DM de logique, théorie des ensembles et fonction

Rendez les exercices dans l'ordre ou chacun sur une feuille séparée (pas tous ensemble en vrac). Ne perdez pas de temps sur les bonus : ce sont des questions intéressantes, mais parfois plus difficiles.

Le barème est indicatif. Il n'est pas nécessaire de tout faire pour obtenir une bonne note. Comme le DM est assez long, la notation sera probablement non linéaire.

À rendre en groupe de 1 à 2.

Ne vous retenez pas de le faire en LaTeX si vous le sentez. Vous gagnerez le bonus de l'indulgence du correcteur.

Exercice 1 : Logique propositionnelle (20 points)

1. Montrer que

$$((\perp \Rightarrow P) \Rightarrow P) \equiv P$$

Solution: La majeure partie de cet exercice avait pour but d'écrire des tables de vérité.

$[P]_\sigma$	$[\perp]_\sigma$	$[(\perp \Rightarrow P)]_\sigma$	$\left[((\perp \Rightarrow P) \Rightarrow P)\right]_\sigma$
ff	ff	tt	ff
tt	ff	tt	tt

Les colonnes de $\left[((\perp \Rightarrow P) \Rightarrow P)\right]_\sigma$ et $[P]_\sigma$ sont les mêmes. Par conséquent, $((\perp \Rightarrow P) \Rightarrow P) \equiv P$.

2. Écrire la négation des formules suivantes :
   1. $(P \Rightarrow Q)$
   2. $(P \wedge (\neg Q))$

3. $\big(P \wedge (Q \wedge R)\big)$
4. $\big(P \vee (Q \wedge R)\big)$
5. $\big((P \wedge Q) \Rightarrow (R \Rightarrow S)\big)$

Solution:

1. On sait que $(P \Rightarrow Q) \equiv \big((\neg P) \vee Q\big)$.

$$\begin{aligned} ((\neg P) \vee Q) &\equiv \Big(\big(\neg(\neg P)\big) \wedge (\neg Q)\Big) \\ &\equiv \big(P \wedge (\neg Q)\big) \end{aligned}$$

2. $$\begin{aligned} \Big(\neg\big(P \wedge (\neg Q)\big)\Big) &\equiv \Big((\neg P) \vee \big(\neg(\neg Q)\big)\Big) \\ &\equiv \big((\neg P) \vee Q\big) \end{aligned}$$

3. $$\begin{aligned} \Big(\neg\big(P \wedge (Q \wedge R)\big)\Big) &\equiv \Big((\neg P) \vee \big(\neg(Q \wedge R)\big)\Big) \\ &\equiv \Big((\neg P) \vee \big((\neg Q) \vee (\neg R)\big)\Big) \end{aligned}$$

4. $$\begin{aligned} \Big(\neg\big(P \vee (Q \wedge R)\big)\Big) &\equiv \Big((\neg P) \wedge \big(\neg(Q \wedge R)\big)\Big) \\ &\equiv \Big((\neg P) \wedge \big((\neg Q) \vee (\neg R)\big)\Big) \end{aligned}$$

5. $$\begin{aligned} \Big(\neg\big((P \wedge Q) \Rightarrow (R \Rightarrow S)\big)\Big) &\equiv \Big((P \wedge Q) \wedge \big(\neg(R \Rightarrow S)\big)\Big) \\ &\equiv \Big((P \wedge Q) \wedge \big(\neg(R \Rightarrow S)\big)\Big) \\ &\equiv \Big((P \wedge Q) \wedge \big(R \wedge (\neg S)\big)\Big) \end{aligned}$$

3. Prouver

$$\begin{aligned} (A \wedge A) &\equiv A \\ (A \vee A) &\equiv A \end{aligned}$$

C'est l'idempotence de $\wedge$ et $\vee$.

Solution:

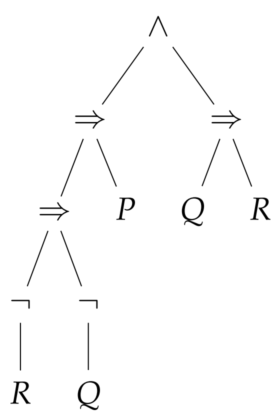
$[A]_\sigma$	$[(A \wedge A)]_\sigma$	$[(A \vee A)]_\sigma$
ff	ff	ff
tt	tt	tt

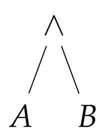
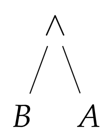
Encore une fois, égalité de colonne...

4. Soit φ la formule

$$\Big(\big(((\neg R) \Rightarrow (\neg Q)) \Rightarrow P\big) \wedge (Q \Rightarrow R)\Big)$$

(a) Écrire φ sous forme d'arbre



Solution: Attention à bien respecter l'ordre avec $\Rightarrow$. Comme chacun sait $(A \wedge B) \equiv (B \wedge A)$ alors on peut réécrire  en , même si avec une approche aussi syntaxique que la notre, c'est pas très classe. Mais $(A \Rightarrow B)$ et $(B \Rightarrow A)$ n'ont rien à voir, donc il faut bien respecter l'ordre.

(b) Donner la table de vérité de φ

Solution:

$[P]_\sigma$	$[Q]_\sigma$	$[R]_\sigma$	$[(\neg R)]_\sigma$	$[(\neg Q)]_\sigma$	$\left[((\neg R) \Rightarrow (\neg Q))\right]_\sigma$
ff	ff	ff	tt	tt	tt
ff	ff	tt	ff	tt	tt
ff	tt	ff	tt	ff	ff
ff	tt	tt	ff	ff	tt
tt	ff	ff	tt	tt	tt
tt	ff	tt	ff	tt	tt
tt	tt	ff	tt	ff	ff
tt	tt	tt	ff	ff	tt

$[P]_\sigma$	$[Q]_\sigma$	$[R]_\sigma$	$\left[\left(((\neg R) \Rightarrow (\neg Q)) \Rightarrow P\right)\right]_\sigma$	$[(Q \Rightarrow R)]_\sigma$
ff	ff	ff	ff	tt
ff	ff	tt	ff	tt
ff	tt	ff	tt	ff
ff	tt	tt	ff	tt
tt	ff	ff	tt	tt
tt	ff	tt	tt	tt
tt	tt	ff	tt	ff
tt	tt	tt	tt	tt

$[P]_\sigma$	$[Q]_\sigma$	$[R]_\sigma$	$[\varphi]_\sigma$
ff	ff	ff	ff
ff	ff	tt	ff
ff	tt	ff	ff
ff	tt	tt	ff
tt	ff	ff	tt
tt	ff	tt	tt
tt	tt	ff	ff
tt	tt	tt	tt

(c) Cette formule est-elle une tautologie ? Justifier.

Solution: Ce n'est pas une tautologie : certains environnements rendent φ faux. Par exemple

$$P \mapsto \textit{ff}$$
$$Q \mapsto \textit{ff}$$
$$R \mapsto \textit{ff}$$

J'ai très rarement vu de contre-exemple, c'est pourtant la preuve la plus convaincante (et souvent la plus simple).

(d) Cette formule est-elle une contradiction ? Justifier.

Solution: Ce n'est pas une contradiction : certains environnements rendent φ vrai. Par exemple

$$P \mapsto \textit{tt}$$
$$Q \mapsto \textit{tt}$$
$$R \mapsto \textit{tt}$$

5. Dans cette question, on va se donner pour but de prouver qu'il existe au moins une formule pour n'importe quelle fonction des variables dans $\{\textit{tt}, \textit{ff}\}$
On pose $\mathcal{A} = \{x_1, \ldots, x_n\}$ un alphabet de n variables logiques.

(a) Trouver une formule qui ne soit vraie que pour une unique assignation des variables $x_1 = v_1, \ldots, x_n = v_n$ et fausse dans tous les autres cas. On pourra illustrer sur des exemples.

Solution: Il suffit de prendre

$$x_1^* \wedge \ldots \wedge x_n^*$$

avec $x_i^* = \begin{cases} x_i & \text{si } v_i = \textit{tt} \\ (\neg x_i) & \text{si } v_i = \textit{ff} \end{cases}$

(b) Soit $f : \mathcal{A} \to \{\textit{tt}, \textit{ff}\}$. Se convaincre qu'on peut écrire f comme la disjonction $f_1 \vee \ldots \vee f_m$ d'un certain nombre de fonctions f_i qui ne sont vraies que pour une unique assignation. Conclure. Exemples aussi.

Solution: Pour chaque assignation $x_1 = v_{1,j}, \ldots, x_n = v_{n,j}$ qui rend f vraie, on construit $f_j = x_{1,j}^* \wedge \ldots \wedge x_{n,j}^*$.

Exercice 2 : Fonctions (15 points)

1. Soit
$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} A$$
On suppose que $h \circ g \circ f$ et $g \circ f \circ h$ sont injectives et $f \circ h \circ g$ est surjective. Montrer que f, g et h sont bijectives.

Solution: $h \circ g \circ f$ est injective donc f est injective. D'autre part $f \circ h \circ g$ est surjective, donc f est surjective, donc bijective.

Donc $h \circ g$ est injective et surjective donc bijective. h est donc surjective et g injective. De plus h est injective. puisque $g \circ f \circ h$ est injective. Donc h est bijective, donc g est bijective puisque $h \circ g$ l'est.

2. Soit
$$\begin{aligned} f : [1; +\infty[&\to [0; +\infty[\\ x &\mapsto x^2 - 1 \end{aligned}$$
f est elle injective, surjective, bijective ?

Solution:
- Injectivité : Soit $(x, y) \in [1; +\infty[^2$. On suppose $f(x) = f(y)$.
$$\begin{aligned} x^2 - 1 &= y^2 - 1 \\ x^2 &= y^2 \\ x = y &\text{ ou } x = -y \end{aligned}$$
Or $x > 0$ et $y > 0$. Donc $x = y$. Donc f est injective.
- Surjective : Soit $y \in [0; +\infty[$. On cherche x tel que $f(x) = y$, ie. $x^2 - 1 = y$, $x^2 = y + 1$. $x = \sqrt{y+1}$ convient. f est surjective.
- f est donc bijective.

3. (5 points bonus) Trouver une bijection entre $\mathbb{R}$ et $\mathbb{R}^2$.

Exercice 3 : Relations (15 points)

1. On dit que m divise n, et on écrit $m|n$ si $\exists k \in \mathbb{Z} : mk = n$. La relation "divise" est-elle une relation d'ordre sur $\mathbb{N}$? Sur $\mathbb{Z}$? Est-elle totale ?

> **Solution:**
> — Sur $\mathbb{N}$,
>   — Réflexivité : pour tout n, n divise n.
>   — Antisymétrie : soit n et m. Si n divise n et m divise n, on a $m = kn$ et $n = jm$. Donc $n = kjn$, donc $kj = 1$. Avec $(k, j) \in \mathbb{N}^2$, $j = k = 1$. Donc $n = m$.
>   — Transitivité : soit m, n et p. On suppose que $km = n$ et $jn = p$, donc $(kj)m = p$, donc m divise p.
>
>   C'est donc une relation d'ordre sur $\mathbb{N}$.
> — On a -1 divise 1 et 1 divise -1, donc la relation n'est pas antisymétrique, ce n'est donc pas un ordre sur $\mathbb{Z}$. C'est toutefois un préordre (réflexif et transitif).
> — L'ordre sur $\mathbb{N}$ n'est pas total : 5 et 7 ne sont pas comparables par exemple.

2. Trouver le(s) plus petit(s) et plus grand(s) éléments de $\mathbb{N}$ selon la relation $|$.

> **Solution:** Pour tout $n \in \mathbb{N}$, on a $n \cdot 0 = 0$. Donc 0 est le plus grand élément.
> Pour tout $n \in \mathbb{N}$, on a $1 \cdot n = n$. Donc 1 est le plus petit élément.

3. (5 points bonus) Cet ordre est il bien fondé ?

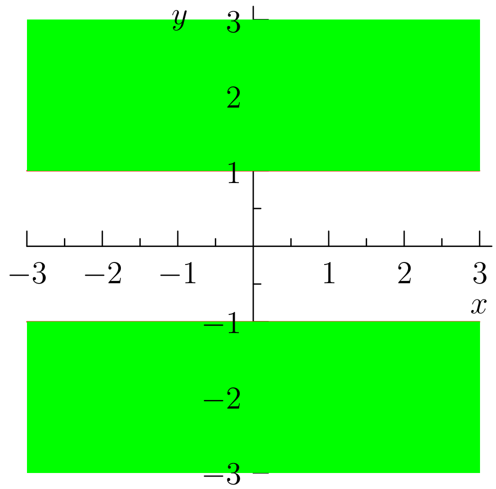
> **Solution:** Oui, car si n divise m, alors $n \leqslant m$. Donc toute suite strictement décroissante pour la relation « divise » est strictement décroissante pour $\leqslant$.

Exercice 4 : Théorie des ensembles (15 points)

1. Dessiner les parties suivantes de $\mathbb{R}^2$

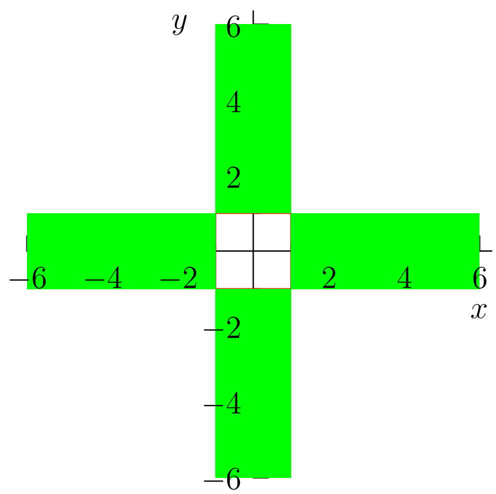
(a) $\complement\left(\mathbb{R} \times [-1;1]\right)$

Solution: On note que les bordures (en rouge), ne font pas partie de l'ensemble.



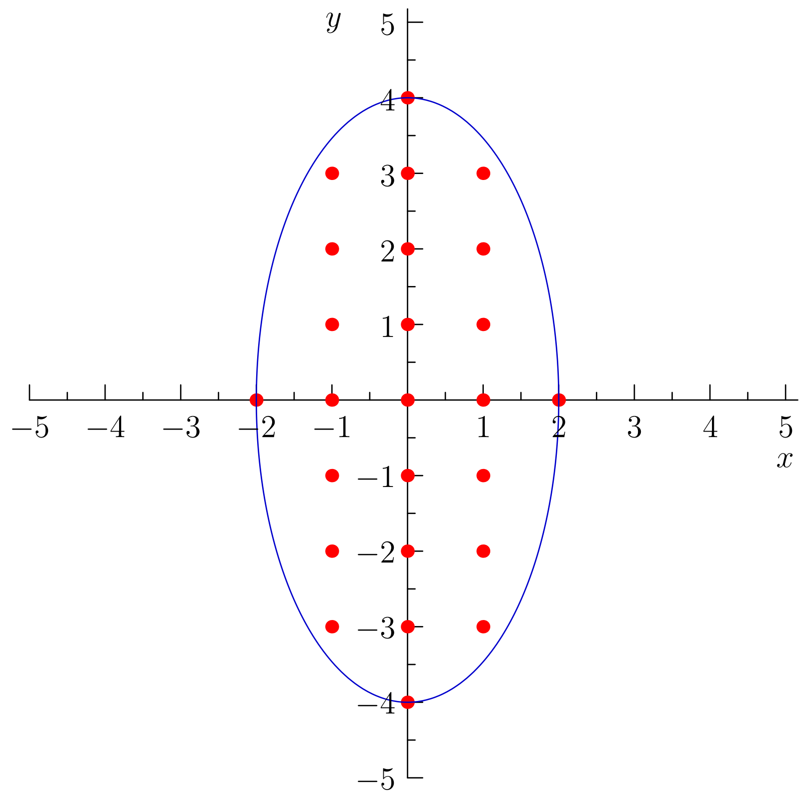
(b) $\left([-1,1] \times \mathbb{R}\right) \Delta \left(\mathbb{R} \times [-1,1]\right)$

Solution: On note que les bordures (en rouge), ne font pas partie de l'ensemble.



(c) $\left\{(a,b) \in \mathbb{Z}^2 \;\middle|\; a^2 + \frac{1}{4}b^2 \leqslant 4\right\}$

Solution:



2. (5 points bonus) (a) Montrer qu'il existe une injection de E dans $\mathcal{P}(E)$.

Solution: Il suffit de prendre la fonction

$$\begin{aligned} i : E &\to \mathcal{P}(E) \\ x &\mapsto \{x\} \end{aligned}$$

On prouve que c'est une injection, car si $i(x) = i(y)$, alors $\{x\} = \{y\}$, donc $x = y$.

(b) On pose $A = \left\{x \in E \,\middle|\, x \notin f(x)\right\}$. S'en servir pour montrer l'absence de bijection de E dans $\mathcal{P}(E)$ (théorème de Cantor).

Solution: Soit f une application de E dans $\mathcal{P}(E)$. Montrons que f ne peut pas être surjective. On va montrer que A n'a pas d'antécédent par f. Supposons que A a un antécédent a :
— si $a \in A$, alors $a \notin A$;
— si $a \notin A$, alors $a \in A$.
Ce qui est absurde. Ce qui prouve le théorème.

Exercice 5 : Récurrence (15 points)

1. On définit la fonction $\mathscr{A}$ d'ACKERMANN-PÉTER par

$$\begin{aligned}\mathscr{A} : \mathbb{N}^2 &\to \mathbb{N}\\ (m,n) &\mapsto \begin{cases} n+1 & \text{si } m=0\\ \mathscr{A}(m-1,1) & \text{si } m>0 \text{ et } n=0\\ \mathscr{A}(m-1,\mathscr{A}(m,n-1)) & \text{si } m>0 \text{ et } n>0\end{cases}\end{aligned}$$

(a) Montrer que $\forall n \in \mathbb{N}, \mathscr{A}(1,n) = 2+(n+3)-3$.

Solution:
— Initialisation $n=0$. $\mathscr{A}(1,0) = \mathscr{A}(0,1) = 2 = 2+(0+3)-3$. Ok.
— Hérédité. Soit $n \in \mathbb{N}$, on suppose la propriété vraie au rang n.

$$\begin{aligned}\mathscr{A}(1,n+1) &= \mathscr{A}(0,\mathscr{A}(1,n))\\ &= \mathscr{A}(0,\mathscr{A}(1,n))\\ &= \mathscr{A}(0,2+(n+3)-3)\\ &= 2+(n+3)-3+1\\ &= 2+((n+1)+3)-3\end{aligned}$$

Ok.

(b) Montrer que $\forall n \in \mathbb{N}, \mathscr{A}(2,n) = 2(n+3)-3$.

Solution:

— Initialisation $n = 0$. $\mathscr{A}(2,0) = \mathscr{A}(1,1) = \mathscr{A}(0,\mathscr{A}(1,0)) = \mathscr{A}(0,\mathscr{A}(0,1)) = \mathscr{A}(0,1)+1 = 1+1+1 = 3$

— Hérédité. Soit $n \in \mathbb{N}$, on suppose la propriété vraie au rang n.

$$\begin{aligned}
\mathscr{A}(2,n+1) &= \mathscr{A}(1,\mathscr{A}(2,n)) \\
&= \mathscr{A}(1,2(n+3)-3) \\
&= \mathscr{A}(0,\mathscr{A}(1,2(n+3)-4)) \\
&= \mathscr{A}(1,2(n+3)-4)+1 \\
&= 2+(2(n+3)-4+3)-3+1 \\
&= 2+(2(n+3)-1)-3+1 \\
&= 2(n+3)-3+2 \\
&= 2((n+1)+3)-3
\end{aligned}$$

Ok.

2. On pose

$$\begin{aligned}
H_n :\ & \mathbb{N}^2 \to \mathbb{N} \\
& (a,b) \mapsto \begin{cases} b+1 & \text{si } n=0 \\ a & \text{si } n=1 \text{ et } b=0 \\ 0 & \text{si } n=2 \text{ et } b=0 \\ 1 & \text{si } n \geqslant 3 \text{ et } b=0 \\ H_{n-1}(a,H_n(a,b-1)) & \text{sinon.} \end{cases}
\end{aligned}$$

(a) Montrer que $\forall (a,b) \in \mathbb{N}^2, H_1(a,b) = a+b$.

Solution: Récurrence sur b

— Initialisation : $H_1(a,0) = a$.

— Hérédité : Soit $b \in \mathbb{N}$, on suppose que la propriété est vraie au rang b.

$$\begin{aligned}
H_1(a,b+1) &= H_0(a,H_2(a,b)) \\
&= H_n(a,b)+1 \\
&= a+b+1
\end{aligned}$$

Ok.

(b) Montrer que $\forall (a,b) \in \mathbb{N}^2, H_2(a,b) = ab$.

Solution: Récurrence sur b

— Initialisation : $H_2(a,0) = 0$.

— Hérédité : Soit $b \in \mathbb{N}$, on suppose que la propriété est vraie au rang b.

$$\begin{aligned} H_2(a,b+1) &= H_1(a, H_2(a,b)) \\ &= H_1(a, ab) \\ &= a + ab \\ &= a(b+1) \end{aligned}$$

Ok.

(c) Montrer que $\forall (a,b) \in \mathbb{N}^2, H_3(a,b) = a^b$.

Solution: Récurrence sur b

— Initialisation : $H_3(a,0) = 1$.

— Hérédité : Soit $b \in \mathbb{N}$, on suppose que la propriété est vraie au rang b.

$$\begin{aligned} H_3(a,b+1) &= H_2(a, H_3(a,b)) \\ &= H_2(a, a^b) \\ &= aa^b \\ &= a^{b+1} \end{aligned}$$

Ok.

(d) Comprendre comment ça continue : H_n est l'itéré de l'opérateur H_{n-1}. Ne pas hésiter à me demander si besoin.

(e) Montrer

$$\forall i \in \mathbb{N} \setminus \{0,1\}, H_i(2,1) = 2$$

Solution: Soit $i \in \mathbb{N} \setminus \{0,1\}$,
$H_i\left(2,1\right) = H_{i-1}\left(2, H_i\left(2,0\right)\right)$.

— Si $i = 2$: $H_1\left(2, H_2(2,0)\right) = H_1(2,0) = 2$
— Si $i = 3$: $H_2\left(2, H_3(2,0)\right) = H_2(2,1) = 2$, en se ramenant au cas précédent.
— Si $i > 3$: $H_{i-1}\left(2, H_i(2,0)\right) = H_{i-1}(2,1) = 2$, par une récurrence évidente sur i.

(f) Montrer

$$\forall i \in \mathbb{N}^*, H_i(2,2) = 4$$

Solution: Soit $i \in \mathbb{N}^*$,
$H_i(2,2) = H_{i-1}\left(2, H_i(2,1)\right) = H_{i-1}\Big(2, H_{i-1}\left(2, H_i(2,0)\right)\Big)$.
— Si $i = 1$: $H_0\Big(2, H_0\left(2, H_1(2,0)\right)\Big) = H_0\left(2, H_0(2,2)\right) = H_0(2,3) = 4$
— Si $i = 2$: $H_1\Big(2, H_1\left(2, H_2(2,0)\right)\Big) = H_1\left(2, H_1(2,0)\right) = H_1(2,2) = 4$, en se ramenant au cas précédent.
— Si $i \geqslant 3$: $H_{i-1}\Big(2, H_{i-1}\left(2, H_i(2,0)\right)\Big) = H_{i-1}(2,2) = 4$, par une récurrence évidente sur i.

(g) (5 points bonus) Trouver un ordre $\sqsubseteq$ sur $\mathbb{N}^2$ tel que

$$\forall (n,m,k) \in \mathbb{N}^3, \begin{cases} (m,k) & \sqsubseteq (m+1,n) \text{ et} \\ (m,n) & \sqsubseteq (m,n+1) \end{cases}$$

Solution: Il suffit de prendre l'ordre lexicographique :

$$(a,b) \sqsubseteq (c,d) :\Leftrightarrow \begin{cases} a < c & \text{ou} \\ a = c \text{ et } b = d \end{cases}$$

(h) (5 points bonus) Montrer que cet ordre est bien fondé.

Solution: On va prouver qu'il n'existe pas de suite de $\mathbb{N}^2$ strictement décroissante infinie au sens de $\sqsubseteq$. Pour cela, on va prouver par récurrence forte sur $\mathbb{N}$ le prédicat P_n : « Il n'existe pas de suite infinie de $\mathbb{N}^2$ strictement décroissante pour $\sqsubseteq$ dont le premier terme est de la forme (n,k) avec $k \in \mathbb{N}$ ».

— Initialisation : Pour $n = 0$. On cherche donc à prouver qu'il n'existe pas de suite strictement décroissante commençant par $(0,k)$ où k est un naturel. Tous les éléments strictement inférieurs sont de la forme $(0,j)$ avec $j < k$. Il existe donc un nombre fini de ces éléments et par conséquent, il n'existe pas de suite infinie strictement décroissante.

— Hérédité : Soit $n \in \mathbb{N}$. On suppose la propriété vraie jusqu'au rang n. On veut la prouver au rang $n+1$. Soit $k \in \mathbb{N}$. On veut prouver qu'il n'existe pas de suite strictement décroissante commençant par $(n+1,k)$. Les éléments strictement plus petits que $(n+1,k)$ sont soit de la forme (a,b) avec $a < n+1$ ou $(n+1,b)$ avec $b < k$. Il n'existe qu'un nombre fini de cette dernière catégorie, une fois arrivée à $(n+1,0)$, la seule solution est de passer à des éléments de la forme (a,b) avec $a < n+1$. On appelle (x,y) le premier élément qui n'est pas de la forme $(n+1,j)$. On utilise alors la proposition P_x pour prouver qu'il n'existe pas de suite strictement décroissante commençant par (x,y). Il n'existe donc pas de suite strictement décroissante commençant par $(n+1,k)$.

La propriété est donc vraie à tous les rangs. $\sqsubseteq$ est donc bien fondé.

(i) (5 points bonus) Montrer que

$$\forall (m,n) \in \mathbb{N}^2, \mathscr{A}(m,n) = H_m(2,n+3) - 3$$

Solution: On prouve cette égalité par induction sur $\mathbb{N}^2$.
Si $m = 0$, $\forall n \in \mathbb{N}, H_0\left(2,(n+3)\right) - 3 = (n+3)+1-3 = n+1 = \mathscr{A}(m,n)$
Si $m > 0$ et $n = 0$, $H_m(2,3) - 3 = H_{m-1}\left(2, H_m(2,2)\right) - 3 = H_{m-1}(2,4) - 3 = \mathscr{A}(m-1,1)$

Sinon,

$$\begin{aligned} H_m\left(2, n+3\right) - 3 &= H_{m-1}\left(2, H_m\left(2, (n-1)+3\right)\right) \\ &= \mathscr{A}\left(m-1, \mathscr{A}\left(m, n-1\right)\right) \end{aligned}$$