IRL
-
Formalisation du théorème de décomposition de Hahn avec le démonstrateur interactif Isabelle

LIG - Equipe CAPP

Marie Cousin

ISI

Encadrants

Mnacho Echenim et Hervé Guiol

Table des matières

1 Introduction

Je vais ici m'atteler à présenter la formalisation réalisée du théorème de décomposition de Hahn à l'aide de l'assistant de preuve Isabelle dans le cadre de l'IRL, en présentant dans un premier temps ce qu'est un assistant de preuve, puis en explicitant le théorème de décomposition de Hahn et les étapes de la formalisation. Pour finir, j'expliciterai le théorème de décomposition de Jordan, qui découle de celui de Hahn. La formalisation en Isabelle est disponible sur git.

De nombreux résultats mathématiques ont, de nos jours, été trouvés et prouvés, et de nouveaux sont en train de l'être. Aussi, les preuves de ces résultats peuvent parfois être très longues et complexes. Un assistant de preuve interactif prend alors tout son intérêt, car il permet de valider une preuve de manière sûre, sans erreur humaine possible.

1.1 Description du sujet

J'ai travaillé dans le cadre du projet d'IRL (Introduction à la Recherche en Laboratoire) sur la formalisation du théorème de décomposition de Hahn, qui intervient dans le domaine de la théorie de la mesure en mathématiques. Il utilise une mesure signée sur un espace mesurable, et permet alors de séparer l'univers de cet espace mesurable en deux sous-espaces disjoints, ayant chacun des propriétés intéressantes.

Il existe de nos jours des outils permettant de vérifier des raisonnements et résultats mathématiques. En effet, les assistants de preuve sont des logiciels à l'aide desquels on peut formaliser une preuve ou un raisonnement mathématique. Lors de la formalisation dans un assistant de preuve, chaque étape de la preuve est vérifiée. Ils permettent donc d'assurer qu'une preuve est correcte. De plus en plus de résultats mathématiques sont formalisées, et cette formalisation est un domaine de recherche qui occupe et intéresse de plus en plus de mathématiciens et informaticiens.

Dans ce projet d'IRL [Ech20], je vais formaliser dans le démonstarteur interactif le théorème de décomposition de Hahn et celui de Jordan qui en est une conséquence, et donc prendre part à cette formalisation des résultats mathématiques.

1.2 Résultats attendus

L'objectif de ce projet d'IRL est de me faire manipuler des notions de la théorie de la mesure (et en particulier la notion de mesure signée), ainsi que l'assistant de preuve Isabelle, afin d'ajouter aux résultats déjà formalisés le théorème de décomposition de Hahn et ses conséquences. Si possible, à la fin de ce projet, nous pourrons publier cette formalisation dans l'archive des preuves formelles d'Isabelle.

1.3 Histoire et principe de la formalisation de preuves

Le souci de pouvoir valider ou réfuter une preuve ou un raisonnement existe depuis longtemps. En effet, en 1910 était publié *Principia Mathematica* d'Alfred Whitehead et Bertrand Russell. Ils sont les premiers à avoir détaillé une méthode afin d'être capable de prouver (ou réfuter) un raisonnement mathématique. Cependant, leur méthodologie, si elle convenait parfaitement à des raisonnement simples, donnait des formules beaucoup trop compliquées dès lors qu'on l'appliquait à des raisonnements plus longs et complexes [Del12]. Néanmoins, c'est la première fois qu'il était montré qu'il était possible d'assurer (ou non) qu'un raisonnement mathématique était correct. C'est un véritable tournant dans l'histoire des mathématiques, car avant cela, il fallait se convaincre de certaines preuves, qui ressemblaient à des exercices littéraires aussi bien qu'à des preuves mathématiques. A partir de ce moment, de plus en plus de scientifiques ont essayé de trouver des méthodes plus simples de formalisation.

Un demi-siècle plus tard, avec l'arrivée de l'informatique et de la puissance de calcul qu'elle propose, les scientifiques ont continué de chercher comment formaliser des raisonnements, mais à l'aide des machines cette fois, et avec succès ! Aussi, Nicolas de Bruijn a développé le logiciel Automath en 1966 aux Pays-Bas, suivi par les logiciels Mizar en Pologne, Isabelle au Royaume-Uni (Cambridge) et en Allemagne (Munich), et Coq en France [Del12]. Ces logiciels sont des assistants de preuve interactifs, c'est à dire qu'ils permettent aux mathématiciens d'utiliser un système informatique interactif et un formalisme de démonstration, afin de formaliser et prouver leurs résultats au sein de ce même logiciel. Aussi, la vérification formelle des preuves (d'autant plus fastidieuse que la preuve est longue) n'est plus réalisée par l'homme (le mathématicien), mais par le logiciel. De plus, les résultats prouvés antérieurement par d'autres mathématiciens sont disponibles au sein de ces logiciels, et sont réutilisables par tout utilisateur, afin de poursuivre ce grand travail de formalisation des preuves existantes.

De tels logiciels comportent bien sûr un risque d'erreur, mais très faible devant le risque de l'erreur humaine. En effet, Isabelle découpe chaque étape de raisonnement en déductions élémentaires (étapes auxquelles on peut accéder pour les vérifier), et les formalisations entières sont vérifiées par des *proof checkers*, indépendamment d'Isabelle. Ces *proof checkers* justifient et assurent la sûreté de la correction des formalisations en Isabelle. Les assistants de preuve sont donc des outils très intéressants de nos jours, afin de vérifier les preuves des résultats mathématiques qui existent. Ils utilisent par ailleurs des langages hybrides, proches des langages de programmation et du langage naturel mathématique, afin d'être compris des mathématiciens et des machines, même si une preuve formalisée est parfois très peu intuitive car trop détaillée pour un humain (mais nous verrons cela plus précisément dans la partie 3).

1.4 Motivation

Le théorème de décomposition de Hahn est un théorème qui manipule de nombreuses notions mathématiques, comme l'est également le théorème de décomposition de Jordan, conséquence de celui de Hahn. Le but de formaliser ces théorèmes est de me permettre de découvrir la notion de mesure signée, manipuler ces mesures et des ensembles, pour finalement aboutir à la preuve de théorèmes importants de la théorie de la mesure. De plus, cela me permet de manipuler Isabelle, et découvrir le domaine des assistants de preuves, domaine que je trouve intéressant, et vers lequel je voudrai poursuivre mes études.

Le théorème de Hahn demande de généraliser la notion de mesure standard pour aboutir à la notion de mesure signée, et celui de Jordan permet de faire le lien entre ces deux notions de mesure. Il y a donc un lien très fort entre ces théorèmes et la théorie de la mesure.

Ces résultats, une fois formalisé en Isabelle, pourront être utilisé par d'autres mathématiciens, pour prouver d'autres résultats de la théorie de la mesure, tels qu'une extension du théorème de Radon-Nikodým aux mesures signées.

2 Éléments principaux

2.1 Isabelle HOL : un assistant de preuve interactif

FIGURE 1 – Logo d'Isabelle

2.1.1 Présentation générale

Isabelle HOL est un démonstrateur interactif basé sur la logique d'ordre supérieur (HOL pour Higher Order Logic), développé en partenariat par les universités de Cambridge et Munich. C'est un logiciel libre publié sous licence BSD. La première version date de 1986, et de nouvelles versions sont régulièrement publiées.

L'assistant de preuve Isabelle permet en effet d'exprimer des formules mathématiques, et par extension des raisonnements mathématiques complets, dans le langage formel *Isar*, intuitif à lire pour un humain et compris en même temps par les machines [Uni21]. Cette formalisation permet entre autre la vérification formelle des preuves, et c'est ce à quoi nous nous intéresserons.

2.1.2 Environnement

Il y a dans Isabelle beaucoup d'automatisation, et des outils de raisonnement qui permettent de construire automatiquement certaines preuves sans avoir besoin de tout développer. De plus, on peut aussi invoquer des démonstrateurs automatiques externes à Isabelle, via l'outil *sledgehammer* [Uni21].

L'interface graphique d'Isabelle utilise JEdit, qui donne un retour en temps réel de l'avancée de la preuve en cours, permettant de savoir ligne par ligne si ce qu'on a écrit est valide ou non [Uni21]. Cet IDE a aussi le bon goût d'avoir une coloration syntaxique et la complétion automatique. Voici un aperçu de l'interface graphique d'Isabelle :

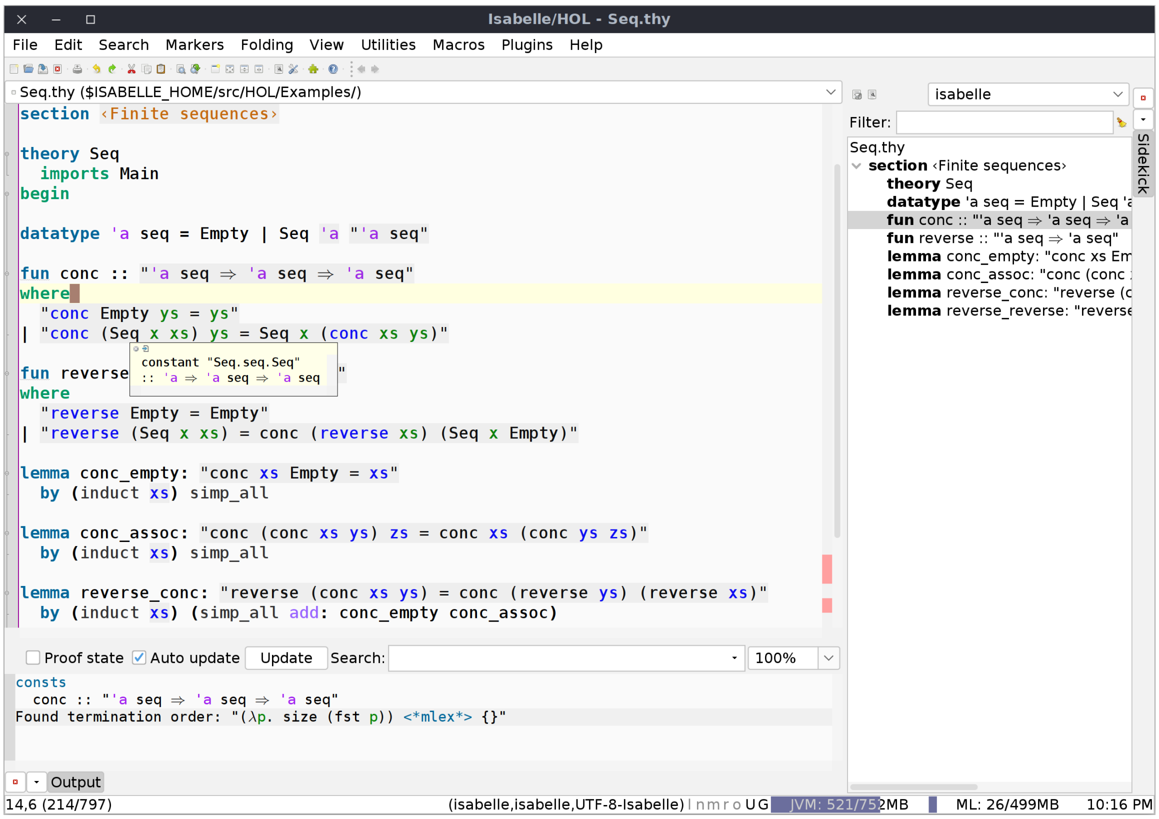

Figure 2 – Aperçu de l'interface utilisateur JEdit d'Isabelle

Aussi, l'interaction avec Isabelle est grandement facilitée grâce à cette interface graphique.

2.1.3 Archive des preuves formelles

Par ailleurs, tous les résultats prouvés jusqu'à présent en Isabelle sont disponibles sur la page internet archive of formal proofs. Ces résultats peuvent également être disponibles au sein du logiciel, il suffit de les importer au début de la formalisation. En effet, chaque fichier Isabelle est une théorie, et l'extension d'un tel fichier est *.thy*. Pour importer une autre théorie, il suffit de rentrer la commande "**import** `maTheorie.thy`". L'environnement mathématique d'Isabelle est donc particulièrement adapté à la formalisation de preuves.

Ainsi, énormément de résultats de la théorie de la mesure ont déjà été formalisé en Isabelle et sont donc réutilisables, comme la théorie `HOL-Probability.Probability` [HH11], qui possède entre autres les formalisations des résultats sur les espaces probabilisés et les mesures non signées.

2.2 Principe de la formalisation

2.2.1 But de la formalisation

De manière générale, il est important de bien raisonner, j'entends par là avoir un raisonnement clair et compréhensible, afin que les autres puissent suivre ce raisonnement d'une part, et afin d'éviter de se tromper et de tout mélanger d'autre part. Formaliser une preuve est une solution pour structurer un raisonnement, qui, si elle est longue et fastidieuse, est très pratique, universelle, peut être vérifiée indépendamment par des *proof checkers*.

2.2.2 Méthodologie

Le principe de la formalisation d'un raisonnement est de décortiquer ce même raisonnement en petites étapes simples, et de structurer ses étapes entre elles.

Par exemple, considérons le raisonnement suivant : *J'ai* 50 *euros, je suis allée m'acheter une robe en soldes à* 30%*, qui coûtait initialement* 40 *euros, il me reste* 22 *euros.* Si on le formalise, il devient :

> ***Au départ*** *j'ai* 50 *euros.*
> ***Ensuite****, je suis allée acheter une robe en soldes à* 30%*, qui coûtait initialement* 40 *euros.*
> ***Donc*** *le prix de la robe soldée est de* $40 - \frac{30}{100} * 40$ *euros.*
> ***Or****,* $40 - \frac{30}{100} * 40 = 40 - 12$.
> ***Et*** $40 - 12 = 28$.
> ***Ainsi****, je devrai payer* 28 *euros, sachant que la robe coûte* $40 - \frac{30}{100} * 40$ *euros, que* $40 - \frac{30}{100} * 40 = 40 - 12$ *et que* $40 - 12 = 28$.
> ***Par conséquent****, il me restera* $50 - 28$ *euros.*
> ***Or****,* $50 - 28 = 22$.
> ***Donc****, il me restera finalement* 22 *euros, sachant qu'il me restera* $50 - 28$ *euros et que* $50 - 28 = 22$.

On peut d'emblée remarquer que le raisonnement de 2 lignes initialement se fait en 9 étapes (donc au moins 9 lignes). De plus, il est tout à fait possible qu'un assistant de preuve, donc une machine, ait besoin de plus de détail que cela.

Cependant, si formaliser des raisonnements simples est facile, lorsqu'il s'agit de raisonnements plus complexes, les preuves formalisées deviennent rapidement non intuitives et compliquées à lire. En effet, il s'agit d'expliciter chaque étape, aussi petite soit elle, afin de s'assurer qu'il n'y a aucune erreur, et régulièrement, un résultat caractérisé de "trivial" prend en réalité plusieurs lignes (parfois beaucoup de lignes) à être démontré ; le résultat n'était donc pas si trivial. C'est pour cela que les preuves que l'on rencontre (dans les livres, articles, etc.) sont rarement formalisées. Il est donc d'autant plus important de les formaliser, afin de pouvoir valider la preuve de ces résultats. Le théorème de Hahn ne déroge pas à cela, c'est à partir d'une preuve plutôt intuitive et non formalisée que j'ai travaillé, afin de la formaliser pour prouver la preuve du théorème de décomposition de Hahn, et les notions, propositions et lemmes qu'il utilise.

2.3 Cadre du théorème de décomposition de Hahn

Le théorème de décomposition de Hahn [DiB16] est le suivant :

Théorème 1 *soit* $\{X, \mathcal{A}\}$ *un espace mesurable et* μ *une mesure signée sur* $\{X, \mathcal{A}\}$*. Alors il existe une partition de* X *en* X^+ *un ensemble positif et* X^- *un ensemble négatif. Cette partition est unique à tout ensemble de mesure* μ *nulle près.*

Pour comprendre ce théorème (puis sa preuve) il faut introduire quelques notions.

2.3.1 Mesure signée

Nous allons maintenant présenter la notion de mesure signée. C'est une notion proche de la notion standard de mesure, sauf que dans le cas d'une mesure signée, l'image des ensembles mesurables peut être positive ou négative.

Définition 1 *Une **mesure signée** μ associée à un espace mesurable $\{X, \mathcal{A}\}$ est une application de $\mathcal{A}$ dans $\overline{\mathbb{R}}$ telle que :*
- $\mu(\emptyset) = 0$
- *elle ne peut contenir à la fois $+\infty$ et $-\infty$ dans son ensemble image*
- *μ est σ-additive.*

2.3.2 Théorie HahnDecomp

Dans la théorie Isabelle que j'ai écrite avec l'aide de Mnacho Echenim et Hervé Guiol, j'ai eu besoin de pouvoir manipuler des mesure signées, des ensembles particuliers (les ensembles positifs et négatifs, qui sont explicités dans la section suivante) très rapidement. Étant donné que je débutais en Isabelle, et que la définition d'une mesure signée et de l'environnement qui va avec était compliquée, c'est Mnacho Echenim qui a défini cela proprement, en introduisant finalement la *locale* suivante au début de la théorie, pendant que je comprenais et formalisais sur papier le théorème de décomposition et la proposition qu'il utilise.

Une *locale* est basée sur un (ou plusieurs) contextes (un contexte est un schéma de formule, contenant des paramètres, des prémisses et des conclusions : $\forall x_1, x_2, ..., x_n,\ [A_1, A_2, ..., A_n] \Rightarrow C$. Si la formule C est une conclusion de ce schéma, alors elle est un théorème dans la locale.) [Bal10]. On peut définir dans une théorie une locale, puis déclarer des définitions et des résultats au sein de la locale. C'est particulièrement adapté aux théories nécessitant des paramètres, comme ici où nous avons besoin d'un espace mesurable et d'une mesure signée sur cet ensemble.

locale SIGNED_MEASURE_SPACE =
  fixes M **and** μ
  assumes `sgn_meas` : `signed_measure` M μ

2.3.3 Ensembles positifs et négatifs

Nous allons commencer par définir (au sein de la *locale* précédente) ce qu'est un ensemble positif et un ensemble négatif [DiB16] :

Définition 2 *Soit $\{X, \mathcal{A}\}$ un espace mesurable et μ une mesure signée sur $\{X, \mathcal{A}\}$. E est un **ensemble positif** si :*
- *E est mesurable (i.e. $E \in \mathcal{A}$)*
- *pour tout sous ensemble A mesurable de E, on a : $\mu(A) \geq 0$*

Définition 3 *Soit $\{X, \mathcal{A}\}$ un espace mesurable et μ une mesure signée sur $\{X, \mathcal{A}\}$. Un **ensemble négatif** E est tel que :*
- *E est mesurable (i.e. $E \in \mathcal{A}$)*
- *pour tout sous ensemble A mesurable de E, on a : $\mu(A) \leq 0$*

La formalisation en Isabelle [Her21] de ces définitions est la suivante :

definition (*in* `signed_measure_space`) POS_MEAS_SET
  where `pos_meas_set` $E \longleftrightarrow E \in \mathit{sets}\ M \wedge (\forall A \in$ `sets` $M.\ A \subseteq E \rightarrow 0 \leq \mu\ A)$

definition (*in* `signed_measure_space`) NEG_MEAS_SET
  where NEG_MEAS_SET $E \longleftrightarrow E \in \mathit{sets}\ M \wedge (\forall A \in$ `sets` $M.\ A \subseteq E \rightarrow 0 \geq \mu\ A)$

Par ailleurs, il existe quelques propriétés sur des opérations sur ces ensembles particuliers. Dans ce qui suit, on considère μ une mesure signée sur l'espace mesurable $\{X, \mathcal{A}\}$.

Lemme 1 *La différence de deux ensembles positis (resp. négatifs) est un ensemble positif (resp. negatif).*

Lemme 2 *L'union de deux ensembles positifs (resp. négatifs) est un ensemble positif (resp. négatif).*

Ces résultats sont formalisés en Isabelle [Her21], de même que leur preuve :

lemma (*in* `signed_measure_space`) POS_MEAS_SET_DIFF :
  assumes `pos_meas_set` E
  and `pos_meas_set` F
shows `pos_meas_set` $(E - F)$

lemma (*in* `signed_measure_space`) POS_MEAS_UNION :
  assumes `pos_meas_set` A
  and `pos_meas_set` B
shows `pos_meas_set` $(A \cup B)$

Il en découle alors le lemme suivant, lui aussi formalisé en Isabelle :

Lemme 3 *Soit $(A_i)_{i\in\mathbb{N}}$ une collection d'ensembles mesurables tous positifs, et tels que pour tout i, $|\mu(\cup A_i)| < \infty$. Alors $\cup A_i$ est un ensemble positif.*

lemma (*in* `signed_measure_space`) POS_MEAS_SET_UNION :
  assumes $\forall i \in \mathbb{N}.$ `pos_meas_set` $(A\ i)$
  and $\forall i \in \mathbb{N}.\ A\ i \in$ `sets` M
  and $|\mu\ (\cup\ i.\ A\ i)| < \infty$
shows `pos_meas_set` $(\cup\ i.\ A\ i)$

2.3.4 Lemme et proposition préliminaires

Pour pouvoir prouver le théorème de décomposition de Hahn, on aura besoin [DiB16] d'une proposition, s'appuyant elle-même sur un lemme. Si j'ai eu le temps de détailler mathématiquement la proposition, je n'ai pas pu le faire pour le lemme, et je n'ai formalisé aucun des deux dans Isabelle. Avoir détaillé mathématiquement la proposition m'a cependant permis de bien comprendre le théorème de décomposition de Hahn. Je mets les deux résultats ici, afin de mieux présenter la preuve du théorème de Hahn.

Lemme 4 *Soit $\{X, \mathcal{A}\}$ un espace mesurable et μ une mesure signée sur $\{X, \mathcal{A}\}$. Soit $A \subset X$ un ensemble mesurable tel que $|\mu(E)| < \infty$. Alors tout sous-ensemble mesurable $A \subseteq E$ satisfait $|\mu(A)| < \infty$.*

Proposition 1 *Soit $\{X, \mathcal{A}\}$ un espace mesurable et μ une mesure signée sur $\{X, \mathcal{A}\}$. Tout ensemble mesurable E de mesure positive et finie contient un sous-ensemble positif A de mesure strictement positive.*

Une fois tout cela fait, nous pouvons passer à la formalisation des théorèmes de décomposition de Hahn puis de Jordan.

3 Formalisation du théorème de décomposition de Hahn

Nous allons ici voir la preuve du théorème de décomposition de Hahn. Dans un premier temps nous verrons la preuve mathématique détaillée que j'en avais faite, puis la comparaison à la preuve en Isabelle, qui est encore plus détaillé que ce que j'avais initialement fait.

3.1 Preuve mathématique détaillée

Nous allons reprendre la preuve du théorème de Hahn [DiB16] et la formaliser une première fois, afin de bien comprendre tous les mécanismes mis en jeu, pour pouvoir par la suite la formaliser en Isabelle.

Preuve 1 *Soit* $\{X, \mathcal{A}\}$ *un espace mesurable et* μ *une mesure signée sur* $\{X, \mathcal{A}\}$*. Considérons le cas où :* $\forall E \subseteq X, \mu(E) < \infty$*. Posons* $M = \sup_{E \in \mathcal{A}}\{\mu(E)|\ E \text{ est positif}\}$*. On peut construire* $(A_n)_{n\in\mathbb{N}}$ *une suite dans* $\mathcal{A}$ *telle que :*

— $\forall n\ A_n$ *est positif*

— $\forall n\ \mu(A_n) \leq M$

— $\forall n\ \mu(A_{n-1}) \leq \mu(A_n)$

— $\mu(A_n) \longrightarrow_{n\to+\infty} M$

Remarquons que pour construire une telle suite, il suffit de prendre des ensembles A_n *tous positifs et vérifiant* $\forall n\ \mu(A_{n-1}) \leq \mu(A_n)$*. Les deux autres propriétés découlent de la définition de* M *et de la construction de la suite.*

Soit $A = \cup_{n\in\mathbb{N}} A_n$*. Alors* A ***est positif*** *d'après le lemme 3. et* $\mu(A) \leq M$ *par construction de* M*.*

Soit $n \in \mathbb{N}$*. Par définition de l'union,* $A = (A - A_n) \cup A_n$*. Comme* $(A - A_n)$ *et* A_n *sont disjoints, et que* A *et* A_n *sont positifs, on en déduit que* $(A - A_n)$ *est positif car c'est la différence de deux ensembles positifs. De plus,* μ *étant une mesure signée, on a* $\mu(A) = \mu(A - A_n) + \mu(A_n)$*. Comme* A *et* $(A - A_n)$ *sont positifs, on a* $\mu(A) \geq 0$ *et* $\mu(A - A_n) \geq 0$*, on en déduit que* $\mu(A) \geq \mu(A_n)$*. Comme cette inégalité est valable pour tout* n*,* $\mu(A)$ *est donc un majorant de la série* (A_n)*, dont* M *en est la borne supérieure. On en déduit que* $\mu(A) \geq M$*. Comme* $\mu(A) \geq M$ *et* $\mu(A) \leq M$*, on a* $\mu(A) = M$*. De plus,* $\mu(E) < \infty$ *pour tout ensemble mesurable* E*, donc* $M < \infty$*.*

Montrons maintenant par l'absurde que $(X - A)$ ***est négatif****. Supposons* $(X - A)$ *non négatif, il existe donc un ensemble* $E \subseteq (X - A)$ *tel que* $\mu(E) > 0$*. Par la proposition 1, il existe alors* $A_0 \subseteq E$ *tel que* A_0 *est positif, et* $\mu(A_0) > 0$*. Par construction,* A *et* A_0 *sont positifs et disjoints, donc* $A \cup A_0$ *est positif d'après le lemme 2. De plus,* $\mu(A \cup A_0) = \mu(A) + \mu(A_0) = M + \mu(A_0) > M$*. Or* $M = \sup_{E\in\mathcal{A}}\{\mu(E)|\ E \text{ est positif}\}$*, d'où la contradiction.*

Ainsi, en considérant les ensembles A *et* $X - A$ *définis ci-dessus et qui sont respectivement positifs et négatifs, on obtient bien une décomposition de l'univers* X *en deux ensembles respectivement positif et négatif.*

Maintenant que nous avons compris tous les tenants et les aboutissants de ce théorème, nous pouvons le formaliser sous Isabelle.

3.2 Principe de la preuve de l'unicité essentielle de la décomposition de Hahn

La décomposition de Hahn est essentiellement unique, mais pas unique. Je n'ai pas formalisé cette partie du théorème, aussi, je vais ici expliquer le principe de la preuve de l'unicité essentielle.

Définition 4 *Soit* $\{X, \mathcal{A}\}$ *un espace mesurable et* μ *une mesure signée sur* $\{X, \mathcal{A}\}$*. Un ensemble mesurable* $E \in \mathcal{A}$ *est* ***nul*** *si tous ses sous-ensembles sont de mesure nulle.*

Soit $\{X, \mathcal{A}\}$ un espace mesurable et μ une mesure signée sur $\{X, \mathcal{A}\}$. Soit X^+ et X^- les ensembles respectivement positif et négatif de la décomposition de Hahn de X. Considérons un ensemble nul $\mathcal{E}$ inclut dans X^+. Alors, $(X^+ - \mathcal{E})$ reste un ensemble positif, et $(X^- \cup \mathcal{E})$ reste un ensemble négatif. De plus, on a toujours $X = (X^+ - \mathcal{E}) \cap (X^- \cup \mathcal{E})$. Ainsi, $(X^+ - \mathcal{E})$ et $(X^- \cup \mathcal{E})$ est une autre décomposition de Hahn pour X. Cette décomposition n'est alors pas unique [DiB16]. Cependant, elle est unique à des ensembles nuls près. En effet, si on considère (X^+, X^-) et (X_0^+, X_0^-) deux décompositions de Hahn de X, on a $\mu(X^+ \cup X_0^-) = 0$ et $\mu(X^- \cup X_0^+) = 0$ [Wik18]. La décomposition de Hahn est donc essentiellement unique.

3.3 Formalisation en Isabelle

Pour la formalisation avec Isabelle, nous allons avoir besoin de manipuler régulièrement l'espace des ensembles positifs et l'image de cet espace par μ. Aussi, nous posons ces deux définitions, qui sont disponibles dans la sous-section "Some definitions" de la section "Hahn decomposition theorem".

Ensuite, la suite $(A_n)_{n\in\mathbb{N}}$ va intervenir régulièrement, nous déclarons deux définitions et prouvons deux lemmes pour factoriser et simplifier la preuve du théorème par la suite. Ces éléments sont disponible dans la théorie HahnDecomp [Her21], dans la sous-section "Increasing sequence of positive measurable sets".

Finalement, nous pouvons formaliser le cas où $\forall E \subseteq X, \mu(E) < \infty$ dans le lemme suivant. Pour rappel, c'est celui-là qui avait été explicité dans la preuve détaillée 1.

lemma (*in* `signed_measure_space`) HAHN_DECOMP_INFINITY
  assumes $\forall E \in sets\ M.\ \mu\ E < \infty$
  shows $\exists\ M1\ M2.$ (`pos_meas_set` $M1$) $\wedge$ (`neg_meas_set` $M2$)
  $\wedge(space\ M = M1 \cup M2) \wedge (M1 \cap M2 = \{\})$

Certaines déductions de la formalisation de ce lemme ont été à détailler en Isabelle plus précisément encore que dans la section précédente.

Enfin, pour prouver l'autre cas, où μ peut prendre $+\infty$ comme valeur (mais alors pas $-\infty$ par définition d'une mesure signée (definition 1), nous allons poser m une mesure signée, qui à tout ensemble E associe $-\mu(E)$. Ainsi, nous pouvons appliquer le lemme HAHN_DECOMP_INFINITY à l'espace mesurable $\{X, \mathcal{A}\}$ et la mesure signée m sur $\{X, \mathcal{A}\}$. Il faut ensuite montrer qu'un espace positif par rapport à μ est un espace négatif par rapport à m, et vice-versa. Nous utiliserons pour cela deux autres lemmes, POS_MEAS_SET_OPP et NEG_MEAS_SET_OPP.

lemma (*in* `signed_measure_space`) POS_MEAS_SET_OPP
  assumes `signed_measure_space.pos_meas_set` $M\ (\lambda\ A.\ -\mu\ A)\ A$
  shows `neg_meas_set` A

Voici pour finir l'énoncé du théorème 1 en lui-même :

theorem (*in* `signed_measure_space`) HAHN_DECOMPOSITION
  shows $\exists\ M1\ M2.$ (`pos_meas_set` $M1$) $\wedge$ (`neg_meas_set` $M2$)
  $\wedge(space\ M = M1 \cup M2) \wedge (M1 \cap M2 = \{\})$

3.3.1 Résultats

En fin de compte, nous avons prouvé le théorème de décomposition de Hahn, en admettant la proposition 1 (qui repose sur le lemme 4 qui n'a pas été prouvé non plus), nous avons pu formaliser et prouver le théorème de décomposition de Hahn en Isabelle.

La question s'est ensuite posée de formaliser et prouver cette proposition et son lemme, mais nous avons trouvé (Mnacho Echenim, Hervé Guiol et moi), que formaliser et prouver le théorème de Jordan, qui découle du théorème de Hahn, serait plus intéressant dans le cadre de l'IRL.

4 Formalisation du théorème de Jordan

Le théorème de Jordan est une conséquence du théorème de décomposition de Hahn, qui montre qu'il existe une décomposition de la mesure signée μ en deux mesures standard μ^+ et μ^-, de manière à ce que $\mu = \mu^+ - \mu^-$.

4.1 Énoncé

L'énoncé formalisé du théorème de Jordan est le suivant :

Théorème 2 *Soit* $\{X, \mathcal{A}\}$ *un espace mesurable. Toute mesure* μ *sur* $\mathcal{A}$ *possède une unique décomposition de la forme* $\mu = \mu^+ - \mu^-$*, où* μ^+ *et* μ^- *sont deux mesures positives, dont au moins l'une est finie, et telles que :*

— $\mu^+(E) = 0$ *pour tout* E *mesurable tel que* $E \subseteq N$

— $\mu^-(E) = 0$ *pour tout* E *mesurable tel que* $E \subseteq P$

où P *et* N *sont les deux ensembles respectivement positifs et négatifs de la décomposition de Hahn, i.e. tels que* $X = P \cup N$*.*

On peut alors remarquer que μ^+ est la partie positive de μ et μ^- est sa partie négative.

4.2 Formalisation en Isabelle

Pour formaliser le théorème, j'ai travaillé directement sur Isabelle, sans formaliser la preuve au préalable. J'avais en effet mieux compris et assimilé comment le logiciel fonctionnait, et le théorème me paraissait suffisamment clair pour pouvoir faire cela. Voici l'énoncé formalisé du théorème, disponible dans la section "Jordan decomposition theorem" de la formalisation [Her21].

theorem (*in* `signed_measure_space`) JORDAN_DECOMPOSITION
shows $\exists\ m1\ m2.\ \forall A.\ A \in \texttt{sets}\ M \ \rightarrow\ \mu\ A = (m1\ A) - (m2\ A)$

4.3 Résultats

La formalisation de la preuve du théorème de Jordan réutilise le théorème de décomposition de Hahn. De plus, il a fallu faire le lien entre la mesure signée μ de la locale, et les mesures standard $m1$ et $m2$ de la décomposition de Jordan.

5 Conclusion

Ainsi, nous avons pu formaliser en Isabelle le théorème de décomposition de Hahn ainsi que celui de Jordan. Cependant, je n'ai pas formalisé l'unicité essentielle de la décomposition de Hahn, ni l'unicité de la décomposition de Jordan. Ce sont des résultats intéressants qu'il serait utile de prouver. J'ai trouvé cela très enrichissant et intéressant, d'un côté de par les notion manipulées (nous ne manipulons plus d'ensembles ou presque en cours), et d'un autre côté de par la logique et le raisonnement qu'il faut utiliser pour formaliser le théorème.

J'ai découvert que formaliser un résultat mathématique à l'aide d'un assistant de preuve impliquait un certain formalisme et une certaine rigueur pour écrire la preuve dans la syntaxe du langage Isar, et j'ai adoré le faire.

Par contre, je ne pensais pas que cela serait aussi chronophage. En effet, j'ai passé plusieurs semaines sur la compréhension mathématique des preuves (sans laquelle la formalisation est impossible), puis deux semaines à bien les formaliser sur papier d'une part, et prendre en main Isabelle d'autre part en faisant des petits exercices pour m'habituer au langage [Ger20]. C'est seulement en commençant à les formaliser que je me suis rendue compte de tous les lemmes qui étaient requis pour le théorème, autres que les définitions et propriétés des ensembles positifs ou négatifs. En effet, pour prouver les deux théorèmes (de décomposition de Hahn et de décomposition de Jordan), il aura fallu un peu plus de 900 lignes en Isabelle !

Avec le théorème de décomposition de Jordan et son corollaire, j'ai aussi bien vu l'importance de factoriser du code en lemmes intermédiaires lorsque celui-ci est réutilisé à différents endroits. En effet, le langage Isar, s'il est intuitif, est compliqué à relire dès que la preuve dépasse la dizaine de lignes, ce qui arrive très vite, car il faut vraiment tout préciser dans la moindre étape à Isabelle, ce qui est fastidieux, et prend des lignes.

J'ai énormément apprécié ces quelques heures d'IRL par semaine, et cela m'a conforté dans mon envie de poursuivre mes études dans la voie de la recherche. J'envisage en effet de poursuivre mes étude en faisant une thèse dans le domaine de l'informatique théorique.

6 Remerciements

Je voudrais remercier Mnacho Echenim et Hervé Guiol, qui sont deux professeurs et chercheurs formidables, et qui ont su me proposer un sujet d'IRL qui correspond exactement à ce mélange de mathématiques et d'informatique que j'apprécie. Je tenais à les remercier pour leur patience, leur gentillesse, leur pédagogie et leur disponibilité. Merci infiniment de m'avoir aidé à comprendre et m'approprier ce sujet et ces notions mathématiques, merci infiniment d'avoir été là et de m'avoir aidé quand j'avais des soucis (avec Isabelle ou les théorèmes), merci pour m'avoir rééxpliqué ce que je n'avais pas compris. Merci pour tout, ce projet d'IRL a été une expérience très enrichissante que j'ai beaucoup aimé.

Références

[Bal10] Clemens Ballarin. "Tutorial to Locales and Locale Interpretation". In : *Contribuciones Científicas en honor de Mirian Andrés* (2010).

[HH11] Johannes Hölzl et Armin Heller. "Three Chapters of Measure Theory in Isabelle/HOL". In : (2011).

[Del12] Jean-Paul Delahaye. "Du rêve à la réalité des preuves". In : *interstices.info* (2012). doi : `https://interstices.info/du-reve-a-la-realite-des-preuves/`.

[DiB16] Emmanuele DiBenedetto. *Real Analysis*. Birkhäuser Advanced Texts Basler Lehrbücher, 2016.

[Wik18] Wikipedia. "Hahn decomposition theorem". In : *Wikipedia* (2018). doi : `https://en.wikipedia.org/wiki/Hahn_decomposition_theorem`.

[Ech20] Mnacho Echenim. "IRL - Formalisation du théorème de décomposition de Hahn avec le démonstrateur interactif Isabelle". In : *ensiwiki.ensimag.fr* (2020). doi : `https://ensiwiki.ensimag.fr/index.php?title=IRL_-_Formalisation_du_thÃľorÃĺme_de_dÃľcomposition_de_Hahn_avec_le_dÃľmonstrateur_interactif_Isabelle`.

[Ger20] Tobias Nipkow et Gerwin Klein. *Concrete Semantics*. Springer Verlag, 2020.

[Her21] Mnacho Echenim et Hervé Guiol et Marie Cousin. In : (2021). doi : `https://gitlab.ensimag.fr/cousinm/irl-hahndecompositionthm`.

[Uni21] Technische Universität München et University of Cambridge. "Overview". In : *isabelle.in.tum.de* (2021). doi : `https://isabelle.in.tum.de/overview.html`.