CHAPITRE 12 : ENSEMBLES ORDONNÉS ET INDUCTIFS

L'objectif est de synthétiser ce dont nous avons besoin en informatique concernant les ensembles ordonnés (étudiés plus en détail en mathématiques) et les ensembles inductifs (principalement utilisés pour définir les arbres et formules propositionnelles). On revient aussi sur la terminaison et correction des fonctions récursives.

I. Ensembles ordonnés

1. Relations sur un ensemble

Définition (relation n-aire)

Considérons un ensemble non vide E.
Pour $n \in \mathbb{N}$, on appelle **relation n-aire** sur E toute partie $\mathcal{R}$ de E^n.
n est appelé **arité** de la relation.

Exemple
$\mathcal{R} = \{(a, b, c) \in \mathbb{R}^3 \mid a + b = c\}$ est une relation ternaire sur $\mathbb{R}$.
Ici, $(1, 2, 3) \in \mathcal{R}$ mais $(1, 3, 2) \notin \mathcal{R}$.

On ne s'intéressera en informatique qu'aux relations binaires.

Définition ($x\mathcal{R}y$)

Pour deux éléments x, y de E, on note $x\mathcal{R}y$ et on dit que x **est en relation avec** y si et seulement si $(x, y) \in \mathcal{R}$.

On considérera désormais que E est un ensemble non vide et que $\mathcal{R}$ est une relation binaire sur E.

Définition (réflexivité, transitivité, symétrie, antisymétrie)

On dit que $\mathcal{R}$ est :
- **réflexive** si et seulement si $\forall xE, x\mathcal{R}x$
- **transitive** si et seulement si $\forall (x, y, z) \in E^3, x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$
- **symétrique** si et seulement si $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- **antisymétrique** si et seulement si $\forall (x, y) \in E^2, x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$

Définition (relation induite)

Soit $F \subseteq E, F \neq \emptyset$.
$\mathcal{P} = \mathcal{R} \cap F^2$ définit une relation binaire sur F qui a les mêmes propriétés (au sens des quatre définies ci-dessus) que $\mathcal{R}$.
On appelle $\mathcal{P}$ **relation induite** par $\mathcal{R}$ sur $\mathcal{F}$.

2. Relation d'équivalence

Définition (relation d'équivalence, classe d'équivalence)

On dit que $\mathcal{R}$ est une **relation d'équivalence** si et seulement si elle est réflexive, transitive et symétrique.
Pour $x \in E$, on définit la **classe d'équivalence** de x, notée $\dot{x}$, par $\dot{x} = \{y \in E \mid x\mathcal{R}y\}$.

Remarque : $\dot{x}$ est parfois noté $[x]$, ou encore $\text{Cl}(x)$.

Exemple
Soit E l'ensemble des droites du plan. La relation // de parallélisme est une relation d'équivalence.
Montrons-le :

- réflexivité : $\forall d \in E, d//d$ (une droite est bien parallèle à elle-même)
- transitivité : $\forall (d_1, d_2, d_3) \in E^3, d_1//d_2$ et $d_2//d_3 \Rightarrow d_1//d_3$ (si d_1 et d_2 sont parallèles et d_2 et d_3 sont parallèles, alors d_1 et d_3 sont parallèles)
- symétrie $\forall (d_1, d_2) \in E^2, d_1//d_2 \Rightarrow d_2//d_1$ (si d_2 est parallèle à d_1, alors d_1 est parallèle à d_2)

Les classes d'équivalence sont les directions.

Exercice
Montrer que la relation suivante sur l'ensemble des graphes orientés est une relation d'équivalence :

$$x\mathcal{R}y \Leftrightarrow (x \text{ accessible depuis } y \text{ et } y \text{ accessible depuis } x)$$

Les classes d'équivalence sont les composantes fortement connexes.

Propriété

Pour $(x, y) \in E^2$, soit $y \in \dot{x}$ auquel cas $\dot{x} = \dot{y}$, soit $y \notin \dot{x}$ auquel cas $\dot{x} \cap \dot{y} = \emptyset$.

Preuve
On a forcément $y \in \dot{x}$ ou $y \notin \dot{x}$.
Dans le premier cas, y est en relation avec x, donc par transitivité tout élément en relation avec y sera en relation avec x, d'où $\dot{y} \subset \dot{x}$. L'autre inclusion découle de la symétrie de $\mathcal{R}$.
Dans le second cas, si l'intersection était non vide, il existerait $a \in E$ tel que $a\mathcal{R}x$ et $a\mathcal{R}y$. Par symétrie et transitivité, on aurait alors $x\mathcal{R}y$, ce qui contredit $y \notin \dot{x}$.

Corollaire (ensemble quotient)

L'ensemble des classes d'équivalence par $\mathcal{R}$ forme une partition de E.
Cet ensemble est appelé ensemble quotient de l'ensemble E par la relation $\mathcal{R}$ et est noté $E/\mathcal{R}$.

3. Relation d'ordre

Définition (relation d'ordre, ensemble ordonné)

On dit que $\mathcal{R}$ est une **relation d'ordre** si et seulement si elle est réflexive, transitive et antisymétrique.
On note généralement une telle relation $\leqslant$.
Un couple $(E, \leqslant)$ où $\leqslant$ est une relation d'ordre sur E est appelé **ensemble ordonné**.

Exemple
L'ordre usuel $\leqslant$ sur l'ensemble $\mathbb{N}$ est une relation d'ordre :

- $\forall x \in \mathbb{N}, x \leqslant x$
- $\forall (x, y, z) \in \mathbb{N}^3, x \leqslant y$ et $y \leqslant z \Rightarrow x \leqslant z$
- $\forall (x, y) \in \mathbb{N}^2, x \leqslant y$ et $y \leqslant x \Rightarrow x = y$

Exercice
(1) Montrer que la relation suivante sur l'ensemble des entiers naturels est une relation d'ordre :

$$n|m \Leftrightarrow \exists k \in \mathbb{N} \mid m = nk$$

(2) Montrer que la relation suivante sur l'ensemble des graphes orientés acycliques est une relation d'ordre :

$$x \rightsquigarrow y \Leftrightarrow y \text{ est accessible depuis } x$$

Définition (ordre strict)

Soit $(E, \leqslant)$ un ensemble ordonné. L'**ordre strict** $<$ associé à $\leqslant$ est défini par

$$\forall (x, y) \in E^2, x < y \Leftrightarrow \begin{cases} x \leqslant y \\ x \neq y \end{cases}$$

Un ordre strict n'est pas une relation d'ordre (il n'est pas réflexif).

Définition (prédécesseur, successeur)

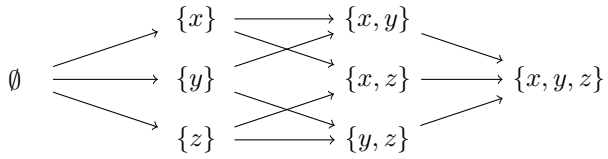
Soit $(E, \leqslant)$ un ensemble ordonné, et $(x, y) \in E^2$.
On dit que x est un **prédécesseur** (resp. **successeur**) de y si et seulement si $x < y$ (resp. $y < x$).
On dit que x est un **prédécesseur immédiat** (resp. **successeur immédiat**) de y si et seulement si :

$$\begin{cases} x < y \text{ (resp. } y < x) \\ \nexists z \in E \mid x < z < y \text{ (resp. } y < z < x) \end{cases}$$

Définition (graphe d'un ensemble ordonné)

On peut représenter un ensemble ordonné $(E, \leqslant)$ par un graphe orienté $G = (S, A)$ avec $S = E$ et $(x \to y) \in A$ si et seulement si y est un successeur immédiat de x.

Exemple
Voici le graphe de $(\mathcal{P}(\{x, y, z\}), \subseteq)$:



Exercice
Dessiner le graphe de $(\llbracket 1, 12 \rrbracket, |)$ avec $|$ la relation de divisibilité définie dans l'exercice précédent.

Propriété

Soit $(E, \leqslant)$ un ensemble ordonné et x un élément de cet ensemble.
L'ensemble des sommets accessibles depuis x dans le graphe de $(E, \leqslant)$ est l'ensemble $\{y \in E \mid x \leqslant y\}$.

Exercice
Vérifier que l'ensemble des sommets accessibles depuis 2 dans le graphe de $(\llbracket 1, 12 \rrbracket, |)$ est bien l'ensemble des multiples de 2.

Propriété

Le graphe d'un ensemble ordonné est acyclique.

Exercice
Montrer la propriété précédente.

Définition (ordre total)

Soit $(E, \leqslant)$ un ensemble ordonné.
La relation d'ordre $\leqslant$ est dite **totale** si et seulement si $\forall (x, y) \in E^2, x \leqslant y$ ou $y \leqslant x$.
On dit alors que E est un **ensemble totalement ordonné**.

Exemple
La relation usuelle $\leqslant$ sur $\mathbb{N}$ est totale.
$(\mathbb{N}, |)$ n'est pas total : $2 \nmid 3$ et $3 \nmid 2$.

4. Ordre bien fondé

Définition (élément minimal, élément maximal)

Soit $(E, \leqslant)$ un ensemble ordonné.
Un **élément minimal** (resp. maximal) de E est un élément $x \in E$ tel que $\forall y \in E, x \neq y \Rightarrow y \not\leqslant x$ (resp. $\forall y \in E, x \neq y \Rightarrow x \not\leqslant y$).

Il n'y a pas toujours unicité des éléments minimaux et maximaux.

Exemple
Pour $(\{2, 3, 6, 9, 12\}, |)$, les éléments minimaux sont 2 et 3.

Exercice
Quels sont les éléments minimaux de la relation $x \rightsquigarrow y$ des graphes orientés acycliques ?
Et les éléments maximaux ?

Définition (minimum, maximum)

Soit $(E, \leqslant)$ un ensemble ordonné.
Un **minimum** (resp. maximum) pour E est un élément $x \in E$ tel que $\forall y \in E, x \leqslant y$ (resp. $y \leqslant x$).
On parle parfois aussi de plus petit élément (resp. plus grand élément), ou de minorant (resp. majorant).

Le minimum, s'il existe, est unique et est un élément minimal.
Si l'ordre est total, être un élément minimal est équivalent à être un minimum.

Exemple
$(\{2, 3, 6, 9, 12\}, |)$ n'a pas de minimum.
Par contre, $(\mathbb{N}, |)$ a pour minimum 1.

Définition (ordre bien fondé)

Soit $(E, \leqslant)$ un ensemble ordonné.
On dit que $(E, \leqslant)$ est un **ensemble bien fondé**, ou que $\leqslant$ est un ordre bien fondé, si et seulement si $\forall F \subseteq E$ non vide, F admet un élément minimal.
Autrement dit, E est un bien fondé si toute partie non vide de E admet un élément minimal.

Si $\leqslant$ est un ordre total et bien fondé, alors toute partie non vide de E admet un minimum. On parle d'ensemble bien ordonné, et on dit que $\leqslant$ est un **bon ordre**.

Exemple
$\mathbb{N}$ muni de l'ordre usuel est bien fondé et bien ordonné.
$\mathbb{Z}$ muni de l'ordre usuel n'est pas bien fondé : $\mathbb{Z}$ n'a pas d'élément minimal.
$\mathbb{R}_+$ muni de l'ordre usuel n'est pas bien fondé : R_+^* n'a pas d'élément minimal.
$\mathbb{N}$ muni de l'ordre de divisibilité est bien fondé mais pas bien ordonné.

Théorème

$(E, \leqslant)$ est bien fondé $\Leftrightarrow$ (il n'existe pas de suite infinie strictement décroissante d'éléments de E).

Preuve
Montrons le sens $\Rightarrow$ par l'absurde. Considérons $(E, \leqslant)$ bien fondé et supposons qu'il existe une suite $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ strictement décroissante. On note $A = \{u_n \mid n \in \mathbb{N}\}$. A est une partie non vide de E et admet donc un élément minimal a_0. Il existe alors, par définition de A, $n_0 \in \mathbb{N}$ tel que $a_0 = u_{n_0}$. Par stricte décroissante de (u_n), on aurait alors $u_{n_0+1} < u_{n_0}$ ce qui contredit la minimalité de a_0.
Montrons le sens $\Leftarrow$ en montrant la contraposée. Supposons que $(E, \leqslant)$ n'est pas bien fondé. Il existe donc $A \subseteq E \neq \emptyset$ n'admettant pas d'élément minimal. Soit a_0 l'un des éléments de A. a_0 n'est pas minimal dans A, donc il existe $a_1 \in A$ tel que $a_1 < a_0$. On peut alors construire selon ce procédé une suite $(a_n)_{n\in\mathbb{N}}$ infinie d'éléments de E strictement décroissante.

Définition (ordre produit)

Soient $(E_1, \leqslant_1)$ et $(E_2, \leqslant_2)$ deux ensembles ordonnés.
On définit l'**ordre produit** $\leqslant$ sur $E_1 \times E_2$ par :

$$\forall((x_1, y_1), (x_2, y_2)) \in {E_1}^2 \times {E_2}^2, \quad (x_1, x_2) \leqslant (y_1, y_2) \Leftrightarrow \begin{cases} x_1 \leqslant_1 y_1 \\ x_2 \leqslant_2 y_2 \end{cases}$$

Propriété

Le produit de deux ordres bien fondés est bien fondé.

Remarque : le produit de deux ordres n'est pas forcément total même si les deux ordres le sont.

On peut généraliser la notion d'ordre produit aux n-uplets.

Définition (ordre lexicographique)

Soient $(E_1, \leqslant_1)$ et $(E_2, \leqslant_2)$ deux ensembles ordonnés.
On définit l'**ordre lexicographique** $\leqslant$ sur $E_1 \times E_2$ par :

$$\forall((x_1, y_1), (x_2, y_2)) \in {E_1}^2 \times {E_2}^2, \quad (x_1, x_2) \leqslant (y_1, y_2) \Leftrightarrow \left(x_1 <_1 y_1 \text{ ou } \begin{cases} x_1 = y_1 \\ x_2 \leqslant_2 y_2 \end{cases} \right)$$

Propriété

L'ordre lexicographique issu de deux ordres bien fondés (resp. totaux) est bien fondé (resp. total).

On peut généraliser la notion d'ordre lexicographique aux n-uplets.

> **Exemple**
> $(0,1,3) \leqslant (0,2,3)$ avec un ordre produit et avec un ordre lexicographique.
> $(0,2,3) \leqslant (0,4,2)$ avec un ordre lexicographique mais pas avec un ordre produit.
> Dans un dictionnaire français, les mots sont rangés dans l'ordre lexicographique.
> La fonction `strcmp` en C utilise un ordre lexicographique.

5. Retour sur la terminaison des fonctions

Le théorème précédent sur les ensembles bien fondés permet de montrer la terminaison d'algorithmes pour lesquels les techniques vues au premier semestre ne peuvent pas être appliquées.

a. Exemple introductif : la fonction d'Ackermann

La fonction d'Ackermann est définie pour $m, n \geqslant 0$ par :

- $A(0,n) = n+1$
- $A(m,0) = A(m-1,1)$ si $m \geqslant 1$
- $A(m,n) = A(m-1, A(m,n-1))$ si $m \geqslant 1$ et $n \geqslant 1$

Si on cherche à prouver la terminaison de cette fonction, on est confronté à un problème :

- le premier argument ne décroît pas strictement : un appel à $A(m,n)$ donne un appel $A(m,n-1)$;
- le second argument ne décroît pas strictement non plus : un appel à $A(m,n)$ donne un appel $A(m-1,x)$ avec $x = A(m,n-1)$ qui n'a aucune raison d'être strictement inférieur à n[1].

On peut par contre utiliser l'ordre lexicographique $\leqslant$ sur $\mathbb{N}^2$: si un appel $A(m,n)$ engendre un appel $A(m',n')$, on a bien $(m',n') < (m,n)$. En effet, il y a 3 appels engendrés à vérifier :

- $A(m-1,1)$: comme $m-1 < m$, on a bien $(m-1,1) < (m,0)$ selon l'ordre lexicographique ;
- $A(m,n-1)$: comme $n-1 < n$, on a bien $(m,n-1) < (m,n)$ selon l'ordre lexicographique ;
- $A(m-1,x)$ (avec $x = A(m,n-1)$) : comme $m-1 < m$, on a bien $(m-1,x) < (m,n)$ selon l'ordre lexicographique.

Comme $(\mathbb{N}, \leqslant)$ est bien fondé, l'ordre lexicographique sur $\mathbb{N}^2$ est également bien fondé. Ce qui signifie qu'il n'existe pas de suite décroissante infinie d'éléments de $\mathbb{N}^2$. Ainsi, en munissant (m,n) de l'ordre lexicographique, on a montré que la suite des appels engendrés par $A(m,n)$ est finie.

Les autres instructions terminent trivialement (additions, soustractions), donc la fonction d'Ackermann termine.

[1] Et qui est en fait beaucoup, *beaucoup*, plus grand que n.

b. Terminaison d'une boucle

Terminaison des boucles

Pour montrer la terminaison d'une boucle, on peut généraliser la notion de variant de boucle en considérant une quantité strictement décroissante dans un ensemble bien fondé.

Remarque : Cette nouvelle définition englobe la définition d'un variant vue en début d'année, puisque nous considérions des quantités entières positives strictement décroissantes, et que $(\mathbb{N}, \leqslant)$ est bien fondé.

Exercice

(1) Montrer la terminaison de la boucle suivante (x et y entiers positifs en entrée) :

```
TANT QUE x > 0 OU y > 0 FAIRE
  SI y > 0 ALORS
    y ← y − 1
  SINON
    x ← x − 1
    y ← 4x + 7
  FIN SI
FIN TANT QUE
```

(2) Montrer la terminaison de la boucle suivante (m et n entiers strictement positifs en entrée) :

```
TANT QUE m > 0 FAIRE
  SI m ⩾ n ALORS
    m ← m − n
  SINON
    n ← n − 1
    m ← 2m
  FIN SI
FIN TANT QUE
```

(3) Montrer la terminaison de la boucle suivante (M une matrice d'entiers de dimensions $l \times c$ et x un entier en entrée) :

```
i ← 0
j ← 0
TANT QUE i < l ET j < c ET M_{i,j} ≠ x FAIRE
  j ← j + 1
  SI j = c ALORS
    i ← i + 1
    j ← 0
  FIN SI
FIN TANT QUE
```

c. Terminaison d'une fonction récursive

Terminaison des fonctions récursives

Prouver qu'une fonction récursive termine revient à prouver deux choses :
- un appel, considéré seul (sans les appels récursifs engendrés), termine toujours ;
- l'arbre d'appels est fini.

Le premier point est le plus souvent évident, et quand il ne l'est pas les techniques pour le prouver sont les mêmes que pour un programme itératif (typiquement variant de boucle, et preuves de terminaison des autres fonctions appelées).

Pour le second point, il faut montrer que toute suite d'appels récursifs est finie :

- Le cas le plus simple est celui où le paramètre est un entier naturel qui décroît strictement au cours des appels.
- Dans le cas où le paramètre n'est pas un entier naturel, on peut souvent se ramener à $\mathbb{N}$ en prenant l'image du paramètre par une fonction bien choisie (longueur d'une liste par exemple).
- Dans les autres cas, il faut munir chaque paramètre d'une relation d'ordre bien fondée, puis munir l'ensemble des paramètres de l'ordre lexicographique ou de l'ordre produit. Ces deux ordres étant alors bien fondés, il n'existe pas de suite d'appels récursifs infinie et on peut conclure.

Exercice

(1) Montrer que la fonction suivante, définie avec $a, b, c \in \mathbb{N}$, termine :

- $F(0, b, c) = b + c$
- $F(a, b, c) = a$ si $b = 0$ ou $c = 0$
- $F(a, b, c) = F(a, b-1, F(a, 0, c-1))$ si $a = b + c$
- $F(a, b, c) = F(a-1, F(a, b-1, c+1), F(a, b, c-1))$

(2) On considère le processus suivant. Un homme possède une somme d'argent en euros strictement positive et chaque jour, soit il jette une pièce de monnaie dans une fontaine, soit il change un de ses billets contre plusieurs pièces à la banque. Montrer que ce processus termine (c'est-à-dire que l'homme n'a plus d'argent au bout d'un temps fini).

II. Ensembles inductifs

1. Définition d'ensembles inductifs

Définition (ensemble inductif)

Soit X un ensemble. Une définition inductive sur X est la donnée :
- d'une partie $\mathcal{B} \subset X$ (les **assertions**, ou éléments de base) ;
- d'un ensemble $\mathcal{K}$ de fonctions φ, éventuellement partielles, de $X^{a(\varphi)}$ dans X. L'entier $a(\varphi) \in \mathbb{N}^*$ est appelé **arité** de la fonction φ, et les fonctions sont appelées **règles d'inférence** (ou constructeurs).

L'ensemble inductif E correspondant à cette définition est alors la plus petite partie de X telle que :
- $\mathcal{B} \subset E$
- pour toute règle d'inférence φ, si $x_1, ..., x_{a(\varphi)} \in E$ et si $\varphi(x_1, ..., x_{a(\varphi)})$ est défini, alors $\varphi(x_1, ..., x_{a(\varphi)}) \in E$

Autrement dit, E est la plus petite partie de X qui contient toutes les assertions et est stable par application des règles d'inférence.

Exemple
On peut définir les entiers naturels de manière inductive : 0 est un entier naturel (assertion), et si n est un entier naturel alors $S(n)$ (le successeur immédiat de n au sens de la relation d'ordre $\leqslant$) est un entier naturel (règle d'inférence).
L'ensemble $\mathcal{D}$ des mots de Dyck (mots bien parenthésés) sur l'ensemble $\{(,)\}$ est défini par $\varepsilon \in \mathcal{D}$ (mot vide) et $(x, y) \in \mathcal{D}^2 \Rightarrow (x)y \in \mathcal{D}$.

Exercice
(1) Définir par induction l'ensemble des entiers pairs, puis définir l'ensemble des entiers impairs.
(2) Quel est l'ensemble inductif défini par $\mathcal{B} = \{1\}$ et $\mathcal{K} = \{x \mapsto 2x, x \mapsto 2x + 1, x \mapsto -x\}$?
(3) Définir par induction l'ensemble les listes chaînées.

Les ensembles définis par induction qui sont particulièrement importants en informatique sont ceux des **arbres binaires** et des **formules propositionnelles**.

Remarque : les types sommes en OCaml sont particulièrement bien adaptés pour définir des ensembles inductifs.

Définition (dérivation)

Soit E un ensemble inductif.
On appelle **dérivation** d'un élément de E la suite composée des assertions et des règles d'inférence successives utilisées pour construire cet élément.

Exemple
Sur l'ensemble des entiers naturels défini inductivement, l'élément 4 a comme dérivation l'assertion 0 suivie de la règle d'inférence S quatre fois, $S(S(S(S(0))))$.

Exercice
Donner une dérivation de -14 avec l'ensemble inductif défini par $\mathcal{B} = \{1\}$ et $\mathcal{K} = \{x \mapsto 2x, x \mapsto 2x + 1, x \mapsto -x\}$.

Définition (hauteur)

On appelle **hauteur** d'un élément d'un ensemble inductif le nombre de règles d'inférence minimal d'une de ses dérivations.

Remarque : cette définition correspond bien aux définitions de la hauteur d'une formule propositionnelle et d'un arbre non vide.

Définition (ambiguïté)

Une définition inductive d'un ensemble E est non ambiguë si ces deux conditions sont remplies :

- $\forall \varphi \in \mathcal{K}, \forall x_1, ..., x_{a(\varphi)} \in E, \varphi(x_1, ..., x_{a(\varphi)}) \notin \mathcal{B}$
- $\forall \varphi, \psi \in \mathcal{K}, \forall x_1, ..., x_{a(\varphi)}, y_1, ..., y_{a(\psi)} \in E, \ \Big(\varphi(x_1, ..., x_{a(\varphi)}) = \psi(y_1, ..., y_{a(\psi)})\Big) \Rightarrow$

$$\Big(\varphi = \psi \text{ et } x_1 = y_1 \text{ et ... et } x_{a(\varphi)} = y_{a(\psi)}\Big)$$

Autrement dit, une définition inductive d'un ensemble E est non ambiguë si chaque élément de E ne peut s'obtenir que d'une seule façon à partir des assertions et des règles d'inférence.

Exemple
On définit l'ensemble $\mathcal{A}$ des expressions arithmétiques ainsi :

- l'ensemble des entiers naturels est inclus dans $\mathcal{A}$;
- pour tout $op \in \{+, \times, -, /\}$, on a $(a, b) \in \mathcal{A}^2 \Rightarrow a \ op \ b \in \mathcal{A}$.

Cet définition est ambiguë : par exemple, on peut obtenir $1 - 2 \times 3$ à partir de $1 - 2$ et 3, mais aussi à partir de 1 et 2×3. C'est problématique car si on souhaite définir l'évaluation d'un élément de $\mathcal{A}$, une valeur donnée à l'évaluation de $1 - 2 \times 3$ serait dépendante de la manière dont elle a été construite, et un même élément aurait plusieurs valeurs différentes.

Voici une autre définition de l'ensemble des expressions arithmétiques :

- l'ensemble des entiers naturels est inclus dans $\mathcal{A}$;
- pour tout $op \in \{+, \times, -, /\}$, on a $(a, b) \in \mathcal{A}^2 \Rightarrow (a \ op \ b) \in \mathcal{A}$.

Cette définition est non ambiguë : par exemple, les deux dérivations qui donnaient $1 - 2 \times 3$ précédemment donnent maintenant $((1 - 2) \times 3)$ et $(1 - (2 \times 3))$.

Exercice
Les définitions suivantes sont-elles ambiguës ?

- $\mathcal{B} = \{0\}, \mathcal{K} = \{n \mapsto n + 1\}$;
- $\mathcal{B} = \{0, 1\}, \mathcal{K} = \{n \mapsto n + 1\}$;
- $\mathcal{B} = \{0\}, \mathcal{K} = \{n \mapsto n + 1, n \mapsto 2n\}$.

Dans un ensemble inductif doté d'une définition non ambiguë, les éléments s'identifient à leur dérivation.

2. Preuve par induction structurelle

Définition (ordre induit par une définition inductive)

Soit E un ensemble inductif.
On peut définir un ordre sur E par : $\forall x, y \in E, x \leqslant y \Leftrightarrow x$ apparaît dans une dérivation de hauteur minimale de y.

Exercice
Montrer qu'il s'agit bien d'une relation d'ordre.

Propriété

L'ordre induit sur les ensembles inductifs est bien fondé.

Preuve
Par l'absurde, supposons qu'il existe une suite infinie strictement décroissante d'éléments de E. Alors la suite correspondant aux hauteurs de ces éléments est également strictement décroissante. Or, pour tout $(x, y) \in E^2$ tels que $x < y$, il existe $n \in \mathbb{N}$ tel qu'une suite de n applications successives de règles d'inférence à x donne y. Comme $x \neq y$, $n > 0$, on a donc (avec h la hauteur) $h(y) \geqslant h(x) + n \geqslant h(x) + 1 > h(x)$. Ce qui prouve que la suite des hauteurs des éléments de E est strictement croissante, contradiction avec l'hypothèse de départ. Ainsi l'existence d'une telle suite est absurde et l'ordre est bien fondé.

Théorème (principe d'induction bien fondée)

Soit $(E, \leqslant)$ un ensemble bien fondé, et P un prédicat sur cet ensemble ($P : E \mapsto \{\text{Vrai, Faux}\}$).
On a alors :

$$(\forall x \in E, P(x)) \Leftrightarrow (\forall x \in E, (\forall y \in E, y < x \Rightarrow P(y)) \Rightarrow P(x))$$

Preuve
Le sens $\Rightarrow$ est trivial.
Montrons le sens $\Leftarrow$ par l'absurde. Supposons qu'il existe $x \in E$ tel que $P(x)$ soit faux. On note $F = \{z \in E \mid P(z) \text{ faux}\}$. $x \in F$ donc F est non vide. $(E, \leqslant)$ est bien fondé, donc F admet un élément minimal x_0. Soit $y \in E$ tel que $y < x_0$. $P(y)$ est nécessairement vrai, car sinon on aurait $y \in F$ ce qui contredirait la minimalité de x_0. On a donc $\forall y \in E, y < x_0 \Rightarrow P(y)$. Or on sait que $(\forall y \in E, y < x_0 \Rightarrow P(y)) \Rightarrow P(x_0)$. Ce qui contredit le fait que $P(x_0)$ soit faux ($x_0 \in F$).

Le principe d'induction bien fondée donne une méthode de démonstration d'un prédicat P :

- Pour tout élément $x \in E$ minimal, on démontre $P(x)$.
- Pour tout élément $x \in E$ tel que $\forall y \in E, y < x \Rightarrow P(y)$, on démontre $P(x)$.

Remarque : avec $E = \mathbb{N}$, on retrouve le principe de récurrence forte.

L'ordre induit sur les ensembles inductifs est bien fondé, on peut donc utiliser le principe d'induction bien fondée.

Théorème (preuve par induction structurelle)

Soient E un ensemble inductif et P un prédicat sur E.
Pour montrer que $P(x)$ est vrai pour tout élément de E, il suffit de montrer :

- $P(b)$ est vrai pour tout $b \in \mathcal{B}$
- pour toute règle d'inférence $\varphi \in \mathcal{K}$, pour tous $x_1, ..., x_{a(\varphi)} \in E$, $(P(x_1)$ et ... et $P(x_{a(\varphi)})) \Rightarrow P(\varphi(x_1, ..., x_{a(\varphi)}))$

On appelle ce raisonnement une **preuve par induction structurelle**.

Autrement dit, un prédicat est vrai pour tout élément d'un ensemble inductif s'il est vrai pour toutes les assertions et s'il reste vrai par application des règles d'inférence.

Exemple
Montrons par induction structurelle sur l'ensemble des expressions arithmétiques que la valeur associée à toute expression arithmétique correctement définie ne faisant pas intervenir « $-$ » est positive.

- Les assertions sont les entiers naturels, positifs par définition. La propriété est donc vraie pour les assertions.
- Montrons que la propriété reste vraie par application des règles d'inférence. Soient e_1 et e_2 deux expressions ne faisant pas intervenir le symbole $-$ et vérifiant la propriété. Soit $op \in \{+, \times, /\}$. Montrons la propriété pour $(e_1\ op\ e_2)$.
  L'addition et multiplication de deux entiers naturels donne un entier naturel, et la division de deux entiers naturels (en supposant le second non nul pour que la division soit correctement définie) donne un rationnel positif. Or on a $e_1 \geqslant 0$ et $e_2 \geqslant 0$ par hypothèse d'induction. Donc $\forall op \in \{+, \times, /\}, (e_1\ op\ e_2) \geqslant 0$.

La propriété est vraie pour les assertions et reste vraie par application des règles d'inférence, elle est donc vraie pour toute expression arithmétique.

Exercice
(1) Montrer par induction structurelle que tout mot de Dyck possède autant de parenthèses fermantes que d'ouvrantes.
(2) Montrer par induction structurelle sur les arbres binaires stricts que le nombre de nœud `n` vérifie `n = 2f-1` avec `f` le nombre de feuilles.

Il faut impérativement savoir mener des raisonnements par induction structurelle, indispensables en informatique.

3. Fonctions sur un ensemble inductif

Définition (fonction sur un ensemble inductif)

Soit E un ensemble inductif défini de manière non ambiguë. Alors la donnée de :
- valeurs de $f(x)$ pour tout $x \in \mathcal{B}$
- valeurs de $f(\varphi(x_1, ..., x_{a(\varphi)}))$ en fonction des x_i et des $f(x_i)$ pour toute règle d'inférence φ

permet de définir une fonction f sur E.

Exemple
La hauteur h d'un arbre binaire peut être définie comme une fonction sur l'ensemble inductif des arbres binaires. L'arbre vide a pour hauteur -1, et $h(Noeud(\text{etiquette}, g, d)) = 1 + \max(h(g), h(d)))$.

Exercice
En partant de la définition inductive des entiers naturels, définir :
- L'addition de deux entiers naturels.
- La multiplication de deux entiers naturels.
- La factorielle d'un entier naturel.

Analyse d'une fonction inductive

Considérons un ensemble inductif E défini de manière non ambiguë.
Une fonction sur E se programme naturellement de manière récursive à la manière de la définition précédente, et s'analyse ainsi :
- sa terminaison découle du fait que l'ordre induit sur E est bien fondé ;
- sa correction se montre par induction structurelle ;
- sa complexité se calcule de la même manière qu'une fonction récursive quelconque.

Exercice
On considère le type OCaml suivant pour représenter l'ensemble inductif des entiers naturels :
```
type entier = Zero | S of entier
```
Implémenter les trois fonctions de l'exercice précédent et montrer leur correction totale.