Formalisation, arithmetization and automatisation of geometry

Julien Narboux

University of Strasbourg

ADG 2023, Belgrade

Claims

- Everybody make mistakes.
- Even mathematicians
- Even **excellent** mathematicians
- We can use computers to help checking proofs.

Errors/Gaps in mathematics

Incomplete proofs:

The Elements. The first construction assumes the existence of the intersection of two given circles.

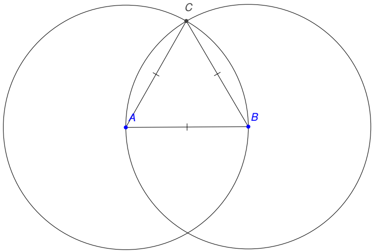
Die Grundlagen der Geometrie. Some non trivial proofs are presented as obvious in early editions.

One example

Proposition (Book I, Prop. 1)

Let A and B two points, build an equilateral triangle on AB.

Proof: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ the circles of center A and B and of radius AB.
Let C the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$.
The distance AB is congruent to AC and AB is congruent to BC.
Hence ABC is equilateral.



Gaps in the Elements

Problem

Euclids postulates do not allow to ensure that C exists.

- Hilbert proposed an axiomatic system to fill the gaps in Euclid, the proofs are not the same.
- Avigad, Dean and Mumma have proposed an alternative formal system to justify the original proofs [1].

[1] Jeremy Avigad, Edward Dean, and John Mumma (2009). "A Formal System for Euclid's Elements". In: The Review of Symbolic Logic 2

Many incorrect proofs of Euclid's fifth postulate:

In 1763, in his thesis Klügel provides a list of 30 incorrect proofs.

- Ptolemée admits the uniqueness of parallels.
- Proclus admits that given two parallel lines, each line which intersect one intersect the other.
- Legendre has published several incorrect 'proofs' in its 'best-seller' "Éléments de géométrie".
- ...

Triangle Postulate

$$\widehat{A} + \widehat{B} + \widehat{C} = 180^\circ$$

Adrien-Marie Legendre

(caricature

Julien Léopold Boilly)

Triangle Postulate

“Il n’en est pas moins certain que le théorème sur la somme des trois angles du triangle doit être regardé comme l’une de ces vérités fondamentales qu’il est impossible de contester [...].”

Adrien-Marie Legendre

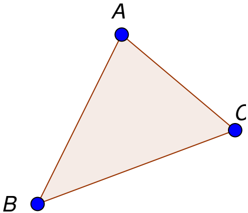
(caricature

Julien Léopold Boilly)

Table des matières

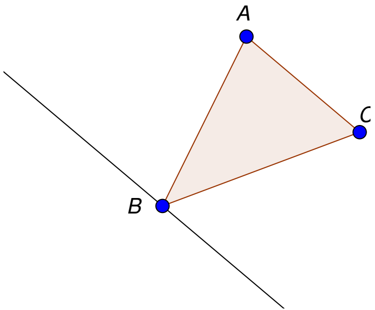
The sum of angles of a triangle

Let l be a line parallel to AC through B.



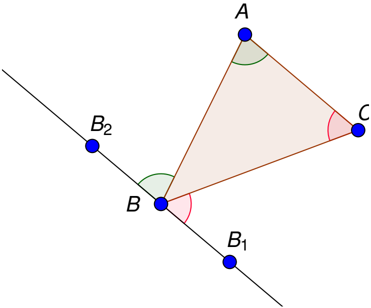
The sum of angles of a triangle

Let l be a line parallel to AC through B.



The sum of angles of a triangle

Let l be a line parallel to AC through B.

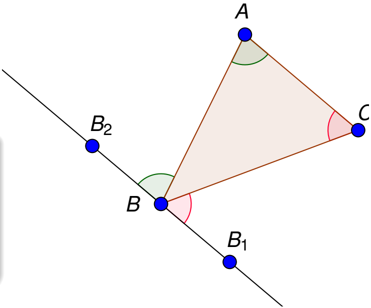


The sum of angles of a triangle

Let l be a line parallel to AC through B.

Problem !

One has to prove (or admit) that the angles are really alternate angles.



Outline

Foundations of geometry

1. Synthetic geometry
2. Analytic geometry
3. Metric geometry
4. Transformations based approaches

Synthetic approach

Assume some undefined geometric objects + geometric predicates + axioms ...
The name of the assumed types are not important.

- Hilbert's axioms:

  types: points, lines and planes
  predicates: incidence, between, congruence of segments, congruence of angles

- Tarski's axioms:

  types: points
  prédicats: between, congruence

- ...many variants

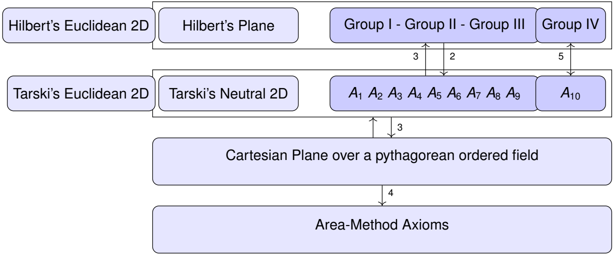
Example of books using a synthetic approach:

- Euclide (1998). Les Éléments. *Les Éléments*
- David Hilbert (1899). Grundlagen der Geometrie. *Grundlagen der Geometrie*
- Borsuk and Szmielew: *Foundations of Geometry*
- Robin Hartshorne (2000). Geometry : Euclid and beyond. Undergraduate texts in mathematics *Geometry: Euclid and Beyond*
- Marvin J. Greenberg (1993). Euclidean and Non-Euclidean Geometries - Development and Histor *Euclidean and non-euclidean Geometries, Development and History*
- Specht *et. al.*: *Euclidean Geometry and its Subgeometries*

Analytic approach

We assume we have numbers (a field $\mathbb{F}$).
We define geometric objects by their coordinates.
Points := $\mathbb{F}^n$

Overview of the axiom systems



---

[2] Gabriel Braun, Pierre Boutry, and Julien Narboux (June 2016). "From Hilbert to Tarski". In: Eleventh International Workshop on Automated Deduction in Geometry. Proceedings of ADG 2016

[3] Gabriel Braun and Julien Narboux (Sept. 2012). "From Tarski to Hilbert". English. In: Post-proceedings of Automated Deduction in Geometry 2012. Vol. 7993. LNCS

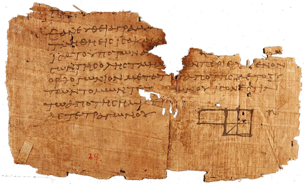
[4] Pierre Boutry, Gabriel Braun, and Julien Narboux (2019). "Formalization of the Arithmetization of Euclidean Plane Geometry and Applications". In: Journal of Symbolic Computation 98

[5] Pierre Boutry et al. (2017). "Parallel postulates and continuity axioms: a mechanized study in intuitionistic logic using Coq". In: Journal of Automated Reasoning

Outline

The Elements

- A very influential mathematical book (more than 1000 editions).
- First known example of an axiomatic approach.



Book 2, Prop V, Papyrus d'Oxyrhynchus (year 100)

Euclid

First project

- Joint work with Charly Gries and Gabriel Braun
- Mechanizing proofs of Euclid's **statements**
- Not Euclid's proofs!
- Trying to minimize the assumptions:
  - Parallel postulate
  - Elementary continuity
  - Archimedes' axiom

Second project

- Joint work with Michael Beeson and Freek Wiedijk [6]
- Formalizing Euclid's **proofs**
- A not minimal axiom system
- Filling the gaps in Euclid

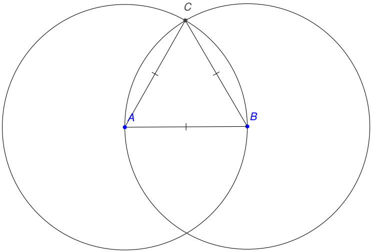
[6] Michael Beeson, Julien Narboux, and Freek Wiedijk (2019). "Proof-checking Euclid". In: Annals of Mathematics and Artificial Intelligence 85.2-4

Example

Proposition (Book I, Prop 1)

Let A and B be two points, build an equilateral triangle on the base AB.

Proof: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ the circles of center A and B and radius AB. Take C at the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$. The distance AB is congruent to AC, and AB is congruent to BC. Hence, ABC is an equilateral triangle.

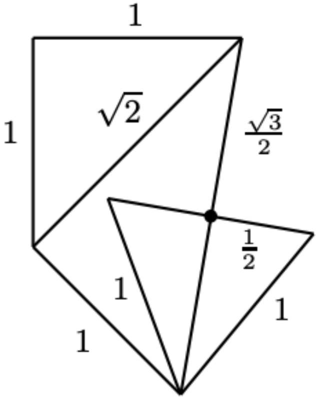


Book I, Prop 1

In the spirit of *reverse mathematics*, we proved two statements:

1. Assuming no continuity, but the parallel postulate (solving a challenge proposed by Beeson)[7].
2. Assuming circle/circle continuity, but not the parallel postulate (trivial).

Pambuccian has shown that these assumptions are minimal.



[7] Michael Beeson (2013). "Proof and Computation in Geometry". In: Automated Deduction in Geometry (ADG 2012). Vol. 7993. Springer Lecture Notes in Artificial Intelligence

```
Section Book_1_prop_1_euclidean.
Context `{TE:Tarski_2D_euclidean}.

Lemma prop_1_euclidean :
 forall A B,
  exists C, Cong A B A C /\ Cong A B B C.
Proof. ... Qed.

End Book_1_prop_1_euclidean.
```

```
Section Book_1_prop_1_circle_circle.
Context `{TE:Tarski_2D}.

Lemma prop_1_circle_circle :
circle_circle_bis ->
 forall A B,
  exists C, Cong A B A C /\ Cong A B B C.
Proof.
intros.
unfold circle_circle_bis in H.
destruct (H A B B A A B) as [C [HC1 HC2]];Circle.
exists C.
unfold OnCircle in *.
split;Cong.
Qed.

End Book_1_prop_1_circle_circle.
```

Outline

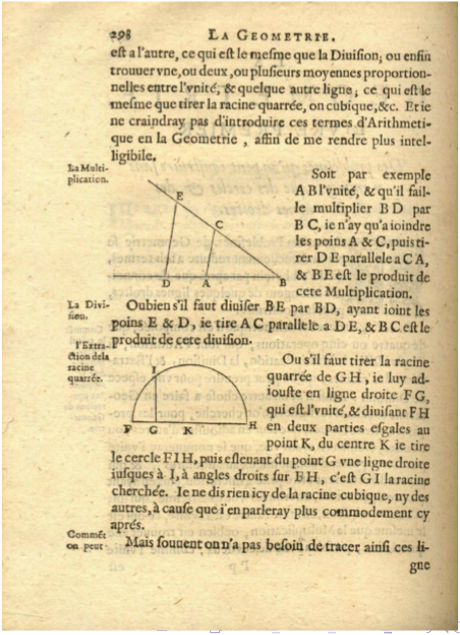
1. Why checking proof mechanically ?

2. Formalization of foundations of geometry
   - Foundations
   - Two formalizations of the Elements
   - Arithmetization of Geometry
   - Continuity axioms
   - 34 parallel postulates

3. The parallel postulate: a syntactic proof of independence

Arithmetization of Geometry

René Descartes (1925).
La géométrie.



eſt a l'autre, ce qui eſt le meſme que la Diuiſion; ou enfin trouuer vne, ou deux, ou pluſieurs moyennes proportionnelles entre l'vnité, & quelque autre ligne; ce qui eſt le meſme que tirer la racine quarrée, ou cubique, &c. Et ie ne craindray pas d'introduire ces termes d'Arithmetique en la Geometrie, affin de me rendre plus intelligibile.

La Multiplication.

Soit par exemple A B l'vnité, & qu'il faille multiplier B D par B C, ie n'ay qu'a ioindre les poins A & C, puis tirer D E parallele a C A, & B E eſt le produit de cete Multiplication.

La Diuiſion.

Oubien s'il faut diuiſer B E par B D, ayant ioint les poins E & D, ie tire A C parallele a D E, & B C eſt le produit de cete diuiſion.

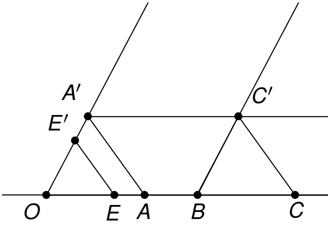
l'Extraction de la racine quarrée.

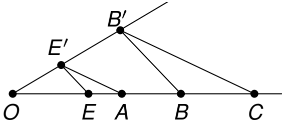
Ou s'il faut tirer la racine quarrée de G H, ie luy adiouſte en ligne droite F G, qui eſt l'vnité, & diuiſant F H en deux parties eſgales au point K, du centre K ie tire le cercle F I H, puis eſleuant du point G vne ligne droite iuſques à I, à angles droits ſur F H, c'eſt G I la racine cherchée. Ie ne dis rien icy de la racine cubique, ny des autres, à cauſe que i'en parleray plus commodement cy aprés.

Commét on peut

Mais ſouuent on n'a pas beſoin de tracer ainſi ces ligne

Addition and multiplication





Automation

This is not a theorem about polynoms:

```
Lemma centroid_theorem : forall A B C A1 B1 C1 G,
  Midpoint A1 B C ->
  Midpoint B1 A C ->
  Midpoint C1 A B ->
  Col A A1 G ->
  Col B B1 G ->
  Col C C1 G \/ Col A B C.
Proof.
intros A B C A1 B1 C1 G; convert_to_algebra; decompose_coordinates.
intros; spliter. express_disj_as_a_single_poly; nsatz.
Qed.
```

Hilbert's line completeness

Axiom V.2: "An extension (An extended line from a line that already exists, usually used in geometry) of a set of points on a line with its order and congruence relations that would preserve the relations existing among the original elements as well as the fundamental properties of line order and congruence that follows from Axioms I-III and from V-1 is impossible."

> *Hilbert's own completeness axiom, added in other editions as V-2, takes the somewhat awkward form of requiring that it be impossible to properly extend the sets and relations satisfying the other axioms so that all the other axioms still hold.*
>
> – Martin 1998, p. 175

Formalization in Coq

We need to quantify over models of other axioms[8] :

```
Definition completeness_for_planes := forall
  (Tm: Tarski_neutral_dimensionless)
  (Tm2 : Tarski_neutral_dimensionless_with_decidable_p
  (M : Tarski_2D Tm2)
  (f : @Tpoint Tn -> @Tpoint Tm),
 @archimedes_axiom Tm ->
 extension f ->
 forall A, exists B, f B = A.
```

[8] Charly Gries, Julien Narboux, and Pierre Boutry (Jan. 2019). "Axiomes de continuité en géométrie neutre : une étude mécanisée en Coq". In: Journées Francophones des Langages Applicatifs 2019. Acte des Journées Francophones des Langages Applicatifs (JFLA 2019)

Algebra/Geometry

Continuity	Axiom
	ordered Pythagorean field[9]
circle/line continuity	ordered Euclidean field [10]
FO Dedekind cuts	real closed field [11]
Dedekind	reals

[9] the sum of squares is a square

[10] positive are square

[11] F is euclidean and every polynomial of odd degree has at least one root in F.

Outline

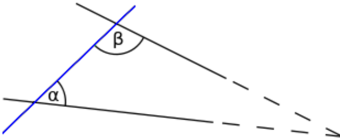
1. Why checking proof mechanically ?

2. Formalization of foundations of geometry
   - Foundations
   - Two formalizations of the Elements
   - Arithmetization of Geometry
   - Continuity axioms
   - 34 parallel postulates

3. The parallel postulate: a syntactic proof of independence

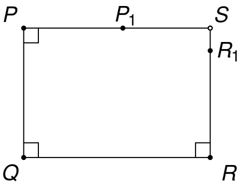
Euclid 5th postulate

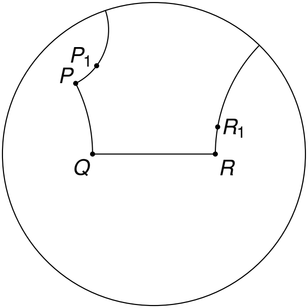
"If two lines are drawn which intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough."



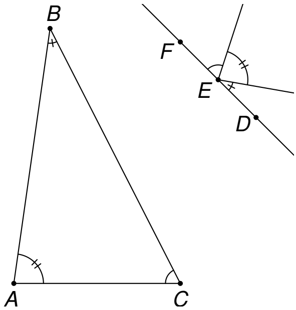
Bachmann's Lotschnittaxiom

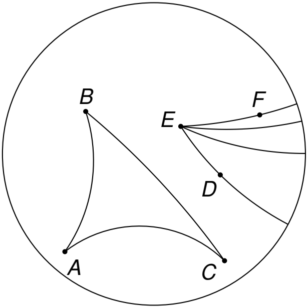
If $p \perp q$, $q \perp r$ and $r \perp s$ then p and s meet.



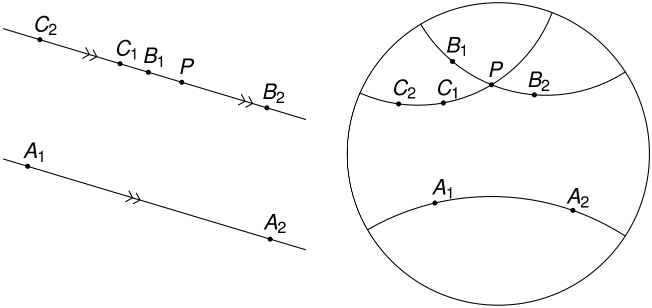


Triangle postulate

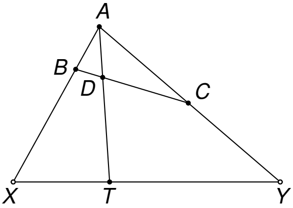


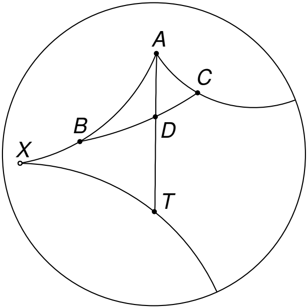


Playfair's postulate

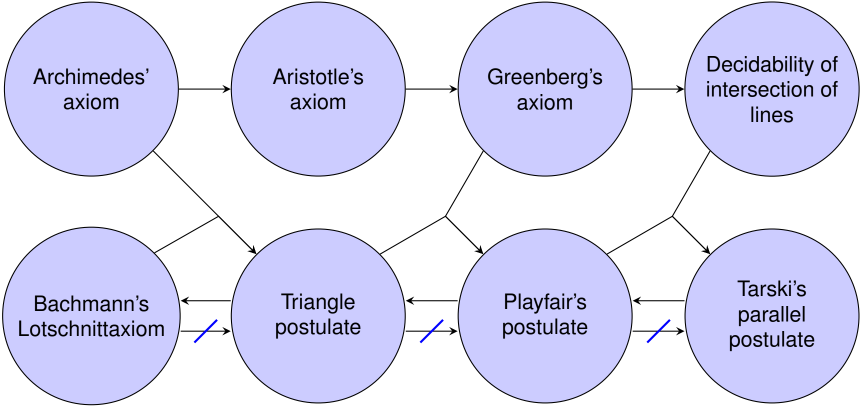


Tarski's postulate



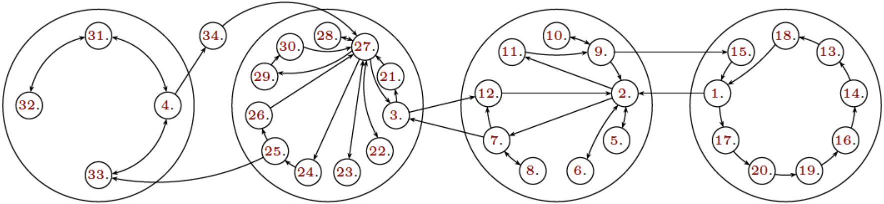


Four groups



Archimedes' axiom
Aristotle's axiom
Greenberg's axiom
Decidability of intersection of lines
Bachmann's Lotschnittaxiom
Triangle postulate
Playfair's postulate
Tarski's parallel postulate

Sorting 34 postulates



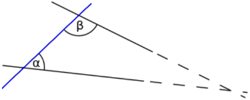
[12]

[12] Pierre Boutry et al. (2017). "Parallel postulates and continuity axioms: a mechanized study in intuitionistic logic using Coq". In: Journal of Automated Reasoning

Outline

This part of the talk:
Herbrand's theorem and non-Euclidean geometry
Michael Beeson, Pierre Boutry, Julien Narboux
Bulletin of Symbolic Logic, Association for Symbolic Logic, 2015, 21 (2), pp.12.
`https://hal.inria.fr/hal-01071431v3`

If a line segment intersects two straight lines forming two interior angles on the same side that sum to less than two right angles, then the two lines, if extended indefinitely, meet on that side on which the angles sum to less than two right angles.



A long history

From antiquity, mathematicians felt that Euclid 5th was less “obviously true” than the other axioms, and they attempted to derive it from the other axioms. Many false “proofs” were discovered and published.

Examples:

- Ptolemy assumes implicitly Playfair axioms (uniqueness of parallel).
- Proclus assumes implicitly “If a line intersects one of two parallel lines, both of which are coplanar with the original line, then it must intersect the other also.”
- Legendre published several incorrect proofs of Euclid 5 in his best-seller “Éléments de géométrie”.

Outline

About independence

We want to show that the parallel postulate is independent of the other axioms:

Theorem

The parallel postulate is not a theorem.

About independence

We want to show that the parallel postulate is independent of the other axioms:

Meta-Theorem

The parallel postulate is not a theorem.

A toy example

Example

The language :

One predicate : R (arity 2)
One constant : $\blacksquare$
One function symbol : μ (arity 1)

One axiom : $R(\blacksquare, \blacksquare)$

One rule : $\forall x, R(x, x) \Rightarrow R(\mu(x), \mu(x))$

Question

Is $R(\mu(\mu(\blacksquare)), \mu(\blacksquare))$ a theorem ?

Answer 1 (syntactic proof)

No, because :

1. It is not an axiom.
2. We cannot apply the rule.

Answer 2 (semantic proof)

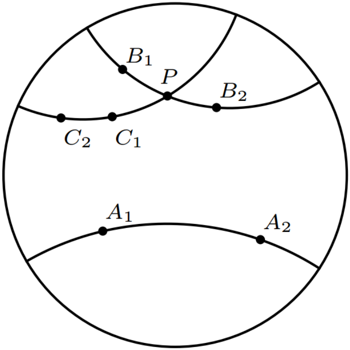
No, because if you interpret:

- R by the equality $=$
- $\blacksquare$ by the integer 0
- μ by the function $x \mapsto x + 1$

It holds that $0 = 0$ and $\forall x, x = x \Rightarrow x + 1 = x + 1$ but we don't have $2 = 1$.

Semantic proofs of the independence of Euclid's 5th postulate

Using Poincaré disk model: straight lines consist of all segments of circles contained within that disk that are orthogonal to the boundary of the disk, plus all diameters of the disk.



Outline

Tarski's axioms

- 11 axioms
- two predicates ($\beta\ A\,B\,C$, $AB \equiv CD$)
- no definition inside the axiom system

Part 1

Six axioms without existential quantification:

Congruence Pseudo-Transitivity $AB \equiv CD \wedge AB \equiv EF \Rightarrow CD \equiv EF$

Congruence Symmetry $AB \equiv BA$

Congruence Identity $AB \equiv CC \Rightarrow A = B$

Between identity $\beta\, A\, B\, A \Rightarrow A = B$

Five segments $\begin{array}{l} AB \equiv A'B' \wedge BC \equiv B'C' \wedge \\ AD \equiv A'D' \wedge BD \equiv B'D' \wedge \\ \beta\, A\, B\, C \wedge \beta\, A'\, B'\, C' \wedge A \neq B \Rightarrow CD \equiv C'D' \end{array}$:

Side-Angle-Side expressed without angles.

Upper dimension

$$P \neq Q \wedge AP \equiv AQ \wedge BP \equiv BQ \wedge CP \equiv CQ \Rightarrow Col\ ABC$$

Part 2

Five axioms with existential quantification:

1. Lower dimension
2. Segment construction
3. Pasch
4. Parallel postulate
5. Continuity: Dedekind cuts or line-circle continuity

Lower Dimension

$$\exists ABC, \neg Col(A, B, C)$$

Segment construction axiom

$$\exists E, \beta\ A\,B\,E \wedge BE \equiv CD$$

Pasch's axiom

Allows to formalize some gaps in Euclid's Elements.
We have the inner form :

$$\beta\ A\,P\,C \wedge \beta\ B\,Q\,C \Rightarrow \exists X, \beta\ P\,X\,B \wedge \beta\ Q\,X\,A$$

Moritz Pasch
(1843-1930)

Parallel postulate

$$\exists XY, \beta\ A\ D\ T \wedge \beta\ B\ D\ C \wedge A \neq D \Rightarrow \beta\ A\ B\ X \wedge \beta\ A\ C\ Y \wedge \beta\ X\ T\ Y$$

- This statement is equivalent to Euclid 5th postulate.
- Comes from an incorrect proof of Euclid 5th by Legendre.

Adrien-Marie Legendre (1752-1833) (watercolor caricature by Julien Léopold Boilly)

Main idea

Study the maximum distance between the points in the axioms with existential quantification:

- **Lower dim** Initial Constant.
- **Inner Pasch** The distance is conserved.
- **Segment Construction** The distance is at most doubled.
- **Line Circle Continuity** The distance at most doubled.
- **Euclid** We can build points arbitrarily far.

The proof

- Skolemize the axiom system: replace existential quantification with function symbols.
- Apply Herbrand's theorem.

Herbrand's theorem

Herbrand's theorem says that under some assumptions (the theory is first-order and does not contain existential symbols), if the theory proves an existential theorem $\exists y\, \phi(a, y)$, with ϕ quantifier-free, then there exist finitely many terms $t_1, \ldots, t_n$ such that the theory proves

$$\phi(a, t_1(a)) \vee \phi(a, t_2(a)) \ldots \vee \ldots \phi(a, t_n(a)).$$

Example in geometry

Dropping or erecting a perpendicular.

Conclusions

- GeoCoq is the only formalization of geometry that goes up to the arithmetization and connects to automation using algebraic methods.
- While formalizing old results about geometry with a new tool (the proof assistant), we learned that:
  - Using constructive logic we get a finer classification of parallel postulates.
  - This inspired a new syntactic proof of the independence of the parallel postulate.

Thank you for you attention.