Structures des nombres

I Nature et écriture des nombres

1) Les entiers naturels

Leur ensemble, dans le système positionnel décimal est :

$$\mathbb{N} = \{0\,;1\,;2\,;3\,;4\,;5\,;6\,;7\,;8\,;9;10\,;\dots\}$$

Dans le système binaire, on dit en base 2, il devient :

$$\mathbb{N} = \{0\,;1\,;10\,;11\,;100\,;101\,;110\,;111\,;1000\,;1001;1010\,;\dots\}$$

Dans ce système positionnel , la colonne de droite reste la colonne des unités, celle venant en premier à gauche, celle des « paquets de 2 » et non plus de 10 (on pourrait dire des deuxaines par analogie avec les dixaines, la suivante celle des « quartaines » puis des « huitaines ». Ainsi, l'écriture 1001 en base 2 se traduit en base dix par le nombre :

$$\overline{1001}^2 = 1 \times 8 + 0 \times 4 + 0 \times 2 + 1 \times 1$$

Soit :

$$\overline{1001}^2 = 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

L'écriture d'un nombre en base 2 est donc une décomposition de ce nombre sur les puissances de 2, qui sont :

$$2^0 = 1\,,2^1 = 2\,,2^2 = 4\,,2^3 = 8\,,2^4 = 16\,,2^5 = 32\,,2^6 = 64\,,2^7 = 128\,,2^8 = 256\,,2^9 = 512\,,\dots$$

A contrario, le nombre 1001 écrit en base 10, s'écrit ainsi en base 2 :

$$1001 = 512 + 256 + 128 + 64 + 32 + 8 + 1$$

$$1001 =$$

$$1 \times 2^9 + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$1001 = \overline{111110101}^2$$

2) Les entiers relatifs

Leur ensemble, appelé symétrisé de $\mathbb{N}$ s'écrit :

$$\mathbb{Z} = \{\ldots ; -2;\ -1\ ;\ 0\ ;\ 1\ ;\ 2\ ;\ \ldots\}$$

3) Les décimaux

Leur ensemble est :

$$\mathbb{D} = \left\{\frac{\mathrm{p}}{10^{\mathrm{n}}}\ :\quad \mathrm{p} \in \mathbb{Z}\,,\mathrm{n} \in \mathbb{N}\right\}$$

Ils peuvent s'écrire dans le système positionnel en faisant apparaître éventuellement des chiffres appelés **décimales** à droite de la colonne des unités. Ainsi :

$$13{,}451 = \frac{13\,451}{10^3}$$

$$-3 = \frac{-3}{10^0}$$

Ils contiennent donc les entiers relatifs

4) Les quotients d'entiers ou nombres rationnels

Leur ensemble est :

$$\mathbb{Q} = \left\{\frac{\mathrm{p}}{\mathrm{n}}\ :\quad \mathrm{p} \in \mathbb{Z}\,,\mathrm{n} \in \mathbb{N}^*\right\}$$

Ils peuvent s'écrire dans le système positionnel en faisant apparaître éventuellement des chiffres appelés **décimales** en nombre éventuellement infini à droite de la colonne des unités. Cette représentation est appelée **développement décimal**. Ainsi :

$$\frac{-1}{3} = -0{,}33\hat{3}\ \ldots.$$

le chapeau sur le 3 indiquant qu'il est répété à l'infini, la partie sous le chapeau étant appelée **période**.

$$\frac{15}{7} = 2{,}142857\ \overbrace{142857}\ \ldots.$$

Tous les nombres rationnels sont des nombres dont le développement décimal présente une répétition périodique de ses décimales.

Inversement, tout nombre formé par un entier ,suivi après la virgule d'un nombre fini ou infini de décimales présentant une répétition périodique, est le développement décimal d'un nombre rationnel. Voyons quelques exemples :

Partons de : $x = 0{,}18\ \widehat{18}\ \ldots$ et décalons la virgule de deux rangs vers la droite en le multipliant par 100. On a :

$$100\,x = 18,\widehat{18}\ \ldots$$

Soit :

$$100\,x = 18 + x$$

$$99\ x = 18$$

Finalement :

$$0{,}18\ \widehat{18}\ \ldots = \frac{18}{99} = \frac{2}{11}$$

De même :

$$0{,}253\ \widehat{253}\ \ldots = \frac{253}{999}$$

$$0{,}27140\ \widehat{27140}\ \ldots = \frac{27140}{99999}$$

Voyons un peu plus compliqué, encore que !!

$$4{,}2318\ \widehat{18}\ \ldots = 4{,}23 + \frac{0{,}18\ \widehat{18}\ \ldots}{100} = \frac{423}{100} + \frac{2}{11} \times \frac{1}{100} = \frac{423 \times 11 + 2}{1100} = \frac{4655}{1100} = \frac{931}{220}$$

Quelques bizarreries cependant concernant le développement décimal. Il n'est pas forcément unique, comme le montrent ces exemples :

$$1 = 1{,}0\hat{0}\ \ldots = 0{,}9\hat{9}\ \ldots$$

$$2{,}3 = 2{,}30\hat{0}\ \ldots = 2{,}29\hat{9}\ \ldots$$

5) Les nombres réels

Le développement décimal d'un nombre rationnel invite à imaginer des nombres formés d'un entier relatif, suivi après la virgule de décimales en nombre infini, mais sans répétition périodique. Ainsi :

$$0{,}10\ 100\ 1000\ 10000\ \ldots$$

où il est convenu d'ajouter la puissance de dix supérieure à chaque fois

$$0{,}123456789101112131415\ \ldots$$

où il est convenu d'ajouter l'entier naturel supérieur à chaque fois

Ces nombres seront qualifiés d'**irrationnels.**

On constate tout de suite une propriété essentielle. Aussi proche soit on d'un nombre rationnel, il existe un nombre irrationnel et vice versa. Prenons en effet le rationnel $2{,}341\ \widehat{41}$ … Pour trouver un irrationnel qui lui soit proche à moins de $0{,}001$, il suffit de considérer : $2{,}341\ 10\ 100\ 1000$ … autrement dit de remplacer ses décimales à partir du quatrième rang par une suite non périodique quelconque de décimales.

L'ensemble des nombres réels est alors l'union de l'ensemble des rationnels et de l'ensemble des irrationnels, noté :

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

Propriétés spécifiques des irrationnels :

A la différence des autres ensembles de nombre stables pour les opérations d'addition et de multiplication, nous avons :

La somme de deux irrationnels peut être soit un rationnel, soit un irrationnel, comme le montrent ces exemples :

$$0{,}10\ 100\ 1000\ 10000\ \ldots + 0{,}01\ 011\ 0111\ 01111\ \ldots = 0{,}111\hat{1}\ \ldots . = \frac{1}{9} \in \mathbb{Q}$$

$$0{,}10\ 100\ 1000\ 10000\ \ldots + 0{,}10\ 100\ 1000\ 10000\ \ldots = 0{,}20\ 200\ 2000\ 20000\ \ldots \in \mathbb{I}$$

En revanche, **la somme (ou la différence) d'un irrationnel et d'un rationnel est toujours un irrationnel**. Prouvons-le par l'absurde.

Soit $(r, q) \in \mathbb{I} \times \mathbb{Q}$, posons : $q' = r + q$ et supposons $q' \in \mathbb{Q}$ alors $r = q' - q$ donc $r \in \mathbb{Q}$, absurde

Le produit de deux irrationnels peut être soit un rationnel, soit un irrationnel, comme le montrent ces exemples :

Anticipant que $\sqrt{2} \in \mathbb{I}$, $\sqrt{3} \in \mathbb{I}$, $\sqrt{6} \in \mathbb{I}$ nous avons :

$$\sqrt{2} \times \sqrt{2} = 2 \in \mathbb{Q}$$

$$\sqrt{2} \times \sqrt{3} = \sqrt{6} \in \mathbb{I}$$

En revanche, **le produit d'un irrationnel par un rationnel est toujours un irrationnel**. Prouvons-le par l'absurde.

Soit $(r, q) \in \mathbb{I} \times \mathbb{Q}$, posons : $q' = r \times q$ et supposons $q' \in \mathbb{Q}$ alors $r = q' \div q$ donc $r \in \mathbb{Q}$, absurde

De même, **le quotient d'un irrationnel par un rationnel ou d'un rationnel par un irrationnel est toujours un irrationnel**. La preuve est analogue à la précédente.

Retenons que vis-à-vis des quatre opérations de base les rationnels restent dans une même famille, ce qui va amener à la notion de corps vue après, tandis que les irrationnels imposent aux rationnels leur nature dans les opérations, et qu'entre eux, il n'y a pas de règle.

Nature irrationnelle des racines des nombres premiers :

L**a racine carrée d'un nombre premier est un nombre irrationnel**

Commençons par voir ce qu'il en est pour les deux premiers nombres premiers qui sont 2 et 3.

Etablissons pour cela deux résultats préliminaires avec des moyens élémentaires, avant de les généraliser ensuite :

$\forall \mathbf{n} \in \mathbb{N}$: **2 divise $\mathbf{n^2} \Rightarrow$ 2 divise n**
$\forall \mathbf{n} \in \mathbb{N}$: **3 divise $\mathbf{n^2} \Rightarrow$ 3 divise n**

Preuve de : 2 divise $n^2 \Rightarrow$ 2 divise n :

Soit donc un entier naturel n . Supposons 2 divise n^2 alors, par disjonction de cas selon les restes possibles de la division de n par 2 :

1er cas : n est pair soit $n = 2\,m$, $m \in \mathbb{N}$

$n^2 = 4\,m^2$ donc 2 divise n^2

2ème cas : n est impair soit $n = 2\,m + 1$, $m \in \mathbb{N}$

$n^2 = (2\,m + 1)^2 = 4\,m^2 + 4\,m + 1$ donc 2 ne divise pas n^2

Le premier cas est donc le seul cas possible et donc 2 divise n.

Preuve de : 3 divise $n^2 \Rightarrow 3$ divise n :

Soit donc un entier naturel n . Supposons 3 divise n^2 alors, par disjonction de cas selon les restes possibles de la division de n par 3 :

1er cas : $n = 3m , m \in \mathbb{N}$

$n^2 = 9m^2$ donc 3 divise n^2

2ème cas : $n = 3m + 1 , m \in \mathbb{N}$

$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1$ donc 3 ne divise pas n^2

3ème cas : $n = 3m + 2 , m \in \mathbb{N}$

$n^2 = (3m + 2)^2 = 9m^2 + 12m + 4$ donc 3 ne divise pas n^2

Le premier cas est donc le seul cas possible et donc 3 divise n

Généralisation pour un nombre premier p :

$$\forall \mathbf{n} \in \mathbb{N} : \quad \mathbf{p \text{ divise } n^2 \Rightarrow p \text{ divise } n}$$

Preuve :

Nous utiliserons un résultat qui est le suivant et qui sera démontré ultérieurement :

Soit p un nombre premier qui divise un produit de deux entiers naturels $n \times m$ alors p divise n ou p divise m.

On en déduit que si p divise n^2 alors il divise le produit $n \times n$ donc divise n

Nous pouvons alors démontrer que la racine carrée d'un nombre premier est un irrationnel en procédant par l'absurde.

Soit donc p un nombre premier. Supposons $\sqrt{p}$ rationnel, alors il existe deux entiers naturels non nuls et premiers entre eux (sans diviseur commun autre que 1) n t et m tels que :

$$p = \frac{n}{m} \times \frac{n}{m}$$

soit :

$$p \times m^2 = n^2$$

donc p divise n^2 , par conséquent, il divise n, donc il existe un entier naturel non nul q tels que : $n = p \times q$ d'où :

$$p \times m^2 = p^2 \times q^2$$

en simplifiant par p :

$$m^2 = p \times q^2$$

donc p divise m^2 , par conséquent, il divise m ce qui est contradictoire car n et m n'ont pas de diviseurs communs.

De façon plus générale, considérons la décomposition, qui est unique, d'un nombre entier naturel non nul quelconque n, en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \, p_2^{\alpha_2} \dots \, p_m^{\alpha_m}$$

si un seul des α_i est impair, alors $\sqrt{n}$ est un irrationnel. Exemple :

$$\sqrt{2^3 \times 7} \in \mathbb{I}$$

II Propriétés des opérations sur les nombres

On a défini en Mathématiques, pour les besoins de l'idéalisation de la réalité perçue, des objets géométriques comme des points et des ensembles qui leur sont rattachés, segments, droites, plans, courbes, etc. Le besoin de mesurer de tels objets a motivé l'introduction de nombres et défini une logique d'opération. Ainsi, un segment de 2 cm mis bout à bout avec un segment de 3 cm est un segment de 2 + 3 = 5 cm. L'addition des nombres est donc un procédé intuitif, mais il existe différents systèmes pour représenter les nombres : le système décimal qui est le plus employé par les humains, mais aussi le système binaire qui est celui employé par les ordinateurs, le système romain étant tombé en désuétude par sa trop grande complexité.

Quelque soit le système employé, nous pouvons dégager des propriétés évidentes pour les opérations élémentaires que sont l'addition et la multiplication, la soustraction et la division étant rattachée à ces dernières. Ces propriétés pour l'ensemble le plus complet qui est l'ensemble des nombres réels (si on omet de parler de l'ensemble des nombres complexes) sont les suivantes :

1) La commutativité de l'addition

$$\forall\,(x\,,y\,)\in\mathbb{R}^2\ :\quad x+y=y+x$$

2) L'associativité de l'addition

$$\forall\,(x\,,y\,,z)\in\mathbb{R}^2\ :\quad (x+y)+z=(x+y+z)$$

Ces deux premières propriétés sont à la source de l'écriture sans parenthèse $x+y+z$ qui permet d'additionner en premier n'importe lequel des deux termes sur les trois.

3) L'existence d'un élément neutre

$$\forall\, x \in \mathbb{R} \ : \quad x + 0 = 0 + x = x$$

Autrement dit, il y a un nombre qui n'a pas d'effet dans l'addition, c'est le 0. On l'appelle **élément neutre additif**.

4) <u>L'existence d'un symétrique pour tout nombre</u>

$$\forall\, x \in \mathbb{R} \ : \quad x + (-x) = (-x) + x = 0$$

Autrement dit, pour tout nombre, il y a un nombre qui ajouté à lui donne l'élément neutre. Ce nombre est en fait son opposé.

Si on ne considère que ces quatre propriétés, on dit que l'ensemble $\mathbb{R}$ des nombres réels forme un **groupe commutatif** pour l'addition. Nous écrirons pour simplifier :

$$(\mathbb{R}, +) : \ \mathrm{C\ A\ N\ S}$$

5) <u>La commutativité de la multiplication</u>

$$\forall\, (x\,, y\,) \in \mathbb{R}^2 \ : \quad x \times y = y \times x$$

6) <u>L'associativité de la multiplication</u>

$$\forall\, (x\,, y\,, z) \in \mathbb{R}^2 \ : \quad (x \times y) \times z = x \times (y \times z)$$

Ces deux premières propriétés sont à la source de l'écriture sans parenthèse $x \times y \times z$ qui permet de multiplier en premier n'importe lequel des deux termes sur les trois.

7) <u>L'existence d'un élément neutre</u>

$$\forall\, x \in \mathbb{R} \ : \quad x \times 1 = 1 \times x = x$$

Autrement dit, il y a un nombre qui n'a pas d'effet dans la multiplication, c'est le 1. On l'appelle **élément neutre multiplicatif**.

8) <u>L'existence d'un symétrique pour tout nombre non nul</u>

$$\forall\, x \in \mathbb{R} \ : \quad x \times \frac{1}{x} = \frac{1}{x} \times x = 1$$

Autrement dit, pour tout nombre, il y a un nombre qui, multiplié à lui, donne l'élément neutre. Ce nombre est en fait son **inverse**.

Nous écrirons pour simplifier :

$$(\mathbb{R},\times) : \ C\ A\ N\ S^*$$

Noter que l'ensemble $\mathbb{R}$ des nombres réels ne forme pas un groupe commutatif pour la multiplication car l'élément neutre additif 0 n'a pas d'inverse.

9) <u>La distributivité de la multiplication par rapport à l'addition</u>

$$\forall\,(x\,,y\,,z)\in\mathbb{R}^2\ :\quad x\times(y+z)=(x\times y)+(x\times z)$$

Si on considère toutes ces propriétés, on dit que l'ensemble $\mathbb{R}$ des nombres réels forme un **corps commutatif** pour l'addition et la multiplication. Nous écrirons pour simplifier :

$$(\mathbb{R},+,\times):\ C\ A\ N\ S\ C\ A\ N\ S^*\ D$$

Voyons alors la structure des sous ensembles notables de $\mathbb{R}$:

L'ensemble des entiers naturels $\mathbb{N}$:

$$(\mathbb{N},+,\times):\ C\ A\ N\ \ C\ A\ N\ \ D$$

$(\mathbb{N},+)$ n'est pas un groupe commutatif car le nombre 1 par exemple n'a pas d'opposé dans $\mathbb{N}$. De plus, le nombre 2, par exemple, n'a pas d'inverse dans $\mathbb{N}$.

L'ensemble des entiers relatifs $\mathbb{Z}$:

$$(\mathbb{Z},+,\times):\ C\ A\ N\ \ S\ C\ A\ N\ \ D$$

$(\mathbb{Z},+)$ est bien un groupe commutatif cette fois-ci, car tout nombre y a un opposé, ce qui fait qualifier cet ensemble de « symétrisé de $\mathbb{N}$ ». Mais le nombre 2, par exemple, n'a pas d'inverse dans $\mathbb{Z}$, ce qui fait que cet ensemble n'est pas un corps.

On qualifie toutefois sa structure **d'anneau commutatif**.

L'ensemble des décimaux $\mathbb{D}$:

$$(\mathbb{D},+,\times):\ C\ A\ N\ \ S\ C\ A\ N\ \ D$$

$(\mathbb{D},+)$ est encore un groupe commutatif, mais le nombre 3, par exemple, n'a pas d'inverse dans $\mathbb{D}$, ce qui fait que cet ensemble n'est pas un corps. C'est cependant encore un **anneau commutatif**.

L'ensemble des rationnels (quotients d'entiers) $\mathbb{Q}$:

$$(\mathbb{Q}\,,+,\times):\ C\ A\ N\ \ S\ C\ A\ N\ S^*D$$

$\mathbb{Q}$ est un corps commutatif tout comme $\mathbb{R}$

Nous voyons ainsi qu'à partir de l'ensemble des entiers naturels ont été définis des ensembles plus grands qui ont à chaque fois une propriété supplémentaire.

Notons que $\mathbb{R}$ et $\mathbb{Q}$ ont une même structure de corps commutatif mais $\mathbb{R}$ a une propriété supplémentaire essentielle sur laquelle nous reviendrons dans un fichier ultérieur : Toute suite de Cauchy y est convergente, ce qui en fera un corps qualifié de complet. $\mathbb{R}$ est d'ailleurs appelé « complété de $\mathbb{Q}$ ».

III D'autres exemples de corps à nombre d'éléments fini

Considérons une forme d'addition qui peut sembler étrange a priori, mais qui présente de nombreuses applications, l'addition modulo un nombre donné.

1) Addition modulo 2

Prenons un nombre entier naturel quelconque n et portons-le sur un axe gradué. En reculant de deux divisions entières de façon à s'approcher le plus près de 0, nous parvenons en 0 ou 1, c'est-à-dire, le reste de la division de n par 2. Ce reste est la plus petite valeur de n modulo 2.

Ainsi la plus petite valeur de 44 modulo 2 est 0 et de 45 modulo 2 est 1.

De façon générale, la plus petite valeur d'un nombre pair modulo 2 est 0 et d'un nombre impair 1.

Nous sommes alors amenés à définir une forme d'addition un peu spéciale, dans laquelle on ne fait apparaître que les plus petites valeurs modulo 2. Ainsi :

La plus petite valeur modulo 2 de $1 + 1 = 2$ étant 0, nous posons :

$$1 \oplus 1 = 0$$

Nous pouvons ainsi considérer l'ensemble à deux éléments suivants :

$$\mathbb{K}_2 = \{0\,;1\}$$

et définir sur cet ensemble une opération que nous qualifierons d'addition $\oplus$ et une de multiplication $\otimes$ par les tables suivantes :

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0

1	0	1

On peut alors sans peine vérifier que $(\mathbb{K}_2, \oplus, \otimes)$ est un corps commutatif

Noter que l'opposé de 1 est 1 et son inverse est 1 également.

2) Addition modulo 3

Reprenons l'approche précédente, mais en faisant des sauts de 3. Nous avons trois plus petites valeurs possibles modulo 3 qui sont les restes possibles de la division euclidienne de n par 3 à savoir, 0, 1, 2.

Notant, par exemple, que la plus petite valeur de $2 + 2 = 4$ modulo 3 est 1, nous pouvons considérer l'ensemble à trois éléments suivants :

$$\mathbb{K}_3 = \{0 ; 1 ; 2\}$$

et définir sur cet ensemble une opération $\oplus$ et une $\otimes$ par les tables suivantes :

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

On peut alors sans peine vérifier que $(\mathbb{K}_3, \oplus, \otimes)$ est un corps commutatif

3) Addition modulo 4

Selon la même logique que précédemment, on définit sur :

$$\mathbb{K}_4 = \{0 ; 1 ; 2 ; 3\}$$

Les opérations suivantes

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

En revanche $(\mathbb{K}_4, \oplus, \otimes)$ n'est un corps commutatif mais seulement un anneau commutatif.

En effet, on constate que 2 n'a pas d'inverse. Cela vient du fait que : $2 \otimes 2 = 0$