

Chapitre 5 : Ordres et inductions

Table des matières

1	Ensembles ordonnés	3
1.1	Vocabulaire	3
1.1.1	Définition (relation d'ordre)	3
1.1.2	Exemples	3
1.1.3	Définition (ordre strict)	3
1.1.4	Remarque	3
1.1.5	Définition (prédécesseur, successeur)	4
1.1.6	Représentation graphique d'un ensemble ordonné	4
1.1.7	Définition (ordre total)	4
1.1.8	Exemple	4
1.1.9	Définition (élément minimal / mininum)	5
1.1.10	Remarque	5
1.2	Ordres et inductions bien fondés	5
1.2.1	Définition (ordre bien fondé)	5
1.2.2	Exemple	5
1.2.3	Proposition	5
1.2.4	Remarque	6
1.2.5	Ordre produit	6
1.2.6	Ordre lexicographique	6
1.2.7	Théorème (principe d'induction bien fondée)	7
1.2.8	Remarque	7
2	Ensembles inductifs, induction structurelle	8
2.1	Définition par induction	8
2.1.1	Définition (système de règles d'inférence)	8
2.1.2	Exemple	8
2.1.3	Définition (dérivation)	8
2.1.4	Exemple	8
2.1.5	Définition (ensemble inductif)	9
2.1.6	Exemple	9
2.1.7	Remarque	9
2.2	Preuves par induction	9
2.2.1	Définition (ordre induit par une définition inductive)	9
2.2.2	Exemple	10
2.2.3	Proposition (admise)	10
2.2.4	Corollaire	10

2.2.5	Remarque	10
2.2.6	Exemple	11
2.3	Justification des définitions par induction (H.P)	11
2.3.1	Définition (treillis complet)	11
2.3.2	Proposition	11
2.3.3	Théorème (Knaster - Tarski)	11
2.3.4	Application (définition d'ensemble inductif)	12
2.3.5	Remarque	12

1 Ensembles ordonnés

1.1 Vocabulaire

1.1.1 Définition (relation d'ordre)

Soit E un ensemble. Une relation \leq sur E est une relation d'ordre si elle est :

- Réflexive : $\forall x \in E, x \leq x$;
- Antisymétrique : $\forall x, y \in E, \begin{cases} x \leq y \\ y \leq x \end{cases} \Rightarrow x = y$;
- Transitive : $\forall x, y, z \in E, \begin{cases} x \leq y \\ y \leq z \end{cases} \Rightarrow x \leq z$.

On appelle ensemble ordonné tout couple (E, \leq) où \leq est une relation d'ordre sur E .

1.1.2 Exemples

- $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ avec l'ordre \leq usuel.
- $(\mathcal{P}(E), \subseteq)$ où $A \subseteq B \Leftrightarrow \forall x \in A, x \in B$:
 - Réflexivité : $\forall x \in A, x \in A$ donc $A \subseteq A$;
 - Transitivité : $\forall A, B \in \mathcal{P}(E) \mid A \subseteq B$ et $B \subseteq C$, on a $\forall x \in A, x \in B$ donc $x \in C$
 - Antisymétrie : $\forall A, B \in \mathcal{P}(E) \mid A \subseteq B$ et $B \subseteq A, x \in A \Leftrightarrow x \in B$ (par double implication) donc $A = B$
- (\mathbb{N}, \mid) où $\forall n, m \in \mathbb{N}, n \mid m \Leftrightarrow \exists k \in \mathbb{N} \mid m = nk$:
 - Réflexivité : $\forall n \in \mathbb{N}, n = 1 \cdot n$;
 - Antisymétrie : $\forall n, m \in \mathbb{N} \begin{cases} n \mid m \\ m \mid n \end{cases}, \exists k, l \in \mathbb{N}, \begin{cases} nk = m \\ ml = n \end{cases} \text{ donc } nkl = n \text{ donc } kl = 1 \text{ donc } k = l = 1 \text{ donc } n = m$;
 - Transitivité : $\forall n, m, p \in \mathbb{N} \begin{cases} n \mid m \\ m \mid p \end{cases} \exists k, l \in \mathbb{N}, \begin{cases} nk = m \\ ml = p \end{cases} \text{ donc } n(kl) = p \text{ donc } n \mid p$

1.1.3 Définition (ordre strict)

Soit (E, \leq) un ensemble ordonné.

L'ordre strict $<$ associé à \leq est défini par $\forall x, y \in E, x < y \Leftrightarrow \begin{cases} x \leq y \\ x \neq y \end{cases}$

1.1.4 Remarque

Un ordre strict n'est pas un ordre (il n'est pas réflexif)

1.1.5 Définition (prédécesseur, successeur)

Soit (E, \leq) un ensemble ordonné et $x, y \in E$.

- x est un *prédécesseur* (resp. *successeur*) de y si, et seulement si :

$$x < y \text{ (resp. } y < x)$$

- x est un *prédécesseur immédiat* (resp. *successeur immédiat*) de y si, et seulement si :

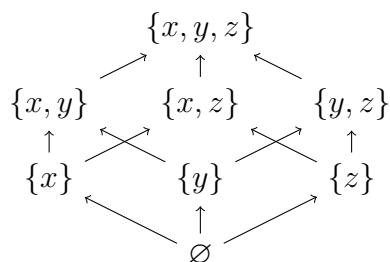
$$\begin{cases} x < y & \text{(resp. } y < x) \\ \nexists z \in E \mid x < z < y & \text{(resp. } y < z < x) \end{cases}$$

1.1.6 Représentation graphique d'un ensemble ordonné

Soit (E, \leq) un ensemble ordonné fini.

On représente (E, \leq) par son diagramme de *Hasse* qui est un graphe dont tous les sommets sont les éléments de E et tel qu'un arc $x \rightarrow y$ existe si x est un prédécesseur immédiat de y .

Exemple avec $(\mathcal{P}(\{x, y, z\}), \subseteq)$:



1.1.7 Définition (ordre total)

Soit (E, \leq) un ensemble ordonné.

La relation d'ordre \leq est totale si, et seulement si :

$$\forall x, y \in E, x \leq y \text{ ou } y \leq x$$

On dit alors que E est totalement ordonné.

1.1.8 Exemple

- \leq sur \mathbb{N} , \mathbb{Z} , \mathbb{R} est total.
- $(\mathcal{P}(E), \subseteq)$ n'est pas toujours total (s'il y a au moins 2 éléments $x, y \in E$, $\{x\}$ et $\{y\}$ ne sont pas comparables).
- $(\mathbb{N}, |)$ n'est pas total : $2 \nmid 3$ et $3 \nmid 2$.

1.1.9 Définition (élément minimal / minimum)

Soit (E, \leq) un ensemble ordonné et $P \in \mathcal{P}(E)$.

- Un élément *minimal* de P est un élément $x \in P$ tel que :

$$\forall y \in P, y \leq x \Rightarrow y = x$$

- Un *minimum* pour P est un élément $x \in P$ tel que :

$$\forall y \in P, x \leq y$$

1.1.10 Remarque

Le minimum, s'il existe, est unique et est minimal.

Si l'ordre est total, être minimal est équivalent à être minimum.

Il peut y avoir plusieurs éléments minimaux. Par exemple, avec $\{2, 3, 6, 9\}$ pour $(\mathbb{N}, |)$, 2 et 3 sont minimaux.

1.2 Ordres et inductions bien fondés

1.2.1 Définition (ordre bien fondé)

Soit (E, \leq) un ensemble ordonné.

On dit que (E, \leq) est un *ensemble bien fondé*, ou que \leq est un *ordre bien fondé* si, et seulement si :

$$\forall P \in \mathcal{P}(E) \setminus \{\emptyset\}, P \text{ admet un élément minimal}$$

1.2.2 Exemple

(\mathbb{N}, \leq) et $(\mathbb{N}, |)$ sont bien fondés.

(\mathbb{Z}, \leq) n'est pas bien fondé car \mathbb{Z} n'admet pas d'élément minimal.

$(\mathbb{Z}, |)$ n'est pas ordonné.

Exo Définir un ordre bien fondé sur \mathbb{Z} .

1.2.3 Proposition

Soit (E, \leq) un ensemble ordonné.

$$\leq \text{ bien fondé } \Leftrightarrow \nexists (u_n)_{n \in \mathbb{N}} \subset E \mid \forall n \in \mathbb{N}, u_{n+1} < u_n$$

□ Démonstration :

\Rightarrow

Supposons $\exists (u_n)_{n \in \mathbb{N}} \in E^{\mathbb{N}}$ strictement décroissante.

On note $P = \{u_n \mid n \in \mathbb{N}\} \neq \emptyset$.

Comme l'ordre est bien fondé, P admet un élément minimal u_n pour $n \in \mathbb{N}$.

Or $u_{n+1} \in P$ et $u_{n+1} < u_n$, i.e $u_{n+1} \neq u_n$ et $u_{n+1} \leq u_n$.

Or $u_{n+1} \leq u_n \Rightarrow u_{n+1} = u_n$ par minimalité de u_n : contradiction.

\Leftarrow

Soit $P \in \mathcal{P}(E) \setminus \{\emptyset\}$.

$\exists u_0 \in P$.

Si u_0 est minimal, c'est fini. Sinon, $\exists u_1 \in P \mid u_1 < u_0$ et on recommence.

On construit ainsi une suite strictement décroissante d'éléments de P , qui est nécessairement finie par hypothèse sur (E, \leq) .

Donc $\exists n \in \mathbb{N} \mid u_n$ est minimal dans P ■

1.2.4 Remarque

On peut généraliser la notion de variant en considérant une quantité strictement décroissante dans un ensemble bien fondé.

1.2.5 Ordre produit

• Définition : Soient (E_1, \leq_1) et (E_2, \leq_2) des ensembles ordonnés.

On définit l'ordre produit \leq sur $E_1 \times E_2$ par :

$$\forall ((x_1, y_1), (x_2, y_2)) \in E_1^2 \times E_2^2, \quad (x_1, x_2) \leq (y_1, y_2) \Leftrightarrow \begin{cases} x_1 \leq_1 y_1 \\ x_2 \leq_2 y_2 \end{cases}$$

• Proposition : 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.

1.2.6 Ordre lexicographique

• Définition : Soit (E_1, \leq_1) et (E_2, \leq_2) deux ensembles ordonnés.

On définit l'ordre lexicographique sur $E_1 \times E_2$ par :

$$\forall ((x_1, y_1), (x_2, y_2)) \in E_1^2 \times E_2^2, \quad (x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 <_1 y_1 \text{ ou } \begin{cases} x_1 = y_1 \\ x_2 \leq_2 y_2 \end{cases}$$

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



- Remarque : On peut généraliser l'ordre lexicographique aux n -uplets ou aux suites finies (pas nécessairement de même longueur) dans un ensemble ordonné (ex : l'ordre du dictionnaire).

Exo : utiliser un ordre lexicographique pour prouver la terminaison de l'algorithme d'Euclide (PGCD)

1.2.7 Théorème (principe d'induction bien fondée)

On parle aussi d'induction noethérienne en l'honneur d'Emmy Noether (1882 - 1935).

Soit (E, \leq) un ensemble bien fondé et P un prédicat sur cet ensemble ($P : E \rightarrow \text{bool}$).

On a :

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

□ Démonstration :

\Rightarrow évident.

\Leftarrow Supposons $\exists x \in E \mid P(x)$ soit faux.

On note $Q = \{y \in E \mid P(y) \text{ faux}\}$.

$x \in Q$, donc $Q \neq \emptyset$.

(E, \leq) est bien fondé, donc Q admet un élément minimal x_0 .

On sait que $(\forall y \in E, y < x_0 \Rightarrow P(y)) \Rightarrow P(x_0)$

Montrons que $\forall y \in E, y < x_0 \Rightarrow P(y)$, ce qui conclut car $P(x_0)$ est faux ($x_0 \in Q$).

Soit $y \in E \mid y < x_0$.

On ne peut pas avoir $P(y)$ faux, car sinon $y \in Q$ et $y < x_0$ minimal dans Q .

Donc $P(y)$ vrai ■

1.2.8 Remarque

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

- Initialisation : $\forall x \in E$ minimal, on démontre $P(x)$

- Hérédité : $\forall x \in E \mid \forall y \in E, y < x \Rightarrow P(y)$, on démontre $P(x)$.

- Le principe d'induction bien fondée généralise le principe de récurrence forte (sur (\mathbb{N}, \leq)) ;

- Le principe d'induction bien fondée généralise aussi le principe de récurrence (si l'on considère des relations bien fondées qui ne sont pas forcément des ordres : $(\mathbb{N}, <)$ où $x < y \Leftrightarrow y = x + 1$) ;

- Le principe d'induction bien fondée généralise également un autre principe d'induction lié à la définition d'ensembles à la manière des types sommes en OCaml (et donc aussi du filtrage par motif).

2 Ensembles inductifs, induction structurelle

2.1 Définition par induction

2.1.1 Définition (système de règles d'inférence)

Un *système de règles d'inférences* est donné par un ensemble d'assertions (propriétés) et de règles pour démontrer ces assertions (on parle de règles d'inférence). Une règle d'inférence est donnée par un ensemble de $n \in \mathbb{N}$ prémisses (hypotheses de la règle) et par une assertion qu'on appelle la conclusion. On note une telle règle :

$$\frac{\text{prémisse}_1 \text{ prémisse}_2 \dots \text{prémisse}_n}{\text{conclusion}}$$

Si $n = 0$, on parle d'axiome.

2.1.2 Exemple

Avec l'assertion « être un entier naturel », on peut définir les règles :

$$\frac{}{0 \text{ est un entier naturel}}^{(0)} \quad \text{et} \quad \frac{n \text{ est un entier naturel}}{S(n) \text{ est un entier naturel}}^{(S)}$$

Où $S(n)$ est le successeur de n .

2.1.3 Définition (dérivation)

Étant donné un système de règles d'inférences, une assertion est dite *dérivable* si elle est la conclusion d'un axiome ou d'une règle dont les prémisses sont dérivables.

On appelle (arbre de) dérivation l'ensemble des règles utilisées pour dériver une assertion.

2.1.4 Exemple

On ajoute un opérateur $+$ et la règle :

$$\frac{n \text{ est un entier naturel } m \text{ est un entier naturel}}{n + m \text{ est un entier naturel}}^{(+)}$$

On peut alors dériver l'assertion $S(S(0)) + S(0)$ est un entier naturel :

$$\frac{\frac{\frac{}{0 \text{ est un entier naturel}}^{(0)}}{S(0) \text{ est un entier naturel}}^{(S)} \quad \frac{\frac{}{0 \text{ est un entier naturel}}^{(0)}}{S(0) \text{ est un entier naturel}}^{(S)}}{S(S(0)) \text{ est un entier naturel } S(0) \text{ est un entier naturel}}^{(+)}$$

2.1.5 Définition (ensemble inductif)

Un *ensemble inductif*, ou ensemble défini par induction, est le plus petit ensemble (au sens de l'inclusion) engendré par un système de règles d'inférence (avec l'assertion « appartient à cet ensemble »).

2.1.6 Exemple

On définit inductivement l'ensemble *Expr* des expressions arithmétiques sur les entiers naturels par :

$$\frac{n \in \mathbb{N}}{n \in Expr} (nat) \quad \frac{e_1 \in Expr \ e_2 \in Expr}{e_1 + e_2 \in Expr} (+)$$

$$\frac{e_1 \in Expr \ e_2 \in Expr}{e_1 - e_2 \in Expr} (-) \quad \frac{e_1 \in Expr \ e_2 \in Expr}{e_1 * e_2 \in Expr} (*)$$

2.1.7 Remarque

On procède de manière analogue à la définition d'un type somme récursif en OCaml en associant une règle à chaque constructeur du type : si le constructeur n'a pas d'argument, alors il correspond à un axiome, sinon, la règle qui lui correspond à pour prémisses l'appartenance des arguments à leurs types respectifs.

```

1 | type expr =
2 |   Nat of nat
3 |   Plus of expr*expr
4 |   Minus of expr*expr
5 |   Mult of expr*expr
6 | and nat =
7 |   Zero
8 |   S of nat
9 |
```

2.2 Preuves par induction

2.2.1 Définition (ordre induit par une définition inductive)

Soit E un ensemble inductif. On peut définir un ordre sur E par :

$\forall x, y \in E, x \leq y \Leftrightarrow$ l'assertion $x \in E$ apparaît dans une dérivation de taille minimale (en termes du nombre de règles utilisées) de l'assertion $y \in E$.

□ Démonstration :

– Réflexivité : $\forall x \in E, x \leq x$ car $x \in E$ est la conclusion de la dérivation ;

– Transitivité : Soient $x, y, z \in E \mid \begin{array}{l} x \leq y \\ y \leq z \end{array}$

L'assertion $y \in E$ apparaît dans une dérivation minimale de $z \in E$. Dans cette dérivation on utilise bien une dérivation minimale de $y \in E$ (sinon on pourrait réduire la taille de la dérivation de $z \in E$). Donc l'assertion $x \in E$ y apparaît. Donc $x \leq z$;

– Antisymétrie : Soient $x, y \in E$ $\left| \begin{array}{l} x \leq y \\ y \leq x \end{array} \right.$

Si $x \neq y$, dans une dérivation minimale de $x \in E$, on trouve une dérivation minimale de $y \in E$, qui elle-même contient une dérivation de $x \in E$, nécessairement strictement plus petite, ce qui est absurde. ■

2.2.2 Exemple

L'ordre induit sur les entiers naturels donne l'ordre usuel.

L'ordre induit sur les expressions arithmétiques est la propriété d'être une sous-expression (ex : $S(0) + 0 \leq (S(0) + 0) * S(S(0))$)

2.2.3 Proposition (admise)

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

2.2.4 Corollaire

On peut utiliser le principe d'induction bien fondée sur les ensembles inductifs.

2.2.5 Remarque

Soit E un ensemble inductif.

On peut, comme dans la remarque 1.2.8, se passer de l'ordre induit pour lui préférer la relation bien fondée $x < y \Leftrightarrow x \in E$ est une prémisse de la dernière règle d'une dérivation de $y \in E$.

On obtient alors le principe d'*induction structurelle* que l'on peut écrire aussi :

Soit P in prédicat sur E . Si pour toute règle d'inférence de la forme

$$\frac{x_1 \in E \ \dots \ x_n \in E}{C(x_1 \ \dots \ x_n) \in E}$$

on a la propriété

$$\forall (x_k)_{k \in \llbracket 1 ; n \rrbracket} \subset E, \forall k \in \llbracket 1 ; n \rrbracket, P(x_k) \Rightarrow P(C(x_1 \ \dots \ x_n))$$

alors $\forall x \in E, P(x)$.



2.2.6 Exemple

On retrouve le principe de récurrence sur les entiers naturels.

On démontre par induction structurelle que la valeur associée à toute expression arithmétique ne faisant pas intervenir le symbole $-$ est positive :

- Règle (*nat*) : si $n \in \mathbb{N}$, alors $n \geq 0$ (par induction structurelle sur les entiers naturels)
- Règle $(+)/(*):$ si $e_1, e_2 \in Expr$ ne font pas intervenir le symbole $(-)$, alors par induction $e_1 \geq 0$ et $e_2 \geq 0$

Donc $e_1 + e_2 \geq 0$ et $e_1 * e_2 \geq 0$.

2.3 Justification des définitions par induction (H.P)

2.3.1 Définition (treillis complet)

Soit (E, \leq) un ensemble ordonné.

(E, \leq) est un *treillis complet* si, et seulement si :

$$\forall A \in \mathcal{P}(E), \begin{cases} A \text{ admet un plus grand minorant } \bigwedge A \\ A \text{ admet un plus petit majorant } \bigvee A \end{cases}$$

Rappel :

- m est un majorant pour $A \Leftrightarrow \forall a \in A, a \leq m$
- $m = \bigvee A \Leftrightarrow m$ est un majorant et $\forall m'$ majorant de $A, m \leq m'$

2.3.2 Proposition

Soit E un ensemble.

Alors $(\mathcal{P}(E), \subseteq)$ est un treillis complet.

□ Démonstration :

Soit $A \in \mathcal{P}(\mathcal{P}(E))$. On définit

$$\begin{cases} \bigcap A = \bigcap_{P \in A} P & (E \text{ si } A \neq \emptyset) \\ \bigcup A = \bigcup_{P \in A} P & (\emptyset \text{ si } A = \emptyset) \end{cases}$$

Exo : $\bigcap A = \bigwedge A$ et $\bigcup A = \bigvee A$

2.3.3 Théorème (Knaster - Tarski)

Soit (E, \leq) un treillis complet et $f : E \rightarrow E$ croissante.

On définit l'ensemble des pré-points fixes de f par

$$P_f = \{x \in E, \mid f(x) \leq x\}$$

Alors $\wedge P_f$ est un point fixe de f (le plus petit)

□ Soit $x \in P_f$.

Alors par définition, $\wedge P_f \leq x$, donc par croissance de f , $f(\wedge P_f) \leq f(x) \leq x$.

Donc $f(\wedge P_f)$ est un minorant de P_f .

Donc par définition, $f(\wedge P_f) \leq \wedge P_f$ donc par croissance, $f(f(\wedge P_f)) \leq f(\wedge P_f)$

donc $f(\wedge P_f) \in P_f$, donc par définition, $\wedge P_f \leq f(\wedge P_f)$

donc par antisymétrie, $\boxed{f(\wedge P_f) = \wedge P_f}$ ■

2.3.4 Application (définition d'ensemble inductif)

Étant donné des ensembles prédéfinis B_1, \dots, B_t , on définit par induction un ensemble à l'aide de constructeurs C_1, \dots, C_k où $\forall i \in \llbracket 1 ; k \rrbracket$, C_i est associé à un tuple de type d'arguments $a_i^1, \dots, a_i^{n_i}$ où $\forall j \in \llbracket 1 ; n_i \rrbracket$,

$$a_i^j = \begin{cases} B_m \text{ pour un certain } m \\ \text{rec (cas d'induction)} \end{cases}$$

On définit alors

$$f_{C_1 \dots C_k}(S) = \bigcup_{i \in \llbracket 1 ; k \rrbracket} \left\{ C_i(u_1 \dots u_{n_i}), \forall j \in \llbracket 1 ; n_i \rrbracket, \begin{cases} u_j \in B_m \text{ si } a_i^j = B_m \\ u_j \in S \text{ si } a_i^j = \text{rec} \end{cases} \right\}$$

On admet que $f_{C_1 \dots C_k}$ est croissante sur le treillis complet des parites.

Le théorème de Knaster-Tarski assure l'existence du plus petit ensemble stable par application des constructeurs, *i.e* l'ensemble inductif défini par les C_i .

2.3.5 Remarque

On pourrait de même utiliser les théorème de Knaster-Tarski pour justifier le principe d'induction structurelle, ou pour justifier la définition par induction de fonctions sur un ensemble inductif.

Ceci permet donc le filtrage par motif.

Finalement, on a défini inductivement la notion de dérivation, on peut donc faire des preuves par induction structurelle sur les dérivations.