# Chapitre 0

# Remarques préliminaires

"Induction :" qu'est-ce que ça veut dire et pourquoi s'y intéresser ? Ensuite quelques rappels sur la théorie des ensembles.

## 0.1 Qu'entend-on par "induction" ?

Le mot "induction" est utilisé dans des sens différents.

**Tradition logico-philosophique.** Le syllogisme d'Aristote, c'est la règle d'inférence "Modus Ponens" :

$$\frac{P \Rightarrow Q \qquad P}{Q}$$

Il y a plusieurs façons d'exploiter cette règle :

**déduction :** à partir de $P$ et $P \Rightarrow Q$ on déduit $Q$. C'est la formulation (dérivation) de nouvelles conclusions.

**abduction :** si on sait que $P \Rightarrow Q$ et qu'on observe $Q$, alors on pourrait formuler l'hypothèse $P$ pour expliquer l'observation. C'est la formulation d'hypothèses.

**induction :** si chaque fois qu'on observe $P$, on observe $Q$ aussi, on peut formuler l'hypothèse scientifique que le domaine obéit à la loi $P \Rightarrow Q$. C'est la formulation de règles généralisantes : apprentissage, IA.

Ce sens du mot "induction" n'est pas celui auquel on s'intéressera dans ce cours.

**Tradition mathématique.** on connait la notion de récurrence :

- définition par récurrence (suites)
- démonstration par récurrence :

$$\left.\begin{array}{l} P(0) \\ P(n) \;\Rightarrow\; P(n+1) \end{array}\right\} \Rightarrow \; \forall n \in \mathbb{N}\; P(n)$$

On peut réexaminer la notion de récurrence dans un cadre plus général : celui de l'induction. C'est à ce sens du mot "induction" qu'on va s'intéresser.

## 0.2 Pourquoi s'y intéresser ?

**Définition récursive de fonction.** Considérons une définition informatique classique récursive de la fonction factorielle :

$$\mathrm{fact}(n) \quad = \quad \textbf{si} \;\; x = 0 \;\; \textbf{alors} \;\; 1 \;\; \textbf{sinon} \;\; n * \mathrm{fact}(n-1)$$

- qu'est-ce que ça veut dire de définir fact en terme d'elle-même ?
- ce qu'on a écrit n'est pas une fonction ! Tout au plus, c'est la description d'un algorithme pour calculer les valeurs qu'une certaine fonction prend à chaque point de son domaine.
- alors qu'elle est la véritable fonction mathématique qui correspond à cet algorithme ?
- on peut vouloir prouver des propriétés de cette fonction : par exemple qu'elle calcule bien la factorielle de son argument !

**Définition inductive de types.** on utilise souvent des types de données définis de manière inductive. Par exemples, les listes d'entiers :

```
type IntList = nil | int :: IntList
```

ou sa version polymorphique :

```
type List(a) = nil | a :: List(a)
```

- qu'est-ce que ça veut dire ?
- raisonnement par induction structurelle (analyse par cas)

**Plus généralement :** on utilisera les techniques d'induction et de point fixe pour :

- sémantique de programmes :
  - fonctionnel (induction)
  - logique (co-induction)
- démonstration de propriétés de programmes

## 0.3 Rappels de théorie des ensembles

**Appartenance :** c'est le concept primitif. On l'exprime par des formules atomiques $x \in A$. C'est sur ce concept qu'on construit la théorie des ensembles.

**Axiome d'extension :** définit l'égalité :

$$\begin{array}{lcl} A = B & \text{ssi} & \forall x \; (x \in A \Leftrightarrow x \in B) \\ A \subseteq B & \text{ssi} & \forall x \; (x \in A \Rightarrow x \in B) \\ A = B & \text{ssi} & A \subseteq B \;\wedge\; B \subseteq A \end{array}$$

**Axiome de spécification :** si on a un ensemble $A$ et un prédicat unaire $P$, alors on peut former un nouvel ensemble $B$ de la manière suivante :

$$B = \{x \in A \mid P(x)\}$$

Dans la période pré-axiomatique de la théorie des ensembles, on tenait pour évident l'existence d'un *univers* $\mathcal{U}$, c'est à dire un ensemble de tous les ensembles. Une conséquence de l'axiome de spécification, c'est que cela n'est pas possible. C'est le paradoxe de Russell :

Supposons qu'il existe un ensemble $\mathcal{U}$ contenant tous les ensembles. Alors, selon l'axiome de spécification, en prenant $A = \mathcal{U}$ et $P(x) \equiv x \notin x$, on peut construire l'ensemble $B$ suivant :

$$B = \{S \in \mathcal{U} \mid S \notin S\}$$

Mais, comme vous pouvez le vérifier en utilisant la définition de $B$, cet ensemble $B$ a la curieuse propriété :

$$B \in B \quad \Leftrightarrow \quad B \notin B$$

Donc l'hypothèse de l'existence de $\mathcal{U}$ amène à une contradiction. On a donc prouvé, par l'absurde, qu'un tel $\mathcal{U}$ ne peut pas exister.

Toute collection d'ensembles n'est pas nécessairement un ensemble. Certaines collections sont plus vastes que des ensembles. Ce ne sont pas des ensembles ; donc on ne peut pas leur appliquer e.g. l'axiome de spécification pour construire de nouveaux ensembles. On évite ainsi le paradoxe de Russell.

**Comment démarrer ?** si pour avoir la théorie des ensemble on a besoin d'une inexplicable "collection", on n'a pas beaucoup avancé ! Au lieu de cela, on pose l'axiome suivant :

il existe un ensemble

Appelons cet ensemble $A$. Alors, grâce à l'axiome de spécification, nous pouvons définir l'ensemble $B$ suivant :

$$B = \{x \in A \mid x \neq x\}$$

$B$ est vide. Donc il existe un ensemble vide, qu'on notera $\emptyset$ et on peut en prouver l'unicité grâce à l'axiome d'extension. Pour tout ensemble $A$ on a bien sur $\emptyset \subseteq A$.

**Singletons.** on se donne un nouveau moyen de créer des ensembles. Si $A$ est un ensemble, alors $\{A\}$ est un ensemble.

**Union et intersection.** si $A$ et $B$ sont des ensembles, alors on peut en définir l'intersection $A \cap B$ et l'union $A \cup B$. Plus généralement, si $S$ est un ensemble d'ensembles, on pose :

$$\begin{aligned} \cup S &= \{x \mid \exists A \in S,\ x \in A\} \\ \cap S &= \{x \mid \forall A \in S,\ x \in A\} \end{aligned}$$

**Ensemble des parties d'un ensemble.** (powerset)

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Au lieu de $\mathcal{P}(A)$ on écrit souvent $2^A$.

**Paire ordonnée.** on peut définir formellement la notion de paire ordonnée $(a, b)$. Pour simplifier, cette définition est omise ici.

**Produit cartésien.** si $A$ et $B$ sont des ensembles, on peut définir leur produit cartésien $A \times B$ de la manière suivante :

$$A \times B \quad = \quad \{(a, b) \mid \forall a \in A,\ \forall b \in B\}$$

**Relation binaire.** soit $R$ une relation binaire entre éléments de $A$ et de $B$. On peut identifier $R$ avec l'ensemble des couples $(a, b)$ vérifiant cette relation :

$$R \subseteq A \times B$$

On utilise souvent différentes notations pour exprimer que $x$ est en relation $R$ avec $y$ :

$$(x, y) \in R \qquad\qquad x\, R\, y \qquad\qquad R(x, y)$$

On dit que $y$ est une image de $x$, et $x$ est un antécédent de $y$. Une relation binaire $R$ à un domaine et un codomaine :

$$\begin{array}{rcl} \mathrm{dom}(R) & = & \{x \mid \exists y \quad x\, R\, y\} \\ \mathrm{codom}(R) & = & \{y \mid \exists x \quad x\, R\, y\} \end{array}$$

**Fonction.** une fonction est un cas particulier d'une relation où chaque $x$ du domaine apparait dans exactement une paire de la relation : autrement dit il a une image unique.

On note $B^A$ l'ensemble des fonctions de $A$ dans $B$.