Définir le fini : deux formalisations d'espaces de dimension finie

Florian Faissole

Définir le fini : deux formalisations d'espaces de dimension finie

Florian Faissole[1]

Inria, Université Paris-Saclay, F-91120 Palaiseau
LRI, CNRS & Université Paris-Sud, F-91405 Orsay
florian.faissole@inria.fr

Résumé

Les espaces de dimension finie permettent de décrire mathématiquement certaines méthodes numériques comme la méthode des éléments finis. Leur formalisation est nécessaire pour certifier que ces méthodes sont correctes et plus précisément qu'elles sont convergentes. Dans cet article, nous présentons deux méthodes pour formaliser les espaces de dimension finie en Coq, dans un cadre de topologie générale. Les deux approches utilisent des mécanismes différents et ne présentent pas les mêmes avantages et inconvénients. La première repose sur l'extension, à l'aide de structures canoniques, de la hiérarchie algébrique de la bibliothèque Coquelicot. Elle permet aisément de montrer que les espaces $\mathbb{R}^n$ sont de dimension finie et plus généralement que le produit cartésien d'espaces de dimension finie est de dimension finie. La seconde repose sur l'utilisation de sous-espaces en tant que prédicats sur l'espace total. Elle permet d'extraire des propriétés topologiques sur des sous-espaces de dimension finie d'un espace de dimension infinie, comme la fermeture des sous-espaces de dimension finie des espaces de Hilbert. Nous proposons par ailleurs une étude comparative de ces deux approches.

1 Introduction

Il y a un intérêt grandissant pour la formalisation de résultats d'analyse, qui servent de fondements à des applications critiques comme la résolution d'équations différentielles en médecine ou en aéronautique. Il y a plusieurs exemples de formalisations d'espaces de dimension finie dans des assistants de preuves comme HOL-Light [8], Isabelle/HOL [5] et Coq [3, 7] : dans la bibliothèque Mathematical Component, les espaces de dimension finie sont notamment utilisés dans la preuve du théorème de Feit-Thompson, un résultat important en théorie des groupes [7]. Les travaux de Harrison [8] et de Brunel [3] portent plus particulièrement sur les espaces euclidiens, $i.e.$ les espaces de Hilbert de dimension finie. Dans ces développements, les espaces de dimension finie sont des citoyens de première classe et nous ne pouvons que considérer des sous-espaces de dimension finie de ces espaces de dimension finie, dont ils héritent des propriétés topologiques. Nous pouvons néanmoins citer les travaux de Mahmoud, Aravantinos et Tahar [11] en Isabelle/HOL, qui définissent les espaces vectoriels de dimensions finie et infinie au même niveau, mais n'en extraient pas de propriétés topologiques.

Nous proposons deux formalisations d'espaces de dimension finie dans l'assistant de preuves Coq. Ces deux formalisations n'ont pas vocation à se substituer l'une à l'autre, mais sont complémentaires. En effet, alors que la première approche ($\mathcal{A}_1$) consiste à définir le type des espaces de dimension finie, la seconde ($\mathcal{A}_2$) permet de considérer les sous-espaces de dimension finie d'un module quelconque de dimension potentiellement infinie. Ainsi est-il possible de définir un module de dimension finie via l'approche $\mathcal{A}_1$ puis d'y considérer un sous-espace de dimension finie plus petite via l'approche $\mathcal{A}_2$. Conceptuellement, on pourrait imaginer ne pas faire de distinguo et construire ces deux espaces au même niveau, puis montrer que l'un est sous-espace de l'autre. Néanmoins, contrairement à d'autres systèmes comme PVS, il n'y a pas de mécanisme de sous-typage dans Coq. Définir une sous-structure est d'ailleurs connu pour être un problème difficile [9, 1].

Ce travail est basé sur la bibliothèque Coquelicot, une extension conservative de la bibliothèque réelle standard de Coq [2]. Cette bibliothèque permet de raisonner sur des structures algébriques très générales. Elle comporte en effet des structures à lois internes (`AbelianGroup`, `Ring`) ou à opérations externes (`ModuleSpace`) ainsi que des structures munies de propriétés topologiques (`UniformSpace`, `CompleteSpace`) ou des espaces munis d'une norme (`NormedModule`, `CompleteNormedModule`). Ces ensembles généraux sont construits grâce au mécanisme de structures canoniques [10] qui permet d'inférer et de hiérarchiser les structures algébriques, et de caractériser des espaces comme $\mathbb{R}$ en tant qu'instances de ces structures.

Dans Coquelicot, la topologie est définie via la notion de filtres (ensembles de voisinages enrichis de certaines propriétés). Ils permettent notamment de représenter des voisinages, comme ceux de la Figure 1.

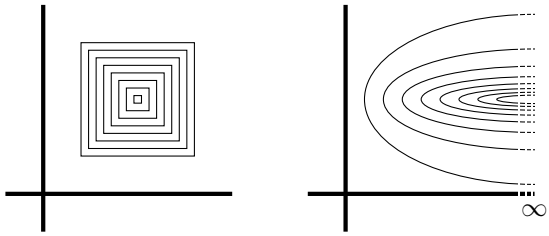

FIGURE 1 – Exemples de filtres, autour d'un point fini (gauche), à l'infini (droite).

Les filtres sont utilisés pour définir l'ensemble des notions topologiques, comme la fermeture, la complétude ou les notions de convergence. Un filtre propre (`ProperFilter`) est un filtre ne contenant pas d'ensembles vides. Un filtre de Cauchy (`cauchy`) est un filtre contenant des boules de rayon arbitrairement petit (généralisation des suites de Cauchy). Un espace complet `T` est muni d'une fonction limite `lim : ((T -> Prop) -> Prop) -> T` prenant un filtre en entrée et retournant un élément de `T` défini comme la limite de ce filtre. Elle vérifie la propriété de complétude (convergence de tout filtre propre de Cauchy) :

```
forall F, ProperFilter F -> cauchy F ->
          forall eps : posreal, F (ball (lim F) eps)
```

D'autres notions topologiques propres à nos preuves sont définies dans la Section 3, comme la notion de fermeture et celle de filtre implicite sur un sous-ensemble.

2 Structures canoniques et espaces de dimension finie

Il est possible, en utilisant les structures canoniques, d'étendre la hiérarchie algébrique de Coquelicot. Par exemple, Boldo, Clément, Faissole, Martin et Mayero étendent la hiérarchie algébrique de Coquelicot aux espaces préhilbertiens et hilbertiens [1]. À notre tour, nous proposons de l'enrichir de la structure de $\mathbb{R}$-module de dimension finie :

```
Record mixin_of (E : ModuleSpace R_Ring) := Mixin {
          dim : nat ;
          B : nat -> E ;
          B0 : B 0 = zero ;
          col : forall u : E, exists L : nat -> R,
                    u = sum_n (fun n => scal (L n) (B n)) dim }.
```

Un $\mathbb{R}$-module de dimension finie est muni d'un entier `dim` est d'une "famille génératrice" `B : nat -> E`. Par ailleurs, `B(0)` est défini comme le vecteur nul afin de caractériser l'espace de dimension 0. Enfin, la dernière propriété `col` assure que tout vecteur du module de dimension finie est combinaison linéaire des `dim` premiers vecteurs de `B`. Ce choix induit deux astuces facilitant les preuves. Premièrement, la suite `B` peut être définie arbitrairement au-delà du rang `dim`. Par ailleurs, `dim` est une surestimation de la dimension du module de dimension finie. En effet, nous nous autorisons à avoir `B(i) = 0` pour $0 \leq$ `i` $\leq$ `dim`. Par exemple, nous définissons la suite $B^{\mathbb{R}}$ telle que $B_0^{\mathbb{R}} = 0$ et $\forall n \in \mathbb{N}^*, B_n^{\mathbb{R}} = 1$. Nous montrons facilement que $\mathbb{R}$ est un module de dimension finie (de dimension 1 et de famille génératrice $B^{\mathbb{R}}$).

Afin d'éprouver notre choix de formalisation, nous définissons le produit cartésien de modules de dimension finie. Nous considérons E_1 et E_2 des $\mathbb{R}$-modules de dimensions finies respectives dim_1 et dim_2 et de familles génératrices respectives B^{E_1} et B^{E_2}. Nous définissons une famille génératrice produit cartésien $B^{E_1 \times E_2}$ de la façon suivante :

$$\begin{cases} B_0^{E_1 \times E_2} = (0,0) \\ \forall n \in \mathbb{N}^*, n \leq dim_1 \Rightarrow B_n^{E_1 \times E_2} = \left(B_n^{E_1}, 0\right) \\ \forall n \in \mathbb{N}^*, dim_1 < n \leq dim_1 + dim_2 \Rightarrow B_n^{E_1 \times E_2} = \left(0, B_{n-dim_1}^{E_2}\right) \\ \forall n \in \mathbb{N}^*, n > dim_1 + dim_2 \Rightarrow B_n^{E_1 \times E_2} = (0,0) \end{cases}$$

Nous prouvons ensuite que le produit cartésien de modules de dimension finie est un module de dimension finie :

Lemme 1. *Soit E_1 et E_2 des $\mathbb{R}$-modules de dimensions finies respectives dim_1 et dim_2 et de familles génératrices respectives B^{E_1} et B^{E_2}. Alors $E_1 \times E_2$ est un $\mathbb{R}$-module de dimension finie $dim_1 + dim_2$ et de famille génératrice $B^{E_1 \times E_2}$.*

Démonstration. Par définition d'un module de dimension finie :

$$\begin{gathered} \exists \lambda^{E_1} : nat \to \mathbb{R}, \forall u \in E_1, u = \textstyle\sum_{i=0}^{dim_1} \lambda_i^{E_1} B_i^{E_1} \\ \text{et} \\ \exists \lambda^{E_2} : nat \to \mathbb{R}, \forall u \in E_2, u = \textstyle\sum_{i=0}^{dim_2} \lambda_i^{E_2} B_i^{E_2} \end{gathered}$$

Nous définissons la suite $\lambda^{E_1 \times E_2}$ de la façon suivante :

$$\begin{cases} \forall n, n \leq dim_1 \Rightarrow \lambda_n^{E_1 \times E_2} = \lambda_n^{E_1} \\ \forall n, n > dim_1 \Rightarrow \lambda_n^{E_1 \times E_2} = \lambda_{n-dim_1}^{E_2} \end{cases}$$

Donc, pour tout $(u_1, u_2) \in E_1 \times E_2$:

$$\begin{aligned} (u_1, u_2) &= \left(\textstyle\sum_{i=0}^{dim_1} \lambda_i^{E_1} B_i^{E_1}, \sum_{i=0}^{dim_2} \lambda_i^{E_2} B_i^{E_2}\right) = \left(\sum_{i=1}^{dim_1} \lambda_i^{E_1} B_i^{E_1}, \sum_{i=1}^{dim_2} \lambda_i^{E_2} B_i^{E_2}\right) \\ &= \left(\textstyle\sum_{i=1}^{dim_1} \lambda_i^{E_1} B_i^{E_1}, \sum_{i=1}^{dim_1+dim_2} \lambda_{i-dim_1}^{E_2} B_{i-dim_1}^{E_2}\right) \\ &= \textstyle\sum_{i=1}^{dim_1} \lambda_i^{E_1 \times E_2} B_i^{E_1 \times E_2} + \sum_{i=dim_1+1}^{dim_1+dim_2} \lambda_i^{E_1 \times E_2} B_i^{E_1 \times E_2} \\ &= \textstyle\sum_{i=0}^{dim_1+dim_2} \lambda_i^{E_1 \times E_2} B_i^{E_1 \times E_2} \end{aligned}$$

Donc, comme de plus $B_0^{E_1 \times E_2} = (0,0)$, $E_1 \times E_2$ est un $\mathbb{R}$-module de dimension finie $dim_1 + dim_2$ et de famille génératrice $B^{E_1 \times E_2}$. □

Ainsi, nous pouvons en déduire que pour tout $n \in \mathbb{N}$, $\mathbb{R}^n$ est un $\mathbb{R}$-module de dimension finie. Sur papier, un résultat comme celui-ci peut paraître relativement simple, mais sa formalisation induit des écueils. D'une part, il est nécessaire d'inférer la bonne famille génératrice produit B, qui ne peut pas être caractérisée par une unique expression qui dépend du rang n, mais varie suivant que n soit ou non supérieur à la dimension de E_1. Par ailleurs, il faut trouver les coefficients λ_i de la combinaison linéaire de vecteurs de B, ce qui mène à des raisonnements calculatoires. Souvent ellipsés par les mathématiciens, ces raisonnements sont difficilement automatisables en Coq et doivent être minutieusement conduits par l'utilisateur.

3 Sous-espaces de dimension finie

En analyse fonctionnelle, certains résultats mathématiques comme le théorème de Lax–Milgram peuvent être appliqués à des sous-modules de dimension finie d'espaces de Hilbert (un espace de Hilbert est un module muni d'un produit scalaire et qui est complet). Le théorème de Lax–Milgram établit l'existence d'une unique solution de la formulation faible d'une équation aux dérivées partielles sur tout sous-module fermé d'un espace de Hilbert.

La formalisation utilisant les structures canoniques (voir Section 2) n'est pas commode pour définir un espace de dimension finie comme sous-espace d'un espace E de dimension potentiellement infinie. Dans cette section, nous définissons les sous-espaces de dimension finie comme prédicats de type $E \to Prop$.

3.1 Définitions

On suppose que $E : Hilbert$. On définit les sous-espaces de dimension finie comme prédicats munis d'une propriété proche de celle définie pour les espaces dans la Section 2 ((`sum_n f n`) est la somme des $f(i)$ pour $0 \leq i \leq n$ et `scal` est la multiplication par un scalaire).

```
Variables (E:Hilbert)(n:nat)(B:nat→E).
Definition FDIM (phi:E → Prop) :=
    match (eq_nat_dec n 0) with
     |left _ ⇒ ∀ u, phi u ↔ u=zero (* n=0 *)
     |right _ ⇒ ∀ u, phi u ↔ (* n>0 *)
       ∃ L:nat → R, u = sum_n (fun i ⇒ scal (L i) (B i)) (n-1) end.
```

3.2 Fermeture des sous-espaces de dimension finie des espaces de Hilbert

Le théorème de Lax–Milgram a été prouvé formellement dans l'assistant de preuves Coq [1]. Ce théorème s'applique aux sous-modules fermés des espaces de Hilbert. Afin de vérifier la convergence de la méthode des éléments finis, nous souhaitons appliquer le théorème sur un espace de Hilbert entier (volume irrégulier) et sur un de ses sous-espaces de dimension finie (maillage). L'espace de Hilbert entier est trivialement un sous-module fermé de lui-même et le théorème peut s'y appliquer. Il reste à prouver que tout sous-espace de dimension finie d'un espace de Hilbert est fermé. La preuve formelle de ce résultat est disponible en ligne [1] et est décrite de façon détaillée par Faissole [6] (nous ne donnons ici qu'une intuition des preuves). Sans types dépendants, il n'est pas possible de dire qu'un filtre est un filtre sur un sous-espace φ de E, car il est de type $(E \to Prop) \to Prop$ (donc c'est un filtre sur E). Néanmoins, on peut donner une relation entre un filtre de E et le sous-espace φ :

1. https://github.com/FFaissole/FDIM_Topology

Définition 1. *Soit $E : Type$. Soit $\mathcal{F} : (E \to Prop) \to Prop$ un filtre sur E. Soit $\varphi : E \to Prop$ un sous-espace de E. $\mathcal{F}$ est un filtre implicite sur φ si :*

$$\forall \psi : E \to Prop, \mathcal{F}(\psi) \Rightarrow \exists x \in E, \psi(x) \wedge \varphi(x).$$

Il s'agit d'un filtre dont tous les éléments ont une intersection non vide avec φ. On dit que φ est fermé si tout filtre propre de Cauchy implicite sur φ a sa limite dans φ :

Définition 2. *Soit $E : CompleteSpace$, $\varphi : E \to Prop$. Le sous-espace φ est fermé dans E ssi pour tout filtre $\mathcal{F} : (E \to Prop) \to Prop$, si $\mathcal{F}$ est propre, de Cauchy et implicite sur φ alors $lim(\mathcal{F}) \in \varphi$.*

Le sous-module engendré par $u \in E$ (noté `span u`) est le sous-ensemble des vecteurs de E colinéaires à u. Tout vecteur d'un sous-espace de dimension finie est en fait somme de vecteurs des sous-modules engendrés par les vecteurs de la famille génératrice B.

```
Definition span (u : E) := fun x:E ⇒ (∃ (l : R), x = scal l u).
```

On prouve que le sous-module engendré par un élément d'un espace de Hilbert est fermé :

Lemme 2. *On suppose que $E : Hilbert$, $u \in E$. Alors $span(u)$ est fermé dans E.*

Démonstration. Dans la preuve papier standard, il s'agirait de considérer une suite de Cauchy de la forme $(\lambda_n u)_{n\in\mathbb{N}}$ (dans $span(u)$) et de prouver qu'elle converge. On extrairait la suite $(\lambda_n)_{n\in\mathbb{N}}$ (également de Cauchy) et on prouverait qu'elle converge vers une limite ℓ car $\mathbb{R}$ est complet. On en déduirait que $(\lambda_n u)_{n\in\mathbb{N}}$ converge vers ℓu. Comme nous travaillons avec des filtres, on considère $\mathcal{F}$ un filtre propre, de Cauchy et implicite sur $span(u)$. On doit construire un transformeur de filtre pour obtenir le filtre sur $\mathbb{R}$ équivalent à la suite $(\lambda_n)_{n\in\mathbb{N}}$, prouver qu'il est de Cauchy, puis qu'il converge, et enfin en déduire que $\mathcal{F}$ converge. □

Cette preuve est difficile car elle nécessite la traduction de la preuve papier dans le cadre des filtres. Les transformeurs de filtres peuvent notamment être difficiles à définir. Afin de faciliter les preuves, nous considérons ces transformeurs comme des fonctions totales mais les utilisons toujours sur les filtres *implicites* sur l'ensemble adéquat.

Théorème 1. *Soit $E : Hilbert$ et $\varphi : E \to Prop$. On suppose que φ est de dimension finie n et de famille génératrice orthonormée B. Alors φ est fermé.*

Démonstration. Si $u \in E : Hilbert$, $span(u)$ est un sous-espace fermé de E. On peut en déduire que la somme directe d'un sous-module fermé de E et de $span(u)$ est également fermé (1). Or, on montre qu'un sous-module de dimension finie n est somme directe d'un autre sous-module de dimension finie $n-1$ et de $span(B_n)$ (2). On raisonne par induction en supposant que tout sous-module de dimension $n-1$ est fermé. Par (1) et (2), tout sous-module de dimension n est fermé. □

4 Conclusion et perspectives

Nous proposons deux niveaux de formalisation d'espaces de dimension finie en Coq, tous deux fondés sur la bibliothèque Coquelicot. Le premier d'entre eux place ces espaces au même plan que les autres structures algébriques de Coquelicot. Son avantage est la possibilité d'instancier des espaces usuels comme $\mathbb{R}$ ou $\mathbb{R}^n$ comme cas particuliers de modules de dimension finie. La deuxième approche considère tout espace de dimension finie comme sous-espace d'un espace plus grand, de dimension potentiellement infinie. Nous proposons une preuve formelle de la fermeture des sous-espaces de dimension finie des espaces de Hilbert (utilisant des filtres pour la topologie). Notre développement comporte

environ 2500 lignes de Coq, dont 1500 pour la preuve de fermeture. Les preuves papier de ce résultat [4] excèdent rarement 3 pages. La longueur de notre preuve est due à la construction de transformeurs de filtres (les preuves papier utilisent des transformeurs de suites). La deuxième "recette" de formalisation est retenue pour servir à l'application des théorèmes de Lax–Milgram et Céa sur les sous-espaces de dimension finie d'espaces de Hilbert. Ces résultats doivent servir à la vérification de la méthode des éléments finis (convergence notamment), mais nous devons formaliser des espaces particuliers comme $L^2(\Omega)$ et $H^1(\Omega)$, dont il faut prouver le caractère hilbertien et extraire un maillage de dimension finie. La vérification de la méthode pourra servir de base à la preuve de programmes l'implémentant, comme la bibliothèque C++ FELiScE [2].

Remerciements

Nous remercions Sylvie Boldo, François Clément, Vincent Martin et Micaela Mayero pour leur aide dans la formalisation des résultats.

Références

[1] S. Boldo, F. Clément, F. Faissole, V. Martin, and M. Mayero. A Coq Formal Proof of the Lax–Milgram theorem. In *6th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 79–89, Paris, France, January 2017.

[2] S. Boldo, C. Lelay, and G. Melquiond. Coquelicot : A user-friendly library of real analysis for Coq. *Mathematics in Computer Science*, 9(1) :41–62, 2015.

[3] A. Brunel. Non-constructive complex analysis in Coq. In *18th International Workshop on Types for Proofs and Programs, TYPES 2011, September 8-11, 2011, Bergen, Norway*, pages 1–15, 2011.

[4] F. Clément and V. Martin. The Lax-Milgram Theorem. A detailed proof to be formalized in Coq. Research Report RR-8934, Inria Paris, July 2016.

[5] J. Divasón Mallagaray. *Formalisation and execution of Linear Algebra : theorems and algorithms*. PhD thesis, Universidad de La Rioja, 2016.

[6] F. Faissole. Formalization and closedness of finite dimensional subspaces. In *19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, SYNASC 2017, September 2017.

[7] G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. Ould Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi, and L. Théry. A machine-checked proof of the odd order theorem. In *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, pages 163–179, 2013.

[8] J. Harrison. A HOL theory of Euclidean space. In Joe Hurd and Tom Melham, editors, *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005*, volume 3603 of *Lecture Notes in Computer Science*, Oxford, UK, 2005. Springer-Verlag.

[9] A. Mahboubi. The Rooster and the Butterflies. In Jacques Carette, David Aspinal, Christopher Lange, Petr Sojka, and Wolfgang Windsteiger, editors, *CICM 2013 - Conference on Intelligent Computer Mathematics - 2013*, volume 7961 of *Lecture Notes in Artificial Intelligence*, pages 1–18, Bath, United Kingdom, July 2013. Springer.

[10] A. Mahboubi and E. Tassi. Canonical structures for the working Coq user. In *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, pages 19–34, 2013.

[11] M. Y. Mahmoud, V. Aravantinos, and S. Tahar. Formalization of infinite dimension linear spaces with application to quantum theory. In *NASA Formal Methods, 5th International Symposium, NFM 2013, Moffett Field, CA, USA, May 14-16, 2013. Proceedings*, pages 413–427, 2013.

2. Finite Elements for Life Sciences and Engineering : https://gforge.inria.fr/projects/felisce/