

Compléments pour le L1.

Dans les livres concernant les mathématiques à l'université, il est rare que les ensembles de nombres usuels soient construits. Dans ce complément, on donne sous forme d'exercices une construction des ensembles \mathbb{Z} , \mathbb{Q} et \mathbb{R} à partir de l'ensemble \mathbb{N} des entiers naturels donné par les axiomes de Peano. On vérifie un certain nombre de propriétés de ces ensembles.

Propriétés de \mathbb{N} .

On se propose de déduire des propriétés usuelles de l'ensemble des entiers naturels \mathbb{N} des axiomes de Peano suivants.

Axiomes de Peano : on postule l'existence d'un triplet $(0, \mathbb{N}, S)$, où \mathbb{N} est un ensemble, 0 un élément particulier de \mathbb{N} et $S : \mathbb{N} \longrightarrow \mathbb{N}$ une application qui vérifient :

- P1 : S est injective.
- P2 : $S(\mathbb{N}) = \mathbb{N} \setminus \{0\} =: \mathbb{N}^*$.
- P3 : Si A est une partie de \mathbb{N} telle que $0 \in A$ et

$$\forall n \in \mathbb{N}, (n \in A) \implies (S(n) \in A),$$

alors $A = \mathbb{N}$.

L'ensemble \mathbb{N} est l'ensemble des entiers naturels, 0 est l'élément zéro, S est l'application "successeur" et P3 est l'axiome de récurrence.

1. Montrer le théorème de récurrence suivant. Soit $\mathcal{P}(n)$ une assertion dépendant de $n \in \mathbb{N}$. Les assertions $(\mathcal{P}(0))$ et $(\forall n \in \mathbb{N}, \mathcal{P}(n) \implies \mathcal{P}(n+1))$ impliquent $(\forall n \in \mathbb{N}, \mathcal{P}(n))$.
2. On montre maintenant le résultat suivant. Soit \mathcal{E} un ensemble non vide, $b \in \mathcal{E}$ et $g : \mathcal{E} \longrightarrow \mathcal{E}$ une application. Il existe une unique application $\phi : \mathbb{N} \longrightarrow \mathcal{E}$ telle que $\phi(0) = b$ et $\phi \circ S = g \circ \phi$.
On considère l'application $h : \mathbb{N} \times \mathcal{E} \longrightarrow \mathbb{N} \times \mathcal{E}$ définie par $h(x, y) = (S(x), g(y))$. On note par \mathcal{F} l'ensemble des parties A de $\mathbb{N} \times \mathcal{E}$ vérifiant $h(A) \subset A$ et $(0, b) \in A$. On pose $G = \bigcap_{A \in \mathcal{F}} A$. Soit \mathcal{U} l'ensemble des $x \in \mathbb{N}$ tels que $G_x := \{y \in \mathcal{E}; (x, y) \in G\}$ soit un singleton. Nous allons montrer que G est le graphe d'une application ϕ qui répond à la question.

- (a) En utilisant le 1., montrer l'unicité de ϕ .

- (b) Vérifier que \mathcal{F} est non vide (donc G est une partie de $\mathbb{N} \times \mathcal{E}$).
- (c) Montrer, en utilisant le 1., que $pr_1(G) = \mathbb{N}$ ($pr_1 : \mathbb{N} \times \mathcal{E} \rightarrow \mathbb{N}$ étant la première projection).
- (d) Soit $c \in \mathcal{C}$ tel que $(0, c) \in G$. Soit $B = (0, b) \cup h(G)$. Montrer que $B \in \mathcal{F}$. En déduire que $(0, c) \in B$. Conclure que $G_0 = \{b\}$ (donc $0 \in \mathcal{U}$).
- (e) Vérifier que $B = G$.
- (f) Pour $x \in \mathcal{U}$, montrer que $G_{S(x)} \neq \emptyset$. Soit $y \in G_{S(x)}$, montrer que $(S(x), y) \in h(G)$. Pour $y_1, y_2 \in G_{S(x)}$, on peut donc trouver x'_1, x'_2, y'_1, y'_2 tels que $(S(x), y_i) = h(x'_i, y'_i)$, pour $i \in \{1; 2\}$. Montrer que $x'_1 = x'_2$. En déduire que $y'_1 = y'_2$. Conclusion ?
- (g) Montrer, en utilisant le 1., que G est un graphe fonctionnel.
- (h) Soit $\phi : \mathbb{N} \rightarrow \mathcal{E}$ l'application de graphe G . Vérifier que ϕ convient.
3. Soit $\psi : \mathcal{D} \rightarrow \mathcal{E}$ et $\tilde{g} : \mathcal{D} \times \mathcal{E} \rightarrow \mathcal{E}$ deux applications. Déduire du 2., qu'il existe une unique application $\tilde{\phi} : \mathcal{D} \times \mathbb{N} \rightarrow \mathcal{E}$ telle que

$$\forall d \in \mathcal{D}, \quad \tilde{\phi}(d, 0) = \psi(d), \quad (1)$$

$$\forall d \in \mathcal{D}, \forall n \in \mathbb{N}, \quad \tilde{\phi}(d, S(n)) = \tilde{g}(d, \tilde{\phi}(d, n)). \quad (2)$$

4. Déduire du résultat précédent qu'il existe une unique application, notée $+$, de \mathbb{N}^2 dans \mathbb{N} vérifiant

$$\forall n \in \mathbb{N}, \quad n + 0 = n, \quad (3)$$

$$\forall p \in \mathbb{N}, \forall q \in \mathbb{N}, \quad p + S(q) = S(p + q). \quad (4)$$

A partir de ce résultat, on vérifie facilement par récurrence que $+$ est associative, commutative et que tout élément est simplifiable. De plus, pour tout $n \in \mathbb{N}$, $S(n) = n + 1$, où $1 := S(0)$.

5. Déduire du 3., qu'il existe une unique application, notée \cdot , de \mathbb{N}^2 dans \mathbb{N} vérifiant

$$\forall n \in \mathbb{N}, \quad n \cdot 0 = 0, \quad (5)$$

$$\forall p \in \mathbb{N}, \forall q \in \mathbb{N}, \quad p \cdot (q + 1) = (p \cdot q) + p. \quad (6)$$

Là aussi, il est facile de déduire de ce résultat les propriétés usuelles de la multiplication (associativité, commutativité, distributivité sur $+$, 1 est élément neutre, tout élément non nul est simplifiable).

6. Déduire du 3., qu'il existe une unique application, appelée exponentiation et notée $(a, b) \mapsto a^b$, de \mathbb{N}^2 dans \mathbb{N} , vérifiant

$$\forall n \in \mathbb{N}, \quad n^0 = 1, \quad (7)$$

$$\forall p \in \mathbb{N}, \forall q \in \mathbb{N}, \quad p^{(q+1)} = (p^q) \cdot p. \quad (8)$$

7. Montrer que la relation binaire “ $a \leq b$ ssi il existe $d \in \mathbb{N}$ tel que $b = a + d$ ” définit un ordre total sur \mathbb{N} .

Construction de l’ensemble des entiers relatifs.

Sur $\mathbb{N}^2 := \mathbb{N} \times \mathbb{N}$, on considère la relation binaire \mathcal{R} définie par : $(a, b)\mathcal{R}(a', b')$ ssi $a + b' = a' + b$.

1. Montrer que \mathcal{R} est une relation d’équivalence. On pose $\mathbb{Z} := \mathbb{N}^2/\mathcal{R}$, c’est l’ensemble des nombres entiers relatifs.
2. Montrer que l’application $\phi : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par $\phi(n) = \mathcal{C}((n, 0))$ (la classe de $(n, 0)$) est injective. \mathbb{N} est donc en bijection avec une partie de \mathbb{Z} . On identifie \mathbb{N} à cette partie.
3. On définit sur \mathbb{Z} l’addition suivante :

$$\forall ((a, b), (a', b')) \in \mathbb{N}^2 \times \mathbb{N}^2, \quad \mathcal{C}((a, b)) + \mathcal{C}((a', b')) := \mathcal{C}((a + a', b + b')).$$

Montrer que cette application est bien définie.

4. Montrer que $(\mathbb{Z}, +)$ est un groupe abélien d’élément neutre $\mathcal{C}((0, 0))$. On note par $-s$ l’opposé de $s \in \mathbb{Z}$.
5. On définit sur \mathbb{Z} la multiplication suivante :

$$\forall ((a, b), (a', b')) \in \mathbb{N}^2 \times \mathbb{N}^2, \quad \mathcal{C}((a, b)) \cdot \mathcal{C}((a', b')) := \mathcal{C}((aa' + bb', ab' + a'b)).$$

Montrer que cette application est bien définie. Montrer qu’elle est associative, commutative, distributive sur l’addition et que $\mathcal{C}((1, 0))$ est son élément neutre. \mathbb{Z} est donc un anneau commutatif.

6. Montrer que la relation binaire “ $a \leq b$ ssi $(-a) + b \in \phi(\mathbb{N})$ ” définit un ordre total sur \mathbb{Z} qui prolonge celui de \mathbb{N} .

Construction de l’ensemble des rationnels.

Sur $\mathbb{Z} \times \mathbb{Z}^*$, on considère la relation binaire \mathcal{R} définie par : $(a, b)\mathcal{R}(a', b')$ ssi $ab' = a'b$.

1. Montrer que \mathcal{R} est une relation d’équivalence. On pose $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\mathcal{R}$, c’est l’ensemble des nombres rationnels.
2. Montrer que l’application $\phi : \mathbb{Z} \longrightarrow \mathbb{Q}$ définie par $\phi(n) = \mathcal{C}((n, 1))$ (la classe de $(n, 1)$) est injective. \mathbb{Z} est donc en bijection avec une partie de \mathbb{Q} . On identifie \mathbb{Z} avec cette partie. On note l’élément $\mathcal{C}((a, b))$ de \mathbb{Q} par a/b . Ainsi, pour $n \in \mathbb{Z}$, $n/1$ représente n vu dans \mathbb{Q} .

3. On définit sur \mathbb{Q} l'addition suivante :

$$\forall ((a, b), (a', b')) \in (\mathbb{Z} \times \mathbb{Z}^*)^2, \quad \frac{a}{b} + \frac{a'}{b'} := \frac{ab' + a'b}{bb'}.$$

Montrer que cette application est bien définie. On note encore par 0 l'élément 0/1.

4. On définit sur \mathbb{Q} la multiplication suivante :

$$\forall ((a, b), (a', b')) \in (\mathbb{Z} \times \mathbb{Z}^*)^2, \quad \frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}.$$

Montrer que cette application est bien définie. On note encore par 1 l'élément 1/1.

5. Montrer que $(\mathbb{Q}, +)$ est un groupe abélien. Montrer que $(\mathbb{Q}, +, \cdot)$ est un anneau commutatif. Vérifier que (\mathbb{Q}^*, \cdot) est un groupe ($\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$).

On a donc construit le corps des nombres rationnels. Il est possible de mettre sur \mathbb{Q} un ordre qui prolonge celui de \mathbb{Z} .

Ordre total sur \mathbb{Q} .

1. Montrer que si $a/b \in \mathbb{Q}$ avec $ab \in \mathbb{N}$ alors, pour tout $(a', b') \in a/b$, on a $a'b' \in \mathbb{N}$. On peut donc définir le sous-ensemble \mathbb{Q}^+ de \mathbb{Q} des rationnels dont un représentant (a, b) vérifie $ab \in \mathbb{N}$. On note $\mathbb{Q}^{+*} := \mathbb{Q}^+ \setminus \{0\}$.
2. Montrer que la relation binaire " $a/b \leq a'/b'$ ssi $a/b - a'/b' \in \mathbb{Q}^+$ " définit un ordre total sur \mathbb{Q} .
3. Vérifier que \mathbb{Q} est archimédien c'est-à-dire que la propriété suivante est vraie.

$$\forall (a, b) \in \mathbb{Q}^{+*} \times \mathbb{Q}, \exists n \in \mathbb{N}; \quad n \cdot a \geq b.$$

4. Vérifier que \mathbb{Q} est partout dense dans \mathbb{Q} c'est-à-dire que la propriété suivante est vraie. Pour tout $(a, b) \in \mathbb{Q}$ avec $a < b$, il existe $c \in \mathbb{Q}$ tel que $a < c < b$.

Bien sûr, on peut définir sur \mathbb{Q} une valeur absolue par $|q| = \max(q, -q)$. Elle prolonge celle de \mathbb{Z} et on a les propriétés suivantes : $|q| = 0 \iff q = 0$, $|qq'| = |q| |q'|$ et $|q+q'| \leq |q| + |q'|$.

Une construction de \mathbb{R} .

Soit \mathcal{S} l'ensemble des suites de rationnels (i.e. $\mathcal{S} = \mathbb{Q}^{\mathbb{N}}$). On note par \mathcal{C} le sous-ensemble de \mathcal{S} formé des suites de Cauchy et par \mathcal{C}_0 le sous-ensemble de \mathcal{C} formé des suites convergent vers 0. On rappelle que \mathcal{S} , muni de l'addition $(u_n)_n + (v_n)_n = (u_n + v_n)_n$, est un groupe abélien dont l'élément neutre est la suite nulle.

1. Montrer que \mathcal{C} muni de la (restriction de la) loi $+$ précédente est un groupe. On dit que c'est un sous-groupe de \mathcal{S} . Montrer que \mathcal{C}_0 est aussi un sous-groupe de \mathcal{S} .
2. Soit \mathcal{R} la relation binaire sur \mathcal{C} définie par : $x\mathcal{R}y \iff x-y \in \mathcal{C}_0$. Montrer qu'il s'agit d'une relation d'équivalence. On note par $\pi : \mathcal{C} \longrightarrow \mathcal{C}/\mathcal{R}$ sa projection canonique.
3. On définit sur le quotient \mathcal{C}/\mathcal{R} une addition par $\pi(x) + \pi(y) = \pi(x+y)$. Vérifier qu'elle est bien définie et que \mathcal{C}/\mathcal{R} , muni de cette loi, est un groupe abélien.
4. Soit $J : \mathbb{Q} \longrightarrow \mathcal{S}$, qui à $q \in \mathbb{Q}$ associe la suite constante égale à q . Montrer que J est injective et que $J(\mathbb{Q}) \subset \mathcal{C}$. Montrer que l'application $I = \pi \circ J$ est injective. On identifiera donc \mathbb{Q} avec $I(\mathbb{Q}) \subset \mathcal{C}/\mathcal{R}$.
5. Soit \leq' la relation binaire sur \mathcal{C} définie par : $x \leq' y$ si, et seulement si, il existe $a \in \mathbb{Q}^{+*}$ et $N \in \mathbb{N}$ tels que $n \geq N \implies y_n - x_n \geq a$. Vérifier qu'il s'agit d'une relation d'ordre sur \mathcal{C} qui vérifie, de plus, la propriété suivante : $x \leq' y$ et $x\mathcal{R}x'$ et $y\mathcal{R}y'$ implique $x' \leq' y'$.
6. Montrer que l'on définit une relation d'ordre \leq sur \mathcal{C}/\mathcal{R} en posant, pour $X, Y \in \mathcal{C}/\mathcal{R}$, $X \leq Y$ si $X = Y$ ou bien si $x \leq' y$ pour tout $(x, y) \in X \times Y$. On remarque que cet ordre prolonge celui de \mathbb{Q} (indentifié à $I(\mathbb{Q})$). Montrer, de plus, que $X < Y$ si, et seulement si, il existe $(x, y) \in X \times Y$ tel que $x \leq' y$.
7. On montre que \leq est un ordre total. Pour cela, prenons $X \neq Y$ dans \mathcal{C}/\mathcal{R} et des représentants $x = (x_n)_n$ et $y = (y_n)_n$ dans \mathcal{C} de X et Y respectivement.
 - (a) Montrer qu'il existe $a \in \mathbb{Q}^{+*}$ et une suite d'indices $(n_k)_k$ tels que, pour tout k , $|x_{n_k} - y_{n_k}| \geq a$.
 - (b) Soit $\epsilon \in]0; a/3]$ (c'est un intervalle de \mathbb{Q}). Pour cet ϵ , traduire le fait que x et y sont de Cauchy et en déduire l'existence d'un k pour lequel $n \geq n_k$ implique $|y_n - x_n| \geq \epsilon$.
 - (c) Conclure, grâce au 6, que $X < Y$ ou bien $Y < X$ (utiliser le signe de $x_{n_k} - y_{n_k}$).
8. On établit que l'ordre \leq possède la propriété de simplification suivante : $\forall (X, Y, H) \in (\mathcal{C}/\mathcal{R})^3$, $X \leq Y$ implique $X + H \leq Y + H$. Pour ce faire, prenons $X < Y$ (pour $X = Y$, il n'y a rien à démontrer), H quelconque, et des représentants x, y, h de X, Y, H respectivement. Montrer que $X + H \leq Y + H$.
9. On note $(\mathcal{C}/\mathcal{R})^* = (\mathcal{C}/\mathcal{R}) \setminus \{0\}$ (0 désigne l'élément neutre de \mathcal{C}/\mathcal{R}) et par $(\mathcal{C}/\mathcal{R})^{+*}$ l'ensemble des éléments X de \mathcal{C}/\mathcal{R} vérifiant $X > 0$. En utilisant les propriétés de \mathbb{Q} , montrer que $(\mathcal{C}/\mathcal{R})^{+*}$ n'admet pas de plus petit élément.
10. On montre maintenant que \mathcal{C}/\mathcal{R} est archimédien. Soit $X, Y > 0$ dans \mathcal{C}/\mathcal{R} , représentés respectivement par x, y dans \mathcal{C} .
 - (a) Montrer qu'il existe deux suites constantes a, b telles que $0 < A < X$ et $Y < B$, où A, B sont les classes de a et b respectivement.
 - (b) Conclure en utilisant le fait que \mathbb{Q} est archimédien.

11. Montrer que \mathbb{Q} (plus précisément $I(\mathbb{Q})$) est partout dense dans \mathcal{C}/\mathcal{R} .
12. Soit $x \in \mathcal{C}$ et $X \in \mathcal{C}/\mathcal{R}$ sa classe. On considère la suite $(X_n)_n \in (\mathcal{C}/\mathcal{R})^{\mathbb{N}}$ où, pour tout n , X_n est la classe dans \mathcal{C}/\mathcal{R} de la suite constante égale à x_n , notée $[x_n]$.
 - (a) Soit $E > 0$ dans \mathcal{C}/\mathcal{R} . Trouver $\epsilon' \in \mathbb{Q}$ tel que $E > 2E' > 0$ dans \mathcal{C}/\mathcal{R} , où E' est la classe de ϵ' .
 - (b) Trouver un $N \in \mathbb{N}$ tel que, pour $n \geq N$, on ait, dans \mathcal{C}/\mathcal{R} , $-E' \leq X - X_n \leq E$.

On a donc montré que $(X_n)_n$ converge vers X dans \mathcal{C}/\mathcal{R} . En voyant la suite de Cauchy x sur \mathbb{Q} dans un autre ensemble, à savoir \mathcal{C}/\mathcal{R} , on lui a trouvé une limite dans cet ensemble.

13. On montre enfin que \mathcal{C}/\mathcal{R} est complet. Pour cela, considérons $(X_n)_n$ une suite de Cauchy dans \mathcal{C}/\mathcal{R} . On montre qu'elle converge dans \mathcal{C}/\mathcal{R} . Soit $(\epsilon_n)_n \in (\mathbb{Q}^{+*})^{\mathbb{N}}$ tendant vers 0. On note par E_n la classe dans \mathcal{C}/\mathcal{R} de la suite constante égale à ϵ_n .
 - (a) Montrer qu'il existe une suite $(G_n)_n \in (I(\mathbb{Q}))^{\mathbb{N}}$ telle que, pour tout n , $-E_n \leq G_n - X_n \leq E_n$.
 - (b) En déduire que $(G_n)_n$ est de Cauchy dans \mathcal{C}/\mathcal{R} . Pour tout n , soit $g_n \in \mathbb{Q}$ tel que $I(g_n) = G_n$. Montrer que $(g_n)_n$ est de Cauchy dans \mathbb{Q} .
 - (c) Soit X la classe dans \mathcal{C}/\mathcal{R} de la suite $(g_n)_n$. Montrer que $(X_n)_n$ converge vers X dans \mathcal{C}/\mathcal{R} .

Le groupe abélien complet \mathcal{C}/\mathcal{R} n'est autre que \mathbb{R} . On peut ensuite contruire une multiplication sur \mathbb{R} qui prolonge celle de \mathbb{Q} et qui fait de \mathcal{C}/\mathcal{R} un corps. Notons qu'il existe au moins une autre construction de \mathbb{R} qui donne le "même résultat" dans le sens où le corps obtenu est "isomorphe" à \mathcal{C}/\mathcal{R} .

Propriété de la borne supérieure dans \mathbb{R} .

On va voir ici quelques conséquences de la complétude de \mathbb{R} . Ces résultats, qui ne sont pas valables pour \mathbb{Q} , sont la principale motivation pour la construction de \mathbb{R} , ce qui explique que la construction précédente a été pensée de façon à garantir la complétude.

La première conséquence est la "propriété des segments emboîtés", la seconde celle de la borne supérieure.

1. Soit $(a_n)_n$ une suite croissante de réels, $(b_n)_n$ une suite décroissante de réels, de sorte que la différence $(b_n - a_n)_n$ soit une suite positive et tende vers 0.
 - (a) Montrer que $(a_n)_n$ et $(b_n)_n$ sont des suites de Cauchy. On appelle A et B leurs limites respectives. Montrer que $A \leq B$.
 - (b) Vérifier que A est la borne supérieure de $\{a_n; n \in \mathbb{N}\}$ et que B est la borne inférieure de $\{b_n; n \in \mathbb{N}\}$.

- (c) En déduire que $A = B$ et que l'ensemble $\bigcap_{n \in \mathbb{N}} [a_n; b_n]$ est un singleton.
2. Soit $(a_n)_n$ une suite croissante majorée de réels. Montrer par l'absurde qu'elle est de Cauchy, donc convergente.
3. Soit E une partie non vide de \mathbb{R} , majorée par b . Soit $a \in E$. On suppose que E n'admet pas de maximum (car sinon c'est évidemment la borne supérieure de E).
- (a) Construire par récurrence une suite $(a_n)_n$ d'éléments de E et une suite $(b_n)_n$ de majorants de E , vérifiant $a_0 = a$, $b_0 = b$, et la propriété \mathcal{P}_n suivante :
- $$a_0 \leq a_1 \leq \dots \leq a_n < b_n \leq \dots \leq b_1 \leq b_0 \quad \text{et} \quad \forall i \in \llbracket 0; n \rrbracket, 2^i(b_i - a_i) \leq b_0 - a_0.$$
- (b) Montrer que la suite $(b_n - a_n)_n$ converge vers 0.
- (c) D'après 2, $(a_n)_n$ converge vers un certain réel S . D'après 1, $(b_n)_n$ converge aussi vers S et on a $S = \sup\{a_n; n \in \mathbb{N}\} = \inf\{b_n; n \in \mathbb{N}\}$. En déduire que S est la borne supérieure de E .