Les Nombres

A.Balan

4 août 2017

1 Les nombres entiers naturels

1.1 Définition

On appelle ici nombres entiers naturels **N** les cardinaux des ensembles finis [J]. En particulier 0 est le cardinal de l'ensemble vide $\emptyset$, 1 est le cardinal des singletons. Les nombres entiers possèdent une structure de double monoide qui provient, sur les ensembles, à prendre la réunion de deux ensembles disjoints pour la loi interne somme $a+b$, et leur produit cartésien pour la loi interne multiplication $a.b$, ces lois ayant une propriété de distributivité entre elles qui peut se démontrer par récurrence $(a+b).c = (a.c) + (b.c)$; 0 est élément absorbant et 1 est élément neutre pour la multiplication. Il existe un ordre sur les nombres entiers naturels, résultant de l'inclusion des ensembles.

1.2 Le théorème fondamental de l'arithmétique

La division de n par m n'existe que si $n = k.m$, elle est par définition égale à k. Tout nombre entier naturel est divisible par 1 et lui-même. Les nombres premiers $\mathcal{P}$ sont ceux qui ne sont divisibles que par 1 et eux-mêmes. Par convention 1 n'est pas premier, et donc le premier nombre premier est 2 ; les nombres entiers naturels divisibles par 2 sont dits pairs, et les autres impairs.

Le théorème fondamental de l'arithmétique est le suivant :

Théorème :

Tout nombre entier $n \in \mathbf{N}$, $n \geq 2$, peut s'écrire de façon unique sous la forme d'un produit fini :

$$n = \prod_i p_i^{\alpha_i(n)}$$

le produit portant sur les nombres premiers p_i mis à une certaine puissance $\alpha_i(n)$.

Démonstration :

par récurrence sur n, $P(2)$: 2 est premier et si n est premier alors $P(n)$. Si n n'est pas premier, alors $n = ab$, avec a,b plus petits que n ; on peut donc appliquer $P(a)$,$P(b)$ et donc $n = \prod_i p_i^{\alpha_i(a)+\alpha_i(b)}$. De plus cette écriture est unique car si :

$$\prod_i p_i^{\alpha_i} = \prod_i p_i^{\beta_i}$$

alors si α_j est non nul, p_j divise le produit et donc, on obtient :

$$\prod_{i \neq j} p_i^{\alpha_i} p_j^{\alpha_j - 1} = \prod_{i \neq_j} p_i^{\alpha_i} p_j^{\beta_j - 1}$$

et on applique la propriété de récurrence à n/p_j. D'où P(n).

□

On a aussi (exercice):

$$n.m = \prod_i p_i^{\alpha_i(n)+\alpha_i(m)}$$

Le pgcd de deux nombres est le plus grand commun diviseur de ces nombres, le ppcm est le plus petit commun multiple. On a (exercice) :

$$pgcd(n,m) = \prod_i p_i^{min(\alpha_i(n),\alpha_i(m))}, ppcm(n,m) = \prod_i p_i^{max(\alpha_i(n),\alpha_i(m))}$$

1.3 Conjectures

Il existe de nombreuses conjectures concernant les nombres premiers. La conjecture de Goldbach dit que tout nombre pair est la somme de deux nombres premiers $\forall n \in \mathbf{N} \setminus \{0,1\}, \exists (p,q) \in \mathcal{P}^2, 2n = p + q$. La conjecture des nombres premiers jumeaux dit qu'il existe une infinité de nombres premiers $(p,q) \in \mathcal{P}^2$ tels que leur différence soit deux : $p - q = 2$.

1.4 La division euclidienne

Théorème : Soient la donne de deux entiers naturels n,m avec $n \geq m$, alors on a la division euclidienne suivante :

$$n = km + r$$

avec (k,r) deux entiers et $r < m$, r est appelé le reste de la division euclidienne de n par m. Les deux entiers k,r sont uniques.

Démonstration : par récurrence sur n, si $n = m$, alors $(k,r) = (1,0)$. Si on a $n = km + r$, alors si $r \geq m-2$, on a $n+1 = km + (r+1)$ et si on a $r = m-1$, alors $n+1 = (k+1)m$. Les deux entiers (k,r) sont uniques (exercice).

□

1.5 L'algorithme d'Euclide

Il s'agit dans cet algorithme d'itérer des divisions euclidiennes successives. Au rang a, on a deux entiers $A_a = (r_a,r_{a+1})$; au rang $a+1$, on fait la division euclidienne de r_a par r_{a+1}, ce qui donne (k_{a+2},r_{a+2}) et on définit $A_{a+1} = (r_{a+1},r_{a+2})$. Comme la suite des r_a est strictement décroissante, l'algorithme est fini et on obtient une suite de nombres r_a à partir de deux entiers n,m. L'algorithme d'Euclide donne le $pgcd(n,m)$; en effet, par récurrence on a : $pgcd(r_a,r_{a+1}) = pgcd(r_{a+1},r_{a+2})$ et comme l'algorithme est fini, on a au dernier rang le pgcd.

2 Les nombres entiers relatifs

2.1 Définition

Les nombres entiers relatifs $\mathbf{Z}$ est le groupe de Grothendieck de $\mathbf{N}$, il s'agit en fait d'inverser les entiers pour l'addition :

$$\mathbf{Z} = \{(n,m) \in \mathbf{N}^2 / \sim ; (n,m) \sim (n',m') \quad ssi \quad n + m' = m + n'\}$$

$\mathbf{N}$ s'injecte canoniquement dans $\mathbf{Z}$ par i tel que $i(n) = (n,0)$. Les nombres entiers relatifs possèdent une structure d'anneau, c'est à dire deux opérations, l'une de groupe additif commutatif et une autre de monoide multiplicatif, avec une distributivité. Les nombre entiers relatifs possèdent un ordre total compatible avec l'inclusion i et avec les opérations, et tel que les nombres positifs sont les entiers naturels.

2.2 Les idéaux de Z

Les idéaux de $\mathbf{Z}$ sont des sous-groupes additifs de $\mathbf{Z}$ dont un plus petit élément positif est n, ce sont donc forcément les sous-groupes $n\mathbf{Z}$ car on montre par division euclidienne qu'un élément de l'idéal est forcément multiple de n. On dit que $\mathbf{Z}$ est euclidien donc principal et est, de ce fait, factoriel.

2.3 Les modulos

On dit que a est égal à b modulo c (dans $\mathbf{Z}$) si c divise $a - b$ et on note $a \equiv b \, mod(c)$. Les entiers relatifs égaux modulo c fixé forment une relation d'équivalence compatible avec la structure d'anneau, le quotient par cette relation d'équivalence se note $\mathbf{Z}/c\mathbf{Z}$, il s'agit d'un ensemble à c éléments qui possède

une structure d'anneau commutatif; si $a \equiv b\, mod(c)$ et $d \equiv e\, mod(c)$, alors $a+d \equiv b+e\, mod(c)$ et $ad \equiv be\, mod(c)$; c'est le quotient des anneaux $\mathbf{Z}$ et $c\mathbf{Z}$. Si p est un nombre premier, alors $\mathbf{Z}/p\mathbf{Z}$ est un corps ; en effet la multiplication par a non nul est injective donc bijective car l'ensemble est fini et de ce fait il existe b tel que $ab \equiv 1\, mod(p)$, on note aussi $\mathbf{F}_p$ ce corps.

2.4 Le théorème chinois

Théorème :

Si

$$n = \prod_i p_i^{\alpha_i}$$

alors

$$\mathbf{Z}/n\mathbf{Z} \cong \prod_i (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})$$

Démonstration :

Si $pgcd(n,m) = 1$, alors $\mathbf{Z}/n.m\mathbf{Z} \cong (\mathbf{Z}/n\mathbf{Z}).(\mathbf{Z}/m\mathbf{Z})$. En effet on considère l'application cannonique $\mathbf{Z} \to (\mathbf{Z}/n\mathbf{Z}).(\mathbf{Z}/m\mathbf{Z})$; le noyau est $n.m\mathbf{Z}$ vu que $pgcd(n,m) = 1$ et donc on a une application injective de $\mathbf{Z}/nm\mathbf{Z}$ dans $(\mathbf{Z}/n\mathbf{Z}).(\mathbf{Z}/m\mathbf{Z})$ qui est aussi surjective en comparant les cardinaux, d'où l'isomorphisme.

□

2.5 Le théorème de Bézout

Théorème :

Soient deux entiers n,m, il exite deux entiers relatifs a,b tels que :

$$an + bm = pgcd(n,m)$$

Démonstration :

On montre que la réunion des idéaux $n\mathbf{Z}$ et $m\mathbf{Z}$ est $pgcd(n,m)\mathbf{Z}$. (de même leur intersection est $ppcm(n,m)\mathbf{Z}$.)

□

3 Les nombres rationnels

3.1 Définition

Les nombres rationnels sont le corps $\mathbf{Q}$ des fractions de l'anneau intègre des entiers. On définit cet ensemble :

$$\mathbf{Q} = \{(a,b) \in \mathbf{Z}.\mathbf{Z}^* / \sim ; (a,b) \sim (c,d) \quad ssi \quad ad = bc\}$$

(a,b) est noté a/b ; son inverse, avec a,b non nuls, est b/a.

3.2 L'ordre sur les rationnels

Un ordre est définit sur $\mathbf{Q}$ $a \geq b$ ssi $a - b \geq 0$, les éléments positifs étant ceux pour lesquels a,b sont tous deux positifs ou négatifs. $\mathbf{Q}$ est un corps archimédien, c'est-à-dire que pour tous $a > 0, b > 0$, il existe $n \in \mathbf{N}$ tel que $a < nb$. Tout élément strictement positif se met de façon unique sous la forme n/m, avec n,m dans $\mathbf{N}^*$ et $pgcd(n,m) = 1$.

3.3 La topologie des nombres rationnels

Topologiquement, les rationnels forment un ensemble totalement discontinu au sens où les seuls sous-ensembles connexes sont l'ensemble vide et les singletons.

4 Les nombres réels

4.1 Définition

On considère les suites dites de Cauchy de nombres rationnels, il s'agit des suites $(a_n)_{n \in \mathbf{N}}$ telles que pour tout $\epsilon > 0$, il existe N tel que pour tous $n > N$ et $m > N$, $|a_n - a_m| < \epsilon$. On quotiente alors l'ensemble de ces suites par les suites tendant vers zéro qui forment un idéal maximal pour obtenir le corps des nombres réels $\mathbf{R}$.

4.2 L'ordre sur les réels

Les nombres réels possèdent un ordre qui résulte de l'ordre des rationnels dans la mesure où une suite est dite positive si ses termes sont positifs à partir d'un certain rang. L'ordre ainsi défini est compatible avec les opérations du corps $\mathbf{R}$.

4.3 La topologie des nombres réels

Les intervalles des nombres réels sont des parties connexes. En effet si $]a,b[= A \cup B$ avec A,B des ensembles ouverts non vides alors $]a,(a+b)/2[$ ou $](a+b)/2,b[$ possède la même propriété et par dichotomie on trouve un nombre de $]a,b[$ qui ne peut être dans aucun des ouverts A,B.

5 Les nombres p-adiques

5.1 Définition

Les entiers p-adiques sont définis comme une suite projective. On considère dans le produit infini $\prod_n \mathbf{Z}/p^n\mathbf{Z}$ les suites $(z_n)_{n\in\mathbf{N}^*}$ telles que $z_n \equiv z_m$ modulo p^m si $m < n$. Il s'agit d'un anneau intègre, l'anneau des entiers p-adiques $\mathbf{Z}_p$ dont le corps des fractions est le corps des nombres p-adiques $\mathbf{Q}_p$.

5.2 La topologie des nombres p-adiques

La limite projective qui définit les entiers p-adiques possède une topologie produit qui en fait un ensemble compacte car fermé dans le produit infini de compactes. Les nombres entiers s'injectent densément dans les nombres entiers p-adiques par l'application qui envoie $z \in \mathbf{Z}$ dans la suite stationnaire à partir d'un certain rang des réductions de z modulo p^n. Les nombres p-adiques $\mathbf{Q}_p$ forment un ensemble complet car complété des rationnels pour la valuation p-adique. Les p-adiques forment un ensemble totalement discontinu, chaque élément est sa propre composante connexe.

6 Les nombres non-standards

6.1 Les infinitésimaux

Soit (K,τ_K), un corps topologique non séparé, les infinitésimaux sont les éléments du corps qui sont dans tout voisinage de zéro.

6.2 Les réels non-standards et les p-adiques non-standards

Etant donné un corps (K,τ_K) séparé, il est possible de construire des infinitésimaux. On considère des suites d'éléments $K^{\mathbf{N}}$ que l'on quotiente par un ultrafiltre des entiers. On a $(a_n) = (b_n)$ s'il existe U, élément de l'ultrafiltre $\mathcal{U}$ tel que $a_n = b_n$ pour tout $n \in U$. Les suites convergentes sur $\mathcal{U}$, plus les suites tendant vers l'infinii forment alors un corps topologique. Dans le cas des nombres réels, il s'agit des nombres réels non-standards et dans le cas des p-adiques, ce sont les nombres p-adiques non-standards.

Références

[J] T.Jech, "Set Theory", Springer Verlag, Berlin, 2006.

[E] H.-D. Ebbinghaus, & co, "Numbers", Springer-Verlag, Berlin, 1991.