UNIVERSITÉ LOUIS PASTEUR
IREM
10, RUE DU GÉNÉRAL ZIMMER
67084 STRASBOURG CEDEX
TÉL. (88) 35 34 02

DES ENTIERS AUX RÉELS

1973

PRESENTATION

Lorsqu'on a la curiosité de consulter les divers manuels scolaires en usage dans le second cycle, on est rapidement étonné de voir combien les diverses présentations de l'ensemble $\mathbb{R}$ "escamotent" en quelque sorte l'essentiel du problème.

Pour quelle(s) raison(s) a-t-on besoin de réels ? Qu'apportent-ils de plus que les éléments de $\mathbb{Q}$? Pourquoi la structure de corps de ce dernier ensemble ne suffit-elle pas à résoudre les problèmes rencontrés au niveau de l'enseignement secondaire ?

Nous nous sommes efforcés de répondre à ces diverses questions et nous avons rassemblé ici le résultat de nos réflexions.

En fait, très vite nous avons constaté l'impossibilité de parler des réels sans partir de plus haut.... et nous avons finalement choisi de présenter une construction cohérente complète des ensembles de nombres de $\mathbb{N}$ à $\mathbb{R}$: ceci fait l'objet de la première partie.

Dans la deuxième partie, nous reprenons certains chapîtres sous un autre aspect : tel qu   est (ou peut être) présenté actuellement dans l'enseignement secondaire (ou même primaire pour les cardinaux). Ainsi, au lieu de "passer" de $\mathbb{Z}$ à $\mathbb{R}$ par l'intermédiaire des rationnels on préfère (en $4^{\text{ème}}$) construire les décimaux puis directement les réels. Mais il ne s'agit ni d'un cours type ni même de remplacer un manuel. Notre but était de fournir aux <u>enseignants</u> une justification <u>théorique</u> accessible de ce qu'ils ont à enseigner. Ce faisant nous avons bien conscience de n'avoir réalisé que la partie la plus facile du travail d'un enseignant.....Mais il faut bien commencer!......

1ère Partie

1. LES ORDINAUX : Construction de N

Dans l'enseignement secondaire on construit Z,Q,R en considérant que l'ensemble N est connu..
Une construction axiomatique de N peut se baser sur les axiomes de Péano (1889).
L'introduction du langage ensembliste permet d'exposer cette théorie d'une manière relativement simple, c'est ce que nous ferons ici en nous inspirant largement du livre de R. Halmos (Introduction à la théorie des ensembles. Gauthier Villars).

I Définition de l'ensemble N

a. Successeur d'un ensemble

Pour tout ensemble x, nous définissons le successeur $x^{\bullet}$ de x comme l'ensemble obtenu en adjoignant x aux autres éléments de x :

$$\underline{x^{\bullet} = x \cup \{x\}}$$

On peut donc définir les ensembles :

$0 = \emptyset$

$1 = 0^{\bullet} = \{0\} = \{\emptyset\}$

$2 = 1^{\bullet} = \{0,1\} = \{\emptyset,\{\emptyset\}\}$

$3 = 2^{\bullet} = \{0,1,2\} = \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}$

etc... ("etc..." qui paraît aller de soi, mais qui appelle cependant une justification fournie par :

b. L'Axiome d'infinité

"Il existe un ensemble contenant 0 et le successeur de chacun de ses éléments."
Un tel ensemble est appelé auto-successeur.

.../...

c. Existence d'un plus petit ensemble auto-successeur

Il est tout d'abord immédiat de constater que l'intersection d'ensembles auto-successeurs est un ensemble auto-successeur.
Mais on ne peut parler de l'ensemble intersection de la collection de tous les ensembles auto-successeurs parce qu'on ne sait pas si cette collection est un ensemble.
On contourne cette difficulté en définissant N_A et N_B, intersections de tous les sous-ensembles auto-successeurs de deux ensembles auto-successeurs A et B donnés et en montrant que $N_A = N_B$. Or comme $A \cap B$ est un sous-ensemble auto-successeur de A, il contient N_A qui est ainsi un sous-ensemble auto-successeur de B ; donc $N_A \supset N_B$. En échangeant les rôles joués par A et B on obtient finalement $N_A = N_B$
Il existe donc un plus petit ensemble auto-successeur. On le note N et on appelle nombres entiers naturels ses éléments.

Remarques : Par construction même notons tout de suite les deux propriétés :
1. Un naturel est à la fois élément et sous-ensemble de son successeur.
2. Tout naturel est sous-ensemble de N.

II Les "axiomes" de Péano

Par définition l'ensemble N possède les trois propriétés :
1. $0 \in N$ (où $0 = \emptyset$)
2. Si $n \in N$, alors $n^\circ \in N$ où $n^\circ = n \cup \{n\}$ est lesuccesseur de n.
3. Principe de l'induction mathématique : il exprime que N est l'ensemble auto-successeur minimal. Si $S \subset N$, si $0 \in S$ et si chaque fois que $n \in S$, $n^\circ \in S$ alors $S = N$.

Etablissons les deux propriétés suivantes qui avec les propriétés 1,2,3 constituent les "axiomes de Péano" (dans notre présentation il n'y a qu'un axiome nouveau en plus de ceux de la théorie des ensembles) :

4. Pour tout $n \in N$; $n^\circ \neq 0$

En effet, $n^\circ = n \cup \{n\}$
donc $n \in n^\circ$ et n° n'est pas vide.
Or $0 = \emptyset$

5. Si n et m sont deux entiers naturels et si $n^\circ = m^\circ$ alors $n = m$. Cette dernière propriété qui est à la base des propriétés arithmétiques de N se démontre en utilisant les deux lemmes suivants :

.../...

<u>Lemme i)</u> : aucun nombre naturel n'est sous-ensemble de l'un de ses éléments.
<u>Lemme ii)</u> : tout élément d'un nombre naturel en est un sous-ensemble.

* Le lemme i) exprime que la situation "pathologique" $x = \{x, \ldots\}$ ne peut pas exister dans N.
* Le lemme ii) est illustré par l'exemple suivant : $5 \in N$
$5 = \{4,3,2,1,0\}$; $3 \in 5$ et $3 \subset 5$ puisque
$3 = \{2,1,0\} \subset \{4,3,2,1,0\}$
et de même pour chacun des éléments de 5. Bien sûr on n'obtient pas ainsi tous les sous-ensembles de 5.
* Le lemme ii) a la conséquence suivante : dans N la relation d'appartenance est <u>transitive</u> : en effet si $n \in m$ et si $m \in p$, $m \subset p$ (lemme ii)) donc $n \in p$. En fait, l'appartenance est dans N une relation d'ordre total strict qui est un bon ordre (i.e toute partie non vide possède un plus petit élément).

Ces deux lemmes se démontrent grâce au principe de l'induction mathématique.

<u>Démonstration du lemme i)</u> :
Soit S l'ensemble de tous les naturels qui ne sont pas inclus dans l'un de leurs éléments :
$S = \{n \in N \mid \forall x \in n,\ n \not\subset x\}$
Le lemme i) affirme que $S = N$ ce qui sera établi si S vérifie les 3 propriétés :
a) $S \subset N$
b) $0 \in S$
c) Si $n \in S$, alors $n^{\circ} \in S$.
a) et b) sont évidents puisque $0 = \emptyset$
démonstration de c) : Soit $n \in S$ c'est-à-dire tel que $\forall x \in n$, $n \not\subset x$. Montrons que $n^{\circ} \in S$. S'il n'en était pas ainsi, il existerait un élément a de n° tel que $n^{\circ} \subset a$.
- a ne peut être un élément de n car alors on aurait $n \subset a$ puisque $n \subset n^{\circ}$ et $n^{\circ} \subset a$. et ceci contredirait $n \in S$.
- l'élément a ne peut donc être que n. Mais alors si $n^{\circ} \subset n$ c'est que $n \in n$. Or comme $n \subset n$, n serait sous-ensemble de l'un de ses éléments ce qui contredirait encore $n \in S$.

Démonstration du lemme ii) :

Soit $S = \{n \in N \mid \forall x,\ x \in n \Rightarrow x \subset n\}$.

Le lemme ii) affirme ici encore que $S = N$ et sera établi si on prouve :

a) $S \subset N$

b) $0 \in S$

c) Si $n \in S$ alors $n^\circ \in S$

a et b sont immédiats.

démonstration de c) : Soit $n \in S$

Alors si $x \in n^\circ$, on a soit $x \in n$, soit $x = n$

- si $x \in n$, comme $n \in S$, $x \subset n$ et donc à fortiori $x \subset n^\circ = n \cup \{n\}$
- si $x = n$, $n \subset n^\circ = n \cup \{n\}$.

Démonstration de la propriété 5

Soient n et m deus entiers naturels tels que $n^\circ = m^\circ$

- comme $n \in n^\circ$, n doit appartenir à m°

donc ou bien $n \in m$ ou bien $n = m$.

- de même $m \in m^\circ = n^\circ$ donc

ou bien $m \in n$ ou bien $n = m$

Finalement si $n \neq m$, on a $n \in m$ et $m \in n$ et comme la relation "$\in$" est transitive dans N, on aurait $n \in n$ ce qui contredit le lemme i) donc $n = m$.

II Théorème de récurrence.

Définir une suite d'éléments d'un ensemble X, c'est donner une application $u : N \to X$.

Pour cela il est fréquent qu'on se donne $u(o)$ puis un moyen connaissant $u(n)$ de calculer $u(n^\circ)$ (En pratique on se donne une application $f : X \to X$ et on veut que que $u(n^\circ) = f(u(n))$.

Mais il faut pour cela justifier que l'on fabrique bien ainsi une application de $N \to X$. Le principe de l'induction nous permet seulement de dire que si une telle application existe, elle est unique. Pour affirmer son existence il faut le théorème de récurrence.

Théorème : Si a est un élément d'un ensemble X et si f est une application de X dans X, alors il existe une application u de N dans X telle que $u(o) = a$ et que pour tout élément n de N on ait $u(n^\circ) = f(u(n))$.

Soit $\mathcal{C} = \{A \subset N \times X \mid (0,a) \in A$ et $\forall x \in X, \forall n \in N$
$(n,x) \in A \Rightarrow (n^{\bullet};f(x)) \in A\}$

Chaque fois qu'un couple $(n,x) \in A$, le couple formé du successeur de n et de l'image par f de x est encore dans A.

L'intersection U de tous les ensembles A constituant l'ensemble $\mathcal{C}$ est encore un élément de $\mathcal{C}$. (la propriété précédente est conservée).
Comme tout sous-ensemble de $N \times X$, U est le graphe d'une relation de N dans X.
Le théorème sera établi si on prouve qu'en réalité U est le graphe d'une <u>application</u> u de N dans X c'est-à-dire si on montre que pour chaque $n \in N$, il y a **un et** <u>au plus</u> un $x \in X$ tel que $(n,x) \in U$.

La démonstration se fait par induction :

- Existence : Si $S = \{n \in N \mid \exists x \in X$ tel que $(n,x) \in U\}$
. Le couple (O,a) est un élément de tous les ensembles A qui constituent C donc de leur intersection U ; ainsi $(O,a) \in S$.
. D'autre part lorsque $n \in S$, il existe un x tel que $(n,x) \in U$ mais alors puisque U est un élément de C, $(n^{\bullet},f(x)) \in U$ donc $n^{\bullet} \in S$

- Unicité

Soit $S = \{n \in N \mid (n,x) \in U$ pour un x au plus$\}$
$= \{n \in N \mid \forall x \in X, \forall y \in X$
$(n,x) \in U$ et $(n,y) \in U \Rightarrow x = y\}$

S est donc le sous-ensemble de N "pour lequel U est le graphe d'une application" et le théorème sera établi si on prouve que $S = N$, donc si on prouve :

a) $S \subset N$

b) $0 \in S$

c) Si $n \in S$; alors $n^{\circ} \in S$.

Démonstration de b) : Raisonnons par l'absurde et supposons que 0 n'appartient pas à S. Il existerait alors à côté des couple $(0,a) \in U$ un couple $(0,b) \in U$ avec $a \neq b$. Donc $(0,a) \in U' = U - \{(0,b)\}$.

Montrons que $U' \in \mathcal{C}$ ce qui contredirait le fait que par construction U est le plus petit élément de $\mathcal{C}$ (pour l'inclusion).

Or * $(0,a) \in U'$ (on vient de le voir)

* si $(n,x) \in U'$ alors à fortiori $(n,x) \in U$

donc $(n^\circ, f(x)) \in U$ mais $(n^\circ, f(x))$ ne peut être le couple $(0,b)$ puisque $n^\circ \neq 0$ (4ème axiome de Péano)

donc $(n^\circ, f(x)) \in U - \{(0,b)\} = U'$ et $U' \in \mathcal{C}$.

Démonstration de c) : elle est tout-à-fait analogue :

Par l'absurde supposons que $n \in S$ et $n^\circ \notin S$.

Alors pour au moins un élément x de X en plus du couple $(n^\circ, f(x)) \in U$ il existerait un couple $(n^\circ, y) \in U$ avec $y \neq f(x)$.

Posons $U' = U - \{(n^\circ, y)\}$ et montrons que $U' \in \mathcal{C}$ ce qui contredira le fait que U est le plus petit élément de $\mathcal{C}$. Par construction $(n^\circ, f(x)) \in U'$.

Or * $(0,a) \in U'$ car $(0,a) \in U$ et $n^\circ \neq 0$ donc $(0,a)$ ne peut être le couple (n°, y) } et $(0,a) \in U'$

* Si $(m,t) \in U'$ montrons que $(m^\circ, f(t)) \in U'$.

Or : - si $m = n$, comme $n \in S$ le seul couple de U (donc aussi de U') de première coordonnée n est (n,x) et $(n^\circ, f(x)) \in U'$ (cf ci-dessus)

- si $m \neq n$ et si $(m,t) \in U'$ donc à $U (U' \subset U)$, $(n^\circ, f(t)) \in U$ or $m^\circ \neq n^\circ$ puisque $m \neq n$ (5ème axiome de Péano) donc le couple $(m^\circ, f(t))$ ne peut être le couple (n°, y) et donc $\forall m \in N$, si $(m,t) \in U'$, $(m^\circ, f(t)) \in U'$.

L'utilisation du théorème de récurrence est appelé définition par induction qu'on ne confonde donc pas avec la démonstration par induction.

Un exemple de ce qu'il ne faut pas faire est analysé dans "Mathématique pour l'élève professeur" (G. Glaeser).

IV LES OPERATIONS DANS N

Nous allons voir que l'addition comme la multiplication constitue un exemple de définition par induction.

Nous établirons les propriétés algébriques fondamentales de ces opérations pour donner une idée des difficultés (ou des facilités...) que cela comporte (comparer avec les propriétés analogues des cardinaux dans la partie II,1)

1° Addition

a) Définition : Du théorème de récurrence il résulte qu'il existe pour tout naturel m, une application $s_m : N \to N$ telle que $s_m(o) = m$ et que $s_m(n^\bullet) = (s_m(n))^\bullet$ (il suffit d'utiliser l'application

$$f : N \to N$$
$$n \mapsto n^\bullet$$

L'élément $s_m(n)$ sera noté $\underline{m + n}$.

On aura donc avec cette écriture : $m + 0 = m$ (1)

$m + n^\bullet = (m + n)^\bullet$ (2)

En particulier on a (2') $n^\bullet = n + 1$ puisque $n + 1 = n + 0^\bullet = (n + 0)^\bullet = n^\bullet$

Attention ! Pour l'instant ne pas perdre de vue le caractère disymétrique de l'expression $m + n$ où m et n ne jouent pas le même rôle (c'est clair sur l'écriture $s_m(n)$).

b) Propriétés de l'addition :

i) 0 est élément neutre : $m + 0 = m$ (1)

$0 = m = s_o(m) = m$ car s_o est l'application identique : en effet, l'application identique Id vérifie bien les 2 propriétés : $Id(0) = 0$ et $Id(n^\bullet) = n^\bullet = (Id\ n)^\bullet$

Or le principe de l'induction affirme qu'il n'y à qu'une telle application donc $s_o = Id$

ii) Associativité Il s'agit de montrer que

$\forall a \in N, \forall b \in N, \forall c \in N, a + (b + c) = (a + b) + c$

ou encore $s_a(s_b(c)) = s_{a+b}(c)$.

Pour cela a et b étant fixés on considère l'ensemble $A = \{n \in N \mid (a+b) + n = a + (b+n)\}$

L'associativité sera établie si on montre que $A = N$.

.../...

Et ceci sera démontré si on prouve (induction)

a) $A \subset N$

b) $0 \in A$

c) Si $n \in A$, alors $n^{\bullet} \in A$.

<u>Démonstration de b)</u> : $(a+b) + 0 = a + b$ (1)

$a + (b+0) = a + (b)$ ((1))

donc $0 \in A$

<u>Démonstration de c)</u> : Soit $n \in A$: $(a+b) + n = a + (b+n)$

Alors $(a+b) + n^{\bullet} = [(a+b) + n]^{\bullet}$ ((2))

$= [a + (b+n)]^{\bullet}$ ($n \in A$)

$= a + (b+n)^{\bullet}$ ((2))

$= a + (b+n^{\bullet})$ ((2))

On pourra donc sans ambiguïté écrire : $a + b + c$ (en conservant <u>l'ordre</u>).

iii) <u>Commutativité</u> : La démarche est analogue mais se fait en deux étapes :

- On montre que tout naturel commute avec 1
- puis on établit la commutativité :

$\forall a \in N, \forall b \in N \; a + b = b + a$

en montrant que l'ensemble B des éléments qui commutent avec a est N tout entier.

- <u>Tout naturel commute avec 1</u> : $\forall n, \; n + 1 = 1 + n \; (= n^{\bullet})$

Soit $A = \{ n \in N \mid n + 1 = 1 + n \}$.

$A = N$ car a) $A \subset N$

b) $0 \in N$ puisque 0 est élément neutre.

c) Si $n \in A$, $n^{\bullet} \in A$ car $n^{\bullet} + 1 = (n+1) + 1$ ((2'))

$= (1+n) + 1$ ($n \in A$)

$= 1 + (n+1)$ (associativité)

$= 1 + n^{\bullet}$ ((2'))

- <u>Commutativité</u> : $\forall a \in N, \forall b \in N \; a + b = b + a$.

Fixons a et posons $B = \{n \in N \mid a + n = n + a\}$.

$B = N$ car a) $B \subset N$

b) $0 \in B$ puisque 0 est élément neutre

c) Si $n \in B$, alors $n^{\bullet} \in S$ car

$a + n^{\bullet} = (a+n)^{\bullet}$ ((2))

$= (n+a)^{\bullet}$ ($n \in B$)

$= 1 + (n+a)$ (propriété précédente)

$= (1+n) + a$ (associativité)

$= n^{\bullet} + a$ (propriété ci-dessus).

.../...

Remarquons ici l'importance de l'ordre dans lequel on établit les propriétés : la commutativité nécessite d'avoir d'abord établi que 0 est élément neutre et l'associativité de l'addition.

iv) <u>0 est le seul élément ayant un symétrique</u> :

: $\forall x \in N\ \forall y \in N\ x + y = 0 \Leftrightarrow x = y = 0$

Cette propriété tient au fait que dans N, 0 est le seul élément n'ayant pas de "précédent" (On appellera précédent de $a \in N$ l'entier naturel s'il existe (il est alors <u>unique</u> d'après le "5ème axiome" de Péano noté ${}^{\bullet}a$ tel que $({}^{\bullet}a)^{\bullet} = a$.

- Montrons que $S = \{0\} \cup \{n \in N \mid {}^{\bullet}n \text{ existe}\}$ est N tout entier : a) $S \subset N$

  b) $0 \in S$ par contruction

  c) Si $n \in S$, alors $n^{\bullet} \in S$

En effet on a même la propriété plus forte : si $n \in N$, $n^{\bullet} \in S$ puisqu'alors $n^{\bullet}$ est bien le successeur d'un entier à savoir n.

- Supposons que $x + y = 0$ avec $y \neq 0$.
  y a alors un précédent ${}^{\bullet}y$ et on a :
  $x + y = x + ({}^{\bullet}y+1) = (x+{}^{\bullet}y) + 1 = (x+{}^{\bullet}y)^{\bullet} = 0$
  ce qui contredit l'"axiome" 4ème de Péano.

v) <u>Tout élément est régulier</u> : Cette propriété et fondamentale pour la construction ultérieure de Z.

Remarquons que le 5ème "axiome" de Péano établit la régularité de l'élément 1.
La propriété s'établit pas induction en montrant, a et b étant choisis que l'ensemble $A = \{n \in N \mid a + n = b + n \Rightarrow a = b\}$ est N tout entier.

En effet * $0 \in A$ puisqu'il est neutre

* Si $n \in A$, $n^{\bullet} \in A$ car si $a + n^{\bullet} = b = n^{\bullet}$ alors $(a+n)^{\bullet} = (b+n)^{\bullet}$ et par le 5ème "axiome de Péano, $a + n = b + n$ donc $a = b$ puisque $n \in A$.

2° <u>Multiplication</u>

a) <u>Définition</u> :

On utilise à nouveau le théorème de récurrence pour construire pour chaque entier naturel m une application $p_m : N \to N$ telle que

$p_m(0) = 0$

$p_m(n^{\bullet}) = p_m(n) + m$ (qui est donc associé à l'application $f : N \to N$, $x \mapsto x + m$)

L'élément $p_m(n)$ sera noté $m \times n$ ou encore mn et on a donc :

$- \; m \times 0 = 0$

$- \; m \times n^{\bullet} = (m \times n) + m$

On adoptera la convention habituelle de "priorité" de la multiplication sur l'addition qui permet d'écrire
$mn + m$ au lieu de $(mn) + m$.

b) Propriétés de la multiplication

i) 0 est absorbant pour la multiplication : $\forall x \in N, 0 \times x = x \times 0 = 0$
on établit par récurrence sur x.

ii) Commutativité $\forall (x,y) \in N^2 \; xy = yx$
pour établir cette propriété on utilise le lemme suivant ;
$\forall (x,y) \in N \; x^{\bullet}y = xy + y$
On le démontre par recurrence sur y en utilisant la propriété de l'addition
$n + x^{\bullet} = n + (x+1) = (n+1) + x = n^{\bullet} + x$
La commutativité s'établit alors par récurrence sur y.

iii) 1 est élément neutre pour la multiplication
Il suffit d'établir que 1 est élément neutre à droite.

$$x \times 1 = x \times 0^{\bullet} = x \times 0 + x = 0 + x = x$$

iv) La multiplication est distributive pour l'addition
Il suffit d'établir la propriété à droite

$$\forall (x,y,z) \in N^3 \; (x+y)z = xz + yz$$

On opère par récurrence sur z

v) Associativité $\forall (x,y,z) \in N^3 \quad (x,y)z = x(yz)$
La propriété s'établit par recurrence sur z en utilisant la propriété iv)

vi) Dans N, si un produit est nul, alors l'un des facteurs, au moins est nul.

$$xy = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Si $y \neq 0$ alors y a un précédent ; notons le ${}^{\bullet}y$
$xy = x({}^{\bullet}y) + x = 0 \Rightarrow x = 0$ (propriété 5e) de l'addition)
Donc $xy = 0 \Rightarrow x = 0$ ou $y = 0$

vii) Dans N, 1 est le seul élément qui a un symétrique pour la multiplication.
$xy = 1 \Rightarrow x = y = 1$
On établit la propriété en prenant le précédent de y
$xy = x^{\bullet}y + x$
puis le précédent de x

.../...

viii) Dans $N^* = N - \{0\}$, tout élément est régulier

La propriété s'établit par récurrence

Remarquez ici encore l'ordre dans lequel s'établissent les propriétés.

V RELATION D'ORDRE DANS N

1°) Définition

Nous avons vu que la relation d'appartenance est transitive dans N. Il résulte du lemme i) servant à démontrer la 5ème propriété de Péano que $\forall n \in N,\ n \notin n$; on ne peut donc avoir à la fois $a \in b$ et $b \in a$ dans N. La relation d'appartenance est donc dans N une relation d'ordre strict. On retrouve la relation d'ordre "habituelle" en posant :

$\forall a \in N,\ \forall b \in N\ \ a \leq b$ signifie : $a = b$ ou $a \in b$

2°) Cet ordre est total

Il s'agit d'établir qu'étant donnés deux entiers naturels a et b on a :
ou bien $a = b$ ou bien $a \in b$ ou bien $b \in a$.

Pour cela on établit par induction que l'ensemble des éléments comparables à a : $A = \{n \in N \mid n \in a \text{ ou } a \in n \text{ ou } a = n\}$ et N tout entier

Pour cela on commence par établir deux propriétés :

i) $\forall\ n \in N,\ n \neq 0 \Rightarrow 0 \in n$

ii) $\forall n \in N,\ \forall x \in n$ ou bien $x^* \in n$ ou bien $x^* = n$

Chacune de ces propriétés s'établit par récurrence (induction)

i) $0 \in 1$ puisque $1 = \{0\}$

Si $0 \in n$, comme $n \subset n^*$, $0 \in n^*$

ii) Soit $S = \{n \in N \mid \forall x \in n,\ x^* \in n \text{ ou } x^* = n\}$

Alors * $0 \in S$ puisque $0 = \emptyset$

* Si $n \in S$ et si $x \in n^* = n \cup \{n\}$

- ou bien $x \in n$ alors ou bien $x^* \in n$ donc à fortiori $x^* \in n^*$
  ou bien $x^* = n \in n^*$
- ou bien $x = n$ alors $x^* = n^*$

Dans tous les cas, si $x \in n^*$, $x^* \in n^*$, ou $x^* = n^*$

Une fois ces propriétés établies,

- i) montre que $0 \in A$
- si $n \in A$, ou bien $a \in n$, alors à fortiori $a \in n^*$
- ou bien $n = a$ alors $a \in \{n\} \subset n^*$
- ou bien $n \in a$ alors (propriété ii) $n^* \in a$ ou $n^* = a$

Finalement on a : ou bien $n^* \in a$, ou bien $a \in n^*$ ou bien $a = n^*$

Nous laissons en exercice ou au lecteur le soin de démontrer qu'en réalité c'est un bon ordre, ou encore qu'étant donné un ensemble non vide E de naturels il y existe un naturel $k \in E$ tel que $\forall m \in E\ m \neq k \Rightarrow k \in m$.

Bien sûr il est facile (en considérant les paires) de démontrer que l'ordre est total si on a déjà montré que c'est un bon ordre.

3°) <u>Compatibilité de la relation d'ordre avec lâddition</u>

Il s'agit d'établir que $\forall a \in N,\ \forall b \in N,\ \forall c \in N,\ a \leq b \Rightarrow a+c \leq b+c$

Comme bien sûr si $a = b$, $a+c = b+c$, il suffit d'établir qui si $a \in b$ alors $a+c \in b+c$.

Pour cela, a et b (avec $a \in b$) étant fixés on considère l'ensemble $A = \{n \in N \mid a + n \in b + n\}$ et on montre par induction que $A = N$.

a) $0 \in A$ puisqu'il est neutre

b) Si $n \in A$, alors puisque $a + n \in b + n$, ou bien $a + n^{\bullet} = (a+n)^{\bullet} \in b + n$, ou bien $a + n^{\bullet} = b + n$ (propriété ii) ci-dessus). Dans les deux cas $a + n^{\bullet} \in b + n^{\bullet}$

2. SYMETRISATION

Introduction : La construction de $\mathbb{Z}$ à partir de $\mathbb{N}$ qui figure actuellement au programme de Terminale relève d'un procédé général connu sous le nom de "théorème de symétrisation". Le problème qui suit a pour objet d'exposer ce sujet (il a été donné en Terminale C).

Problème : On considère un ensemble E muni d'une loi de composition interne notée $*$. Cette loi possède les propriétés suivantes : elle est commutative, associative, admet un élément neutre que l'on notera e et chaque élément est supposé régulier. (On dit que $(E,*)$ est un semi-groupe commutatif "simplifiable").

1) L'équation $a * x = b$ où a et b sont deux éléments donnés de E admet-elle toujours au moins une solution sur E ? Justifier la réponse par un exemple ou par toute autre méthode). Montrer que si cette équation admet une solution elle n'en admet pas d'autre.

2) Sur $E^2 = E \times E$ on définit une relation binaire R en posant $(a,b)\ R\ (a',b') \Leftrightarrow a * b' = b * a'$. Montrer que R est une relation d'équivalence. On désignera par $E^2/_R$ l'ensemble quotient associé et par q l'application quotient telle que :

$$q : E^2 \to E^2/_R$$
$$(a,b) \mapsto q(a,b)$$ (classe d'équivalence selon R de (a,b)).

3) Sur E^2 on définit une loi de composition interne, notée O, en posant $(a,b)\ O\ (c,d) = (a * c,\ b * d)$. Montrer que cette opération "passe au quotient" en rappelant d'abord avec précision ce que signifie cette locution et en décomposant ensuite soigneusement les diverses étapes de la démonstration. L'opération ainsi induite dans $E^2/_R$ sera également notée O.

4) Montrer que $(E^2/_R,\ O)$ est un groupe commutatif.

...

5) Montrer que dans $E^2/_R$ il existe un sous-ensemble isomorphe à E, l'isomorphisme faisant se correspondre les lois O et *.

Application : En "identifiant" E au sous-ensemble de $E^2/_R$ que l'on vient de mettre en évidence, montrer que la résolution de $a * x = b$ devient possible dans tous les cas sur $E^2/_R$ et donner la solution en justifiant son unicité.

6) Donner trois exemples "classiques" d'application de cette théorie. Sans entrer dans des détails superflus, on s'attachera à bien préciser les ensembles désignés et à vérifier que les hypothèses nécessaires à l'application de cette théorie sont bien réalisées.

Solution commentée

1) Dans $(\mathbb{N},+)$ qui est un semi -groupe commutatif simplifiable, l'équation $a + x = b$ n'a pas de solution dès que $a > b$.

Lorsqu'il y a une solution elle est unique car si $a * x_1 = b = a * x_2$, l'élément a étant régulier on a $x_1 = x_2$.

2) Avant d'aborder la démonstration, indiquons en quelques lignes comment on peut motiver une telle étude.

Dans $(\mathbb{N},+)$, si d est une solution de $a + x = b$, on note $d = b - a$ mais on sait que d peut s'écrire d'une infinité de façons sous la forme $d = b - a = b' - a'$.(avec $b' > a'$).

Un couple (a',b') "représentera" donc aussi d, si $b - a = b' - a'$ donc si $a + b' = b + a'$ expression qui peut être écrite sans restriction sur les nombres a, b, a', b'.

R est une relation d'équivalence :

En effet, elle est :

a) réflexive : $(\forall(a,b) \in E^2,\ (a,b)R(a,b)) \Leftrightarrow (\forall(a,b) \in E^2, a * b = b * a)$ ce qui est une proposition vraie d'après la commutativité de * dans E.

b) symétrique : $(a,b)R(a',b') \Leftrightarrow a*b' = b*a' \Leftrightarrow a'*b = b'*a \Leftrightarrow (a',b')R(a,b)$

c) transitive : $\left.\begin{matrix}(a,b)R(a',b') \\ \text{et} \\ (a',b')R(a'',b'')\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}(a*b'=b*a') \\ \text{et} \\ a'*b''=b'*a''\end{matrix}\right\} \Rightarrow \begin{matrix}(a*b')*(a'*b'') = \\ (b*a')*(b'*a'')\end{matrix}$

en "composant" membre à membre les égalités précédentes

D'après la commutativité et l'associativité de $*$ la dernière égalité équivaut à : $(a*b")*(b'*a') = (b*a")*(b'*a')$ ce qui équivaut, puisque $b'*a'$ est régulier, à $a*b" = b*a"$ qui signifie que $(a,b)R(a",b")$.

3) Montrons que la loi O "passe au quotient" ce qui exige que R soit compatible avec l'opération O c'est-à-dire que :

$$(\forall (a,b) \in E^2, \forall (c,d) \in E^2, (a,b)R(a',b') \text{ et } (c,d)R(c',d')) \Rightarrow$$
$$(a,b) \text{ O } (c,d)R(a',b') \text{ O } (c',d').$$

Cette dernière proposition équivaut à $(a*c,b*d)R(a'*c',b'*d')$
$\Leftrightarrow (a*c)*(b'*d') = (b*d)*(a'*c')$
$\Leftrightarrow (a*b')*(c*d') = (a'*b)*(c'*d)$.
Or, les hypothèses se traduisent par $a*b' = b*a'$ et $c*d' = d*c'$ et en composant membre à membre les deux égalités on obtient bien la précédente.

$$\begin{tikzcd}
E^2 \times E^2 \arrow[r, "\mathrm{O}"] & E^2 \\
((a,b),(c,d)) \arrow[r, mapsto] \arrow[d, mapsto, "q"] & (a*c,b*d) \arrow[d, mapsto, "q"] \\
(c(a,b),c(c,d)) \arrow[r, dashed, mapsto] & c(a*c,b*d) \\
(E^2/_R \times E^2/_R) \arrow[r] & E^2/_R
\end{tikzcd}$$

Conformément au tableau ci-contre, on pourra poser $q(a,b) \text{ O } q(c,d) = q((a,b) \text{ O } (c,d)) = q(a*c,b*d)$ définissant ainsi une application de $(E^2/_R)^2$ dans $E^2/_R$ c'est-à-dire une loi de composition interne, notée également O, dans $E^2/_R$.

4) $(E^2/_R, \text{O})$ est un groupe commutatif.

En effet, la loi O est :

a) associative : $q(a,b) \text{ O } [q(c,d) \text{ O } q(e,f)] = [q(a,b) \text{ O } q(c,d)] \text{ O } q(e,f)$
$$\Updownarrow$$
$$q(a*(c*e),b*(d*f)) = q((a*c)*e,(b*d)*f)$$
$$\Updownarrow$$
$$(a*(c*e),b*(d*f))R((a*c)*e,(b*d)*f)$$

Cette dernière proposition est vraie car $*$ est associative et R est réflexive.

b) commutative : $q(a,b) \text{ O } q(c,d) = q(c,d) \text{ O } q(a,b) \Leftrightarrow$
$q(a*c,b*d) = q(c*a,d*b) \Leftrightarrow (a*c,b*d)R(c*a,d*b)$ ce qui est vrai car $*$ est commutative et R est réflexive.

...

c) <u>pourvue d'un élément neutre</u> : $q(\alpha,\beta)$ est élément neutre $\Leftrightarrow$
$(\forall\ q(a,b) \in E^2/_R,\ q(a,b)\ O\ q(\alpha,\beta) = q(a,b)) \Leftrightarrow$
$(\forall\ q(a,b) \in E^2/_R,\ q(a*\alpha,b*\beta) = q(a,b)) \Leftrightarrow (\forall\ q(a,b) \in E^2/_R, (a*\alpha,b*\beta)R(a,b)) \Leftrightarrow$
$(\forall\ q(a,b) \in E^2/_R,\ (a*\alpha)*b = (b*\beta)*a) \Leftrightarrow \alpha = \beta$ d'après l'associativité, la commutativité et le fait que tout élément de E est régulier.
Il existe donc un élément neutre dans $E^2/_R$: $q(\alpha,\alpha)$ (que l'on peut aussi noter $q(e,e)$)

d) <u>tout élément admet un symétrique</u> :
$q(a,b)\ O\ q(a',b') = q(e,e) \Leftrightarrow q(a*b',b*a') = q(e,e) \Leftrightarrow$
$(a*b')*e = (b*a')*e \Leftrightarrow a*b' = b*a'$ et pour que cette dernière égalité soit vraie, il suffit de prendre $a' = b$ et $b' = a$ d'où sym $\underline{q(a,b) = q(b,a)}$

5) <u>E peut être "plongé" dans $E^2/_R$ par isomorphisme</u>

a) Considérons $A = \{q(a,e) \mid a \in E\} \subset E^2/_R\}$
Soit $f : E \to A$
$a \mapsto f(a) = q(a,e)$
f est bijective car $q(a,e) = q(b,e) \Leftrightarrow a = b$ (injectivité), la surjectivité résultant de la définition même de f.

b) La restriction de O à A définit une loi de composition interne sur A (en d'autres termes, A est stable ou fermé pour la loi O définie dans $E^2/_R$). En effet :
$q(a,e)O\ q(a',e) = q(a*a',e*e) = q(a*a',e)$

c) f est compatible avec * dans E et O dans A. En effet :

$$\begin{tikzcd} E \times E \arrow[r, "*"] & E \\ (a,a') \arrow[r, mapsto] \arrow[d, "f"'] & a*a' \arrow[d, "f"] \\ (q(a,e),q(a',e)) \arrow[r, mapsto] & q(a*a',e) = q(a,e)O\ q(a,e') \end{tikzcd}$$

$A \times A \xrightarrow{O} A$ et l'on remarque que $q(a,e)O\ q(a',e) = q(a*a',e)$ est bien réalisé. Donc f définit un isomorphisme entre $(E,*)$ et (A,O) et par cet isomorphisme on peut identifier E à A.

...

Application : résolution de $a*x = b$

1) Si a admet un symétrique a' dans E $a*x = b \Leftrightarrow x = a'*b$

2) Si a n'admet pas de symétrique dans E, l'équation associée à $a*x = b$ après "plongement" de E dans $E^2/_R$, par identification de E à A, s'écrit : $q(a,e) O X = q(b,c)$. Celle ci équivaut à $X =$ sym $q(a,e)$ O $q(b,e) = q(e,a) O q(b,e)$ car $E^2/_R$ est un groupe et sym $q(a,e) = q(e,a)$. Donc $X = q(e*b, a*e) = q(b,a)$ qui est l'unique solution de l'équation "$a*x = b$".

Ecriture canonique des éléments de $E^2/_R$.

Comme $q(a,b) = q(a,e) O q(e,b)$ et que $q(e,b)$ est le symétrique de $q(b,e)$ qui est un élément de A, on voit que tout élément de $E^2/_R$ est le composé d'un élément de A (donc de E) et du symétrique d'un élément de A (donc de E).

Lorsqu'on a adopté une notation pour le symétrique (par exemple $-x$, opp x, inv x, x^{-1}, $\frac{1}{x}$ etc...) on peut noter la loi O comme la loi * et justifier des notations telles que $b + (-a)$ ou $\frac{b}{a}$.

6) Exemples :

a) $(N,+)$ est un semi-groupe commutatif simplifiable et conduit par application de la théorie précédente au groupe additif Z dans lequel l'équation $a + x = b$ admet une solution unique $x = b +$ opp a.

b) $(Z^*,\times)$ de même se prête à l'application de la théorie et conduit ainsi à $(Q^*,\times)$ qui est un groupe dans lequel l'équation $ax = b$ admet toujours une seule solution $x = b\ a^{-1}$

c) l'ensemble $\mathcal{P}^*$ des polynômes formels non nuls à un générateur et à coefficients dans Q possède pour la multiplication une structure adéquate et conduit ainsi au groupe multiplicatif des fractions de polynômes dans lequel l'équation $AX = B$ avec $A \neq 0$ admet toujours une seule solution $X = \frac{B}{A}$

Remarque : Dans le cas de Z, on démontre que tout élément est soit dans N (identifié à une partie de Z) soit le symétrique (opposé) d'un élément de N : c'est ce qui justifie l'écriture des éléments de Z où le couple n'apparaît plus, alors que la notation habituelle $\frac{a}{b}$ des éléments de Q (rationnels) conserve la marque du couple.

La règle de "simplification" : $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba'$ n'est autre que la relation d'équivalence dans $(Q^*)^2$ (où $Q^* = Q - \{0\}$)

Commentaires : On est tenté pour étudier le champ d'application de cette théorie de réduire les hypothèses au minimum.

. En particulier on pourrait songer à renoncer à la commutativité de la loi *. Dans la présentation donnée celle ci intervient souvent et déjà pour montrer que $\dot{R}$ est réflexive. Il s'agit là d'une difficulté façile à lever : il suffit de prendre pour définition de R :

$(a,b)R(a',b') \Leftrightarrow a*b' = a'*b$.

Mais même en imposant aux éléments d'être réguliers à gauche et à droite, on ne peut plus alors établir la transitivité.

. Plus intéressante est la tentative qui consiste à s'affranchir de la régularité. En effet, on dispose au niveau secondaire de plusieurs exemples d'opérations non régulières :

-Dans $(\mathcal{P}(E), \cup)$ $A \cup B = A \cup C$ n'implique pas $B = C$. Il en est de même de $(\mathcal{P}(E), \cap)$ alors qu'il s'agit là de semi-groupes commutatifs.

-$(Z/nZ,\times)$ lorsque n n'est pas premier admet des diviseurs de zéro donc des éléments (non nuls) qui ne sont pas réguliers : dans $Z/8Z$ $\bar{4} . \bar{2} = \bar{4} . \bar{4}$ $(=\bar{0})$ par exemple.

On peut développer une théorie tout à fait analogue sans supposer la régularité des éléments mais en remplaçant R par la relation :

$(a,b)\ R'\ (a',b') \Leftrightarrow \exists\ u \in E$ tel que $a'*b*u = a*b'*u$.

Malheureusement, la présence d'un élément absorbant dans chacun des cas cités (que l'on ne peut retrancher comme on le fait pour construire Q car la loi ne reste pas <u>interne</u> dans l'ensemble privé de l'élément absorbant) conduit à l'existence d'<u>une seule classe</u> d'équivalence (en choisissant pour u l'élément absorbant on voit que deux couples quelconques sont équivalents). Autrement dit dans chaque cas on obtient pour groupe associé le groupe réduit à l'élément neutre !...

Un autre exemple (amusant...) est constitué par le "semi-groupe des esquimaux" M = {0, 1, 2, 3, 4, beaucoup} avec une addition définie par la table :

+	0	1	2	3	4	5	beaucoup (b)
0	0	1	2	3	4	5	b
1	1	2	3	4	5	b	b
2	2	3	4	5	b	b	b
3	3	4	5	b	b	b	b
4	4	5	b	b	b	b	b
5	5	b	b	b	b	b	b
b	b	b	b	b	b	b	b

Comme l'élément "beaucoup" est absorbant, on retrouve ici encore le groupe nul comme symétrisé. Pas étonnant que les esquimaux ne se soient pas fait un renon en mathématiques !

3. POURQUOI CONSTRUIRE R ?

L'impossibilité dans certains ensembles de résoudre certaines opérations ou de conclure à certaines propriétés nous conduit à construire de nouveaux ensembles où les opérations et les propriétés souhaitées soient réalisables. La méthode de symétrisation conduit à l'ensemble Q des rationnels, mais actuellement en 4ème on préfère éviter cet ensemble et construire l'ensemble D des décimaux.

Des considérations algébriques nous incitent à construire un nouvel ensemble à partir de D, car dans celui-ci l'équation $ax = b$ ($a \in D^*$, $b \in D$) n'a pas toujours une solution.

> Certains nombres ont un inverse dans D (4;10;0,25 par exemple) d'autres n'en ont pas. Montrons par exemple que 3 n'a pas d'inverse dans D. S'il en avait un, il serait tel que $3x = 1$. Posons $x = A, a_1\ a_2 \dots a_n$ a_n étant le dernier chiffre non nul après la virgule. Le dernier chiffre du nombre $3x$ est le dernier chiffre du nombre $3a_n$. Pour que $3x = 1$, il faut que $3 \times (A, a_1 \cdot a_2 \dots a_n) = 1{,}00\dots0$; il faut donc que le dernier chiffre de $3a_n$ soit un 0. Or $3a_n$ ne se termine jamais par 0 quelque soit a_n. Le nombre 3 n'a pas d'inverse dans D.

Ce qui nous conduit à construire Q.

L'ensemble Q muni de l'addition et de la multiplication présente une structure de corps. Comme dans l'ensemble Q, il n'est pas toujours possible de trouver des éléments dont le carré soit égal à un nombre rationnel, on pourrait penser à prolonger Q par un ensemble où cette opération puisse être réalisable, mais il ne nous conduirait pas à l'ensemble R. Il nous faut donc envisager Q sous un autre aspect.

Des considérations topologiques vont nous conduire à définir un nouvel ensemble à partir de Q. L'ensemble N est tel que tout sous-ensemble non vide et majoré de N admette une Borne supérieure (plus petit des majorants). Z a conservé cette propriété. Par contre l'ensemble Q des rationnels a perdu cette qualité de N comme le montre l'exemple suivant :

.../...

Soit E l'ensemble des rationnels positifs dont le carré est au plus égal à 3.

$E = \{x \mid x \in Q^{+} \text{ et } x^{2} \leq 3\}$. E n'est pas vide : $1 \in E$

E est majoré : le rationnel 2 est un majorant de E :

$\forall x \in E \mid x^{2} \leq 3 < 2^{2} \mid\Rightarrow x \leq 2$

mais montrons que E n'a pas de borne supérieure dans Q.

Supposons qu'il existe une borne supérieure a de l'ensemble E.

a est un élément de E ou du complémentaire E' de E dans Q.

a) Supposons $a \in E'$ alors $a^{2} > 3$. Soit $u = a^{2} - 3$, $u \in Q^{**}$ (ensemble des rationnels strictement positifs). Montrons qu'on peut trouver un majorant a_o de E inférieur à a c'est-à-dire qu'il existe $\lambda \in Q^{**}$ tel que $a_o = a - \lambda$

Considérons $d = a_o^{2} - 3 = (a - \lambda)^{2} - 3 = u - 2a\lambda + \lambda^{2}$, il suffit de choisir λ tel que $a\lambda < \frac{u}{2a}$ alors $u - 2a\lambda > 0$ donc $\alpha > 0$.

Le rationnel a_o est alors un majorant de E, inférieur à a, donc a n'est pas la borne supérieure de E.

b) Supposons $a \in E$ alors $a^{2} < 3$ (puisqu'il n'existe aucun rationnel dont le carré soit égal à 3). Soit $u = 3 - a^{2}$, $u \in Q^{**}$.

Démontrons qu'on peut trouver un élément a_o de E supérieur à a, c'est-à-dire qu'il existe $\lambda \in Q^{**}$ tel que $a_o = a + \lambda$.

Considérons $d = 3 - a_o^{2} = u - 2a\lambda - \lambda^{2}$; il suffit de choisir le rationnel λ tel que $0 < \lambda < \frac{u}{4a}$ car $0 < 1 < \frac{u}{4a} \Rightarrow 0 < 2a\lambda < \frac{u}{2}$

$$0 < 1 < \frac{u}{4a} \Rightarrow u - 2a\lambda > \frac{u}{2} \qquad (1)$$

Et montrons que $\lambda^{2} < \frac{u}{2}$

$$\frac{3}{2} \in E \Rightarrow a \geq \frac{3}{2}$$

$$a \geq \frac{3}{2} \Rightarrow a^{2} \geq \frac{9}{4} \quad \text{or } u = 3 - a^{2} \text{ donc } o < u < 1$$

$$\left.\begin{array}{l} 0 < u < 1 \\ a^{2} \geq \frac{9}{4} \end{array}\right| \Rightarrow u < 8a^{2} \qquad (u < 8a^{2}) \Rightarrow \lambda^{2} < \frac{u}{2} \quad (2)$$

(1) et (2) entraînent $u^{2} - 2a\lambda - \lambda^{2} > 0$ donc $3 - a^{2} > 0$

Le rationnel a_o est élément de E, supérieur à a, donc a n'est pas la borne supérieure de E.

La recherche d'un ensemble possédant toutes les propriétés des ensembles N,Z,D,Q, et où tout sous-ensemble non vide et majoré admette une borne supérieure conduit à l'introduction de l'ensemble R "des nombres réels".

3. DECIMAUX

L'étude des nombres décimaux, faite dans les nouveaux programmes de 4ème, permet une construction de R par une variante de la "méthode des suites de Cauchy".
(Cette technique a été exposée par Mr Kittel dans le bulletin de l'A.P.M.E.P N° 279 pages 325 et suivantes)
Les matériaux de base sont constitués par : l'ensemble D défini comme réunion des ensembles Dn. Chaque Dn est l'ensemble des décimaux "ayant n chiffres après la virgule" ; on assimile Z à D_o.
D est muni d'une structure d'anneau ordonné prolongeant celle de Z.

1ère étape.

Nous distinguerons désormais les catégories suivantes :

- <u>Le nombre décimal</u> Ex : 47,374 (C'est un élément d'un Dn)
- <u>La suite de décimaux</u> Ex : $u_1 = 3,25$ $u_2 = 4,7389$ $u_3 = 0,304$......
  C'est une application de N dans D. On notera (u_n) une telle suite et on rappelle que :
  (u_n) est croissante si et seulement si $\forall\ n \in N$, $u_{n+1} \geq u_n$
  (u_n) est décroissante si et seulement si $\forall\ n \in N$, $u_{n+1} \leq u_n$
  Une suite (u_n) converge vers un nombre décimal d si on peut rendre la différence entre u_n et d aussi petite que possible en valeur absolue c'est-à-dire :
  $\forall\ m \in N, \exists\ m' \in N / \forall\ n > m'\ |u_n - d| < 10^{-m}$
- <u>Le développement décimal</u> Ex : $u_0 = 2,5$ $u_1 = 2,53$ $u_2 = 2,538$.....
  C'est une suite de décimaux dans laquelle chaque terme de rang n est un élément de D_n qui "reprend" le terme de rang n - 1. En d'autres termes, passer d'un terme au suivant c'est ajouter un nouveau chiffre à sa droite.
  Si on se borne aux éléments de D^+ de telles suites sont caractérisées par l'égalité : $10^n . u_n = 10 . 10^{n-1} . u_{n-1} + a$ (a étant un nombre de un chiffre).

.../...

Lorsque tous les termes du développement décimal sont positifs, on dit que le développement décimal est positif et on appellera développement décimal négatif, tout développement (u_n) tel que $(- u_n)$ soit un développement décimal positif.

* L'ensemble Δ des développements décimaux "contient" D. En effet, soit par exemple le nombre 3,7282 ; on peut l'assimiler au développement décimal suivant :

  $u_1 = 3{,}7 \quad u_2 = 3{,}72 \quad u_3 = 3{,}728 \quad u_4 = 3{,}7282 \quad u_5 = 3{,}72820 \quad u_6 = 3{,}728200$

  et pour $n \geq 4 \quad u_n = u_4$.

Un développement décimal de ce type est une suite convergente vers u_4 mais, malheureusement, ce n'est pas le seul développement décimal à converger vers ce nombre ; nous verrons qu'il y en a un autre (c'est-à-dire le développement 3,72819999999999....)

Une autre remarque importante à faire est que Δ contient d'autres éléments que ceux qui sont assimilables aux éléments de D. On peut considérer par exemple : 3,4592742742742742....

Un tel développement décimal présente l'avantage d'avoir une composition qui permet de prévoir un terme de rang donné puisque à partir du 5ème rang le chiffre à ajouter à droite est successivement un 7, un 4, un 2 et ainsi de suite.

On dit qu'un tel développement est périodique.

Il est bon de se souvenir que "prévisible" et "périodique" ne sont pas synonymes et que par exemple le développement décimal bien connu :

1,020030004000050000060000007000000080000000090000000001000000000011....

est prévisible mais non périodique.

* On va donc essayer d'établir une relation entre les éléments de Δ et on dit que deux développements (u_n) et (v_n) sont équivalents lorsque la suite $(u_n - v_n)$ converge vers 0.

  Cette relation r est bien une relation d'équivalence et nous allons maintenant étudier les éléments de chaque classe d'équivalence.

2ème étape

Théorème : Chaque classe d'équivalence de la relation r contient un ou deux éléments ; elle n'en contient deux que si et seulement si l'un des deux est un nombre décimal.

La démonstration de ce théorème suit le programme suivant :

.../...

1) Dans un développement décimal positif la différence entre deux termes (de rang n + k et n) est toujours inférieure à 10^{-n}

2) Deux développements décimaux ne sont pas équivalents si la différence entre les chiffres de ces développements qui occupent le même rang est supérieure ou égale à 2.
Par exemple 1,325 et 1,327 sont les débuts de deux développements qui ne sont pas équivalents parce que 7 - 5 = 2.

3) Deux développements équivalents ne peuvent être l'un positif et l'autre négatif.

4) Si on considère deux développements équivalents et distincts, à partir d'un certain rang m, l'un a toutes ses décimales égales à 0 et l'autre toutes ses décimales égales à 9. Le premier est donc un nombre décimal).

Afin de faciliter la compréhension des démonstrations nous suivrons leur développement formalisé sur un exemple concret.

Théorème 1°)

$1,325875 - 1,32 = 0,005875$

$0 \leq 5875 \leq 9999 = 10^4 - 1$

$0,005875 \leq 0,01$

$\forall\, k \in N^*\; d_{n+k} = d_n + a_k . 10^{-(n+k)}$

et $0 \leq a_k \leq 10^k - 1$

d'où $\forall\, n \in N,\ \forall\, k \in N$

$d_{n+k} - d_n \leq 10^{-n}$

Théorème 2°)

$1,32732 - 1,32548 =$

$(1,32732 - 1,327)+(1,327 - 1,325) +$

$(1,325 - 1,32548)$

$0,00184 > 0,002 - 0,00048$

$0,002 = 0,001 \times 2$

$0,00184 > 0,001$

$\forall\, k \in N\; d_{n+k} - d'_{n+k} =$

$(d_{n+k} - d_n)+(d_n - d'_n)+(d'_n - d'_{n+k})$

Or, $d_{n+k} - d_n \geq 0$ donc :

$d_{n+k}-d'_{n+k} \geq (d_n-d'_n)-(d'_{n+k}-d'_n)$

Supposons que $d_n-d'_n > 10^{-n}$ alors

$d_n - d'_n \geq 2.10^{-n}$

et, d'après la conclusion du théor 1°)

$d_{n+k} - d'_{n+k} > 2.10^{-n} - 10^{-n} = 10^{-n}$

$(d_p - d'_p)$ ne peut pas converger vers 0.

Théorème 3°)

Ce théorème est une quasi évidence qui n'appelle pas de commentaires

Théorème 4°)

$d_1 = d'_1 = 1,2$

$d_2 = 1,25 \quad d'_2 = 1,24$

$d_2 - d'_2 = 0,01 = 10^{-2}$

$d_5 - d'_5 = 10^{-2} + (a_3 - a'_3).10^{-5} \leq 10^{-5}$

$(a'_3 - a_3) \,.\, 10^{-5} \geq 10^{-2} - 10^{-5}$

$a'_3 - a_3 \geq 10^3 - 1$

or $a'_3 \leq 999$ et $a_3 \leq 999$

donc $a'_3 = 999$ et $a_3 = 0$

d'où : $d_5 = 1,25000 \quad d'_5 = 1,24999$

Supposons que la composition des 2 développements soitla même jusqu'au rang m - 1 et qu'au rang suivant la différence soitégale en valeur absolue à 10^{-m} (contraposée du théorème 2)

Au delà du rang m on peut écrire :

$$d_{m+k} - d'_{m+k} = d_m - d'_m + (a_k - a'_k).10^{-(m+k)}$$

(voir théorème 1)

de plus $d_{m+k} - d'_{m+k} \leq 10^{-(m+k)}$ d'où

$10^{-m} + (a_k - a'_k).10^{-(m+k)} \leq 10^{-(m+k)}$

$(a'_k - a_k).10^{-(m+k)} \geq 10^{-m} - 10^{-(m+k)}$

$a'_k - a_k \geq 10^k - 1$

ce qui combiné au théorème 1) éxige

$a'_k = 10^k - 1$ et $a_k = 0$

<u>Définition</u> :

On appelle <u>nombre réel</u> chaque classe d'équivalence de la relation r dans Δ , $R = \Delta /_r$

On convient de prendre comme <u>représentation d'un nombre réel</u>, l'unique élément de la classe lorsque celle-ci est un singleton et le <u>nombre décimal</u> lorsque c'est une paire.

3ème étape

Nous allons maintenant définir une <u>relation d'ordre</u> dans R :
Si a et b sont des réels de <u>représentants</u> (cf plus haut) (a_n) et (b_n) on dit que a est inférieur à b(on écrit $a \leq b$) lorsque $\forall\ n \in N,\ a_n \leq b_n$.

.../...

Cet ordre possède les propriétés suivantes :

1° Il est <u>total</u> : (c'est-à-dire qu'on peut toujours ranger deux réels)

2° Il <u>prolonge</u> celui de D

3° D est <u>dense</u> dans R pour cet ordre (c'est-à-dire que dans tout intervalle entourant un réel il y a un décimal).

1° et 2° tiennent à la remarque suivante, si $a \neq b$, il existe un indice n tel que $a_n \neq b_n$. On peut alors ranger a_n et b_n et vu la définition des suites décimales "si $a_n < b_n$ on a $a_p < b_p$ pour tout $p \geq n$ et donc $a_p \leq b_p$ pour tout $p \in \mathbb{N}$.

4ème étape.

Si x et y sont deux réels de représentants canoniques(xn)et(yn), les suites $(x_n + y_n)$ et $(x_n y_n)$ ne sont pas nécessairement des développement décimaux.

Exemple : $x = 0,666$ $y = 3,512\ldots$ $x_0 + y_0 = 3$ $x_1+y_1 = 4,1$

$x_1y_1 = 2,1$ $x_2y_2 = 2,31$

On ne peut donc définir des lois de composition dans R à l'aide de cette méthode;c'est alors qu'on est amené à introduire les notions de suite de décimaux convergentes dans R et de suite de Cauchy de décimaux.

On dit qu'une suite de décimaux (un) converge vers le réel r de représentant (dn) lorsque les suites (un) et (dn) sont équivalentes. Il est évident que deux suites de décimaux qui convergent vers la même limite sont équivalentes.

On peut alors donner les définitions suivantes:

Si (xn) et (yn) sont les représentants canoniques des réels x et y, on appelle somme de x et de y (x+y) le réel limite de la suite $(x_n + y_n)$ et produit de x et de y (xy) le réel limite de la suite $(x_n y_n)$.

Il reste maintenant à justifier l'existence de ces limites et c'est alors qu'interviennent les suites de Cauchy de décimaux.

4. Construction de $\mathbb{R}$ par les suites de Cauchy

I. Introduction :

1°) On dispose de l'ensemble $\mathbb{Q}$ des nombres rationnels qui constitue un corps commutatif unitaire totalement ordonné. De plus, $\mathbb{Q}$ est archimédien ($\forall\ a \in \mathbb{Q},\ \forall\ b \in \mathbb{Q},\ a > 0 \Rightarrow \exists\ n \in \mathbb{N},\ b \leq a\, n$) et il est "dense" sur lui même" c'est-à-dire qu'entre deux rationnels (distincts) il y en a toujours un troisième (distinct des deux premiers) :
$\forall\ a \in \mathbb{Q},\ \forall\ b \in \mathbb{Q}\ a < b \Rightarrow (\exists\ c \in \mathbb{Q},\ a < c < b)$.
Notons que ni $\mathbb{N}$, ni $\mathbb{Z}$ ne possédaient cette dernière propriété.

2°) Pour les "nombres irrationnels connus" ($\sqrt{2}, \pi$, e par exemple) on possédait des algorithmes permettant de les approcher par des suites décimales ou rationnelles (algorithme de la division, de la racine carrée etc...). Mais pour un même "nombre" deux algorithmes qui en réalisent des approximations peuvent conduire à des suites différentes : par exemple e peut être approché par la suite des rationnels $a_n = (1 + \frac{1}{n})^n$ ou par la suite de rationnels $b_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!}$.

On peut montrer

1°) que la différence entre les termes généraux de deux telles suites devient aussi petite qu'on le souhaite pourvu que le rang soit suffisamment élevé.

2°) que chacune de ces suites, si elle ne converge pas dans $\mathbb{Q}$, possède la propriété suivante : la différence entre deux termes quelconques peut être rendue aussi petite qu'on le veut en prenant des termes de rang assez élevé.

Cette double remarque motive sur un cas particulier la construction qui suit.

...

II. Suites de Cauchy de rationnels

1°) Définition d'une suite dé rationnels :

On appelle ainsi toute application $r : \mathbb{N} \longrightarrow \mathbb{Q}$

$n \longmapsto r_n$

On note (r_n) la suite de terme général r_n.

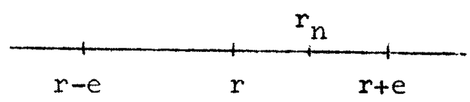
2°) Suite convergente (dans $\mathbb{Q}$) :

$(r_n$ converge vers le rationnel $r \Leftrightarrow (\forall e \in \mathbb{Q}+^*;\ \exists\ N(e) \in \mathbb{N} \mid \forall\ n \in \mathbb{N}$

$n > N(e) \Rightarrow |r_n - r| < e)$. On note $\lim\limits_{n \to +\infty} r_n = r$ et r s'appelle limite de r_n.

On note aussi $r_n \to r$.

Dans la définition on trouve : $|r_n - r| < e$. Ceci équivaut à $r - e < r_n < r + e$. La définition revient donc à dire que dès que l'on a choisi e, tous les termes de la suite (r_n) dont le rang est suffisamment grand (ce qui se formalise par $N > N(e)$) se situent dans l'intervalle (de $\mathbb{Q}$ ...) de centre r et d'amplitude 2 e, ou encore à une distance de r inférieure à e.



3°) Unicité de la limite d'une suite convergente :

Si $\lim\limits_{n \to +\infty} r_n = r$ et $\lim\limits_{n \to +\infty} r_n = r'$ alors $r = r'$

Démonstration :

$(r_n \to r) \Leftrightarrow (\forall\ \frac{e}{2} \in \mathbb{Q}_+^*,\ \exists N(e) \in \mathbb{N} \mid \forall n \in \mathbb{N}\ n > N(e) \Rightarrow |r_n - r| < \frac{e}{2})$

$(r_n \to r') \Leftrightarrow (\forall\ \frac{e}{2} \in \mathbb{Q}_+^*,\ \exists N'(e) \in \mathbb{N} \mid \forall\ n \in \mathbb{N}\ \ n > N'(e) \Rightarrow |r_n - r| < \frac{e}{2})$

Posons $N'' = \mathrm{Sup}(N(e), N'(e))$. Alors, $\forall\ e \in \mathbb{Q}_+^*$, $\forall\ n \in \mathbb{N}\ n > N'' \Rightarrow$ $|r - r'| \leq |r - r_n| + |r_n - r'| < \frac{e}{2} + \frac{e}{2} = \epsilon$, en utilisant l'inégalité triangulaire et les hypothèses ci-dessus.

Il en résulte que $r = r'$.

Remarque : tout rationnel r peut être considéré comme limite d'une suite au moins de nombres rationnels, ne serait ce que la suite définie par $r_n = r$ pour tout n.

4°) Suite de Cauchy de rationnels :

On appelle ainsi toute suite (r_n) de rationnels vérifiant la propriété suivante :

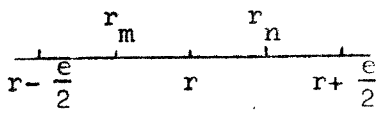
$(\forall\ e \in Q_+^*,\ \exists\ N(e) \in \mathbb{N} \mid \forall\ m \in \mathbb{N},\ \forall\ n \in \mathbb{N}\ m > N(e)$ et $n > N(e) \Rightarrow |r_m - r_n| < e)$

En clair cette propriété signifie que la distance entre deux éléments r_m et r_n de cette suite est inférieure à tout nombre rationnel $e > 0$ donné (on peut donc en particulier prendre e arbitrairement petit) pourvu que les rangs m et n considérés soient suffisamment grands [ce qui se formalise par $m > N(e)$ et $n > N(e)$].

Propriétés :

a) Toute suite convergente de rationnels est une suite de Cauchy.

Compte-tenu du commentaire précédent cette propriété paraît intuitivement évidente. Elle s'illustre comme suit :



Par contre l'intuition serait disposée à admettre la compatibilité entre un rapprochement de plus en plus "étroit" de deux termes de rang assez grand et un "déplacement" continu de ces termes.

Démonstration :

$$(r_n \to r) \Leftrightarrow \begin{cases} \forall \frac{e}{2} \in Q+^*,\ \exists N'(e) \in \mathbb{N} \mid \forall m \in \mathbb{N}\ m > N'(e) \Rightarrow |r_m - r| < \frac{e}{2} \\ \forall\ \frac{e}{2} \in Q+^*,\ \exists N''(e) \in \mathbb{N} \mid \forall n \in \mathbb{N}\ n > N''(e) \Rightarrow |r_n - r| < \frac{e}{2} \end{cases} \text{ Il en}$$

résulte, en posant $N(e) = \text{Sup}\ (N'(e), N''(e))$, que

$\forall\ e \in\ Q+^*,\ \exists\ N(e) \in\ \mathbb{N} \mid \forall\ m \in \mathbb{N},\ \forall\ n \in\ \mathbb{N},\ m > N(e)$ et $n > N(e) \Rightarrow$
$|r_m - r_n| \leq |r_m - r| + |r - r_n| < \frac{e}{2} + \frac{e}{2} = E.$

b) Toute suite de Cauchy est bornée.

Démonstration :

Dans la définition il suffit de fixer n pris supérieur à $N(e)$ pour que l'on ait, pour tout $m > N(e)$ $|r_m - r_n| < e$ ce qui implique $r_m < r_n + e$; le second membre étant un réel déterminé celà prouve bien que (r_m) est majorée. De même $r_m > r_n - e$ ce qui prouve que (r_m) est minorée, donc en définitive que (r_m) est bornée.

Remarque (non triviale) : Il existe des suites de Cauchy de rationnels non convergentes dans Q. Un exemple, entre autre, est celui de la suite de terme général $1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}$. Il fait l'objet d'un exercice

5°) Théorème :

Si (r_n) et (s_m) sont des suites de Cauchy de rationnels il en est de même des suites $(-r_n)$; $(r_n + s_n)$; $(r_n - s_n)$; $(\frac{1}{r_n})$ (sauf, dans ce dernier cas, si $r_n \to 0$).

Démonstration :

a) Pour les trois premiers cas il suffit d'établir le dernier résultat. En prenant ensuite $r_n = 0$ (pour tout n) le premier en résulte et le second découle du fait que $r_n + s_n = r_n - (-s_n)$.

(r_n) suite de Cauchy $\Leftrightarrow$ $(\forall \frac{e}{2} \in Q+^*, \exists N'(e) \in N \,|\, \forall m \in N, \forall n \in N \; m > N'$ et $n > N'$
$\Rightarrow |r_m - r_n| < \frac{e}{2})$

(s_n) suite de Cauchy $\Leftrightarrow$ $(\forall \frac{e}{2} \in Q+^*, \exists N''(e) \in N \,|\, \forall m \in N, \forall n \in N \; m > N''$ et $n > N''$
$\Rightarrow |s_m - s_n| < \frac{e}{2})$

Or, $(r_m - s_m) - (r_n - s_n) = (r_m - r_n) + (s_n - s_m)$ et si on prend m et n supérieur à $N(e) = \text{Sup}\,(N', N'')$ il en résulte bien que
$|(r_m - s_m) - (r_n - s_n)| \leq |r_m - r_n| + |s_n - s_m| < \frac{e}{2} + \frac{e}{2} = e$.

b) Démontrons le résultat pour $(r_m s_n)$. On a $r_m s_m - r_n s_n = r_m(s_m - s_n) + s_n(r_m - r_n)$. Il en résulte que :

$|r_m s_m - r_n s_n| \leq |r_m|\,|s_m - s_n| + |s_n|\,|r_m - r_n|$. Or, (r_m) et (s_m) étant des suites de Cauchy sont bornés par des nombres positifs A et B respectivement. Donc $|r_m s_m - r_n s_n| \leq A|s_m - s_n| + B|r_m - r_n|$. Posons alors $e' = \frac{e}{2B}$ et $e'' = \frac{e}{2A}$ où $e \in Q+^*$. Puisque (r_m) est de Cauchy, $\exists\, N'(e') \in N \,|\, m$ et $n > N' \Rightarrow |r_m - r_n| < e'$. De même puisque (s_m) est de Cauchy, $\exists\, N''(e'') \,|\, m$ et $n > N'' \Rightarrow |s_m - s_n| < e''$. Soit $N = \text{Sup}\,(N', N'')$, N dépendant de e. Il en résulte que $\forall\; e \in Q+^*$, si l'on prend m et n supérieurs à N(e) ainsi défini
$|r_m s_m - r_n s_n| \leq A \times e'' + B \times e' = \frac{e}{2} + \frac{e}{2} = e$ ce qui établit le résultat.

c) La démonstration repose sur le lemme suivant : si (r_n) est une suite de Cauchy de rationnels qui ne converge pas vers 0 alors, à partir d'un certain rang, tous les termes de la suite sont de même signe et minorés en valeur absolue par un nombre non nul.

...

Supposons ce lemme établi et posons $s_n = \frac{1}{r_n}$(avec $s_n = 1$ pour toute valeur de n telle oue $r_n = 0$).

$s_m - s_n = \frac{1}{r_m} - \frac{1}{r_n} = \frac{r_n - r_m}{r_m\, r_n}$ et $|s_m - s_n| = \frac{|r_n - r_m|}{|r_m\, r_n|}$. Or, d'après le lemme

précédent, pour m et $n > k \in N$, il existe un rationnel $q > 0$ tel que $r_m < -q$ et $r_n < -q$ ou bien $r_m > q$ et $r_n > q$ soit dans les deux cas $|r_m r_n| > q^2$. Il en résulte qu'alors $|s_m - s_n| < \frac{r_n - r_m}{q^2}$. Mais puisque (r_n) est une suite de Cauchy, pour m et n supérieurs à un entier k' dépendant de e, $(r_n - r_m) < q^2 e$ et par conséquent si on prend m et n supérieurs à $N(e) = \text{Sup}\ (k,k')$ alors $|s_m - s_n| < \frac{q^2 e}{q^2} = e$ ce qui prouve que (s_n) est une suite de Cauchy.

<u>Démonstration du lemme</u> :

Soit (r_n) une suite de Cauchy qui ne tend pas vers zéro. Elle vérifie les deux propriétés :

. $\forall e > 0,\ \exists k \in N,\ \forall p \in N, \forall q \in N,\ p \geq k$ et $q \geq k \Rightarrow |r_p - r_q| < e$

. $\exists\ a > 0,\ \forall n \in N,\ \exists n' \in N\ \ |r_{n'}| > a$.

choisissons alors l'entier k_o associé par la première relation au nombre $e = \frac{a}{2}$. Et appelons k'_o l'entier associé par la deuxième relation à l'entier $n = k_o$.

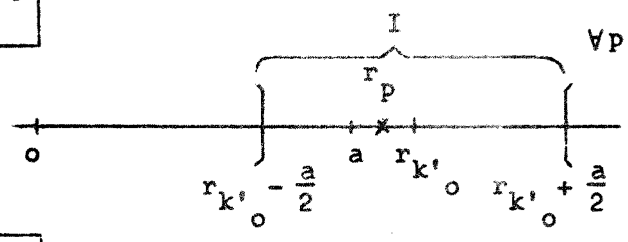
On aura puisque $k'_o \geq k_o$:

$\forall p \in N,\ p \geq k_o \Rightarrow |r_{k'_o} - r_p| < \frac{a}{2}$

et d'autre part $|r_{k'_o}| > a$.

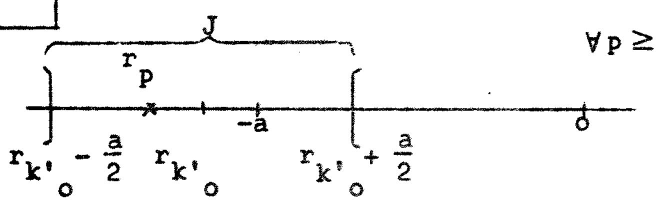
On est donc dans ou l'autre des situations illustrées ci-dessous :

$\boxed{r_{k'_o} > o}$



$\forall p \geq k_o\ \ r_p \in I$

$\boxed{r_{k'_o} < o}$



$\forall p \geq k_o\ \ r_p \in J$

Dans chaque cas pour $p \geq k_o$, r_p a le signe de $r_{k'_o}$ et est minoré en valeur absolue par : $|r_{k'_o} - \frac{a}{2}|$. ...

Soit S l'ensemble des suites de Cauchy de rationnels. On définit sur S une relation binaire en posant $(r_n) \sim (s_n) \Leftrightarrow (r_n - s_n) \to 0$

Lemme : La relation précédente est une relation d'équivalence

Démonstration :

a) réflexivité : $(r_n) \sim (r_n) \Leftrightarrow (r_n - r_n) \to 0$ ce qui est évident

b) symétrie : $[(r_n) \sim (s_n) \Leftrightarrow (r_n - s_n) \to 0] \Leftrightarrow [(s_n - r_n) \to 0 \Leftrightarrow (s_n) \sim (r_n)]$

c) transitivité : $\begin{matrix} (r_n) \sim (s_n) \\ (s_n) \sim (t_n) \end{matrix} \Leftrightarrow \begin{matrix} (r_n - s_n) \to 0 \\ \text{et} \\ (s_n - t_n) \to 0 \end{matrix}$

Or $r_n - t_n = (r_n - s_n) + (s_n - t_n)$ et donc $r_n - t_n \to 0$ ce qui prouve que $(r_n) \sim (t_n)$.

Définition : L'ensemble quotient de S par la relation précédente est appelé ensemble des nombres réels et sera noté $\mathbb{R}$. Un nombre réel est donc une classe d'équivalence de suites de Cauchy de rationnels.

III. Structure de $\mathbb{R}$ (corps commutatif)

D'après II 5°) l'ensemble S est muni de deux lois de composition internes l'addition et la multiplication qui lui confèrent manifestement une structure d'anneau commutatif unitaire. Si l'on désigne par O l'ensemble des suites de Cauchy de rationnels qui convergent vers O on peut remarquer que O est un sous-groupe de S et également un idéal de S. En se basant sur des théorèmes d'algèbre générale on peut :

a) Trouver directement la définition de $\mathbb{R}$ comme groupe quotient de S par le sous-groupe O.

b) A partir de O considéré comme idéal de S en déduire que l'addition et la multiplication de S "passent au quotient" et confèrent à $\mathbb{R}$ une structure d'anneau commutatif unitaire.

Toutefois le lecteur trouvera ci-dessous une démonstration directe du "passage au quotient".

Pour l'addition il s'agit de montrer que si $(r_n) \sim (r'_n)$ et $(s_n) \sim (s'_n)$ alors $(r_n + s_n) \sim (r'_n + s'_n)$. Il suffit de remarquer que $(r_n + s_n) - (r'_n + s'_n) = (r_n - r'_n) + (s_n - s'_n)$, somme de deux termes dont chacun tend vers O. Pour la multiplication, avec les mêmes hypothèses il s'agit de montrer que $(r_n s_n) \sim (r'_n s'_n)$. On remarque que $r_n s_n - r'_n s'_n = s_n(r_n - r'_n) + r'_n(s_n - s'_n)$ qui tend vers O compte tenu du fait que $\lim\limits_{n\to+\infty} (r_n - r'_n) = \lim\limits_{n\to+\infty}(s_n - s'_n) = 0$ et du fait que (s_n) et (r'_n) sont bornés.

Il en résulte donc la définition d'une addition et d'une multiplication dans $\mathbb{R}$ obtenue en posant, si $(\dot{r_n})$ et $(\dot{s_n})$ désignent les classes définissant les réels r et s : d'une part, $r + s = (\widehat{r_n+s_n})$ et $rs = (\widehat{r_n s_n})$ d'autre part.

La vérification des propriétés qui confèrent à $\mathbb{R}$ la structure d'anneau commutatif unitaire peut se faire directement et ne présente pas de difficultés particulières. Il ne reste plus qu'à montrer que tout réel $r \neq 0$ admet un inverse. Il en résultera en définitive la structure de corps commutatif de $\mathbb{R}$.

Démonstration :

Soit $r \neq 0$. Ce réel r est défini par (r_n) où (r_n) est une suite de Cauchy de rationnels qui ne converge pas vers 0. Considérons la suite $(s_n) = (\frac{1}{r_n})$ (avec $s_n = 1$ pour chaque valeur de n telle que $r_n = 0$. Nous savons que (s_n) est une suite de Cauchy de rationnels qui définit donc un réel s. Or $(r_n s_n) = (r_n \times \frac{1}{r_n})$ **(pour n assez grand) est une suite de Cauchy qui définit évidemment le réel 1.**

Le réel s est donc l'inverse de r pour la multiplication.

IV. Q est isomorphe à un sous-corps de $\mathbb{R}$.

D'après la remarque du II 3°) tout rationnel r est limite de la suite r_n définie par $(\forall n \in \mathbb{N},\ r_n = r)$. Désignons par (r) cette suite. Il en résulte que $r = (\dot{r})$ et tout rationnel peut-être ainsi "assimilé" à un réel.

De façon plus précise considérons l'application $f : Q \longrightarrow \mathbb{R}$

$$r \longmapsto f(r) = (\dot{r})$$

Cette application est manifestement injective, donc bijective sur $f(Q)$. De plus :

$f(r+s) = (\widehat{r+s}) = (\dot{r})+(\dot{s}) = f(r)+f(s)$ et $f(rs) = (\dot{rs}) = (\dot{r}).(\dot{s}) = f(r)f(s)$.

L'application f est donc un isomorphisme de Q sur $f(Q)$ qui apparaît ainsi comme un sous-corps de $\mathbb{R}$. Cet isomorphisme autorise l'assimilation entre Q et $f(Q)$ ce qui conduit à dire que Q est un sous-corps de $\mathbb{R}$.

V. $\mathbb{R}$ est un corps ordonné, archimédien, complet

a) $\mathbb{R}$ est ordonné :

La "construction" d'une relation d'ordre, notée $\leq$ dans $\mathbb{R}$ se fait de manière à ce que sa restriction à Q coïncide avec la relation ainsi notée dans Q. Elle est compatible avec l'addition dans $\mathbb{R}$ ainsi que la multiplication c'est-à-dire que : ...

α) $\forall\ x \in \mathbb{R}, \forall\ (a,b) \in \mathbb{R}^2,\ a \leq b \Rightarrow a + x \leq b + x$

β) $\forall\ (a,b) \in \mathbb{R}^2,\ a \geq 0$ et $b \geq 0 \Rightarrow ab \geq 0$.

On commence par définir les réels positifs (ceux dont un représentant a tous ses termes positifs) et on démontre que l'ensemble $\mathbb{R}^+$ ainsi constitué est stable par addition et multiplication et vérifie $\mathbb{R}^+ \cap \{-\mathbb{R}^+\} = \{0\}$ et $\mathbb{R}^+ \cup \{-\mathbb{R}^+\} = \mathbb{R}$.
Pour une étude complète voir par exemple
- Madame Lelong-Ferrand-Arnaudiès (L.A.) Analyse (page 8)
- Chambadal-Ovaert (C.O.) Notions fondamentales d'algèbre et d'analyse (page 372)

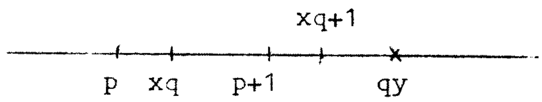
b) <u>$\mathbb{R}$ est archimédien</u> :

On montre que : $\forall\ (a,b) \in \mathbb{R}^2,\ a > 0 \Rightarrow \exists\ n \in \mathbb{N} | b \leq na$

La propriété est évidente si $b \leq a$ et ne nécessite de démonstration que si $b > a$.
Voir L.A. page 11 ou C.O. page 376 par exemple.
Cette propriété a en particulier les conséquences suivantes :

1) Entre deux réels il y a toujours un rationnel.

En effet soient y et x ($y > x$) deux réels.
Il existe un entier q tel que : $q(y - x) > 1$
et un entier p tel que : $p \leq xq < p + 1$.
On a alors la situation



donc $xq < p + 1 < qy$
et le rationnel $z = \dfrac{p + 1}{q}$ répond à la question.

2) Entre deux rationnels il y a toujours un irrationnel

En effet soient e un irrationnel et a et b deux rationnels.
Il existe un entier p tel que $p(b - a) > e$ et le nombre $c = a + \dfrac{e}{p}$ convient (il ne peut être rationnel sinon $e = (c - a).\ p$ le serait).

<u>Remarque</u> : cela ne veut pas dire qu'il y a "autant" de rationnels que d'irrationnels : puisque ceux-ci constituent un ensemble ayant la la puissance du continu alors que $\mathbb{Q}$ est dénombrable.

...

c) $\mathbb{R}$ est complet :

On exprime par ce mot que si on répète à partir des suites de Cauchy de réels la construction faite à partir des suites de Cauchy de rationnels on n'obtient pas un sur-corps de $\mathbb{R}$ mais $\mathbb{R}$ lui-même. Voici à titre indicatif le principe de la méthode :

α) On étend à $\mathbb{R}$ la notion de convergence déjà définie dans Q et on montre d'abord que tout nombre réel est la limite, au sens de la limite dans $\mathbb{R}$, de toute suite de Cauchy de rationnels qui définit ce réel.

β) Soit (r_n) une suite de Cauchy de réels. Chaque réel r_n de cette suite est défini par une suite de Cauchy de rationnels $(q_{n,k})$. En prenant k suffisamment grand, pour chaque n, on construit une suite de Cauchy de rationnels qui "approche" la suite de réels donnée. Cette suite définit un réel a dont on montre qu'il est la limite (au sens de $\mathbb{R}$) de la suite de réels donnée. En résumé toute suite de Cauchy de réels est convergente dans $\mathbb{R}$ ($\mathbb{R}$ est complet) (voir L.A. page 17 ou C.O. page 374)

VI. Où l'on s'assure qu'on a obtenu ce que l'on cherchait...

Il nous reste maintenant à vérifier que le corps ainsi construit répond bien aux objectifs fixés :
- existence de racines carrées
- existence d'une borne supérieure pour toute partie non vide majorée.

Pour cela nous commencerons par établir une propriété qui constitue en fait une traduction géométrique du critère de Cauchy.

1°) Théorème des segments emboîtés

Soit $(I_n)_{n \in N}$ une suite décroissante ($\forall n\ I_{n+1} \subset I_n$) d'intervalles fermés bornés non vides de $\mathbb{R}$ ($I_n = [a_n, b_n]$, $a_n \neq b_n$) tels que $b_n - a_n \to 0$ quand n augmente indéfiniment.

Alors l'ensemble $\bigcap_{n \in N} I_n$ est constitué d'un point et d'un seul soit l qui est la limite commune des deux suites (a_n) et (b_n).

...

Démonstration :

a) existence d'un point commun : Choisissons dans chaque intervalle I_n un point $u_n \in I_n$. On définit ainsi une suite qui est de Cauchy car si $r \leq s$; $|u_s - u_r| \leq |a_r - b_r|$ puisque $u_s \in I_s \subset I_r$ et $|a_r - b_r| \to 0$ donc peut être rendu arbitrairement petit en choisissant r et s assez grands.

La suite (u_n) converge donc vers un réel l.

Et $l \in \bigcap_{n \in N} I_n$ car pour tout $p \in N$ puisque

$I_n \subset I_p$ pour $n \geq p$ on a $a_p \leq u_n \leq b_p$ pour $n \geq p$ donc $a_p \leq l \leq b_p$ et $l \in I_p$.

b) unicité : Soit $l' \in \bigcap_{n \in N} I_n$ alors $\forall$ m, $|l' - l| \leq |a_m - b_m|$

puisque l et l' sont des points de I_m. Comme $|a_m - b_m| \to 0$, on a nécessairement $l = l'$.

c) est un cas particulier de a) en choisissant systématiquement . ou bien $u_n = a_n \ \forall\ n \in N$

. ou bien $u_n = b_n \ \forall\ n \in N$

2°) Existence de racines k ièmes.

On montre qu'étant donné un réel $a > 0$ et un entier $k \neq 0$, il existe un unique réel $x > 0$ tel que $x^k = a$.

On utilise pour cela la suite constituée par les approximations décimales. de cette racine.

Soit p_n le plus grand entier tel que $(10^{-n} p_n)^k \leq a$. Un tel entier existe car l'ensemble des entiers p tels que $10^{-nk} p^k \leq a$ est majoré par $10^n x_1$ (par exemple) où $x_1 = E(x) + 1$ (E(x) : partie entière de x).

Les nombres $a_n = 10^{-n} p_n$ et $b_n = 10^{-n}(p_n + 1) = a_n + 10^{-n}$ vérifient :

(1) $a_n^k \leq a \leq b_n^k$

et $a_n \leq a_{n+1} < b_{n+1} \leq b_n$

Les intervalles $I_n = [a_n, b_n]$ réalisent donc les hypothèses du théorème précédent puisque

$$b_n - a_n = 10^{-n} \to 0$$

Les suites (a_n) et (b_n) ont donc une limite commune : le nombre x unique élément de $\bigcap_{n \in N} I_n$.

La relation (1) montre alors que l'on a :

$$x^k \leq a \leq x^k \text{ donc } a = x^k.$$

L'unicité provient de ce que la fonction $\begin{array}{l} R^+ \to R^+ \\ x \to x^k \end{array}$ est strictement croissante donc injective.

Remarquons que, puisque a_n et b_n sont des nombres décimaux qui vérifient : $a_n \leq x \leq b_n$ et $b_n - a_n = 10^{-n}$, les suites (a_n) et (b_n) constituent les approximations décimales par défaut et par excès de la racine x.

3°) Borne supérieure d'une partie non vide majorée

Soit E une partie non vide de R, majorée par m : $\forall\ x \in E,\ x \leq m$. Rappelons qu'on appelle borne supérieure de E, le plus petit des majorants donc : un élément b tel que 1) $\forall\ x \in E\quad x \leq b$

2) $\forall$ m m majore E $\Rightarrow m \geq b$.

Remarquons que comme dans R l'ordre est total, il revient au même de dire que b est borne supérieure ou de dire que b est un majorant et que tout nombre $c \in R$ tel que $c < b$ n'est plus un majorant de E autrement dit :

$\forall\ c \in R,\ c < b \Rightarrow \exists\ x \in E,\ x > c.$

On peut encore exprimer ceci (c'est la définition la plus souvent utilisée) en remarquant que si $c < b$, c peut s'écrire $c = b - e$ avec $e > 0$. La propriété 2) devient :

"$\forall\ e > 0\ \exists\ x \in E\ x > b - e$

Nous allons maintenant établir l'une des propriétés ayant motivé la construction de R : toute partie non vide majorée de R admet une borne supérieure.

Pour cela on construit une suite I_n d'intervalles vérifiant les hypothèses du théorème précédant, on en déduit l'existence d'un unique point commun à ces intervalles, dont on montre qu'il est la borne supérieure de E.

Soit m un majorant de E et $x \in \mathbb{R}$ un nombre qui ne soit pas un majorant de E (donc tel qu'il existe $y \in E$ avec $y > x$). Un tel x existe parce que $E \neq \emptyset$.

Posons $I_1 = [x_1, m]$ et soit $x_2 = \frac{x_1 + m}{2}$ le milieu de I_1 :

. ou bien x_2 est un majorant de E et on pose $I_2 = [x_1, x_2]$

. ou bien x_2 n'est pas un majorant de E et on pose $I_2 = [x_2, m]$.

On a ainsi construit un intervalle $I_2 = [\alpha_2, \beta_2]$ tel que α_2 ne majore pas E et β_2 majore E.

On recommence le même procédé et on fabrique ainsi une suite (I_n) d'intervalles $[\alpha_n, \beta_n]$ tels que α_n ne soit pas un majorant de E alors que β_n majore E. Cette suite (I_n) vérifie les hypothèses du théorème précédant puisque I_n a pour longueur $\frac{m - x_1}{2^n}$ (on coupe à chaque étape l'intervalle en deux).

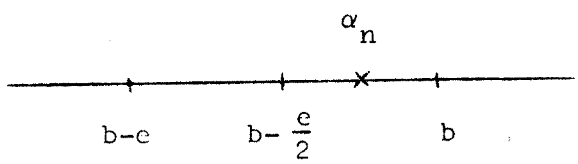
Soit alors $\{b\} = \bigcap_{n \in N} I_n$.

. <u>b est un majorant de E</u> : car $b = \lim \beta_n$ et chaque β_n vérifie $\forall\ x \in E \quad \beta_n \geq x$ donc $b \geq x$.

. <u>b est le plus petit des majorants</u> : on montre que $\forall\ e > 0$ $b - e$ n'est plus un majorant.

Or comme $b = \lim \alpha_n$ (suite croissante) il existe un entier n_o tel que si $n \geq n_o$ on ait

$b - \frac{e}{2} < \alpha_n < b.$



Or α_n n'est pas un majorant de E donc a fortiori $b - e$ n'en est pas un.

<u>Remarque</u> : Rien n'interdit à b d'appartenir à E. On dit alors que b est le plus grand élément de E.

II ème Partie

1. CARDINAUX

Nous abordons ici une introduction <u>cardinale</u> du nombre. L'intérêt de cette approche est qu'elle semble actuellement prévaloir dans l'enseignement primaire (où bien entendu on ne fait pas la "théorie" mais où l'on adopte une démarche qui en découle).

Nous ne ferons pas une étude exhaustive ni même rigoureuse des cardinaux mais essaierons de montrer comment à partir de notions ensemblistes simples il est possible d'atteindre rapidement les cardinaux et leurs opérations dont les propriétés s'établissent le plus souvent de manière beaucoup plus simple que dans le cas des ordinaux. Malheureusement sans une théorie axiomatique assez poussée des ensembles il n'est pas possible de donner un fondement correct à cette construction. Pour ceux qui s'intéressent à cette question consulter par exemple : J-L Krivine : Théorie axiomatique des ensembles Collection Sup.

L'étude des cardinaux nous conduira ensuite très naturellement à aborder quelques problèmes liés aux notions d'infini.

1°) <u>ENSEMBLES EQUIPOTENTS</u>

On dira que deux ensembles A et B sont équipotents <u>s'il existe une bijection de A sur B</u>. On écrira : <u>A eq. B.</u>

Remarquons tout de suite que nous ne faisons aucune hypothèse sur A et B : par exemple les ensembles $A = \{0,\square,\Delta\}$ et $B = \{Z,U,T\}$ sont équipotents mais aussi les ensembles $]0,1[$ et $]1,+\infty[$ en considérant la bijection $f :]0,1[\to]1,+\infty[$

$$x \mapsto \frac{1}{x}$$

ou encore les ensembles N et 2N (nombres pairs) par la bijection $g : N \to 2N$

$$x \mapsto 2x$$

Bien entendu en général, il y a <u>plusieurs</u> bijections entre deux ensembles équipotents.

Propriétés : a) $\forall A$ A eq. A (l'identité est une bijection!)

b) $\forall A, \forall B$, A eq. B $\Rightarrow$ B eq. A (prendre la bijection réciproque)

c) $\forall A, \forall B, \forall C$, (A eq. B) et (B eq. C) $\Rightarrow$ (A eq. C) (le composé de deux bijections est une bijection).

.../...

On a donc les propriétés d'une relation d'équivalence. Mais on ne peut parler des ensembles qui seraient les classes d'équivalence puisque "eq" n'est pas une relation dans un ensemble (il n'y a pas d'ensemble de tous les ensembles). On parlera alors de classes d'ensembles équipotents. Tous les membres d'une même classe ont une propriété commune : on dit qu'ils ont même cardinal. On écrit Card A = Card B pour A eq. B et on notera les cardinaux par des lettres minuscules : a = Card A.

2°) OPERATIONS ENTRE CARDINAUX

Addition

Soient a et b des cardinaux. Choisissons des ensembles disjoints A et B ($A \cap B = \emptyset$) tels que a = Card A et b = Card B.

Ceci est toujours possible car si $A \cap B \neq \emptyset$ on remplace A et B par $A_1 = A \times \{0\}$ et $B_1 = B \times \{1\}$ qui sont disjoints et ont respectivement même cardinal que A et B (prendre pour bijection la première projection).

On définit alors le cardinal somme des cardinaux a et b, qu'on note $a + b$, par $a + b = \text{Card}(A \cup B)$ (rappelons que $A \cap B = \emptyset$)

Justification : Pour que cette définition ne soit pas stupide il faut s'assurer (c'est facile !) que s'il y a une bijection f de A sur A' et une bijection g de B sur B', il y en a une de $A \cup B \to A' \cup B'$: c'est bien le cas si $A \cap B = A' \cap B' = \emptyset$ puisqu'alors il suffit de prendre l'application qui, restreinte à A est f et restreinte à B est g.

Propriétés : on a immédiatement la traduction en terme de cardinaux des propriétés de l'opération $\cup$ entre ensembles : associativité, commutativité, existence d'un élément neutre : card $\emptyset$ noté 0.

- il est naturel de chercher à retrouver la régularité.

Mais on sait bien que sans hypothèse supplémentaire cette tentative est vouée à l'echec puisque par exemple : Card N + Card $\{-1\}$ = Card N (prendre la bijection $f(x) = x + 1$) alors que Card $\{-1\} = 1 \neq 0$.
On ne pourra établir la régularité que pour des cardinaux finis dont la définition et l'étude sera faite au chapitre suivant.

Multiplication

Soient a et b deux cardinaux et A et B deux ensembles tels que a = Card A et b = Card B. On définit le produit des cardinaux a et b (qu'on note $a \times b$ ou ab) par :

.../...

$a \times b = \mathrm{Card}(A \times B)$ (où $A \times B$ désigne le produit cartésien des ensembles A et B)

Une justification de cette définition, analogue à celle de l'addition, est laissée au lecteur...

Propriétés : 1°) Cette fois-ci, le produit cartésien n'étant ni commutatif ni associatif, les seules propriétés qui soient la traduction de propriétés ensemblistes sont :

* La distributivité par rapport à l'addition, puisque $A \times (B \cup C) = (A \times B) \cup (A \times C)$ et que si $B \cap C = \emptyset$, $(A \times B) \cap (A \times C) = \emptyset$

* Le fait que 0 est absorbant puisque $A \times \emptyset = \emptyset$ donc $a \times 0 = 0$.

2°) Les propriétés "habituelles" de la multiplication s'établissent alors comme suit :

* Commutativité : Les ensembles $A \times B$ et $B \times A$ sont équipotents : considérer la bijection $A \times B \to B \times A$

$$(x,y) \mapsto (y,x).$$

donc $a \times b = b \times a$.

* Associativité : Les ensembles $A \times (B \times C)$ et $(A \times B) \times C$ sont équipotents : considérer la bijection :

$(A \times B) \times C \to A \times (B \times C)$

$((x,y),z) \mapsto (x,(y,z))$

* Elément neutre : On dit que A est un ensemble à un élément (ou un singleton) si : $(\forall x \in A,\ \forall y \in A,\ x = y)$ et $A \neq \emptyset$

Tous les singletons ont même cardinal noté 1. Le cardinal 1 est neutre pour la multiplication car $A \times \{x_o\} \to A$

$(x,x_o) \mapsto x$ est une bijection

donc $a \times 1 = a$

3°) Le problème de la régularité (pour les cardinaux $\neq 0$) se pose de manière analogue au cas de l'addition.

3°) Relation d'ordre

On dira que le cardinal a est inférieur ou égal au cardinal b et on écrira $a \leq b$, si A et B étant des ensembles de cardinal a et b respectivement, il existe une injection de A dans B.

.../...

On constate qu'une telle définition est licite en remarquant que le composé d'une injection et de bijections est une injection.

Propriétés.

a) * Réflexivité : $a \leq a$ car une bijection est une injection.

* Antisymétrie : il s'agit de montrer que s'il y a une injection de A dans B et une injection de B dans A, il y a une bijection de A dans B. Cette propriété n'est pas du tout "évidente" : c'est le théorème de Schroeder-Bernstein (1897) (ou de Cantor-Bernstein suivant les auteurs) dont on peut par exemple trouver une démonstration dans : Glaeser (Mathématique pour l'élève professeur page 142) ou dans Krivine (déjà cité) p. 38.

* Transitivité : il suffit de composer les injections.

La relation définie est donc une relation d'ordre

b) Cet ordre est total

Autrement dit, étant donnés deux cardinaux a et b, on a $a \leq b$ ou $b \leq a$.
Ce sera établi si on montre qu'étant donnés deux ensembles A et B, il y a une injection de A dans B ou une injection de B dans A.
Cette propriété démontrée par Zermelo en 1904 utilise l'axiome du choix.
Voir par exemple Glaeser page 143.

c) Compatibilité avec l'additon et la multiplication

a) Si $a \leq b$ alors $a + c \leq b + c$ (a,b,c désignent des cardianux).
En effet choisissons des ensembles A,B,C tels que $a = \text{Card } A$, $b = \text{Card } B$, $c = \text{Card } C$ et $A \cap C = B \cap C = \emptyset$.
Par hypothèse, il y a une injection $f : A \to B$.
Alors en posant $g(x) = f(x)$ si $x \in A$
$g(x) = x$ si $x \in C$
On définit une application (puisque $A \cap C = \emptyset$) de $A \cup C$ dans $B \cup C$ qui est une injection (puisque $B \cap C = \emptyset$ et f injective).

b) Si $a \leq b$ alors $a \times c \leq b \times c$
Avec les notations précédentes, il suffit de remarquer que l'application
$h : A \times C \to B \times C$
$(x,y) \mapsto (f(x),y)$ est encore injective.

2. FINI - INFINI

Si l'existence d'ensembles finis est une conséquence immédiate des axiomes ensemblistes, celle d'ensembles infinis est beaucoup moins évidente et c'est même un des axiomes des théories mathématiques généralement adoptées.

Théorème A :

Soit X un ensemble. Les propriétés suivantes sont équivalentes :

1° Le seul ensemble contenu dans X et équipotent à X est **X lui-même.**

2° On a $\text{card } X \neq \text{card } X + 1$

Montrons non (2) $\Rightarrow$ non (1)

Si $\text{card } X = \text{card } X + 1$, en désignant par a un objet non élément de X, il existe une bijection f de $x \cup \{a\}$ sur X, l'image de $X \cup \{a\}$ par f est équipotente à X et contenue dans X d'où non 1.

Montrons non (1) $\Rightarrow$ non (2).

Soit X' équipotent à X et $X' \subset X$.

On a si $X' \subset X$ $X = X' \cup (X - X')$ avec $X' \cap (X - X') = \emptyset$

donc $\text{card } X = \text{card } X' + \text{card } (X - X')$ mais X' équipotent à X implique $\text{card } X' = \text{card } X$, et $X - X'$ non vide implique $\text{card } (X - X') \geq 1$ donc d'une part $\text{card } X \geq \text{card } X + 1$; d'autre part $\text{card } X + 1 \geq \text{card } X$, d'où $\text{card } X = \text{card } X + 1$.

Définitions :

On dit qu'un ensemble X est fini s'il possède l'une des propriétés (1) ou (2). On dit qu'un ensemble X est infini dans le cas contraire .

De même un cardinal x est fini si $x \neq x + 1$

" " " " " " infini si $x = x + 1$

Un cardinal fini est un entier naturel

" " infini " un nombre transfini

Dans la suite nous allons nous intéresser plus particulièrement à deux sortes d'infinis : les infinis dénombrables et les infinis contenus.

Théorème B.

$\mathbb{N}$ est défini précédemment. Montrons que $\mathbb{N}$ est infini.

Il existe une bijection de $\mathbb{N}$ sur $\mathbb{P}$ (ensemble des naturels pairs).

$$\begin{cases} \mathbb{N} \to \mathbb{P} \\ x \mapsto 2x \end{cases}$$

donc $\mathbb{N}$ est équipotent à un ensemble $\mathbb{P} \neq \mathbb{N}$ et tel que $\mathbb{P} \subset \mathbb{N}$ donc d'après le théorème A (1) $\mathbb{N}$ est infini.

Le cardinal de $\mathbb{N}$ (card $\mathbb{N}$) s'appelle la puissance du dénombrable.

Définition:

Remarque :

Si on a construit $\mathbb{N}$ comme dans la première partie, l'axiome introduit portait le nom "d'axiome de l'infini"

Si on adopte une définition par les cardinaux (comme dans Krivine) il faut introduire l'axiome : les cardinaux finis (au sens du théorème B) forment un ensemble. (Alors que la collection de tous les cardinaux n'en est pas un.)

Dans toutes les présentations il faut un axiome pour affirmer l'existence d'un ensemble (pas d'une collection) infini. La nécessité d'un tel axiome devient manifeste quand on dispose d'un modèle qui vérifie tous les axiomes de la théorie des ensembles sauf celui-là et dans lequel on peut montrer (mais bien sûr de l'extérieur de la théorie) qu'aucun ensemble n'y est infini. Un tel modèle est exposé dans un article de Laurent SCHWARTZ dans le Bulletin de l'A.P.M. n° 261 (mars-avril 1968).

Un ensemble X est dénombrable s'il existe une bijection de X sur $\mathbb{N}$.

Exemple :

(1) Il est facile de montrer que $\mathbb{Z}$ est dénombrable.

(2) Montrons que $\mathbb{Q}^+$ est dénombrable. Il suffit de montrer qu'il existe une bijection de $\mathbb{Q}^+$ sur $\mathbb{N}$. Pour cela, il suffit d'écrire les éléments de $\mathbb{Q}^+$ sous forme d'une suite illimitée contenant chacun des éléments une fois et une seule, par exemple on écrit d'abord les éléments dont la somme des termes est 1, puis 2....

1 $\frac{0}{1}$

2 $\frac{1}{1}$

3 $\frac{1}{2}$ $\frac{2}{1}$

4 $\frac{1}{3}$ $\frac{3}{1}$

5 $\frac{1}{4}$ $\frac{2}{3}$ $\frac{3}{2}$ $\frac{4}{1}$

etc....

il est alors aisé de mettre cet ensemble en bijection avec $\mathbb{N}$.

L'idée qu'il n'existe "pas plus" de rationnels que de naturels

est à première vue contraire au "bon sens" mais c'est précisément l'une des plus grandes réussites de Cauter que d'avoir pu disqualifier l'emploi du "bon sens" en mathématique.
Nous allons montrer maintenant qu'il existe des ensembles infinis qui ne peuvent pas être mis en bijection avec $\mathbb{N}$.

Théorème C : (Cantor)

Pour tout cardinal x on a $x < 2^x = \text{card } \mathcal{P}(x)$.
Pour faire la démonstration on peut considérer un ensemble X et une application f de X dans $\mathcal{P}(X)$ (ensemble des parties de X)

si $\text{card } X = x$

$\text{card } \mathcal{P}(X) = 2^x$

et on montre qu'il n'existe aucune application surjective de X dans $\mathcal{P}(X)$ d'où $\text{card } X < \text{card } \mathcal{P}(X)$.
On en tire donc $\text{card } \mathbb{N} < \text{card } \mathcal{P}(\mathbb{N})$.
Si $\mathbb{R}$ est l'ensemble des nombres réels on montre que $\text{card } \mathbb{R} = 2^{\text{card } \mathbb{N}} = \text{card } \mathcal{P}(\mathbb{N})$ (voir par exemple Glaeser p. 146).

$\mathbb{R}$ n'est donc pas dénombrable. Tout ensemble en bijection avec $\mathbb{R}$ a la puissance du continu. (Mais, par exemple, $\mathcal{P}(\mathbb{R})$ n'a pas la puissance du continu, mais une puissance strictement plus grande).
Depuis le début du siècle on a cherché en vain à établir "l'hypothèse du continu" à savoir que toute partie infini de $\mathbb{R}$ est équipotente à $\mathbb{N}$ ou à $\mathbb{R}$ (c'est-à-dire qu'il n'y a pas de cardinal intermédiaire entre $\text{card } \mathbb{N}$ et $\text{card } \mathbb{R}$).
Fin 1962 et conformément à ce que certains logiciens soupçonnaient depuis une trentaine d'années un jeune mathématicien américain Paul Cohen, a établi que l'hypothèse du continu est indécidable.
Ce résultat formidable montre qu'on a le droit d'ajouter aux mathématiques un nouvel axiome indépendant des précédents à savoir l'hypothèse du continu ou sa négation, au choix !

Ces quelques réflexions nous conduisent à des remarques surprenantes. Cantor a démontré le théorème suivant :

"Le plan R^2 et la droite R sont équipotents"
"Il y a "autant de points" dans le plan que sur une droite mais la bijection construite n'est pas continue (autrement dit la dimension est un invariant topologique mais pas ensembliste)
Pour démontrer le théorème précédent (qui fut très violemment contesté au début de ce siècle) on peut se borner à montrer, qu'il y a "autant de points" dans le carré $\begin{cases} 0 < x \leq 1 \\ 0 < y \leq 1 \end{cases}$

que sur le segment $0 < z \leq 1$.
Considérons le développement décimal illimité de x et de y et divisons la suite de leurs chiffres en groupes ne contenant qu'un seul chiffre différent de 0.
A partir du couple (x,y) nous formons z en écrivant après la virgule, le premier groupe de chiffres de x, puis le premier groupe de chiffres de y et ainsi de suite : par exemple, au couple :

$$x = 0{,}4108007....$$

$$y = 0{,}03700062.....$$

on fait correspondre

$$z = 0{,}403170800060072....$$

Réciproquement, à tout z ($0 < z \leq 1$), à partir de son développement illimité on fera correspondre le nombre x obtenu en écrivant après la virgule le premier groupe de décimales de z, puis le $3^{\text{ème}}$, etc... et le nombre y obtenu en écrivant après la virgule le $2^{\text{ème}}$ groupe de décimales de z, puis le quatrième, etc...
L'application ainsi définie est bien une bijection ; le résultat est démontré.

<u>Exercices</u> :

1° Montrer qu'il y a "autant de points" sur $]0,1[$ que sur $]1, +\infty[$ (l'application de $]0,1[\to]1, +\infty[$ telle que

$$x \mapsto \frac{1}{1-x}$$ réalise la bijection)

2° Montrer que l'ensemble des suites de nombres réels, comme l'ensemble des suites de nombres entiers a la puissance du contenu.

3° Montrer que l'ensemble des fonctions <u>continues</u> de R dans R a la puissance du continu (alors que l'ensemble des fonctions (et même des fonctions monotones) de R dans R a une puissance strictement supérieure à celle de R.

Pour terminer, reprenons le problème de la régularité des cardinaux finis pour l'addition et pour la multiplication.

1° Si a,b,et c sont des cardinaux finis, $a + b = a + c \Rightarrow b = c$.

Soient A,B,C trois ensembles tels que $a = \text{Card } A$, $b = \text{Card } B$, $c = \text{Card } C$ et tels que $A \cap B = A \cap C = \emptyset$. Comme l'ordre est total, si $b \neq c$, ou bien $b < c$ ou bien $c < b$. Supposons $b < c$, c'est-à-dire qu'il existe une injection $f : B \to C$ qui n'est pas une bijection donc telle que $f(B) \neq C$.

Alors f permet de définir une bijection de B sur f(B) donc de $A \cup B$ sur $A \cup f(B)$ et on a $\text{Card } (A \cup B) = \text{Card } (A \cup f(B)) = \text{Card } (A \cup C)$. Et il existerait une bijection de $A \cup C$ sur $A \cup f(B)$ qui en est une partie propre, contrairement à l'hypothèse que les cardinaux considérés sont finis.

2° On peut en fait démontrer la propriété plus forte : si a est un cardinal fini, $a + b = a + c \Rightarrow b = c$.

Le cas $a = 1$ est très facile à établir (c'est un excellent exercice !).

3° Pour la multiplication, la démarche est tout à fait analogue et nous en laissons le soin au lecteur.....

ANNEXE 2

LES COUPURES

Il s'agit de la construction de $\mathbb{R}$ proposée par Dedekind basée sur l'idée suivante : les nombres rationnels constituent un corps muni d'un ordre tel que :

1° Entre deux éléments il y en a toujours un troisième (ceci est faux dans $\mathbb{N}$ et dans $\mathbb{Z}$).

2° Tout élément sépare l'ensemble en deux classes non vides telles que tout élément de la première classe minore tout élément de la seconde.

On obtiendra l'ensemble des réels en cherchant le corps "maximum" (prolongeant $\mathbb{Q}$) possédant les propriétés. Pour cela il suffit d'exiger pour l'"opération" du 2ème) la même fermeture que pour les opérations arithmétiques habituelles .

1) Coupures dans $\mathbb{Q}$. Nombres réels

A partir du 2°, le plus naturel serait d'appeler coupure toute partition de $\mathbb{Q}$ en deux sous-ensembles A et B (qui seraient donc non vides et complémentaires) tels que :

$\forall a \in A,\ \forall b \in B,\ a < b$.

Il suffirait de constater que si dans le cas où l'un des ensembles A ou B possède un élément extrémal ($A = \{x \in \mathbb{Q} \mid x \leq 2\}$ par exemple) on "retrouve" les rationnels déjà connus, par contre dans d'autres cas ni A ni B n'ont d'éléments extrémaux (exemple :

$A = \{x \in \mathbb{Q} \mid x \geq 0 \text{ et } x^2 > 2\}$ $B = \mathbb{Q} - A$) et la partition (A,B) "encadre" ce qu'on appellera un nombre irrationnel.

Nous indiquerons ultérieurement pourquoi on ne peut pas adopter ce point de vue.

Remarquons alors que si(A,B) est une partition de $\mathbb{Q}$ telle que $\forall a \in A,\ \forall b \in B\ a < b$, les trois propriétés suivantes sont vérifiées :

i) $\forall a \in A\ \forall x \in \mathbb{Q} \quad x \leq a \Rightarrow x \in A$

ii) $\forall b \in B,\ \forall x \in \mathbb{Q} \quad b \leq x \Rightarrow x \in B$

iii) A et B sont <u>adjacent</u> c'est-à-dire que :

a) $\forall a \in A,\ \forall b \in B \quad a \leq b$

b) $\forall \varepsilon \in \mathbb{Q}^+_*,\ \exists\, a \in A,\ \exists b \in B \quad b - a < \varepsilon$

(Nous notons $\mathbb{Q}^+_*$ l'ensemble des rationnels <u>strictement</u> positifs et $\mathbb{Q}^+ = \mathbb{Q}^+_* \cup \{0\}$).

Mais la réciproque n'est pas exacte : par exemple $A = \{x \in \mathbb{Q} \mid x \leq 2\}$ et $B = \{x \in \mathbb{Q} \mid x \geq 2\}$ vérifient i), ii), et iii) mais ne forment pas une partition parce que $A \cap B = \{2\} \neq \emptyset$. De même $A' = \{x \in \mathbb{Q} \mid x < 2\}$, $B' = \{x \in \mathbb{Q} \mid x > 2\}$ vérifient i, ii), et iii) alors que $A' \cup B' = \mathbb{Q} - \{2\} \neq \mathbb{Q}$.

Toutefois, on peut établir que :

1° $A \cap B$ est $\emptyset$ ou un singleton

2° $A \cup B$ est : $\mathbb{Q}$ ou $\mathbb{Q} - \{r\}$. Autrement dit il y a au plus un rationnel non classé.

<u>Définition</u> :

On appellera coupure dans $\mathbb{Q}$ tout couple (A,B) de sous-ensembles de $\mathbb{Q}$ vérifiant i), ii), iii).

Il y a plusieurs sortes de coupures :

- A ou B possède un élément extrémal (ils peuvent en avoir tous deux : c'est alors le même soit r et $A \cap B = \{r\}$).
- ni A ni B n'ont d'élément extrémal. Ceci se produit dans deux cas :
  1) il y a un rationnel non classé : $A \cup B = \mathbb{Q} - \{r\}$: A et B encadrent le rationnel r.
  2) tous les rationnels sont classés : la coupure n'encadre aucun rationnel (cf. exemple donné au début) et définit un <u>irrationnel</u>. Dans ce cas la coupure est une partition.

Remarquons encore qu'à tout rationnel $r \in \mathbb{Q}$ sont associés 4 coupures différentes :

1° $A = \{x \leq r\} \quad B = \{x \geq r\}$

2° $A = \{x < r\} \quad B = \{x \geq r\}$

3° $A = \{x \leq r\} \quad B = \{x > r\}$

4° $A = \{x < r\} \quad B = \{x > r\}$

Après avoir identifié ces coupures on appellera :

Nombre réel : toute coupure dans le corps $\mathbb{Q}$.

On notera $\alpha = (A,B)$ un réel et $\mathbb{R}$ l'ensemble (dont on admet l'existence) qu'ils constituent.

Remarquons enfin que tout nombre réel peut être représenté par une coupure qui est une partition de $\mathbb{Q}$: pour les irrationnels c'est évident, pour les rationnels les coupures (2) et (3) sont des partitions.

2° Relation d'ordre dans $\mathbb{R}$

Soient $\alpha = (A,B)$ et $\alpha' = (A',B')$ deux réels qu'on suppose représentés par des coupures qui sont des partitions de $\mathbb{Q}$.

On dira alors que α est inférieur ou égal à α' et on écrira

$\alpha \leq \alpha'$ si $A \subset A'$.

Les propriétés bien connues de l'inclusion montrent que c'est une relation d'ordre.

Cet ordre est total. En effet si $A \not\subset A'$, c'est qu'il existe un élément $a \in A$ tel que $a \notin A'$. Comme $B' = \mathbb{Q} - A'$, c'est que $a \in B'$. Soit alors a' un élément quelconque de A'. Puisque $a \in B'$ et $a' \in A'$ on a : $a' \leq a$. Mais alors puisque $a \in A$ on en déduit que $a' \in A$. Et donc $A' \subset A$. Donc pour 2 coupures ou bien $A \subset A'$ ou bien $A' \subset A$.

Remarquons que $\alpha \geq 0$ signifie $0 \in A$ si $\alpha = (A,B)$ est une coupure qui est une partition (donc $\mathbb{Q}^- \subset A$).

3° Opérations dans $\mathbb{R}$

ADDITION

Si $\alpha = (A,B)$ et $\alpha' = (A',B')$ sont deux réels on pose :

$A'' = \{a + a' \mid a \in A,\ a' \in A'\} = A + A'$ (par définition)

$B'' = B + B'$

On vérifie que (A'',B'') constitue une coupure dans $\mathbb{Q}$ donc un nombre réel qu'on note $\alpha + \alpha'$.

Pour cela il suffit d'établir :

i) Soit $a'' \in A''$ donc $a'' = a + a'$ avec $a \in A$ et $a' \in A'$ et soit $x \in \mathbb{Q}$ tel que $x \leq a''$ montrons que $x \in A''$.

Or $x = a'' - h$ avec $h \in \mathbb{Q}^+$ (puisque $x \leq a''$) donc

$x = a + a' - h = a - \frac{h}{2} + a' - \frac{h}{2}$

$$\left.\begin{array}{l} \text{et } a - \frac{h}{2} \leq a \text{ donc } a - \frac{h}{2} \in A \\ a' - \frac{h}{2} \leq a' \text{ donc } a' - \frac{h}{2} \in A' \end{array}\right\} \text{donc } x \in A''.$$

ii) est identique

iii) a) $\forall a'' \in A''$, $\forall b'' \in B''$, $a'' \leq b''$ puisque
$(a' \leq b'$ et $a \leq b) \Rightarrow a + a' \leq b + b'$

b) Soit $\epsilon \in \mathbb{Q}^{+}_{*}$, alors $\exists a \in A$, $\exists b \in B$ $b - a < \frac{\epsilon}{2}$

et $\exists a' \in A'$ $\exists b' \in B'$ $b' - a' < \frac{\epsilon}{2}$

donc $a'' = a + a'$ $(\in A'')$ et $b'' = b + b'$ $(\in B'')$ sont tels que $b'' - a'' < \epsilon$.

Remarquons que c'est cette définition de l'addition qui empêche d'exiger qu'une coupure soit une partition. En effet, si (A,B) et (A',B') sont des partitions telles que A (resp. A') minore B (resp. B'), $(A + A', B + B')$ n'est pas toujours une <u>partition</u> comme le montre l'exemple ci-dessous :

$A = \{x \in \mathbb{Q}^+ \mid x^2 < 2\} \cup \mathbb{Q}^-\}$
$B = \{x \in \mathbb{Q}^+ \mid x^2 > 2\}$ } encadrent $\sqrt{2}$

$A' = \{x \in \mathbb{Q}^- \mid x^2 > 2\}$
$B' = \{x \in \mathbb{Q}^- \mid x^2 < 2\} \cup \mathbb{Q}^+\}$ } encadrent $-\sqrt{2}$

Alors $(A + A') \cup (B + B') = \mathbb{Q} - \{0\}$: A'' et B'' encadrent 0 mais 0 ne peut s'écrire comme somme d'un élément de A et d'un élément de A', ni d'un élément de B et d'un élément de B'.

<u>Propriétés</u> :

- <u>L'associativité</u> et la <u>commutativité</u> ne posent aucun problème
- <u>0 est élément neutre</u> : 0 est associé par exemple à la coupure : $(\mathbb{Q}^-, \mathbb{Q}^+)$. Alors si $\alpha = (A,B)$ $A + \mathbb{Q}^- = A$ et $B + \mathbb{Q}^+ = B$ car
  * si $a \in A$ $a = a + 0$ donc $a \in A + \mathbb{Q}^-$ $(0 \in \mathbb{Q}^-)$
  * si $x = a + r \in A + \mathbb{Q}^-$ comme $r \leq 0$, $x \leq a$ donc $x \in A$ puisque $a \in A$.
- <u>Tout réel a un opposé</u> puisque si $\alpha = (A,B)$, on vérifie que $(- B, - A)$, où $- A = \{- a \mid a \in A\}$, est également une coupure qui définit un réel α' tel que : $\alpha + \alpha' = (A - B, B - A) = 0$ car si $a - b \in A - B$, $a \leq b$ puisque $a \in A$ et $b \in B$ donc $A - B \subset \mathbb{Q}^-$.

De même $B - A \subset \mathbb{Q}^+$ donc puisque $\alpha + \alpha'$ est une coupure, elle ne peut définir que 0.

Remarquons que l'opposé d'un réel positif est un réel négatif puisque si $0 \in A$ $0 \in -A$.

- Enfin il est facile de vérifier que cette addition prolonge bien celle de $\mathbb{Q}$.

- La compatibilité de l'ordre avec l'addition s'établit sans difficultés.

PRODUIT

La démarche est analogue mais compliquée par le fait qu'il faut tenir compte du signe : ceci est naturel puisqu'en multipliant une inégalité par un nombre négatif on en change le sens.

Le plus rapide est alors de définir :

1° Le produit de deux réels <u>positifs</u>

2° Le produit d'un réel $\alpha > 0$ avec un réel $\alpha' < 0$ par $\alpha \times \alpha' =$ **opp** $(\alpha \times \text{opp}(\alpha))$

3° Le produit de deux réels négatifs par :

$\alpha \times \alpha' = (\text{opp } \alpha) \times (\text{opp } \alpha')$

Soient donc $\alpha = (A,B)$ et $\alpha' = (A',B')$ deux coupures <u>positives</u> : $\mathbb{Q}^- \subset A$ et $\mathbb{Q}^- \subset A'$ (donc $B \subset \mathbb{Q}^+$ et $B' \subset \mathbb{Q}^+$).

Posons $A'' = \mathbb{Q}^- \cup \{a'' = a \,.\, a' \mid a \in A \cap \mathbb{Q}^+ \text{ et } a' \in A' \cap \mathbb{Q}^+\}$

$B'' = \{b'' = b \,.\, b' \mid b \in B,\ b' \in B'\}$. (donc $B'' \subset \mathbb{Q}^+$).

On vérifie que $\alpha'' = (A'',B'')$ constitue une coupure et on note $\alpha'' = \alpha \times a'$.

i) Soit $a'' \in A''$ et $x \in \mathbb{Q}$, avec $x \leq a''$ alors ou bien $x \in \mathbb{Q}^-$ donc $x \in A''$ ou bien $x \in \mathbb{Q}^+$ donc aussi a'' qui s'écrit $a'' = a \times a'$ avec $a \in A$ $(a \geq 0)$

$a' \in A'$ $(a' \geq 0)$ **Alors**

puisque $0 \leq x \leq a''$ on peut écrire $x = ka''$ avec $0 \leq k \leq 1$, soit $x = ka \,.\, a'$ et $0 \leq ka \leq a$ donc $ka \in A$ et $x \in A''$.

ii) identique

iii) a) Soit $a'' \in A''$ et $b'' \in B''$ alors :

- ou bien $a'' \in \mathbb{Q}^-$ et comme $b'' \geq 0$, $a'' \leq b''$
- ou bien $a'' \in \mathbb{Q}^+$ et $a'' = a.a'$ avec $0 \leq a \leq b$

$0 \leq a' \leq b'$

donc $0 \leq a \,.\, a' \leq b \,.\, b'$ soit $a'' \leq b''$.

b) Soit $\epsilon \in \mathbb{Q}^+_*$.

Choisissons un élément $m_0 > 0$ dans B'. Alors $\forall a' \in A'$ $a' \leq m$.

En prenant $\epsilon_1 = \frac{\epsilon}{2\,m}$ il existe $a \in A$ et $b \in B$ tels que $b - a < \frac{\epsilon}{2\,m}$. Et on peut choisir $a \geq 0$ puisque si l'inégalité est vraie pour un $a \leqslant 0$, elle est a fortiori vraie pour un $a \geq 0$ et que $A \cap B^+ \neq \emptyset$.

Posons alors $\epsilon_2 = \frac{\epsilon}{2b}$, il existe $a' \in A'$ $(a' \geq 0)$ et $b \in B'$ tels que $b' - a' < \frac{\epsilon}{2b}$.

Formons $b'' = b \, . \, b' \in B''$ et $a'' = aa' \in A''$.

On aura :

$b'' - a'' = bb' - aa' = b(b' - a') + a(b - a)$

$b'' - a'' \leq b \times \frac{\epsilon}{2b} + m \times \frac{\epsilon}{2m} = \epsilon$

Les propriétés classiques du produit s'établissent plus ou moins laborieusement de manière analogue au cas de l'addition.

Puis, toujours par le même genre de méthode, on établit :

1) l'existence de racines carrées

2) que $\mathbb{R}$ est bien "maximal" c'est-à-dire que toute coupure dans $\mathbb{R}$ encadre un nombre réel et ne permet donc plus de définir un nouveau nombre.

Signalons en guise de conclusion que ce procédé convient parcequ'il s'agit de compléter un corps totalement ordonné alors que c'est la notion de structure uniforme qui se cache sous les suites de Cauchy (i.e tous les points de $\mathbb{Q}$ ont des voisinages du "même ordre de grandeur".)

ANNEXE 3

EXEMPLE D'UNE SUITE DE CAUCHY DE RATIONNELS NON CONVERGENTE DANS $\mathbb{Q}$.

On considère la suite $U : \mathbb{N}^* \to \mathbb{Q}$ avec $U_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots\cdots + \frac{1}{n!}$

$$n \mapsto U_n$$

1) Montrons tout d'abord que cette suite rationnelle est une suite de Cauchy

a) $\forall n \in \mathbb{N}$ et $\forall\ p \in \mathbb{N} - \{0,1\}$: $\dfrac{1}{(n+2)(n+3)\cdots(n+p)} < \dfrac{1}{(n+1)^{p-1}}$.

En effet, $\forall i \geq 2$, $n + i > n + 1$.
D'où $\dfrac{1}{n+i} < \dfrac{1}{n+1}$ et en multipliant membre à membre ces inégalités pour $i = 2,3\ldots p$ on obtient bien celle qui est demandée.

b) Posant $m = n + k$ avec $k \in \mathbb{N}^*$ montrons que $U_m - U_n < \dfrac{1}{n - n!}$. En effet,

$$U_m - U_n = U_{n+k} - U_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\cdots + \frac{1}{(n+k)!} =$$

$$\frac{1}{(n+1)!}\left[1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \cdots\cdots + \frac{1}{(n+2)\cdots(n+k)}\right]$$

et le deuxième facteur de ce produit, compte tenu du a) qui précède est inférieur à : $1 + \dfrac{1}{n+1} + \dfrac{1}{(n+1)^2} + \cdots\cdots + \dfrac{1}{(n+1)^{k-1}}$.

Il en résulte que

$$U_m - U_n < \frac{1}{(n+1)!}\ \frac{1 - \frac{1}{(n+1)^k}}{1 - \frac{1}{n+1}}$$

en considérant la somme comme celle des termes d'une suite géométrique de raison $\dfrac{1}{n+1}$.

Par suite $U_m - U_n < \frac{1}{nn!} \left(1 - \frac{1}{(n+1)^k}\right) < \frac{1}{nn!}$

c) On en déduit que U_n est de Cauchy. En effet, il s'agit de prouver pour celà que $(\forall\ \varepsilon \in \mathbb{Q}^*_+,\ \exists\ \eta(\varepsilon) \in \mathbb{N}^* \mid \forall (m,n) \in \mathbb{N}^{*2},\ m = n + k \text{ et } n > \eta(\varepsilon) \Rightarrow U_m - U_n < \varepsilon)$.

Dans la dernière inégalité on n'a pas besoin de valeur absolue car $m > n$ implique évidemment $U_m > U_n$.

Or d'après b) $U_m - U_n < \frac{1}{nn!}$ et $U_m - U_n$ sera donc inférieur à ε pourvu que $\frac{1}{nn!} < \varepsilon$.

Il suffit pour cela de prendre n supérieur à $\eta(\varepsilon)$ ou $\eta(\varepsilon)$ est le plus petit entier vérifiant $\frac{1}{n(\varepsilon)\ n(\varepsilon)!} < \varepsilon$ (ce qui est possible car l'inégalité équivaut à :

$$\eta(\varepsilon)\ .\ \eta(\varepsilon)! > \frac{1}{\varepsilon}$$ et nn! est une fonction croissante de n).

A titre d'application numérique on pourra vérifier que pour $\varepsilon = 10^{-3}$, $\eta(\varepsilon) = 6$.

2° <u>Montrons maintenant que la suite U_n ne peut converger sur Q.</u>

<u>1ère méthode</u> :

a) Montrons que, sous réserve d'existence de cette limite, $\lim\limits_{k \to \infty} \left(\frac{1}{(p+1)!} + \frac{1}{(p+2)!} + \dots\dots + \frac{1}{(p+k)!}\right)$ est inférieur ou égale à $\frac{1}{pp!}$ (p désigne un élément fini de $\mathbb{N}^*$ et k une variable dans $\mathbb{N}^*$)

Aux notations près, d'après un calcul fait au 1° b) :

$$\frac{1}{(p+1)!} + \frac{1}{(p+2)!} + \dots\dots + \frac{1}{(p+k)!} < \frac{1}{pp!}$$

$$\text{D'où } \lim_{k \to \infty} \left(\frac{1}{(p+1)!} + \frac{1}{(p+2)!} + \dots\dots\dots + \frac{1}{(p+k)!}\right) \leq \frac{1}{pp!}$$

b) Montrons de plus que si U_n admet une limite l, celle-ci est comprise entre 2,5 et 2,75. En effet ,

$U_n = U_2 + \frac{1}{3!} + \frac{1}{4!} + \dots\ \frac{1}{(2+k)!}$ avec $n = 2 + k$.

D'où $l = \lim\limits_{k \to +\infty} U_m = 2,5 + \lim\limits_{k \to +\infty} (\ldots) \leq 2,5 + \frac{1}{pp!} = 2,5 + \frac{1}{4} = 2,75.$
(avec $p = 2$)

Par ailleurs $l > U_2 = 2,5$ est évident.

Donc $2,5 < l \leq 2,75$

Montrons enfin, par l'absurde que l ne peut être un rationnel.
Supposons que $l = \frac{p}{q}$ avec $p \in N$ et $q \in N^*$. Pour $n > q$, $0 < U_n - U_q < \frac{1}{qq!}$
ce qui équivaut à $U_q < U_n < U_q + \frac{1}{qq!}$ et il en résulte, en faisant tendre n vers $+\infty$ que $U_q < \frac{p}{q} \leq U_q + \frac{1}{qq!}$. Cet encochement équivaut à
$U_q \cdot q! < p \cdot (q - 1)! \leq U_q \cdot q! + \frac{1}{q} \Leftrightarrow 0 < p(q - 1)! - U_q q! \leq \frac{1}{q}$.
Puisque $p(q - 1)! - U_q q!$ est un élément de $\mathbf{N}$ il en résulte que $p(q - 1)! - U_q q! = 1$ ce qui est compatible avec l'encochement précédent que si $q = 1$, auquel cas $l = p \in \mathbf{N}$ ce qui est en contradiction avec le fait que $2,5 < l \leq 2,75$.
(On obtiendrait d'ailleurs $p = 3$).

<u>$2^{ème}$ méthode</u>

Posons $r_n = u_n + \frac{1}{n!}$. Si la suite u_n a une limite (rationnelle) la suite r_n a la même limite. Ce sont d'ailleurs deux suites adjacentes puisque :

- r_n décroit $(r_n - r_{n+1} = \frac{1}{n!}(1 - \frac{2}{n+1}) > 0)$
- u_n croit
- $\forall n$, $r_n \leq u_n$ et $r_n - u_n = \frac{1}{n!} \to 0$.

Si ces deux suites admettaient la limite rationnelle $\frac{p}{q}$ on aurait donc $\forall n \in \mathbf{N}$, $u_n < \frac{p}{q} < r_n$. En particulier, $u_q < \frac{p}{q} < r_q$ ou encore on multiplie par $q!$:

$$\underbrace{q!\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{q!}\right)}_{A \in N} < p\,(q-1)! < \underbrace{q!\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{q!}\right)}_{A} \underbrace{+\,1}_{+1}$$

L'entier $p(q - 1)!$ devrait donc être compris strictement entre les deux entiers consécutifs A et $A + 1$.

Signalons enfin qu'un exemple, plus simple, est constitué par la suite $v_n = 1 + \frac{1}{10} + \frac{1}{10^4} + \ldots + \frac{1}{10^{n^2}}$ mais, si les calculs sont plus simples cette suite n'a pas l'importance mathématique de la suite u_n.