Simplicité — compte rendu d'expérience en formalisation de preuves

Antoine Chambert-Loir (*Université Paris Cité*)

Colloquium mathématique de Caen, 25 novembre 2022

Sommaire

Formules mathématiques et mathématiques formelles

Fin du 19e s., début du 20e s. :

- Apparence de la nécessité de définitions plus précises (Dedekind, Heine, Cantor, Zermelo…)
- Plusieurs entreprises de rédactions formelles, symboliques, des mathématiques depuis leur début.

Giuseppe Peano

G. Peano (1889), *Arithmetices principa, nova methodo exposita*

« Leibniz a énoncé, il y a deux siècles, le projet de créer une écriture universelle, dans laquelle toutes les idées composées fussent exprimées au moyen de signes conventionnels des idées simples, selon des règles fixes. »

Alfred N. Whitehead & Bertrand Russell

A. N. Whitehead & B. Russell (1927), *Principia mathematica*

« We have found it necessary to give very full proofs, because otherwise it is scarcely possible to see what hypotheses are really required, or whether our results follow from our explicit premisses. (It must be remembered that we are not affirming merely that such and such propositions are true, but also that the axioms stated by us are sufficient to prove them.) »

N. Bourbaki

N. Bourbaki (1935), *Éléments de mathématique*

« (...) l'analyse du mécanisme des démonstrations dans des textes mathématiques bien choisis a permis d'en dégager la structure, du double point de vue du vocabulaire et de la syntaxe. On arrive ainsi à la conclusion qu'un texte mathématique suffisamment explicite pourrait être exprimé dans une langue conventionnelle ne comportant qu'un petit nombre de "mots" invariables assemblés suivant une syntaxe qui consisterait en un petit nombre de règles inviolables : un tel texte est dit formalisé. »

N. Bourbaki, encore

« Si la mathématique formalisée était aussi simple que le jeu d'échecs, une fois décrit le langage formalisé que nous avons choisi, il n'y aurait plus qu'à rédiger nos démonstrations dans ce langage, comme l'auteur d'un traité d'échecs écrit dans sa notation les parties qu'il se propose d'enseigner, en les accompagnant au besoin de commentaires. Mais les choses sont loin d'être aussi faciles, et point n'est besoin d'une longue pratique pour s'apercevoir qu'un tel projet est absolument irréalisable ; la moindre démonstration du début de la *Théorie des Ensembles* exigerait déjà des centaines de signes pour être complètement formalisée. »

N. Bourbaki, toujours

« Une estimation grossière montre que le terme *désigné* [par “1”] est un assemblage de plusieurs dizaines de milliers de signes (chacun de ces signes étant l’un des signes τ, $\square$, $\vee$, $\neg$, $=$, $\in$). »

A. R. D. Mathias

A. R. D. Mathias (2002), Hold my beer !

« Bourbaki suggest that their definition of the number 1 runs to some tens of thousand of symbols. We show that that is a considerable under-estimate, the true number of symbols being that in the title [4 523 659 424 929] not counting 1 179 618 517 981 links between symbols that are needed to disambiguate the whole expression. »

Assistants de preuves

L'avénement des ordinateurs depuis les années 50 a conduit à chercher à mécaniser ces vérifications. Plusieurs logiciels ont vu le jour, entre autres :

- N.G. De Bruijn, `Automath` (1967)
- A. Trybulec, `Mizar` (1973)
- G. Huet et al., `Coq` (1989)
- C. Coquand, `Agda` (1999)
- L. de Mourra, `Lean` (2013)...

Chacun correspond à des choix (techno)logiques. Par exemple, `Mizar` est fondé sur la théorie des ensembles, `Coq` et `Lean` sur la théorie des types dépendants, `Agda` sur la théorie homotopique des types.

Assistants de preuves : succès

- G. Gonthier et al. (2008), le théorème des 4 couleurs d'Appell et Haken
- G. Gonthier et al. (2013), le théorème de Feit Thompson
- T. Hales (2017), la conjecture de Kepler (prouvée par lui)
- J. Commelin et al. (2022), un théorème de Scholze dans l'algèbre commutative des mathématiques condensées ("Large tensor experiment")
- P. Massot et al. (2022), le h-principe de Gromov et le retournement de la sphère

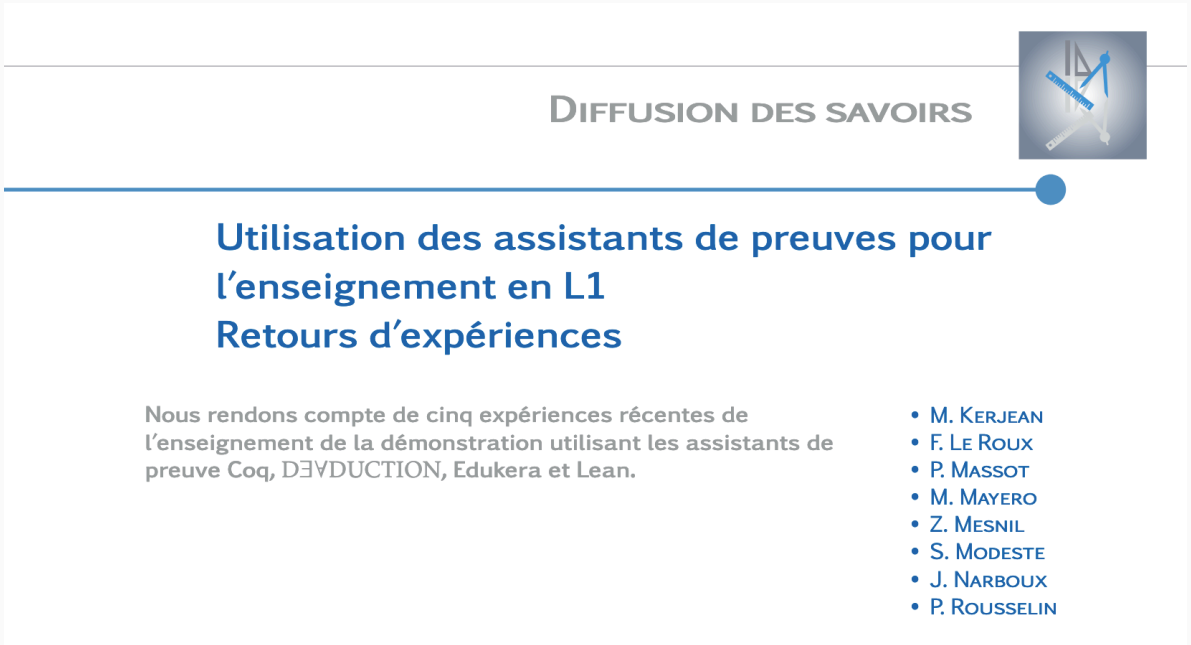
Que fait un assistant de preuve ?

C’est une sorte de compilateur qui « lit » des énoncés de théorèmes et leurs démonstrations supposées, écrites dans un langage approprié et garantit que les démonstrations atteignent leur but.

Ils sont aussi capables (avec plus ou moins de bonheur) de faire tout seul des bouts de démonstration (en gros, du niveau d’un exercice de licence).

Assistants de preuves : un outil d'enseignement ?

Depuis quelques années, des collègues en maths et info utilisent ces assistants de preuves comme aide à l'enseignement des preuves, entre L1 et L3.



DIFFUSION DES SAVOIRS

Utilisation des assistants de preuves pour l'enseignement en L1
Retours d'expériences

Nous rendons compte de cinq expériences récentes de l'enseignement de la démonstration utilisant les assistants de preuve Coq, DƎVDUCTION, Edukera et Lean.

- M. KERJEAN
- F. LE ROUX
- P. MASSOT
- M. MAYERO
- Z. MESNIL
- S. MODESTE
- J. NARBOUX
- P. ROUSSELIN

Gazette de la Société mathématique de France, oct. 2022

Assistants de preuves : un outil quotidien ?

Peut-on imaginer que dans un futur proche, nos théorèmes seront directement implémentés dans de tels outils.

Intérêts :

- garantit la sûreté des démonstrations ;
- déplace le travail de communication vers la compréhension

Difficultés :

- nécessité d'une sorte de « bibliothèque de Babel mathématique »
- passerelles entre les différents logiciels
- obsolescence logicielle

Mathlib

Adossée au logiciel `lean`, on trouve une librairie *mathlib* qui fait déjà plus d'un million de lignes de codes et couvre une large partie des mathématiques :

- théorie de la mesure, théorie ergodique,
- algèbre générale, théorie des corps,
- analyse complexe,
- analyse fonctionnelle,
- variétés différentielles...

C'est aujourd'hui une motivation importante pour participer à ce projet.

Sommaire

Simplicité du groupe alterné

Théorème

Si $n \geqslant 5$, le groupe alterné $\mathfrak{A}_n$ est simple : ses seuls sous-groupes distingués sont $\{e\}$ et lui-même.

Une des briques de la classification des groupes finis simples ; les autres sont

- les groupes cycliques d'ordre premier,
- des familles de groupes venant de la géométrie (comme $\mathrm{PSL}(n, F)$) si F est un corps fini de cardinal $\geqslant 4$),
- 26 groupes « sporadiques » liés à des géométries combinatoires.

Pourquoi faire simple...

Pourquoi faire simple...

Le théorème de simplicité est accessible dans un cours de L3/M1, par une démonstration un peu ad hoc, et dont les présentations principales demandent des calculs qui ne sont pas aisées à communiquer à l'ordinateur. (J'ai pu le faire...)

Dès le début, j'avais souhaité le démontrer d'une façon plus compliquée, en faisant usage d'un critère de simplicité général introduit par Iwasawa (1941) pour prouver la simplicité de groupes géométriques.

Ce critère peut être réutilisé pour prouver d'autres résultats de simplicité, de façon plus uniforme, par exemple les groupes de Mathieu.

Le critère d'Iwasawa

Proposition (Iwasawa, 1941)

Soit G un groupe opérant sur un ensemble X. On suppose que l'action est 2-transitive et que pour tout $x \in X$, on dispose d'un sous-groupe A_x de G tels que

- *Pour $g \in G$ et $x \in X$, on a $A_{g \cdot x} = g A_x g^{-1}$;*
- *Les groupes A_x sont commutatifs et leur réunion engendrent G.*

Alors tout sous-groupe distingué de G qui agit non trivialement sur X contient le groupe dérivé G' de G.

Groupe dérivé

Rappel : c'est le sous-groupe engendré par les commutateurs.

(Plus petit noyau d'un morphisme vers un groupe commutatif.)

Exemples :

- $\mathfrak{A}_n' = \mathfrak{A}_n$ si $n \geqslant 5$, et c'est bien plus facile que la simplicité (lié à la non-résolubilité de $\mathfrak{A}_n$).
- $\mathrm{SL}(n, F)' = \mathrm{SL}(n, F)$ si $n \geqslant 3$ ou $\mathrm{Card}(F) \geqslant 3$.

“Simplicité” de $\mathrm{SL}(n, F)$

Soit V un espace vectoriel de dimension finie $\geqslant 2$ sur un corps F. On fait agir $\mathrm{SL}(V)$ sur l'espace des droites de V, qui est l'espace projectif $\mathbf{P}(V)$. L'action est 2-transitive.

Pour une droite $D \subseteq V$, on note A_D l'ensemble des transvections u de la forme $x \mapsto x + \varphi(x)e$, où $e \in D$ et $D \subseteq \ker(\varphi)$. C'est un sous-groupe commutatif de $\mathrm{SL}(V)$.

On a $A_{g.D} = gA_Dg^{-1}$.

Ces groupes engendrent $\mathrm{SL}(V)$.

Tout sous-groupe distingué N de $\mathrm{SL}(V)$ qui agit non trivialement sur $\mathbf{P}(V)$ contient donc le sous-groupe des commutateurs de $\mathrm{SL}(V)$. La condition est que N ne soit pas contenu dans le centre de $\mathrm{SL}(V)$.

Si $\dim(V) \geqslant 3$ *ou* $\mathrm{Card}(F) \geqslant 4$, *alors* $\mathrm{PSL}(V)$ *est simple.*

Simplicité de $\mathfrak{A}_5$

On applique le critère d'Iwasawa à l'action de $\mathfrak{A}_5$ sur $X = \{1, 2, 3, 4, 5\}$.

Pour $x \in X$, on définit A_x comme le groupe des double-transpositions qui fixent x : c'est un groupe de Klein.

- Cette action est 2-transitive.
- Relation de conjugaison $A_{g.x} = gA_xg^{-1}$
- Ils engendrent $\mathfrak{A}_5$.

Conclusion : tout sous-groupe distingué non trivial de $\mathfrak{A}_5$ contient le groupe dérivé, donc est égal à $\mathfrak{A}_5$.

Simplicité de $\mathfrak{A}_n$

Il va falloir appliquer une variante du critère d'Iwasawa à l'action de $\mathfrak{A}_n$ sur l'ensemble des parties de $X = \{1, \ldots, n\}$ à k éléments, pour $k = 3$ ou $k = 4$.

Si S est une telle partie, on définit A_S comme

- le groupe alterné $\mathfrak{A}_S$ de cette partie si $k = 3$,
- le groupe des double transpositions à support dans cette partie si $k = 4$.

Ce sont des groupes commutatifs, isomorphes à $\mathbf{Z}/3\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$.

On a la relation $A_{g.S} = gA_Sg^{-1}$.

Leur réunion engendre $\mathfrak{A}_n$ (parce que les 3-cycles engendrent, ou bien les double transpositions).

Simplicité de $\mathfrak{A}_n$

Il va falloir appliquer une variante du critère d'Iwasawa à l'action de $\mathfrak{A}_n$ sur l'ensemble des parties de $X = \{1, \ldots, n\}$ à k éléments, pour $k = 3$ ou $k = 4$.

Si S est une telle partie, on définit A_S comme

- le groupe alterné $\mathfrak{A}_S$ de cette partie si $k = 3$,
- le groupe des double transpositions à support dans cette partie si $k = 4$.

Ce sont des groupes commutatifs, isomorphes à $\mathbf{Z}/3\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$.

On a la relation $A_{g.S} = gA_Sg^{-1}$.

Leur réunion engendre $\mathfrak{A}_n$ (parce que les 3-cycles engendrent, ou bien les double transpositions).

Problème : l'action n'est pas 2-transitive.

Sommaire

Actions primitives

On appelle **bloc** de X une partie $B \subseteq X$ telle que pour tout $g \in G$, soit $B = g \cdot B$, soit $B \cap g \cdot B = \emptyset$.

$B = \emptyset$, les singletons, $B = X$ sont des blocs, dits *triviaux*.

Définition

Une action d'un groupe G sur un ensemble X est primitive si les seuls blocs sont les blocs triviaux.

Variante : les seules relations d'équivalences sur X qui sont compatibles avec l'action de G sont triviales (discrète ou grossière).

Introduit par Galois dans sa lettre à Auguste Chevalier : alors X est l'ensemble des racines d'un polynôme sur lequel agit le groupe de Galois G.

Transitivité et primitivité

Une orbite est un bloc, donc *une action primitive est transitive*.

Transitivité et primitivité

Une orbite est un bloc, donc *une action primitive est transitive.*

Une action 2-transitive est primitive.

Soit B un bloc non trivial.
Soit $x, y \in B$, et soit $z \in X \setminus B$.
Par 2-transitivité, il existe $g \in G$ tel que $g \cdot x = x$ et $g \cdot y = z$.
Alors, $x \in B \cap g \cdot B$, donc $B = g \cdot B$.
Comme $y \in B$ et $z = g \cdot y$, on a $z \in B$; contradiction.

Actions primitives : géométrie

L'action de $\mathrm{SO}(3, \mathbf{R})$ *sur les droites de* $\mathbf{R}^3$ *est*

- *transitive :* si u, v sont des vecteurs unitaires, il existe $g \in \mathrm{SO}(3, \mathbf{R})$ tel que $g \cdot u = v$.
- *non 2-transitive :* les rotations préservent les angles de droites
- mais est *primitive :* si un bloc contient (la droite passant par) le pôle nord et un autre point, il contient tout le parallèle correspondant, puis toute la sphère.

On en déduit que le groupe $\mathrm{SO}(3, \mathbf{R})$ est simple.

Actions primitives : géométrie

L'action de $\mathrm{SO}(3, \mathbf{R})$ *sur les droites de* $\mathbf{R}^3$ *est*

- *transitive :* si u, v sont des vecteurs unitaires, il existe $g \in \mathrm{SO}(3, \mathbf{R})$ tel que $g \cdot u = v$.
- *non 2-transitive :* les rotations préservent les angles de droites
- mais est *primitive :* si un bloc contient (la droite passant par) le pôle nord et un autre point, il contient tout le parallèle correspondant, puis toute la sphère.

On en déduit que le groupe $\mathrm{SO}(3, \mathbf{R})$ est simple.

Cas général ? — Pour un groupe orthogonal "non compact", Tamagawa (1958)

Actions primitives : combinatoire

Si $n \geqslant 3$ et $k \neq 0, n/2, n$, l'action de $\mathfrak{A}_n$ sur les parties à k éléments de $\{1, \ldots, n\}$ est

- *transitive :* pour $a_1, \ldots, a_k$ et $b_1, \ldots, b_k$, prendre $g \in \mathfrak{S}_n$ tel que $g \cdot a_i = b_i$ pour tout i ; si nécessaire, composer avec une transposition $(b_1\, b_2)$ si $k \geqslant 2$, ou avec une transposition $(c\, c')$ si $n - k \geqslant 2$.
- *non 2-transitive :* on a $\mathrm{Card}(g \cdot A \cap g \cdot B) = \mathrm{Card}(A \cap B)$...
- mais est *primitive*.

Simplicité de $\mathfrak{A}_n$

On en déduit une preuve un peu compliquée, mais « géométrique », de la simplicité de $\mathfrak{A}_n$:

- Si $n \geqslant 5$ et $n \neq 8$, prendre $k = 4$ et associer à une partie S de cardinal 4 le groupe des double transpositions à support dans S.
- Si $n \geqslant 5$ et $n \neq 6$, prendre $k = 3$ et associer à une partie S de cardinal 3 le groupe des permutations circulaires à support dans S.

Sommaire

Primitivité et maximalité

Proposition

Considérons un groupe G agissant transitivement et non trivialement sur un ensemble X.

L'action de G sur X est primitive

$\Leftrightarrow$ *Pour tout $x \in X$, le stabilisateur G_x de x est un sous-groupe maximal de G.*

Plus généralement, les applications

$$B \mapsto G_B, \qquad H \mapsto H \cdot x$$

sont des bijections croissantes entre l'ensemble des blocs de X contenant x et l'ensemble des sous-groupes de G contenant G_x.

Preuve du critère d'Iwasawa

Soit N un sous-groupe distingué de G qui opère non trivialement sur X.

- *N opère transitivement sur X*
- Comme l'action de G sur X est primitive, G_x est un sous-groupe maximal ; comme N est distingué, on a $G = \langle N, G_x \rangle = N \cdot G_x$. etc.
- Pour tout $x, y \in X$, on a $A_y \leqslant \langle N, A_x \rangle$.
  On peut écrire $y = n \cdot x$, pour $n \in N$, et $A_y = n \cdot A_x \cdot n^{-1}$, etc.
- Pour tout $x \in X$, on a $G = \langle N, A_x \rangle$.
  Car les A_y engendrent G.
- L'homomorphisme $A_x \to G \to G/N$ est surjectif, donc G/N est abélien.
- Donc N contient le sous-groupe dérivé de G.

Sous-groupes maximaux

Le critère d'Iwasawa justifie d'étudier systématiquement les sous-groupes maximaux d'un groupe (par exemple simple) donné. Cette étude est aussi une première étape d'une classification éventuelle des actions de groupes finis fondée sur la classification des groupes finis simples.

Ils sont explicités

- par un théorème de O'Nan–Scott (1980–81) pour le groupe symétrique/alterné ;
- par un théorème d'Aschbacher (1984) pour les groupes classiques sur un corps fini.

Le théorème de O'Nan et Scott pour le groupe alterné

Si G est un sous-groupe maximal de $\mathfrak{A}_n$, alors G est la trace sur $\mathfrak{A}_n$ d'un groupe de l'un des types suivants (à conjugaison près) :

- $G = \mathfrak{S}_k \times \mathfrak{S}_{n-k}$ pour $0 < k < n - k < n$
- $G = \mathfrak{S}_k \wr \mathfrak{S}_m$, où $n = mk$ et $m, k > 1$
- $n = p^k$ et G est le groupe affine de $\mathbf{F}_{p^k}$

et trois autres cas...

Noter que ces groupes apparaissent comme des stabilisateurs de structures naturelles dans $\mathfrak{S}_n$: d'une partie, d'une partition, d'une bijection $\{1, \ldots, n\} \to \{1, \ldots, p\}^k$, etc.

La réciproque : Liebeck, Praeger, Saxl (1987)

Essentiellement, tous les sous-groupes maximaux proposés par O'Nan sont maximaux, avec quelques exceptions.

En particulier : si $1 \leqslant k < n/2$ (et $n \geqslant 5$), le stabilisateur d'une partie de cardinal k est un sous-groupe maximal de $\mathfrak{A}_n$. Autrement dit, l'action de $\mathfrak{A}_n$ sur les parties à k éléments de $\{1, \ldots, n\}$ est primitive.

C'est ce qu'il fallait pour conclure notre preuve pas très simple de la simplicité de $\mathfrak{A}_n$.

Preuve du résultat de primitivité

Proposition

Pour $k \in \mathbf{N}$ tel que $1 \leqslant k < n - k$ et $n \geqslant 5$, le sous-groupe $G = (\mathfrak{S}_k \times \mathfrak{S}_{n-k}) \cap \mathfrak{A}_n$ de $\mathfrak{A}_n$ est maximal.

Cas $k = 1$. Alors G est le stabilisateur de $\{1\}$, pour $n \geqslant 3$, l'action de $\mathfrak{A}_n$ sur $\{1, \ldots, n\}$ est 2-transitive donc primitive, donc G est maximal.

Cas $k \geqslant 2$. Soit H un groupe tel que $G < H \leqslant \mathfrak{A}_n$; on veut prouver $H = \mathfrak{A}_n$. On utilise un théorème de Jordan (1870) : *un sous-groupe primitif de $\mathfrak{A}_n$ qui contient un 3-cycle est égal à $\mathfrak{A}_n$*. Il reste à prouver que H est primitif, qui est l'endroit où l'on utilise que $k \neq n - k$!


C'EST TOUT
POUR AUJOUR
D'HUI