UNIVERSITÉ DE POITIERS

Institut de Recherche
sur l Enseignement des Mathématiques

Octobre 1979

Sur les Nombres Décimaux...

Bernard REVRANCHE

S O M M A I R E

$\mathbb{D}$ EST UN ANNEAU DE FRACTIONS DE $\mathbb{Z}$

Les notations utilisées sont les mêmes que dans le premier exposé.

I - SOIT A UN ANNEAU COMMUTATIF, intègre, on note 1 l'élément unité.

Une partie S de A^* est dite multiplicativement stable si : quels que soient x, y des éléments de S

$xy \in S$

De plus on impose $1 \in S$.

Exemples : Considérons le cas où $A = \mathbb{Z}$, la partie $S = \{10^n \; ; \; n \in \mathbb{N}\}$ est une partie multiplicativement stable.

- Autre cas : $A = \mathbb{Z}$, S le complémentaire de l'idéal $3\mathbb{Z}$ dans $\mathbb{Z}$, est une partie multiplicativement stable.

- Enfin : A^* est une partie multiplicativement stable de A.

Pour poursuivre cet exposé, nous utilisons le résultat :

A étant intègre, il existe un corps K contenant A, vérifiant : quel que soit le corps k contenant A, k est une extension de K.

K est le corps des fractions de A.

Exemple : $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.

Soit donc K le corps des fractions de A et S une partie multiplicativement stable de A.

On désigne par $S^{-1}A$, le sous-ensemble de K défini par :

$S^{-1}A = \{\frac{a}{s} \; ; \; a \in A \; ; \; s \in S\}$.

On vérifie facilement que $S^{-1}A$ est un sous-anneau de K contenant A (car $1 \in S$). On dit :

$S^{-1}A$ est le localisé de A par rapport à S.

Exemples :

1°) $A = \mathbb{Z}$; $S = \{10^n ; n \in \mathbb{N}\}$.

$S^{-1} \mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$; on pose par définition

$\mathbb{D} = S^{-1} A$: $\mathbb{D}$ est le localisé de $\mathbb{Z}$ par rapport à S.

2°) Si $A = \mathbb{Z}$ et $S = \complement_{\mathbb{Z}}^{3\mathbb{Z}}$ on pose $\mathbb{Z}_3 = S^{-1} \mathbb{Z}$;

$\mathbb{Z}_3$ est un anneau intègre, dans cet anneau, les éléments non inversibles constituent un idéal qui est l'unique élément maximal dans l'ensemble des idéaux de $\mathbb{Z}_3$ ordonné par l'inclusion.

3°) Si A est un anneau intègre et $S = A^*$, on a : $S^{-1} A = K$.

II - VOYONS MAINTENANT QUELS SONT LES INVERSIBLES DE $S^{-1} A$:

Le groupe des inversibles de $S^{-1} A$ est noté $U(S^{-1} A)$.

Si u est un élément de $U(S^{-1} A)$, on peut l'écrire $\frac{a}{s}$ où a est élément de A et s élément de S ; de plus, il existe un couple $(b, s') \in A \times S$ tel que :

$$\frac{a}{s} \times \frac{b}{s'} = 1$$

donc a divise dans A un élément de S d'où :

Si $u \in U(S^{-1} A)$, u s'écrit $\frac{a}{s}$ où a diviseur dans A d'un élément de S.

La réciproque est facile.

$U(S^{-1} A) = \{\frac{a}{s} / (a, s) \in (A, S)$ et a divise dans A un élément de $S\}$.

Appliquons ce résultat à l'anneau $\mathbb{D}$.

L'ensemble des inversibles de $\mathbb{D}$ est l'ensemble des éléments s'écrivant $\frac{a}{10^n}$, avec $a \in \mathbb{Z}$, $n \in \mathbb{N}$, et $a = \varepsilon.2^{\alpha}.5^{\beta}$, α et β désignant deux entiers naturels, et ε l'un des deux entiers 1 ou -1.

L'égalité $\dfrac{\varepsilon.2^{\alpha}\ 5^{\beta}}{10^{n}} = \varepsilon.2^{\alpha-n}.5^{\beta-n}$

nous prouve :

$U(\mathbb{D})$ est isomorphe au groupe : $\{-1\ ;\ +1\} \times U + (\mathbb{D})$ et

$$\boxed{U_{+}(\mathbb{D}) = \{2^{\alpha}\ 5^{\beta}\ ;\ (\alpha, \beta) \in \mathbb{Z}^{2}\}}$$

Exercice : Montrer directement que : $U_{+}(\mathbb{D}) = \{2^{\alpha}.5^{\beta},\ (\alpha, \beta) \in \mathbb{Z}^{2}\}$

III - LES IDEAUX DE $\mathbb{D}$:

Nous donnerons les résultats concernant les idéaux de $\mathbb{D}$ comme conséquences des propositions données sur les anneaux de fractions.

S désigne une partie multiplicativement stable d'un anneau A.

1°) Une proposition, avec les notations habituelles :

Si A est principal alors $S^{-1}\ A$ est principal.

Preuve : si I désigne un idéal de $S^{-1}\ A$, $I \cap A$ est un idéal de A, engendré par un élément a de A.

Si x désigne un élément de I, il s'écrit $\frac{b}{s}$ où $b \in A$, $s \in S$ en particulier b est élément de $I \cap A$, donc multiple de a dans A, donc $x \in (S^{-1}\ A)\ .\ a$.

$I = (S^{-1}\ A)\ a$ d'où le résultat annoncé.

En application ; comme $\mathbb{Z}$ est un anneau principal

$\mathbb{D}$ est principal.

2°) Un théorème important

a) Une définition : I un idéal de A est saturé pour la partie S, si :

Quel que soit $a \in A$, quel que soit $s \in S$

si $a.s \in I$, alors $a \in I$.

b) Un exercice : (dont on trouvera la solution un peu plus loin).

A désigne un anneau <u>principal</u> ; a désigne un élément de A^*, montrez l'équivalence :

Aa est un idéal saturé pour S si et seulement si quel que soit $s \in S$, $(a) + (s) = A$.

c) <u>Les idéaux propres de $\mathbb{Z}$</u>, saturés pour la partie $\{10^n \; ; \; n \in \mathbb{N}\}$ sont les idéaux engendrés par un élément étranger à 10. (Il suffit d'appliquer le résultat précédent).

d) <u>Le théorème</u> :

Il y a correspondance biunivoque entre les idéaux de $S^{-1}A$ et les idéaux, saturés pour S, de A.

Preuve : on désigne par

$\mathcal{J}$: l'ensemble des idéaux de $S^{-1}A$, ordonné par l'inclusion

$\mathfrak{I}$: l'ensemble des idéaux saturés de A, ordonné par l'inclusion.

Soit $J \in \mathcal{J}$; $J \cap A$ est alors élément de $\mathfrak{I}$; en effet si $a \in A$ et $s \in S$ tel que $s.a \in J \cap A$, la relation $\frac{1}{s}.sa \in J$, nous prouve que $a \in J \cap A$ qui est donc saturé pour S.

Ceci nous permet de définir l'application :

$$\Psi : \mathcal{J} \longrightarrow \mathfrak{I}$$
$$J \longrightarrow J \cap A.$$

<u>Ψ est injective</u> : J et J' désignent des éléments de $\mathcal{J}$ tel que $J' \cap A = J \cap A$; soit x un élément de J que l'on écrit $\frac{a}{s}$ $(a, s) \in A \times S$; a est donc élément de $J \cap A$, donc de $J' \cap A$, d'où x appartient à J' ; nous avons donc $J \subset J'$; J et J' jouant le même rôle finalement $J = J'$.

<u>Ψ est surjective</u> : Soit I un élément de $\mathfrak{I}$, on pose $S^{-1}I = \{\frac{i}{s} \; ; \; i \in I \; ; \; s \in S\}$. On vérifie aisément que $S^{-1}I$ est un idéal de $S^{-1}A$. Comme 1 appartient à S, I est sous-ensemble de $S^{-1}I$; d'où $I \subset (S^{-1}I) \cap A$, montrons l'autre inclusion : si x désigne un élément de $A \cap S^{-1}I$, il existe $s \in S$ tel $s.x \in I$; I étant saturé $x \in I$.

Donc $I = S^{-1} I \cap A$ et $\Psi(S^{-1} I) = I$, Ψ est surjective.

Ψ est bien une bijection de $\mathcal{J}$ dans $\mathcal{I}$.

Remarque :

La bijection réciproque de Ψ est l'application qui à tout élément I de $\mathcal{I}$ associe l'élément $S^{-1} I$.

Exercice :

Ψ est une bijection strictement croissante, pour la relation d'ordre. De plus si I est un idéal quelconque de A : $I \subset S^{-1}(I) \cap A$.

3°) En conclusion des résultats précédents :

Les idéaux propres de $\mathbb{D}$ sont les idéaux de la forme $b.\mathbb{D}$ où b est un entier naturel premier avec 10.

4°) Les idéaux premiers de $S^{-1} A$:

On peut vérifier que l'application Ψ précédente restreinte à l'ensemble des idéaux premiers de $S^{-1} A$, est une bijection sur l'ensemble des idéaux premiers de A, disjoints de S.

Les idéaux propres premiers de $\mathbb{D}$ sont donc les idéaux engendrés par un nombre premier de $\mathbb{N}$ distinct de 2 et 5.

5°) Dans un anneau principal, les notions d'idéal premier, d'idéal maximal, se confondent :

Il suffit de prouver que tout idéal propre et premier P, d'un anneau principal, est maximal.

Soit I un idéal contenant strictement P ; on sait que P est engendré par un élément premier de A, noté p, et I par un élément de a.

Comme $(p) \subsetneq (a)$ a divise p, a est un inversible de A, donc $I = A$ et P est un idéal maximal.

On connaît donc exactement les idéaux maximaux de $\mathbb{D}$.

IV - L'AUTRE QUESTION :

Où l'on montre le théorème de transfert :
"Si A est euclidien alors $S^{-1} A$ est euclidien".

1°) Donnons la définition d'un anneau euclidien, ainsi qu'un certain nombre de conséquences de cette définition :

Un anneau A est un anneau euclidien, s'il est commutatif intègre, et s'il existe une application φ de A^* dans $\mathbb{N}^*$ tel que : quels que soient a ; b éléments de A^*:

1 - si a divise b alors $\varphi(a) \leqslant \varphi(b)$

2 - il existe un couple (q, r) d'éléments de A tel que $a = bq + r$ et si $r \neq o$ $\varphi(r) < \varphi(b)$.

Nous avons sous ces hypothèses le

Lemme 1 : Posons $a = \operatorname{Inf}_{x \in A^+} \varphi(x)$

Quel que soit x élément de A^* : $\varphi(x) = a \iff x \in U(A)$.

Preuve : si x est élément de $U(A)$, pour tout élément b de A^* $(b) \subset (x)$ donc $\varphi(x) < \varphi(b)$ et $\varphi(x) = a$.

x désigne maintenant un élément de A^* tel que $\varphi(x) = a$.

Soit $u \in U(A)$, il existe $(q, r) \in A^2$ tel que $u = xq + r$ nécessairement r est nul ; l'égalité $1 = x.q.u^{-1}$ montre que $x \in U(A)$.

Lemme 2 : Quels que soient a élément de A^*

u élément de $U(A)$

on a $\varphi(a) = \varphi(u.a)$.

En effet (a) et (ua) sont deux idéaux égaux, donc a divise $u.a$ et réciproquement.

Une autre proposition découle de la définition précédente :

Tout anneau euclidien est principal.

La démonstration est calquée sur celle prouvant que $\mathbb{Z}$ est un anneau principal.

Soit donc I un idéal propre de A ; $\varphi(I - \{o\})$ est une partie non vide de $\mathbb{N}^*$, qui admet un plus petit élément de a.

On note r_o un antécédent dans I de a, pour l'application φ.

Nous avons $A\,r_o \subset I$, montrons l'autre inclusion x désigne un élément de I ; il existe alors un couple $(q, r) \in A^2$ tel que : $x = r_o.q + r$ donc r est élément de I. La définition de r_o impose $r = o$. c.q.f.d.

2°) <u>Le théorème de Transfert</u> :

A désigne un anneau euclidien ; S une partie multiplicativement stable de A^*.

Démontrons, tout de suite, un résultat posé en exercice antérieurement :

<u>Lemme 3</u> : Quel que soit a élément de A^*, (a) est saturé pour $S \Longleftrightarrow$ pour tout élément s de S $(s) + (a) = A$.

Preuve : $\boxed{\Longleftarrow}$ a désigne un élément de A^* tel que : si $s \in S$ alors $(a) + (s) = A$; montrons que l'idéal (a) est saturé : soit $\alpha \in A$ et $z \in S$ tel que $z\alpha \in (a)$.

L'égalité $A = (a) + (z)$ nous donne μ et λ deux éléments de A tel que $1 = \lambda a + \mu z$, d'où $\alpha = \lambda.\alpha a + \mu.z\alpha$ d'où $\alpha \in (a)$. (a) est saturé.

$\boxed{\Longrightarrow}$ (a) est un idéal saturé, et s désigne un élément quelconque de S. L'anneau A étant euclidien, est en particulier principal ; il existe $d \in A$ tel que $(d) = (a) + (s)$.

En particulier, il existe β et α deux éléments de A tel que :

$$s = \beta.d \quad \text{et} \quad a = \alpha.d \quad (*)$$

d'où $\alpha.s = \beta.(\alpha d) = \beta.a$ donc $\alpha.s \in (a)$ qui est saturé α est donc élément de (a) ; il existe $\beta' \in A$ tel que $\alpha = \beta'\,a$ (Θ).

L'égalité $a = \beta' ad$, déduite de $(*)$ et de (Θ), que l'on peut écrire $a(1 - \beta' d) = o$, donne : d est inversible, donc : $(a) + (s) = A$.

Utilisons ce lemme pour montrer le résultat suivant :

<u>Tout élément de $S^{-1}A^{+}$ s'écrit $a \times c$, où c est un inversible de $S^{-1}A$, et a un élément de A, étranger à tout élément de S.</u> L'écriture est unique à la multiplication près d'un inversible de A. (ie : si $a \times c = a' \times c'$ alors il existe $u \in U(A)$ tel que $a' = u.a$).

Preuve : x désigne un élément non nul de $S^{-1}A$. Posons J l'idéal de $S^{-1}A$ engendré par x ; $J \cap A$ est un idéal saturé de A, engendré par un élément non nul a, de A (en effet A est un anneau principal). Le théorème sur les idéaux donne $S^{-1}(a) = J$; a est donc générateur de J, donc x et a sont associés dans $S^{-1}A$; il existe donc $c \in U(S^{-1}A)$ tel que :

$$x = a \times c.$$

Comme l'idéal Aa est saturé, le lemme 3 nous montre que a est étranger à tout élément de S.

L'existence de la décomposition de x en produit $a \times c$ étant assurée, voyons "l'unicité".

Soit a', c' où c' est inversible de $S^{-1}A$ et a' un élément de A étranger à tout élément de S, tel que :

$$a \times c = a' \times c'.$$

a et a' <u>étant associés</u> dans $S^{-1}A$, les idéaux de $S^{-1}A$ engendrés par a et a' sont égaux ; les idéaux (a) et (a') de A, étant saturés pour S, le théorème rappelé permet d'écrire $(a) = (a')$ et a et a' <u>sont associés dans A</u>, il existe $u \in U(A)$ tel que $ua = a'$ et évidemment $c' = u^{-1} . c$, d'où l'unicité de la décomposition à un inversible de A près.

Ceci étant dit : nous savons qu'il existe une application φ de A^{*} dans $\mathbb{N}^{*}$ qui fait de A un anneau euclidien.

<u>Construisons une application $\hat{\varphi}$ de $S^{-1}A^*$ dans $\mathbb{N}^*$</u>

Soit x un élément de $S^{-1}A^*$, x s'écrit $a \times c$, de manière unique, à la multiplication près d'un élément de $U(A)$.

Posons :

$\hat{\varphi}(x) = \varphi(a)$.

Le lemme 2 nous prouve que $\hat{\varphi}$ est bien une application de $S^{-1}A$ dans $\mathbb{N}^*$.

Afin d'alléger les notations dans la démonstration qui suit, si $x \in S^{-1}A$, on note l'idéal $x.S^{-1}A$ <u>par le symbole $((x))$</u>, la notation (a) étant réservée à l'idéal Aa quand : $a \in A$.

Nous avons posé $\hat{\varphi}(x) = \varphi(a)$ alors, on remarque :

$(a) = ((x)) \cap A$.

Soient maintenant x et y deux éléments de $S^{-1}A^*$,

x s'écrit : $a \times c$; $c \in U(S^{-1}A)$; (a) idéal saturé de A

y s'écrit : $b \times d$; $d \in U(S^{-1}A)$; (b) idéal saturé de A.

1 - Supposons que x divise y ; l'idéal $((y))$ est inclus dans l'idéal $((x))$ comme (a) et (b) sont des idéaux saturés de A : $(a) = ((x)) \cap A$ et $(b) = ((y)) \cap A$ d'où $(b) \subset (a)$, donc a divise b et $\varphi(a) \leqslant \varphi(b)$.

Si <u>x divise y alors $\hat{\varphi}(x) \leqslant \hat{\varphi}(y)$</u>.

2 - Montrons qu'il existe un couple $(Q\ ;\ R) \in (S^{-1}A)^2$ tel que :

$x = Qy + R$ et si $R \neq o$ $\hat{\varphi}(R) < \hat{\varphi}(y)$.

A est un anneau euclidien, il existe un couple $(q, r) \in A^2$ tel que :

$a = bq + r$ et si $r \neq o$ $\varphi(r) < \varphi(b)$.

On en déduit :

$a.c = bd \times (c.d^{-1}.q) + r.c$

soit <u>$x = y \times (q.cd^{-1}) + R$</u> en posant $R = r.c$.

Supposons $R \neq o$, R se décompose en $r_1 . c_1$ où $(r_1, c_1) \in A \times U(S^{-1} A)$ (1). Il est facile de vérifier que $(r) \subset ((r)) \cap A$; mais $((r)) = ((R))$ car r et R sont associés dans $S^{-1} A$, donc $(r) \subset ((R)) \cap A$; comme $((R)) \cap A = (r_1)$ on a évidemment $(r) \subset (r_1)$ et $\varphi(r_1) \leqslant \varphi(r)$.

Comme par définition de $\hat{\varphi}$: $\hat{\varphi}(R) = \hat{\varphi}(r_1)$, nous avons les relations :

$\hat{\varphi}(R) = \varphi(r_1) \leqslant \varphi(r) < \varphi(b) = \hat{\varphi}(y)$:

si $R \neq o$; $\hat{\varphi}(R) < \hat{\varphi}(y)$

$\boxed{S^{-1} A \text{ est un anneau euclidien}}$

Une propriété de l'application $\hat{\varphi}$:

Il est facile de vérifier que $\hat{\varphi}$ et φ coïncident sur les éléments de A qui sont étrangers à tout élément de S.

En résumé : <u>$\hat{\varphi}$ prolonge "presque" l'application φ</u>.

Nous verrons que l'application $\hat{\varphi}$ n'est pas unique.

3°) <u>Application à l'anneau $\mathbb{D}$</u> :

$A = \mathbb{Z}$; $S = \{10^n \; ; \; n \in \mathbb{N}\}$.

$\mathbb{Z}$ est un anneau euclidien, il suffit de prendre l'application : $\mathbb{Z}^* \longrightarrow \mathbb{N}^*$

$x \longmapsto |x|$

Donc $\mathbb{D} = S^{-1} \mathbb{Z}$ est un anneau euclidien.

4°) <u>Quelques exercices</u>

L'application φ dont il est question dans la définition d'un anneau euclidien, s'appelle un algorithme d'anneau euclidien.

a) On peut vérifier qu'un corps K commutatif est un anneau euclidien. Donner un algorithme.

---

(1) Cette décomposition est celle réalisant : (r_1) est un idéal saturé de A!

b) On peut vérifier :

Si φ est un algorithme pour un anneau euclidien A et si f est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ alors $f \circ \varphi$ est aussi un algorithme pour A.

En particulier, si $a \in \mathbb{N}$; $\varphi + a$ est un algorithme pour A et :
Il existe donc une infinité d'algorithmes sur A.

c) $(\varphi i)_{i} \in I$ désigne une famille d'algorithmes indexés par un ensemble I. Alors l'application $\varphi = \operatorname{Inf}_{i \in I} \varphi i$ est un algorithme pour A. (On attire l'attention du lecteur sur le fait suivant : soit $i \in I$ et φi un des algorithmes de la famille, si a et b désignent deux éléments de A, $b \neq o$, il existe q_i, le "quotient", et r_i, le "reste" tel que $a = bq_i + r_i$ et si $r_i \neq o$ $\varphi i(r_i) < \varphi i(b)$: q_i et r_i dépendent de l'indice i !)

Afin de montrer que φ est un algorithme, il est conseillé d'utiliser i_o qui réalise $\varphi i_o(b) = \operatorname{Inf}_{i \in I} \varphi i(b)$; (il existe !).

d) A un anneau euclidien muni d'un algorithme φ : nous avons alors A est un corps $\Longleftrightarrow \varphi$ est constante.

SOMMAIRE

L'étude des décimaux constitue une partie assez importante dans le programme de mathématique des élèves de classe de quatrième. En particulier, plusieurs présentations de l'ensemble $\mathbb{D}$ sont possibles, et les commentaires des programmes officiels nous en suggèrent une. Ces instructions nous rappellent d'ailleurs, qu'au cours de la présentation de cette construction, obtenue à partir de l'ensemble $\mathbb{Z}$, des difficultés techniques apparaîtront et sur lesquelles on ne s'attardera pas.

Un des buts de ces quelques feuilles, est de situer ces difficultés et de donner au lecteur des démonstrations de chaque résultat que l'on demande, en général, d'admettre aux élèves.

Ce recueil rassemble donc un ensemble de propositions et leurs preuves ; il pourra être consulté pour vérifier la véracité ou les raisons de telle ou telle affirmation sur cette partie essentielle du programme de la classe de quatrième.

Des exercices sont insérés dans le texte dont certains indiquent une idée qui éventuellement sert de base à l'élaboration de sujets d'étude à soumettre aux élèves.

Une autre présentation de l'ensemble $\mathbb{D}$ est possible ; c'est celle qui fait apparaître $\mathbb{D}$ comme un anneau localisé de $\mathbb{Z}$, par rapport à une partie multicativement stable ; à cette occasion nous avons redonné quelques résultats sur les anneaux de fractions.

Nous verrons enfin qu'il existe sur $\mathbb{D}$, une notion de divisibilité "compatible" avec la relation d'ordre sur $\mathbb{N}$, un peu analogue à la division euclidienne sur $\mathbb{Z}$; en deux mots, $\mathbb{D}$ est un anneau euclidien.

Une dernière précaution ; ce fascicule est, bien entendu réservé aux professeurs, et ne saurait être utilisé tel quel, par ou pour les élèves.

NOTATIONS ET CONVENTIONS

Tous les anneaux considérés ici sont commutatifs unitaires.

Si A désigne un tel anneau, on pose

$A^{*} = A - \{0\}$ où 0 désigne l'élément neutre pour la loi notée habituellement $+$

$U(A)$: le groupe des inversibles de A (pour la loi notée $\times$).

$U_{+}(\mathbb{D})$: le groupe des inversibles positifs, pour la loi $\times$, de $\mathbb{D}$.

Soient a et b deux éléments de A, l'expression a divise b sera notée parfois : $a \,/\, b$.

L'idéal engendré par a sera noté Aa ou (a).

I - UNE CONSTRUCTION DE L'ENSEMBLE $\mathbb{D}$

L'ensemble $\mathbb{Z}$ est supposé connu, ainsi que les propriétés classiques attachées à $\mathbb{Z}$ (division euclidienne, ordre dans $\mathbb{N}$, etc).

Cette construction se déroule en deux étapes ; la construction du groupe des puissances de 10, puis celle de $\mathbb{D}$.

a) Construction de $(\mathcal{P},\times)$: groupe des puissances de 10

On considère la partie de $\mathbb{N}$:

$P = \{10^{n} \; ; \; n \in \mathbb{N}\}$ qui, munie de la multiplication, est stable, de plus : $1 \in P$ (P est un monoïde unitaire que l'on va symétriser).

Sur l'ensemble $P \times P$ nous mettons la relation : notée R quels que soient a, b, c, d des éléments de $\mathbb{N}$

$(10^{a}, 10^{b}) \; R \; (10^{c}, 10^{d})$ si et seulement si $10^{b+c} = 10^{a+d}$.

La relation R est une relation d'équivalence sur $P \times P$; on peut le montrer directement ou on peut remarquer que cette relation sur $P \times P$ est la simple transcription de la relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$ permettant de construire $\mathbb{Z}$.

Cette transcription étant la bijection $\mathbb{N} \times \mathbb{N} \xrightarrow{\mathcal{C}} P \times P$

$$(a,\ b) \rightsquigarrow (10^a,\ 10^b)$$

On définit sur $P \times P$ une multiplication de la façon suivante : quels que soient a, b, a', b' des éléments de $\mathbb{N}$

$$(10^a,\ 10^b) \times (10^{a'},\ 10^{b'}) = (10^{a+a'},\ 10^{b+b'}).$$

Cette multiplication est compatible avec la relation d'équivalence R (ce qui signifie : avec des notations simplifiées, quels que soient x, y, z des éléments de $P \times P$:

si $x\ R\ y$ alors $(x \times z)\ R\ (y \times z)$.

On peut montrer ce résultat directement, ou bien comme dans le cas précédent, on remarque que la multiplication sur $P \times P$ est la simple transcription de l'addition habituelle définie sur $\mathbb{N} \times \mathbb{N}$ qui est, elle-même, compatible avec la relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$ permettant de définir $\mathbb{Z}$. En d'autres termes ; $\mathcal{C}$ désignant la bijection donnée ci-dessus :

si a, b, a', b' désignent des entiers naturels, on peut vérifier que :

$$\mathcal{C}\left[(a,b) + (a',b')\right] = \mathcal{C}\left[(a,b)\right] \times \mathcal{C}\left[(a',b')\right]$$

<u>Exercice</u> : en utilisant ce résultat, écrire que la multiplication sur $P \times P$ est compatible avec la relation R.

On considère alors l'ensemble quotient $\frac{P \times P}{R}$ noté $\mathcal{P}$, qui, en vertu de ce que l'on vient de montrer, peut être muni d'une multiplication : "le produit de 2 classes étant défini comme la classe du produit". Si a et b sont deux naturels, on note $\overline{(10^a,\ 10^b)}$ un élément de $\mathcal{P}$;

il est alors facile de montrer :

que pour tout couple (a,b) d'entiers naturels, il existe un seul entier naturel n tel que :

$$\overline{(10^a,\ 10^b)} = \begin{cases} \overline{(1,\ 10^n)} \\ \text{ou} \\ \overline{(10^n,\ 1)} \end{cases}$$

L'injection $i : \begin{array}{ccc} P & \longrightarrow & \mathcal{P} \\ 10^n & \longmapsto & \overline{(10^n,\ 1)} \end{array}$ permet d'identifier P à une partie de $\mathcal{P}$; on pose alors $\overline{(10^n,\ 1)} = 10^n$; $\overline{(1,\ 10^n)} = 10^{-n}$.

On a alors $\boxed{\mathcal{P} = \{10^n\ ;\ n \in \mathbb{Z}\}}$

On vérifie alors : quels que soient n et m éléments de Z : $10^n \times 10^m = 10^{n+m}$

L'application : $\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathcal{P} \\ n & \longmapsto & 10^n \end{array}$ est une bijection telle que : si n et m désignent deux entiers : $\varphi(n + m) = \varphi(n) \times \varphi(m)$, $(\mathcal{P},\times)$ est donc un groupe abélien.

L'application φ, permet d'introduire une relation d'ordre total sur $\mathcal{P}$ qui prolonge celle connue sur P ; compatible avec la multiplication.

> *<u>En fait</u> :*
>
> $(\mathcal{P}, \times\ ;\ \leqslant)$ *est un groupe abélien, totalement ordonné, isomorphe au groupe* $(\mathbb{Z}, +, \leqslant)$

b) <u>Construction de l'ensemble $\mathbb{D}$</u> :

La principale difficulté de cette présentation est le fait que : 3×10^{-1} n'ait pas de sens, (pour l'instant).

On considère le produit cartésien $\mathbb{Z} \times \mathcal{P}$ sur lequel on met la relation notée S.

Quels que soient a, b, n, m des entiers :

$$(a,\ 10^n)\ S\ (b,\ 10^m) \quad \text{si et seulement si} \quad \begin{cases} a = b \cdot 10^{m-n} & \text{quand } m \geq n \\ \text{ou} & \\ b = a \cdot 10^{n-m} & \text{quand } n \geq m. \end{cases}$$

<u>Cette relation est une relation d'équivalence</u> :

Preuve : cette relation est réflexive car $10^o = 1$, et elle est visiblement symétrique (l'écrire si l'on n'est pas convaincu). Seule la transitivité présente quelques difficultés.

Soient donc a, b, c, n, m, p des entiers relatifs tel que :

$$\left.\begin{aligned} &(a,\ 10^n)\ S\ (b,\ 10^m) \\ &\qquad\text{et} \\ &(b,\ 10^m)\ S\ (c,\ 10^p) \end{aligned}\right\}$$

Nous présentons les conséquences de ces relations sous forme de tableau étant donnée la lourdeur de la démonstration :

$$\Rightarrow \begin{cases} m \geq n \ ;\ a = b\,10^{m-n} \begin{cases} p \geq m \ ;\ b = c \cdot 10^{p-m} \longrightarrow p \geq n \ ;\ a = c \cdot 10^{p-n} \\ \qquad \text{ou} \\ p \leq m \ ;\ c = b \cdot 10^{m-p} \rightarrow \begin{cases} n \geq p \ ;\ c = b \cdot 10^{m-n} \times 10^{n-p} = a \cdot 10^{n-p} \\ \text{ou} \\ n \leq p \ ;\ a = b \cdot 10^{m-p} \times 10^{p-n} = c \cdot 10^{p-n} \end{cases} \end{cases} \\ \qquad \text{ou} \\ m \leq n \ ;\ b = a \cdot 10^{n-m} \begin{cases} p \geq m \ ;\ b = c \cdot 10^{p-m} \rightarrow \begin{cases} n \leq p \ ;\ a \cdot 10^{n-m} = c \cdot 10^{p-m} \Rightarrow a \cdot 10^{n-m} = \\ = c \cdot 10^{p-n+(n-m)} \Rightarrow a = c \cdot 10^{p-n} \\ \text{ou} \\ n \geq p \ ;\ a \cdot 10^{n-m} = c \cdot 10^{p-m} \Rightarrow a \cdot 10^{n-p+(p-m)} \\ = c \cdot 10^{p-m} \Rightarrow a \cdot 10^{n-p} = c. \end{cases} \\ \qquad \text{ou} \\ p \leq m \ ;\ c = b \cdot 10^{m-p} \longrightarrow n \geq p \ ;\ c = a \cdot 10^{n-m} \times 10^{m-p} = a \cdot 10^{n-p} \end{cases} \end{cases}$$

c.q.f.d.

La relation S est une relation d'équivalence sur $\mathbb{Z} \times \mathcal{P}$.

On pose : $\mathbb{D} = \dfrac{\mathbb{Z} \times \mathcal{P}}{S}$; c'est à dire l'ensemble quotient obtenu à partir de la relation S sur $\mathbb{Z} \times \mathcal{P}$.

On définit une multiplication dans $\mathbb{Z} \times \mathcal{P}$ en posant :

quels que soient : a, b, n, m des éléments de $\mathbb{Z}$:

$$(a,\ 10^n) \times (b,\ 10^m) = (ab,\ 10^{n+m})$$

Cette multiplication est compatible avec la relation d'équivalence S, en effet :

si a, b, c, n, m, r désignent des entiers : vérifiant :

$$(a,\ 10^n)\ S\ (c,\ 10^r) \quad \text{alors} \quad \left\{\begin{array}{l} a = c\ .\ 10^{r-n} \\ \text{ou} \\ c = a\ .\ 10^{n-r} \end{array}\right. \quad \text{d'où} \quad \left\{\begin{array}{l} a\ .\ b = bc\ .\ 10^{r-n} \\ \\ b\ .\ c = ab\ .\ 10^{n-r} \end{array}\right.$$

ce qui signifie exactement :

$$(b,\ 10^m) \times (a,\ 10^n)\ S\ (b,\ 10^m) \times (c,\ 10^r) \qquad \text{c.q.f.d.}$$

Ceci nous permet de définir une multiplication sur $\mathbb{D}$, de façon habituelle :

$$\mathbb{D} \times \mathbb{D} \xrightarrow{\times} \mathbb{D}$$

$$(\overline{(a,\ 10^n)},\ \overline{(b,\ 10^m)}) \longmapsto (\overline{(a\ .\ b,\ 10^{n+m})})$$

Un exercice classique consiste à montrer que cette définition ne dépend pas des représentants choisis.

Voici maintenant une <u>remarque</u> : "choix d'un dénominateur commun".
$(a,\ 10^n)$ et $(b,\ 10^m)$ sont deux éléments de $\mathbb{Z} \times \mathcal{P}$.

Soit r un entier tel que : $r \leqslant \mathrm{Inf}(n,m)$. $\mathrm{Inf}(n,m)$ étant le plus petit de n et de m.

Il est facile de vérifier que $(a,\ 10^n)\ S\ (a\ .\ 10^{n-r},\ 10^r)$
et $(b,\ 10^m)\ S\ (b\ .\ 10^{m-r},\ 10^r)$

Il existe donc 3 entiers : α, β, r tels que :
$(a,\ 10^n)\ S\ (\alpha,\ 10^r)$ et $(b,\ 10^m)\ S\ (\beta,\ 10^r)$.

<u>Cette remarque nous permet de définir une addition sur $\mathbb{Z} \times \mathcal{P}$</u>

Soient a, b, n, m des entiers relatifs ; posons : $r = \mathrm{Inf}(n,m)$ on écrit alors :

$$(a,\ 10^n) + (b,\ 10^m) = (a\ .\ 10^{n-r} + b\ .\ 10^{m-r},\ 10^r).$$

En remarquant que : "si $\overline{(A,\ B)} \in \mathbb{D}$ avec $A \in \mathbb{Z}$, $B \in \mathcal{P}$ et si $n \in \mathbb{N}$,

$$\overline{(A,\ B)} \times \overline{(10^n,\ 10^{-n})} = \overline{(A,\ B)}\text{"}$$

il est facile de vérifier que pour tout entier t inférieur à r :

$$(a\ .\ 10^{n-r} + b\ 10^{m-r},\ 10^r)\ S\ (a\ .\ 10^{n-t} + b\ 10^{m-t},\ 10^t).$$

Cette addition que l'on vient de définir sur $\mathbb{Z} \times \mathcal{P}$ est compatible avec la relation S, en effet : a, b, c, n, m, p désignent des entiers ;

Supposons $(a,\ 10^n)\ S\ (b,\ 10^m)$ et $(c,\ 10^p)$ désigne un élément de $\mathbb{Z} \times \mathcal{P}$ posons $\gamma = \mathrm{Inf}(n,m,p)$.

Le dernier résultat nous montre que $(a,\ 10^n) + (c,\ 10^p)$ est équivalent à $(a\ .\ 10^{n-\gamma} + c\ .\ 10^{p-\gamma},\ 10^\gamma)$.

De même $(b,\ 10^m) + (c,\ 10^p)$ est équivalent à $(b\ .\ 10^{m-\gamma} + c\ .\ 10^{p-\gamma},\ 10^\gamma)$.

La relation $(a,\ 10^n)\ S\ (b,\ 10^m)$ prouve :

$$a\ 10^{n-\gamma} = b\ .\ 10^{m-\gamma}$$

d'où $(a,\ 10^n) + (c,\ 10^p)\ S\ (b,\ 10^m) + (c,\ 10^p)$.

L'addition définie sur $\mathbb{Z} \times \mathcal{P}$ est compatible avec la relation S. Ainsi $\mathbb{D}$ est muni d'une addition :

$$\overline{(a,\ 10^n)} + \overline{(b,\ 10^m)} = \overline{(a,\ 10^n) + (b,\ 10^m)}$$

On a donc une multiplication, une addition sur $\mathbb{D}$ qui confèrent (on peut le vérifier) à cet ensemble une structure d'anneau commutatif, unitaire ($\overline{(10^n,\ 10^{-n})}$ où n est un entier naturel, est l'unité, intègre.

L'injection $\begin{array}{l} \mathcal{P} \hookrightarrow \mathbb{D} \\ 10^n \longmapsto \overline{(1,\ 10^n)} \end{array}$ permet d'identifier $\mathcal{P}$ à une partie de $\mathbb{D}$, et la multiplication sur $\mathbb{D}$ restreinte à $\mathcal{P}$ est la multiplication déjà connue sur $\mathcal{P}$.

On pose pour tout n élement de $\mathbb{Z}$, $\overline{(1,\ 10^n)} = 10^n$.

On considère l'injection $\begin{array}{rcl} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{D} \\ n & \longmapsto & \overline{(n, 10^o)} \end{array}$ qui fait apparaître $\mathbb{Z}$ comme un sous anneau unitaire de $\mathbb{D}$: (φ est homomorphisme d'anneaux unitaire).

On pose alors pour tout n de $\mathbb{Z}$, $\overline{(n, 10^o)} = n$.

Considérons $\overline{(a, 10^n)}$ un élément de $\mathbb{D}$, a et n désignant deux entiers ; on a les relations :

$$\overline{(a, 10^n)} = \overline{(a, 10^o)} \times \overline{(1, 10^n)}$$

d'où, avec les notations précédentes :

$$\overline{(a, 10^n)} = a \times 10^n = a \,.\, 10^n.$$

En résumé : $\overline{(a, 10^n)}$ où $a \in \mathbb{Z}$, $n \in \mathbb{Z}$, s'écrit $a \,.\, 10^n$ mais cette écriture n'est pas unique.

<u>CONCLUSION</u> :

$\mathbb{D}$ ainsi construit <u>est un sur-anneau de $\mathbb{Z}$, contenant $\mathcal{P}$</u>.

Tout élément de $\mathbb{D}$ s'écrit $a \,.\, 10^n$ avec a, n deux entiers et l'écriture n'est pas unique.

a, b, n, m désignant quatre entiers :

$$a \,.\, 10^n \times b \,.\, 10^m = ab \times 10^{n+m}$$

$$a \,.\, 10^n + b \,.\, 10^m = \underbrace{(a \,.\, 10^{n-\mathrm{Inf}(n,m)} + b \,.\, 10^{m-\mathrm{Inf}(n,m)})}_{\text{Somme dans } \mathbb{Z}} \times 10^{\mathrm{Inf}(n,m)}$$

<u>Exercice</u> : Démontrez que $\boxed{\mathbb{D} \text{ est dénombrable}}$:

(Indication : on peut utiliser l'écriture de tout décimal sous forme $a \,.\, 10^p$, pour construire une surjection de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{D}$).

<u>Une remarque sur l'écriture décimale d'un décimal</u> :

Le décimal -25×10^{-3} que l'on peut encore écrire -250×10^{-4}, a pour écriture décimale : $-0{,}025$, et il est bien connu que cette écriture est unique.

<u>Analysons cette question, et montrons que chaque décimal a une écriture décimale unique.</u>

L'étude peut se faire sur l'ensemble des décimaux positifs, et l'on suppose, bien entendu, connue l'écriture en base 10 d'un entier naturel ; on rappelle que l'existence de cette écriture est une conséquence de la division euclidienne dans $\mathbb{N}$, et on trouvera dans cet exposé un lemme, non "strictement nécessaire" au déroulement, qui permet de prouver l'unicité de l'écriture d'un entier en base 10.

Soit z un entier naturel ; il existe une suite d'entiers naturels $(a_i)_{i \in \mathbb{N}}$, tous nuls sauf un nombre fini d'entre eux ; chaque entier a_i étant inférieur ou égal à 9 (dorénavant nous dirons chiffre), tel que :

$$z = a_o + a_1 \,.\, 10 + a_2 \,.\, 10^2 + \ldots + a_i\, 10^i + \ldots$$

égalité que l'on peut encore écrire : $z = \sum_{i=0}^{+\infty} a_i\, 10^i$

Dans un premier temps, montrons <u>l'existence</u> d'une écriture décimale de tout élément de $\mathbb{D}_+^*$. Soit $z \,.\, 10^m$ un tel élément ; m est un entier négatif, le cas où m est positif étant supposé connu.

Soient $(a_i)_{i \in \mathbb{N}}$ les chiffres de l'écriture de z.

$$z = a_o + a_1\, 10 + a_2\, 10^2 + \ldots + a_i\, 10^i + \ldots$$

d'où $z \,.\, 10^m = a_o\, 10^m + a_1\, 10^{m+1} + \ldots + a_i\, 10^{i+m} + \ldots$

Comme m est négatif, il existe i_o un entier naturel tel que $i_o + m = 0$, d'où :

$$z\, 10^m = a_o\, 10^{-i_o} + \ldots + a_{i_o - 1}\, 10^{-1} + a_{i_o} + a_{i_o+1}\, 10 + \ldots + a_{i_o+k}\, 10^k + \ldots$$

Egalité que l'on peut écrire :

$$z\, 10^m = b_{-p}\, 10^{-p} + \ldots + b_{-1}\, 10^{-1} + b_o + b_1\, 10 + b_2\, 10^2 + \ldots + b_n\, 10^n + \ldots$$

avec un simple changement de notations : précisons, $p \in \mathbb{N}$; $n \in \mathbb{N}$; chaque b_i est un chiffre ; tous sont nuls sauf un nombre fini d'entre eux.

<u>Nous voilà assurés de l'existence ; montrons l'unicité d'une telle écriture</u>. Nous utiliserons le

<u>Lemme</u> : <u>Soient $(n+1)$ éléments de $\mathbb{Z}$, notés a_i ; $i = 0$ à n, tel que $|a_i| \leqslant 9$. Si $\sum_{i=0}^{n} a_i\, 10^i = 0$ alors pour tout i, $a_i = 0$.</u>

Ceci se montre par récurrence sur n ; le résultat étant immédiat pour $n = 0$, soient donc $(a_i)_{i=0}^{n}$, $(n+1)$ entiers tel que $|a_i| \leqslant 9$ et $\sum_{i=0}^{n} a_i \, 10^i = 0$. Cette dernière relation entraîne :

$$|a_o| = 10 \times |a_1 + a_2 \, 10 + \ldots + a_n \, 10^{n-1}|$$

Si $|a_1 + a_2 \, 10 + \ldots + a_n \, 10^{n-1}|$ est différent de zéro, alors $|a_o| \geqslant 10$ ce qui est une contradiction. L'hypothèse de récurrence nous permet alors de conclure. Le lemme est démontré.

Soient donc deux écritures de $z \, . \, 10^m$, élément de $\mathbb{D}$.

$(a_j)_{j \geqslant -p}$ la première suite de chiffres ; $p \in \mathbb{N}$

$(a'_i)_{i \geqslant -p'}$ la deuxième suite de chiffres ; $p' \in \mathbb{N}$

tel que (1) : $\sum_{j \geqslant -p} a_j \, 10^j = \sum_{i \geqslant -p'} a'_i \, 10^i$

Le fait que tous ces chiffres soient nuls, exceptés quelques uns, et que l'on peut ajouter, si besoin est, des termes nuls, sans changer une somme nous permet de ramener l'égalité (1) à :

Il existe n, p des entiers naturels tel que :

$$a_{-p} \, 10^{-p} + \ldots + a_{-1} \, 10^{-1} + a_o + \ldots + a_n \, 10^n =$$
$$a'_{-p} \, 10^{-p} + \ldots + a'_{-1} \, 10^{-1} + a'_o + \ldots + a'_n \, 10^n$$

Multiplions par 10^p la différence des deux écritures, on obtient :

$$(a_n - a'_n) \, 10^{n+p} + \ldots + (a_o - a'_o) \, 10^p + \ldots + (a_{-p} - a'_{-p}) = 0$$

Il est facile de vérifier que :

$|a_i - a'_i| \leqslant 9$ pour $i \in \{p, \ldots, n\}$.

Le lemme nous permet d'écrire : quel que soit $i \in \{-p, \ldots, n\}$ $a_i = a'_i$.

D'où l'unicité de l'écriture décimale d'un décimal. Une remarque d'ordre pratique : on écrit 19,79 pour ... 0019,7900...0...

<u>Multiplication d'un décimal pour une puissance de 10</u>

Soit d un décimal (que l'on peut supposer positif) et $(ai)_{i \in \mathbb{Z}}$ des entiers naturels strictement inférieurs à 10, tous nuls, sauf pour un nombre fini d'entre eux et tel que :

$$d = \sum_{i=-\infty}^{+\infty} a_i \, 10^i \quad \text{égalité que l'on peut écrire :}$$

$$d = \ldots\ 0 \ldots\ a_2\ a_1\ a_o,\ a_{-1}\ a_{-2}\ a_{-3} \ldots\ 0 \ldots\ 0 \ldots$$

soit $d = \ldots + a_2\ 10^2 + a_1\ 10^1 + a_o\ 10^o + a_{-1}\ 10^{-1} + a_{-2}\ 10^{-2} + \ldots$

Soit m un entier, multiplions par 10^m le décimal d, en remarquant "que l'on place la virgule après le coefficient de la puissance 10^o", on vérifie :

. Si m est positif, pour multiplier d par 10^m, il suffit de déplacer la virgule de m rangs vers la droite.

. Si m est négatif, pour multiplier d par 10^m, il suffit de déplacer la virgule de m rangs vers la gauche.

On retrouve ainsi la règle pratique, de multiplication d'un décimal par une puissance de 10.

<u>Un exercice</u> : sur l'ensemble $\mathbb{Z} \times \mathcal{P}$ nous considérons la relation $\mathcal{R}$ définie par : a, b, n, m désignent des entiers, $(a,\ 10^n)\ \mathcal{R}\ (b,\ 10^m)$ si et seulement si on a l'égalité dans $\mathbb{Z}$:

$$a \times 10^{n-\mathrm{Inf}(n,m)} = b \times 10^{m-\mathrm{Inf}(n,m)}$$

Vérifier que la relation $\mathcal{R}$ est une relation d'équivalence, dont la définition est équivalente à la relation S.

Cet exercice nous permet de définir une relation d'ordre total sur $\mathbb{D}$.

<u>On note $\leqslant$ la relation d'ordre sur $\mathbb{Z}$</u>

Nous dirons, avec les notations habituelles :

$$(a,\ 10^n) \leqslant (b,\ 10^m) \quad \text{si} \quad a\ .\ 10^{n-\mathrm{Inf}(n,m)} \leqslant b\ .\ 10^{m-\mathrm{Inf}(n,m)}$$

après avoir vérifié facilement que la relation $\leqslant$ sur $\mathbb{Z} \times \mathcal{P}$ est compatible avec la relation $\mathcal{R}$, nous pouvons conclure que la relation $a\ 10^n \leqslant b\ 10^n$, définie par l'inégalité dans $\mathbb{Z}$ précédente, est indépendante des représentants choisis. De plus, cette relation, est une relation d'ordre total sur $\mathbb{D}$, qui prolonge celle connue sur $\mathbb{Z}$ (prendre $n = o$; $m = o$).

<u>Exercice</u> : Montrez que la relation $\leqslant$ définie sur $\mathbb{D}$ est transitive.

Une indication : $a \cdot 10^n$; $b \cdot 10^m$; $c \cdot 10^p$ étant trois décimaux, utilisez $r = \mathrm{Inf}(n,m,p)$.

<u>Quelques remarques sur la relation d'ordre</u> :

Voyons tout d'abord une proposition :

soit x et y deux éléments de $\mathbb{D}$ tel que $x \leqslant y$ alors quel que soit p élément de $\mathbb{Z}$; $x \times 10^p \leqslant y \times 10^p$.

Nous utiliserons deux remarques facilement vérifiables :

Soient a, b, n, m des entiers :

(1) dire que $a \cdot 10^n \leqslant b \cdot 10^n$ équivaut à dire $a \leqslant b$

(2) dire que $a \cdot 10^m \leqslant b \cdot 10^m$ équivaut à dire : pour tout entier r inférieur à n et m :

$$a \cdot 10^{n-r} \leqslant b \cdot 10^{m-r}$$

Muni de ces deux remarques, montrons la proposition :

Soient $a\,10^n$, $b\,10^m$ deux décimaux tel que $a \cdot 10^n \leqslant b \cdot 10^m$

Soit p un élément de $\mathbb{Z}$, si on pose $r = \mathrm{Inf}(n,m,p)$, on a les relations :

ce sont des inégalités dans $\mathbb{Z}$
$$\begin{cases} a \cdot 10^{n-r} \leqslant b \cdot 10^{m-r} & \text{utilisez (2)} \\ a \cdot 10^{n-r} \cdot 10^{p-r} \leqslant b \cdot 10^{m-r} \cdot 10^{p-r} & ;\ 10^{p-r} \in \mathbb{N}^* \\ a \cdot 10^{n+p-2r} \leqslant b \cdot 10^{m+p-2r} \end{cases}$$

d'où l'inégalité cherché :

$$a \cdot 10^{n+p} \leqslant b \cdot 10^{m+p} \text{ ; utilisez (1).}$$

La proposition est donc montrée.

On pose alors :

$D_+ = \{a \cdot 10^n \ ;\ a \in \mathbb{N} \ ;\ n \in \mathbb{Z}\}$

$D_- = \{a \cdot 10^n \ ;\ a \in \mathbb{Z}- \ ;\ n \in \mathbb{Z}\}$

On a évidemment :

$\mathbb{D}_+ \cup \mathbb{D}_- = \mathbb{D}$; $\mathbb{D}_+ \cap \mathbb{D}_- = \{0\}$

$\mathbb{D}_+ = \{d / d \in \mathbb{D}$ et $d \geqslant 0\}$; $\mathcal{P} \subset \mathbb{D}_+$

$\mathbb{D}_- = \{d / d \in \mathbb{D}$ et $d \leqslant 0\}$.

Ces remarques permettent de montrer que $(\mathbb{D}, +, \times, \leqslant)$ est un anneau totalement ordonné, c'est-à-dire, en particulier :

Quels que soient x, y, z des éléments de $\mathbb{D}$

Si $x \leqslant y$ alors $x + z \leqslant y + z$

Si $\left.\begin{array}{l} x \leqslant y \\ 0 \leqslant z \end{array}\right\}$ alors $x . z \leqslant y . z$

<u>CONCLUSION</u> :

$(\mathbb{D}, +, \times, \leqslant)$ est un sur-anneau de $\mathbb{Z}$, totalement ordonné.

II - <u>LES INVERSIBLES DE $\mathbb{D}$</u>

1°) <u>Vérifier que l'ensemble $U(\mathbb{D})$</u> des inversibles de $\mathbb{D}$, muni de la multiplication, est un groupe abélien.

2°) <u>En remarquant que</u> : $U(\mathbb{D})$ est isomorphe au groupe $\{-1 ; +1\} \times U_+(\mathbb{D})$ (c'est un produit direct de groupes), il suffit d'étudier $U_+(D)$. Montrer que pour tout α entier naturel :

$2^\alpha \in U_+(\mathbb{D})$; $5^\alpha \in U_+(\mathbb{D})$; $10^\alpha \in U_+(\mathbb{D})$; $10^{-\alpha} \in U^+(\mathbb{D})$

Puis : que pour tout α, β des éléments de $\mathbb{N}$:

$2^\alpha . 5^\beta \in U_+(\mathbb{D})$

Enfin, si n désigne un entier relatif :

$2^\alpha . 5^\beta . 10^n \in U_+(\mathbb{D})$.

En fait, nous allons montrer :

$U_+(\mathbb{D}) = \{a . 10^n / n \in \mathbb{Z}$ et $\exists (\alpha, \beta) \in \mathbb{N}^2$; $a = 2^\alpha . 5^\beta\}$.

Nous avons vu : si α, β sont des éléments de $\mathbb{N}$; si n est un entier alors $2^{\alpha} \cdot 5^{\beta} \cdot 10^{n} \in U_{+}(\mathbb{D})$.

Soit maintenant, u un élément de $U_{+}(\mathbb{D})$; en écrivant $U = a \cdot 10^{n}$, montrer que a divise dans $\mathbb{N}$, une puissance de 10 à exposant positif. Conclure.

Exercice : Soit a et b deux éléments de $\mathbb{D}$, tel que $a < b$. On pose $]a, b[= \{x \;/\; x \in \mathbb{D} \text{ et } a < x < b\}$.

Montrer que $]a, b[$ est non vide, et contient une infinité de décimaux. (On peut utiliser le fait que $2 \in U(\mathbb{D})$).

3°) A priori 2^{-1} ou 2^{-3} n'ont pas de sens (en effet, dans ce développement le corps $\mathbb{Q}$ n'est pas connu).

Donnons un sens à ces symboles :

comme 2 admet un inverse dans $\mathbb{D}$; on pose $2^{-1} = 0{,}5$; on pose aussi, pour n un entier naturel :

$$2^{-n} = (2^{-1})^{n} = (0{,}5)^{n}.$$

Si a est un élément de $U(\mathbb{D})$ on pose a^{-1} = inverse de a et pour $n \in \mathbb{N}$; $a^{-n} = (a^{-1})^{n}$.

On vérifie alors : Quels que soient n, m des entiers a, b des éléments de $U(\mathbb{D})$:

$$a^{-n} = (a^{n})^{-1} = (a^{-1})^{n}$$

$$a^{n} \times a^{m} = a^{n+m}$$

$$(a \cdot b)^{m} = a^{m} \times b^{m}$$

Ainsi : 5^{-3} est l'inverse de 5^{3}.

4°)

$$\boxed{U_{+}(\mathbb{D}) = \{2^{\alpha} 5^{\beta},\ \alpha \in \mathbb{Z},\ \beta \in \mathbb{Z}\}}$$

En écrivant ; pour $m \in \mathbb{Z}$; $10^m = 2^m \times 5^m$, montrer que $U_+(\mathbb{D}) \subset \{2^\alpha . 5^\beta ; \alpha \in \mathbb{Z} ; \beta \in \mathbb{Z}\}$, puis conclure.

Montrer que $U_+(\mathbb{D})$ est isomorphe au groupe $\mathbb{Z}^2$.

5°) Deux problèmes

(1)

a) Démontrer que tout décimal non nul est le produit d'un entier naturel étranger à 10, par un inversible de $\mathbb{D}$. Cette décomposition est-elle unique ?

b) On construit une application : h de $\mathbb{D}$ vers $\mathbb{N}$ définie de la façon suivante :

Soit x un élément non nul de $\mathbb{D}$, d'après la question a) il existe un unique couple $(a, u) \in \mathbb{N}^* \times U(\mathbb{D})$ tel que $x = a \times U$. On pose alors $h(x) = a$ (on note $h(x)$: est la hauteur de x).

On pose $h(0) = 0$.

Montrer : quel que soit x élément de $\mathbb{D}$:

$h(x) = 0$ si et seulement si $x = 0$.

quels que soient x et y éléments de $\mathbb{D}$:

$h(x \times y) = h(x) \times h(y)$.

Soient a et b des éléments de $\mathbb{D}$:

on dit a divise b, et on note a/b s'il existe c un élément de $\mathbb{D}$ tel que : $b = a \times c$.

Vérifier : quels que soient x, y des éléments de $\mathbb{D}^*$ si x divise y alors $h(x) \leqslant h(y)$.

Montrer qu'il existe des éléments de D tel que

$x \in \mathbb{D}$, $y \in \mathbb{D}$ et $h(x + y) > h(x) + h(y)$.

Trouver l'ensemble des décimaux égaux à leur hauteur.

c) <u>Calculer</u> :

h(31,25) ; h(-4,2) ; h(18) ; h(-42,78) ; h(3) ; h(15×10^{-3}) ; h(-8,05) ; h(0,0032) ; h(6,2) ; h(-420,3).

Trouver plusieurs décimaux ayant pour hauteur 18.

Cette question c) peut être posée à des élèves de quatrième (bien entendue en modifiant la présentation), la résolution nécessite une bonne connaissance des inversibles de $\mathbb{D}$, et sera le prétexte à l'utilisation de la décomposition d'un entier naturel en produit de facteurs premiers.

d) Que dire de deux décimaux ayant la même hauteur ? Caractériser les décimaux de hauteur 1.

e) Nous avons vu que l'application h n'est pas injective.

Est-elle surjective ?

f) On donne des thèmes d'étude page 44 ; 45.

(2) <u>Nous allons donner la preuve de l'affirmation suivante</u> :

<u>Entre deux éléments distincts de $\mathbb{D}$, il existe un, et par la suite une infinité d'inversibles de $\mathbb{D}$.</u> Cette affirmation qui semble "évidente au début", nécessite pourtant un assez long développement, pour la prouver.

Signalons une démonstration dans le bulletin de l'A.P.M.E.P. n° 314 de Juin 1978 à la page 593.

Cette démonstration est basée sur des résultats d'Arithmétique et sur des propriétés de $\mathbb{D}$.

A l'opposé notre démonstration suppose connu $\mathbb{R}$, les fonctions logarithme et exponentielle. En premier lieu, donnons le

<u>Lemme</u> : a et b désignent deux réels non nuls dont le quotient n'est pas rationnel alors : le sous-groupe additif $a\mathbb{Z} + b\mathbb{Z}$ est dense dans $\mathbb{R}$.

En effet, supposons que le groupe $a\mathbb{Z} + b\mathbb{Z}$ ne soit pas dense alors, il est fermé et de la forme $c\mathbb{Z}$ où c $\mathbb{R}_+^*$ (Voir pour ce fait N. BOURBAKI, fascicule V, Livre III p. 7).

Donc $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$, ce qui contredit le fait que $\frac{a}{b} \notin Q$ (écrire $a = c.n$; $b = c.m$, avec n, m des éléments de $\mathbb{Z}$).

Montrons la proposition :

a et b désignent deux décimaux distincts tel que par exemple $a < b$. On peut supposer de plus $0 < a$.

En effet si ce n'est pas le cas :

soit $a < b < 0$; remarquez que si $U \in U(\mathbb{D})$ alors $-U \in U(\mathbb{D})$

soit $a < 0 < b$ ou $a = 0$; remarquez que : $]\frac{b}{2}, b[\subset]a, b[$.

a et b désignent donc deux décimaux tel que :

$0 < a < b$

d'où $\text{Log } a < \text{Log } b$.

Le lemme nous donne : le groupe $\text{Log } 2\ \mathbb{Z} + \text{Log } 5\ \mathbb{Z}$ est dense dans $\mathbb{R}$. (Il est facile de vérifier que $\text{Log } 2 / \text{Log } 5 \notin \mathbb{Q}$).

Il existe alors deux entiers α et β tel que :

$\alpha \text{ Log } 2 + \beta \text{ Log } 5 \in]\text{Log } a, \text{Log } b[$.

L'exponentielle réelle, fonction strictement croissante, nous permet de conclure :

$2^\alpha . 5^\beta \in]a, b[$ c.q.f.d.

III - LES IDEAUX DE $\mathbb{D}$

$\mathbb{D}$ et $\{0\}$ sont des idéaux de $\mathbb{D}$, nous utilisons le mot idéal propre pour un idéal différent des deux idéaux précédents.

1°) Tout idéal propre de $\mathbb{Z}$ est monogène (c'est à dire engendré par un élément). On dit que $\mathbb{Z}$ est un anneau principal. En voici une preuve : si c'est bien connu : GO TO 2°), sinon : soit I un idéal propre de $\mathbb{Z}$. Vérifier que $I \cap \mathbb{N}^* \neq \phi$, ce qui nous permet de poser $a = \mathrm{Min}(I \cap \mathbb{N}^*)$. Rechercher l'argument qui nous permet d'assurer l'existence du plus petit élément a de $I \cap \mathbb{N}^*$.

Remarquez que $a\,\mathbb{Z} \subset I$. Si x désigne un élément de I écrire les relations exprimant la division euclidienne de x par a (se convaincre que $a \neq o$). Montrer que le reste est élément de I. Vous pouvez conclure.

Ainsi tout idéal de $\mathbb{Z}$ étant monogène, $\mathbb{Z}$ est un anneau principal.

Un anneau principal est un anneau commutatif unitaire, intègre tel que tout idéal est monogène.

Donnons en vrac quelques anneaux principaux :

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ ; \ a \in \mathbb{Z} \ ; \ b \in \mathbb{Z}\}$;

$\mathbb{Z}[i] = \{a + i\,b \ ; \ a \in \mathbb{Z} \ ; \ b \in \mathbb{Z}\}$; l'anneau des entiers de Gauss, $i^2 = 1$.

$\mathbb{R}[X]$; l'anneau des polynômes à un indéterminée à coefficients réels.

$\mathbb{Z}$; on vient de montrer que cet anneau est principal mais $\mathbb{Z}[X]$ n'est pas principal ; $(2) + (X)$ non monogène !

2°) Les idéaux de $\mathbb{D}$:

$\{o\}$ et $\mathbb{D}$ sont des idéaux de $\mathbb{D}$.

Soit I un idéal de $\mathbb{D}$. $I \cap \mathbb{Z}$ est un idéal de Z.

Il existe donc un élément a de $\mathbb{Z}$ tel que $a\,\mathbb{Z} = I \cap \mathbb{Z}$.

Nous avons évidemment $a\mathbb{D} \subset I$; montrons l'autre inclusion x un élément quelconque de I peut s'écrire $b \,.\, 10^n$, $(b, n) \in \mathbb{Z}^2$, comme I est un idéal, b est élément de I, donc de $I \cap \mathbb{Z}$; b est multiple de a dans A donc x est multiple de a, et $a\mathbb{D} = I$.

D'où le résultat que l'on vient de prouver :

$\mathbb{D}$ est un anneau principal. (S'assurer que $\mathbb{D}$ est intègre !).

Remarque : en déduire que tout idéal propre*, de $\mathbb{D}$ est engendré par un entier naturel différent de 1 étranger à 10. Posez-vous le problème de l'unicité d'un tel élément : utilisez, pour répondre à cette question la remarque aisément vérifiable : "Si I est un idéal, d'un anneau A commutatif unitaire, contenant un inversible de A, alors $I = A$".

3°) Les idéaux premiers de $\mathbb{D}$:

Soit A est un anneau ; un idéal P de A est premier s'il vérifie :

Quels que soient a et b des éléments de A, si $a \,.\, b \in P$ alors $a \in P$ ou $b \in P$.

Il est équivalent de dire que l'anneau A/P est intègre. (Vérifier cette proposition).

Montrer que les idéaux propres* et premiers de $\mathbb{Z}$ sont exactement les idéaux engendrés par un nombre premier !

Voyons maintenant les idéaux premiers de $\mathbb{D}$:

Si I désigne un tel idéal propre*, nous savons qu'il est engendré par un entier b naturel étranger à 10, qui engendre aussi $I \cap \mathbb{Z}$. Comme $I \cap \mathbb{Z}$ est un idéal propre* et premier de $\mathbb{Z}$ (le vérifier, si besoin est) b est un nombre premier distinct de 2 et de 5.

---

* *Voir la définition page 17.*

On vient de prouver : tout idéal premier et propre* de $\mathbb{D}$ est de la forme $\mathbb{D}_p$ où p représente un entier naturel premier distinct de 2 et de 5.

Etudier la réciproque (une méthode consiste à utiliser la décomposition de tout décimal en produit d'un entier par une puissance de 10, puis à raisonner sur des éléments de $\mathbb{Z}$).

Ecrivons la conclusion : I est un idéal de $\mathbb{D}$.

I est un idéal propre* et premier si et seulement si Il existe un nombre premier p étranger à 10 tel que : $I = \mathbb{D}_p$

4°) Idéaux premiers, idéaux maximaux :

a) Voici un résultat bien connu : les seuls entiers naturels a qui confèrent à $\mathbb{Z}/a\mathbb{Z}$ une structure de corps, sont les nombres premiers (en redonner une preuve ; il est possible de s'inspirer de ce qui suit).

a étant un nombre premier, il est aisé de vérifier que l'idéal $a\mathbb{Z}$ possède la propriété suivante :

Tout idéal I de $\mathbb{Z}$ contenant strictement $a\mathbb{Z}$, est égal à $\mathbb{Z}$. On dit alors que $a\mathbb{Z}$ est un idéal maximal.

Généralisons : A un anneau, M un idéal de A, $M \neq A$.
M est un idéal maximal si : pour tout idéal I de A :

$M \subsetneq I$ implique $I = A$.

Il est équivalent de dire : A/M est un corps.

Voici une preuve de cette équivalence :

Avec les notations précédentes, supposons que A/M soit un corps et soit I un idéal contenant strictement M.

---

* *Voir la définition page 17.*

y désigne un élément de $I - M$, sa classe (modulo M), $\overline{y}$ est non nulle, donc inversible dans A/M. Il existe, m un élément de M et y' un élément de A tel que :

$1 = m + y'y$; donc $1 \in I$ et $I = A$

Si A/M est un corps alors M est un idéal maximal.

Etudier la réciproque :

Tous ces résultats nous prouvent que : <u>les idéaux maximaux</u> de $\mathbb{Z}$ sont <u>exactement les idéaux premiers de $\mathbb{Z}$</u> (c'est-à-dire <u>ceux engendrés par un nombre premier</u>).

En fait : <u>les deux notions d'idéal premier, d'idéal maximal coïncident dans un anneau principal</u>.

Dans l'anneau $\mathbb{R}[X, Y]$ des polynômes à deux indéterminées X et Y, à coefficients réels, ces notions sont distinctes : en voici la preuve : si c'est connu GO TO b) sinon : $\mathbb{R}[X, Y]$ peut être considéré comme l'anneau des polynômes à une indéterminée Y, à coefficients dans $\mathbb{R}[X]$.

$$\mathbb{R}[X, Y] \simeq \mathbb{R}[X]\,[Y]$$

On remarque que le polynôme $X^2Y + 5Y^2 + X + 3$ peut s'écrire $Y(X^2 + 5Y) + X + 3$.

D'une manière générale, soit $P(X, Y)$ un élément de $\mathbb{R}[X]\,[Y]$, il existe $(n + 1)$ éléments $a_i(X)$ de $\mathbb{R}[X]$ tel que :

$$P(X, Y) = a_n(X) \cdot Y^n + \dots + a_1(X) \cdot Y + a_o(X)$$

que l'on écrit :

$$P(X, Y) = Y \cdot \left[a_n(X) \cdot Y^{n-1} + \dots + a_1(X)\right] + a_o(X)$$

On en déduit, qu'étant donné un polynôme $P(X, Y)$, il existe un polynôme $Q(X, Y)$ et un polynôme $R(X)$ tel que :

$$P(X, Y) = Y \cdot Q(X, Y) + R(X).$$

Cette écriture est unique (utilisez la remarque : si $Y \,.\, P(X, Y) \in \mathbb{R}[X]$ alors $P(X, Y) = 0$; en effet le degré en Y du polynôme $Y \,.\, P(X, Y)$ est nécessairement inférieur ou égal à zéro).

On considère l'application qui à tout polynôme $P(X, Y)$ de $\mathbb{R}[X][Y]$ associe le polynôme $R(X)$ (défini ci-dessus), de $\mathbb{R}[X]$.

$$\varphi : \mathbb{R}[X][Y] \longrightarrow \mathbb{R}[X]$$
$$P(X, Y) \longmapsto R(X).$$

est évidemment un homomorphisme d'anneaux unitaires surjective. Il est facile de vérifier que le noyau de φ est l'idéal de $\mathbb{R}[X][Y]$ engendré par Y : notons le (Y).

On a alors l'isomorphisme d'anneaux :

$$\mathbb{R}[X][Y] / (Y) \simeq \mathbb{R}[X]$$

$\mathbb{R}[X]$ est un anneau intègre : donc (Y) est un idéal premier

$\mathbb{R}[X]$ n'est pas un corps : donc (Y) n'est pas un idéal maximal.

b) Les idéaux maximaux de $\mathbb{D}$:

$\mathbb{D}$ est un anneau principal ; si l'on applique la remarque faite sur les anneaux principaux, on peut conclure tout de suite. Mais il est préférable d'observer ces idéaux de près :

Soit I un idéal maximal de $\mathbb{D}$; $\mathbb{D}/I$ est un corps, qui est évidemment intègre, I est un idéal premier et en particulier il existe un nombre premier p étranger à 10 tel que $I = \mathbb{D}_p$

Tout idéal maximal de $\mathbb{D}$ est un idéal de $\mathbb{D}$ premier (cette proposition reste vraie dans un contexte beaucoup plus vaste).

Voyons la réciproque : p désigne un nombre premier, $p \neq 2$; $p \neq 5$. Soit I un idéal de $\mathbb{D}$ contenant strictement $\mathbb{D}_p$.

Comme $\mathbb{D}_p \cap \mathbb{Z} = p\mathbb{Z}$; $I \cap \mathbb{Z}$ apparait comme un idéal de $\mathbb{Z}$, contenant strictement $p\mathbb{Z}$ (l'inclusion est stricte ; en est-on certain ?). Donc $I \cap \mathbb{Z} = \mathbb{Z}$ et l'idéal I contient 1 ce qui prouve $I = \mathbb{D}$.

Si p est un nombre premier étranger à 10. $\mathbb{D}_p$ est un idéal maximal de $\mathbb{D}$.

Il y a identité entre les notions d'idéal premier, d'idéal maximal, dans $\mathbb{D}$.

En conclusion :

Les idéaux maximaux de $\mathbb{D}$ sont exactement les idéaux engendrés par un nombre premier de $\mathbb{N}$, différent de 2 et 5.

IV - UNE APPLICATION

On se propose d'étudier les anneaux quotients $\mathbb{D}/\mathbb{D}_p$ où p est un nombre premier $(p \neq 2 ; p \neq 5)$. (Cela nous changera du traditionnel $\mathbb{Z}/p\mathbb{Z}$... ; cette affirmation est peut être prématurée).

a) Etude de $\mathbb{D}/3\mathbb{D}$:

Si x est élément de $\mathbb{D}$, $\overline{x}$ désigne sa classe modulo 3 dans $\mathbb{D}/3\mathbb{D}$. Comme $3\mathbb{D}$ est un idéal maximal de $\mathbb{D}$, $\mathbb{D}/3\mathbb{D}$ est un corps commutatif. On considère l'application

$$\mathbb{Z} \xrightarrow{\varphi} \mathbb{D}/3\mathbb{D}$$
$$x \longmapsto \overline{x}$$

montrer que φ est un homomorphisme unitaire d'anneaux (il est possible d'écrire φ comme composée de deux applications connues...). La remarque : "Si un entier est multiple de 3 dans $\mathbb{D}$" ; il est aussi multiple de 3 dans $\mathbb{Z}$; aisément vérifiable, permet de montrer : $\mathrm{Ker}\,\varphi = 3\mathbb{Z}$.

Nous allons prouver que φ est surjertive : pour cela nous utilisons le

Lemme : Pour chaque élément x de $\mathbb{D}$, on peut trouver un décimal d, et un entier n, tel que : $x = 3d + n$.

Montrer, dans un premier temps, par récurrence sur m : que pour tout entier m, il existe un décimal b_m tel que $10^m = 3 \times bm + 1$

On envisagera le cas où m est positif, puis celui où m est négatif.

On peut s'aider des relations :

$10 = 9 + 1 \quad ; \quad 10^{-1} = -0{,}9 + 1.$

Il suffit maintenant d'écrire x sous la forme $a \cdot 10^p$ $(a, p) \in \mathbb{Z}^2$. Conclure.

Ce lemme nous permet de vérifier que φ est surjective : comment ?

D'où la conclusion, résumée ici sous forme d'un diagramme écrit avec les notations habituelles :

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathbb{D}/3\mathbb{D} \\ \mathbb{Z}/3\mathbb{Z} \arrow[ur, "\hat{\varphi}"'] & \end{tikzcd} \qquad n \mapsto \bar{n}$$

π : la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$

φ : la surjection étudiée ci-dessus

$\hat{\varphi}$: l'isomorphisme de corps tel que $\hat{\varphi} \circ \pi = \varphi$.

Donc :

$\boxed{\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{D}/3\mathbb{D}}$; $\mathbb{D}/3\mathbb{D}$ est un corps à 3 éléments !

b) Etude de $\mathbb{D}/q\mathbb{D}$: où q est un nombre premier distinct de 2,5.

Il suffit de vérifier le lemme précédent, dans lequel on aura remplacer 3 par q. Enoncer ce lemme.

Montrons que toute puissance de 10 à exposant négatif, 10^{-n} où $n \in \mathbb{N}$, s'écrit $10^{-n} = q \times d + r$ où d est un décimal et r un entier ; c'est suffisant pour prouver le lemme ! Pourquoi ?

Soit donc n un entier naturel, les hypothèses faites sur q imposent que 10^n et q soient étrangers :

La relation de Bezout nous permet d'affirmer qu'il existe deux entiers λ et μ tel que :

$\lambda\, 10^n + \mu\, q = 1$

D'où $10^{-n} = q \cdot (\mu \cdot 10^{-n}) + \lambda$; le lemme est ainsi prouvé.

Exemple : $n = -1$; $q = 13$ trouver un couple $(d, r) \in \mathbb{D} \times \mathbb{Z}$ tel que $10^{-1} = q \times d + r$.

(Posez-vous le problème de l'unicité de ce couple).

De ce travail, il ressort :

Quel que soit le nombre premier q étranger à 10.

$\mathbb{D}/q\mathbb{D}$ est isomorphe à $\mathbb{Z}/q\mathbb{Z}$.

V - UNE AUTRE QUESTION

1°) Nous avons vu que : $\mathbb{Z}$ est un anneau principal, et pour montrer ce résultat, nous utilisons de façon primordiale la division euclidienne dans $\mathbb{Z}$. Cette façon de procéder se retrouve d'ailleurs lors de l'étude de certains anneaux : $\mathbb{R}[X]$; $\mathbb{Z}[i]$ par exemples. Ces anneaux sont tous munis d'une "division euclidienne" ; plus précisément :

Si A désigne l'un des anneaux précités : il existe une application φ de A^* dans $\mathbb{N}^*$ tel que :

Soient $a \in A^*$; $b \in A^*$

Si a divise b alors $\varphi(a) \leqslant \varphi(b)$.

Il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ et si r est non nul $\varphi(r) < \varphi(b)$.

(On aura reconnu en q et r, dans le cas de $\mathbb{Z}$, le quotient et le reste de la division euclidienne).

On dit que ces anneaux sont des anneaux <u>euclidiens</u>.

Donnons des applications qui "font" des anneaux précédents des anneaux euclidiens.

Pour $\mathbb{Z}$: $\varphi \quad Z^* \longrightarrow N^*$

$$x \longmapsto |x|$$

pour $\mathbb{R}[X]$: $\varphi \quad \mathbb{R}[X]^* \longrightarrow \mathbb{N}^*$

$$P(X) \longmapsto (\text{degré de } P) + 1$$

pour $\mathbb{Z}[i]$: $\varphi \quad \mathbb{Z}[i]^* \longrightarrow \mathbb{N}^*$

$$a + ib \longmapsto a^2 + b^2$$

2°) <u>Nous avons vu que</u> : $\mathbb{D}$ est un anneau principal, mais est-il possible de le classer comme anneau euclidien ?

La réponse est affirmative, et nous montrerons ce résultat de 2 façons différentes. La première démonstration présentée est une conséquence des propriétés intrinsèques de $\mathbb{D}$, la seconde fait appel au théorème de Transfert que l'on montrera et que l'on peut résumer ainsi : "Si A est euclidien alors $S^{-1} A$ est euclidien". (Il est demandé au lecteur de se reporter au 2ème fascicule pour suivre cette deuxième preuve).

Etudions la première démonstration :

$(\mathbb{D}, +, \times)$ est un anneau commutatif, intègre ; afin de montrer que $\mathbb{D}$ est un anneau euclidien, il suffit de donner une application φ de $\mathbb{D}^*$ dans $\mathbb{N}^*$ vérifiant : quels que soient a et b éléments de $\mathbb{D}^*$; si a/b alors $\varphi(a) \leqslant \varphi(b)$ et quels que soient a et b tels que $(a, b) \in \mathbb{D} \times \mathbb{D}^*$.

Il existe un couple $(q, r) \in \mathbb{D} \times \mathbb{D}$ vérifiant :

$a = bq + r$ et si $r \neq 0$ alors $\varphi(r) < \varphi(b)$.

Pour construire l'application $\varphi : \mathbb{D}^* \longrightarrow \mathbb{N}^*$ nous utiliserons :

<u>lemme</u> : <u>Tout élément de $\mathbb{D}^*$ s'écrit de manière unique $a \times c$ où c désigne un inversible de $\mathbb{D}$, et a un entier naturel premier avec 10.</u>

Preuve : Tout élément de $\mathbb{D}^*$ s'écrit $b \times 10^p$ où b est élément de $\mathbb{Z}^*$ et p un élément de $\mathbb{Z}$.

L'égalité $b \times 10^p = \frac{|b|}{\mathrm{PGCD}(10\ ;\ |b|)} \times \mathrm{PGCD}(10\ ;\ |b|).\mathrm{sgn}(b)\ .\ 10^p$ où $\mathrm{sgn}(b) = \frac{b}{|b|}$; nous permet de donner une telle décomposition ; avec les notations du lemme, il suffit de poser :

$$a = \frac{|b|}{\mathrm{PGCD}(10\ ;\ |b|)}\ ;\quad C = \mathrm{PGCD}(10\ ;\ |b|).\mathrm{sgn}(b)\ .\ 10^p\ ;$$

Voyons l'unicité ; soient a' et c' deux éléments de $\mathbb{D}$ tel que $a' \times c' = a \times c$ et $c' \in U(\mathbb{D})$, $a' \in \mathbb{N}^*$ a' étant premier avec 10.

L'égalité $a' = a \times (c\ .\ c'^{-1})$ permet d'obtenir : il existe $G \in U_+(D)$ tel que $a' = a \cdot G$, comme G est élément de $U_+(D)$, il existe α et β deux entiers relatifs tel que $G = 2^\alpha\ .\ 5^\beta$ donc :

$$a' = a\ .\ 2^\alpha\ .\ 5^\beta$$

l'égalité : $a'\ .\ 2^{|\alpha|}.\ 5^{|\beta|} = a\ .\ 2^{|\alpha|+\alpha}\ 5^{|\beta|+\beta}$ et les hypothèses faites sur a et a' donnent :

a/a' et a'/a d'où $a = a'$.

$\mathbb{D}$ est intègre donc $c = c'$, le lemme est démontré.

Construisons l'application φ de $\mathbb{D}^*$ dans $\mathbb{N}^*$.

Si x désigne un élément de $\mathbb{D}^*$; le lemme précédent nous permet d'écrire, de manière unique ; $x = a \times c$ où c est inversible et a un entier naturel premier avec 10.

On pose alors $\varphi(x) = a$.

<u>Etudions les propriétés de cette application</u> :

x et y désignent deux éléments de $\mathbb{D}^*$; écrivons $x = a \times c$; $y = b \times d$ où a et b sont les entiers naturels, c et d les inversibles, donnés par la décomposition de x et de y.

Supposons que x divise y ; il existe donc α un élément de $\mathbb{D}$ tel que $y = \alpha\ .\ x$. La décomposition de α et l'unicité de la décomposition de y, données par le lemme prouvent que a divise b : donc $\varphi(x) \leqslant \varphi(y)$. Concluons : si x divise y alors $\varphi(x) \leqslant \varphi(y)$.

Montrons qu'il existe un couple $(Q, R) \in \mathbb{D} \times \mathbb{D}$ tel que $x = y \cdot Q + R$ et si $R \neq 0$; $\varphi(R) < \varphi(y)$.

La division euclidienne dans $\mathbb{N}$ nous donne un couple $(q, r) \in \mathbb{N}^2$ tel que :

$a = bq + r$ et $0 \leqslant r < b$

d'où $a \times c = b \times d \times (d^{-1} \times c \times q) + rc$

Il suffit de démontrer, pour conclure, que :

si $r \neq 0$ alors $\varphi(r.c) < \varphi(y)$: (1). Voyons ce dernier point.

La décomposition de r nous permet d'écrire : $r = r_1 \times c_1$ où $c_1 \in U(\mathbb{D})$, et $r_1 \in \mathbb{N}^*$; mais $r_1 = \dfrac{r}{\mathrm{PGCD}(10, r)}$ d'où $r_1 \leqslant r$.

Comme $\varphi(rc) = r_1$ et $\varphi(y) = b$ l'inégalité (1) est prouvée.

Il suffit alors de poser :

$Q = d^{-1} \times c \times q$ et $R = r \cdot c$; et on vient de prouver

$\boxed{\mathbb{D} \text{ est un anneau euclidien}}$

<u>Remarque</u> : L'unicité du "quotient" et du "reste" n'est pas assurée comme le montrent les exemples suivants :

$28 = 6 \times 4 + 4$	$\varphi(4) = 1 < \varphi(6) = 3$	; $q = 4$
$28 = 6 \times 3 + 10$	$\varphi(10) = 1 < \varphi(6) = 3$	; $q = 3$
$28 = 6 \times 2 + 16$	$\varphi(16) = 1$ " "	$q = 2$
$28 = 6 \times 8 + -20$	$\varphi(-20) = 1 <$ "	$q = 8$

3°) <u>Un argument</u> "prouvant" qu'il était pratiquement certain que $\mathbb{D}$ est un anneau euclidien.

$\mathbb{D}$ est un anneau principal, et les seuls exemples d'anneaux principaux que l'on a donnés ici sont des anneaux euclidiens ; il faut d'ailleurs reconnaître, qu'il est difficile d'exhiber un exemple d'anneau principal non euclidien ; les exemples donnés étant le plus souvent, d'une étude assez difficile. $\mathbb{D}$, anneau principal fort connu, avait donc de grandes chances d'être euclidien ! et ce n'est pas une démonstration.

4°) <u>L'algorithme</u> (c'est l'application φ de la démonstration) <u>d'anneau euclidien</u>, <u>défini sur $\mathbb{D}$</u>, <u>n'est pas unique</u> loin de là ; il existe une infinité d'algorithmes d'anneaux euclidiens sur $\mathbb{D}$ (se reporter à l'exercice donné sur le second fascicule, pour s'en convaincre).

Cependant celui que l'on a donné, vérifie :

l'application φ, restreinte à l'ensemble des entiers relatifs étrangers à 10, coïncide avec l'algorithme : $\begin{aligned} \mathbb{Z}^* &\longrightarrow \mathbb{N}^* \\ x &\longmapsto |x| \end{aligned}$

On peut résumer ce fait par :

φ prolonge "presque" l'algorithme $\begin{aligned} \mathbb{Z}^* &\longrightarrow \mathbb{N}^* \\ x &\longmapsto |x| \end{aligned}$

<u>Exercice</u> : Montrer que l'application φ défini précédemment n'est pas surjective. Donner une infinité d'éléments de $\mathbb{N}^*$ n'ayant aucun antécédent par φ.

VI - <u>QUELQUES PARTITIONS DE $\mathbb{D}$</u>

(Où l'on découpe $\mathbb{D}$ en tranches plus ou moins fines). Tous les intervalles donnés ici sont des sous-ensembles de $\mathbb{D}$.

1°) Une partition d'un ensemble $\mathcal{E}$ non vide, est une famille non vide de parties de $\mathcal{E}$... c'est bien connu (mais le lecteur est prié de compléter !).

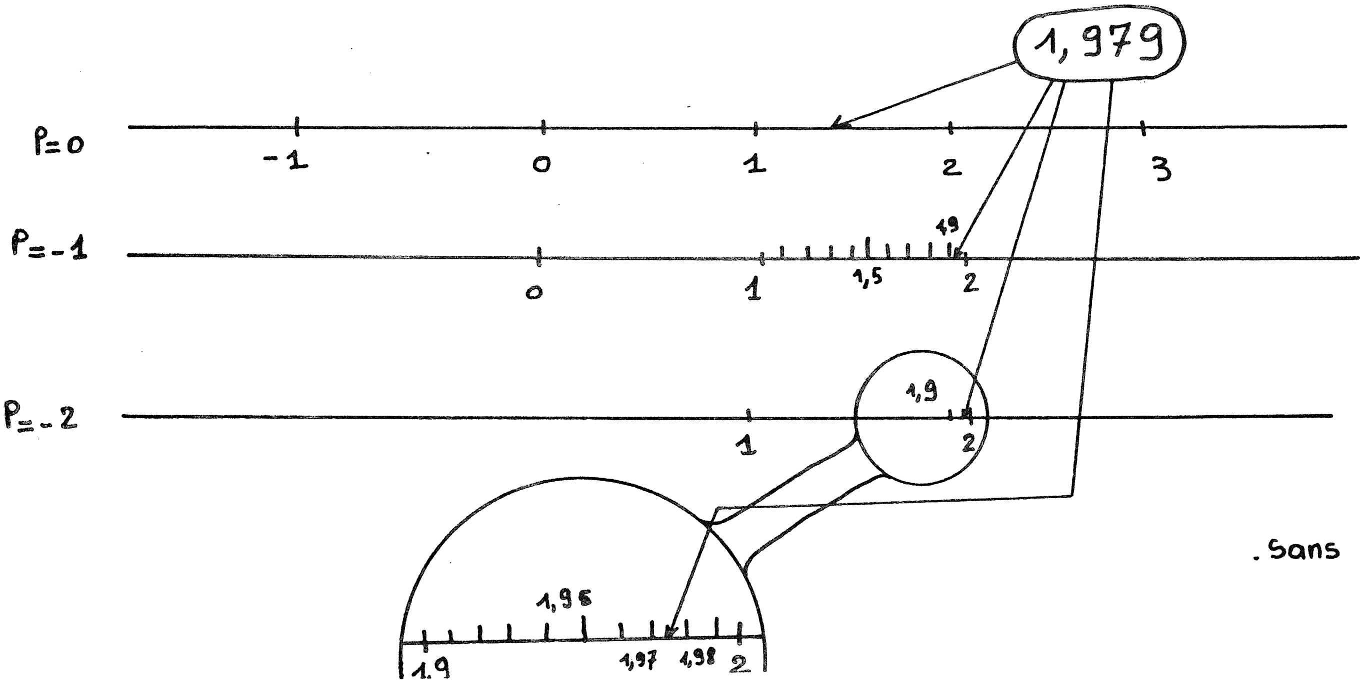
<u>Exercice classique</u> : montrer que : se donner une partition sur $\mathcal{E}$, c'est se donner une relation d'équivalence sur $\mathcal{E}$ et réciproquement.

2°) <u>On se propose de classer les décimaux</u>, en utilisant des partitions de plus en plus fines de $\mathbb{D}$; plus précisément, montrons :

Quels que soient p élément de $\mathbb{Z}$, et d élément de $\mathbb{D}$, il existe un unique entier a tel que :

$$d \in [a \cdot 10^p \; ; \; (a+1) \cdot 10^p[$$

Voici quelques schémas explicatifs :



. Sans paroles.

Pour montrer le résultat annoncé, utilisons le :

<u>Lemme</u> : Pour $p = 0$ le théorème cité précédemment est vrai :

Quels que soit d élément de $\mathbb{D}$, il existe un unique entier a tel que : $a \leqslant d < a + 1$.

(on aura reconnu en a, la partie entière de d, notée $E(d)$ et parfois $[d]$).

Preuve : On peut se ramener à $d \geqslant 0$: en effet si d est négatif strictement, et non entier, il existe $a \in \mathbb{N}$ tel que $a < -d < a + 1$ et dans ce cas :

$$-(a+1) < d < -(a+1) + 1$$

on peut donc se restreindre à $d \in \mathbb{D}+$.

L'unicité s'obtient aisément : voyons l'existence.

Soit $d \in \mathbb{D}+$; d peut s'écrire $b \,.\, 10^n$ où $(b, n) \in \mathbb{N} \times \mathbb{Z}$. Connaissant l'ordre dans $\mathbb{D}$, vérifier que $10^n \leqslant 10^{|n|}$; donc nous avons $b \,.\, 10^n \leqslant b \,.\, 10^{|n|}$.

Il existe donc un entier naturel, en l'occurence $b \,.\, 10^{|n|}$, qui majore d.

La partie $\mathscr{E}$ de $\mathbb{N}$, définie par : $\mathscr{E} = \{m/m \in \mathbb{N} \ ; \ d < m\}$ est non vide. Donc $\mathscr{E}$ admet un plus petit élément, nécessairement non nul, que l'on peut noter $a + 1$ avec $a \in \mathbb{N}$,

d'où $a \leqslant d < a + 1$.

Si l'on tient à s'assurer de l'unicité de a, on peut penser à la remarque suivante : si un entier relatif est strictement inférieur à un autre entier relatif, le suivant du plus petit des deux entiers, est encore inférieur ou égal au plus grand.

Le lemme est ainsi prouvé.

Exercice : Reprendre la démonstration précédente, mais de la façon suivante.

1 - Soit A une partie de $\mathbb{Z}$ non vide, majorée dans $\mathbb{Z}$, montrer que A admet un plus grand élément. (On peut envisager deux cas : $A \cap \mathbb{N} = \phi$; $A \cap \mathbb{N} \neq \phi$).

2 - Montrer que tout décimal $b \,.\, 10^n$ $(b \in \mathbb{Z} \ ; \ n \in \mathbb{Z})$ vérifie $|b \,.\, 10^n| \leqslant |b| \,.\, 10^{|n|}$.

3 - Retrouver que tout décimal appartient à un intervalle $[a, a + 1[$ où $a \in \mathbb{Z}$. Par définition a est la partie entière de d

En résumé :

$\mathscr{T}_o = \{[a, a + 1[\ ; \ a \in \mathbb{Z}\}$ est une partition de $\mathbb{D}$.

Exercices sur les parties entières

Montrer que les propositions suivantes sont fausses :

quels que soient x, y des éléments de $\mathbb{D}$:

(1) $E(x + y) = E(x) + E(y)$

(2) $E(x) \times E(y) = E(x \times y)$

(3) $E(x - y) = E(x) - E(y)$.

Donner $E(0)$; $E(-1)$; $E(0,1)$; $E(-0,1)$; $E(1)$.

Montrer : quels que soient x, y des éléments de $\mathbb{D}$:

si $x \leqslant y$ alors $E(x) \leqslant E(y)$.

On pose $f : \mathbb{D} \longrightarrow \mathbb{D}$

$$x \longmapsto x - E(x)$$

montrer qu'il existe un décimal non nul p tel que :

pour tout x élément de $\mathbb{D}$ $f(x + p) = f(x)$

montrer que l'ensemble des décimaux p, réalisant l'égalité précédente est un sous-groupe additif de $\mathbb{D}$; donnez ce sous-groupe.

Montrons maintenant le théorème :

Soit p un entier relatif ; l'application $\varphi : \mathbb{D} \longrightarrow \mathbb{D}$

$$x \longmapsto x \,.\, 10^p$$

est une bijection strictement croissante (le prouver rapidement). Si x et y désignent deux décimaux tel que $x < y$; l'image de l'intervalle $[x ; y[$ par l'application φ est l'intervalle $[\varphi(x) ; \varphi(y)[$.

d étant fixé, il existe $x_o \in \mathbb{D}$ tel que $\varphi(x_o) = d$, le lemme précédent donne ; il existe $a \in \mathbb{Z}$ tel que :

$$a \leqslant x_o < a + 1 \quad \text{d'où} \quad \varphi(a) \leqslant \varphi(x_o) < \varphi(a + 1)$$

d'où $a \,.\, 10^p \leqslant d < (a + 1)10^p$. Réciproquement si $d \in [a \,.\, 10^p ; (a + 1)10^p[$ $\varphi^{-1}(d) \in [a, a + 1[$ (car φ^{-1} est une bijection strictement croissante) et nécessairement $a = E(d \,.\, 10^{-p})$.

Donc il existe un unique entier a tel que $d \in [a \,.\, 10^p, (a + 1) \,.\, 10^p[$.

On peut démontrer ce théorème sans utiliser l'artifice de l'application φ, mais elle nous rendra service par la suite.

<u>Exemples</u> : encadrer par des décimaux du type $[a \, . \, 10^p, (a + 1)10^p[$ où $a \in \mathbb{Z}$, le décimal $-1,979$ pour $p = 100$; $p = 1$; $p = -2$; $p = -3$.

Si l'on calcule l'amplitude (c.a.d. la longueur) d'un intervalle $[a \, . \, 10^p, (a + 1)10^p[$ on obtient 10^p ; est-ce les seuls intervalles ayant cette propriétés ?

Dans notre exemple : $10^{100} > 10^1 > 10^{-2} > 10^{-3}$, on obtient un encadrement de $-1,979$ de plus en plus fin.

3°) <u>Le partage de $\mathbb{D}$ en sections de plus en plus fines</u>

Si p est un élément de $\mathbb{Z}$, on pose :

$$\mathcal{F}_p = \{[a \, 10^p, (a + 1)10^p[\; ; \; a \in \mathbb{Z}\}.$$

d'après le théorème précédent $\mathcal{F}_p$ est une partition de $\mathbb{D}$. Nous avons alors le résultat :

Quels que soient p et q des éléments de $\mathbb{Z}$, si $p \leqslant q$ alors $\mathcal{F}_p$ est plus fine que $\mathcal{F}_q$.

(ce qui signifie : pour chaque élément de $\mathcal{F}_p$, il existe un élément de $\mathcal{F}_q$ qui le contient).

En premier lieu ; montrons le

<u>Lemme</u> : Soit n un entier strictement négatif, et a un entier, il existe alors un entier b tel que :

$$[a \, . \, 10^n, (a + 1)10^n[\subset [b, b + 1[$$

Deux cas sont à envisager :

$$\text{(a) } E(a \, . \, 10^n + 10^n) = E(a \, . \, 10^n)$$

par exemple : $a = 295$; $n = -2$; $a \, . \, 10^n = 2,95$; $(a + 1)10^n = 2,96$, et $E(295 \, . \, 10^{-2} + 10^{-2}) = E(295 \, . \, 10^{-2})$.

La définition de la partie entière d'un décimal et la relation précédente, nous permettent d'écrire :

$$E(a \, . \, 10^n) \leqslant a \, . \, 10^n < a \, . \, 10^n + 10^n < E(a \, . \, 10^n) + 1$$

il suffit alors de poser $b = E(a \, . \, 10^n)$ et $b \in \mathbb{Z}$.

$$(b)\ E(a\ .\ 10^n + 10^n) > E(a\ .\ 10^n)$$

par exemple : $a = 299$; $n = -2$; vérifiez la relation b) dans ce cas particulier.

Nous pouvons d'ailleurs apporter une précision :

comme $a\ .\ 10^n < E(a\ .\ 10^n) + 1$ (par définition de la partie entière)

$10^n + a\ .\ 10^n < E(a\ .\ 10^n) + 1 + 10^n < E(a\ .\ 10^n) + 2$; car $10^n < 1$

d'où $E(a\ .\ 10^n + 10^n) < E(a\ .\ 10^n) + 2$

D'où la relation (b) devient :

$$E(a\ .\ 10^n + 10^n) = E(a\ .\ 10^n) + 1.$$

Sous ces hypothèses, montrer que :

(1) $[E(a\ .\ 10^n) + 1]\ .\ 10^{-n} \leqslant a + 1$

Comme $a\ .\ 10^n < E(a\ .\ 10^n) + 1$ (définition de la partie entière)

alors $a < [E(a\ .\ 10^n) + 1]\ .\ 10^{-n}$ (Multiplication par 10^{-n})

donc $a + 1 \leqslant [E(a\ .\ 10^n) + 1]\ .\ 10^{-n}$ (Propriété remarquable de la relation d'ordre dans $\mathbb{N}$)

d'où $a + 1 = [E(a\ .\ 10^n) + 1]\ .\ 10^{-n}$ (Utilisez la relation (1))

et $(a + 1)10^n = E(a\ .\ 10^n) + 1.$

Il devient facile de vérifier que :

$$[a\ .\ 10^n\ ;\ (a + 1)10^n[\ \subset\ [E(a\ .\ 10^n)\ ;\ E(a\ .\ 10^n) + 1[$$

et l'on pose : $b = E(a\ .\ 10^n)$.

(Remarquons que ce cas b) généralise le fait que : $2{,}99 + 10^{-2} \in \mathbb{Z}$).

Le lemme est prouvé : voyons maintenant le théorème :

Soient $p < q$ deux entiers, $\mathcal{F}_p$ et $\mathcal{F}_q$ les familles définies ci-dessus. Soit $[a\ .\ 10^p\ ;\ (a + 1)\ .\ 10^p\ [\ \in \mathcal{F}_p$, posons $n = p - q$, comme n est négatif, nous pouvons appliquer le lemme précédent : il existe un entier b tel que :

$[a\ .\ 10^n\ ;\ (a + 1)\ .\ 10^n[\ \subset [b\ ;\ b + 1[$, ce qui s'écrit encore :

$$[a\ .\ 10^{p-q}\ ;\ (a + 1)10^{p-q}[\ \subset [b\ ;\ b + 1[$$

Les propriétés de l'application : $\varphi : \mathbb{D} \longrightarrow \mathbb{D}$

$$x \longmapsto x \, . \, 10^q$$

nous donnent $[a \, . \, 10^p \, ; \, (a+1)10^p[\, \subset \, [b \, . \, 10^q \, ; \, (b+1)10^q[$.

Donc pour chaque élément de $\mathcal{F}_p$, il existe un élément de $\mathcal{F}_q$ qui le contient.

<u>En conclusion</u> : les familles $(\mathcal{F}_p)_{p \in \mathbb{Z}}$ sont des partitions de $\mathbb{D}$ vérifiant : p, q désignent deux entiers ; si $p \leqslant q$ alors $\mathcal{F}_p$ est plus fine que $\mathcal{F}_q$.

Ce résultat correspond à une remarque qui semble bien naturelle : si l'on connaît l'encadrement d'un décimal d de la forme $[a \, . \, 10^{-4}, \, (a+1)10^{-4}[$, et bien on connaît les encadrements de ce type, de d, d'amplitude 10^{-3} ; 10^{-2} ; 10^p, pourvu que $p \geqslant -4$.

<u>Exemples</u> : $x \in \mathbb{D}$, si $x \in [2{,}95 \, ; \, 2{,}96[$

alors $x \in [2{,}9 \, ; \, 3[$ ou bien ; $x \in [2 \, ; \, 3[$ ou $x \in [0 \, ; \, 10[$ etc...

VII - <u>DES FAIBLESSES ET DES INSUFFISANCES DE $\mathbb{D}$</u>

A) <u>Le problème de l'inverse approché dans $\mathbb{D}_+^*$</u>

1°) Certains décimaux non nuls n'ont pas d'inverse (3 par exemple) dans $\mathbb{D}$, ou autrement dit, l'équation $3x = 1$ n'admet pas de solution dans $\mathbb{D}$; d'où une faiblesse de l'ensemble $\mathbb{D}$. On peut alors se poser la question : existe-t-il un décimal qui multiplié par 3, approche suffisamment 1 ? (avec un écart fixé à l'avance).

Précisons : p étant un entier fixé, existe-t-il un entier a tel que

$$1 \in [3 \, . \, a \, . \, 10^p \, ; \, 3(a+1) \, . \, 10^p[\ ? \quad \text{(Unicité de } a \text{ ?)}$$

Avant de répondre à cette question, revenons sur certains détails :

Montrons que 3 n'a pas d'inverse dans $\mathbb{D}$: (la démonstration qui suit a été donnée en 4ème et comprise par un bon groupe d'élèves).

Nous avons besoin d'un résultat intermédiaire :

Quel que soit l'entier naturel n ; 3 ne divise pas, dans $\mathbb{N}$, 10^n.

En voici une preuve :

Soit n un entier naturel :

10^n s'écrit $\underbrace{99...9}_{n \text{ chiffres}} + 1$; (les élèves semblent convaincus de ce fait ; si on[1] ne l'est pas, le montrer par récurrence à partir de la formule : $10^n = (10^{n-1} + 9 \cdot 10^{n-1})$; nous faisons alors une démonstration par l'absurde (belle occasion pour présenter ce type de démonstration).

Supposons que 3 divise 10^n ; comme $10^n = \underbrace{9...9}_{n \text{ chiffres}} + 1$, 3, divisant le nombre 9...9, divise la différence $10^n - 9...9$, c'est-à-dire 1, ce qui est absurde.

Donc 3 ne divise pas 10^n.

Une autre preuve de ce résultat intermédiaire

(Nous présentons cette démonstration car elle est aisément généralisable pour un nombre premier autre que 2 ; 5).

Comme $10 = 2 \times 5$ on a $10^n = 2^n \times 5^n$. On rappelle que la décomposition d'un entier en facteurs premiers est unique. 3 ne divise pas 10^n, puisque 3 n'apparaît pas dans la décomposition de 10^n.

Enfin une dernière preuve

Si $n \in \mathbb{N}^*$, 10^n s'écrit en base 10, uniquement avec le chiffre 1, une fois employé, et le chiffre 0.

---

(1) On : remplace le lecteur et non pas les élèves !

La somme des chiffres de l'écriture de 10^n, est 1, et n'est pas multiple de 3 ; donc 3 ne divise pas 10^n.

Utilisons ce résultat intermédiaire pour prouver que 3 n'a pas d'inverse dans $\mathbb{D}$:

Nous referons une démonstration par l'absurde :

Supposons que 3 ait un inverse dans $\mathbb{D}$; il existe, alors, a et n deux entiers tel que :

$3 \cdot a \cdot 10^n = 1$: cette égalité implique : $a \in \mathbb{N}^*$

on a : $3a = 10^{-n}$ et comme $a \geqslant 1$ alors $3a \geqslant 3$ et $10^{-n} > 1$; $-n$ est donc un entier positif.

$3a = 10^{-n}$ se traduit en français par : 3 est un diviseur dans $\mathbb{N}$, d'une puissance de 10 à exposant positif ; ce qui est absurde.

<u>3 n'a pas d'inverse dans $\mathbb{D}$</u>.

<u>Exercice</u> :

(a) Montrer que 6 n'a pas d'inverse dans $\mathbb{D}$. Trouver une partie infinie de $\mathbb{D}$, constituée d'éléments non inversibles.

(b) Soit p un nombre premier strictement plus grand que 5 ; montrer en utilisant la méthode précédente que p n'a pas d'inverse dans $\mathbb{D}$.

2°) <u>Réponse à la question posée</u> : (voir page 35 : "Précisons")

<u>Théorème</u> : Etant donné un entier p, et un décimal d strictement positif, il existe un unique entier naturel a tel que :

$1 \in [d \cdot a \cdot 10^p \,;\, d \times (a+1) \cdot 10^p[$

<u>Par définition</u>

$a \cdot 10^p$ est l'inverse décimal approché à 10^p près par défaut de d

$(a+1) \cdot 10^p$ est l'inverse décimal approché à 10^p près par excès de d.

<u>Preuve du théorème</u> :

(On indique dans cette démonstration, la recherche de l'entier a ; cependant on pourrait parfaitement poser : soit a le quotient de la division euclidienne de $10^{|n+p|}$ par $b \,.\, 10^{p+n+|n+p|}$ avec bien entendu les notations utilisées ci-dessous.

On préférera expliquer comment on aboutit à considérer ce quotient). Si l'on choisit d'étudier un cas particulier tout d'abord on passera au n° 3 ; on reviendra ensuite au cas général.

Soit $p \in \mathbb{Z}$; vérifier que $10^{p+|p|} \in \mathbb{N}^*$

Soit $d \in D_+^*$; il existe $(b, n) \in \mathbb{N}^* \times \mathbb{Z}$ tel que : $d = b \,.\, 10^n$.

Analyse du problème :

Supposons qu'il existe $a \in \mathbb{Z}$ tel que

$$d \,.\, a \,.\, 10^p \leqslant 1 < d \,.\, (a+1) \,.\, 10^p$$

on a $a \,.\, b \,.\, 10^{p+n} \leqslant 1 < (a+1) b \,.\, 10^{p+n}$

d'où $a \,.\, (10^{p+n+|p+n|} \,.\, b) \leqslant 10^{|p+n|} < (a+1) \,.\, (10^{n+p+|n+p|} \,.\, b)$

si l'on pose accessoirement $c = 10^{n+p+|n+p|} \,.\, b$; $c \in \mathbb{N}^*$ et

$a \,.\, c \leqslant 10^{|p+n|} < (a+1) \,.\, c$.

a apparaît comme le quotient exact de la division euclidienne de $10^{|p+n|}$ par c.

Synthèse du problème :

Vérifier que le quotient de la division euclidienne de $10^{|n+p|}$ par $b \,.\, 10^{n+p+|n+p|}$ convient, et nous donne l'existence de l'entier a cité dans le théorème.

Faisons une remarque sur l'unicité de a :

Soient a et b deux entiers définis par les relations :

$a \,.\, 10^p \,.\, d \leqslant 1 < (a+1) 10^p\, d$ et $b \,.\, 10^p \,.\, d \leqslant 1 < (b+1) 10^p\, d$

Si les entiers a et b ne sont pas égaux ; l'un d'eux est le plus grand ; supposons que ce soit a. On en déduit : $b + 1 \leqslant a$ d'où :

$(b + 1) \cdot 10^p \cdot d \leqslant a \cdot 10^p \cdot d$

ce qui donne :

$1 < b + 1 \cdot 10^p \cdot d \leqslant a \cdot 10^p \cdot d \leqslant 1$: contradiction.

D'où l'unicité de l'entier a.

3°) <u>Voyons un exemple ne posant pas de problème à un élève de 4ème</u> : $d = 6{,}23$; $p = -3$.

Supposons qu'il existe un entier a tel que

$a \cdot 10^{-3} \cdot 6{,}23 \leqslant 1 < (a + 1) \cdot 10^{-3} \cdot 6{,}23$

D'où $a \cdot 623 \leqslant 10^5 < (a + 1) \cdot 623$.

a est le quotient de la division euclidienne de 10^5 par 623.

On trouve $a = 160$.

Réciproquement : $a = 160$ convient parfaitement.

$a \cdot 10^{-3} = 0{,}16$ est donc l'inverse décimal par défaut à 10^{-3} près de 6,23.

De plus :

$6{,}23 \times 0{,}160 = 0{,}9968$

$6{,}23 \times 0{,}161 = 1{,}00303$

$0{,}9968 \leqslant 1 < 1{,}00303$

donc "0,16 porte bien son nom d'inverse approché par défaut de 6,23".

<u>Exercice</u> : Donner l'inverse approché par défaut, $a \cdot 10^p$, de 6,23 pour $p = -2$; $p = 0$; $p = 100$.

Donner l'inverse par défaut à 10^{-7} près de 19, puis le produit de 19 par ce résultat. (Conseil : se munir d'une calculette ; entrer l'entier 19, puis appuyer sur la touche 1/X).

4°) <u>Une remarque</u> (et les négatifs alors ?)

Pourquoi ne s'intéresse-t-on qu'aux inverses approchés de décimaux positifs ? Voici une réponse :

Soit d un décimal strictement négatif et $p \in \mathbb{Z}$.

Prouver qu'il n'existe pas d'entier b tel que :

$10^p \,.\, b \,.\, d \leqslant 1 < 10^p \,.\, d \,.\, (b + 1)$.

On ne peut donc pas généraliser la définition donnée pour les décimaux positifs.

On peut tout de même chercher à définir l'inverse approché à 10^p près, par excès et par défaut de d ; en effet : soit $a \,.\, 10^p$ l'inverse par défaut de $-d$: ($-d$ est positif).

Dans un premier temps on posera : (A)

$-a\ 10^p$ est l'inverse par défaut de d

$-(a+1)10^p$ " " excès de d

et l'on a : $d \times -a \,.\, 10^p \leqslant 1 < d \,.\, 10^p[-(a + 1)]$

Prenons par exemple :

$d = -6,23$

$-a \,.\, 10^{-3} = -160 \,.\, 10^{-3}$

et $-160 \times 10^{-3} - 6,23 \leqslant 1 < -161 \times 10^{-3} \,.\, -6,23$

et la définition de l'inverse par défaut : $-160 \,.\, 10^{-3}$ semblerait ne pas se prêter à des objections. Cependant : l'ensemble $\mathbb{Q}$ étant connu, on remarque que les notions d'approximation décimale par défaut (ou excès) d'ordre 3 près de $\frac{1}{6,23}$ et d'<u>inverse</u> approché à 10^{-3} près de 6,23 coïncident : ce qui est logique. Mais si l'on adopte notre définition (A) pour $-6,23$, celle-ci ne coïncide plus avec l'approximation décimale de $\frac{1}{-6,23}$ (dans $\mathbb{Q}$) : (Le vérifier pour s'en assurer).

Voilà quelques raisons pour lesquelles on choisit dans ce paragraphe des décimaux positifs.

<u>Exercice</u> : Reprendre l'exemple donné en 3°) mais en choisissant pour d un inversible positif.

B) L'équation $x^2 = 2$ n'a pas de racine dans $\mathbb{D}$

En voici une preuve : Supposons en effet qu'il existe un décimal, que l'on écrit $a \cdot 10^p$ où a et p désignent deux entiers, tel que :

$$a^2 \cdot 10^{2p} = 2$$

cette égalité nous prouve que $p < 0$ et $a \neq 0$.

D'où l'égalité entre entiers naturels :

$$a^2 = 2 \cdot 10^{-2p}$$

L'unicité de la décomposition en produit de facteurs premiers de a nous montre que l'on aboutit à une contradiction. (En effet, remarquer que dans la décomposition primaire du terme écrit à gauche, 2 apparaît à une puissance paire ; alors que dans celle de droite, 2 apparaît à une puissance impaire).

<u>Exercice</u> : Recherchez une infinité d'équations du type $x^2 = A$ où $A \in \mathbb{D}_+$, n'ayant pas de racines dans $\mathbb{D}$. Que dire des équations :

$$x^2 = 0{,}4 \quad ; \quad x^2 = 0{,}04 \ ?$$

Par analogie avec le paragraphe précédent, on peut se poser la question de l'existence (et de l'unicité) d'un décimal, dont le carré approche suffisamment 2.

Plus précisément : p étant fixé, existe-t-il un décimal $a \cdot 10^p$, $(a, p) \in \mathbb{Z}^2$, tel que :

$$(a \cdot 10^p)^2 \leqslant 2 < [(a+1) \cdot 10^p]^2 \ ?$$

<u>Exemple</u> : pour $p = -3$ essayer l'entier $a = 1414$.

Si l'on désire observer un exemple avant d'étudier le cas général GOTO 2°).

Etudions le cas général : nous avons le

<u>Théorème</u> : Soit d un décimal positif et p un entier relatif, il existe un unique entier naturel a tel que :

$$a^2 \cdot 10^{2p} \leqslant d < (a+1)^2 \quad 10^{2p}$$

Donnons une conséquence immédiate de ce résultat :

La famille d'intervalles $\{[a^2 \,.\, 10^{2p} \,;\, (a+1)^2 \,.\, 10^{2p}[\,;$ $a \in \mathbb{N}\}$ est une partition de $\mathbb{D}+$; on s'assurera que deux éléments distincts de cette famille, sont disjoints.

Preuve du théorème : Nous utilisons le

<u>Lemme</u> : Etant donné un décimal d positif, il existe un unique entier naturel a tel que :

$$a^2 \leqslant d < (a+1)^2$$

remarquons que ce lemme est la simple traduction du théorème pour $p = 0$.

Afin de prouver ce lemme posons : $\mathcal{E} = \{n \,/\, n \in \mathbb{N} \text{ et } n^2 \leqslant d\}$ est une partie non vide de $\mathbb{N}$, majorée par l'entier naturel $E(d) + 1$; soit donc a le plus grand élément de $\mathcal{E}$; alors

$$a^2 \leqslant d < (a+1)^2.$$

Se convaincre alors de l'unicité de a.

Nous sommes en mesure de montrer le théorème :

Soit $p \in \mathbb{Z}$; appliquer le lemme précédent au décimal positif $d \,.\, 10^{-2p}$ puis conclure.

<u>Nous poserons</u> :

$a \,.\, 10^p$ est la racine carrée décimale approchée par défaut, à 10^p près de d.

2°) <u>Etude d'un exemple</u>

Quelle est la racine carrée décimale par défaut de 3 à 10^{-3} près :

Recherchons l'entier naturel a tel que :

$$(a \,.\, 10^{-3})^2 \leqslant 3 < ((a+1) \,.\, 10^{-3})^2$$

soit $a^2 \leqslant 3 \,.\, 10^6 < (a+1)^2$.

Si l'on dispose d'une table des carrés on obtient :

$$(1732)^2 \leqslant 3 \,.\, 10^6 < (1733)^2.$$

Sinon on procède par approximations successives :

$a \in [1000, 2000[$

puis $a \in [1500, 2000[$

$a \in [1700, 1800[$

etc, mais c'est plus long !

Finalement : la racine carrée par défaut à 10^{-3} près de 3 est 1,732.

3°) <u>Il semble raisonnable de penser</u> :

Si l'on connaît la racine carrée par défaut du décimal d à 10^{-3} près, on la connaît aussi à 10^{-2} près, à 10^{p} près pourvu que $p \geqslant -3$.

Autrement dit :

Soit $p \in \mathbb{Z}$; soit $d \in \mathbb{D}+$, désignons par a l'entier naturel tel que : $d \in [(a\ 10^{p})^2\ ;\ ((a+1)\ .\ 10^{p})^2[$

Soit $q \in \mathbb{Z}$ tel que $p \leqslant q$, existe-t-il un entier b tel que $[(b\ .\ 10^{q})^2\ ;\ ((b+1)\ .\ 10^{q})^2[$ contienne l'intervalle $[(a\ 10^{p})^2\ ;\ ((a+1)\ .\ 10^{p})^2[$?

Ce problème peut se formuler différemment ; pour cela, on pose $\mathcal{R}_p = \{[a^2\ .\ 10^{2p}\ ;\ (a+1)^2\ .\ 10^{2p}[\ ;\ a \in \mathbb{N}\}$ et, quel que soit p entier, $\mathcal{R}_p$ est une partition de $\mathbb{D}+$.

<u>Prouvons que</u> :

Si p et q désignent deux entiers tel que $p \leqslant q$, alors $\mathcal{R}_p$ est plus fine que $\mathcal{R}_q$.

Soient donc p et q deux entiers relatifs $(p \leqslant q)$ et $[a^2\ 10^{2p},\ (a+1)^2\ 10^{2p}[$ un élément de $\mathcal{R}_p$: nous avons vu dans un paragraphe précédent qu'il existe un entier b tel que :

$[a\ .\ 10^{p}\ ;\ (a+1)10^{p}[\ \subset\ [b\ .\ 10^{q}\ ;\ (b+1)\ .\ 10^{q}[$; nous faisons allusion au fait que $\mathcal{T}_p$ est plus fine que $\mathcal{T}_q$; vérifier que $b \in \mathbb{N}$.

D'où : $b \cdot 10^q \leqslant a \cdot 10^p < (a+1) \cdot 10^p \leqslant (b+1) \cdot 10^q$

Le fait que la fonction $\begin{array}{rcl} \mathbb{D}+ & \longrightarrow & \mathbb{D}+ \\ x & \longmapsto & x^2 \end{array}$ soit strictement croissante

nous permet de conclure.

Un peu de géométrie !

Projecteur : comme tout décimal non nul x se décompose d'une manière unique en $a \times U$ où $U \in U(\mathbb{D})$ et où a est un entier naturel étranger à 10 ; on peut poser :

$\mathbb{D}^* = \mathcal{E} \otimes U(\mathbb{D})$ où $\mathcal{E}$ désigne l'ensemble des entiers naturels étrangers à 10. On remarquera que

$\mathcal{E} \cap U(D) = \{1\}$.

L'application h définie par $h(x) = a$, avec les notations précédentes, est une application de $\mathbb{D}^*$ sur $\mathcal{E}$; tel que, pour tout x, y de $\mathbb{D}^*$ $h(x.y) = h(x) \cdot h(y)$ et pour tout x de $U(\mathbb{D})$: $h(x^{-1}) = [h(x)]^{-1}$
Si l'on cherche le "noyau de h", c'est à dire : $\{x \,/\, x \in \mathbb{D}^*, h(x) = 1\}$ on trouve bien entendu $U(\mathbb{D})$. De plus, pour tout x de $\mathbb{D}^*$ $h \circ h(x) = h(x)$. Quelques abus de langage permettent de qualifier h "de projecteur sur $\mathcal{E}$ parallèlement à $U(\mathbb{D})$".

L'application g, qui à tout x de $\mathbb{D}^*$ (s'écrivant $a \cdot U$, $U \in U(\mathbb{D})$ a étranger à 10) associe U est le "projecteur sur $U(\mathbb{D})$ parallèlement à $\mathcal{E}$". En effet :

$\forall x \in \mathbb{D}^*$ $g \circ g(x) = g(x)$

$\{x \,/\, x \in \mathbb{D}^*, \; g(x) = 1\} = \mathcal{E}$

$g(\mathbb{D}^*) \subset U(\mathbb{D})$

$g(x.y) = g(x) \times g(y)$

On a alors :

$\forall x \in \mathbb{D}^*$ $g \circ h(x) = 1 = h(g(x))$

$x = h(x) \times g(x)$.

On a de même $D_+^* = \mathcal{E} \otimes U + (\mathbb{D})$; et pour tout x de D_+^*, $x = h(x) \times g(x)$.

Affinité :

Soit α un entier relatif non nul et différent de 1 ; avec les notations précédentes : l'application Af définie par :

$Af(x) = h(x) \times [g(x)]^{\alpha}$ vérifie :

Pour tout x, y éléments de $\mathbb{D}_+^*$, $Af(x \times y) = Af(x) \times Af(y)$ et pour tout z de $U_+(\mathbb{D})$, $Af(z^{-1}) = [Af(z)]^{-1}$

"Le noyau de Af" est réduit à {1} et les hypothèses faites sur α imposent, que les invariants de Af constituent l'ensemble $\mathcal{E}$. Af, après quelques abus de langage", peut être appelée : Affinité de rapport α, de base $\mathcal{E}$, de direction $U_+(\mathbb{D})$.

Symétrie par rapport à $\mathcal{E}$:

On pose pour tout x de $\mathbb{D}_+^*$:

$s_{\mathcal{E}}(x) = h(x) \times [g(x)]^{-1}$

Après avoir vérifié que, pour tout x, y de $\mathbb{D}_+^*$, $s_{\mathcal{E}}(xy) = s_{\mathcal{E}}(x) \times s_{\mathcal{E}}(y)$ et pour tout z de $U_+(\mathbb{D})$, $s_{\mathcal{E}}(z^{-1}) = [s_{\mathcal{E}}(z)]^{-1}$, et que $s_{\mathcal{E}}^2 = Id_{\mathbb{D}^*}$, on s'aperçoit que l'ensemble $\mathcal{E}$ est l'ensemble des invariants de $s_{\mathcal{E}}$. On peut écrire :

$\mathbb{D}_+^* = \{x \mid x \in \mathbb{D}_+^*,\ s_{\mathcal{E}}(x) = x\} \otimes \{x \mid x \in U_+(\mathbb{D})\ ;\ s_{\mathcal{E}}(x) = x^{-1}\}$.

s peut apparaître comme la "symétrie par rapport à $\mathcal{E}$; parallèlement à $U_+(\mathbb{D})$".