Recommandations :

- portables éteints pendant le cours.
  (ensoleillé entre les cours)
  cf. fatigue
- travail personnel régulier primordial.
  Chercher les exos. à l'avance,
  voir des bouquins, réviser le cours
- déf. et résultats du cours : vitaux.
  dém. : utiles.

Programme :

- → Nbs et suites réelles
- → Suites et séries de fonctions
- → Analyse asymptotique.
- → Calcul différentiel
- → Topologie d'un espace vectoriel normé de dim. finie.

(motivations :
- $\mathbb{N}$ sert à construire $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$
- l'étude correcte de $\mathbb{N}$ n'y jamais faite
- récu. et divisibi.)

Nombres et suites réelles.

Construction de $\mathbb{N}$. (voir Arnaudiès - Fraysse, cours de mathématiques 1, Algèbre).

Intuition de l'ensemble des entiers naturels $\mathbb{N}$:

- → numérotation (aspect ordinal).
- → comptage (aspect cardinal)
- → ensemble infini "simple" : $\mathbb{N} = \{0; 1; 2; 3; \dots\}$.

Ici on ne construit pas l'ens. $\mathbb{N}$ (à partir de la théorie des ensembles), on postule son existence sous la forme des axiomes de Peano.

Axiomes de Peano : On postule l'existence d'un triplet $(0; \mathbb{N}, S)$ où $\mathbb{N}$ est un ens., 0 un élé. particulier de $\mathbb{N}$ et $S : \mathbb{N} \to \mathbb{N}$, tel que :

(P1) S est injective.

(P2) L'image $S(\mathbb{N})$ de $\mathbb{N}$ par S est exactement $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.

(P3) Soit A une partie de $\mathbb{N}$. Si $0 \in A$ et si

(*) $\left(\forall n \in \mathbb{N},\ (n \in A \Rightarrow S(n) \in A) \right)$

est vraie, alors $A = \mathbb{N}$.

$\mathbb{N}$: ens. des entiers naturels.
0 : zéro.
S : appl. successeur.
(P3) : axiome de récurrence. ($0 \in A$: initialisation ; (*) : hérédité)

Notations : $1 := S(0)$, $2 := S(1)$, $3 = S(2)$

Th. de récurrence : Soit $\mathcal{P}(n)$ une assertion dépendante de $n \in \mathbb{N}$. On a :

$$\left(\mathcal{P}(0) \text{ et } \left(\forall n \in \mathbb{N},\ \mathcal{P}(n) \Rightarrow \mathcal{P}(S(n)) \right) \right) \Rightarrow \left(\forall n \in \mathbb{N},\ \mathcal{P}(n) \right).$$

Preuve : Soit $A = \{n \in \mathbb{N};\ \mathcal{P}(n)\}$. On appl. (P3). □.

Exemple : Montrons par récurrence la propriété :

$$\forall n \in \mathbb{N},\quad S(n) \neq n.$$

Preuve :
Posons, pour $n \in \mathbb{N}$, $\mathcal{P}(n) = (S(n) \neq n)$.

D'après (P2), on a $S(0) \neq 0$ donc $\mathcal{P}(0)$ est vraie.

Supposons, pour un $n \in \mathbb{N}$, que $\mathcal{P}(n)$ soit vraie.
On vérifie $\mathcal{P}(S(n))$: On a $S(n) \neq n$ (par $\mathcal{P}(n)$).
Comme S est injective, $S(S(n)) \neq S(n)$ et $\mathcal{P}(S(n))$ est vraie. Par le Th. de récu., $\mathcal{P}(n)$ est vraie pour tout n. □

Lorsqu'on étudie les suites récurrentes, on admet implicitement qu'elles sont bien définies (on ne peut pas vérifier que tous les termes sont bien définis !)
D'autre part, on a souvent besoin de construire des applications par récurrence. Dans les deux cas, le bien-fondé de la procédure est basé sur les résultats admis suivants.

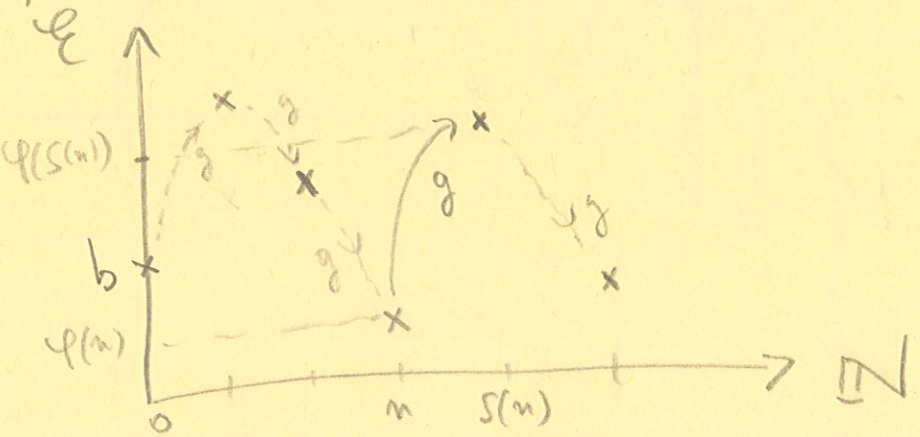
Th. 1 : Soit $\mathcal{E}$ un ens. non vide, $b \in \mathcal{E}$ et $g : \mathcal{E} \to \mathcal{E}$.
Il existe une unique appl. $\varphi : \mathbb{N} \to \mathcal{E}$ t.q.

$$\varphi(0) = b \quad \text{et} \quad \varphi \circ S = g \circ \varphi$$

Rq. : on peut voir une preuve dans la réf. donnée.

Pb. : on doit définir une appl. φ sur un ens. infini ! On ne peut pas donner toutes les images ! Le Th. 1 résout ce problème.

Interprétation graphique du Th. 1 :



Version à paramètre du Th. 1 :

Th. 2 : Soit $\mathcal{E}, \mathcal{F}$ deux ens. non vides, $g : \mathcal{E} \to \mathcal{E}$ et $\psi : \mathcal{F} \to \mathcal{E}$. Il existe une unique appl. $\varphi : \mathcal{F} \times \mathbb{N} \to \mathcal{E}$ vérifiant

(1) $\forall f \in \mathcal{F}, \quad \varphi(f;0) = \psi(f)$

(2) $\forall f \in \mathcal{F}, \forall n \in \mathbb{N}, \quad \varphi(f;S(n)) = g(\varphi(f;n))$.

Th. 2' : Soit $\mathcal{E}, \mathcal{F}$ non vides, $g : \mathcal{F} \times \mathcal{E} \to \mathcal{E}$, $\psi : \mathcal{F} \to \mathcal{E}$

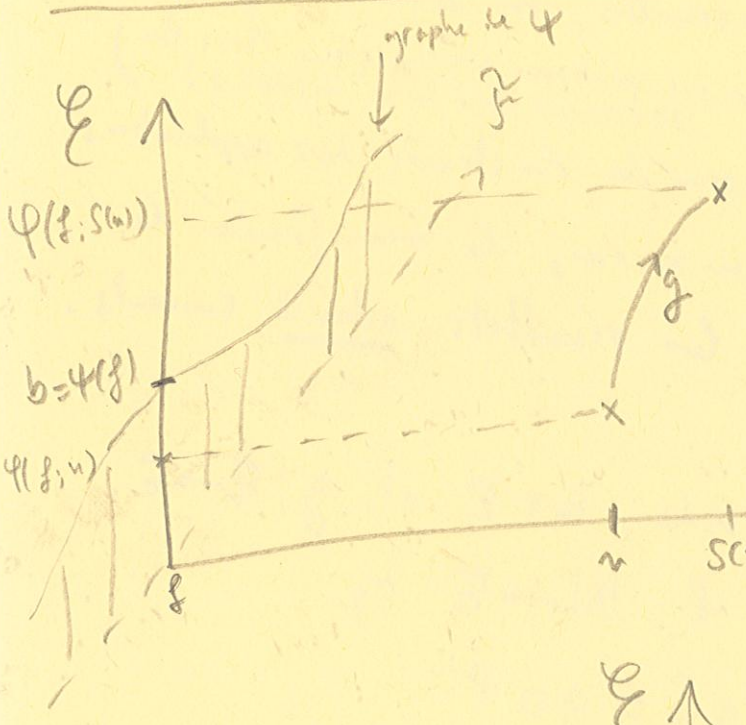
$\exists !\ \varphi : \mathcal{F} \times \mathbb{N} \to \mathcal{E}$ vérifiant

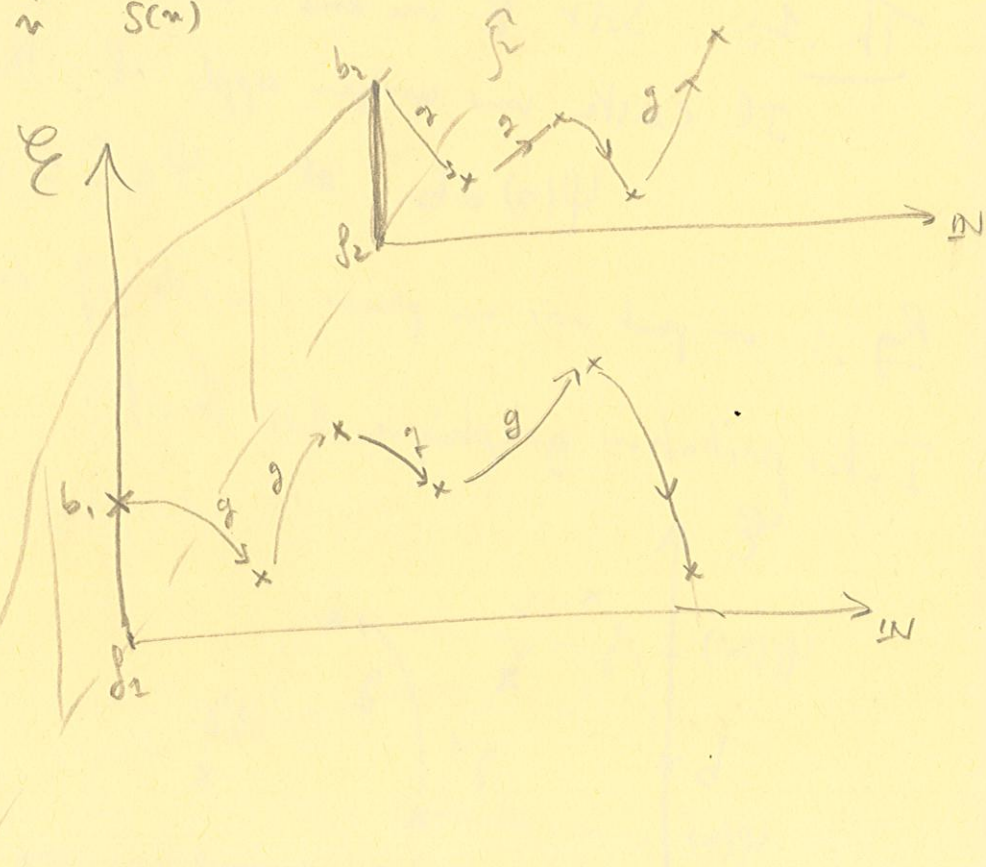
(1) $\forall f \in \mathcal{F}, \ \varphi(f;0) = \psi(f)$

(2) $\forall f \in \mathcal{F}, \forall n \in \mathbb{N}, \ \varphi(f;S(n)) = g(f;\varphi(f;n))$

A vérifier ✓

Interprétation graphique du Th. 2.





Addition dans $\mathbb{N}$:

Comme précédemment, on a le problème de définir une appl. $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sur un ens. infini $(\mathbb{N} \times \mathbb{N})$.

On cherche à définir l'addition de manière récursive en utilisant l'appl. S.

Idée : calcul de $1+2$:

$$1+2 = 1+S(1) = 1+(1+1) = (1+1)+1$$
$$= S(1+1).$$

Connaissant $1+1$, on en déduit $1+2$.

$$1+1 = 1+S(0) = S(1) = S(1+0).$$

Th. 3 : Il existe une unique appl. $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ vérifiant

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

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

Preuve : on appl. le Th. 2 avec $E = F = \mathbb{N}$, $\psi = id_{\mathbb{N}}$ et $g = S$. $+ = \varphi$ convient. □.

Propriétés :

Associativité : $\forall (p,q,r) \in \mathbb{N}^3, \quad (p+q)+r = p+(q+r)$.

Commutativité : $\forall (p,q) \in \mathbb{N}^2, \quad p+q = q+p$.

Régularité : $\forall (p,q,r) \in \mathbb{N}^3, \quad p+r = q+r \Rightarrow p = q$.

$\forall (p,q) \in \mathbb{N}^2, \quad p+q = 0 \Rightarrow (p = 0 \text{ et } q = 0)$.

$\forall n \in \mathbb{N}, \quad S(n) = n+1$. $(1+n)$

On démontre l'associativité : Soit $(p,q) \in \mathbb{N}^2$ fixé.
Pour $r \in \mathbb{N}$, soit $A(r) = \big((p+q)+r = p+(q+r)\big)$.

Comme $(p+q)+0 \overset{(1)\,Th.3}{=} p+q \overset{(2)\,Th.3}{=} p+(q+0)$, $A(0)$ est vraie.

Supp. $A(r)$ vraie. $(p+q)+S(r) \overset{(2)\,Th.3}{=} S\big((p+q)+r\big) \overset{HR}{=} S(p+(q+r))$

$\overset{(2)\,Th.3}{=} p+S(q+r) \overset{(2)\,Th.3}{=} p+(q+S(r))$

Donc $A(S(r))$ est vraie. Par le Th. de réc., $A(r)$ est vraie pour tout r. Ceci étant vrai pour tout p,q, on a l'asso. □.

laissé !

On démontre la commutativité.

Pour $p \in \mathbb{N}$, soit $\mathcal{P}(p) = \big(\forall q \in \mathbb{N},\ p+q = q+p\big)$.

Pour $n \in \mathbb{N}$, soit $Q(n) = (0+n = n+0)$.

Par (1) du Th. 3, $Q(0)$ est vraie. Supp. $Q(n)$ vraie.

On a $0+S(n) = S(0+n) = S(n+0) \overset{\text{cf. (1) Th.3}}{=} S(n) = S(n)+0$.

Donc $Q(S(n))$ est vraie. Par réc., $Q(n)$ est vraie pour tout n.

Donc $\mathcal{P}(0)$ est vraie.

Supp. $\mathcal{P}(p)$ vraie. Pour $q \in \mathbb{N}$, soit $Q_{S(p)}(q) = \big(S(p)+q = q+S(p)\big)$

$Q_{S(p)}(0)$ est vraie (cf. $\mathcal{P}(0)$). Supp. $Q_{S(p)}(q)$ vraie.

$S(p)+S(q) \overset{(2)\,Th.3}{=} S\big(S(p)+q\big) \overset{Q_{S(p)}(q)}{=} S(q+S(p)) = S\circ S(q+p)$

$\overset{\mathcal{P}(p)\text{ vraie}}{=} S\circ S(p+q) \overset{(2)\,Th.3}{=} S(p+S(q)) \overset{\mathcal{P}(p)\text{ vraie}}{=} S(S(q)+p) \overset{(2)\,Th.3}{=} S(q)+S(p)$.

Donc $Q_{S(p)}(S(q))$ est vraie. Par réc., $Q_{S(p)}(q)$ est vraie pour tout q. Donc $\mathcal{P}(S(p))$ est vraie.

Par réc., $\mathcal{P}(p)$ est vraie pour tout p. □.

Régularité : Pour $r \in \mathbb{N}$, soit $R(r) = (p+r = q+r \Rightarrow p = q)$.

$R(0)$ est vraie. Supp. $R(r)$ vraie.

Soit $p, q \in \mathbb{N}$ tq. $p + S(r) = q + S(r)$.

Or $p + S(r) = S(p+r)$ et $q + S(r) = S(q+r)$,

donc, comme S est inj., $p + r = q + r$. Par H.R., $p = q$.

Donc $R(S(r))$ est vraie. Par le Th. de réc.

$R(r)$ est vraie pour tout r. □

Preuve de : $p+q=0 \Rightarrow (p=0)$

On montre : non $(p=0$ et $q=0) \Rightarrow$ non $(p+q=0)$.

Soit $p, q \in \mathbb{N}$ avec $p \neq 0$. Il existe $r \in \mathbb{N}$; $p = S(r)$.

$p + q = S(r) + q = q + S(r) = S(q+r) \in \mathbb{N}^*$. □

Preuve de : $(p+q=0) \Rightarrow (p=0$ et $q=0)$.

On a $(p+q=0) \Rightarrow (p=0)$

$(p+q=0) \Leftrightarrow (q+p=0) \Rightarrow (q=0)$. □.

Preuve de : $\forall n$, $S(n) = n+1$.

Soit $\mathcal{P}(n) = (S(n) = n+1)$. Comme $S(0) = 1 = 0+1$ (commut. + (a) Th. 3),

$\mathcal{P}(0)$ est vraie. Comme $S(1) = S(1+0) = 1 + S(0) = 1+1$,

$\mathcal{P}(1)$ est vraie. Supp. $\mathcal{P}(n)$ vraie. On a : (a) Th. 3 ; (2) Th. 3.

$S(S(n)) \overset{HR}{=} S(n+1) \overset{(2)\text{Th.}3}{=} n + S(1) = n + (1+1) \overset{\text{asso.}}{=} (n+1)+1 \overset{HR}{=} S(n)+1$.

Donc $\mathcal{P}(S(n))$ est vraie. Par le Th. de récu., $\mathcal{P}(n)$ est vraie pour tout n. □

Reformulation du Th. de récu. :

Th. 4 : Soit $\mathcal{P}(n)$ une assertion dépendant de $n \in \mathbb{N}$.

$$\Big(\mathcal{P}(0) \text{ et } \big(\forall n \in \mathbb{N},\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)\big) \Big) \Rightarrow \big(\forall n \in \mathbb{N},\ \mathcal{P}(n)\big)$$

Suites récurrentes.

Soit $g : \mathbb{R} \to \mathbb{R}$. On s'intéresse à la suite $(u_n)_{n \in \mathbb{N}}$ donnée par : $\begin{cases} u_0 \in \mathbb{R} \\ \forall n \in \mathbb{N},\ u_{n+1} = g(u_n). \end{cases}$

Il n'est cependant pas clair que les conditions précédentes définissent une seule suite l'elle. Une suite est une appl. $u : \mathbb{N} \to \mathbb{R}$. Comme $\mathbb{N}$ est infini, on retombe sur le pb. précédent : on ne peut pas énumérer toutes les images. Mais la reformulation suivante du Th. 1 donne une réponse positive :

Th. 5 : Soit E un ens. non vide, $b \in E$ et $g : E \to E$. Il existe une unique appl. $\varphi : \mathbb{N} \to E$ t.q. $\varphi(0) = b$ et pour tout $n \in \mathbb{N}$, $\varphi(n+1) = g(\varphi(n))$.

Dans l'exemple préc., le Th. 5 s'applique avec $E = \mathbb{R}$, $b = u_0$ et $u = \varphi$.

On peut aussi reformuler le Th. 2 sous la forme :

Th. 6 : Soit E et F deux ens. non vides, $g : E \to F$ et $\psi : F \to E$. Il existe une unique appl. $\varphi : F \times \mathbb{N} \to E$ vérifiant

(1) $\forall f \in \mathcal{F}, \quad \varphi(f;0) = \varphi(f)$

(2) $\forall f \in \mathcal{F}, \forall n \in \mathbb{N}, \quad \varphi(f;n+1) = g(\varphi(f;n))$.

Itérées successives d'une appl.

Soit $\mathcal{E}$ un ens. non vide et $g : \mathcal{E} \to \mathcal{E}$.

Pour chaque $x \in \mathcal{E}$, soit $\varphi_x : \mathbb{N} \to \mathcal{E}$ (donnée par Th. 5) vérifiant

$$\varphi_x(0) = x \text{ et } \forall n \in \mathbb{N}, \quad \varphi_x(n+1) = g(\varphi_x(n)). \qquad (**)$$

Pour $k \in \mathbb{N}$, soit $f_k : \mathcal{E} \to \mathcal{E}$, $x \mapsto \varphi_x(k)$.

On a $f_0 = Id_{\mathcal{E}}$ et, pour $k \in \mathbb{N}^*$, pour $x \in \mathcal{E}$,

$$f_k(x) = \varphi_x(k) = \underbrace{g \circ g \circ g \circ \cdots \circ g}_{k \text{ fois}}(x).$$

On note f_k par $g^{<k>}$, c'est l'itérée $k$ième de g.

On a construit ci-dessus $g^{<k>}$ "point par point".

On peut aussi les construire globalement, à Soit

On peut aussi les construire globalement, à Soit $\mathcal{G} = \mathcal{E}^{\mathcal{E}}$ l'ens. des appl. de $\mathcal{E}$ dans $\mathcal{E}$ et $G : \mathcal{G} \to \mathcal{G}$ laissé ? donnée par $G(f) = g \circ f$. Par le Th. 5 (avec $\mathcal{E} = \mathcal{G}$, $g = G$), il existe $\Phi : \mathbb{N} \to \mathcal{G}$ t.q. $\Phi(0) = id_{\mathcal{E}}$ et

$$\forall n \in \mathbb{N}, \quad \Phi(n+1) = G(\Phi(n)) = g \circ \Phi(n).$$

On vérifie que $\Phi(k) = g^{<k>}$ et que

$$\forall (n,p) \in \mathbb{N}^2, \quad g^{<n+p>} = g^{<n>} \circ g^{<p>}.$$

Pour tout $x \in E$, tout $n \in \mathbb{N}$,

$$\Phi(n+1)(x) = G(\Phi(n))(x)$$
$$= (g \circ \Phi(n))(x) = g(\Phi(n)(x)).$$

De plus $\Phi(0)(x) = x$. Par l'unicité de (**), on a, pour tout n, $\Phi(n)(x) = \varphi_x(n) = g^{\langle n \rangle}(x)$. □

Pour $n \in \mathbb{N}$, soit $\mathcal{P}(n) = (\forall p \in \mathbb{N},\ g^{\langle n+p \rangle} = g^{\langle n \rangle} \circ g^{\langle p \rangle})$.

$\mathcal{P}(0)$ est vraie car $g^{\langle 0 \rangle} = id_E$. Supp. $\mathcal{P}(n)$ vraie.

Soit $p \in \mathbb{N}$. On a

$$g^{\langle n+1+p \rangle} = g^{\langle (n+p)+1 \rangle} = G(g^{\langle n+p \rangle})$$
$$\overset{H.R.}{=} g \circ (g^{\langle n \rangle} \circ g^{\langle p \rangle}) = (g \circ g^{\langle n \rangle}) \circ g^{\langle p \rangle}$$
$$= g^{\langle n+1 \rangle} \circ g^{\langle p \rangle}.$$

Par le Th. de réc., $\mathcal{P}(n)$ est vraie pour tout n. □

Multiplication dans $\mathbb{N}$.

Th. 7. : Il existe une unique appl. $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ vérifiant

(1) $\forall n \in \mathbb{N},\ n \times 0 = 0$

(2) $\forall (p,q) \in \mathbb{N}^2,\ p \times (q+1) = (p \times q) + p$.

Preuve : On appl. le Th. 2' avec $E = F = \mathbb{N}$, $\psi : \mathbb{N} \to \mathbb{N}$, $n \mapsto 0$,

$g : \mathbb{N}^2 \to \mathbb{N}$, $(p,q) \mapsto p+q$. □

Propriétés :

Distributivité :

$\forall (p,q,r) \in \mathbb{N}^3$, $p \times (q+r) = p \times q + p \times r$, et

$(q+r) \times p = q \times p + r \times p$.

Associativité :

$\forall (p,q,r) \in \mathbb{N}^3$, $p \times (q \times r) = (p \times q) \times r$.

Commutativité :

$\forall (p,q) \in \mathbb{N}^2$, $p \times q = q \times p$.

Régularité des élé. de $\mathbb{N}^*$:

$\forall (p,q,r) \in \mathbb{N}^2 \times \mathbb{N}^*$, $(p \times r = q \times r \Rightarrow p = q)$.

Remarque : Pour $p \in \mathbb{N}$, $p \times 1 = p \times (0+1)$

$\overset{\text{(2) Th.7}}{=} p \times 0 + p$

$\overset{\text{(1) Th.7}}{=} p$

Par commutativité on a aussi $1 \times p = p$.

1 est l'élé. neutre de $\times$.

Exponentiation :

Th. 8 et déf. : Il existe une unique appl. $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a;b) \mapsto a^b$ vérifiant

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

(2) $\forall (p,q) \in \mathbb{N}^2$, $p^{q+1} = p^q \times p$.

Preuve : on appl. le Th. 2' avec $\mathcal{C} = \mathcal{F} = \mathbb{N}$, $\psi : \mathbb{N} \to \mathbb{N}$, $n \mapsto 1$,

$g : \mathbb{N}^2 \to \mathbb{N}$, $(p,q) \mapsto p \times q$. □.

Propriétés :

$\forall (n,p,q) \in \mathbb{N}^3$, $n^{p+q} = n^p \times n^q$) ∈ exo : à démo par récu. sur q.

$\forall (n;p;q) \in \mathbb{N}^3$, $(n^p)^q = n^{pq}$

$\forall (n,p,q) \in \mathbb{N}$, $(np)^q = n^q p^q$.

Remarque : Par ex, $n^1 = n^{0+1} = n^0 \times n = 1 \times n = n$.

En parti., $0^1 = 1$ mais pour $p \in \mathbb{N}^*$

$0^p = 0$.

Soustraction :

Soit $\mathcal{G} = \{ (a;b) \in \mathbb{N}^2 ; \exists c \in \mathbb{N} ; a = b+c \}$.

Pour $(a;b) \in \mathcal{G}$, il n'y a qu'un seul c vérifiant

$a = b+c$.

En effet, si c et c' conviennent, on a $b+c = b+c'$

et par simplification de b, $c = c'$.

L'unique c tel que $a = b+c$ est la différence de a et de b. On la note : $c = a-b$.

L'appl. : $\mathcal{G} \longrightarrow \mathbb{N}$ est la soustraction.

$(a;b) \longmapsto a-b$

Elle n'est pas définie partout ! En effet,

$(0;1) \notin \mathcal{G}$ (Si on avait $0 = 1+c$ avec $c \in \mathbb{N}$ alors $0 \in S(c)$ Contr.).

Division : Soit $\mathcal{D} = \{ (a;b) \in \mathbb{N} \times \mathbb{N}^* ; \exists c \in \mathbb{N} ; a = b \times c \}$.

Si $a = bc = bc'$ alors par simpl. de b ($\neq 0$), $c = c'$.

Pour $(a;b) \in \mathcal{D}$, le c tel que $a = bc$ est le quotient de a par b. On le note $c = \frac{a}{b} = a/b$.

L'appl. de division (exacte) est :

$$\begin{array}{ccc} \mathcal{D} & \longrightarrow & \mathbb{N} \\ (a;b) & \longmapsto & \frac{a}{b} \end{array}$$

Elle n'est pas définie partout !

Exercice : montrer que $(2;3) \notin \mathcal{D}$. $(7;3) \notin \mathcal{D}$. (on pourra utiliser l'ordre de $\mathbb{N}$)

Ordre naturel de $\mathbb{N}$.

Th. 9 et déf. : La relation binaire $\leq$ sur $\mathbb{N}$, définie par

$$\forall (a;b) \in \mathbb{N}, \quad a \leq b \iff \exists d \in \mathbb{N};\ b = a + d$$

est une relation d'ordre total :

(1) $\forall a \in \mathbb{N}$, $a \leq a$

(2) $\forall (a;b) \in \mathbb{N}^2$, $(a \leq b \text{ et } b \leq a) \Rightarrow a = b$

(3) $\forall (a;b;c) \in \mathbb{N}^2$, $(a \leq b \text{ et } b \leq c) \Rightarrow a \leq c$.

(4) $\forall (a;b) \in \mathbb{N}^2$, $(a \leq b \text{ ou } b \leq a)$.

Preuve : (1) $\forall a \in \mathbb{N}$, $a = a + 0$.

(2) si $a = b + c$ et $b = a + d$ alors $a = a + c + d$ donc (simpl.) $0 = c + d$ $\Rightarrow$ d'où $c = d = 0$ et $a = b$.

(3). Si $a = b+d$ et $b = c+e$ alors

$$a = (c+e)+d = c+\underbrace{(d+e)}_{\in \mathbb{N}}$$

d'où $a \geq c$.

(4). Pour $p \in \mathbb{N}$ soit $S(p) = (\forall q \in \mathbb{N},\ (p \leq q) \text{ ou } (q \leq p))$

$S(0)$ est vraie car, pour $q \in \mathbb{N}$, $q = q+0$ donc $q \geq 0$.

Supp. $S(p)$ vraie.

On a $0 \leq p+1$. Soit $q \in \mathbb{N}^*$. Il existe $q' \in \mathbb{N}$ t.q. $q = q'+1$. Par hyp. de réc., on a $q' \leq p$ ou $q' \geq p$.

1er cas : $q' \leq p$. Alors $p = q'+d$ avec $d \in \mathbb{N}$ et $p+1 = q'+d+1 = (q'+1)+d = q+d$.

Donc $p+1 \geq q$.

2ème cas : $q' \geq p$. Alors $q' = p+d$ avec $d \in \mathbb{N}$ et $q = q'+1 = (p+d)+1 = (p+1)+d$. D'où $q \geq p+1$.

Donc $S(p+1)$ est vraie.

Par le th. de réc., $S(p)$ est vraie pour tout p. Donc l'ordre est total.

Remarque : $(n \leq p \text{ et } n \neq p) \iff (n+1 \leq p)$.

notation : $(n \leq p \text{ et } n \neq p)$ est noté $(n < p)$.

Propriétés : (de simplification)

$\forall (m,n,p) \in \mathbb{N}^3$, $(m \leq n \iff m+p \leq n+p)$

$\forall (m,n,p) \in \mathbb{N}^2 \times \mathbb{N}^*$, $(m \leq n \iff m \times p \leq n \times p)$.

Rq : $(mn = 1) \iff (m = 1 \text{ et } n = 1)$.

Exo : à vérifier.

Rappel : Soit $A \subset \mathbb{N}$ et $b \in \mathbb{N}$.

* b est un majorant (minorant) de A si
$\forall a \in A$, $a \leq b$ $(a \geq b)$.

* $b \in \mathbb{N}$ est un plus gd. (petit) élé de A si $b \in A$ et b majore (minore) A.

* Un plus gd. (petit) élé. est unique.

Th. 10 : $(\mathbb{N}, \leq)$ est bien ordonné : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. ✓

Preuve : Soit $A \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. Soit M l'ens. des minorants de A. $M \neq \emptyset$ car $0 \in M$.
Soit $a \in A$. $a+1 > a$ donc $a+1 \notin M$. En particulier, $M \neq \mathbb{N}$. La proposition
$(\forall n \in \mathbb{N}, \; n \in M \Rightarrow n+1 \in M)$ est fausse.

En effet, si elle était vraie, on aurait, comme $0 \in M$, $M = \mathbb{N}$ par l'axiome de réc.

Contr. Donc

non $\left(\forall n \in \mathbb{N},\ (n \in M) \Rightarrow (n+1 \in M) \right)$

$\Leftrightarrow \exists n \in \mathbb{N},\ (n \in M \text{ et } n+1 \notin M)$.

Soit $n_0 \in \mathbb{N}$ tq. $n_0 \in M$ et $n_0 + 1 \notin M$.

Si $n_0 \notin A$, on aurait pour tout $a \in A$, $n_0 < a$ donc $n_0 + 1 \leq a$ et $n_0 + 1 \in M$.

Contr. Donc $n_0 \in A$. Comme $n_0 \in M$, n_0 est le plus petit élé. de A. □.

Rq : 0 est le plus petit élé. de $\mathbb{N}$.

Thm 11 : Toute partie non vide majorée de $\mathbb{N}$ admet un plus gd. élé.

Preuve : Soit $A \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. Soit M l'ens. (non vide) des maj. de A. Comme $\emptyset \neq M \subset \mathbb{N}$, M admet un plus petit élé. a (cf. Th. 10).

Si $a = 0$ alors $A = \{0\}$ et 0 est le plus gd. élé. de A.

Si $a \neq 0$, $a = 1 + b$ avec $b \in \mathbb{N}$. $b < a$ donc, par déf. de a, $b \notin M$. Il existe donc $c \in A$ tq. $b < c$. Donc $a = b + 1 \leq c$ or, par déf. de a, $c \leq a$. D'où $a = c$ et $a \in A$. Conl. : a est le plus gd. élé. de A. □.

Prop. 1 (principe de "descente infinie" de Fermat).
Il n'existe aucune suite d'entiers naturels strictement décroissante.

Preuve : Soit $u = (u_k)_{k\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$ une suite str. ↓.
Soit $U = \{u_k ; k\in\mathbb{N}\} \subset \mathbb{N}$. Par le Th. 10, U admet un plus petit élé. a. Il existe $k_0\in\mathbb{N}$ tq. $a = u_{k_0}$. Comme u str. ↓, $u_{k_0+1} < a$. Contr. □

Intervalles de $\mathbb{N}$. ("fermés")

Déf. 1 : Un intervalle de $\mathbb{N}$ est une partie I de $\mathbb{N}$ vérifiant
$\forall (a,b)\in I^2, \forall n\in\mathbb{N}, ((a\le n) \text{ et } (n\le b)) \Rightarrow (n\in I)$. (*)

Prop. 2 : Les intervalles de $\mathbb{N}$ sont le vide et
* $[\![a;b]\!] = \{n\in\mathbb{N} ; a\le n \text{ et } n\le b\}$, pour $a\le b$;
* $[\![a;\to[\![= \{n\in\mathbb{N} ; a\le n\}$, pour $a\in\mathbb{N}$.

Preuve : Le vide et les ens. donnés ↑ sont bien des intervalles.
Soit I un int. non vide de $\mathbb{N}$. Par le Th. 10, I admet un plus petit élé. a.
1er cas : I est majoré. Soit b un plus gd. élé. (Th. 11). Donc $I \subset [\![a;b]\!]$. Par (*), tout $n\in[\![a;b]\!]$ appartient à I. Donc $I = [\![a;b]\!]$.
2e cas : I n'est pas majoré. $I \subset [\![a;\to[\![$. Soit $n\ge a$. n ne majore pas I donc il existe $b\in I$ tq. $n<b$. Par (*), $n\in I$. D'où $[\![a;\to[\![\subset I$ et $[\![a;\to[\![= I$. □

Variantes du Th. de récurrence.

Prop. 3 : (récurrence "transfinie").
Soit A une partie de $\mathbb{N}$ vérifiant

$$\forall n \in \mathbb{N},\ (\forall p \in \mathbb{N},\ (p<n) \Rightarrow (p \in A)) \Rightarrow (n \in A).$$

Alors $A = \mathbb{N}$.

Rq. : (**) implique $0 \in A$.

Preuve : Soit $B \subset \mathbb{N} \setminus A$. Si $B \neq \emptyset$, soit b son plus petit élt (cf. Th. 10). Par (**) pour $n=b$ on a $b \in A$. Contr. car $b \in B$. □

Prop. 4 : (récurrence à partir d'un certain rang).
Soit $a \in \mathbb{N}$ et A une partie de $\mathbb{N}$ t.q.

* $a \in A$
* $\forall n \in \mathbb{N},\ n \in A \Rightarrow n+1 \in A$.

Alors $[\![a ; \to [\![\subset A$.

En particulier :

$$\Big(\mathcal{P}(a) \text{ et } \forall n \in [\![a ; \to [\![,\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1) \Big) \Rightarrow \Big(\forall n \in [\![a ; \to [\![,\ \mathcal{P}(n) \Big).$$

Preuve : Le second résultat découle du premier en posant $A = \{ n \in \mathbb{N},\ \mathcal{P}(n) \}$.

laissé | Soit $f : \mathbb{N} \to \mathbb{N}$, $p \mapsto p+a$.
f est inj. car si $f(p)=f(q)$, $p+a=q+a$ et, par simplification, $p=q$.

$\mathrm{Im} f = [\![a;\to[\![$:

(comme $p+a \geq a$, pour $p \in \mathbb{N}$, $\mathrm{Im} f \subset [\![a;\to[\![$.

Pour $q \geq a$, il existe $p \in \mathbb{N}$ tq : $q = a+p$. (déf. de l'ordre)

Donc $q \in \mathrm{Im} f$ et $[\![a;\to[\![\subset \mathrm{Im} f$.

Soit $f^{<-1>}$ la bij. réc. de $f : \mathbb{N} \to [\![a;\to[\![$.

Soit $E = f^{<-1>}(A \cap [\![a;\to[\![)$.

Comme $a \in A$, $0 = f^{<-1>}(a) \in E$.

Pour $k \in E$, on a $f(k) \in A \cap [\![a;\to[\![$,

Par hyp : $f(k+1) = (k+1)+p = (k+p)+1 = f(k)+1 \in A$.

De plus, $(k+1)+p \geq a$ car $f(k) = k+p \geq a$,

Donc $f(k+1) \in A \cap [\![a;\to[\![$ et $k+1 \in E$.

Par l'axiome de réc., $E = \mathbb{N}$.

D'où $A \cap [\![a;\to[\![= [\![a;\to[\![$.

Donc $A \supset [\![a;\to[\![$. □.

(récurrence finie).

Th. 12 : Soit $(a,b) \in \mathbb{N}^2$ avec $a \leq b$.

Soit A une partie de $\mathbb{N}$ tq. $a \in A$ et

$\forall n \in \mathbb{N}$, $(n \in A$ et $n < b) \Rightarrow (n+1 \in A)$. (***)

Alors $[\![a;b]\!] \subset A$.

En particulier :

($\mathcal{P}(a)$ et $\forall n \in \mathbb{N}$, $((\mathcal{P}(n)$ et $(n \leq b)) \Rightarrow \mathcal{P}(n+1))$)

$\Rightarrow \forall n \in [\![a;b]\!]$, $\mathcal{P}(n)$.

Preuve : La seconde assertion découle de la première en posant $A = \{n ; \mathcal{P}(n)\}$.

Supp. $[\![a;b]\!] \not\subset A$. Soit $B = [\![a;b]\!] \setminus A \neq \emptyset$.
Par le Th. 10, B admet un plus petit élé. b'.
On a $a \leq b' \leq b$. $b' \neq a$ car $a \in A$ (y. hyp.)
Donc $a < b'$ et $a+1 \leq b'$. On a $a \leq b'-1 < b' \leq b$.
et $b'-1 \notin B$. Donc $b'-1 \in A \cap [\![a;b[\![$. Par (***),
$b' = b'-1+1 \in A$. Contr. avec $b' \in B$. □.

Corollaire 1 (récurrence descendante) :

Soit $(a,b) \in \mathbb{N}^2$ avec $a \leq b$. Soit A une partie de $\mathbb{N}$ t.q. $b \in A$ et

$\forall n \in \mathbb{N}$, $(n \in A$ et $n > a) \Rightarrow (n-1 \in A)$.

Alors $[\![a;b]\!] \subset A$.

En particulier

$\Big(\mathcal{P}(b)$ et $(\forall n \in \mathbb{N}, ((\mathcal{P}(n)$ et $(n > a)) \Rightarrow \mathcal{P}(n-1)) \Big)$

$\Rightarrow \forall n \in [\![a;b]\!], \mathcal{P}(n)$.

Preuve : On se ramène au Th. précédent en considérant la bij. $f : [\![0; b-a]\!] \to [\![a;b]\!]$
$k \mapsto b-k$. □.

Division euclidienne

Prop. 5 (propriété d'Archimède).
Soit $(a;b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe $n \in \mathbb{N}$ t.q. $nb \geq a$.

Preuve : Si $a = 0$, $n = 1$ convient puisque $b \geq 0$.
Si $a \geq 1$, $n = a$ convient car $b \geq 1$.

Th. 13 : Soit $(a;b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe un unique couple $(q;r) \in \mathbb{N}^2$ t.q.

$$a = bq + r$$
$$\text{et } (0 \leq) r < b.$$

Preuve : a). unicité. Supp. que (q_1, r_1) et (q_2, r_2) conviennent. Alors $bq_1 + r_1 = bq_2 + r_2$ (*)

1er cas : $q_1 > q_2$. Alors $b(q_1 - q_2) + r_1 = r_2$.
Donc $r_2 \geq r_1$ et $r_2 - r_1 \leq r_2 < b$.
or $b < b(q_1 - q_2) = r_2 - r_1$. Contr.

2è cas : $q_2 < q_1$. Alors $b(q_2 - q_1) + r_2 = r_1$
et $r_1 \geq r_2$ et $r_1 - r_2 \leq r_1 < b$. or
$b < b(q_2 - q_1) = r_1 - r_2$. Contr.

D'où $q_1 = q_2$ et, par (*), $r_2 = r_2$.

b). Existence. Par la prop. 5

$M = \{ c \in \mathbb{N};\ cb > a \} \neq \emptyset$

Soit q' le plus petit élé. de M. Par déf. de M, $q' \neq 0$. Donc $q'-1 = 1+q$ pour un $q \in \mathbb{N}$, $q \notin M$ (par déf. de q') donc $bq \leq a$.

On a donc $bq \leq a < bq' = bq + b$.

Donc $r = a - bq \in \mathbb{N}$ et $r < b$. □.

Ex. : Résoudre dans $\mathbb{N}$ les éq. : $2x+3=0$; $2x-3=0$; $3x-6=0$. ✓

Construction de $\mathbb{Z}$.

Motivation : on va plonger $\mathbb{N}$ dans un ens. plus gros ($\mathbb{Z}$) de sorte que la soustraction soit définie partout. On va même obtenir un groupe commutatif pour l'addition.

Intuition : $\mathbb{Z}$ doit être l'ens. de toutes les différences d'entiers.

Sur $\mathbb{N} \times \mathbb{N}$, on déf. la relation $\mathcal{R}$ par

$(a;b) \mathcal{R} (a';b')$ ssi $a+b' = a'+b$.

Remarque : si $(a;b) \mathcal{R} (a';b')$, on a " $a-b = a'-b'$ ".

Prop. 6 $\mathcal{R}$ est une rel. d'équivalence sur $\mathbb{N}^2$.

Preuve : Pour $(a;b) \in \mathbb{N}^2$, on a $a+b = a+b$ donc $(a;b) \mathcal{R} (a;b)$.

Soit $a,b,a',b' \in \mathbb{N}$ tq. $a+b' = a'+b$.
On a bien sûr $a'+b = a+b'$ donc R est symétrique. Soit $a,b,a',b',a'',b'' \in \mathbb{N}$ tq. $(a;b)\,R\,(a',b')$ et $(a';b')\,R\,(a'',b'')$. On a

$$a+b'+b'' = a'+b+b'' = b+a''+b'$$

Donc, en simplifiant par b', $a+b'' = a''+b$ et $(a;b)\,R\,(a'';b'')$. □

Déf. 2 : $\mathbb{Z} = \mathbb{N}^2/R$ est l'ens. des entiers relatifs.

Prop. 7 : L'appl. $J : \mathbb{N} \to \mathbb{Z}$, $a \mapsto C(a;0)$ (classe de $(a;0)$)
est injective. On identifiera $\mathbb{N}$ avec $J(\mathbb{N})$.

Preuve : si $J(a) = J(b)$ alors $(a;0)\,R\,(b;0)$ donc $a+0 = b+0$. D'où $a=b$. □.

Ainsi, on peut "voir" $\mathbb{N}$ comme une partie de $\mathbb{Z}$.

Addition dans $\mathbb{Z}$: On note par $+_{\mathbb{N}}$ l'add. dans $\mathbb{N}$.
On veut définir sur $\mathbb{Z}$ une add. notée $+_{\mathbb{Z}}$.
Pour $(x,y) \in \mathbb{Z}^2$, $x = C(m;n)$ et $y = C(p;q)$ avec $m,n,p,q \in \mathbb{N}$. On pose

$$x +_{\mathbb{Z}} y = C(m+p;n+q).$$

(on pense à "$m-n+p-q = (m+p)-(n+q)$")

On doit vérifier que cette définition ne dépend pas du choix des représentants dans les classes d'éq.

Soit $n', n', p', q' \in \mathbb{N}$ tq. $(n';n') R (n;n)$ et $(p';q') R (p;q)$. On vérifie donc que

$$(n +_{\mathbb{N}} p ; n +_{\mathbb{N}} q) R (n' +_{\mathbb{N}} p' ; n' +_{\mathbb{N}} q').$$

Par hyp. on sait que $n' +_{\mathbb{N}} n = n +_{\mathbb{N}} n'$, $p' +_{\mathbb{N}} q = p +_{\mathbb{N}} q'$.

Donc

$$n +_{\mathbb{N}} p +_{\mathbb{N}} n' +_{\mathbb{N}} q' = (n +_{\mathbb{N}} n') + (p +_{\mathbb{N}} q') = (n' +_{\mathbb{N}} n) + (p' +_{\mathbb{N}} q)$$

$$= n +_{\mathbb{N}} q +_{\mathbb{N}} n' +_{\mathbb{N}} p'.$$

Donc $+_{\mathbb{Z}}$ est bien définie.

Th. 14 : $(\mathbb{Z}, +_{\mathbb{Z}})$ est un groupe commutatif d'élément neutre $0_{\mathbb{Z}} = J(0_{\mathbb{N}}) = C(0_{\mathbb{N}}; 0_{\mathbb{N}})$.

Précisément : $+_{\mathbb{Z}}$ est associative, commutative, a un élé. neutre $(0_{\mathbb{Z}})$. Tout entier admet un opposé.

Rq. : l'opposé de $C(a;b)$, noté $-C(a;b)$ est $C(b;a)$:

$$C(a;b) +_{\mathbb{Z}} C(b;a) = C(a +_{\mathbb{N}} b ; b +_{\mathbb{N}} a) = C(0;0) = 0_{\mathbb{Z}}$$

Rq. : $\mathbb{Z} = J(\mathbb{N}) \cup (-J(\mathbb{N}))$

où $-J(\mathbb{N}) = \{z \in \mathbb{Z} ; -z \in J(\mathbb{N})\}$.

Comme, pour tout $(a;b) \in \mathbb{N}^2$,

$$J(a +_{\mathbb{N}} b) = C(a+b ; 0) = C(a;b)$$
$$= C(a;0) +_{\mathbb{Z}} C(b;0)$$
$$= J(a) +_{\mathbb{Z}} J(b),$$

$a +_{\mathbb{N}} b$ est l'unique antécédent par J de $J(a) +_{\mathbb{Z}} J(b) \in \mathbb{Z}$.
même chose avec $\times_{\mathbb{N}}$.

Donc, sans perdre d'information, on peut identifier $\mathbb{N}$ à $J(\mathbb{N})$.

La soustraction dans $\mathbb{Z}$ prolonge celle de $\mathbb{N}$ vue dans $J(\mathbb{N})$:

Soit $(a;b) \in \mathbb{N}^2$ avec $b = a+c$, $c \in \mathbb{N}$.

On a $J(b) = J(a +_{\mathbb{N}} c) = J(a) +_{\mathbb{Z}} J(c)$

donc $J(b) + (-J(a)) = J(c)$

Soit $J(b-a) = J(b) - J(a)$.

Ordre dans $\mathbb{Z}$: Pour $(x;y) \in \mathbb{Z}^2$, on dit que $x \leq y$ si $y - x = y + (-x) \in J(\mathbb{N})$.

On remarque que si $x = J(a)$ et $y = J(b)$ avec $(a;b) \in \mathbb{N}^2$,

$$x \leq_{\mathbb{Z}} y \iff a \leq_{\mathbb{N}} b.$$

Donc $\leq_{\mathbb{Z}}$ prolonge $\leq_{\mathbb{N}}$ vue dans $J(\mathbb{N})$.

Th. 15 : $\leq_{\mathbb{Z}}$ est une relation d'ordre total.

* $(\mathbb{Z}, \leq_{\mathbb{Z}})$ n'est pas bien ordonné car il n'a pas de plus petit élt.
* Toute partie non vide majorée (resp. minorée) de $\mathbb{Z}$ admet un plus gd (resp. petit) élt.

Preuve : exercice (en s'inspirant des preuves correspondantes dans $\mathbb{N}$).

Intervalles de $\mathbb{Z}$: même déf. que pour $\mathbb{N}$.

On trouve : le vide et

→ $[\![a;b]\!]$, pour $(a,b) \in \mathbb{Z}$ avec $a \leq b$;

→ $[\![a;\to[\![$, pour $a \in \mathbb{Z}$;

→ $]\!\leftarrow;a]\!]$, pour $a \in \mathbb{Z}$.

($\hookrightarrow \{x \in \mathbb{Z} ; x \leq a\}$.)

Valeur absolue : Pour $x \in \mathbb{Z}$, $\{x;-x\} \cap J(\mathbb{N})$ est un singleton noté $\{|x|\}$.

Pour $(x;y) \in \mathbb{Z}^2$, $|x+y| \leq |x| + |y|$

avec $=$ si $(x;y) \in J(\mathbb{N})^2$

ou si $(x;y) \in (-J(\mathbb{N}))^2$.

Multiplication dans $\mathbb{Z}$

Déf. : Pour $(x,y) \in \mathbb{Z}^2$, on pose :

$$x \times_{\mathbb{Z}} y = \underbrace{|x| \times_{\mathbb{N}} |y|}_{\sim} \quad \text{si } (x;y) \in J(\mathbb{N})^2 \text{ ou } (x;y) \in (-J(\mathbb{N}))^2,$$

$$= -(|x| \times_{\mathbb{N}} |y|) \text{ sinon.}$$

$\sim$

Th 16 : La multiplication dans $\mathbb{Z}$ prolonge celle de $\mathbb{N}$.
Elle est associative, commutative, distributive par rapport à l'addition et a 1 pour élément neutre.

$(\mathbb{Z}, +_{\mathbb{Z}}, \times_{\mathbb{Z}})$ est donc un anneau commutatif.

Preuve : exercice.

Propriétés : $\forall x \in \mathbb{Z}$, $0 \times_{\mathbb{Z}} x = x \times_{\mathbb{Z}} 0 = 0$

$$(-1) \times_{\mathbb{Z}} x = -x$$

$$\forall (x;y) \in \mathbb{Z}^2, \quad (-x) \times_{\mathbb{Z}} y = -(xy) = x \times_{\mathbb{Z}} (-y)$$

et $\quad -(-xy) = xy$.

On définit par récurrence, pour $x \in \mathbb{Z}$, $x^0 = 1$ et $\forall n \in \mathbb{N}$, $x^{n+1} = x^n \times_{\mathbb{Z}} x$.

Prop. 8 : $\mathbb{Z}$ est un anneau intègre :

$$\forall (x;y) \in \mathbb{Z}^2, \quad (x \times_{\mathbb{Z}} y) = 0 \iff (x=0) \text{ ou } (y=0).$$

Preuve : exercice.

Déf. : Un élé. $a \in \mathbb{Z}$ est dit inversible s'il existe $b \in \mathbb{Z}$ t.q. $a \times_{\mathbb{Z}} b = b \times_{\mathbb{Z}} a = 1$.

Prop. : Les élé. inversibles de $\mathbb{Z}$ sont -1 et 1.

Preuve : exercice.

Opérations et ordre :

$\forall (a,b,c) \in \mathbb{Z}^3$, $a+c \leq b+c \iff a \leq b$

$\forall (a;b) \in \mathbb{Z}^2 \times \mathbb{N}^*$, $a \times c \leq b \times c \iff a \leq b$

$\forall (a;b) \in \mathbb{Z}^2$, $a \leq b \iff -a \geq -b$

Preuve : exercice.

Division euclidienne dans $\mathbb{Z}$.

Th. 17 : Soit $(a;b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q;r) \in \mathbb{Z}^2$ t.q.

$$\begin{cases} a = bq + r \\ \text{et } 0 \leq r < |b|. \end{cases}$$

Preuve : on déduit ce résultat de la div. eucl. sur $\mathbb{N}$. D. ✓