

# Cours: les réels en Coq

3 novembre 2009

## Introduction

Après  $\mathbb{N}$  et  $\mathbb{Z}$ , il est utile de formaliser  $\mathbb{R}$  dans un assistant de preuves. En effet, les réels servent de base à une grosse partie des mathématiques : l'analyse. De plus, les réels servent de modèle idéal aux calculs faits sur ordinateur. On a donc besoin du comportement idéal des opérateurs  $+$ ,  $-$ ,  $\times$ ,  $\div$ ,  $\sqrt{\quad}$ ,  $\sin. .$  pour les comparer aux opérateurs réellement disponibles dans les processeurs.

## 1 Réels constructifs/axiomatiques

Il existe plusieurs façons de définir les réels.

- par *construction* (méthode mathématique usuelle) ;
- par *axiomatisation*.

La construction permet une grande sûreté de l'approche. Tout est défini proprement et le risque d'erreur est faible. Par contre, l'inconvénient majeur est un gros effort à la fois de formalisation et de développement de preuves. Les lemmes les plus basiques nécessitent de revenir aux définitions complexes et sont donc coûteux en temps.

L'axiomatisation permet de prouver bien plus rapidement des choses intéressantes. Les développements sont donc plus rapides. Par contre, il faut faire très attention aux axiomes choisis. En effet, tout axiome qui permettrait de prouver faux rend inconsistant tout le système.

Par ailleurs, la définition des réels peut être :

- *intuitionniste* ;
- *classique*.

Une formulation constructive permet l'extraction de programmes à partir de preuves. Par contre, l'absence du tiers exclus empêche de prouver certains théorèmes utiles de l'analyse comme le théorème de Rolle. Et une formalisation classique permet de prouver l'existence de fonctions non calculables.

Le problème essentiel des approches intuitionnistes est le test d'égalité : comment savoir si deux nombres réels sont égaux ? En fait, on peut savoir que deux nombres sont différents et on utilise pour ça un prédicat d'*apartness*, noté #.

Voici un tableau récapitulatif des différentes approches :

		intuitionniste	classique
construction	+	prouvé extractible	prouvé
	-	long compliqué	long
axiomatisation	+	rapide ± extractible	rapide simple
	-	non prouvé compliqué	non prouvé non extractible

En Coq, plusieurs approches sont disponibles. Les réels de la bibliothèque standard de Coq sont axiomatiques et classiques [3] tandis que ceux de C-CoRN sont constructifs. C-CoRN (Constructive Coq Repository at Nijmegen) est une bibliothèque Coq de setoids, anneaux et corps constructifs. Elle a été développée pour prouver le théorème fondamental de l'algèbre de façon constructive. Voir [1] et un cours du [2-7-2].

## 2 Réels axiomatiques

Le choix fait dans la bibliothèque standard de Coq est celui de l'axiomatisation. Cela signifie que  $\mathbb{R}$  est un `Parameter` de type `Set`. On suppose qu'il existe un ensemble et des fonctions qui ont le comportement attendu, mais on ne les construit pas.

Cette approche est moins sûre, on limite donc le nombre d'axiomes au maximum (ici 17).

### 2.1 Axiomatisation

On suppose donc l'existence de l'ensemble, des valeurs 0 et 1 et des fonctions  $+$ ,  $\times$ ,  $-$ (unaire),  $/$ (unaire),  $<$  et `up` (voir plus loin).

`Parameter R : Set.`

`Parameter R0 : R.`

`Parameter R1 : R.`

`Parameter Rplus : R -> R -> R.`

`Parameter Rmult : R -> R -> R.`

`Parameter Ropp : R -> R.`

Parameter Rinv :  $\mathbb{R} \rightarrow \mathbb{R}$ .  
 Parameter Rlt :  $\mathbb{R} \rightarrow \mathbb{R} \rightarrow \text{Prop}$ .  
 Parameter up :  $\mathbb{R} \rightarrow \mathbb{Z}$ .

On ajoute alors les axiomes qui définissent les comportements de ces nombres et de ces opérations.

Axiom Rplus\_comm : forall r1 r2:R, r1 + r2 = r2 + r1.  
 Axiom Rplus\_assoc : forall r1 r2 r3:R,  
                                   r1 + r2 + r3 = r1 + (r2 + r3).  
 Axiom Rplus\_opp\_r : forall r:R, r + - r = 0.  
 Axiom Rplus\_0\_l : forall r:R, 0 + r = r.

Axiom Rmult\_comm : forall r1 r2:R, r1 \* r2 = r2 \* r1.  
 Axiom Rmult\_assoc : forall r1 r2 r3:R,  
                                   r1 \* r2 \* r3 = r1 \* (r2 \* r3).  
 Axiom Rinv\_l : forall r:R, r <> 0 -> / r \* r = 1.  
 Axiom Rmult\_1\_l : forall r:R, 1 \* r = r.  
 Axiom Rmult\_plus\_distr\_l : forall r1 r2 r3:R,  
                                   r1 \* (r2 + r3) = r1 \* r2 + r1 \* r3.

Pour éviter que tous les réels soient uniformément nuls, on doit supposer que  $0 \neq 1$  :

Axiom R1\_neq\_R0 : 1 <> 0.

On suppose ensuite que l'ordre (et l'égalité) sont décidables. On peut décider (en particulier dans une fonction) si  $x$  est positif, négatif ou nul.

Axiom total\_order\_T : forall r1 r2:R,  
                           {r1 < r2} + {r1 = r2} + {r1 > r2}.

On ajoute quelques axiomes sur l'ordre :

Axiom Rlt\_asym : forall r1 r2:R, r1 < r2 -> ~ r2 < r1.  
 Axiom Rlt\_trans : forall r1 r2 r3:R,  
                           r1 < r2 -> r2 < r3 -> r1 < r3.

On a ensuite besoin du comportement de l'ordre vis-à-vis des opérations :

Axiom Rplus\_lt\_compat\_l : forall r r1 r2:R,  
                           r1 < r2 -> r + r1 < r + r2.  
 Axiom Rmult\_lt\_compat\_l : forall r r1 r2:R,  
                           0 < r -> r1 < r2 -> r \* r1 < r \* r2.

On définit ensuite  $\leq$  comme étant  $<$  ou  $=$  :

Definition Rle (r1 r2:R) : Prop := r1 < r2  $\vee$  r1 = r2.

On définit ensuite des fonctions INR ( $\mathbb{N} \rightarrow \mathbb{R}$ ) et IZR ( $\mathbb{Z} \rightarrow \mathbb{R}$ ) où  $0 \rightarrow R0$ ,  $1 \rightarrow R1$ , etc.

Le corps des réels est archimédien : on peut trouver un entier supérieur à tout réel. ici, on suppose de plus que ce réel est le plus petit qui est strictement supérieur au réel :

Axiom archimed : forall r:R,  
IZR (up r) > r  $\wedge$  IZR (up r) - r <= 1.

Reste à définir la complétude de  $\mathbb{R}$  : tout ensemble non vide a un plus grand élément.

Definition is\_upper\_bound (E:R -> Prop) (m:R) :=  
forall x:R, E x -> x <= m.

Definition bound (E:R -> Prop) :=  
exists m : R, is\_upper\_bound E m.

Definition is\_lub (E:R -> Prop) (m:R) :=  
is\_upper\_bound E m  $\wedge$   
(forall b:R, is\_upper\_bound E b -> m <= b).

Axiom completeness :  
forall E:R -> Prop,  
bound E -> (exists x : R, E x) -> { m:R | is\_lub E m }.

Ces 17 axiomes suffisent à définir des réels.

Il faut ensuite définir beaucoup (beaucoup) de lemmes de façon à en faire des réels utilisables pour prouver des choses simples.

Notez le choix fait ici : Rinv est une fonction totale. Il est donc licite de manipuler  $\frac{1}{0}$ . Par contre, l'axiome affirmant la propriété de l'inverse, c'est-à-dire  $\frac{1}{x} \times x = 1$  (Rinv\_1) nécessite que  $x \neq 0$ .

On ne peut donc pas montrer que  $\frac{0}{0} = 1$ .

Un autre choix aurait été de définir une fonction Rinv qui prend un réel  $x$  et une preuve que  $x \neq 0$ .

## 2.2 Automatisations

Comme vous le constaterez, ces axiomes sont insuffisants pour prouver des lemmes complexes et le besoin d'automatisations est énorme. On parlera ici des automatisations liées à l'égalité de termes.

Pour les calculs sur les anneaux, on dispose de la tactique `ring` qui permet de résoudre des égalités d'anneau sur  $\mathbb{Z}$  et aussi sur  $\mathbb{R}$ . Comment rajouter les inverses et faire une tactique `field` pour les corps (qui soit générique)?

Voici l'algorithme de `field` :

- Transformer  $x - y$  en  $x + (-y)$  et  $x/y$  en  $x \times 1/y$ .
- Chercher tous les inverses apparaissant dans l'égalité pour en faire un produit.
- Distribuer totalement à gauche et à droite de l'égalité, excepté dans les inverses.
- Associer à droite chaque monôme, excepté dans les inverses.
- Multiplier à gauche et à droite par le produit d'inverses, que l'on a construit précédemment, en générant la condition que tous les inverses doivent être non nuls.
- Distribuer seulement le produit sur la somme de monômes à gauche et à droite sans réassocier à droite.
- Éliminer les inverses des monômes en utilisant la règle de corps  $x \times 1/x = 1$  si  $x \neq 0$  et en permutant les éléments du monôme si nécessaire, c'est-à-dire s'il reste des inverses et que la règle de corps ne peut pas s'appliquer.
- Recommencer le processus s'il reste encore des inverses.

### Exemple

$$x \times \left( \frac{1}{x} + \frac{x}{x+y} \right) = \left( -\frac{1}{y} \right) \times y \times \left( - \left( \frac{x \times x}{x+y} \right) - 1 \right)$$

On transforme  $x - y$  en  $x + (-y)$  et  $x/y$  en  $x \times 1/y$ .

$$x \times \left( \frac{1}{x} + x \times \frac{1}{x+y} \right) = \left( -\frac{1}{y} \right) \times y \times \left( - \left( (x \times x) \times \frac{1}{x+y} \right) + (-1) \right)$$

On construit le produit d'inverses  $p = x \times ((x + y) \times (y \times (x + y)))$ .

On distribue totalement à gauche et à droite de l'égalité, excepté dans les inverses.

$$x \times \frac{1}{x} + x \times x \times \frac{1}{x+y} = (-1) \times \frac{1}{y} \times y \times \left( (-1) \times \left( (x \times x) \times \frac{1}{x+y} \right) \right) + (-1) \times \frac{1}{y} \times y \times (-1)$$

On associe à droite chaque monôme, excepté dans les inverses.

$$x \times \frac{1}{x} + x \times \left( x \times \frac{1}{x+y} \right) = (-1) \times \left( \frac{1}{y} \times \left( y \times \left( (-1) \times \left( (x \times x) \times \frac{1}{x+y} \right) \right) \right) \right) \\ + (-1) \times \left( \frac{1}{y} \times (y \times (-1)) \right)$$

On multiplie à gauche et à droite par  $p$ , en générant la condition de correction.

$$(x \times ((x+y) \times (y \times (x+y)))) \times \left( x \times \frac{1}{x} + x \times \left( x \times \frac{1}{x+y} \right) \right) \\ = (x \times ((x+y) \times (y \times (x+y)))) \times \\ \left( (-1) \times \left( \frac{1}{y} \times \left( y \times \left( (-1) \times \left( (x \times x) \times \frac{1}{x+y} \right) \right) \right) \right) \right) \\ + (-1) \times \left( \frac{1}{y} \times (y \times (-1)) \right)$$

avec  $x \times ((x+y) \times (y \times (x+y))) \neq 0$ .

On distribue ce produit sans réassocier à droite.

$$(x \times ((x+y) \times (y \times (x+y)))) \times \left( x \times \frac{1}{x} \right) \\ + (x \times ((x+y) \times (y \times (x+y)))) \times \left( x \times \left( x \times \frac{1}{x+y} \right) \right) \\ = (x \times ((x+y) \times (y \times (x+y)))) \\ \times \left( (-1) \times \left( \frac{1}{y} \times \left( y \times \left( (-1) \times \left( (x \times x) \times \frac{1}{x+y} \right) \right) \right) \right) \right) \\ + (x \times ((x+y) \times (y \times (x+y)))) \times \left( (-1) \times \left( \frac{1}{y} \times (y \times (-1)) \right) \right)$$

On élimine les inverses en permutant si nécessaire.

$$((x+y) \times (y \times (x+y))) \times x + (x \times (y \times (x+y))) \times x \times x = \\ (x \times (x+y)) \times ((-1) \times (y \times ((-1) \times (x \times x)))) + (x \times ((x+y) \times (x+y))) \times ((-1) \times (y \times (-1)))$$

Il ne reste pas d'inverse, mais une égalité avec additions et multiplications que **ring** sait résoudre.

### 2.3 Limites

Après les réels, on veut naturellement faire de l'analyse et définir les notions de limites, dérivabilité... Pour cela, on définit un espace métrique avec un type de base et une distance.

```
Record Metric_Space : Type :=
  {Base : Type;
   dist : Base -> Base -> R;
   dist_pos : forall x y:Base, dist x y >= 0;
   dist_sym : forall x y:Base, dist x y = dist y x;
   dist_refl : forall x y:Base, dist x y = 0 <-> x = y;
   dist_tri : forall x y z:Base, dist x y <= dist x z + dist z y}.
```

la limite est alors définie de la manière usuelle :

```
Definition limit_in (X X':Metric_Space) (f:Base X -> Base X')
  (D:Base X -> Prop) (x0:Base X) (l:Base X') :=
  forall eps:R,
    eps > 0 ->
      exists alp : R,
        alp > 0 /\
          (forall x:Base X, D x /\ dist X x x0 < alp -> dist X' (f x) l < eps).
```

Les réels sont ensuite considérés comme un espace métrique ( $R_{\text{met}}$ ) avec la distance  $R_{\text{abs}}$  (valeur absolue).

```
Definition limit1_in (f:R -> R) (D:R -> Prop) (l x0:R) : Prop :=
  limit_in R_met R_met f D x0 l.
```

On peut alors démontrer toutes les propriétés usuelles de la limite (addition, multiplication, multiplication par une constante...).

De là, on définit alors la continuité et la dérivabilité :

```
Definition D_x (D:R -> Prop) (y x:R) : Prop := D x /\ y <> x.
```

```
Definition continue_in (f:R -> R) (D:R -> Prop) (x0:R) : Prop :=
  limit1_in f (D_x D x0) (f x0) x0.
```

```
Definition D_in (f d:R -> R) (D:R -> Prop) (x0:R) : Prop :=
  limit1_in (fun x:R => (f x - f x0) / (x - x0)) (D_x D x0) (d x0) x0.
```

On peut là encore démontrer les propriétés usuelles sur la dérivée.

## 2.4 Sommes infinies

On peut définir ensuite  $\sum_{i=0}^N fi$  comme un point fixe et  $\sum_{i=0}^{+\infty} fi$  comme une limite :

```
Fixpoint sum_f_R0 (f:nat -> R) (N:nat) {struct N} : R :=
  match N with
  | 0 => f 0%nat
  | S i => sum_f_R0 f i + f (S i)
  end.
```

```
Definition infinite_sum (s:nat -> R) (l:R) : Prop :=
  forall eps:R, eps > 0 ->
    exists N : nat,
      (forall n:nat, (n >= N)%nat -> R_dist (sum_f_R0 s n) l < eps).
```

On peut alors définir l'exponentielle et le cosinus comme des sommes infinies :

```
Definition exp_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => / INR (fact i) * x ^ i) l.
```

```
Definition cos_n (n:nat) : R := (-1) ^ n / INR (fact (2 * n)).
```

```
Definition cos_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => cos_n i * x ^ i) l.
```

Reste à prouver que ces sommes convergent (cf TD).

## 2.5 Élimination des quantificateurs

Une méthode d'élimination des quantificateurs sur  $\mathbb{R}$  par l'élaboration de tableaux de signes. Voir [2].

## Références

- [1] Herman Geuvers and Milad Niqui. Constructive reals in Coq : Axioms and categoricity. In Paul Callaghan, Zhaohui Luo, James McKinna, and Robert Pollack, editors, *Types for Proofs and Programs : International Workshop, TYPES 2000, Durham, UK, December 8–12, 2000. Selected Papers*, volume 2277 of *Lecture Notes in Computer Science*, pages 79–95. Springer-Verlag, 2002.
- [2] Assia Mahboubi and Loïc Pottier. Élimination des quantificateurs sur les réels en Coq. In *Journées Francophones des Langages Applicatifs, Anglet*, January 2002.
- [3] Micaela Mayero. *Formalisation et automatization de preuves en analyses réelle et numérique*. PhD thesis, Université Paris VI, décembre 2001.