Vers l'utilisation d'un assistant de preuve en classe ?

Julien Narboux

Unité de formation et de recherche
de **mathématique** et d'**informatique**
Université de Strasbourg

Décembre 2018, IREM Strasbourg

Les ordinateurs en maths

Les logiciels sont utilisés en classe pour

1. du calcul numérique
2. du calcul symbolique (Maple...)
3. produire des conjectures (géométrie dynamique)
4. exercices de construction (Euclidea, GeoGebra...,)
5. pour vérifier des conjectures par des méthodes probabilistes ou algébriques (Cabri, GeoGebra, ...)

Mais

l'utilisation d'un logiciel pour construire des démonstrations n'est pas répandue !

Rapport Villani/Torossian

Rééquilibrer les séances d'enseignement de mathématiques : redonner leur place

- au cours structuré et à sa trace écrite ;
- **à la notion de preuve ;**
- aux apprentissages explicites.

Vocabulaire ensembliste et logique L'apprentissage des notations mathématiques et de la **logique ne doit pas faire l'objet de séquences spécifiques** mais prend naturellement sa place dans tous les chapitres du programme. Les élèves doivent connaître les notions d'élément d'un ensemble, de sous-ensemble, d'appartenance et d'inclusion, de réunion, [...] Pour ce qui concerne le raisonnement logique, les élèves rencontrent via des exemples :

- les connecteurs logiques « et », « ou » ;
- les quantificateurs universel et existentiel (les symboles $\forall$ et $\exists$ sont hors programme) ;
- des implications et équivalences logiques ;
- la réciproque d'une implication ;
- l'utilisation d'un contre-exemple pour infirmer une proposition universelle ;
- des raisonnements par disjonction des cas, des raisonnements par l'absurde. Ils distinguent le statut des égalités (identité, équation) et celui des lettres utilisées (variable, indéterminée, inconnue, paramètre).

Qu'est-ce qu'une preuve ?

1. un argument convainquant

Qu'est-ce qu'une preuve ?

1. un argument convainquant
2. une suite de déductions à partir des axiomes

Qu'est-ce qu'une preuve ?

1. un argument convainquant
2. une suite de déductions à partir des axiomes
3. un algorithme (correspondance de Curry-Howard)

Point de vue

On peut voir une preuve informelle comme un argument pour convaincre le lecteur de l'existence d'une preuve formelle.

"Du point de vue épistémologique, les considérations précédentes montrent qu'il suffit de savoir transcrire une démonstration mathématique en déduction naturelle dans le système de Quine pour être assuré de ***l'existence d'une transcription formalisée*** *dans le cadre théorique du calcul des prédicats. Autrement dit, la distance entre démonstration pratique et démonstration formalisée n'est peut-être pas aussi infranchissable qu'on l'affirme parfois." dans MÉTHODES DE RAISONNEMENT ET LEURS MODÉLISATIONS LOGIQUES. SPÉCIFICITÉ DE L'ANALYSE. QUELLES IMPLICATIONS DIDACTIQUES ? Viviane Durand-Guerrier, Gilbert Arsac, volume 23-3, 2003 Recherches en didactique des mathématiques.*

Heureusement !

Par définition vérifier qu'une preuve est correcte est un problème décidable.

Heureusement !

Par définition vérifier qu'une preuve est correcte est un problème décidable.

On peut donc construire des assistants de preuve!

Exemples

- Automath (1967)
- Coq (1984)
- HOL-Light (90s)
- HOL (1988)
- Isabelle (1986)
- Lean (2013)
- Matita (1999)
- Mizar (1973)
- ...

Qu'est-ce qu'un assistant de preuve ?

Un logiciel qui permet de :

- définir des notions mathématiques et/ou des programmes
- démontrer mécaniquement des théorèmes mathématiques mettant en jeu ces définitions

Qu'est-ce qu'un assistant de preuve ?

Un logiciel qui permet de :

- définir des notions mathématiques et/ou des programmes
- démontrer mécaniquement des théorèmes mathématiques mettant en jeu ces définitions

Qu'est-ce que ce n'est pas ?

- Un démonstrateur automatique
- Un outil qui facilite l'obtention des preuves

Les langages pour décrire les preuves

Impérative On donne des ordres (appelés tactiques) pour compléter l'arbre de preuve qui est en construction (LCF Style)

Déclarative On décrit les assertions mathématiques que l'on veut déduire et une justification.

L'enseignement de la démonstration

- Apprentissage par imitation (preuve correcte = bonne note/enseignant d'accord).
- Seulement certaines règles de raisonnement sont données: absurde, contraposée, raisonnement par cas.
- Assez peu d'enseignants en Maths connaissent des rudiments de logique.
- Des vérifications sémantiques sont utilisées plutôt que syntaxiques (voir les travaux de Viviane Durand-Guerrier).

”If you can’t explain mathematics to a machine, it is an illusion to think you can explain it to a student.” De Bruijn ”Invited lecture at the Mathematics Knowledge Management Symposium”, 25-29 November 2003, Heriot-Watt University, Edinburgh, Scotland

Objectifs potentiels

- Enseigner ce qu'est une preuve
- Enseigner la logique
- Enseigner les fondements du logiciels
- Pour automatiser la vérification des démonstrations
- Pour enseigner les maths en général
- Pour offrir un retour à l'élève en général

Objectifs potentiels

- Enseigner ce qu'est une preuve
- Enseigner la logique
- Enseigner les fondements du logiciels
- Pour automatiser la vérification des démonstrations
- ~~Pour enseigner les maths en général~~
- ~~Pour offrir un retour à l'élève en général~~

Je ne propose pas de construire un tuteur, simplement un vérificateur de démonstrations.

Preuve interactive, pourquoi ?

- Clarifier les règles du jeu: les règles de déduction sont explicites.
- Clarifier le langage: axiome, théorème, lemme, hypothèses, définition, conjecture, contre-exemple...
- Critère objectif de la validité d'une démonstration.
- Inter-activité: boucle d'interaction pendant le travail à la maison.
- Motivation: preuve de théorèmes comme un jeu.

Défis

- Trouver le bon langage/une bonne interface utilisateur.
- Construire les bibliothèques.
- Automatiser ce qui doit l'être et pas plus (et cela dépend du contexte).

Sur le langage, les règles de déduction, l'interface

Je souhaite des règles de déduction qui sont:

- correctes
- explicites
- complètes
- pas nécessairement minimales
- pas trop éloignées de la pratique mathématique

Logique cohérente

$$\forall x, H_1(x) \wedge \ldots \wedge H_n(x) \rightarrow \quad \exists y, P_1(x,y) \wedge \ldots P_k(x,y) \vee \ldots$$

Plusieurs auteurs ont identifié ce fragment de la logique du premier ordre.
Ce fragment permet d'avoir des preuves relativement lisibles [1].

[1] Sana Stojanović et al. (2014). "A Vernacular for Coherent Logic". English. In: Intelligent Computer Mathematics. Vol. 8543. Lecture Notes in Computer Science

Outils existants

Deux communautés:

1. Didactique des maths
2. Preuve interactive

Communauté didactique des maths

Geometry Tutor [2], MENTONIEZH [3], DEFI [4], CHYPRE [5], Geometrix [6], Cabri Euclide [7], Baghera [8], AgentGeom, geogebraTUTOR and Turing [9]

---

[2] John R. Anderson, C. F. Boyle, and Gregg Yost (1985). "The geometry Tutor". In: IJCAI Proceedings

[3] Dominique Py (1990). "Reconnaissance de plan pour l'aide à la démonstration dans un tuteur intelligent de la géométrie". PhD thesis. Université de Rennes

[4] Ag-Almouloud (1992). "L'ordinateur, outil d'aide à l'apprentissage de la démonstration et de traitement de données didactiques". PhD thesis. Université de Rennes

[5] Philippe Bernat (1993). CHYPRE: Un logiciel d'aide au raisonnement. Tech. rep. 10. IREM

[6] Jacques Gressier (1988). Geometrix.

[7] Vanda Luengo (1997). "Cabri-Euclide: Un micromonde de Preuve intégrant la réfutation". PhD thesis. Université Joseph Fourier

[8] Nicolas Balacheff et al. (1999). Baghera.

[9] Philippe R. Richard et al. (2011). "Didactic and theoretical-based perspectives in the experimental development of an intelligent tutorial system for the learning of geometry". en. In: ZDM 43.3

Communauté de la preuve interactive

Informatique

- logique
- preuve de programmes, sémantique, fondements du logiciel

U-Penn, Portland, Princeton, Harvard, Warsaw, CNAM, Lyon, Nice, Paris, Strasbourg, ...

Maths

- Licence - Logique: Bordeaux, Warsaw, Pohang, Strasbourg, ...
- Licence - Maths: Nijmegen (ProofWeb), Nice (CoqWeb), ...
- ...

Deux catégories de logiciels:

1. Du sucre syntaxique au dessus d'assistant preuve complexe
   - PCoq [10]
   - Coq Web [11]
   - ProofWeb [12]
   - Edukera [13]
2. Langue pseudo naturelle + déduction automatique

[10] Ahmed Amerkad et al. (2001). "Mathematics and Proof Presentation in Pcoq". In: Workshop Proof Transformation and Presentation and Proof Complexities in connection w

[11] Jérémy Blanc et al. (2007). "Proofs for freshmen with Coqweb". In: PATE'07

[12] CS Kaliszyk et al. (2008). "Deduction using the ProofWeb system". In:

[13] Benoit Rognier and Guillaume Duhamel (2016). "Présentation de la plateforme edukera". In: Vingt-septièmes Journées Francophones des Langages Applicatifs (JFLA 2016)

Deux catégories de logiciels:

1. Du sucre syntaxique au dessus d'assistant preuve complexe
2. Langue pseudo naturelle + déduction automatique
   - SAD [10]
   - Naproche [11]
   - Lurch [12]
   - ELFE [13]
   - CalcCheck [14]
   - Mendes' system [15]

[10] Alexander Lyaletski, Andrey Paskevich, and Konstantin Verchinine (2006). "SAD as a mathematical assistant—how should we go from here to there?". In: Journal of Applied Logic. Towards Computer Aided Mathematics 4.4

[11] Marcos Cramer et al. (2010). "The Naproche Project Controlled Natural Language Proof Checking of Mathematical Texts". In: Controlled Natural Language

[12] Nathan C. Carter and Kenneth G. Monks. "Lurch: a word processor built on OpenMath that can check mathematical reasoning". In:

[13] Maximilian Doré (2018). "The ELFE Prover". In: 25th Automated Reasoning Workshop

[14] Wolfram Kahl (2018). "CalcCheck: A Proof Checker for Teaching the "Logical Approach to Discrete Math"". en. In: Interactive Theorem Proving. Lecture Notes in Computer Science

[15] Alexandra Mendes and João F. Ferreira (2018). "Towards Verified Handwritten

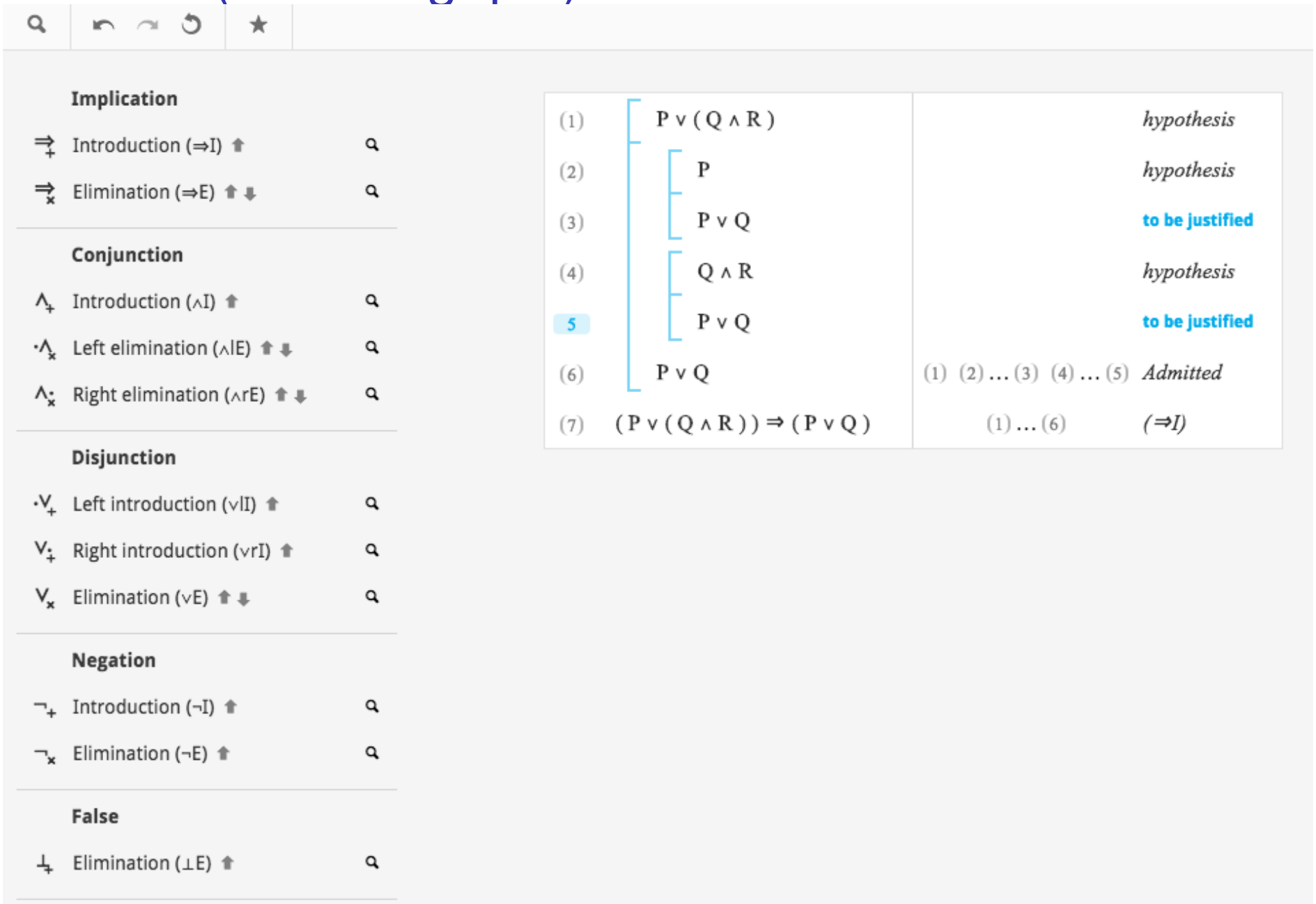
Edukera (Rognier and Duhamel)

- Application Web
- Coq est caché dans la page web
- Interaction sous forme d'ordres + affichage de la démonstration.
- Quelques utilisateurs en France (environ 1000 étudiants, 70k exercices)
- Pas de langage textuel: "preuve par cliques", correction syntaxique par construction (comme Scratch)
- Facile à apprendre à l'aide d'un tuto
- Les applications de règles logiques sont toujours correctes
- Les théorèmes utilisés le sont toujours correctement
- Meta-variables pour gérer les variables du raisonnement

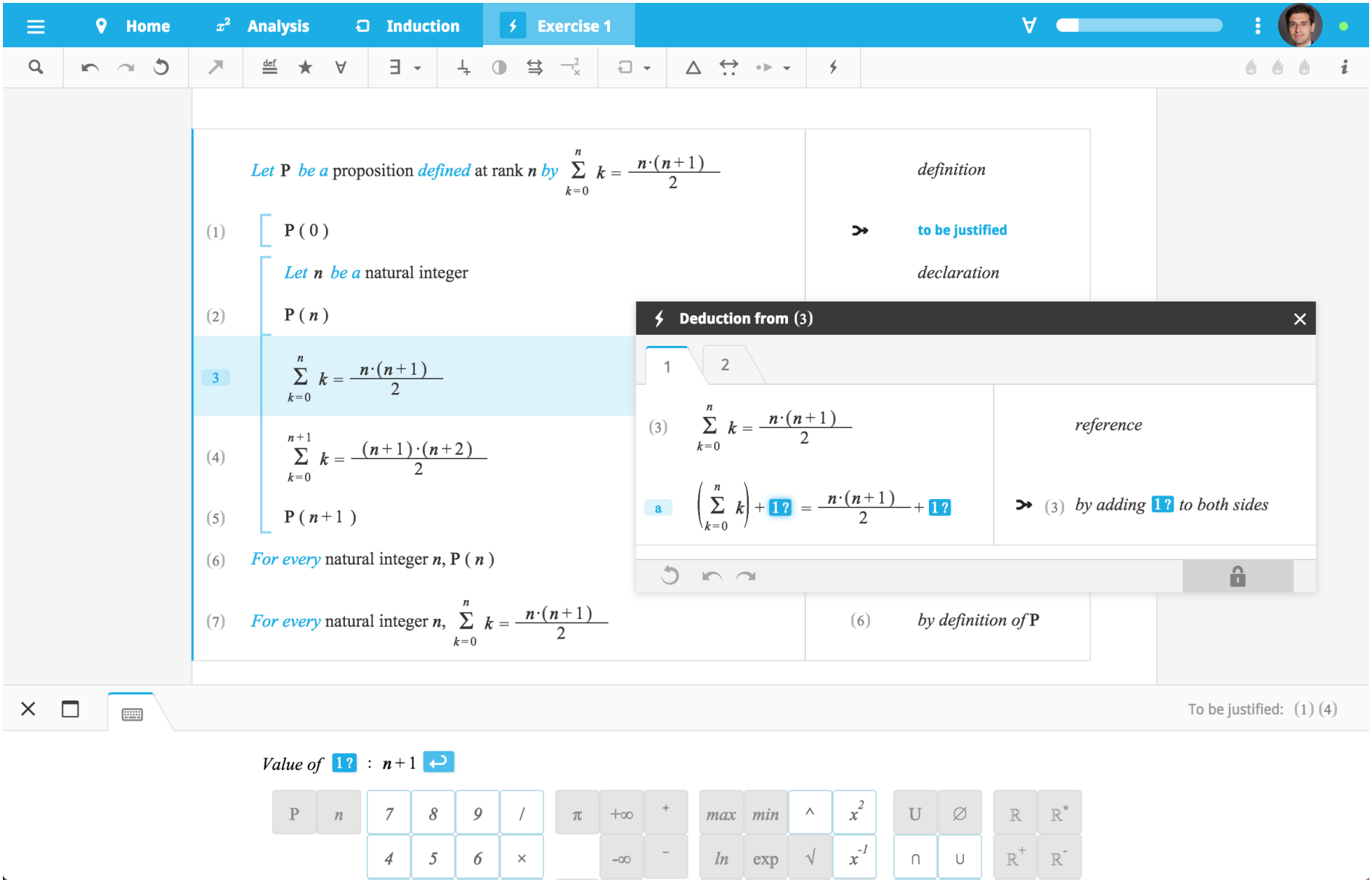
Deux modes

1. Logique
   - Règles de la déduction naturelle.
   - Affichage de l'arbre de preuve possible (style Fitch ou Gentzen).
   - Raisonnement par chaînage arrière (on part de la conclusion).
2. Maths
   - Raisonnement par chaînage avant/arrière.
   - Étapes de preuve à grain plus gros qu'en mode logique.

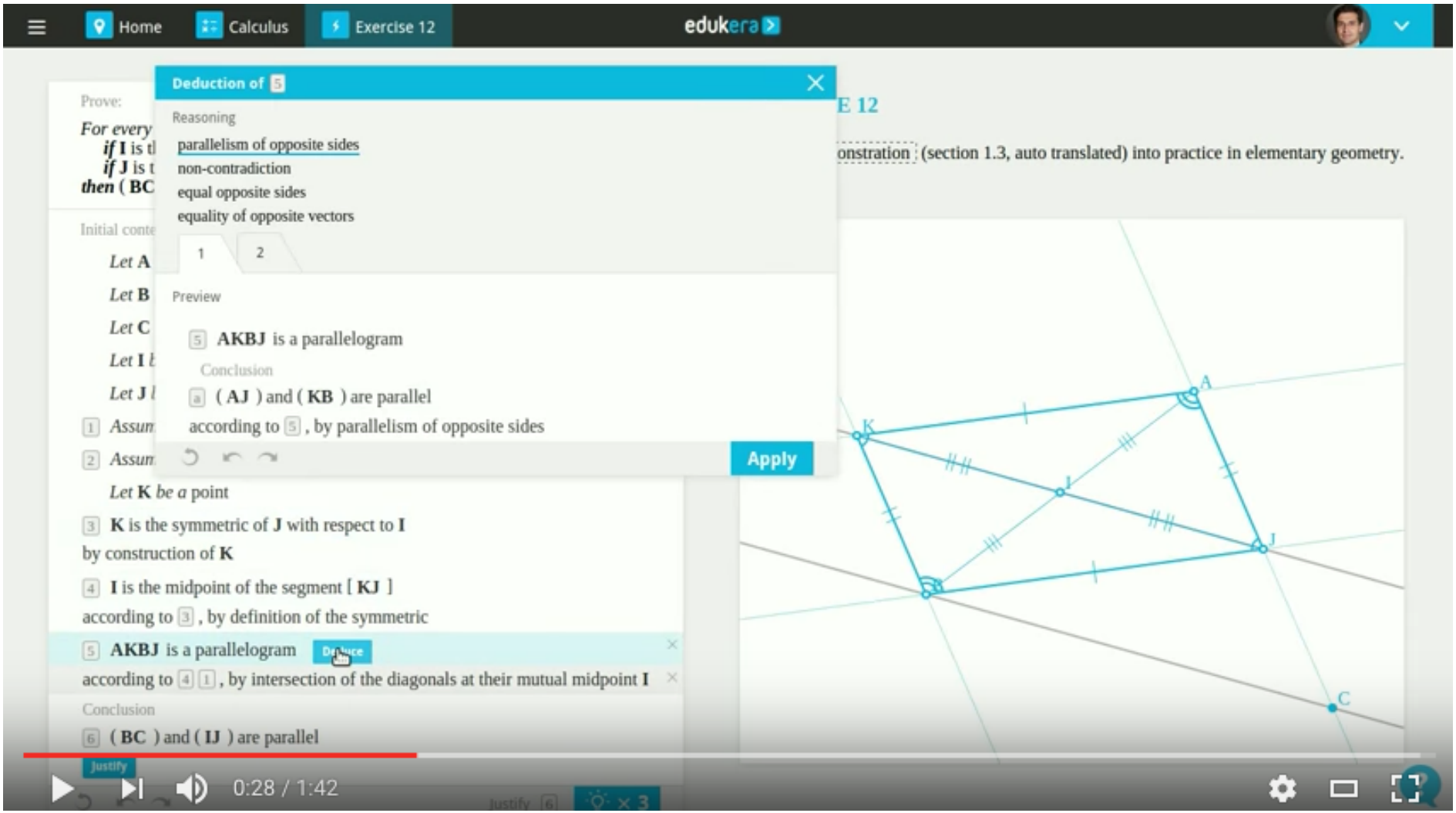
Edukera (Mode logique)

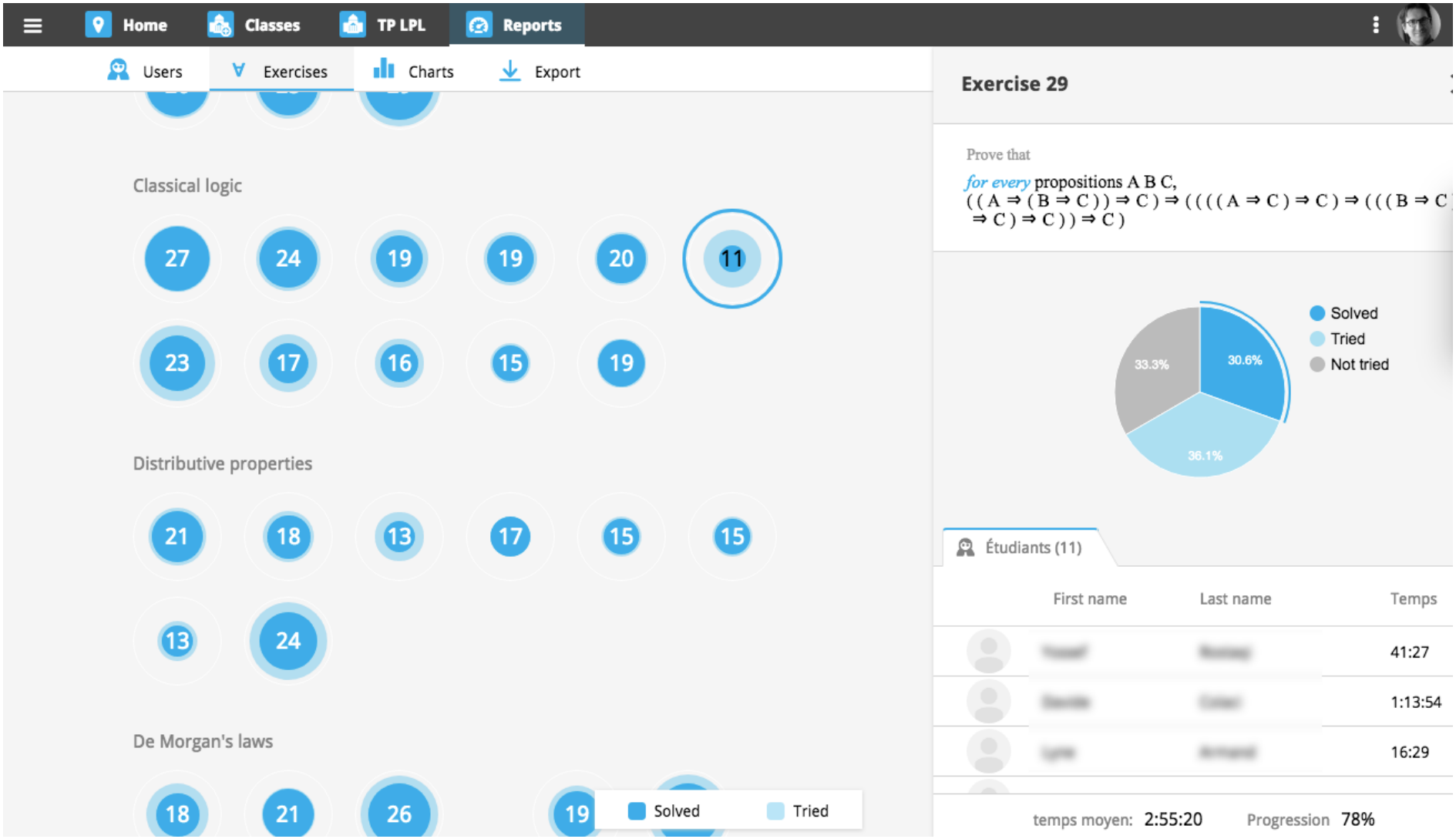


Edukera (Mode maths)



Edukera (prototype pour la géometrie)




Home
Classes
TP LPL
Reports
Users
Exercises
Charts
Export
Classical logic
27
24
19
19
20
11
23
17
16
15
19
Distributive properties
21
18
13
17
15
15
13
24
De Morgan's laws
18
21
26
19
Solved
Tried
Exercise 29
Prove that
for every propositions A B C,
((A ⇒ (B ⇒ C)) ⇒ C) ⇒ ((((A ⇒ C) ⇒ C) ⇒ (((B ⇒ C) ⇒ C) ⇒ C)) ⇒ C)
Solved
Tried
Not tried
33.3%
30.6%
36.1%
Étudiants (11)
First name
Last name
Temps
41:27
1:13:54
16:29
temps moyen: 2:55:20
Progression 78%

Quelques expériences

Années précédentes:

- L2: déduction naturelle (Edukera/Mode Logique)
- M1: preuve assistée par ordinateur (Edukera Logic Mode+Coq)
- M2: sémantique/preuve de programmes (Coq, Frama-c, why3)

Depuis septembre:

- L1 Maths/Info: Le concept de démonstration et quelques notions sur les relations, fonctions et ensembles (Edukera en Mode Maths).

Résultats pour un cours de logique

- 36 étudiants, $>$ 2000 exercices en déduction naturelle
- retour positif des étudiants
- gros progrès en déduction naturelle
- évaluation scientifique à faire

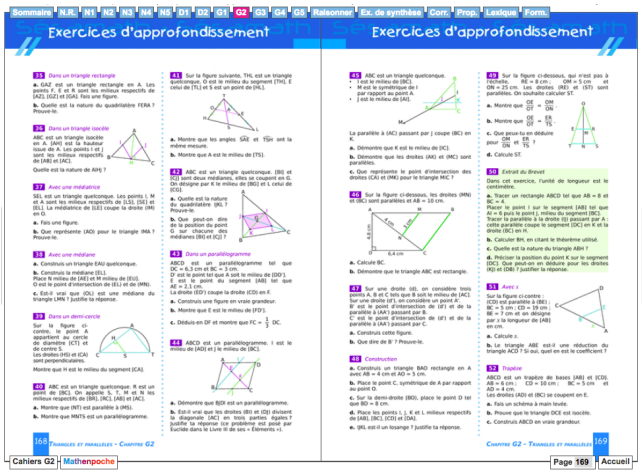
Résultats dans un cours sur l'enseignement de la démonstration interactive

- Edukera comme outil pour apprendre la déduction naturelle.
- Le passage à Coq va plus vite.

Plan

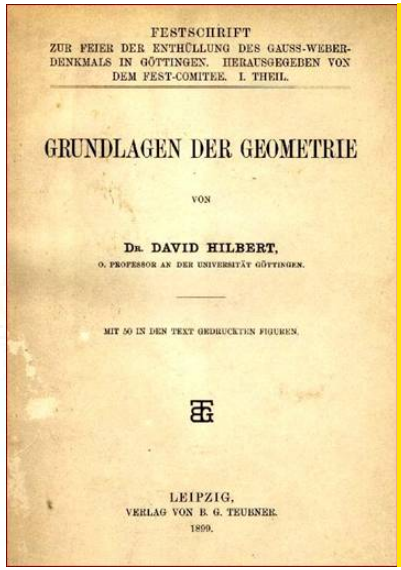
GeoCoq

- Une bibliothèque libre sur les fondements de la géométrie.
- Michael Beeson, Gabriel Braun, Pierre Boutry, Charly Gries, Julien Narboux, Pascal Schreck
- Taille: $>$ 3900 Lemmes, $>$ 130000 lignes
- License: LGPL3

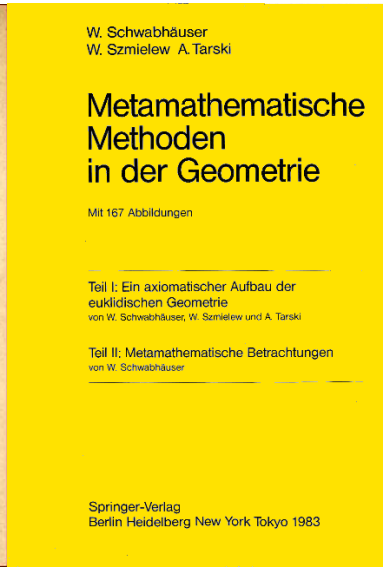


Exercices

Euclide



Hilbert



Tarski

Contenu:

Axiomatiques Tarski, Hilbert, Euclide and variantes.

Fondements En dimension arbitraire, en géométrie neutre. Betweenness, Two-sides, One-side, Collinearity, Midpoint, Symmetric point, Perpendicularity, Parallelism, Angles, Co-planarity, ...

Théorèmes classiques Pappus, Pythagore, Thales, Thales dans le cercle, cercle des neufs points, droite d'Euler, centres usuels des triangles, Varignon, ...

Arithmetisation Coordonnées

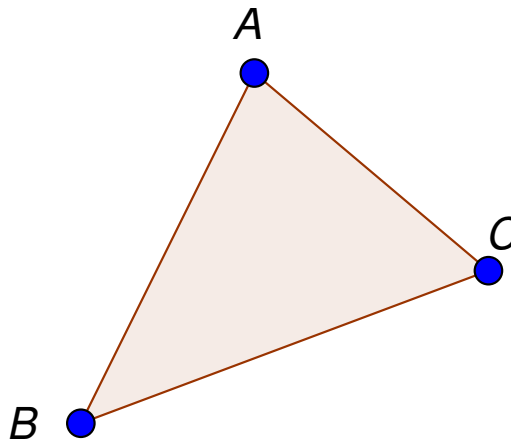
Collège/Lycée Quelques exos

Ce qu'il manque:

- trigo, aires
- lien avec les complexes

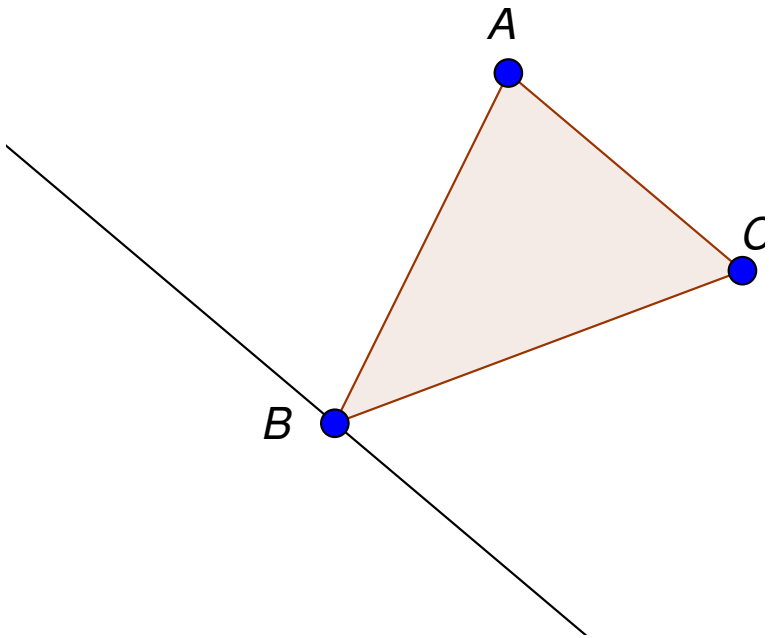
La somme des angles d'un triangle (Euclide Livre I, Prop 32)

Soit l une parallèle à AC passant par B.



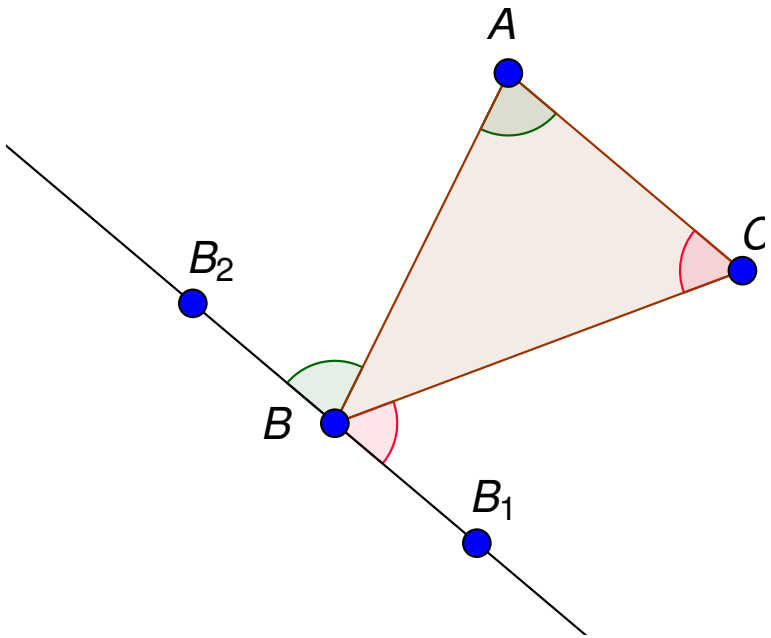
La somme des angles d'un triangle (Euclide Livre I, Prop 32)

Soit *l* une parallèle à *AC* passant par *B*.



La somme des angles d'un triangle (Euclide Livre I, Prop 32)

Soit l une parallèle à AC passant par B.

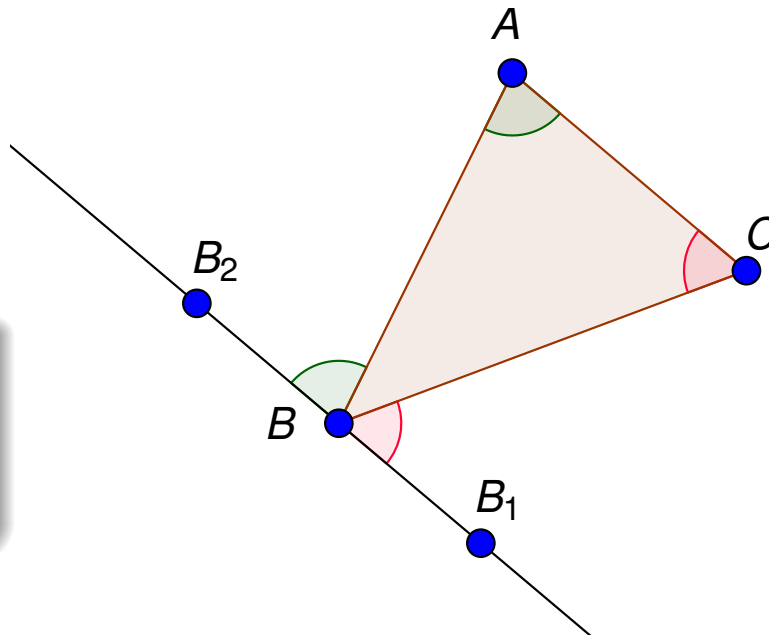


La somme des angles d'un triangle (Euclide Livre I, Prop 32)

Soit l une parallèle à AC passant par B.

Mais !

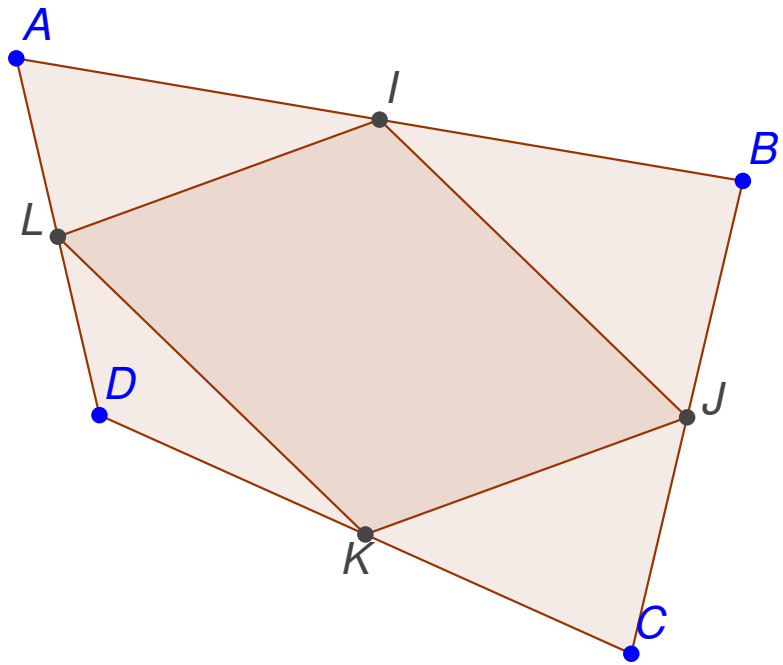
Il faut prouver que les angles sont alterne-internes.



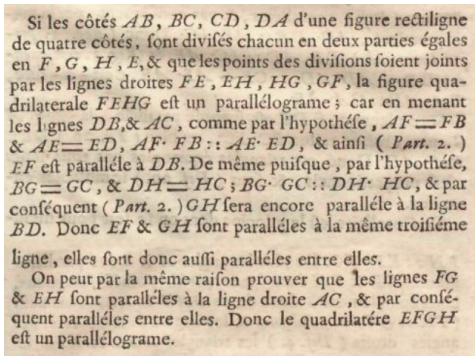
Théorème de Varignon

Theorem

Soit ABCD un quadrilatère. Soient I, J, K et L les milieux de AB, BC, CD, et AD, alors IJKL est un parallèlogramme.



En utilisant le théorème de la droite des milieux, dans le triangle ABC on a $AC \parallel IJ$. On a aussi $AC \parallel LK$.
Donc $LK \parallel IJ$.
De même, $IL \parallel JK$.

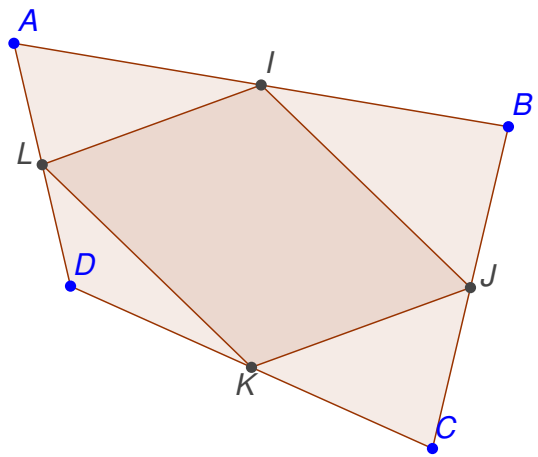


Si les côtés AB, BC, CD, DA d'une figure rectiligne de quatre côtés, sont divisés chacun en deux parties égales en F, G, H, E, & que les points des divisions soient joints par les lignes droites FE, EH, HG, GF, la figure quadrilaterale $FEHG$ est un parallélograme ; car en menant les lignes DB, & AC, comme par l'hypothèse, $AF = FB$ & $AE = ED$, $AF \cdot FB :: AE \cdot ED$, & ainsi (*Part.* 2.) EF est paralléle à DB. De même puisque, par l'hypothèse, $BG = GC$, & $DH = HC$; $BG \cdot GC :: DH \cdot HC$, & par conséquent (*Part.* 2.) GH sera encore paralléle à la ligne BD. Donc EF & GH sont paralléles à la même troisiéme ligne, elles sont donc auſſi paralléles entre elles.

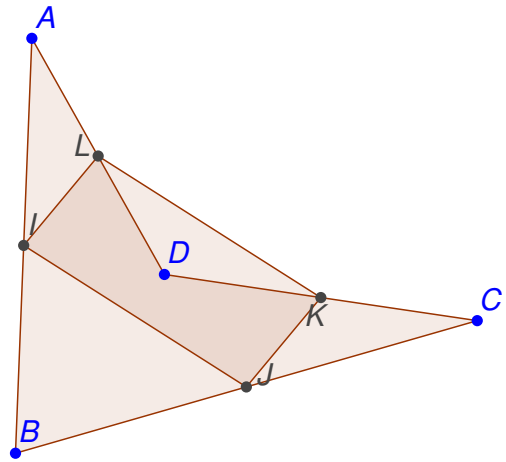
On peut par la même raiſon prouver que les lignes FG & EH ſont paralléles à la ligne droite AC, & par conſéquent paralléles entre elles. Donc le quadrilatére $EFGH$ eſt un parallélograme.

Preuve originale

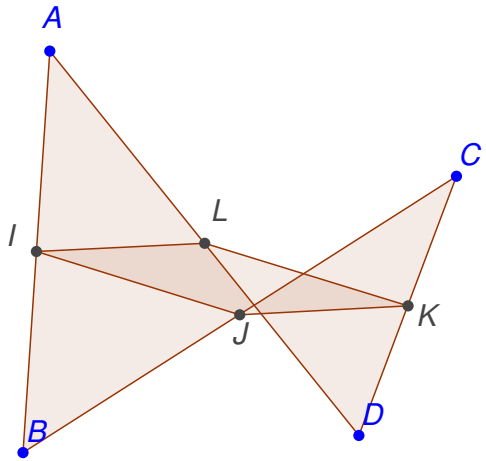
Théorème de Varignon



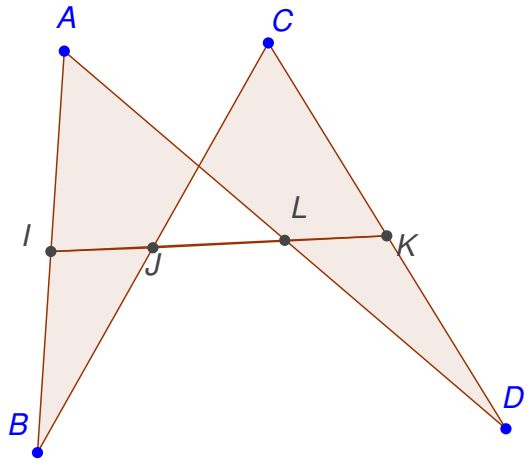
(a) Convex case



(b) Concave case



(c) Self-intersection



(d) Special case

Défis

- Les conditions de non dégénérescence sont faciles à oublier.
- Comme dans les Éléments, les manuels ont tendance à prouver des propriétés **en supposant** les points en position générale, mais **ne vérifie pas cette condition** au moment d'utiliser les théorèmes.
- Comme dans les Éléments, les manuels admettent les propriétés co-exactes.

Conclusion

- Les assistants de preuves peuvent être testés en classe.
- Une évaluation scientifique de l'efficacité reste à faire.
- Des problèmes apparaissent dans le cadre de la géométrie.