

MATHEMATICAL DEFINITIONS
FORMALLY SPEAKING

THOMAS HALES*

UNIVERSITY OF PITTSBURGH



Carnegie
Mellon
University



PITTSBURGH GROUP

FORMAL ABSTRACTS PROJECT

- Floris van Doorn
- Luis Berlioz (Creating a Database of Definitions From Large Mathematical Corpora)
- Jesse Han
- Koundinya Vajjha
- working with Jeremy Avigad (CMU Lean Working Group)
- working with Tran Nam Trung (Thang Long University and Mathematics Institute, VAST, Hanoi)



Location: Thang Long University

Dates: June 5-14

Lecturer: Thomas Hales, Tran Nam Trung, Jonhalnnes Holzl, Mario Carneiro, Jesse Han

Hanoi Lean 2019

Conference on Lean and Formal Abstracts in Hanoi, June 17-20, 2019

HOME

QUY NHON MEETING

BLOG

PARTICIPANTS



Are you ready for Lean in Hanoi?

Formal Abstracts in Mathematics



Alert

But the technology is here now...

A concrete proposal: mathematical FABSTRACTS (formal abstracts)

Given today's technology, it is not reasonable to ask for all proofs to be formalized. But with today's technology, it seems that it should be possible to create a formal abstract service that

- Gives a statement of the main theorem(s) of each published mathematical paper in a language that is both human and machine readable,
- Links each term in theorem statements to a precise definition of that term (again in human/machine readable form), and
- Grounds every statement and definition in the system in some foundational system for doing mathematics.

Why?

- bring the benefits of proof assistants to the general mathematical community;
- set standards for the sciences;
- set the stage for applications to ML in mathematical proofs;
- move math closer to the computer.

The definitions of mathematics

The Oxford English dictionary (2nd edition) has 273,000 headwords and over 600,000 word forms. (The longest entry is for the word set, which continues for 25 pages).

Medicine has a specialized terminology of approximately 250,000 items [Kucharz].

The Math Subject Classification (MSC) lists over 6000 subfields of mathematics.

Mathematics Subject Classification – MSC2010

00 General mathematics	34 Ordinary differential equations	62 Statistics
01 History and biography	35 Partial differential equations	65 Numerical analysis
03 Mathematical logic and foundations	37 Dynamical systems and ergodic theory	68 Computer science
05 Combinatorics	39 Difference and functional equations	70 Mechanics of particles and systems
06 Order, lattices, ordered algebraic structures	40 Sequences, series, summability	74 Mechanics of deformable solids
08 General algebraic systems	41 Approximation and expansions	76 Fluid mechanics
11 Number theory	42 Harmonic analysis on Euclidean spaces	78 Optics, electromagnetic theory
12 Field theory and polynomials	43 Abstract harmonic analysis	80 Classical thermodynamics, heat transfer
13 Commutative algebra	44 Integral transforms, operational calculus	81 Quantum Theory
14 Algebraic geometry	45 Integral equations	82 Statistical mechanics, structure of matter
15 Linear and multilinear algebra; matrix theory	46 Functional analysis	83 Relativity and gravitational theory
16 Associative rings and algebras	47 Operator theory	85 Astronomy and astrophysics
17 Nonassociative rings and algebras	49 Calculus of variations and optimal control; optimization	86 Geophysics
18 Category theory, homological algebra	51 Geometry	90 Operations research, mathematical programming
19 K-theory	52 Convex and discrete geometry	91 Game theory, economics, social and behavioral sciences
20 Group theory and generalizations	53 Differential geometry	92 Biology and other natural sciences
22 Topological groups, Lie groups	54 General topology	93 Systems theory; control
26 Real functions	55 Algebraic topology	94 Information and communication, circuits
28 Measure and integration	57 Manifolds and cell complexes	97 Mathematics education
30 Functions of a complex variable	58 Global analysis, analysis on manifolds	
31 Potential theory	60 Probability theory and stochastic processes	
32 Several complex variables and analytic spaces		
33 Special functions		

- 14B99 None of the above, but in this section
- 14Cxx Cycles and subschemes**
- 14C05 Parametrization (Chow and Hilbert schemes)
- 14C15 (Equivariant) Chow groups and rings; motives
- 14C17 Intersection theory, characteristic classes, intersection multiplicities [See also 13H15]
- 14C20 Divisors, linear systems, invertible sheaves
- 14C21 Pencils, nets, webs [See also 53A60]
- 14C22 Picard groups
- 14C25 Algebraic cycles
- 14C30 Transcendental methods, Hodge theory [See also 14D07, 32G20, 32J25, 32S35], Hodge conjecture
- 14C34 Torelli problem [See also 32G20]
- 14C35 Applications of methods of algebraic K -theory [See also 19Exx]
- 14C40 Riemann-Roch theorems [See also 19E20, 19L10]
- 14C99 None of the above, but in this section
- 14Dxx Families, fibrations**
- 14D05 Structure of families (Picard-Lefschetz, monodromy, etc.)
- 14D06 Fibrations, degenerations
- 14D07 Variation of Hodge structures [See also 32G20]
- 14D10 Arithmetic ground fields (finite, local, global)
- 14D15 Formal methods; deformations [See also 13D10, 14B07, 32Gxx]
- 14D20 Algebraic moduli problems, moduli of vector bundles {For analytic moduli problems, see 32G13}
- 14D21 Applications of vector bundles and moduli spaces in mathematical physics (twistor theory, instantons, quantum field theory) [See also 32L25, 81Txx]
- 14D22 Fine and coarse moduli spaces
- 14D23 Stacks and moduli problems
- 14D24 Geometric Langlands program: algebro-geometric aspects [See also 22E57]
- 14D99 None of the above, but in this section
- 14Exx Birational geometry**
- 14E05 Rational and birational maps
- 14E07 Birational automorphisms, Cremona group and generalizations
- 14E08 Rationality questions [See also 14M20]
- 14E15 Global theory and resolution of singularities [See also 14B05, 32S20, 32S45]
- 14E16 McKay correspondence
- 14E18 Arcs and motivic integration
- 14E20 Coverings [See also 14H30]
- 14E22 Ramification problems [See also 11S15]
- 14E25 Embeddings
- 14E30 Minimal model program (Mori theory, extremal rays)
- 14E99 None of the above, but in this section
- 14Fxx (Co)homology theory [See also 13Dxx]**
- 14F05 Sheaves, derived categories of sheaves and related constructions [See also 14H60, 14J60, 18F20, 32Lxx, 46M20]
- 14F10 Differentials and other special sheaves; D -modules; Bernstein-Sato ideals and polynomials [See also 13Nxx, 32C38]
- 14F17 Vanishing theorems [See also 32L20]
- 14F18 Multiplier ideals
- 14F20 Étale and other Grothendieck topologies and (co)homologies
- 14F22 Brauer groups of schemes [See also 12G05, 16K50]
- 14F25 Classical real and complex (co)homology
- 14F30 p -adic cohomology, crystalline cohomology
- 14F35 Homotopy theory; fundamental groups [See also 14H30]
- 14F40 de Rham cohomology [See also 14C30, 32C35, 32L10]
- 14F42 Motivic cohomology; motivic homotopy theory [See also 19E15]
- 14F43 Other algebro-geometric (co)homologies (e.g., intersection, equivariant, Lawson, Deligne (co)homologies)
- 14G99 None of the above, but in this section
- 14Hxx Curves**
- 14H05 Algebraic functions; function fields [See also 11R58]
- 14H10 Families, moduli (algebraic)
- 14H15 Families, moduli (analytic) [See also 30F10, 32G15]
- 14H20 Singularities, local rings [See also 13Hxx, 14B05]
- 14H25 Arithmetic ground fields [See also 11Dxx, 11G05, 14Gxx]
- 14H30 Coverings, fundamental group [See also 14E20, 14F35]
- 14H37 Automorphisms
- 14H40 Jacobians, Prym varieties [See also 32G20]
- 14H42 Theta functions; Schottky problem [See also 14K25, 32G20]
- 14H45 Special curves and curves of low genus
- 14H50 Plane and space curves
- 14H51 Special divisors (gonality, Brill-Noether theory)
- 14H52 Elliptic curves [See also 11G05, 11G07, 14Kxx]
- 14H55 Riemann surfaces; Weierstrass points; gap sequences [See also 30Fxx]
- 14H57 Dessins d'enfants theory {For arithmetic aspects, see 11G32}
- 14H60 Vector bundles on curves and their moduli [See also 14D20, 14F05]
- 14H70 Relationships with integrable systems
- 14H81 Relationships with physics
- 14H99 None of the above, but in this section
- 14Jxx Surfaces and higher-dimensional varieties {For analytic theory, see 32Jxx}**
- 14J10 Families, moduli, classification: algebraic theory
- 14J15 Moduli, classification: analytic theory; relations with modular forms [See also 32G13]
- 14J17 Singularities [See also 14B05, 14E15]
- 14J20 Arithmetic ground fields [See also 11Dxx, 11G25, 11G35, 14Gxx]
- 14J25 Special surfaces {For Hilbert modular surfaces, see 14G35}
- 14J26 Rational and ruled surfaces
- 14J27 Elliptic surfaces
- 14J28 $K3$ surfaces and Enriques surfaces
- 14J29 Surfaces of general type
- 14J30 3-folds [See also 32Q25]
- 14J32 Calabi-Yau manifolds
- 14J33 Mirror symmetry [See also 11G42, 53D37]
- 14J35 4-folds
- 14J40 n -folds ($n > 4$)
- 14J45 Fano varieties
- 14J50 Automorphisms of surfaces and higher-dimensional varieties
- 14J60 Vector bundles on surfaces and higher-dimensional varieties, and their moduli [See also 14D20, 14F05, 32Lxx]
- 14J70 Hypersurfaces
- 14J80 Topology of surfaces (Donaldson polynomials, Seiberg-Witten invariants)
- 14J81 Relationships with physics
- 14J99 None of the above, but in this section
- 14Kxx Abelian varieties and schemes**
- 14K02 Isogeny
- 14K05 Algebraic theory
- 14K10 Algebraic moduli, classification [See also 11G15]
- 14K12 Subvarieties
- 14K15 Arithmetic ground fields [See also 11Dxx, 11Fxx, 11G10, 14Gxx]
- 14K20 Analytic theory; abelian integrals and differentials
- 14K22 Complex multiplication [See also 11G15]
- 14K25 Theta functions [See also 14H42]
- 14K30 Picard schemes, higher Jacobians [See also 14H40, 32G20]
- 14K99 None of the above, but in this section
- 14Lxx Algebraic groups {For linear algebraic groups, see 20Gxx; for Lie algebras, see 17B45}**
- 14L05 Formal groups, p -divisible groups [See also 55N22]

https://en.wikipedia.org/wiki/Normal

Search

What is normal in math?

There are many unrelated notions of "normality" in mathematics.

Algebra and number theory [\[edit source \]](#)

- [Normal basis](#) (of a Galois extension), used heavily in cryptography
- [Normal degree](#), a rational curve on a surface that meets certain conditions
- Normal domain ([integrally closed domain](#)), a ring integrally closed in its fraction field
 - [Normal ring](#), a reduced ring whose localizations at prime ideals are integrally closed domains
 - [Normal scheme](#), an algebraic variety or scheme that meets certain conditions
- [Normal extensions](#) (or quasi-Galois) field extensions, splitting fields for a set of polynomials over the base field
- Normal variety, a projective variety embedded by a complete linear system, as in a [rational normal scroll](#) (unrelated to the concept of normal scheme above)
- [Normal order of an arithmetic function](#), a type of asymptotic behavior useful in number theory
- [Normal subgroup](#), a subgroup invariant under conjugation

Analysis [\[edit source \]](#)

- [Normal family](#), a pre-compact family of continuous functions
- [Normal number](#), a real number with a "uniform" distribution of digits
- [Normal number \(computing\)](#), a floating-point number within the balanced range supported by a given format (unrelated to the previous notion)
- [Normal operator](#), an operator that commutes with its Hermitian adjoint
 - [Normal matrix](#), a complex square matrix that meets certain conditions
- [Normal modes](#) of vibration in an oscillating system

Geometry [\[edit source \]](#)

- [Normal \(geometry\)](#), a vector perpendicular to a surface (normal vector)
- [Normal bundle](#), a term related to the preceding concept
- [Normal cone](#), of a subscheme in algebraic geometry
- [Normal coordinates](#), in differential geometry, local coordinates obtained from the exponential map (Riemannian geometry)
- [Normal invariants](#), in geometric topology
- [Normal polytopes](#), in polyhedral geometry and computational commutative algebra
- [Normal space](#) (or T_4) spaces, topological spaces characterized by separation of closed sets

Logic and foundations [\[edit source \]](#)

- [Normal function](#), in set theory
- [Normal measure](#), in set theory

Mathematical physics [\[edit source \]](#)

- [Normal order](#) or Wick order in Quantum Field Theory

Probability and statistics [\[edit source \]](#)

- [Normal](#), the middle 95% of a bell curve (see [1.96](#))
- [Normal distribution](#), the Gaussian continuous probability distribution

Other mathematics [\[edit source \]](#)

- [Normal form \(disambiguation\)](#)
- [Normalization \(disambiguation\)](#)

What is a group?

Definitions of group (algebra)

- A group is a set with a binary operation, identity element, and inverse operation, satisfying axioms of associativity, inverse, and identity.
- A group object in a category. A group in the first sense is a group object in the category of sets. A Lie group is a group object in the category of smooth manifolds. A topological group is a group object in the category of topological spaces. An affine group scheme is a group object in the category of affine schemes. (Caution: the Zariski product topology is not the product topology.)
- A Poisson-Lie group a group object in the category of Poisson manifolds, except that the inverse operation is not required to be a morphism of Poisson manifolds. (In

What is a group?

general, the inverse is an anti-Poisson morphism.)

- A quantum group is an object in the opposite category to the category of Hopf algebras.
- A compact matrix quantum group is a C^* -algebra with additional structure (Woronowicz).
- A strict 2-group is a group object in the category of categories (or a category object in the category of groups).
- A 2-group ...
- An n -group ...

Sign Manifesto

Pierre Deligne and Daniel S. Freed

§1. Standard mathematical conventions

- *We apply the sign rule relentlessly.*

§2. Choices

- *A hermitian inner product on a complex vector space V is conjugate linear in the first variable:*

$$(3) \quad \langle \lambda_1 v_1, \lambda_2 v_2 \rangle = \overline{\lambda_1} \lambda_2 \langle v_1, v_2 \rangle, \quad \lambda_i \in \mathbb{C}, \quad v_i \in V.$$

- *If $V = V^0 \oplus V^1$ is a super Hilbert space, then*

$$(4) \quad -i\langle v, v \rangle \geq 0, \quad v \in V^1.$$

§7. Miscellaneous signs

- *Let X be a smooth manifold, ξ a vector field on X , φ_t the one-parameter group of diffeomorphisms generated, and T a tensor field. Then*

$$(39) \quad \text{Lie}(\xi)T = \left. \frac{d}{dt} \right|_{t=0} \varphi_t^* T = \left. \frac{d}{dt} \right|_{t=0} (\varphi_{-t})_* T.$$

Hartshorne (Residues and Duality): “And since the chore of inventing these diagrams and checking their commutativity is almost mechanical, the reader would not want to read them, nor I write them.”

“the reader [of Hartshorne] is left with checking lots and lots of commutative diagrams, some of them depending on very subtle sign conventions in homological algebra!”

Math Words

- rng = ring without i
- lluf subcategory = full backwards
- clopen = closed and open, bananaman = Banach analytic manifold,
- bra and ket (from bracket), parahori = parabola + Iwahori,
- ichthyomorphisms = transformations between Poisson manifolds
- pointless topology, killing fields, abstract nonsense
- alfalfa (derived from alpha by the Iowa school of representation theory)
- the unknot (a circle) was coined during 7-ups uncola advertising campaign.
- Conwayisms: nimber, moonshine, baby monster
- buildings (apartment, chamber, wall, etc.), tree (forest, leaf, root, etc.), quivers (arrows).
- cepstrum (spectrum) in quefrency analysis
- Pin is to O, what Spin is to SO.
- iff, xor, wlog, nth,
- snark, quark, fluxion, gerbe, totient, heteroscedasticity, anabelian, zenzizenzenzic, Nullstellensatz, Entscheidungsproblem

Sylvester, "On a theory of Syzygetic Relations"

allotrious, apocapated, Bezoutic, Bezoutoid, co-bezoutiant, cogredient, contragredient, combinant, concomitant, conjunctive, contravariant, covariant, cumulant, determinant, dialytic, discriminant, disjunctive, effluent, emanant, endoscopic, exoscopic, Hessian, hyperdeterminant, inertia, intercalation, invariance, invariant, Jacobian, kenotheme, **matrix**, minor determinant, monotheme, persymmetrical, quadrinvariant, resultant, rhizoristic, signaletic, semaphoretic, substitution, syrrhizoristic, syzygetic, transform, umbral.

VOCABULARY OF THE KEPLER CONJECTURE

- quoin, negligible, fcc-compatible, decomposition star, score, score adjustment, quasi-regular tetrahedron, contravening, tame graph, pentahedral prism, crown, quarter, upright, flat, quartered octahedron, strict quarter, enclosed vertex, central vertex, corners, isolated quarter, isolated pair, conflicting diagonals, Q-system, S-system, V-cells, barrier, obstructed, face with negative orientation, Delaunay star, colored spaces, compression, quad cluster, mixed quad cluster, standard cluster, standard region, vertex type, quad cluster, Rogers simplex, anchor, anchored simplex, erasing, loops, subcluster, corner cell, truncated corner cell, tame graph, weight assignment, contravening circuit, crowded diagonal, n-crowded, masked, confined, penalties, penalty-free score, exceptional region, special simplex, distinguished edge, nonexternal edge, concave corner, concave vertex, t-cone, partial plane graph, patch, aggregated face,

VOCABUARY OF IUT1/ABC (MOCHIZUKI)

- inter-universal Teichmuller theory, semi-graphs of anabelioids, Frobenioids, etale theta function, log-shells, log-theta-lattices, log-link, log-volume, initial Theta-data, Hodge theaters, absolute anabelian geometry, absolute anabelian reconstruction, tempered fundamental group, prime-strips, local arithmetic holomorphic structure, mono-analyticizations, mono-analytic core, global realified Frobenioid, labels, label crushing, conjugate synchronization, Frobenioid-theoretic theta function, full poly-isomorphisms, multiradiality, alien ring structures, alien arithmetic holomorphic structure, cyclotomic rigidity isomorphism, real analytic container, mono-analytic container, Theta-link, Theta-dilation, Belyi cuspidalization, topological pseudo-monoid, capsule of objects, capsule indices, connected temperoid, commensurably terminal, co-holomorphicization, base-NF-bridges, poly-action, cyclotomes, coric structure, Kummer black-out, Kummer-blind, solvable factorization, dismantling, functorial dynamics, holomorphic procession, entangled structures, indigenous bundle

Trott's MathOverflow data

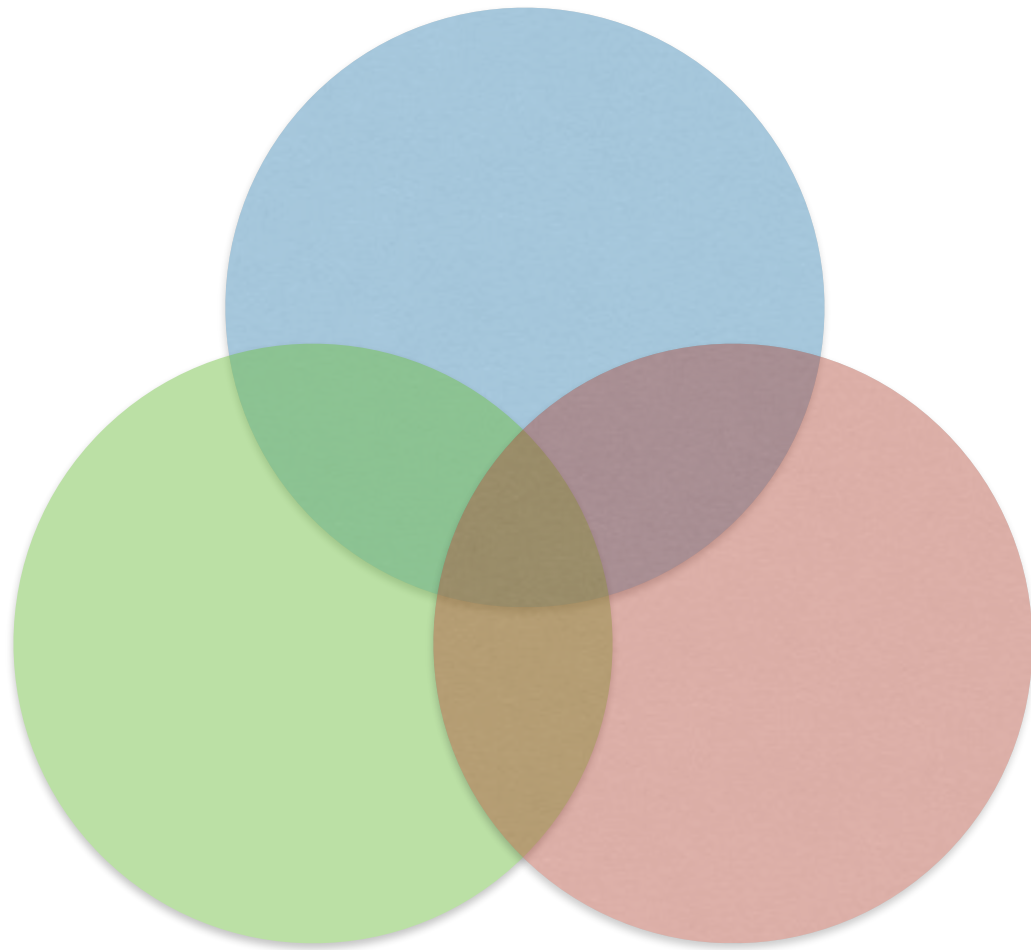
- 1 Chinese remainder theorem
- 2 prime number theorem
- 3 central limit theorem
- 4 Fermat's Last theorem
- 5 Hahn-Banach theorem
- 6 Atiyah-Singer index theorem
- 7 implicit function theorem
- 8 Riemann-Roch theorem
- 9 spectral theorem
- 10 Riemann mapping theorem
- 11 Riesz representation theorem
- 12 Gauss-Bonnet theorem
- 13 Dirichlet's theorem
- 14 Jordan curve theorem
- 15 incompleteness theorem
- 16 Liouville's theorem
- 17 Fubini's theorem
- 18 Brouwer fixed point theorem
- 19 universal coefficient theorem
- 20 intermediate value theorem
- 21 Whitehead theorem
- 22 mean value theorem
- 23 uniformization theorem
- 24 Ramsey's theorem
- 25 Peter-Weyl theorem
- 26 inverse function theorem
- 27 Baire category theorem
- 28 Mordell-Weil theorem
- 29 Frobenius theorem
- 30 Stokes theorem
- 31 Pythagorean theorem
- 32 Cayley-Hamilton theorem
- 33 Perron-Frobenius theorem
- 34 Birkhoff ergodic theorem
- 35 Main theorem
- 36 Lefschetz fixed point theorem
- 37 Bertini's theorem
- 38 Hodge theorem
- 39 Sylow theorem
- 40 fundamental theorem of algebra
- 41 Stone-Weierstrass theorem
- 42 Roth's theorem
- 43 Second Incompleteness theorem
- 44 Riemann Existence theorem
- 45 Cauchy's theorem
- 46 residue theorem
- 47 Torelli theorem
- 48 dominated convergence theorem
- 49 Chevalley's theorem
- 50 open mapping theorem
- 51 Sobolev embedding theorem
- 52 fundamental theorem of calculus
- 53 Tychonoff's theorem
- 54 Taylor's theorem
- 55 Tarski's theorem
- 56 comparison theorem

- 57 Recursion theorem
- 58 Radon-Nikodym
- 59 Value theorem
- 60 theorem
- 61 Whitney embedding theorem
- 62 Lowenheim-Skolem theorem
- 63 Minkowski's theorem
- 64 Vanishing theorem
- 65 van Kampen theorem
- 66 Cayley's theorem
- 67 Noether's theorem
- 68 Rolle's theorem
- 69 Lebesgue density theorem
- 70 Kodaira vanishing theorem
- 71 Weierstrass approximation theorem
- 72 Hall's marriage theorem
- 73 MRDP theorem
- 74 Krull-Schmidt theorem
- 75 Wilson's theorem
- 76 Whitney extension theorem
- 77 Whitney's theorem
- 78 Tauberian theorem
- 79 Weyl's theorem
- 80 Schwartz kernel theorem
- 81 Rice's theorem
- 82 Weil's theorem
- 83 Thue-Siegel-Roth theorem
- 84 Hodge decomposition theorem
- 85 Their theorem
- 86 Wedderburn's theorem
- 87 Stone representation theorem
- 88 Unit theorem
- 89 Turan's theorem
- 90 Yau's theorem
- 91 Tate's theorem
- 92 Mean Value theorem
- 93 Chinese Remainder theorem
- 94 binomial theorem
- 95 intermediate value theorem
- 96 Pythagorean theorem
- 97 Value theorem
- 98 residue theorem
- 99 squeeze theorem
- 100 dominated convergence theorem
- 101 Fermat's little theorem
- 102 fundamental theorem of calculus
- 103 Central Limit theorem
- 104 Lagrange's theorem
- 105 Fubini's theorem
- 106 implicit function theorem
- 107 first isomorphism theorem
- 108 Cauchy's theorem
- 109 Sylow theorem
- 110 inverse function theorem
- 111 rank-nullity theorem
- 112 spectral theorem

- 113 Rolle's theorem
- 117 Cayley-Hamilton theorem
- 118 prime number theorem
- 119 Liouville's theorem
- 120 Fermat's Last theorem
- 121 Green's theorem
- 122 open mapping theorem
- 123 Monotone Convergence theorem
- 124 Heine-Borel theorem
- 125 Cauchy's integral theorem
- 126 fundamental theorem of algebra
- 127 rational root theorem
- 128 Bolzano-Weierstrass theorem
- 129 Stokes theorem
- 130 Master theorem
- 131 identity theorem
- 132 Bayes theorem
- 133 Banach fixed point theorem
- 134 fundamental theorem of arithmetic
- 135 Baire category theorem
- 136 isomorphism theorem
- 137 Dirichlet's theorem
- 138 Stone-Weierstrass theorem
- 139 Riemann mapping theorem
- 140 Pythagoras theorem
- 141 Factor theorem
- 142 Wilson's theorem
- 143 Jordan curve theorem
- 144 Fermat's theorem
- 145 Weierstrass theorem
- 146 Weierstrass approximation theorem
- 147 closed graph theorem
- 148 Cantor's theorem
- 149 orbit-stabilizer theorem
- 150 Radon-Nikodym theorem
- 151 Tonelli's theorem
- 152 convolution theorem
- 153 incompleteness theorem
- 154 fundamental theorem of calculus.
- 155 universal coefficient theorem
- 156 Arzela-Ascoli theorem
- 157 uniqueness theorem
- 158 Picard's theorem
- 159 Sandwich theorem
- 160 Tychonoff's theorem
- 161 correspondence theorem
- 162 Bezout's theorem
- 163 Remainder theorem
- 164 Rouché's theorem
- 165 Cantor-Bernstein theorem
- 166 Tietze extension theorem
- 167 multinomial theorem
- 168 Kanpen theorem

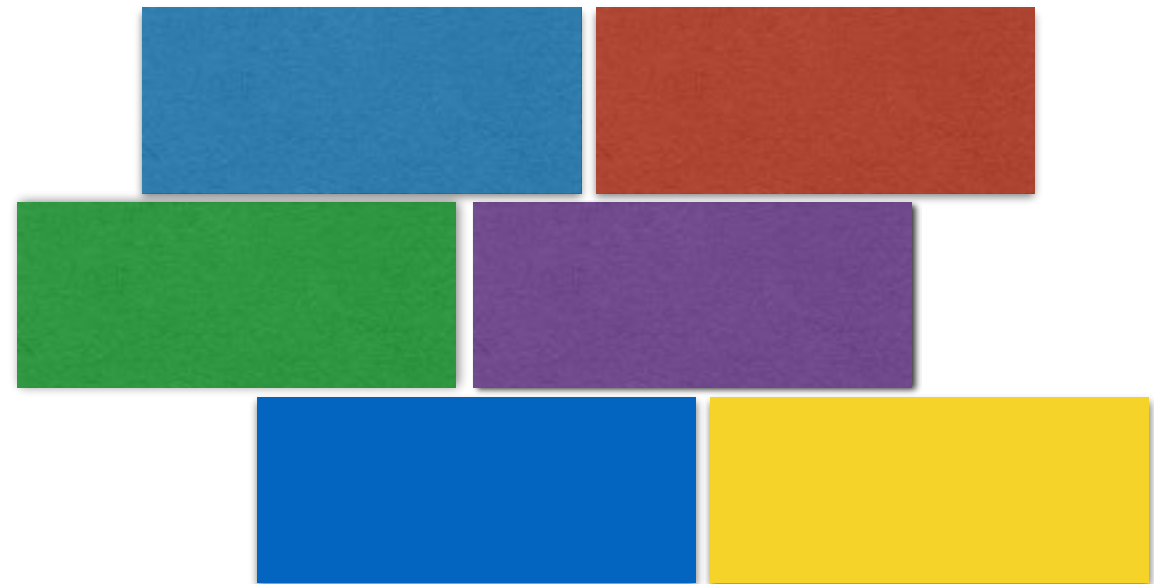
Two responses to Russell's paradox

Set Theory (Zermelo)



Sets mix.

Type Theory (Russell)



Types never mix.



HOL Light

HOL Light has an exquisite minimal design. It has the smallest kernel of any system. John Harrison is the sole



Mizar

Once the clear front-runner, it now shows signs of age. Do not expect to understand the inner workings of this system unless you have been



Coq

Coq is built of modular components on a foundation of dependent type theory. This system has grown one PhD thesis at a time.



Isabelle

Designed for use with multiple foundational architectures, Isabelle's early development featured classical constructions in set theory. However,



Metamath

Does this really work? Defying expectations, Metamath seems to function shockingly well for those who are happy to live without plumbing.



Lean

Lean is ambitious, and it will be massive. Do not be fooled by the name. "*Construction area keep out*" signs are prominently posted on the perimeter fencing.



Lean Theorem Prover

- Lean has a small kernel.
- Its logical foundations are similar to those of Coq.
- Lean is its own metalanguage.

What is great about LEAN?

- Lean sounds wonderful: **open source**, a small trusted kernel, a powerful elaboration engine including a Prolog-like algorithm for type-class resolution, **multi-core support**, incremental compilation, support for both constructive and classical mathematics, successful projects in homotopy type theory, excellent documentation, and a **web browser interface**.
- In more detail, a “**minimalist and high performance kernel**” was an explicit goal of the Lean. Independent implementations of the kernel can have been given (Selsam 2000 lines, etc.) alleviating any concerns about a bug in the C++ implementation of Lean.
- The **semantics of Lean** are now completely spelled out (thanks to Mario Carneiro, building on [Werner]). In particular, Carneiro has built a model of Lean’s logic (CiC with non-cumulative universes) in ZFC set theory (augmented by a countable number of inaccessible cardinals).
- Lean has a **clean syntax**. For example, to add two elements in an abelian group, one can simply write $x+y$ and Lean correctly infers the group in which the addition is to be performed. I have more to say about Lean’s syntax later.
- Lean makes it easy to switch from constructive to **classical logic** (you just open the classical logic module). Lean makes quotient types easy (unlike Coq, which tends to work with awkward setoids).
- **Lean is its own meta language**. I find this very appealing. Contrast this with HOL-Light, which has OCaml as meta-language or Coq which has a domain-specific language Ltac for tactics.
- Finally, there was a personal reason. **CMU is the center of Lean library development**. I live in Pittsburgh and am a regular participant in CMU’s Lean group meetings.

Example. ZF set theory can be embedded into Lean. The construction is due to Aczel and Benjamin Werner and the implementation in Lean was done by Mario Carneiro. It can be done with a single constructor.

$$\text{im} : \Pi(A : \text{Type}), (A \rightarrow \text{Set}) \rightarrow \text{Set}$$

Interpret $\text{im } A f$ as the image of $f : A \rightarrow \text{Set}$ on A . So ZFC sets in Lean consist of all images of functions into sets.

Equality is defined recursively: $\text{im } A f$ is equal to $\text{im } B g$ if for every $a : A$ there exists a $b : B$ such that $f(a)$ and $g(b)$ are equal, and vice versa.

What is terrible about LEAN?

- The kernel is **bloated**. Specifically, from what I hear, for performance reasons, mutually inductive types will soon be moved into the kernel. This bloats the kernel and kills the former claims of a minimalistic kernel.
- Lean is **not backwards compatible**. Lean 3 broke the Lean 2 libraries, and old libraries still haven't been ported to Lean 3. After nearly 2 years, it doesn't look like that will ever happen. Instead new libraries are being built (at great cost). Lean 4 is guaranteed to break the Lean 3 libraries (at what cost?). In short, Lean is experimental, evolving, and unstable.
- The learning curve is steep. It is **very hard to learn** to use Lean proficiently. Are you a graduate student at Stanford or CMU writing a thesis on Lean? Are you a student at Imperial being guided by Kevin Buzzard? If not, Lean might not be for you.
- Lean is its own metalanguage. Lean is new, and the language **libraries are almost non-existent**. 10 million programmers know Java. Hardly any major programs have been written in Lean (Lewis's thesis is a notable exception). **It is impossible to do any serious programming** in Lean.
- **Typing is nominal** rather than structural.
- There are **performance issues**. It is not clear (to me or perhaps even to anyone) why performance is such a big problem, because Lean was implemented in C++ for the sake of performance. However in fact, the compilation of the math libraries is currently very slow. Something is wrong here.
- **Ugly projection chains** are required.
- **Structure depends on notation**. Lean has a library of results about multiplicative groups and a separate library of results about additive groups. The only difference is that one uses the symbol $*$ for the group operation and the other uses the symbol $+$ for the group operation. Mathematician will find it absurd that the theorems in group theory depend on the symbol used for composition.
- **No diamonds are allowed**. (For a review of diamonds in OOP, see https://en.wikipedia.org/wiki/Multiple_inheritance.)
- **Structures are meaninglessly parameterized** from a mathematical perspective. To briefly introduce the topic of parameters and bundling, users choose whether data appears as an external parameter.
- **Lean discards valuable information** that is later reconstructed (at a cost) by its type class resolution engine.

The answer to LEAN's woes: a “Cabarete mode” for Lean

- Structural typing. Long projection chains are avoided. Diamonds are allowed.
- Structures are bundled rather than parametrized.
- Inheritance is eliminated and replaced with go-lang style embeddings and record subtyping.
- OCaml-style destructive substitution.

Here is a fragment of the formal abstract for the statement of the Riemann hypothesis. The full formal abstract will include links to each of the definitions (such as the specification of the field of complex numbers):

```
def holomorphic_on (domain : set ℂ) (f : subtype domain → ℂ) :=
  (∀ z : subtype domain, ∃ f'z,
  has_complex_derivative_at (extend_by_zero domain f) f'z z)

class holomorphic_function :=
  (domain : set ℂ)
  (f : subtype domain → ℂ)
  (open_domain : is_open domain)
  (has_derivative : holomorphic_on domain f)

-- notation f(z), for holomorphic functions
instance : has_coe_to_fun holomorphic_function :=
{ F := λ h, subtype h.domain → ℂ, coe := λ h, h.f }

-- converges for Re(s) > 1
def riemann_zeta_sum (s : ℂ) : ℂ :=
Σ (λ n, complex.pow n (-s) )

-- trivial zeros at -2, -4, -6,...
def riemann_zeta_trivial_zero (s : ℂ) : Prop :=
(∃ n : ℕ, n > 0 ∧ s = (-2)*n)

-- analytic continuation of Riemann zeta function.
axiom riemann_zeta_exists :
(∃! ζ : holomorphic_function, ζ.domain = (set.univ \ {1}) ∧
∀ s : subtype ζ.domain, re(s) > 1 → ζ(s) = riemann_zeta_sum s)

def ζ := classical.some riemann_zeta_exists

-- (s ≠ 1) implicit in the domain constraints:
def riemann_hypothesis :=
(∀ s, ζ(s) = 0 ∧ ¬(riemann_zeta_trivial_zero s) →
re (s) = 1/2)
```

Which mathematical definitions should be formalised in Lean?

Ask Question



The question.

90

Which mathematical objects would you like to see formally defined in the [Lean Theorem Prover](#)?



Examples.



53

In the current stable version of the Lean Theorem Prover, topological groups have been done, schemes have been done, Noetherian rings got done last month, Noetherian schemes have not yet been done (but are probably not going to be too difficult, if anyone is interested in trying), but complex manifolds have not yet been done. In fact I think we are nearer to perfectoid spaces than complex manifolds – maybe because algebra is closer to the axioms than analysis. But actually we also have Lebesgue measure (it's differentiability we're not too strong at), and today we got modular forms. There is a sort of an indication of where we are.

asked 3 months ago

viewed 8,986 times

active 2 months ago

BLOG



[Adios to Winter Bash 2018](#)

Linked

36

[On proof-verification using Coq](#)

LIST OF FINITE SIMPLE GROUPS

1. BACKGROUND

This article assumes basic facts about K -algebras (such as tensor products, ideals, radical ideals), topological spaces (connectedness), and category theory.

Building on those foundations, the article gives a complete specification of all finite simple groups. The definition of a finite simple group of Lie type appears in Definition 3. Unexplained notation from this section will be precisely defined later.

Theorem 1. *Every finite simple group is isomorphic to*

- (1) *a cyclic group of prime order,*
- (2) *an alternating group Alt_n on n letters for some $n \geq 5$,*
- (3) *a finite simple group of Lie type, or*
- (4) *one of the 26 sporadic groups.*

Every group these four families is a finite simple group.

Finite simple groups of Lie type are classified by certain data of the form (D_r, ρ, p, e) (written as ${}^\rho D_r(p^e)$), where D_r is a connected Dynkin diagram with r nodes, ρ is an arrow-forgetful isomorphism of the Dynkin diagram, p is a prime number, and $e \in \mathbb{Q}$ is an exponent. The explicit list of such tuples appears in Definition 1.

What is a group?

Definitions of group (algebra)

- A group is a set with a binary operation, identity element, and inverse operation, satisfying axioms of associativity, inverse, and identity.
- A group object in a category. A group in the first sense is a group object in the category of sets. A Lie group is a group object in the category of smooth manifolds. A topological group is a group object in the category of topological spaces. An affine group scheme is a group object in the category of affine schemes. (Caution: the Zariski product topology is not the product topology.)
- A Poisson-Lie group a group object in the category of Poisson manifolds, except that the inverse operation is not required to be a morphism of Poisson manifolds. (In

CLASSIFICATION OF FSG

GROUP OBJECTS - CATEGORIFICATION ALGORITHM

25 lines (18 sloc) | 980 Bytes

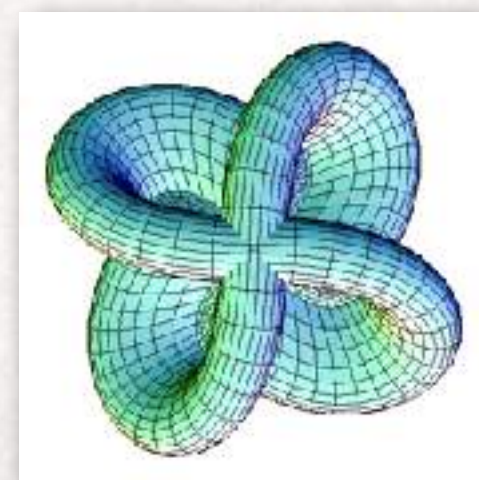
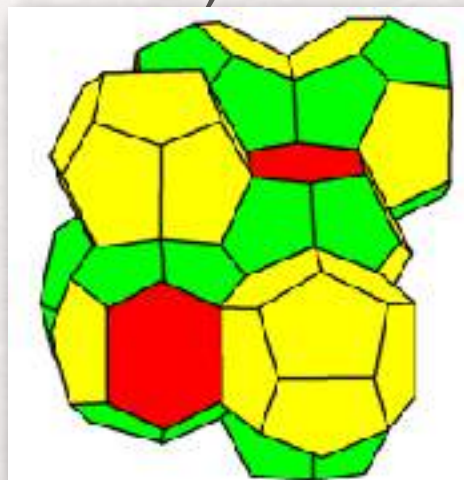
Raw Blame History

```
1  -- Copyright (c) 2019 Jesse Han. All rights reserved.
2  -- Released under Apache 2.0 license as described in the file LICENSE.
3  -- Authors: Jesse Han
4
5  import .finite_limits
6
7  open category_theory category_theory.limits category_theory.limits.binary_product
8      category_theory.limits.finite_limits
9
10 universes u v
11
12 local infix `×`:50 := binary_product
13
14 local infix `×.map`:60 := binary_product.map
15
16 structure group_object (C : Type u) [ℳ : category.{v u} C] [H : has_binary_products C] [H' : has_limits_of_shape
17 (G : C)
18 (mul : G × G → G)
19 (mul_assoc : (by exact reassoc_hom G) » (by apply (1 _) ×.map mul) » mul = (by apply mul ×.map (1 _) ) » mul)
20 (one : term → G)
21 (one_mul : (1 G) = one_mul_inv _ » (by apply one ×.map (1 G)) » mul)
22 (mul_one : (1 G) = mul_one_inv _ » (by apply (1 G) ×.map one) » mul)
23 (inv : G → G)
24 (mul_left_inv : (1 G) = [map_to_product.mk (inv) (1 G)] » mul )
```

$\text{categorify}(\lambda x \ y \ z, x * y * z = (x * y) * z)$

FRUITFUL DIRECTIONS

- Mathematical formalizations are fun!
- Jesse Han and Floris van Doorn have formalized in Lean the unprovability of the continuum hypothesis from the axioms of Zermelo-Fraenkel choice. (The first problem on Hilbert's list of mathematical problems.)
- Tool-building is fun!
- Mathematics is fun! Let's state the Kelvin problem. Let's state Smale's paradox (sphere eversions). Let's state the classification of finite simple groups.



QUESTIONS?