Motivation: why formalise mathematics?

Michael B. Rothgang (he/him)

Symplectic geometry group
Humboldt-Universität zu Berlin

BerLean student workshop
May 10, 2024

Welcome

Who are we?

Welcome

Who are we?

Where are you based at?

Welcome

Who are we?

Where are you based at?

Are you a bachelor's, master's, PhD student, have a PhD, not at university?

Welcome

Who are we?

Where are you based at?

Are you a bachelor's, master's, PhD student, have a PhD, not at university?

Who of you has seen Lean before? (We do not assume so!)

What is a proof?

Proof: formal definition

A mathematical proof is a sequence of *formal* logical deductions, starting from a set of axioms.

Proof: practical definition

A mathematical proof is a sequence of arguments convincing an educated reader.

What is a proof?

Proof: formal definition

A mathematical proof is a sequence of *formal* logical deductions, starting from a set of axioms.

Proof: practical definition

A mathematical proof is a sequence of arguments convincing an educated reader. *In principle*, all details can be filled in.

Proof correctness is a social convention!

What is a proof: practical issues

- proof correctness is a social convention
- folklore results: believed true but no written proof

What is a proof: practical issues

- proof correctness is a social convention
- folklore results: believed true but no written proof
- most papers have errors: most are minor and fixable, some errors are grave

What is a proof: practical issues

- proof correctness is a social convention
- folklore results: believed true but no written proof
- most papers have errors: most are minor and fixable, some errors are grave

Example (Poincaré's, stability of the solar system)

Every single issue of Acta Mathematica retracted and reprinted.

Example (Four-colour theorem)

Proofs by Kempe and Tait (around 1880) each believed correct — for 11 years.

Example (Classification of finite simple groups)

Gap (quasi-thin case), only closed after 21 years

Some papers are wrong

Example (Baker's theorem, 1970)

- key lemma is false (Rempe-Sixsmith 2019)
- many papers using it can be fixed; another bunch is now open
- five much-cited papers "generalised" the argument

Some papers are wrong

Example (Baker's theorem, 1970)

- key lemma is false (Rempe-Sixsmith 2019)
- many papers using it can be fixed; another bunch is now open
- five much-cited papers "generalised" the argument

Example (Hilbert's 21st problem)

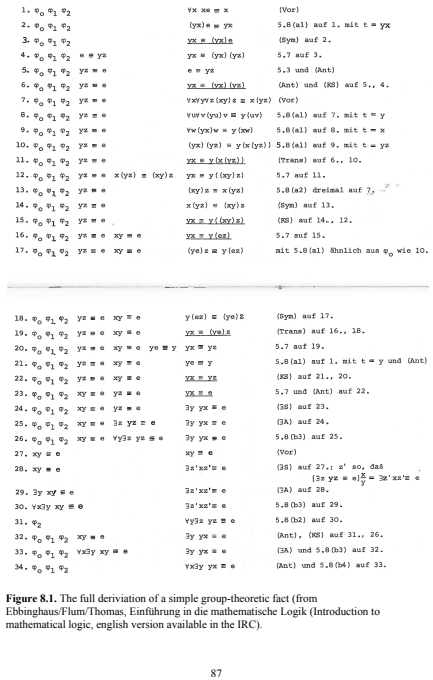
"Proof" by Plemelj (1908) found wrong in 1970s
solved in 1990 with different answer

Example (Hilbert's 16th problem, part 2)

Solution by Dulac (1923), found wrong in 1981

What does formalisation mean?

answer 1: humans write more detailed proofs



1.	$\varphi_0\,\varphi_1\,\varphi_2$	$\forall x\ xe = x$	(Vor)
2.	$\varphi_0\,\varphi_1\,\varphi_2$	$(yx)e = yx$	5.8(a1) auf 1. mit t = yx
3.	$\varphi_0\,\varphi_1\,\varphi_2$	$yx = (yx)e$	(Sym) auf 2.
4.	$\varphi_0\,\varphi_1\,\varphi_2$ $e = yz$	$yx = (yx)(yz)$	5.7 auf 3.
5.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$e = yz$	5.3 und (Ant)
6.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$yx = (yx)(yz)$	(Ant) und (KS) auf 5., 4.
7.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$\forall x\forall y\forall z(xy)z = x(yz)$	(Vor)
8.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$\forall u\forall v(yu)v = y(uv)$	5.8(a1) auf 7. mit t = y
9.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$\forall w(yx)w = y(xw)$	5.8(a1) auf 8. mit t = x
10.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$(yx)(yz) = y(x(yz))$	5.8(a1) auf 9. mit t = yz
11.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$yx = y(x(yz))$	(Trans) auf 6., 10.
12.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $x(yz) = (xy)z$	$yx = y((xy)z)$	5.7 auf 11.
13.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$(xy)z = x(yz)$	5.8(a2) dreimal auf 7.
14.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$x(yz) = (xy)z$	(Sym) auf 13.
15.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$	$yx = y((xy)z)$	(KS) auf 14., 12.
16.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$yx = y(ez)$	5.7 auf 15.
17.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$(ye)z = y(ez)$	mit 5.8(a1) ähnlich aus φ_0 wie 10.
18.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$y(ez) = (ye)z$	(Sym) auf 17.
19.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$yx = (ye)z$	(Trans) auf 16., 18.
20.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$ $ye = y$	$yx = yz$	5.7 auf 19.
21.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$ye = y$	5.8(a1) auf 1. mit t = y und (Ant)
22.	$\varphi_0\,\varphi_1\,\varphi_2$ $yz = e$ $xy = e$	$yx = yz$	(KS) auf 21., 20.
23.	$\varphi_0\,\varphi_1\,\varphi_2$ $xy = e$ $yz = e$	$yx = e$	5.7 und (Ant) auf 22.
24.	$\varphi_0\,\varphi_1\,\varphi_2$ $xy = e$ $yz = e$	$\exists y\ yx = e$	(ZS) auf 23.
25.	$\varphi_0\,\varphi_1\,\varphi_2$ $xy = e$ $\exists z\ yz = e$	$\exists y\ yx = e$	(ZA) auf 24.
26.	$\varphi_0\,\varphi_1\,\varphi_2$ $xy = e$ $\forall y\exists z\ yz = e$	$\exists y\ yx = e$	5.8(b3) auf 25.
27.	$xy = e$	$xy = e$	(Vor)
28.	$xy = e$	$\exists z'xz' = e$	(ZS) auf 27., z' so, daß $[\exists z\ yz = e]^{z}_{z'} = \exists z'xz' = e$
29.	$\exists y\ xy = e$	$\exists z'xz' = e$	(ZA) auf 28.
30.	$\forall x\exists y\ xy = e$	$\exists z'xz' = e$	5.8(b3) auf 29.
31.	φ_2	$\forall y\exists z\ yz = e$	5.8(b2) auf 30.
32.	$\varphi_0\,\varphi_1\,\varphi_2$ $xy = e$	$\exists y\ yx = e$	(Ant), (KS) auf 31., 26.
33.	$\varphi_0\,\varphi_1\,\varphi_2$ $\forall x\exists y\ xy = e$	$\exists y\ yx = e$	(ZA) und 5.8(b3) auf 32.
34.	$\varphi_0\,\varphi_1\,\varphi_2$	$\forall x\exists y\ yx = e$	(Ant) und 5.8(b4) auf 33.

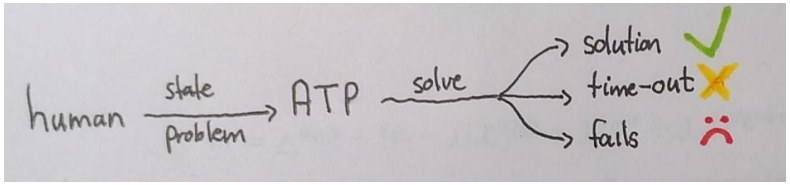
Figure 8.1. The full deriviation of a simple group-theoretic fact (from Ebbinghaus/Flum/Thomas, Einführung in die mathematische Logik (Introduction to mathematical logic, english version available in the IRC).

87

problem: impractical in the large
how to formalise “draw a picture”?

What does formalisation mean? (cont.)

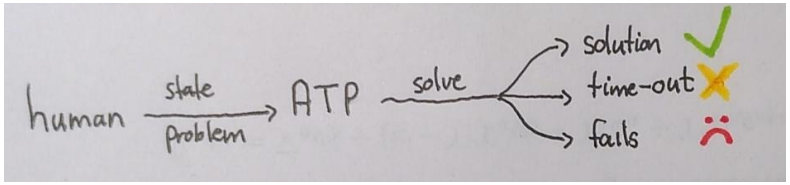
answer 2: automated theorem proving



problems: hit or miss; opaque

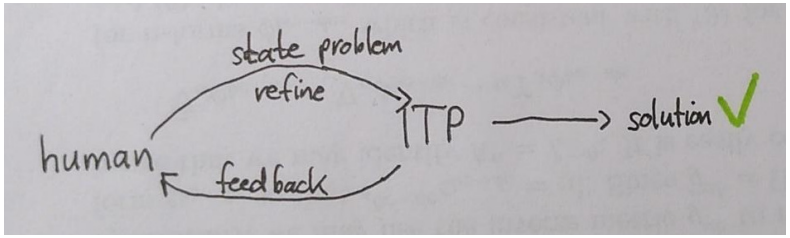
What does formalisation mean? (cont.)

answer 2: automated theorem proving



problems: hit or miss; opaque

answer 3: interactive theorem proving



Why formalise?

Verification

Understanding

Creation

Collaboration

Why formalise?

- verification: peer reviewer's dream
  only check definitions and theorems make sense
- understanding: reader chooses amount of detail

  Demo by Patrick Massot and Kyle Miller:
  `https://www.imo.universite-paris-saclay.fr/~patrick.massot/Examples/ContinuousFrom.html`

Why formalise?

- verification: peer reviewer's dream
  only check definitions and theorems make sense
- understanding: reader chooses amount of detail

  Demo by Patrick Massot and Kyle Miller:
  `https://www.imo.universite-paris-saclay.fr/~patrick.massot/Examples/ContinuousFrom.html`
- database of theorems: searching known and related results
  only requires *statements* of main results
- creation: can this lemma be generalised? unused assumptions?
- collaboration: less trust required

What has been formalised already: let's guess

- Banach–Schauder open mapping theorem
- Birkhoff Ergodic Theorem
- Mandelbrot set is connected
- Cauchy-Kovalevskaya Theorem on existence of an analytical solution of an analytical PDE.
- Denjoy's theorem: a C^2 orientation-preserving diffeomorphism of the circle with an irrational rotation number is conjugate to a rotation.
- Sphere eversion
- Existence of Haar measure
- Existence of a smooth partition of unity
- Feit–Thompson theorem/odd order theorem
- Fermat's Last Theorem
- Four colour theorem
- Galois correspondence
- Herman-Yoccoz theorem on linearization of a circle diffeomorphism
- Jordan curve theorem
- Liouville theorem: an entire holomorphic function is a constant
- Hilbert's Nullstellensatz
- Picard-Lindelöf theorem (existence and uniqueness of solutions of ODEs)
- Poincaré-Bendixson Theorem
- Poincaré recurrence theorem
- Sard's Theorem
- The continuum hypothesis is independent of ZFC.

Let's guess: the answer

Only 5 are not formalised yet (AFAIK)

- Cauchy-Kovalevskaya Theorem on existence of an analytic solution of an analytic PDE
- Denjoy's theorem on rotation number
- Herman-Yoccoz theorem on linearization of a circle diffeomorphism
- Fermat's Last Theorem
- Sard's Theorem

Let's guess: the answer

Only 5 are not formalised yet (AFAIK)

- Cauchy-Kovalevskaya Theorem on existence of an analytic solution of an analytic PDE
- Denjoy's theorem on rotation number
- Herman-Yoccoz theorem on linearization of a circle diffeomorphism
- Fermat's Last Theorem (in progress)
- Sard's Theorem (in progress)

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

2014 Kepler's conjecture (Hales et al)

2019 Ellenberg-Gijswijt's result on the cap set conjecture

2022 Liquid Tensor Experiment (Commelin et al): fundamental lemma about condensed mathematics

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

2014 Kepler's conjecture (Hales et al)

2019 Ellenberg-Gijswijt's result on the cap set conjecture

2022 Liquid Tensor Experiment (Commelin et al): fundamental lemma about condensed mathematics

2022 unit fractions project

2023 upper bound on diagonal Ramsey numbers

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

2014 Kepler's conjecture (Hales et al)

2019 Ellenberg-Gijswijt's result on the cap set conjecture

2022 Liquid Tensor Experiment (Commelin et al): fundamental lemma about condensed mathematics

2022 unit fractions project

2023 upper bound on diagonal Ramsey numbers

2023 polynomial Freiman-Rusza conjecture (Tao et al)

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

2014 Kepler's conjecture (Hales et al)

2019 Ellenberg-Gijswijt's result on the cap set conjecture

2022 Liquid Tensor Experiment (Commelin et al): fundamental lemma about condensed mathematics

2022 unit fractions project before referee report

2023 upper bound on diagonal Ramsey numbers before referee report

2023 polynomial Freiman-Rusza conjecture (Tao et al)

Notable formalisation projects

2005 Four colour theorem

2012 Odd Order Theorem

2014 Kepler's conjecture (Hales et al)

2019 Ellenberg-Gijswijt's result on the cap set conjecture

2022 Liquid Tensor Experiment (Commelin et al):
fundamental lemma about condensed mathematics

2022 unit fractions project before referee report

2023 upper bound on diagonal Ramsey numbers before referee report

2023 polynomial Freiman-Rusza conjecture (Tao et al)
took 3 weeks; complete before paper submitted

Some ongoing projects

- Almost Periodicity in Arithmetic Progressions
- Existence of an aperiodic monotile
- Prime Number Theorem (Kontorovich-Tao et al)
- Fermat's Last Theorem (Buzzard)

A zoo of interactive theorem provers

- four widely used interactive theorem provers: Coq, Isabelle/HOL, Mizar and Lean
- large mathematics libraries: *mathcomp*, *Archive of formal proofs*, *Mizar Mathematical Library*, *mathlib*
- Coq: standard tool for software verification
- Isabelle: simple foundations, powerful automation
- Mizar: huge library
- Lean: newest ($<$10 years old), fast-growing

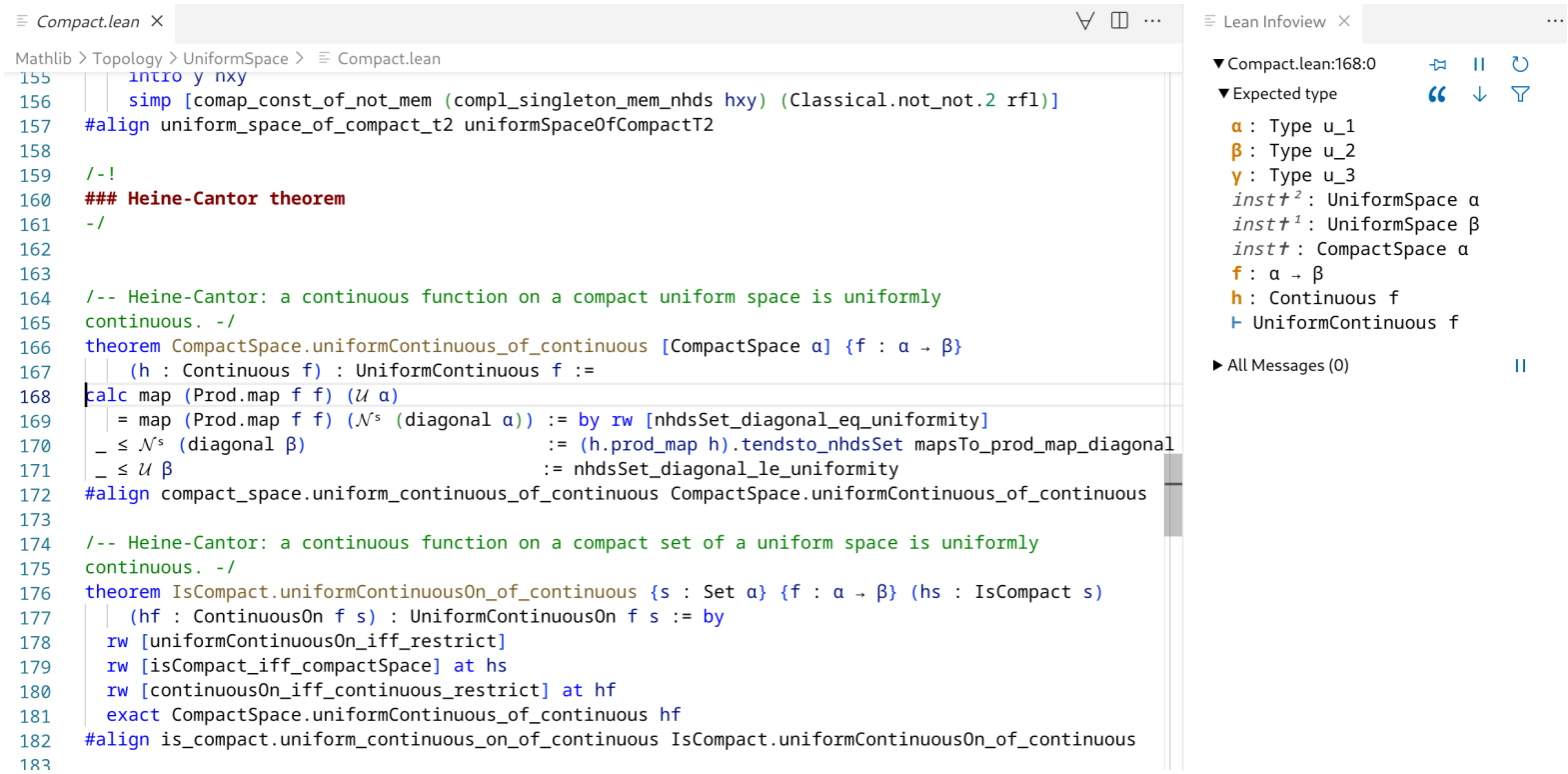
Formalising research mathematics

- need a large library of mathematics
- need an integrated library:
  connecting different fields, in a compatible way

Formalising research mathematics

- need a large library of mathematics
- need an integrated library:
  connecting different fields, in a compatible way
- Why mathlib?
  - large integrated library
  - growing *fast*
  - system and tools are improving quickly
  - friendly and diverse community (github, zulip)

A first glance



What is formalisation like?

- fussy; steep learning curve
- it's fun — like a video game or programming
- makes you understand mathematics better

Learning Lean

Attend today's workshop, ask questions

Continuation possible: another workshop, project groups, ...

Learning Lean at home

- play the natural number game: `https://adam.math.hhu.de/#/g/leanprover-community/NNG4`
- textbook: mathematics in Lean `https://leanprover-community.github.io/mathematics_in_lean/index.html`
- gentler pace: Mechanics of Proof `https://hrmacbeth.github.io/math2001/`
- further resources: `https://leanprover-community.github.io/learn.html`

Learn Lean at a tutorial

- Edinburgh, May 27-31 (registration closed)
  for women and mathematicians of minority gender
- some past events
  - Düsseldorf (September 2023)
  - Regensburg (September 2023)
  - Rome (Jan 2024)
  - Marseille (March 2024)
  - Singapore (March 2024)
  - Bonn (May 2024)
- current list: `https://leanprover-community.github.io/events.html`

Lean in Berlin

- Sebastian Pokutta, Tibor Szabó: Lean-related project
- Marc Kegel had a student using Lean
- anyone else I am not aware of?
- ask your thesis advisor if you can choose a formalisation topic :-)

When you get stuck

- don't despair, this is normal
- ask today, all the time
- ask on zulip, `https://leanprover.zulipchat.com/`
  `#new members` stream welcomes all questions
- email us (but zulip responds faster):
  Yves `jaeckle@zib.de`
  Michael `rothgami@math.hu-berlin.de`
  Nicolas `nicolas.alexander.weiss@gmail.com`

Comparing mathematical libraries: a closer look

- Archive of formal proofs: 4.1 million lines
  not integrated, articles are re-developing theory
  about half is "computer science" (e.g., properties of algorithms and programs)
- Coq's library: different focus from standard mathematics
  (e.g., care about constructivism)
- MML: large and integrated; no statistics on size
- mathlib: 1.5 million lines, integrated