu plus haut que $10^n \equiv 0$ (p^p) et donc $k_n \equiv x$ (p^n) ; mais cette fois on n'a pas $0 \leq x \leq p^n-1$ et donc on ne peut

dire que $k_n=x$ à partir d'un certain rang.
En fait on peut écrire $k_n-x=Kp^n$, avec K dans Z et dépendant de n ; donc $|k_n-x|_p=|Kp^n|_p=1/(p^r)$, avec r exposant de p dans la décomposition en nombres 1er de Kp^n (voir P8.4), donc $r\geq n$ et ainsi $|k_n-x|_p\leq 1/p^n$, quantité qui tend vers 0, au sens habituel, si n tend vers $+\infty$: cela signifie que $\lim_p k_n=x$ donc on a encore $f_p(x)=x$.

Montrons que $f_p(x+y)=f_p(x)+f_p(y)$, pour x et y entiers décadiques quelconques.
$f_p(x+y)=\lim_p k''_n$ avec $k''_n\equiv[x+y]_{n-1}$ (p^n) et $0\leq k''_n\leq p^n-1$
$f_p(x)=\lim_p k_n$ avec $k_n\equiv[x]_{n-1}$ (p^n) et $0\leq k_n\leq p^n-1$
$f_p(y)=\lim_p k'_n$ avec $k'_n\equiv[y]_{n-1}$ (p^n) et $0\leq k'_n\leq p^n-1$
Cf D1.2, pour $n\geq 1$, on a $[x+y]_{n-1}=[x]_{n-1}+[y]_{n-1}-K\times 10^n$, avec K=0 ou 1.
Comme $10^n\equiv 0$ (p^n), on a $k''_n\equiv k_n+k'_n$ (p^n), soit $k''_n-k_n-k'_n=Kp^n$ avec K dans Z et $|k''_n-(k_n+k'_n)|_p=|Kp^n|_p=1/(p^r)$, avec r exposant de p dans la décomposition en nombres 1er de Kp^n (voir P8.4), donc $r\geq n$ et ainsi $|k''_n-(k_n+k'_n)|_p\leq 1/p^n$, quantité qui tend vers 0, au sens habituel, si n tend vers $+\infty$: cela signifie que $\lim_p k''_n-(k_n+k'_n)=0$ donc $\lim_p k''_n=\lim_p (k_n+k'_n)=\lim_p k_n+\lim_p k'_n$, soit $f_p(x+y)=f_p(x)+f_p(y)$.

Montrons que $f_p(-x)=-f_p(x)$.
$f_p(x+(-x))=f_p(x)+f_p(-x)$, cf le résultat précédent. Mais on a aussi $f_p(x+(-x))=f_p(0)=0$ (puisque $f_p(x)=x$, pour x dans Z) et donc $f_p(x)+f_p(-x)=0$, ce qui prouve le résultat annoncé
<u>Remarque</u> :
ce résultat, combiné avec le précédent et le fait que $f_p(x)=x$ pour x dans N, permet de démontrer que $f_p(x)=x$ pour -x dans N.
En effet puisque -x est dans N, $f_p(-x)=-x$, soit $-f_p(x)=-x$ et $f_p(x)=x$, ce qui donne une preuve plus rapide que celle ci-dessus (voir 2ième cas de $f_p(x)=x$).

Montrons que $f_p(xy)=f_p(x)f_p(y)$.
Une fois n'est pas coutume, la preuve est laissée au lecteur : même technique que pour la somme.

Montrons que pour tout x dans NB(10), $f_p(x)=0 \Leftrightarrow$ pour tout $n\geq 1$ p^n divise $[x]_{n-1}$.
Cf P8.5 et la définition de $f_p(x)$ on a $f_p(x)=\lim_p e_0+e_1p+...+e_np^n$ avec $e_0=k_1$ et pour $n\geq 1$, $e_n=(k_{n+1}-k_n)/p^n$ et $k_n\equiv[x]_{n-1}$ (p^n).
Et cf l'unicité des e_i (voir P8.3), on a $f_p(x)=0\Leftrightarrow$ pour tout $i\geq 0$ $e_i=0$ $\Leftrightarrow$ pour tout $n\geq 1$ $k_n=0$ $\Leftrightarrow$pour tout $n\geq 1$ $[x]_{n-1}\equiv 0$ (p^n) $\Leftrightarrow$pour tout $n\geq 1$ p^n divise $[x]_{n-1}$.
On aurait pu utiliser la preuve de la surjectivité de f_p.

Montrons qu'il existe effectivement un entier décadique non nul tel que $f_p(x)=0$.

En utilisant la preuve de la surjectivité de f_p, en y faisant s=0 (donc les k_n son nuls), on voit qu'il existe x entier décadique tel que $f_p(x)=0$ en prenant x_0 quelconque tel que $x_0\equiv 0$ (p), donc par exemple $x_0=p$, et cet x est alors non nul.

Montrons que g_p est aussi un homomorphisme
Il faut cependant vérifier que la définition de $g_p(x)$ ne dépend pas du choix de r.
Soient r et r' deux entiers naturels tels que 10^rx et $10^{r'}x$ soient entiers décadiques : $10^{-r}f_p(10^rx)=10^{-r}f_p(10^{r-r'}\times 10^{r'}x)$, et comme f_p est un homomorphisme on a $10^{-r}f_p(10^rx)=10^{-r}f_p(10^{r-r'})f_p(10^{r'}x)=10^{-r'}f_p(10^{r'}x)$, puisque $f_p(x)=x$ pour x dans Z.

Montrons maintenant que $g_p(x+y)=g_p(x)+g_p(y)$, $g_p(-x)=-g_p(x)$, $g_p(xy)=g_p(x)g_p(y)$.
Soient r et r' deux entiers naturels tels que 10^rx et $10^{r'}y$ soient entiers décadiques : on a alors $g_p(x)=10^{-r}f_p(10^rx)$ et $g_p(y)=10^{-r'}f_p(10^{r'}y)$, mais quitte à augmenter l'un (ce qui ne changera pas le g_p correspondant, cf ce qui précéde) on peut supposer r=r'.

Ainsi $10^r(x+y)$ est entier décadique et
$g_p(x+y)=10^{-r}f_p(10^r(x+y))=10^{-r}(f_p(10^rx)+f_p(10^ry))=g_p(x)+g_p(y)$.

En faisant y=-x dans la relation ci-dessus et en remarquant que $g_p(0)=f_p(0)=0$ on obtient $g_p(-x)=-g_p(x)$.

Pour l'image du produit on remarque que $10^rx\times10^ry=10^{2r}xy$ est entier décadique et
$g_p(xy)=10^{-2r}f_p(10^{2r}xy)=10^{-2r}f_p(10^rx)f_p(10^ry)=(10^{-r}f_p(10^rx))(10^{-r}f_p(10^ry))=g_p(x)g_p(y)$.

Montrons que g_p est surjectif.
Soit q dans Q_p : il faut montrer l'existence d'un nombre décadique tel que $g_p(x)=10^{-r}f_p(10^rx)=q$, avec 10^rx dans EN(10).
On sait qu'on peut augmenter r sans changer $g_p(x)$: si nécessaire, augmentons alors r de telle sorte que $10^rq=s$ soit dans Z_p (cela se justifie à l'aide de P8.3, puisque $10=2\times5$ et que p est soit 2, soit 5).
Donc on doit avoir $f_p(10^rx)=s$: comme f_p est surjective il existe u entier décadique y tel que $f_p(y)=s$ et on prend $x=10^{-r}y$.

<u>**Exercice 3**</u> : preuve de P8.8
Il s'agit de montrer que f application de EN(10) dans $Z_2\times Z_5$ est un isomorphisme d'anneaux.
f est définie par $f(x)=(f_2(x),f_5(x))$.

Le fait que f soit un homorphisme d'anneaux est une conséquence directe du fait que f_2 et f_5 sont des homomorphismes (il suffit de l'écrire).

Montrons que f est injective.
Il s'agit de montrer que f(x)=f(y) entraîne x=y.
f(x)=f(y) équivaut à $f_2(x)=f_2(y)$ et $f_5(x)=f_5(y)$.
On a $f_2(x)=\lim_2 k_n$, $f_5(x)=\lim_2 k'_n$, $f_2(y)=\lim_2 K_n$, $f_5(y)=\lim_5 K'_n$, les quatre suites k_n, k'_n, K_n, K'_n étant cohérentes.
Puisque $f_2(x)=f_2(y)$ et compte-tenu de l'unicité (voir P8.5) c'est que pour tout $n\geq1$ on a $k_n=k'_n$ et donc $[x]_{n-1}\equiv[y]_{n-1}$ (2^n), cf la définition de k_n et k'_n.
De même $[x]_{n-1}\equiv[y]_{n-1}$ (5^n) et comme 2^n et 5^n sont 1er entre eux c'est que $[x]_{n-1}\equiv[y]_{n-1}$ $(2^n\times5^n=10^n)$; mais $[x]_{n-1}$ et $[y]_{n-1}$ sont dans $\{0;1;...;10^n-1\}$, cf D1.1, et donc $[x]_{n-1}=[y]_{n-1}$, cela pour tout $n\geq1$: donc x=y.
Montrons la surjectivité
Il s'agite de montrer que tout élément de $Z_2\times Z_5$ est atteint par f.
Soit (s,t) un élément quelconque de $Z_2\times Z_5$: on cherche x entier décadique tel que f(x)=(s,t).
d'après la réciproque de P8.5
$s=\lim_2 k_n$ avec pour tout $n\geq1$: $0\leq k_n\leq2^n-1$ et $k_{n+1}\equiv k_n$ (2^n)
$t=\lim_2 k'_n$ avec pour tout $n\geq1$: $0\leq k'_n\leq5^n-1$ et $k'_{n+1}\equiv k'_n$ (5^n)
On va utiliser le **théorème dit des restes chinoix**

> a et b étant deux entiers relatifs premiers entre eux, x_0 et x des entiers relatifs quelconques, les solutions du systéme (d'inconnue x) :
>
> $x\equiv x_0$ (a)
> $x\equiv x_1$ (b)
>
> sont les entiers relatifs x tels que $x\equiv aux_1+bvx_0$ (ab) avec u tel que $au\equiv1$ (b) et v tel que $bv\equiv1$ (v) ; en fait il suffit de choisir "un" u et "un" v tels que au+bv=1, l'existence d'un tel couple étant assurée par le théorème de Bezout.
> Donc ce systéme admet une seule solution dans {0;1;...;ab-1}.

<u>Application</u> : pour tout $n\geq1$, il existe un et un seul entier naturel u_n tel que $u_n\equiv k_n$ (2^n) et $u_n\equiv k'_n$ (5^n) et u_n dans $\{0;1;...;10^n-1\}$.
Cet u_n a donc au plus n chiffres, et quitte à mettre des zéros devant il en a n+1. Par ailleurs

u_{n+1}-u_n≡k_{n+1}-k_n≡0 (2^n) ; de même u_{n+1}-u_n≡0 (5^n) et, 2^n et 5^n étant 1er entre eux, u_{n+1}≡u_n (10^n) : donc u_{n+1}, qui a n+1 chiffres (quitte à rajouter des zéros devant), se termine par les n chiffres de u_n.
On peut alors appliquer la réciproque énoncée en fin de D1.1 : il existe un et un seul entier décadique tel que pour tout n≥ 0 $[x]_n$=u_{n+1}.
Cet entier décadique vérifie donc, pour tout n≥1 $[x]_{n-1}$≡k_n (2^n), donc f_2(x)=s et $[x]_{n-1}$≡k'_n (5^n), donc f_5(x) =t et ainsi f(x)=(s,t).
<u>Remarque</u> : f étant surjective, on retrouve le fait que f_2 et f_5 le sont aussi.

Montrons que g application de NB(10) dans Q_2×Q_5 est un isomorphisme d'anneaux.
L'aspect homomorphisme est immédiat, g_2 et g_5 étant des homomorphismes.
Montrons que g est injective
Supposons g(x)=g(y) :
donc $10^{-r}f_2(10^rx)=10^{-r'}f_2(10^{r'}y)$ et $10^{-r}f_5(10^rx)=10^{-r'}f_5(10^{r'}y)$, avec 10^rx et $10^{r'}y$ dans EN(10).
En fait quitte à augmenter r ou r' (ca ne change pas les g_p correspondants), on peut supposer r=r', donc on a $f_2(10^rx)=f_2(10^ry)$ et $f_5(10^rx)=f_5(10^ry)$, soit $f(10^rx)=f(10^ry)$ donc $10^rx=10^ry$ car f injective et ainsi on a bien x=y et g est injective.

Montrons que g est surjective
Soit (q,q') dans Q_2×Q_5 : il faut montrer l'existence d'un nombre décadique tel que g(x)=(q,q'), soit x tel que $10^{-r}f_2(10^rx)$=q et $10^{-r}f_5(10^rx)$=q' avec 10^rx dans EN(10).
Là aussi (voir preuve de la surjectivité de g_p) on peut choisir r assez grand pour que 10^rq=s et 10^rq'=t soient respectivement dans Z_2 et dans Z_5 : il faut alors trouver x tel que $f_2(10^rx)$=s et $f_5(10^rx)$=t, soit f (10^rx)=(s,t) ; comme f est surjective il existe un entier décadique y tel que f(y)=(s,t) et on prend $x=10^{-r}y$.

<u>**Exercice 4**</u> : preuve de P8.9
1) Si x est inversible, c'est qu'il existe y dans NB(10) tel que xy=1, donc g(xy)=g(1), g(x)g(y)=1 et g(x) est inversible, d'inverse g(y) ;
si g(x) est inversible, c'est qu'il existe U∈Q_2×Q_5 tel que g(x)U=1 ; mais g est bijective, donc il existe y dans NB(10) tel que g(y)=U et g(x)g(y)=1, soit g(xy)=g(1) et xy=1, donc x est inversible.
Si x est diviseur de 0 alors x≠0 et il existe y≠0 avec xy=0, donc g(xy)=g(0), soit g(x)g(y)=0, et commme g est bijective, g(x) et g(y) sont non nuls et ainsi g(x) est diviseur de 0 ;
si g(x) est diviseur de 0, alors g(x)≠0, et donc x≠0, et il existe U≠0 tel que g(x)U=0 ; mais il existe y dans NB(10) tel que g(y)=U, donc y≠0, et g(x)g(y)=0, soit g(xy)=g(0) et ainsi xy=0, soit x diviseur de 0.

2) Preuve analogue à celle ci-dessus.

3) soit x∈NB(10) :
x non inversible⇔g(x) non inversible, d'après le 1) ci-dessus, ⇔g(x)=0 ou g(x) diviseur de 0, d'après le 4) de P8.6, ⇔x=0 ou x diviseur de 0, d'après le 1) ci-dessus.

4) Tout a été dit dans l'énoncé.

5) x dans EN(10) est un diviseur de 0 signifie que x est non nul et qu'il existe y dans EN(10) non nul tel que xy=0.
Mais f étant un homomorphsime de EN(10) dans Z_2×Z_5, on a f(x)f(y)=f(xy)=f(0)=0 et comme f est bijectif, f(u)≠0⇔u≠0, et donc f(x) et f(y) sont non nuls et ainsi f(x) est diviseur de 0.
Réciproquement si f(x) est diviseur de 0, il est non nul , donc x aussi et il existe U non nul dans Z_2×Z_5 tel que f(x)×U=0 ; mais f est bijectif donc U=f(y) avec y dans EN(10) non nul et f(x)f(y)=0, soit f(xy)=0 et xy=0, avec x et y non nuls : x est diviseur de 0.
Donc x diviseur de 0 dans EN(10)⇔f(x) diviseur de 0 dans Z_2×Z_5.
Il n'y a plus qu'à appliquer le 1er résultat de P8.6 en remarquant que f(x)=(f_2(x),f_5(x)).

6) Démonstration analogue pour les diviseurs de 0 de NB(10), g étant aussi un isomorphisme.

7) En fait le 1er résultat de P8.9 ci-dessus peut s'écrire
x diviseur de 0 dans EN(10)$\Leftrightarrow$x$\neq$0 et (f_2(x)=0 ou f_5(x)=0), car x$\neq$0 et f_2(x)=0 entraîne f_5(x)$\neq$0 sinon on aurait f(x)=0 et alors x=0, et aussi f_2(x)=0 et f_5(x)$\neq$0 entraîne x$\neq$0 et f_2(x)=0 ; idem si on remplace 2 par 5.
Il suffit alors d'appliquer le résultat de P8.7 relatif à f_p(x)=0.

Justification du fait que le ou est exclusif : si on avait
(pour tout n$\in$N, 2^{n+1} divise $[x]_n$ et 5^{n+1} divise $[y]_n$) et (pour tout n$\in$N, 5^{n+1} divise $[x]_n$ et 2^{n+1} divise $[y]_n$), alors pour tout n$\geq$0, 10^{n+1} diviserait $[x]_n$, donc $[x]_n$ serait nul et donc on aurait x=0, ce qui est exclu.

Quant au dernier chiffre, ce résultat 7) entraîne que, pour un entier décadique diviseur de 0, 2 ou 5 divise x_0 et donc le dernier chiffre est bien pair ou égal à 5 ; par contre s'il agit d'un nombre décadique diviseur de 0 avec r$\geq$1 chiffres après la virgule (par définition son dernier chiffre x_{-r} est non nul), en le multipliant par 10^r on obtient un entier décadique (de dernier chiffre x_{-r}) diviseur de 0 et donc x_{-r} est pair (0 exclu) ou égal à 5.

8) xy=0$\Leftrightarrow$f(x)f(y)=0$\Leftrightarrow$($f_2(x)f_2(y)$,$f_5(x)f_5(y)$)=0 $\Leftrightarrow$ $f_2(x)f_2(y)$=0 et $f_5(x)f_5(y)$=0 ; mais f_2(x) et f_5(x) ne peuvent être tous les deux nuls (sinon f(x)=0 et x=0, ce qui est exclu), de même f_2(y) et f_5(y) ne peuvent être tous les deux nuls et donc il n'y a que deux possibilités :
f_2(x)=0 et f_5(y)=0 (et donc f_5(x) et f_2(y) sont non nuls car x et y sont non nuls)
ou
f_5(x)=0 et f_2(y)=0 (et donc f_2(x) et f_5(y) sont non nuls car x et y sont non nuls)
ce qui donne le résultat annoncé, compte-tenu, là encore, du résultat de P8.7 relatif à f_p(x)=0.

Justification du fait que le ou est exclusif : résulte du 7) ;

9) C'est une application directe du 7) et du 8).
<u>1er cas</u> : α, β, x sont entiers décadiques.

> Quitte à changer α et β, on peut supposer, cf le 7), que pour tout n$\geq$0 2^{n+1} divise $[\alpha]_n$ et que pour tout n$\geq$0 5^{n+1} divise $[\beta]_n$.
> Et, cf le 7), puisque x est un diviseur de 0, c'est que pour tout n$\geq$0 2^{n+1} divise $[x]_n$ ou (exclusif) que pour tout n$\geq$0 5^{n+1} divise $[x]_n$; donc cf le 8), αx=0 ou (exclusif) βx=0 .

<u>2ième cas</u> : α, β, x ne sont pas tous entiers décadiques.

> Il existe alors r$\geq$1 tel que $\alpha'=10^r\alpha$, $\beta'=10^r b$, $x'=10^r x$ soient tous entiers décadiques.
> Comme $\alpha\beta$=0 entraîne $\alpha'\beta'$=0 et que x' reste un diviseur de 0, on peut appliquer le 1er cas :
> $\alpha'x'$=0 ou (exclusif) $\beta'x'$=0, et puisque 10^{2r}u=0 entraîne u=0, on a αx=0 ou (exclusif) βx=0.

Soient x et y deux diviseurs de 0 ; en particulier il existe z$\neq$0 tel que xz=0.
Le résultat précédent donne alors tout de suite : xy=0 (donc x et y associés) ou (exclusif) zy=0 (donc x et z associés à un même 3ième).

<u>Exercice 5</u> : il s'agit de retrouver P4.3.
Soit x dans EN(10) :
x inversible dans EN(10)$\Leftrightarrow$ f(x) inversible (dans $Z_2\times Z_2$), d'après le 2) de P8.9
$\Leftrightarrow$ f_2(x) inversible dans Z_2 et f_5(x) inversible dans Z_5, d'après le 3) de P8.6
mais $f_2(x)=\lim_2 e_0+e_1 2+...+e_n 2^n$, avec $e_0=k_1\equiv[x]_0=x_0$ (2) et $e_0\in\{0;1\}$, d'après P8.7 et P8.5 ;
et d'après P8.3, f_2 est inversible dans $Z_2$$\Leftrightarrow$$e_0\neq0$ $\Leftrightarrow$ 2 ne divise pas x_0,
de même, f_5(x) est inversible dans Z_5 $\Leftrightarrow$ 5 ne divise pas x_0
et donc x est inversible dans EN(10) $\Leftrightarrow$ x_0 n'est pas divisible par 2, ni par 5, ce qui équivaut à x_0 se termine par 1 ou 3 ou 7 ou 9.

<u>Exercice 6</u> : preuve de P8.10
Le polynôme $g_p(P)$ est de degré≤n, car $g_p(c)$ peut être nul, sans que c le soit.

x, dans NB(10), sera une racine de P⇔ P(x)=0⇔ g(P(x))=0=(0,0), puisque g est un isomorphisme.
Or $g(P(x))=(g_2(P(x)),g_5(P(x))=(g_2(P)(g_2(x)),g_5(P)(g_5(x))$, puisque g_2 et g_5 sont des homomorphismes et de part la définition de $g_2(P)$ et $g_5(P)$.
Donc x racine de P équivaut à $g_2(P)(g_2(x))=0$ et $g_5(P)(g_5(x))=0$.

Comme $g_2(P)$ et $g_5(P)$, sont des polynômes à coefficients dans un corps (Q_2 et Q_5), leurs nombres de racines dans ce corps est ≤ à leur degré qui est ≤n, donc chacun des ces polynômes a au plus n racines et donc il y a au plus n possibilités pour $g_2(x)$, de même pour $g_5(x)$, et donc il y a au plus n×n possibilités pour $g(x)=(g_2(x),g_5(x))$; et comme g est une bijection, il y a au plus n^2 possibilités pour x.

cas de $P(X)=X^2$-X
Cf la résultat ci-dessus, x, dans NB(10), est racine de P, équivaut à $g_2(P)(g_2(x))=0$ et $g_5(P)(g_5(x))=0$; mais ici $g_2(P)=P$ et $g_5(P)=P$. Donc x racine de P équivaut à $g_2(x)(g_2(x)-1)=0$ ou $g_5(x)(g_5(x)-1)=0$ et comme Q_2 et Q_5 cela donne $g_2(x)=0$ ou 1 et $g_5(x)=0$ ou 1. Finalement x racine de P⇔g(x)=(0,0) ou (0,1) ou (1,0) ou (1,1) ; comme g est une bijection P a quatre racines, les antécédents (uniques) de ces quatre couples :

> x tel que g(x)=(0,0) : c'est 0 puisque g(0)=(0,0) (pour x dans NB(10), $g_p(x)=f_p(x)$ et pour x dans Z, cas de x=0, $f_p(x)=x$)
> x tel que g(x)=(1,1) c'est 1 puisque g(1)=(1,1)
> x tel que g(x)=(1,0) : notons là a : $g_2(a)=1$ et $g_5(a)=0$ (donc a n'est pas nul car sinon $g_2(a)=0$)
> x tel que g(x)=(0,1) : notons là b : $g_2(b)=0$ et $g_5(b)=1$ (donc b n'est pas nul)

En fait (1,0) est dans $Z_2×Z_5$, et f étant une bijection, il existe un seul entier décadique a' tel que f(a')=(0,1) ; mais pour x entier décadique on a g(x)=f(x) et ainsi g(a')=(1,0)=g(a) et, g étant aussi une bijection, c'est que a=a' :
et ainsi f(a)=(1,0), soit $f_2(a)=1$ et $f_5(a)=0$.
De même f(b)=(0,1) et $f_2(b)=0$ et $f_5(b)=1$.

f étant un homomorphisme, f(a+b)=f(a)+f(b)=(1,0)+(0,1)=(1,1)=f(1) et donc a+b=1 ;
de même f(ab)=f(a)f(b)=(1,0)(0,1)=(0,0)=f(0) et ab=0.
<u>Remarque</u> :
Cf la preuve de la surjectivité de f on a, pour tout n≥1, $[a]_{n-1}\equiv 1$ (2^n) et $[a]_{n-1}\equiv 0$ (5^n), car $s=1=\lim_2 k_n$ avec $k_n=1$ et $t=0=\lim_5 k'_n$ avec $k'_n=0$. En fait la dernière congruence est aussi une conséquence du résultat sur $f_p(x)=0$ de P8.7.
Donc, en particulier 2 divise a_0-1 et 5 divise a_0, ce qui donne $a_0=5$ et a se termine par 5.
De même, pour tout n≥1, $[b]_{n-1}\equiv 0$ (2^n) et $[b]_{n-1}\equiv 1$ (5^n).
Donc 2 divise b_0 et 5 divise b_0-1, ce qui donne $b_0=6$ et b se termine par 6.

<u>Exercice 7</u> : détermination de valeurs approchées de a et b.
Rappelons que a est caractérisé par $f_2(a)=1$ et $f_5(a)=0$, donc puisque $s=1=\lim_2 k_n$ avec $k_n=1$, et $t=0=\lim_2 k'_n$ avec $k'_n=0$,
a est caractérisé par : pour tout n≥1, $[x]_{n-1}\equiv 1$ (2^n) et $[x]_{n-1}\equiv 0$ (5^n). (Bien entendu, pour la dernière congruence on pouvait utiliser directement la caractérisation de $f_p(x)=0$, voir P8.7).
<u>1ière méthode</u> : on applique directement ces deux relations, en commencant par la 2ième, car modulo 5 on n'aura que deux solutions dans {0;1;...;9} et on regarde celle qui convient pour la 1ière congruence.
n=1 donne $x_0\equiv 1$ (2) et $x_0\equiv 0$ (5) ; la 2ième donne $x_0=0$ ou 5, et seul 5 vérifie la 1ière et $\mathbf{x_0=5}$
n=2 donne $10x_1+5\equiv 1$ (4) et $10x_1+5\equiv 0$ (25), soit

$5x_1 \equiv -2$ (2) et $2x_1 \equiv -1$ (5), soit $x_1 \equiv 0$ (2) et $x_1 \equiv 2$ (5) : la 2ième donne $x_1=2$ ou 7 et seul 2 vérifie la 1ière et $\mathbf{x_1=2}$

n=3 donne $100x_2+25 \equiv 1$ (8) et $100x_2+25 \equiv 0$ (125), soit

$25x_2 \equiv -6$ (2) et $4x_2 \equiv -1$ (5), soit $x_2 \equiv 0$ (2) et $x_2 \equiv 1$ (5) : la 2ième donne $x_1=1$ ou 6 et seul 6 vérifie la 1ière et $\mathbf{x_2=6}$

etc.....

2ième méthode : on utilise le théorème sur les restes chinoix.
On peut obtenir directement $[x]_2$ (par exemple) : en effet on a $[x]_2 \equiv 1$ (8) et $[x]_2 \equiv 0$ (125).
On va alors chercher la solution générale de ce système et prendre la solution qui est dans {0;1;...;999}.
On cherche u et v tels que 8u+125v=1 (peuvent s'obtenir en remontant l'algorithme d'Euclide) : u=47, v=-3 est un couple solution et donc $[x]_2=8\times47\times0+125\times(-3)\times1+8\times125\times k$, avec k dans Z, soit $[x]_2=-375+1000k$ et la seule façon d'avoir $[x]_2$ dans {0;1;...;999} est k=1 et $\mathbf{[x]_2=625}$.

Commentaire sur les méthodes :
D'un point de vue programmation, la méthode vue au chapitre 6 présente le gros inconvénient de faire intervenir $([x]_n)^2$ pour trouver x_{n+1} et donc on va manipuler de grands entiers ce qui va poser des problèmes de capacité.
La méthode utilisant le théorème des restes chinoix permet certes de trouver "d'un seul coup" $[x]_n$, mais là aussi on va manipuler (à un degré peut être moindre) de grands nombres, notamment 2^n et 5^n.
C'est la 1ère méthode ci-dessus qui me semble la plus appropriée pour une programmation, puisqu'on travaille toujours au niveau des chiffres et toujours modulo 2 et 5 : on n'a jamais de grands nombres à manipuler, d'autant plus qu'en fait on va faire des divisions par 2^n et 5^n pour obtenir x_n.

retour début du chapitre 8

Retour vers le sommaire de la page sur les nombres décadiques

<- Sommaire Site AP