Ordre et induction

1 Relations

1.1 En général

Définition (*relation n-aire*) :

Soient $X \neq \emptyset$ et $n \in \mathbb{N}^*$. On dit que $\mathcal{R}$ est une relation n-aire sur X ssi $\mathcal{R} \subseteq X^n$.

L'entier n est alors appelé arité de la relation.
De plus, si $(x_i)_{i\in[\![1..n]\!]} \in \mathcal{R}$, on dit que les éléments x_1, x_2,..., x_n vérifient la relation $\mathcal{R}$.

Exemples : • $\mathcal{R}_1 = \{(a,b) \in \mathbb{Z}^2 \,|\, a \equiv b\ [3]\}$.
• $\mathcal{R}_2 = \{(a,b,c) \in \mathbb{R}^3 \,|\, a+b=c\}$ est une relation ternaire sur $\mathbb{R}$.

On a par exemple $(1,2,3) \in \mathcal{R}_1$, mais $(1,3,2) \notin \mathcal{R}_1$.

Définitions (*relations binaires, vocabulaire et propriétés*) :

Soit $X \neq \emptyset$ et $\mathcal{R}$ est une relation binaire sur X. Pour $(x,y) \in X^2$, on note $x\,\mathcal{R}\,y$ ssi $(x,y) \in \mathcal{R}^2$ c'est-à-dire x et y vérifient $\mathcal{R}$. Alors, on dira que :
- $\mathcal{R}$ est réflexive ssi $\forall\, x \in X,\ x\,\mathcal{R}\,x$.
- $\mathcal{R}$ est symétrique ssi $\forall\,(x,y) \in X^2,\ x\,\mathcal{R}\,y \iff y\,\mathcal{R}\,x$.
- $\mathcal{R}$ est antisymétrique ssi $\forall\,(x,y) \in X^2,\ x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,x \implies x = y$.
- $\mathcal{R}$ est transitive ssi $\forall\,(x,y,z) \in X^3,\ x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,z \implies x\,\mathcal{R}\,z$.

Définitions (*relation d'équivalence, relation d'ordre*) :

Soit $\mathcal{R}$ une relation binaire sur un ensemble X non vide. Alors :
- $\mathcal{R}$ est une relation d'ordre ssi $\mathcal{R}$ est réflexive, antisymétrique et transitive.
- $\mathcal{R}$ est une relation d'équivalence ssi $\mathcal{R}$ est réflexive, symétrique et transitive.

Définition (*relation induite*) :

Soit $\mathcal{R}$ une relation binaire sur un ensemble X non vide et $Y \subseteq X$ avec $Y \neq \emptyset$. Alors, $\mathcal{P} = \mathcal{R} \cap Y^2$ définit une relation binaire sur Y qui a les mêmes propriétés que $\mathcal{R}$ (au sens des quatre définies précédemment), et que l'on appellera parfois relation induite par $\mathcal{R}$ sur Y.

Exercice : Soit $X \neq \emptyset$ un ensemble et $\mathcal{R}$ une relation binaire sur X. On note :

- $\mathcal{R}_r = \mathcal{R} \cup \{(x,x) \,|\, x \in X\}$
- $\mathcal{R}_s = \mathcal{R} \cup \{(x,y) \,|\, (y,x) \in \mathcal{R}\}$
- $\mathcal{R}_t = \bigcup_{n\in\mathbb{N}^*} \mathcal{R}_n$ où $\mathcal{R}_1 = \mathcal{R}$ et $\forall\, n \in \mathbb{N}^*,\ \mathcal{R}_{n+1} = \mathcal{R}_n \cup \left\{ (x,z) \in X^2 \,\middle|\, \exists\, y \in X,\ \begin{matrix}(x,y) \in \mathcal{R} \\ (y,z) \in \mathcal{R}_n\end{matrix} \right\}$

Montrer que $\mathcal{R}_r$ est réflexive, $\mathcal{R}_s$ symétrique et $\mathcal{R}_t$ transitive. Pour la transitivité, on pourra en particulier utiliser le lemme suivant après l'avoir démontré :

$$\forall\, n \in \mathbb{N}^*,\ \mathcal{R}_n = \left\{ (x,z) \in X^2 \;\middle|\; \exists\, n' \leq n,\ \exists\, (y_i)_{i\in[0..n']} \in X^{n'} \text{ tels que : } \begin{array}{l} y_0 = x \\ y_{n'} = z \\ \forall\, i \in [0..n'[,\ y_i \,\mathcal{R}\, y_{i+1} \end{array} \right\}$$

1.2 Relations d'équivalence

On considère un ensemble $X \neq \emptyset$ et $\mathcal{R}$ une relation d'équivalence sur X.

Définition (*classes d'équivalence*) :

Pour $x \in X$, on définit la classe d'équivalence de x pour la relation $\mathcal{R}$, notée $[x]$ ou $\dot{x}$, par :

$$[x] = \dot{x} = \{y \in X \,|\, x\,\mathcal{R}\,y\}$$

Propriété : Pour $(x,y) \in X^2$, soit $y \in \dot{x}$ auquel cas $\dot{x} = \dot{y}$, ou bien $y \notin \dot{x}$ auquel cas $\dot{x} \cap \dot{y} = \emptyset$.

Corollaire (*espace quotient*) :

L'ensemble $\{\dot{x} \,|\, x \in X\}$ des classes d'équivalences de la relation $\mathcal{R}$ forme une partition de X. On l'appelle ensemble quotient ou espace quotient de X par la relation $\mathcal{R}$ et on le note $X/\mathcal{R}$.

Définition (*passage au quotient*) :

Soit X et Y deux ensembles, $f \in \mathcal{F}(X,Y)$ et $\mathcal{R}$ une relation d'équivalence sur X.
On dit que f passe au quotient si elle est constante sur les classes d'équivalence, c'est-à-dire :

$$\forall\, (x,x') \in X^2,\ x\,\mathcal{R}\,x') \Longrightarrow f(x) = f(x')$$

ou encore, de manière totalement équivalente :

$$\forall\, (x,x'),\ \dot{x} = \dot{x}' \Longrightarrow f(x) = f(x')$$

Si f passe au quotient, on peut définir sur l'espace quotient la fonction :

$$\bar{f} = \begin{pmatrix} X/\mathcal{R} \to Y \\ \dot{x} \mapsto f(x) \end{pmatrix}$$

Remarque : Passer de f à $\bar{f}$ permet de "gagner en injectivité", au sens où l'on "regroupe" tous les antécédents d'un élément donné de l'ensemble d'arrivée dans une seule classe. Attention cependant, $\bar{f}$ n'est pas nécessairement injective pour autant.

Propriété : Pour toute fonction $f \in \mathcal{F}(X,Y)$ passant au quotient, on a $f(X) = \bar{f}(X/\mathcal{R})$.

1.3 Relations d'ordre

On considère $(X, \leqslant)$ un ensemble ordonné (i.e. muni d'une relation d'ordre notée $\leqslant$), ainsi que $Y \subseteq X$. On note de plus $(Y, \leqslant)$ l'ensemble ordonné induit.

1.3.1 Élements particuliers

Définitions (*majorants et minorants*) :

Soit $x \in X$ quelconque.
- x est un minorant de Y ssi $\forall\, y \in Y,\ x \leqslant y$.
- x est un majorant de Y ssi $\forall\, y \in Y,\ y \leqslant x$.

Dans la suite de ce cours, on notera pour Z un ensemble quelconque, $\mathcal{M}\mathrm{in}(Z)$ l'ensemble de ses minorants et $\mathcal{M}\mathrm{aj}(Z)$ son ensemble de majorants. Alors :
- Y est majoré s'il admet un majorant (*i.e.* $\mathcal{M}\mathrm{in}(Y) \neq \emptyset$)
- Y est minoré s'il admet un minorant (*i.e.* $\mathcal{M}\mathrm{aj}(Y) \neq \emptyset$)
- Y est borné s'il est à la fois majoré et minoré.

Définitions (*minimalité, maximalité, plus grand et plus petit élément*) :

Soit $x \in X$ et $y \in Y$. Alors :
- x est un plus petit élément de Y ssi x est un minorant de Y et $x \in Y$.
- x est un plus grand élément de Y ssi x est un majorant de Y et $x \in Y$.
- y est minimal (dans Y) ssi il n'y a pas d'autre élément plus petit, autrement dit :

$$\forall\, y' \in Y,\ y' \leqslant y \Longrightarrow y' = y \text{ ou encore } \forall\, y' \in Y, y' \neq y \Longrightarrow y' \not\leqslant y$$

- y est maximal (dans Y) ssi il n'y a pas d'autre élément plus petit, c'est-à-dire :

$$\forall\, y' \in Y,\ y \leqslant y' \Longrightarrow y' = y \text{ soit encore } \forall\, y' \in Y, y' \neq y \Longrightarrow y \not\leqslant y'$$

Propriété (*unicité du minimum/maxmimum*) :

Si Y admet un plus petit élément (resp. un plus grand élément), alors il est unique : on l'appelle dans ce cas minimum (resp. maximum) de Y et on le note $\min(Y)$ (resp. $\max(Y)$).

Remarque : En revanche, il n'y a pas toujours unicité des éléments minimaux et maximaux.

Définition (*bornes supérieure et inférieure*) :

On dit que :
- Y admet une borne supérieure si $\mathcal{M}\mathrm{aj}(Y)$ admet un plus petit élément, noté alors $\sup(Y)$.
- Y admet une borne inférieure si $\mathcal{M}\mathrm{in}(Y)$ admet un plus grand élément, qu'on note $\inf(Y)$.

On a donc, lorsque cela existe, $\sup(Y) = \min(\mathcal{M}\mathrm{aj}(Y))$ et $\inf(Y) = \max(\mathcal{M}\mathrm{in}(Y))$.

Remarque : Les bornes inférieure et supérieure d'un ensemble n'appartiennent pas nécessairement à cet ensemble, et elles n'existent pas toujours non plus. Prenons par exemple $Y = \{u_n \,|\, n \in \mathbb{N}\}$ où on a défini $u = (\lfloor 10^n\sqrt{2}\rfloor/10^n)_{n\in\mathbb{N}}$: Y n'a pas de borne sup dans $\mathbb{Q}$, mais elle en a une dans $\mathbb{R}$ qui vaut $\lim_{n\to+\infty} u_n = \sqrt{2}$.

1.3.2 Ordre total

Définition (*relation d'ordre totale*) :

Une relation d'ordre $\mathcal{R}$ sur X est dite totale ssi $\forall\,(x,y) \in X^2$, $x\,\mathcal{R}\,y$ ou $y\,\mathcal{R}\,x$.

Propriété :

Si $\leqslant$ est une relation d'ordre totale sur Y, alors :

$$\forall\, y \in Y,\ y \text{ minimal dans } Y \Longrightarrow y \text{ plus petit élément de } Y$$
$$y \text{ maximal dans } Y \Longrightarrow y \text{ plus grand élément de } Y$$

Preuve :
Soit $y \in Y$. Supposons que y soit minimal dans Y, *i.e.* $\forall\, y' \in Y,\ y \neq y' \Longrightarrow y' \not\leqslant y$.

• Soit alors $y' \in Y \backslash \{y\}$. Comme l'ordre est total, $y \leq y'$ ou $y' \leqslant y$, or $y' \not\leqslant y$ donc on a $y \leqslant y'$.
• De plus, $y \leq y$ par réflexivité.

On a donc $\forall\, y' \in Y,\ y \leqslant y'$, ce qui prouve que y est bien le plus petit élément de Y. La démonstration est identique pour la seconde implication.

Remarque : Il est immédiat que les implications réciproques sont vraies, même lorsque $\leqslant$ n'est pas une relation d'ordre totale : ainsi, pour un ordre total, être minimal ou maximal est exactement équivalent à être le minimum ou le maximum.

Corollaire (*unicité de l'élément minimal/maximal*) :

Si l'ordre $\leqslant$ est total, il y a unicité des éléments minimaux et maximaux (en cas d'existence).

1.3.3 Ordre bien fondé

$(X, \leqslant)$ et $(Y, \preccurlyeq)$ désignent maintenant deux ensembles ordonnés quelconques.

Notation (*ordre strict*) :

Pour $(x, x') \in X^2$, on note $x < x'$ ssi $x \leqslant x'$ et $x \neq x'$.
On définit de même la notation $y \prec y'$ pour y, y' des éléments de Y.

Définitions (*croissance, croissance stricte*) :

Soit $f \in \mathcal{F}(X, Y)$.
- f est croissante ssi $\forall\, (x, x') \in X^2,\ x \leqslant x' \Longrightarrow f(x) \preccurlyeq f(x')$.
- f est strictement croissante ssi $\forall\, (x, x') \in X^2,\ x < x' \Longrightarrow f(x) \prec f(x')$.

On étend ces définitions aux suites de $X^{\mathbb{N}}$ vues comme des fonctions de $(\mathbb{N}, \leq)$ vers $(X, \leqslant)$, $\leq$ désignant l'ordre usuel sur les réels.

Exemple : Considérons la fonction :

$$id = \begin{pmatrix} (\mathbb{N}^*, |) \to (\mathbb{N}^*, \leq) \\ n \mapsto n \end{pmatrix}$$

Elle est croissante car $\forall\, (a, b) \in (\mathbb{N}^*)^2,\ a|b \Longrightarrow a \leq b$.
En fait, elle est même strictement croissante puisqu'elle est injective.

Exercice : Pour $f \in \mathcal{F}(X, Y)$, montrer l'implication :

$$X \text{ ordre total et } f \text{ strictement croissante} \Longrightarrow f \text{ injective}$$

et trouver un contre-exemple quand l'ordre n'est pas total.

Correction : Pour le contre-exemple, on peut considérer l'une des fonctions suivantes :

$$f = \begin{pmatrix} (\mathbb{N}^*, |) \to (\mathbb{N}, \leq) \\ n \mapsto \lfloor n/2 \rfloor \end{pmatrix} \text{ et } g = \begin{pmatrix} (\mathbb{N}^*, |) \to (\mathbb{N}, \leq) \\ n \mapsto \text{Card}\left\{ d \in \mathbb{N} \,\middle|\, d|n \right\} \end{pmatrix}$$

Définition (*ordre bien fondé*) :

On dit que l'ordre $\leqslant$ est bien fondé sur X ssi $\forall\, A \subseteq X$ non vide, A admet un élément minimal.

Propriété (*caractérisation séquentielle des ordres bien fondés*) :

L'ordre $\leqslant$ est bien fondé ssi il n'existe aucune suite de $X^{\mathbb{N}}$ strictement décroissante pour $\leqslant$.

Preuve :
($\Rightarrow$) : Supposons que $(X, \leqslant)$ est bien fondé et supposons par l'absurde qu'il existe une suite $(u_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$ strictement décroissante. On pose alors $A = \{u_n \,|\, n \in \mathbb{N}\} \subseteq X$.

$A \neq \emptyset$ donc il existe a^* un élément minimal de A. Par définition de A, il existe $n^* \in \mathbb{N}$ tel que $a^* = u_{n^*}$. De plus, par stricte décroissance de u, on a $u_{n^*+1} < u_{n^*} = a^*$.

Or, $u_{n^*+1} \in A$, ce qui contredit la minimalité de a^*.

($\Leftarrow$) : Montrons plutôt la contraposée : supposons que $(X, \leqslant)$ n'est pas bien fondé.
Par définition, il existe donc $A \subseteq X$ non vide tel que A n'admet aucun élément minimal.

Comme $A \neq \emptyset$, il existe $a_0 \in A$. a_0 n'est pas minimal donc il existe $a_1 \in A$ tel que $a_1 < a_0$. De même, a_1 n'est pas minimal donc il existe $a_2 \in A$ tel que $a_2 < a_1$, et ainsi de suite.

En réitérant ce processus, on construit une suite $(a_n)_{n\in\mathbb{N}}$ de $A^{\mathbb{N}} \subseteq X^{\mathbb{N}}$ qui est bien strictement décroissante.

Exemples : • $(\mathbb{Z}, \leq)$ n'est pas bien fondé (prendre $(-n)_{n\in\mathbb{N}}$).
• $(\mathbb{R}^+, \leq)$ non plus (prendre $(1/n)_{n\in\mathbb{N}}$).
• $(\mathbb{N}, \leq)$ est bien fondé (*cf.* principe de descente infinie de Fermat).
• $(\mathbb{N}, |)$ est lui aussi bien fondé.

Remarque : Si X est fini, alors $(X, \leqslant)$ est automatiquement bien fondé.

1.3.4 Ordres produit et lexicographique

Soit $n \in \mathbb{N}^*$ et $(X_i, \leqslant_i)_{i\in[1..n]}$ une famille d'ensembles ordonnés. On note $Y = \prod_{i=1}^{n} X_i$.

Définition (*ordre produit*) :

La relation $\mathcal{R}$ définie sur Y par :

$$\forall\,(a,b) \in Y^2,\ a\,\mathcal{R}\,b \iff \forall\, i \in [1..n], a_i \leqslant_i b_i$$

est une relation d'ordre appelée ordre produit des $\leqslant_i$ sur Y.

Définition (*ordre lexicographique*) :

La relation $\mathcal{R}'$ définie sur Y par :

$$\forall\,(a,b) \in Y^2,\ a\,\mathcal{R}'\,b \iff a = b \text{ ou } \exists\, j \in [1..n] \text{ tel que } (\forall\, i \in [1..j[,\ a_j = b_j \text{ et } a_i <_j b_i)$$

est une relation d'ordre sur Y appelée ordre lexicographique sur Y.

Remarque : De manière alternative, on peut définir l'ordre lexicographique sur Y par :

$$\forall\,(a,b) \in Y^2,\ a\,\mathcal{R}'\,b \iff \exists\, j \in [1..n+1],\ \forall\, i \in [1..j[,\ a_i = b_i \text{ et } (j = n+1 \text{ ou } a_j <_j b_j)$$

Les deux définitions sont alors équivalentes, à condition de donner du sens à la proposition "$j = n+1$ ou $a_j <_j b_j$" : il s'agit d'une évaluation paresseuse (en effet $\leqslant_{n+1}$ n'a pas été défini).

Exemple : • $(0,1,3) < (0,1,4)$ pour les ordres produit *et* lexicographique sur $\mathbb{N}^3$.
• $(\mathtt{a},2) < (\mathtt{b},1)$ pour l'ordre lexicographique sur $\Sigma \times \mathbb{N}$, Σ étant l'alphabet usuel

Rappel (*ensemble des mots mots sur un alphabet*) :

Soit Σ un alphabet, c'est-à-dire un ensemble non vide et fini de caractères. On note :

$$\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$$

où Σ^n est l'ensemble des mots de longueur n sur Σ, c'est-à-dire des suites finies de n éléments de Σ (on a en particulier $\Sigma^0 = \varepsilon$ où ε est le mot vide).

Σ^* est l'ensemble des mots sur Σ.

Définition (*ordre alphabétique sur les mots*) :

Si $(\Sigma, \leqslant_\Sigma)$ est un ensemble ordonné, alors la relation $\mathcal{R}$ définie sur Σ^* par :

$$\forall\,(u,v) \in (\Sigma^*)^2,\ u\,\mathcal{R}\,v \iff \exists\, j \in \mathbb{N} \text{ vérifiant } j \leq |u|+1 \text{ et } j \leq |v|+1, \text{ tel que}$$
$$\forall\, i \in [1..j[,\ u_i = v_i \text{ et } \Big(j = |u|+1 \text{ ou } (j \leq |u| \text{ et } j \leq |v| \text{ et } u_j <_\Sigma v_j)\Big)$$

est une relation d'ordre sur Σ^*.

Remarque : Pour cette relation d'ordre, on a $\varepsilon = \min(\Sigma^*)$.
En effet, $\forall\, u \in \Sigma^*$, pour $j = 1$, $j = |\varepsilon| + 1$ et $j \leq |u| + 1$ et $[i..j[= [1..1[= \emptyset$ donc $\varepsilon\,\mathcal{R}\,u$.

2 Induction

2.1 Induction bien fondée

Proposition (*principe d'induction bien fondée*) :

Soit $(X, \leqslant)$ un ensemble ordonné non vide et $\mathcal{P}$ une propriété sur X.
Si $\leqslant$ est un ordre bien fondé, alors on a la proposition suivante :

$$\Big(\forall\, x \in X, (\forall\, y \in X, y < x \Longrightarrow \mathcal{P}(y)) \Longrightarrow \mathcal{P}(x)\Big) \Longrightarrow \forall\, x \in X,\ \mathcal{P}(x)$$

Preuve :
Notons $\mathcal{H}(x)$ la proposition "$(\forall\, y \in X, y < x \Longrightarrow \mathcal{P}(y)) \Longrightarrow \mathcal{P}(x)\Big)$". Supposons alors que l'ordre $\leqslant$ est bien fondé et que $\forall\, x \in X$, $\mathcal{H}(x)$ et montrons que $\forall\, x \in X$, $\mathcal{P}(x)$.

Soit $Y = \{x \in X \,|\, x \text{ ne vérifie pas } \mathcal{P}\}$, supposons par l'absurde que $Y \neq \emptyset$.
Puisque $(X, \leqslant)$ est bien fondé, Y admet un élément minimal x_0, qui vérifie :

$$\{x \in Y \,|\, x < x_0\} = \{x \in X \,|\, x < x_0\} \cap Y = \emptyset$$

Ainsi, $\{x \in X \,|\, x < x_0\} \subseteq Y^{\mathbf{c}}$, autrement dit :

$$\forall\, x \in X,\ x < x_0 \Longrightarrow \mathcal{P}(x)$$

Par $\mathcal{H}(x_0)$, on a donc $\mathcal{P}(x_0)$ soit $x_0 \notin Y$: contradiction, donc $Y = \emptyset$ d'où la propriété.

Remarque : C'est une sorte de "généralisation" du principe de récurrence. En pratique, on montre d'abord que $\mathcal{P}$ est vérifiée par les éléments minimaux (en effet si z est minimal, on a $\mathcal{H}(z) \iff \mathcal{P}(z)$), puis on montre $\mathcal{H}(x)$ pour tout élément x non minimal.

2.2 Construction d'un ensemble par induction

2.2.1 Construction

Définition (*règle de construction*) :

On appelle règle de construction la donnée :
- d'un symbole $\mathcal{S}$
- d'un entier $r \in \mathbb{N}$ (appelé arité de la règle)
- d'un ensemble non vide P.

On notera $\mathcal{S}|_P^r$ une telle règle (attention, cette notaion n'est pas universelle). De plus, on dira que $\mathcal{S}|_P^r$ est une règle de base si $r = 0$, et que c'est une règle d'induction si $r > 0$.

Proposition (*ensemble construit par induction*) :

Soit $\mathscr{C}$ un ensemble de règles de construction avec des symboles que l'on suppose être deux à deux distincts. On note :
- $\mathscr{B}$ l'ensemble des règles de base de $\mathscr{C}$
- $\mathscr{I}$ l'ensemble des règles d'induction de $\mathscr{C}$.

Si $\mathscr{B} \neq \emptyset$, alors on peut définir :
- $X_0 = \left\{(\mathcal{S}, p) \,|\, \mathcal{S}|_P^0 \in \mathscr{B},\, p \in P\right\}$
- $\forall\, n \in \mathbb{N},\, X_{n+1} = X_n \cup \left\{(\mathcal{S}, p, x_1, x_2, ..., x_r) \;\middle|\; \begin{array}{l} \mathcal{S}|_P^r \in \mathscr{I} \\ p \in P \\ \forall\, i \in [1..r],\, x_i \in X_n \end{array}\right\}$
- $X = \bigcup\limits_{n\in\mathbb{N}}^{\uparrow} X_n$ (union croissante)

X alors l'ensemble construit par induction à partir des règles de $\mathscr{C}$.

Remarque : Si $\mathscr{I} \neq \emptyset$, alors X est de cardinal infini. La réciproque est en revanche fausse.

2.2.2 Hauteur des termes

On considère par la suite un ensemble X défini comme ci-dessus, ainsi que les ensembles $\mathscr{C}$, $\mathscr{B}$, $\mathscr{I}$ et $(X_n)_{n\in\mathbb{N}}$ associés.

Définition (*hauteur des éléments*) :

Soit $x \in X$. Par définition de X, il existe $n_0 \in \mathbb{N}$ tel que $x \in X_{n_0}$. Ainsi, $\{n \in \mathbb{N} \,|\, x \in X_n\}$ est une partie non vide de $\mathbb{N}$ donc admet à ce titre un minimum.

On définit alors la hauteur des termes de X grâce à la fonction suivante :

$$h = \left(\begin{array}{l} X \to \mathbb{N} \\ x \mapsto \min\{n \in \mathbb{N} \,|\, x \in X_n\} \end{array}\right)$$

Remarque : Si $x \in X_{n_0}$, alors $h(x) \leq n_0$.

Propriété (*propriétés de la hauteur*) :

On a : ***i.*** $X_0 = \{x \in X \,|\, h(x) = 0\}$
ii. $\forall\, n \in \mathbb{N}^*,\, \{x \in X \,|\, h(x) = n\} = X_n \backslash X_{n-1}$

Preuve :

2.2.3 Relation d'ordre sur un ensemble construit par induction

Notation :

On définit la relation $\mathcal{R}$ sur X par :

$$\forall\,(a,b)\in X^2,\ a\,\mathcal{R}\,b \iff \exists\,\mathcal{S}|_P^r \in \mathscr{I},\ \exists\,p\in P,\ \exists\,(x_i)_{i\in[1..r]}\in X^r \text{ tels que}$$
$$b=(\mathcal{S},p,x_1,...,x_r) \text{ et } \exists\,i\in[1..r],\ a=x_i$$

Remarque : $\forall\,(x,y)\in X^2$, on a $x\,\mathcal{R}\,y \Longrightarrow h(y)\geq h(x)+1$.

Propriété (*ordre bien fondé associé à la construction par induction*) :

On note maintenant $\leqslant_X$ la clôture transitive réflexive de $\mathcal{R}$:

$$\leqslant_X = \bigcup_{n\in\mathbb{N}} \mathcal{R}^n$$

Alors : ***i.*** $\leqslant_X$ est une relation d'ordre
ii. cet ordre est total, autrement dit $(X,\leqslant_X)$ est un ensemble ordonné bien fondé.

Preuve :
i. $\leqslant_X$ est déjà réflexive et transtitive, reste donc à montrer qu'elle est antisymétrique.

Soit $(x,y)\in X^2$. On suppose que $x\leqslant_X y$ et $y\leqslant_X x$. Alors en gardant les notations de l'annexe "construire la clôture transitive d'une relation binaire", il existe :
- $n_1\in\mathbb{N}$ tel que $x\,\mathcal{R}^{n_1}\,y$, *i.e.* $x\xrightarrow{n_1}y$
- $n_2\in\mathbb{N}$ tel que $y\,\mathcal{R}^{n_2}\,x$, *i.e.* $y\xrightarrow{n_2}x$.

On a dans ce cas (*cf.* annexe, propriété) $x\xrightarrow{n_1+n_2}y$ et donc, en itérant la remarque précédente,

$$h(x)\geq h(y)+n_1\geq h(x)+n_1+n_2$$

d'où on déduit $n_1+n_2\leq 0$. Or, $(n_1,n_2)\in\mathbb{N}^2$ donc $n_1=n_2=0$.
Ainsi, on a en particulier $x\,\mathcal{R}^0\,y$ (et $y\,\mathcal{R}^0\,x$) donc $x=y$: $\leqslant_X$ est bien antisymétrique.

ii. Montrons maintenant que l'ordre $\leqslant_X$ est bien fondé sur X.

Par l'absurde, supposons qu'il existe $(x_n)_{n\in\mathbb{N}}\in X^{\mathbb{N}}$ strictement décroissante. Alors, $(h(x_n))_{n\in\mathbb{N}}$ est aussi strictement décroissante.

En effet, pour $(x,x')\in X^2$ tels que $x<_X x'$, il existe $n\in\mathbb{N}$ tel que $x\,\mathcal{R}^n\,x$, c'est-à-dire $x\xrightarrow{n}x'$. Comme $x\neq x'$, $(x,x')\notin\mathcal{R}^0$ donc $n>0$. En itérant la remarque, on a donc

$$h(x')\geq h(x)+n\geq h(x)+1>h(x)$$

ce qui prouve que h est croissante de $(X,\leqslant_X)$ dans $(\mathbb{N},\leq)$.

Or, $(\mathbb{N},\leq)$ est bien fondé, donc $(h(x_n))_{n\in\mathbb{N}}$ ne peut être strictement décroissante : il y a contradiction, ce qui prouve que $(X,\leqslant_X)$ est bien fondé.

À retenir :

Un ensemble construit par induction est naturellement muni d'une relation d'ordre bien fondée.

2.2.4 Preuve par induction sur un ensemble construit par induction

Puisqu'un un ensmeble construit par induction est muni d'une relation d'ordre bien fondée, on peut utiliser le principe d'induction bien fondée pour démontrer des propriétés sur cet ensemble.

En pratique, cela se décline souvent comme dans la propriété qui suit.

Proposition (*preuve par induction*) :

Soit $\mathcal{P}$ une propriété sur X. Si :

- $\forall\, \mathcal{S}|_P^0 \in \mathscr{B},\ \forall\, p \in P,\ \mathcal{P}(\mathcal{S}, p)$ est vraie
- $\forall\, \mathcal{S}|_P^r \in \mathscr{I},\ \forall\, p \in P,\ \forall\, (x_i)_{i\in[1..r]} \in X^r,\ (\forall\, i \in [1..r], \mathcal{P}(x_i)) \Longrightarrow \mathcal{P}(\mathcal{S}, p, x_1,..., x_r)$

alors $\mathcal{P}(x)$ est vérifiée par tout $x \in X$.

Preuve :

2.2.5 Définition de fonctions par induction

Sur un ensemble défini par induction, on peut définir une fonction de manière récursive, pourvu qu'on décrive :

- d'une part, explicitement, comment elle opère sur les termes de base
- d'autre part, comment elle opère sur les termes composés en supposant qu'on sait comment elle opère sur ses sous-termes.

Notations :

Soit $(f_R)_{R\in\mathscr{C}}$ une famille de fonctions.

- si $\mathcal{S}|_P^r$, on notera plutôt $f_{\mathcal{S}}$ au lieu de f_R, notation claire et sans ambiguïté puisque les symboles sont supposés distincts pour deux règles distinctes.
- de plus, pour $x \in X$ on dira "x s'écrit $(\mathcal{S}, p, x_1,..., x_r)$" pour désigner la propriété :

$$\exists\, R = \mathcal{S}|_P^r \in \mathscr{C},\ \exists\, p \in P,\ \exists\, (x_i)_{i\in[1..r]} \in X^r, x = (\mathcal{S}, p, x_1,..., x_r)$$

Définition (*fonction récursivement compatible avec une famille de fonctions*) :

Soit $(f_R)_{R\in\mathscr{C}}$ une famille de fonctions. Pour $Z \subseteq X$ et $g \in \mathcal{F}(Z, Y)$, on dit que g est récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$ ssi :

$$\forall\, z \in Z,\ z \text{ s'écrit } (\mathcal{S}, p, z_1,..., z_r) \text{ avec } (z_1,..., z_r) \in Z^r \Longrightarrow g(z) = f_{\mathcal{S}}(p, g(z_1),..., g(z_r))$$

Propriété (*existence et unicité de la fonction récursivement compatible*) :

Soit Y un ensemble et $(f_R)_{R\in\mathscr{C}}$ une famille de fonctions telle que :

- si $R = \mathcal{S}|_P^r \in \mathscr{B},\ f_R \in \mathcal{F}(P, Y)$
- si $R = \mathcal{S}|_P^r \in \mathscr{I},\ f_R \in \mathcal{F}(P \times Y^r, Y)$

Il existe une unique fonction $f \in \mathcal{F}(X, Y)$ telle que :

$$\forall\, x \in X,\ \text{"}x \text{ s'écrit } (\mathcal{S}, p, x_1,..., x_r)\text{"} \Longrightarrow f(x) = f_R(p, f(x_1), f(x_2),..., f(x_r))$$

c'est-à-dire qui soit récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$.

Preuve :

i. Montrons l'*existence* de cette fonction. On pose :

$\cdot\ f_0 = \begin{pmatrix} X_0 \to Y \\ x \mapsto f_{\mathcal{S}}(p) \text{ où } x \text{ s'écrit } (\mathcal{S}, p) \text{ avec } \mathcal{S}|_P^0 \in \mathscr{B} \text{ et } p \in P \end{pmatrix}$

$$\cdot\ \forall\, n \in \mathbb{N},\ f_{n+1} = \begin{pmatrix} X_{n+1} \to Y \\ x \mapsto \begin{cases} f_n(x) \text{ si } x \in X_n \\ f_{\mathcal{S}}(p, f_n(x_1),..., f_n(x_r)) \text{ sinon,} \\ \text{où } x \text{ s'écrit } (\mathcal{S}, p, x_1,..., x_r) \text{ avec } \begin{cases} \mathcal{S}|_P^r \in \mathscr{I} \\ p \in P \\ (x_i)_{i\in[1..r]} \in X_n^r \end{cases} \end{cases} \end{pmatrix}$$

On remarque que pour $n \in \mathbb{N}$, $f_{n+1}|_{X_n} = f_n$ donc par récurrence élémentaire on a $\forall\, m \geq n$, $f_m|_{X_n} = f_n$. On peut donc définir :

$$f = \begin{pmatrix} X \to Y \\ x \mapsto f_n(x) \text{ si } x \in X_n \end{pmatrix}$$

Montrons que f est récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$: soit $x \in X$.
$\cdot$ Si $x \in X_0$, alors x s'écrit $(\mathcal{S}, p)$ avec $\mathcal{S}|_P^0 \in \mathscr{B}$ et $p \in P$. Alors, comme $x \in X_0$,

$$f(x) = f_0(x) = f_{\mathcal{S}}(p)$$

$\cdot$ Si $x \in X_n$ avec $n \in \mathbb{N}^*$, il existe $\mathcal{S}|_P^r \in \mathscr{I}$, $p \in P$ ainsi que $(x_i)_{i\in[1..r]} \in (X_{n-1})^r$ tels que $x = (\mathcal{S}, p, x_1,..., x_r)$. On a alors :

$$\begin{aligned} f(x) &= f_n(x) \text{ car } x \in X_n \\ &= f_{\mathcal{S}}(p, f_{n-1}(x_1),..., f_{n-1}(x_r)) \\ &= f_{\mathcal{S}}(p, f(x_1),..., f(x_r)) \text{ car } \forall\, i \in [1..r],\ x_i \in X_{n-1} \text{ donc } f_{n-1}(x_i) = f(x_i) \end{aligned}$$

f est donc récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$ (elle l'est en fait par construction).

ii. Montrons à présent l'*unicité* : suppose qu'il existe $g \in \mathcal{F}(X, Y)$ récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$ et montrons par induction la propriété : $\mathcal{P}(x)$: "$f(x) = g(x)$".

$\cdot$ Soit $R = \mathcal{S}|_P^r \in \mathscr{B}$ et $p \in P$.
Alors, $f(\mathcal{S}, p) = g(\mathcal{S}, p) = f_{\mathcal{S}}(p)$ car f et g sont toutes les deux récursivement compatibles avec les $(f_R)_{R\in\mathscr{C}}$, $\mathcal{P}(S, p)$ est donc vraie. Ainsi, $\forall\, x_0 \in X_0$, $\mathcal{P}(x_0)$ est vraie.

$\cdot$ Soit $R = \mathcal{S}|_P^r \in \mathscr{I}$, $p \in P$ et $(x_i)_{i\in[1..r]} \in X^r$. On suppose que $\forall\, i \in [1..r]$, $\mathcal{P}(x_i)$ est vraie. Alors, on a :

$$\begin{aligned} f((\mathcal{S}, p, x_1,..., x_r)) &= f_{\mathcal{S}}(S, p, f(x_1),..., f(x_r)) \text{ car } f \text{ est récursivement compatible} \\ &= f_{\mathcal{S}}(p, g(x_1),..., g(x_r)) \text{ car } \forall\, i \in [1..r],\ \mathcal{P}(x_i) \\ &= g((\mathcal{S}, p, x_1,..., x_r)) \text{ car } g \text{ est récursivement compatible} \end{aligned}$$

d'où $\mathcal{P}((\mathcal{S}, p, x_1,..., x_r))$.

Par principe d'induction, on en déduit $\forall\, x \in X$, $f(x) = g(x)$, d'où l'unicité de f.