Construction des nombres algébriques réels en Coq

Cyril Cohen

INRIA Saclay–Île-de-France
Laboratoire d'Informatique de l'École polytechnique,
91128 Palaiseau CEDEX, France
cohen@crans.org

Résumé

Cet article présente une construction en Coq de l'ensemble des nombres algébriques réels, ainsi qu'une preuve formelle que cet ensemble est muni d'une structure de corps réel clos discret archimédien. Cette construction vient ainsi implémenter une interface de corps réel clos réalisée dans un travail antérieur et bénéficie alors de la propriété d'élimination des quantificateurs, formellement prouvée pour toute instance de l'interface. Ce travail est destiné à servir de fondement à une construction de l'ensemble des nombres algébriques complexes, ainsi que d'implémentation de référence pour la certification des nombreux algorithmes de calcul formel qui utilisent des nombres algébriques.

Introduction

Les nombres algébriques réels sont le sous-ensemble dénombrable des réels formé des racines réelles de polynômes à coefficients rationnels. Les nombres rationnels sont strictement inclus dans les algébriques réels : $\sqrt{2}$ est la racine du polynôme à coefficients rationnels $X^2 - 2$, et ce n'est pas un nombre rationnel. De même, les nombres algébriques réels sont strictement inclus dans les nombres réels, car on peut exhiber des nombres transcendants, c'est à dire des nombres réels qui ne sont pas algébriques, comme π ou e [Hil93].

Ce sous-ensemble des nombres algébriques possède des propriétés intéressantes qui en font un objet important pour l'algorithmique en calcul formel comme pour les mathématiques constructives. Ainsi, il existe une procédure effective de comparaison des nombres algébriques, et toutes les opérations de corps peuvent être implémentées de façon exacte. Par ailleurs, ils sont munis d'une structure de corps réel clos archimédien, c'est à dire de corps ordonné archimédien vérifiant la propriété des valeurs intermédiaires pour les polynômes.

Le but de cet article est de montrer comment définir en Coq un type représentant les nombres algébriques réels et de décrire les preuves formelles mises en oeuvre pour montrer que ce type est muni d'une structure de corps réel clos archimédien. Cette construction et ces preuves sont décrites dans de nombreux textes standard de mathématiques constructives [MRR88] ou de calcul formel [Bos03]. Malgré tout, l'implémentation de ces résultats dans un assistant à la preuve demande comme souvent une réflexion plus poussée sur la nature des objets implémentés et des preuves formalisées. Ainsi notre développement n'est-il pas la formalisation linéaire d'une référence bien choisie, mais une synthèse de la littérature, qui choisit selon les preuves le point de vue le plus aisé pour la formalisation en théorie des types.

Pour implémenter un type de donnée représentant les algébriques réels, la littérature suggère usuellement une des deux stratégies suivantes. La première consiste à partir d'un type représentant les nombres réels (éventuellement les réels effectifs), et de former le type du sous-ensemble de ses

habitants qui sont racines d'un polynôme à coefficients rationnels, grâce à un sigma-type. Il faudra alors montrer que la restriction des opérations d'arithmétique réelle à ce sigma-type a les propriétés attendues. Une autre possibilité est de partir d'un type représentant les nombres rationnels, et de formaliser la construction de la clôture réelle des rationnels, c'est à dire du plus petit corps réel clos qui contient les rationnels. Un élément de la clôture est alors usuellement représenté comme un couple polynôme-intervalle, vérifiant l'invariant que le polynôme a une unique racine dans l'intervalle, cette racine étant l'algébrique encodé par ce couple. D'un point de vue constructif, il n'y a pas de raison absolue de privilégier l'une ou l'autre des stratégies : il est évidemment possible dans les deux cas de mener à bien toutes les preuves nécessaires. Par contre, la formalisation de ces résultats en théorie des types fait apparaître de significatives différences dans la nature des preuves mais aussi des objets que l'on manipule.

Dans ce travail, nous avons combiné ces deux approches, afin de bénéficier de leurs avantages respectifs tout en évitant leurs inconvénients. La présentation des algébriques réels comme sigma-type sur un type de réels exacts permet d'accéder lorsque nécessaire à une approximation arbitrairement précise de tout algébrique. Par contre, la formalisation de la relation d'égalité effective sur ce sous-ensemble des réels demande plus de travail, les réels exacts n'étant pas naturellement munis d'une telle relation. La présentation comme couple polynôme-intervalle demande au contraire du travail pour implémenter les opérations : il faut en effet les construire de sorte qu'elles calculent non seulement un polynôme annulateur du résultat, mais aussi un intervalle suffisamment précis. Par contre, elle permet d'exhiber un type de donnée dénombrable adapté à la construction du type quotient, muni de la relation d'égalité effective attendue.

Des bibliothèques de preuves constructives sur les réels exacts sont disponibles dans le système Coq [GN02]. Néanmoins, pour les besoins de cette formalisation, nous avons développé une courte bibliothèque construisant les nombres réels exacts, comme suites de Cauchy de rationnels. En effet certains choix de formalisation présents dans les bibliothèques déjà disponibles étaient difficilement compatibles avec nos besoins, et le peu de théorie sur les réels exacts nécessaire pour le présent travail nous a convaincus que la solution la plus satisfaisante était de nous essayer à une nouvelle formalisation. Nous expliquons ces choix de formalisation et notre construction dans la section 2, ainsi que la définition d'un premier type pour les algébriques réels, que nous appelons *algébriques réels de Cauchy*.

Puis, nous nous intéressons dans la section 3 à la définition des opérations arithmétiques et de la comparaison sur les *algébriques réels de Cauchy*. En particulier, nous montrons comment calculer les polynômes annulateurs, décider l'égalité et plus généralement la comparaison.

Nous décrivons ensuite dans la section 4 comment réaliser la construction de la clôture réelle des rationnels, afin de former un second type pour les algébriques réels, que nous appelons *domaine des algébriques réels*. Grâce à cette nouvelle construction et à la procédure de décision de l'égalité, nous pouvons alors effectuer un quotient de types.

Une fois le type quotient des *algébriques réels* formé, il faut prouver qu'il s'agit d'un corps réel clos. Dans la section 5 nous montrons qu'il est facile de montrer la plupart des propriétés de corps ordonné par passage au quotient. Nous montrons également comment obtenir, avec un peu plus de travail, la propriété des valeurs intermédiaires pour les polynômes, avant de conclure.

1. Préliminaires

Nous utilisons dans ce travail les librairies fournies par la bibliothèque SSReflect du projet *Mathematical Components* [Pro]. Nous nous basons en particulier sur la hiérarchie algébrique [GGMR09], avec les extensions que nous avons apportées pour décrire les structures discrètes ordonnées [CM]. Nous utilisons ici principalement la structure de corps réel clos discret. Nous bénéficions aussi des outils fournis sur les polynômes à coefficients dans un corps. En particulier nous utilisons

la bibliothèque d'arithmétique polynomiale : opérations arithmétiques, division euclidienne, pgcd, théorème de Bézout, théorème de Gauss.

Voici plus en détail certains des éléments de la bibliothèque SSReflect que nous utilisons.

Structure de choix

Dans la librairie SSReflect, les structures de la hiérarchie algébriques sont munies d'un opérateur de choix. Cela signifie que l'on dispose d'un opérateur `xchoose` de type :

```
xchoose : ∀(P : F →bool), (∃x, P x) →F.
```

qui est un opérateur de choix, au sens où il satisfait la propriété suivante :

```
xchooseP : ∀(P : F →bool) (xP : F), P (f P xP).
```

ainsi que la compatibilité extensionnelle :

```
eq_xchoose : ∀(P Q : F →bool) (xP xQ : F), P =1 Q →f P xP = f Q xQ.
```

En particulier, dans la logique de Coq, tout type présentant un cardinal dénombrable d'habitants est prouvablement muni d'un tel opérateur. Ainsi on peut prendre pour F un type représentant les rationnels $\mathbb{Q}$.

Le résultant de deux polynômes

La notion de résultant est basée sur les matrices de la librairie SSReflect décrites dans [Gon11]. Le résultant de deux polynômes $P = \sum_{i=0}^{m} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$ est défini comme le déterminant de la matrice de Sylvester, qui est carrée de dimension $(m+1)+(n+1)$:

$$\begin{vmatrix} p_m & p_{m-1} & \cdots & p_0 & 0 & 0 & \cdots & 0 \\ 0 & p_m & p_{m-1} & \cdots & p_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & p_m & p_{m-1} & \cdots & p_0 & 0 \\ 0 & \cdots & 0 & 0 & p_m & p_{m-1} & \cdots & p_0 \\ q_n & q_{m-1} & \cdots & q_0 & 0 & 0 & \cdots & 0 \\ 0 & q_n & q_{m-1} & \cdots & q_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & q_n & q_{m-1} & \cdots & q_0 & 0 \\ 0 & \cdots & 0 & 0 & q_n & q_{m-1} & \cdots & q_0 \end{vmatrix}$$

En fait, nous n'utiliserons que deux propriétés du résultant, indépendemment de son implémentation : le résultant de P et Q est une combinaison linéaire de P et Q, et il est non nul si et seulement si P et Q sont premiers entre eux.

La notion de résultant est présentée et traitée dans de nombreux ouvrages (dont par exemple [Lan02]). Dans notre développement, il est nécessaire de prouver que certains résultants de deux polynômes P et Q sont non nuls. La preuve classique, et usuellement présentée, fait intervenir la factorisation de P et Q dans un corps où ils sont scindés. Il y a là un problème, car nous sommes justement en train de construire la clôture algébrique qui nous permettrait de scinder P et Q. On pourrait également se contenter de construire un corps de décomposition pour P et Q, mais cela demanderait un travail important. Heureusement, il existe des preuves arithmétiques de non nullité de chacun des trois résultants que nous utilisons dans cette formalisation. N'ayant pas trouvé les références de ces preuves dans la littérature (elle existent cependant sûrement), nous les détaillons à chaque fois.

2. Construction des *réels et algébriques de Cauchy*

2.1. Description mathématique et type de donnée Coq

On construit les réels de Cauchy comme la donnée d'une suite $(x_n)_n$ d'éléments de F et d'un module de convergence $m_x : F \to \mathbb{N}$, tel qu'à partir de $m_x(\varepsilon)$ tous les éléments de la suite sont à une distance deux à deux de moins de ε. C'est à dire tels que

$$\forall \varepsilon\ \forall i\ \forall j\ ,\ m_x(\varepsilon) \leq i\ \wedge\ m_x(\varepsilon) \leq j\ \Rightarrow\ |x_i - x_j| < \varepsilon$$

Les suites d'éléments de F sont représentées par des fonctions des entiers à valeurs dans F. Pour définir une suite de Cauchy, on adjoint à une telle suite un module de convergence et une preuve que celui-ci est respecté. Le type des réels de Cauchy est donc défini comme la sous-famille des fontions des entiers à valeurs dans F pour lesquelles on sait expliciter un module de convergence :

```
Definition creal_axiom (x : nat →F) :=
  {m : F →nat | ∀ε i j, m ε ≤i →m ε ≤j →`| x i - x j | < ε}.
Inductive creal := CReal {cauchyseq :> nat →F;
                                  _ : creal_axiom cauchyseq}.
```

Rappelons que la notation `{m : F →nat | ...}` se lit "il existe `(m : F →nat)` tel que ...". Il s'agit d'un énoncé existentiel, mais dans la sorte `Type` de la logique de Coq, alors que le connecteur usuel `exists` forme un énoncé dans la sorte `Prop`. Un énoncé dans `Prop` ne pourra être utilisé que dans le contexte d'une preuve dont le but est dans `Prop`. En particulier on ne pourra pas utiliser le témoin pour calculer une valeur dans `Type`.

La bibliothèque C-CoRN [GN02] implémente elle aussi un type de donnée pour les réels de Cauchy, et leur définition repose de la même façon sur un existentiel dans la sorte `Type`, motivé par les même considérations : cette donnée fait partie intégrante des éléments nécessaires au calcul sur les réels et les algébriques. En particulier, on verra en section 2.4 que le module de Cauchy est nécessaire pour calculer l'inverse d'un réel.

Cependant, notre définition diffère de celle choisie dans C-CoRN par deux aspects importants :

La propriété est skolemisée : on utilise une formule du type $\exists m, \forall \varepsilon, \ldots$ où m est une fonction à valeurs entières, plutôt que $\forall \varepsilon, \exists N, \ldots$ où N est un entier. Même si les deux formulations sont en fait équivalentes, on va vraiment tirer parti du fait que l'existentiel soit en tête.

La propriété est symétrique par rapport à i et j. En effet, les termes x_i et x_j de la suite sont échangeable ; i et j sont indépendants l'un de l'autre. On pourra faire les preuves sans se soucier d'avoir à faire apparaître un i ou j particulier.

Dans cet article, nous dénoterons souvent une suite de Cauchy $(x_n)_n$ de module de convergence m_x par la notation $\bar{x}$. Cet élément sera appelé un *réel de Cauchy* et représente un nombre réel constructif. Nous prendrons régulièrement le i^{me} élément de la suite de Cauchy associée à $\bar{x}$ que nous noterons x_i. Par ailleurs, dans le code Coq, m_x correspond à la fonction `((cauchymod x) : F →nat)`. Notons qu'une telle fonction Coq est définissable car l'existentiel dans la définition de suite de Cauchy est dans `Type`.

Par définition des suites de Cauchy, on obtient le lemme suivant :

```
Lemma cauchymodP (x : creal) (ε : F) (i j : nat) :
                    cauchymod x ε ≤i →cauchymod x ε ≤j →`| x i - x j | < ε
```

Il est important de remarquer que lorsqu'on applique ce lemme, on produit des sous-buts de la forme $\varepsilon \leq i$, ce que nous appelons des conditions de bord (side condition). La forme de ces conditions de bord là suit un schéma qui se reproduit de manière générale dans ce développement : on génère dès

que possible des conditions de la forme $f_k(\varepsilon) \leq i$. Si c'est le seul type de contrainte qui peut apparaître sur i, cela veut dire qu'il suffira de choisir i comme le maximum de tous les $f_k(\varepsilon)$ pouvant apparaître au cours d'une preuve donnée. Cela fait d'ailleurs l'objet d'une tactique qui permet d'automatiser la recherche de condition de cette forme et l'ajout du terme $f_k(\varepsilon)$ à une variable existentielle. En particulier un certain nombre de preuves commencent par une tactique signifiant "soit i suffisamment grand".

L'existence de la fonction `cauchymod` permet entre autres choses de définir une fonction ubound permettant de majorer les valeurs prise par les éléments de la suite de Cauchy. Elle vérifie donc la propriété suivante :

```
Lemma uboundP (x : creal) (i : nat) : `| x i | ≤ubound x.
```

Par la suite, une telle fonction servira à calculer les modules de convergence de nombreuses suites de Cauchy. On adopte la notation mathématique $\lceil x \rceil$ pour dénoter `(ubound x)`.

2.2. La comparaison

Pour comparer $\bar{x}$ et $\bar{y}$, il s'agit de savoir si la suite des distances point à point $x_n - y_n$ converge vers 0 ou est minorée par un élément donné. Tout d'abord, ce n'est pas un problème décidable. Le problème de savoir si deux *réels de Cauchy* sont différent est par contre semi-décidable : en regardant suffisamment loin on peut se rendre compte que deux éléments sont distincts, mais l'on est jamais certain qu'ils soient égaux. Ainsi l'opérateur primitif n'est pas l'égalité mais l'inégalité. En effet l'inégalité contient une information supplémentaire : le témoin minorant la suite des $|x_n|$.

Par commodité on écrira $\bar{x} \neq \bar{y}$ si les deux suites sont différentes en tant que *réel de Cauchy*, et $\bar{x} \equiv \bar{y}$ si elles ne sont pas différentes, c'est-à-dire si elles représentent le même *réel de Cauchy* (i.e. si la différence tend vers 0).

On pourrait donc définir l'inégalité ainsi :

```
{ε | 0 < ε & ∀i, cauchymod x ε ≤i → cauchymod y ε ≤i → `|x i - y i| ≥ε}.
```

Si on sait qu'une suite $\bar{x}$ est distincte de 0 (au sens de la comparaison décrite ci-dessus) on devrait pouvoir en extraire le témoin δ, minorant la suite des valeurs absolues. Ce témoin sera utile pour calculer l'inverse (entre autres) et devra donc être extractible.

Malheureusement, cela impose que le témoin soit dans `Type` et donc que l'inégalité soit à valeurs dans `Type` et non dans `Prop`. Ceci pose des problèmes pour munir notre type des *réels de Cauchy* d'une structure de sétoïde. Ce type de problème a déjà été rencontré pour C-CoRN par Russell O'Connor et Robbert Krebbers [KS11] et a été résolu en utilisant le théorème "constructive indefinite description" qui est prouvable pour les propriétés décidables dont le domaine de départ est `nat`. Notre solution consiste à utiliser une variante de ce théorème : grâce à la structure de `choiceType` de `F` et à la bibliothèque SSReflect sur les structures de choix, on peut utiliser le théorème suivant directement sur F :

```
Lemma sigW (P : F → bool) : (∃x, P x) → {x | P x}.
```

Pour que la traduction soit possible, il suffirait donc que la définition de l'inégalité entre *réels de Cauchy* soit de la forme `(∃e, P e)`, où `P` est une propriété booléenne (grâce à l'opérateur de choix). Or, tel qu'exposé ci-dessus, la propriété est de la forme `(∀i, ...)`.

Cependant, comme on travaille sur des suites de Cauchy, on sait contrôler l'écart entre deux éléments de la suite à partir d'un certain rang. Il suffit de définir l'inégalité ainsi :

```
Definition neq_creal (x y : creal) : Prop :=
  ∃ε, (0 < ε) && (ε * 3%:R ≤`|x (cauchymod x ε) - y (cauchymod y ε)|).
```

Et grâce à `sigW`, on peut transformer la quantification existentielle (`∃ε, ...`) dans `Prop` en une existentielle `{ ε | ... }` dans `Type`. Ainsi, à partir de `(cauchymod x ε)` et `(cauchymod y ε)` l'écart entre les x_i est borné par ε, de même pour les y_i, ce qui fait que `‘|x i - y i|` est minorée par ε lorsque i est plus grand que `(cauchymod x ε)` et `(cauchymod y ε)` . Notre nouvelle définition est équivalente à la précédente.

Grâce à ce procédé, on peut définir une fonction (`lbound`: `∀x y, x ≠y →F`) qui vérifie la propriété suivante :

```
Lemma lboundP (x y : creal) (neq_xy : x ≠y) i :
  cauchymod x (lbound neq_xy) ≤i →
  cauchymod y (lbound neq_xy) ≤i →lbound neq_xy ≤‘|x i - y i|.
```

2.3. La relation d'ordre

Le traitement de la relation d'ordre se fait de la même manière que celui des relations d'inégalité et d'égalité. La notion primitive est celle d'ordre strict, dont la négation définit l'ordre large. On s'inquiète finalement assez peu de l'ordre, puisqu'il est possible de prouver le lemme suivant sur les suites de Cauchy :

```
Lemma neq_ltVgt (x y : creal) : x ≠y →{x < y} + {y < x}.
```

On omettra souvent le traitement des propriétés de la relation d'ordre afin de ne pas surcharger cet article, sachant que les notions et preuves sont souvent similaires à celles des relations d'inégalité et d'égalité.

2.4. Opérations arithmétiques sur les *réels de Cauchy*

Il est facile de construire les opérations d'addition, d'opposé et de multiplication, et de prouver qu'il s'agit encore de suites de Cauchy, en explicitant le module de convergence. On procédera systématiquement de la même manière : on fera l'opération sur la suite terme à terme, puis on cherchera à munir la suite des opérations terme à terme d'un module de convergence.

Pour construire l'opposé, l'addition et la multiplication. Nous allons montrer comment construire les modules de convergence pour l'opposé, l'addition et la multiplication de *réels de Cauchy*. On prouve facilement que le module m_x de $\bar{x}$ est aussi un module de convergence pour $(-x_n)_n$.

On vérifie également que le module de $(x_n + y_n)_n$ est donné par $\varepsilon \mapsto \max\left(m_x\left(\frac{\varepsilon}{2}\right), m_y\left(\frac{\varepsilon}{2}\right)\right)$.

Enfin, le module de $(x_n y_n)_n$ est donné par $\varepsilon \mapsto \max\left(m_x\left(\frac{\varepsilon}{2\lceil y\rceil}\right), m_y\left(\frac{\varepsilon}{2\lceil y\rceil}\right)\right)$.

Pour construire l'inverse Il faut savoir trouver un minorant δ pour la suite des valeurs absolues $(|x_n|)_n$, et l'utiliser pour prouver que l'inverse terme à terme $(\frac{1}{x_n})_n$ est une suite de Cauchy. D'après la section 2.2, un tel minorant est donné par `(lbound x_neq0)` dès que l'on a une preuve `(x_neq0 : x ≠0)` que $\bar{x}$ est distinct de 0 (au sens des suites de Cauchy).

Dès lors, on prend i et j suffisamment grands. Et alors si i et j sont plus grands que $m_x(\varepsilon\delta^2)$ on a

$$|x_i - x_j| < \varepsilon\delta^2$$

Par définition de δ et si i et j sont plus grands que $m_x(\delta)$, on a : $|x_j - x_i| < \varepsilon|x_i x_j|$. Et donc

$$\left|\frac{1}{x_i} - \frac{1}{x_i}\right| < \varepsilon$$

C'est pourquoi on peut prendre la fonction $\varepsilon \mapsto \max\big(m_x(\varepsilon\delta^2), m_x(\delta)\big)$ comme module de convergence de la suite $(\frac{1}{x_n})_n$.

Propriété de morphisme des opérations arithmétiques Il est aisé de vérifier que toutes les opérations arithmétiques commutent avec la relation d'égalité des suites de Cauchy, par un simple examen terme à terme. La relation d'ordre aussi est trivialement un morphisme pour l'égalité.

2.5. Bornes sur les polynômes

On va enfin décrire l'application d'un polynôme dans $F[X]$ à un *réel de Cauchy* : il s'agit encore une fois d'une opération terme à terme. Cependant, pour prouver qu'il s'agit d'une suite de Cauchy, il faut savoir borner $|P(x) - P(y)|$ pour $|x - y|$ suffisamment petit.

Pour obtenir de telles bornes avec finesse, l'idéal serait d'utiliser l'arithmétique d'intervalle. Cependant, nous ne nous préoccupons pas ici de savoir faire des calculs efficaces avec les structures que nous avons mises en place, car elles ne sont pas adaptées pour ça. Nous utiliserons donc des bornes grossières données par le développement de Taylor pour les polynômes :

Étant donné un polynôme $P = \sum_{i=0}^{n} p_i X^i$, on définit les bornes suivantes.

$$\begin{aligned}
B_0(P,c,r) &= 1 + \sum_{i=0}^{n} |p_i|(|c| + |r|)^i \\
B_1(P,c,r) &= \max(1,2r)^n(1 + \sum_{i=1}^{n} \frac{B_0(P^{(i)},c,r)}{i!} \\
B_2(P,c,r) &= \max(1,2r)^{n-1}(1 + \sum_{i=2}^{n} \frac{B_0(P^{(i)},c,r)}{i!}
\end{aligned}$$

Ces bornes vérifient les propriétés suivantes : si x et y sont tels que $|x - c| \leq r$ et $|y - c| \leq r$, alors

$$\begin{aligned}
|P(x)| &\leq B_0(P,c,r) \\
|P(y) - P(x)| &\leq |y - x| B_1(P,c,r) \\
\left|\frac{P(y) - P(x)}{y - x} - P'(x)\right| &\leq |y - x| B_2(P,c,r)
\end{aligned}$$

La borne B_1 permet donc de trouver le module de convergence de la suite $P(\bar{x})$. En effet, il suffit de prendre par exemple :

$$\varepsilon \mapsto m_x\left(\frac{\varepsilon}{B_1(P,0,\lceil x \rceil)}\right)$$

On prouve ensuite que $P(\bar{x}) \neq P(\bar{y}) \Rightarrow \bar{x} \neq \bar{y}$. Ce qui entraîne que $\bar{x} \equiv \bar{y} \Rightarrow P(\bar{x}) \equiv P(\bar{y})$ donc que l'évaluation d'un polynôme en un *réel de Cauchy* est un morphisme pour l'égalité (de Leibniz) des polynômes et pour l'égalité (sétoïde) des *réels de Cauchy*.

2.6. Construction des *algébriques réels de Cauchy*

Les constructions de cette section permettent d'aboutir à la formalisation des *algébriques réels de Cauchy*. Ils sont définis comme le sigma-type formé par les *réels de Cauchy* x tels qu'il existe un polynôme unitaire annulant x.

```
Inductive alg_creal := AlgCReal {
  creal_of_alg :> creal;
  poly_of_alg_creal : {poly F};
  _ : monic poly_of_alg_creal;
  _ : poly_of_alg_creal.[creal_of_alg] ≡0
}.
```

C'est avec cette représentation qu'on implémente les opérations arithmétiques sur les algébriques réels, ainsi que l'algorithme de comparaison.

3. Décision de l'égalité et opérations arithmétiques

On commence par prouver que le type des *algébriques réels de Cauchy* est discret, c'est-à-dire que l'égalité sétoïde héritée des *réels de Cauchy* y est décidable. On construira ensuite les opérations arithmétiques.

3.1. Décision de l'égalité

Alors que la comparaison entre *réels de Cauchy* n'est que semi-décidable, la comparaison entre *algébriques réels de Cauchy* est quant à elle décidable. Pour construire la procédure de décision de l'égalité entre $\bar{x}$ et $\bar{y}$, on va bien sûr devoir utiliser l'information apportée par leurs polynômes annulateurs. Ainsi, soient P et Q les polynômes annulateurs de deux *réels de Cauchy* $\bar{x}$ et $\bar{y}$. On a deux cas :

Soit P et Q sont premiers entre eux. Grâce à la relation de Bézout, on peut dire qu'il existe U et V tels que $UP + VQ = 1$. Comme $P(\bar{x})$ tend vers 0 et que U et V sont majorés sur l'intervalle que l'on considère, si n est suffisamment grand on a : $|Q(x_n)| \geq \frac{1}{2\lceil U(x)\rceil}$. $Q(\bar{x})$ ne peut pas s'annuler, donc $P(\bar{x}) \neq Q(\bar{y})$ et nécessairement $\bar{x} \neq \bar{y}$.

Soit P et Q ne sont pas premiers entre eux Comme P et Q sont unitaires, on sait que soit l'égalité $P = Q$ est vérifiée, soit le pgcd de P et Q n'est pas trivial (c'est à dire différent de 1, P, Q).

Dans le cas où le pgcd n'est pas trivial, on sait trouver un facteur D_P de P et un facteur D_Q de Q de degrés respectivement inférieurs à ceux de P et Q tels que $D_P(x) \equiv 0$ et $D_Q(y) \equiv 0$. Ceci permet de se ramener à l'étude de $(\bar{x}, D_P)$ et $(\bar{y}, D_Q)$.

Dans le cas où $P = Q$. Si P et P' ne sont pas premiers entre eux, on peut trouver deux facteurs propres D_P et D_Q de P qui annulent encore respectivement x et y. On se ramène donc encore à l'étude de $(\bar{x}, D_P)$ et $(\bar{y}, D_Q)$.

Si par contre P et P' sont premiers entre eux. Grâce à la relation de Bézout, on peut dire qu'il existe U et V tels que $UP + VP' = 1$. Comme $P(\bar{x})$ tend vers 0 et que U et V sont majorés sur l'intervalle que l'on considère, si n est suffisamment grand on a :

$$|P'(x_n)| \geq \frac{1}{2\lceil U(\bar{x})\rceil} \qquad \text{et} \qquad |P'(y_n)| \geq \frac{1}{2\lceil U(\bar{y})\rceil}$$

On peut en déduire que P est monotone sur deux intervalles $[a, b]$ et $[c, d]$ contenant respectivement x_n et y_n (grâce à la propriété de la borne B_2 décrite en section 2.5). Si l'intersection de ces deux intervalles est vide on en déduit que $\bar{x} \neq \bar{y}$, sinon on en déduit que $\bar{x} \equiv \bar{y}$.

Remarque : la décidabilité de l'ordre est une conséquence directe de ceci et du lemme `neq_ltVgt`, vu en section 2.3.

3.2. Opérations sur les *algébriques réels de Cauchy*

On construit toutes les opérations (addition, opposé, multiplication, inverse) à partir des constantes 0 et 1, de la différence et de la division. Les images des constantes $c \in F$ sont obtenues grâce au couple $(\bar{c}, X - c)$ (où $\bar{c}$ est une suite de Cauchy constante).

Dans le reste de cette section, on considère deux *algébriques réels de Cauchy* x et y, de suites de Cauchy respectives $\bar{x}$ et $\bar{y}$, et de polynômes annulateurs respectifs P et Q.

La différence

On rappelle (cf section 2.4) que la différence est obtenue grâce à la suite des différences terme à terme. Cherchons le polynôme qui annule cette suite de différences.

On considère le résultant

$$R(Y) = \mathrm{Res}_X\left(P(X+Y), Q(X)\right)$$

Il y a deux propriétés essentielles à prouver sur ce résultant : qu'il est non nul, et qu'il annule bien la différence.

R est non nul. On raisonne par l'absurde et on suppose que R est nul.

Par propriété du résultant, $P(X+Y)$ et $Q(X)$ ne peuvent pas être premiers entre eux.

Le théorème de Bézout pour les polynômes non premiers entre eux nous donne l'existence de $U, V \in F[X]$ tels que U est non nul, $\deg_X(U) < \deg(Q)$ et

$$U(X,Y)P(X+Y) = V(X,Y)Q(X)$$

En prenant le coefficient de tête en Y, on obtient :

$$u(X) = v(X)Q(X)$$

où u et v sont les coefficients de têtes respectifs de $U(X,Y)$ et $V(X,Y)$ pris par rapport à la variable Y. Cette équation donne $\deg(Q) \leq \deg(u)$, mais d'autre part $\deg(u) \leq \deg_X(U) < \deg(Q)$ D'où la contradiction.

R annule la différence. Prouvons que R annule la suite de Cauchy $\bar{x} - \bar{y}$. Comme R est dans l'idéal engendré par $P(XY)$ et $Q(X)$, il existe U et V tels que $R(Y) = U(X,Y)P(X+Y) + V(X,Y)Q(X)$. Donc

$$R(x_n - y_n) = U(y_n, x_n - y_n)P(x_n) + U(y_n, x_n - y_n)Q(y_n)$$

Or $P(\bar{x}) \equiv 0$ et $P(\bar{y}) \equiv 0$. Pour prouver que $R(\bar{x} - \bar{y}) \equiv 0$, il suffit de pouvoir majorer les variations de $U(x,y)$ lorsque x et y prennent des valeurs dans des intervalles bornés. On sait déjà majorer les variations en x de $U(x,y)$ par $B_1'(y) = B_1(U(X,y), 0, \lceil x \rceil)$, et il est assez facile de majorer la variation en y de $B_1'(y)$.

La division

On rappelle (cf section 2.4) que la suite de Cauchy pour la division est obtenue grâce à la suite des division terme à terme. En fait on peut même se passer de la condition de non annulation du diviseur, car la comparaison à zéro est décidable. Ce qui permet de faire une discussion suivant la nullité du diviseur.

Quand le diviseur est nul, on renvoie le polynôme X par convention. Lorsque le diviseur n'est pas nul, on peut se ramener à un Q tel que $Q(0) \neq 0$ Le polynôme annulateur est alors obtenu par le résultant

$$R(Y) = \mathrm{Res}_X\left(P(XY), Q(X)\right)$$

Il y a deux propriétés essentielles à prouver sur ce résultant : qu'il est non nul, et qu'il annule bien le quotient.

R est non nul On raisonne par l'absurde et on suppose que R est nul.

Par propriété du résultant, $P(XY)$ et $Q(X)$ ne peuvent pas être premiers entre eux.

Le théorème de Bézout pour les polynômes non premiers entre eux nous donne l'existence de $U, V \in F[X]$ tels que U est non nul, $\deg_X(U) < \deg(Q)$ et

$$U(X,Y)P(XY) = V(X,Y)Q(X)$$

En évaluant la variable Y en 0 on obtient

$$U(X,0)P(0) = V(X,0)Q(X)$$

Si $V(X,0) = 0$, on a déjà $Y|V(X,Y)$, puis il y a deux cas :

- Soit $U(X,0) = 0$, ceci implique que $Y|U(X,Y)$. Il existe donc $U'(X,Y)$ et $V'(X,Y)$, de degrés en Y strictement plus petits, tels que :

$$U'(X,Y)P(XY) = V'(X,Y)Q(X)$$

- Soit $P(0) = 0$, ceci implique $X|P(X)$, et donc $XY|P(XY)$. D'autre part

$$U(0,Y)P(0) = V(0,Y)Q(0)$$

  et comme $Q(0) \neq 0$, on en déduit que nécessairement $V(0,Y) = 0$. Il en découle que $X|V(X,Y)$ et comme on savait déjà que $Y|V(X,Y)$, on en déduit que $XY|V(X,Y)$. Il existe donc P' et V' de degrés strictement plus petits tels que

$$U(X,Y)P'(XY) = V'(X,Y)Q(X)$$

Ainsi on peut supposer, sans perdre de généralité, qu'aucun des deux membres de l'égalité suivante ne s'annule.

$$U(X,0)P(0) = V(X,0)Q(X)$$

Cette équation donne $\deg(Q) \leq \deg(U(X,0))$, mais d'autre part $\deg(U(X,0)) \leq \deg_X(U) < \deg(Q)$. D'où la contradiction.

R annule le quotient De la même manière que pour la différence, on établit que $R(\frac{\bar{x}}{\bar{y}}) \equiv 0$

4. Mise en relation avec le *domaine des algébriques réels*

Le type de donnée des *algébriques réels de Cauchy* constitue un sétoïde, mais ce n'est pas suffisant pour l'équiper d'une structure de corps en utilisant la librairie SSReflect. Pour que cette librairie s'applique, il faut que l'égalité que l'on souhaite avoir sur les éléments soit équivalente à l'égalité de Leibniz, donc deux éléments ne doivent être vus comme égaux que s'ils sont intentionnellement égaux. Cela signifie qu'il faut trouver un type qui représente les nombres algébriques réels directement, et non au travers d'une équivalence et de mécanismes pour simuler le comportement de l'égalité. En plus

d'être adapté à la librairie SSReflect, un tel type est plus facile à manipuler, car il ne repose pas sur un mécanisme de réécriture externe (i.e. la réécriture sétoïde) lors des preuves, ce qui rend le système a priori plus rapide.

Afin d'obtenir un type qui représentera directement les algébriques, on propose d'effectuer un quotient de type. Pour faire cela il faut se ramener dans un cas où l'on sait faire un quotient constructif [Coh10]. On va donc créer un type que l'on appellera *domaine des algébriques réels* et qui servira de type de base pour effectuer le quotient. Pour pouvoir ensuite effectuer un quotient, il faut que ce type ait une structure de `choiceType` et que la relation d'équivalence soit décidable. Or on a déjà montré en 3.1 que la comparaison entre *algébriques réels de Cauchy* était décidable, il suffit donc de trouver une représentation prouvablement équivalente mais ayant une structure de `choiceType`.

On choisit la représentation suivante, dont la signification sera explicitée par la traduction en *algébriques réels de Cauchy*.

```
Inductive alg_dom := AlgRealDom {
  poly_of_alg : {poly F};
  center_alg : F;
  radius_alg : F;
  _ : monic poly_of_alg;
  _ : poly_of_alg.[center_alg - radius_alg]
      * poly_of_alg.[center_alg + radius_alg] ≤0
}.
```

Ce type de donnée est formé uniquement d'éléments de F (un polynôme à coefficients dans F et deux nombres de F) ainsi que de deux preuves booléennes. Ceci fait que `alg_dom` peut être encodé comme un sous-type des séquences d'éléments de F, et hérite ainsi de leur structure de `choiceType`.

On peut remarquer que ce type peut également être muni d'une structure de type dénombrable dès que F est dénombrable. Ce fait n'était pas directement évident pour le sétoïde des *algébriques réels de Cauchy*. En conséquence, le type quotient héritera de la structure de type dénombrable, le cas échéant.

On commence donc par montrer que cette présentation est équivalente à celle des *algébriques réels de Cauchy*, en explicitant les fonctions de traduction dans chaque sens.

4.1. Traduction vers les *algébriques réels de Cauchy*

On va construire la fonction

```
Definition to_alg_creal : alg_dom → alg_creal
```

On rappelle qu'un élément du *domaine des algébriques réels* contient la donnée d'un polynôme P, d'un centre c et d'un rayon r tels que $P(c-r)P(c+r) \leq 0$. La racine que l'on cherche à sélectionner est dans l'intervalle $I = [c-r, c+r]$.

La traduction d'un élément du *domaine des algébriques réels* en *algébrique réel de Cauchy* se fait par dichotomie. On va constituer une suite de Cauchy $\bar{x} = (x_n)_n$ telle que tous les x_n soient dans l'intervalle I et telle que $P(\bar{x}) \equiv \bar{0}$.

On va procéder par récurrence pour définir la suite $\bar{x}$. Celle-ci doit préserver l'invariant suivant :

$$H_n = P((x_n - 2^{-n}r)_n)P((x_n + 2^{-n}r)_n) \leq 0$$

Cas de base. On commence par poser $x_0 = c$. On a bien $P(x_0 - r)P(x_0 + r) \leq 0$

Étape de récurrence. Supposons que l'on ait construit x_n vérifiant l'invariant H_n. C'est-à-dire

$$P((x_n - 2^{-n}r)_n)P((x_n + 2^{-n}r)_n) \leq 0$$

Alors $a = x_n - 2^{-(n+1)}r$ ou $b = x_n + 2^{-(n+1)}r$ vérifie l'invariant H_{n+1} . En effet, sinon :

$$P(a - 2^{-(n+1)}r)P(a + 2^{-(n+1)}r)P(b - 2^{-(n+1)}r)P(b + 2^{-(n+1)}r) \geq 0$$

C'est-à-dire $P(x_n - 2^n r)(P(x_n))^2 P(x_n + 2^n r) \geq 0$, ce qui contredit H_n. On choisi donc

$$x_{n+1} = \begin{cases} a & \text{si } a \text{ vérifie l'invariant} \\ b & \text{sinon} \end{cases}$$

Enfin, on prouve sans problème que la suite $(x_n)_n$ ainsi définie est bien de Cauchy.

Il est important de remarquer ici qu'il n'est plus nécessaire d'imposer que le polynôme soit croissant sur l'intervalle, juste qu'il change de signe. Cette dernière condition n'impose que l'existence d'une racine dans l'intervalle, et non son unicité. En effet, on n'a plus besoin de l'unicité pour sélectionner une racine : il suffit de suivre le processus de dichotomie.

4.2. Traduction depuis les *algébriques réels de Cauchy*

La traduction inverse est plus difficile, on va construire une fonction

```
Definition to_alg_dom : alg_creal → alg_dom
```

qui vérifie la propriété suivante :

```
Lemma to_alg_domK x : to_alg_creal (to_alg_dom x) ≡ x.
```

Cette fois-ci, on va chercher à isoler un intervalle avec une seule racine, pour être sûr que la traduction inverse, décrite ci-dessus, permette d'obtenir le même résultat (modulo $\equiv$).

Il y a deux cas :

Si P et P' sont premiers entre eux, alors il existe U et V tels que $UP + VP' = 1$. Comme $P(\bar{x})$ tend vers 0 et que U et V sont majorés sur l'intervalle que l'on considère, si n est suffisamment grand on a : $P'(x_n) \geq \frac{1}{2\lceil U(x) \rceil}$. En prenant un intervalle $[a, b]$ suffisamment petit et contenant x_n, on obtient que P est monotone sur $[a, b]$ (grâce à la borne B_2 exhibée en section 2.5)

Sans perdre de généralité, on peut supposer que P est croissante. On a alors $P(a) \leq P(x_i) \leq P(b)$ pour tout $i \geq n$. Or $P(x_i)$ tend vers 0, donc $P(a) \leq 0 \leq P(b)$. (En appliquant ce raisonnement à $-P$ on traite le cas décroissant). On a donc isolé un intervalle avec une seule racine.

Si P et P' ne sont pas premiers entre eux, on peut trouver un facteur propre D de P qui annule encore x. Par récurrence, on se ramène donc encore à l'étude de $(\bar{x}, D)$, où le degré de D est strictement inférieur à celui de P.

4.3. Construction du type quotient

On construit le type `alg` des *algébriques réels* comme le quotient de `alg_dom` par la relation d'équivalence $\equiv$. Étant donné un corps F, on adoptera la notation mathématique $\bar{F}$ pour désigner `(alg F)`.

Au passage, on construit une fonction (`to_alg: F → alg F`). On prouve qu'il s'agit d'un morphisme de corps et que ce morphisme est également compatible avec la comparaison. La notation mathématique pour cette fonction sera $\uparrow$.

Il faut alors prouver la compatibilité des opérations arithmétiques (et de la relation d'ordre) avec ce passage au quotient. C'est une conséquence directe de la propriété de morphisme des opérations par rapport à l'égalité sétoïde, que l'on a traité dans la section 3.2.

Remarque : par construction de `alg_dom`, la preuve du théorème des valeurs intermédiaires sur $F[X]$ est triviale. Soit un polynôme $P \in F[X]$ et deux points $a < b \in F$ tels que $P(a) \leq 0 \leq P(b)$. La valeur intermédiaire est donnée par l'algébrique de $\bar{F}$ construit avec le polynôme P, le milieu $\frac{a+b}{2}$ et le rayon $\frac{b-a}{2}$. Par contre, ce n'est pas trivial pour les polynômes de $\bar{F}[X]$

5. Propriétés de corps réel clos

Dans un premier temps, il faut prouver que $\bar{F}$ est un corps discret totalement ordonné archimédien. Comme le corps de départ F possède déjà toute ces propriétés, elle se transmettent très facilement à $\bar{F}$ par étude de la suite terme à terme et par passage au quotient. Cette partie-là est donc triviale à formaliser.

La seule propriété problématique est celle qui permet de passer de corps discret totalement ordonné à corps réel clos : la propriété des valeurs intermédiaires pour les polynômes de $\bar{F}[X]$. Avec la remarque de la fin de la section 4.3, on sait déjà qu'elle est vraie pour les polynômes de $F[X]$.

On cherche donc à résoudre le théorème des valeurs intermédiaires pour les polynômes à coefficients dans $\bar{F}$. Soit P un polynôme de $\bar{F}[X]$ et a et b deux éléments de $\bar{F}$ tels que $a < b$. Montrons que si $P(a) \leq 0 \leq P(b)$, alors il existe $x \in \bar{F}$ tel que $P(x) = 0$.

5.1. De l'itération de la procédure de clôture

Si on se place dans la double extension $\bar{\bar{F}}$, on peut facilement trouver une racine $x \in \bar{\bar{F}}$ de $P \in \bar{F}[X]$ en appliquant la méthode de 4.3 en remplaçant F par $\bar{F}$.

Tout revient donc à prouver qu'il existe une fonction $\downarrow : \bar{\bar{F}} \to \bar{F}$, tel que

$$\forall x \in \bar{\bar{F}}, \quad \uparrow (\downarrow x) = x$$

Le nom Coq de cette fonction sera `from_alg`. L'existence d'une telle fonction permet de prouver que le processus de clôture que l'on a mis en œuvre termine bien en une seule étape.

Soit $x \in \bar{\bar{F}}$, construisons $\downarrow x$. En transformant x en algébrique de Cauchy $(\bar{x}, P)$, on obtient d'une part une suite de Cauchy $\bar{x}$ d'éléments de $\bar{F}$, et d'autre part le polynôme P à coefficients dans $\bar{F}[X]$.

Chacun des éléments x_n est à son tour une suite de Cauchy $(x_{n,k})_k$. On trouve alors une fonction $k : \mathbb{N} \to \mathbb{N}$ telle que la suite $\left(x_{n,k(n)}\right)_n$ soit de Cauchy, ce qui va permettre de définir $(\downarrow x)$.

5.2. Polynôme annulateur de $(\downarrow x)$

Il faut maintenant trouver un polynôme $R \in F[X]$ qui annule cette suite de Cauchy. Les coefficients p_i de P sont en nombresfini à valeurs dans l'extension de corps $\bar{F}$ de F, on peut donc appliquer le théorème de l'élément primitif pour trouver un élément $\alpha \in \bar{F}$, de polynôme minimal Q de degré $q+1$, tel que chacun des p_i est dans l'extension simple $F[\alpha]$. On peut donc re-factoriser P de la manière suivante :

$$P = \sum_{l=0}^{q} \alpha^l P_l$$

On considère le résultant

$$R(Y) = \mathrm{Res}_X \left(\sum_{l=0}^{q} X^l P_l(Y), Q(X) \right)$$

Il faut alors montrer les deux propriétés suivantes : R est non nul et il annule bien $(\downarrow x)$.

R est non nul. On suppose qu'il est nul et on commence par écrire l'équation de Bézout comme pour le résultant de la différence et de la division : il existe $U, V \in F[X]$ tels que U est non nul, $\deg_X(U) < \deg(Q)$ et

$$U(X,Y) \sum_{l=0}^{q} X^l P_l(Y) = V(X,Y)Q(X)$$

Alors en relevant dans $\bar{F}$ et évaluant la variable X en α on obtient :

$$U(\alpha, Y)P(Y) = 0$$

or $P \neq 0$ donc $U(\alpha, Y) = 0$. Puis en prenant le coefficient de tête $u(X)$ de $U(X,Y)$ en Y, on obtient que

$$u(\alpha) = 0 \quad \text{et} \quad u \in F[X] \quad \text{et} \quad u \neq 0 \quad \text{et} \quad \deg(u) < \deg(Q)$$

Ceci contredit le fait que Q est le polynôme minimal de α dans F.

R annule $(\downarrow x)$. On a :

$$R(x_{n,k(n)}) = U(\alpha_m, x_{n,k(n)}) \left(\sum_{l=0}^{q} \alpha_m^l P_l(x_{n,k(n)}) \right) + V(\alpha_m, x_{n,k(n)})Q(\alpha_m)$$

et on observe que le membre droit converge vers 0 quand m et n tendent vers l'infini.

La formalisation de cette dernière partie sur le théorème des valeurs intermédiaires reste inachevée pour le moment. Cependant la seule difficulté spécifique à cette section est l'utilisation du théorème de l'élément primitif, qui a déjà été démontré par Russell O'Connor dans le cadre de la bibliothèque SSReflect.

Conclusion

Ce travail permet d'instancier l'interface de corps réel clos déjà formalisée pour traiter leur théorie [CM]. En particulier les *algébriques réels* bénéficieraient immédiatement d'une procédure d'élimination des quantificateurs, qui rend décidable la théorie du premier ordre des corps réels clos. La formalisation décrite ici est issue de diverses sources classiques qui ont dû être adaptées, rendues constructives et simplifiées pour les besoins de la formalisation. La méthodologie appliquée ici pour construire les algébriques et rendre les preuves faisables et rapides sans avoir à développer trop de théories annexes est, à notre connaissance, originale. C'est aussi, à ce qu'on sache, la première formalisation certifiée des nombres algébriques dans un assistant de preuve.

Un élément intéressant de cette formalisation est que la rédaction des preuves de cet article est très proche des scripts Coq utilisés pour démontrer formellement les théorèmes. En particulier, l'assertion "soit i suffisamment grand" se traduit par une tactique `pose_big_enough i` en Coq, et il n'y a alors pas à se soucier de la valeur à donner à i.

La continuation naturelle de ce travail est de prolonger les *algébriques réels* en faisant l'extension par l'élément imaginaire i. D'après le théorème de d'Alembert-Gauss constructif généralisé au cas des corps

réels clos [CC], ce nouveau corps serait *algébriquement clos*, *partiellement ordonné* et constituerait alors le type des nombres *algébriques (complexes)*. Dans le cadre de la théorie de Galois, il serait également intéressant de formaliser la théorie des extensions algébriques sur les rationnels, que l'on pourrait alors étudier comme en mathématiques classiques : en se plaçant dans leur clôture algébrique.

Enfin, il serait intéressant de fournir une implémentation efficace des nombres algébriques, en s'appuyant par exemple sur les travaux de [Bos03]. La formalisation présentée dans cet article servirait d'implémentation de référence, et il n'y aurait pas besoin de refaire toutes les preuves pour la nouvelle implémentation. En revanche, il faudrait exhiber un opérateur de traduction des algébriques de référence en algébriques efficaces et montrer que cet opérateur est bien un morphisme de structures.

Remerciements

Je souhaite remercier Georges Gonthier pour les nombreuses idées à la base de ce développement. Je remercie également Russell O'Connor pour les discussions qui m'ont permis d'aller plus vite pour trouver les bonnes formulations et preuves de certains énoncés. Et enfin je remercie Assia Mahboubi pour ses nombreuses relectures et commentaires.

Références

[Bos03] Alin Bostan. *Algorithmique efficace pour des opérations de base en Calcul formel.* PhD thesis, École polytechnique, 2003.

[CC] Cyril Cohen and Thierry Coquand. A constructive version of Laplace's proof on the existence of complex roots. http://hal.inria.fr/inria-00592284/PDF/laplace.pdf.

[CM] Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry : from ordered fields to quantifier elimination. http://hal.inria.fr/inria-00593738/PDF/main.pdf.

[Coh10] Cyril Cohen. Types quotients en coq. In Hermann, editor, *Actes des 21ème journées francophones des langages applicatifs (JFLA 2010)*, Vieux-Port La Ciotat, France, January 2010. INRIA.

[GGMR09] François Garillot, Georges Gonthier, Assia Mahboubi, and Laurence Rideau. Packaging mathematical structures. In Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel, editors, *TPHOLs*, volume 5674 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2009.

[GN02] Herman Geuvers and Milad Niqui. Constructive reals in coq : Axioms and categoricity. In *Selected papers from the International Workshop on Types for Proofs and Programs*, TYPES '00, pages 79–95, London, UK, 2002. Springer-Verlag.

[Gon11] Georges Gonthier. Point-free, set-free concrete linear algebra. In *Interactive Theorem Proving, ITP 2011 Proceedings*, Lecture Notes in Computer Sciences. Springer, 2011. to appear.

[Hil93] David Hilbert. Über die transzendenz der zahlen e und π, 1893.

[KS11] Robbert Krebbers and Bas Spitters. Computer certified efficient exact reals in coq. In *Conference on Intelligent Computer Mathematics, CICM 2011 Proceedings*, Lecture Notes in Artifical Intelligence. Springer, 2011. to appear.

[Lan02] S. Lang. *Algebra.* Graduate texts in mathematics. Springer, 2002.

[MRR88] R. Mines, F. Richman, and W. Ruitenburg. *A course in constructive algebra.* Universitext (1979). Springer-Verlag, 1988.

[Pro] The Mathematical Components Project. SSReflect extension and libraries. http://www.msr-inria.inria.fr/Projects/math-components/index_html.