Ordre et induction

1 Relations

1.1 En général

Soient $X \neq \emptyset$ et $n \in \mathbb{N}^*$.

On dit que $\mathcal{R}$ est une relation n-aire sur X ssi $\mathcal{R} \subseteq X^n$, n est alors appelé arité de la relation. Si $(x_i)_{i\in[1..n]} \in \mathcal{R}$, on dit alors que les éléments x_1, x_2,..., x_n vérifient la relation $\mathcal{R}$.

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

Ici, $(1,2,3) \in \mathcal{R}_1$ mais $(1,3,2) \notin \mathcal{R}_1$.

Définitions :

Soit $X \neq \emptyset$ et $\mathcal{R}$ une relation binaire sur X. Pour $(x,y) \in X^2$, on note $x\,\mathcal{R}\,y$ ssi $(x,y) \in \mathcal{R}^2$.

- $\mathcal{R}$ 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 $y\,\mathcal{R}\,z \implies x\,\mathcal{R}\,z$.

$\mathcal{R}$ 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.

Soit $Y \subseteq X$, $Y \neq \emptyset$.

$\mathcal{P} = \mathcal{R} \cap Y^2$ définit une relation binaire sur Y qui a les mêmes propriétés (au sens des quatre définies ci-dessus) que $\mathcal{R}$. On l'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 :
- $\mathcal{R}_r = \mathcal{R} \cup \{(x,x) \,|\, x \in X\}$
- $\mathcal{R}_s = \mathcal{R} \cup \{(x,y) \,|\, (y,x) \in \mathcal{R}\}$
- $\mathcal{R}_t = \bigcup\limits_{n\in\mathbb{N}^*} \mathcal{R}_n$ où $\mathcal{R}_1 = \mathcal{R}$ et $\forall\, n \in \mathbb{N}^*$, $\mathcal{R}_{n+1} = \mathcal{R}_n \cup \left\{ (x,z) \in X^2\, bigg|\ \exists\, y \in X,\ \begin{matrix}(x,y) \in \mathcal{R}\\ (y,z) \in \mathcal{R}_n\end{matrix} \right\}$

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 :

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

1.2 Relations d'équivalence

Soit $X \neq \emptyset$ et $\mathcal{R}$ une relation d'équivalence sur X.
Pour $x \in X$, on définit la classe d'équivalence de x, notée $[x]$ ou $\dot{x}$, par :

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

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 : $\{\dot{x} \mid x \in X\}$ forme une partition de X. Cet ensemble, noté $X/\mathcal{R}$, est appelé espace quotient de X par la relation $\mathcal{R}$.

Définition :

Soit X et Y deux ensembles.
Soit $f \in \mathcal{F}(X, Y)$ 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

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

Si f passe au quotient, on peut définir $\bar{f} = \begin{pmatrix} X/\mathcal{R} \to Y \\ \dot{x} \mapsto f(x) \end{pmatrix}$.

Remarque : Passer de f à $\bar{f}$ permet de "gagner en injectivité" (mais $\bar{f}$ n'est pas nécessairement injective).

Propriété : On a $f(X) = \bar{f}(X/\mathcal{R})$.

1.3 Relations d'ordre

1.3.1 Élements particuliers

Soit $(X, \leqslant)$ un ensemble ordonné (*i.e.* muni d'une relation d'ordre $\leqslant$.)
Soit $Y \subseteq X$, on note $(Y, \leqslant)$ l'ensemble ordonné induit.

· Pour $x \in X$, x est un minorant de Y ssi $\forall y \in Y$, $x \leqslant y$.
· Pour $x \in X$, x est un majorant de Y ssi $\forall y \in Y$, $y \leqslant x$.
· On dit que Y est majoré s'il admet un majorant, minoré s'il admet un minorant et borné s'il est à la fois majoré et minoré.

· $x \in X$ est un plus petit élément de Y ssi x est un minorant de Y et $x \in Y$.
· $x \in X$ est un plus grand élément de Y ssi x est un majorant de Y et $x \in Y$.

· $y \in Y$ est minimal (resp. maximal) (dans Y) ssi il n'y a pas d'autre élément plus petit (resp. plus grand) que lui dans Y. Autrement dit :

$$y \text{ minimal dans } Y \Longleftrightarrow (\forall y' \in Y,\ y' \leqslant y \Longrightarrow y' = y) \Longleftrightarrow (\forall y' \in Y, y' \neq y \Longrightarrow y' \nleqslant y)$$
$$y \text{ maximal dans } Y \Longleftrightarrow (\forall y' \in Y,\ y \leqslant y' \Longrightarrow y' = y) \Longleftrightarrow (\forall y' \in Y, y' \neq y \Longrightarrow y \nleqslant y')$$

Propriété : Si Y admet un plus petit ou plus grand élément, il est unique. On peut donc noter $\min(Y)$ et $\max(Y)$ de tels éléments lorsqu'ils existent.

Remarque : Par contre, il n'y a pas unicité des éléments minimaux et maximaux.

• Une relation d'ordre $\mathcal{R}$ sur X est dit 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.* $\forall\, y' \in Y$, $y \neq y' \Longrightarrow y' \nleqslant y$.
· Soit alors $y' \in Y \backslash \{y\}$. Comme l'ordre est total, $y \leq y'$ ou $y' \leqslant y$, or $y' \nleqslant y$ 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 $\leq$ n'est pas une relation d'ordre totale.

Corollaire : Pour une relation d'ordre totale, il y a unicité des éléments minimaux et maximaux (en cas d'existence).

• On note maintenant $\mathscr{Min}(Y)$ (resp. $\mathscr{Maj}(Y)$) l'ensemble des minorants (resp. majorants) de Y.

On dit alors que : · Y admet une borne supérieure si $\mathscr{Maj}(Y)$ admet un plus petit élément.
· Y admet une borne inférieure si $\mathscr{Min}(Y)$ admet un plus grand élément.

Dans ces cas, on note respectivement $\sup(Y) = \min(\mathscr{Maj}(Y))$ et $\inf(Y) = \max(\mathscr{Min}(Y))$.

Remarque : On n'a pas forcément $\inf(Y) \in Y$ ou $\sup(Y) \in Y$, et les bornes inf et sup n'existent pas toujours. Si on considère par exemple une suite de rationnels $(u_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ telle que $(u_n) \xrightarrow{>} \sqrt{2}$ et $\forall\, n \in \mathbb{N}$, $u_n \geq \sqrt{2}$, l'ensemble $Y = \{u_n \,|\, n \in \mathbb{N}\}$ n'a pas de borne inf dans $\mathbb{Q}$.

1.3.2 Ordre bien fondé

Soient $(X, \leqslant)$ et $(Y, \preccurlyeq)$ deux ensembles ordonnés.
Pour $(x, x') \in X^2$, on note $x < x'$ ssi $x \leqslant x'$ et $x \neq x'$ (on définit de même la notation $y \prec y'$).

Définitions :

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 : $id = \begin{pmatrix} (\mathbb{N}^*, |) \to (\mathbb{N}^*, \leq) \\ n \mapsto n \end{pmatrix}$ est croissante car $\forall\, (a, b) \in (\mathbb{N}^*)^2$, si $a \leq b$.
Elle est même strictement croissante car injective.

Exercice : Pour $f \in \mathcal{F}(X, Y)$, montrer l'implication (X ordre total et f strictement croissante) $\Longrightarrow$ f injective et trouver un contre-exemple quand l'ordre n'est pas total.

⧫ **Correction :**

Pour le contre-exemple, considérer $f = \begin{pmatrix} (\mathbb{N}^*, |) & \to & (\mathbb{N}, \leq) \\ n & \mapsto & \lfloor n/2 \rfloor \end{pmatrix}$.

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

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

⧫ **Preuve :**

($\Rightarrow$) : On suppose que $(X, \leqslant)$ est bien fondé. Soit $(u_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$.
Par l'absurde, on suppose que u est 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 $a^* = u_{n^*}$. 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^*. u ne peut donc être strictement décroissante.

($\Leftarrow$) : 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 $A^{\mathbb{N}} \subseteq X^{\mathbb{N}}$.

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.

1.3.3 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 $Y = \prod_{i=1}^{n} X_i$.

Définitions :

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

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

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

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

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

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

Remarque : La proposition "$j = n + 1$ ou $a_j <_j b_j$" dans la définition alternative de l'ordre lexicographique exploite l'évaluation paresseuse (car ici $\leqslant_{n+1}$ n'a pas été défini !).

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

• 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-à-d* les suites finies de n éléments de Σ. En notant ε le mot vide, on a en particulier $\Sigma^0 = \{\varepsilon\}$.

Σ^* est alors l'ensemble des mots sur Σ.

Propriété :

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

Théorème :

Soit $(X, \leqslant)$ un ensemble ordonné non vide.
Soit $\mathcal{P}$ une propriété sur X.

Si $\leqslant$ est un ordre bien fondé, alors on a le principe d'induction bien fondée :

$$\Big(\forall\, x \in X, \underbrace{(\forall\, y \in X, y < x \Longrightarrow \mathcal{P}(y)) \Longrightarrow \mathcal{P}(x)}_{:=\mathcal{H}(x)}\Big) \Longrightarrow \forall\, x \in X,\, \mathcal{P}(x)$$

♦ **Preuve :**

On suppose que $\leqslant$ est bien fondé et que $\forall\, x \in X$, $\mathcal{H}(x)$. Montrons que $\forall\, x \in X$, $\mathcal{P}(x)$.

Notons $Y = \{x \in X \,|\, x \text{ ne vérifie pas } \mathcal{P}\}$ et supposons par l'absurde que $Y \neq \emptyset$.
Puisque $(X, \leqslant)$ est bien fondé, Y admet alors un élément minimal x_0. On a dans ce cas $\{x \in X \,|\, x < x_0\} \cap Y = \emptyset$ (car sinon x_0 ne serait pas minimal dans Y).

Ainsi, $\{x \in X \,|\, x < x_0\} \subseteq Y^c$, 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 $x_0 \notin Y$, d'où la contradiction.

Y est donc vide, *i.e.* $\forall\, x \in X$, $\mathcal{P}(x)$.

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 (puisque 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

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 la notera dans ce cours $\mathcal{S}|_P^r$ (mais cette notaion n'est pas universelle).

Si $r = 0$, on parle de règle de base, tandis que si $r > 0$, on parle de règle d'induction.

Définition :

Soit $\mathscr{C}$ un ensemble de règles de construction avec des symboles 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 :

- $X_0 = \left\{(\mathcal{S}, p) \,|\, \mathcal{S}|_P^0 \in \mathscr{B},\, p \in P\right\}$
- $\forall\, n \in \mathbb{N},\ X_{n+1} = X_n \cup \left\{ (\mathcal{S}, p, x_1, x_2, ..., x_r) \,\middle|\, \begin{array}{l} \mathcal{S}|_P^r \in \mathscr{I} \\ p \in P \\ \forall\, i \in [1..r],\ x_i \in X_n \end{array} \right\}$

ainsi que $X = \biguplus_{n \in \mathbb{N}} X_n$ (union croissante).

Remarque : Si $\mathscr{I} \neq \emptyset$, $\mathrm{Card}(X) = \infty$. Attention cependant, la réciproque est fausse.

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

2.2.2 Hauteur des termes

Pour tout $x \in X$, il existe $n_0 \in \mathbb{N}$ tel que $x \in X_{n_0}$ donc $\{n \in \mathbb{N} \,|\, x \in X_n\} \in \mathcal{P}(\mathbb{N}) \backslash \{\emptyset\}$: cette partie de $\mathbb{N}$ admet par conséquent un minimum.

Définition :

On définit la hauteur des termes de X par :

$$h = \begin{pmatrix} X \to \mathbb{N} \\ x \mapsto \min\{n \in \mathbb{N} \,|\, x \in X_n\} \end{pmatrix}$$

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

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

⧫ **Preuve :**

2.2.3 Relation d'ordre sur un ensemble construit par induction

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

• On note maintenant $\leqslant_X$ la clôture transitive réflexive de $\mathcal{R}$ (*i.e.* $\leqslant_X = \bigcup\limits_{n\in\mathbb{N}} \mathcal{R}^n$).

Propriété : $\leqslant_X$ est une relation et $(X, \leqslant_X)$ est un ensemble ordonné bien fondé.

Preuve :

(Relation d'ordre)

Elle 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 $y \leqslant_X x$.
En gardant les notations de l'annexe (2), 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.* propriété de l'annexe (2)) $x \xrightarrow{n_1+n_2} y$ et donc, en itérant la remarque précédente,

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

donc $n_1 + n_2 \leq 0$. 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 alors antisymétrique.

(Bien fondé)

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 une l'existence d'une telle suite est absurde.
$(X, \leqslant_X)$ est par conséquent bien fondé.

Propriété : On voit ainsi qu'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.

Propriété :

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 $\forall\, x \in X$, $\mathcal{P}(x)$.

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.

Propriété :

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

$$\forall\, x \in X, \Big(\exists\, R = \mathcal{S}|_P^r \in \mathscr{C}, \exists\, p \in P, \exists\, (x_i)_{i\in[1..r]} \in X^r, x = (\mathcal{S}, p, x_1, ..., x_r)\Big)$$
$$\text{(ce que l'on notera “}x\text{ s'écrit }(\mathcal{S}, p, x_1, ..., x_r)\text{”)} \Longrightarrow f(x) = f_R(p, f(x_1), f(x_2), ..., f(x_r))$$

Si $R = \mathcal{S}|_P^r$, on notera $f_{\mathcal{S}}$ pour désigner f_R (puisque les symboles sont supposés distincts pour deux règles distinctes).

De plus, si $Z \subseteq X$ et $g \in \mathcal{F}(Z, Y)$, on dit que g est récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$ si

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

La propriété précédente affirme donc que pour une telle famille de fonctions $(f_R)_{R\in\mathscr{C}}$, il existe une unique fonction $f \in \mathcal{F}(X, Y)$ qui soit récursivement compatible avec elle.

Preuve :

(Existence)

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

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

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

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

Montrons que f est récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$: soit $x \in X$.

$\to$ 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 $x \in X_0$, $f(x) = f_0(x) = f_{\mathcal{S}}(p)$.

$\to$ Si $x \in X_n$ avec $n \in \mathbb{N}^*$, il existe $\mathcal{S}|_P^r \in \mathscr{I}$, $p \in P$, $(x_i)_{i\in[1..r]} \in (X_{n-1})^r$ 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 par construction !).

(Unicité)

On suppose qu'il existe $g \in \mathcal{F}(X, Y)$ récursivement compatible avec les $(f_R)_{R\in\mathscr{C}}$. 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 $R = \mathcal{S}|_P^r \in \mathscr{I}$ et $p \in P$ et soit $(x_i)_{i\in[1..r]} \in X^r$. On suppose que $\forall\, i \in [1..r]$, $\mathcal{P}(x_i)$ est vraie.
On a alors :

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

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.