Seminari lògica: Introducció a la lògica

Marc Herault i Edgar Moreno

Primavera 2022

Una mica de filosofia

Que volem quan fem matemàtiques?

Una mica de filosofia

Que volem quan fem matemàtiques?

- Abstreure: de vectorets de Batxillerat a espais vectorials.

Una mica de filosofia

Que volem quan fem matemàtiques?

- Abstreure: de vectorets de Batxillerat a espais vectorials.
- Formalitzar: teorema de Bolzano (necessitem ínfims!!)

Una mica més

Que és un espai vectorial?

Una mica més

Que és un espai vectorial?

1. Definir que és un cos arbitrari.

Una mica més

Que és un espai vectorial?

1. Definir que és un cos arbitrari.
2. Definir que són operacions.

Una mica més

Que és un espai vectorial?

1. Definir que és un cos arbitrari.
2. Definir que són operacions.
3. Definir quines propietats poden tenir les operacions.

Una mica més

Que és un espai vectorial?

1. Definir que és un cos arbitrari.
2. Definir que són operacions.
3. Definir quines propietats poden tenir les operacions.
4. Definir conjunts!

Abstracció i formalització a la vegada: categories

Categoria

Una col·lecció de objectes $Ob(C)$.
Aplicacions entre ells $Hom_C(A, B)$:

- Associatives
- Amb identitat

Abstracció i formalització a la vegada: categories

Categoria

Una col·lecció de objectes $Ob(C)$.
Aplicacions entre ells $Hom_C(A, B)$:

- Associatives
- Amb identitat

Exemples?

Abstracció i formalització a la vegada: categories

Categoria

Una col·lecció de objectes $Ob(C)$.
Aplicacions entre ells $Hom_C(A, B)$:

- Associatives
- Amb identitat

Exemples? Conjunts, anells, grups, cossos, espais vectorials, mòduls, superficies de $\mathbb{R}^n$... Fins i tot grafs!

Comencem amb la lògica

Axiomes per fonamentar.

Postulats d'Euclides

1. Entre dos punts es pot dibuixar un segment recte.
2. Tot segment recte es pot estendre a una recta (infinita).
3. Donat un segment podem dibuixar un cercle de radi la llargada d'aquests i centre un dels punts finals.
4. Tots els angles rectes són iguals.
5. Donats dos segments, si un altre els talla tal que la suma dels angles de un costat és menys de $180°$, llavors si estenem els segments les rectes que formen es tallaran.

Comencem amb la lògica

Axiomes per fonamentar.

Postulats d'Euclides

1. Entre dos punts es pot dibuixar un segment recte.
2. Tot segment recte es pot estendre a una recta (infinita).
3. Donat un segment podem dibuixar un cercle de radi la llargada d'aquests i centre un dels punts finals.
4. Tots els angles rectes són iguals.
5. Donats dos segments, si un altre els talla tal que la suma dels angles de un costat és menys de $180°$, llavors si estenem els segments les rectes que formen es tallaran.

Cal el 5?

Comencem amb la lògica

Axiomes per fonamentar.

Postulats d'Euclides

1. Entre dos punts es pot dibuixar un segment recte.
2. Tot segment recte es pot estendre a una recta (infinita).
3. Donat un segment podem dibuixar un cercle de radi la llargada d'aquests i centre un dels punts finals.
4. Tots els angles rectes són iguals.
5. Donats dos segments, si un altre els talla tal que la suma dels angles de un costat és menys de 180°, llavors si estenem els segments les rectes que formen es tallaran.

Cal el 5? Altres geometries! (hiperbòlica o el·líptica) (1823!!!)

Com raonem?

Lògica proposicional

$(a \wedge b) \implies c$. Cada interpretació descriu un món, però amb relacions.

Com raonem?

Lògica proposicional

$(a \wedge b) \implies c$. Cada interpretació descriu un món, però amb relacions.

Lògica de primer ordre

$(\forall c(a \wedge c) \iff (b \wedge c)) \implies a = b$ o $\exists a, f(a)$

Com raonem?

Lògica proposicional

$(a \wedge b) \implies c$. Cada interpretació descriu un món, però amb relacions.

Lògica de primer ordre

$(\forall c(a \wedge c) \iff (b \wedge c)) \implies a = b$ o $\exists a, f(a)$

Lògica de segon ordre

Podem raonar sobre predicats. $\forall P, \forall x(Px \vee \neg Px)$

Axiomes del pensament

Identitat

$\forall a, a = a$
(de fet transitivitat i reflexivitat també)

Axiomes del pensament

Identitat

$\forall a, a = a$

(de fet transitivitat i reflexivitat també)

No contradicció

$\forall A, \neg(A \wedge \neg A)$

Axiomes del pensament

Identitat

$\forall a, a = a$

(de fet transitivitat i reflexivitat també)

No contradicció

$\forall A, \neg(A \wedge \neg A)$

Tercer exclòs

$\forall A, (A \vee \neg A)$

No li agrada a tothom, constructivistes.

Que és un conjunt?

Axioma: Donada la relació $\in$ un conjunt B és un objecte tal que $a \in B \iff f(a)$ per una f funció booleana donada.

Que és un conjunt?

Axioma: Donada la relació $\in$ un conjunt B és un objecte tal que $a \in B \iff f(a)$ per una f funció booleana donada.
Sigui $f(a) = \{a \text{ és un conjunt i } a \notin a\}$.

Que és un conjunt?

Axioma: Donada la relació $\in$ un conjunt B és un objecte tal que $a \in B \iff f(a)$ per una f funció booleana donada.
Sigui $f(a) = \{a \text{ és un conjunt i } a \notin a\}$.

Autoreferència

El nombre natural més petit que es pot definir en menys de vint paraules.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.
5. Unió: Donat X existeix $Y = \bigcup_{x \in X} x$.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.
5. Unió: Donat X existeix $Y = \bigcup_{x \in X} x$.
6. Potència: donat A existeix el conjunt dels subconjunts de A.
   Exercici (Cantor): $|P(A)| > |A|$

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.
5. Unió: Donat X existeix $Y = \bigcup_{x \in X} x$.
6. Potència: donat A existeix el conjunt dels subconjunts de A. Exercici (Cantor): $|P(A)| > |A|$
7. Infinit: existeix un conjunt infinit.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.
5. Unió: Donat X existeix $Y = \bigcup_{x \in X} x$.
6. Potència: donat A existeix el conjunt dels subconjunts de A. Exercici (Cantor): $|P(A)| > |A|$
7. Infinit: existeix un conjunt infinit.
8. Regularitat: donat A hi ha un conjunt minimal per $\in$ començant en A.

Conjunts ben fets?

Zermelo-Fraenkel($\approx$ 1921)

1. Extensionalitat: si X, Y tenen els mateixos elements $X = Y$.
2. Parell: Donats a, b existeix un conjunt $C = \{a, b\}$.
3. Separació: Donat A i una propietat $P(u, v)$ existeix $B = \{u \in A | P(u, v)\}$ per tot v.
4. Reemplaçament: Donat A i una funció $P(u)$ existeix $B = \{P(u) | u \in A\}$.
5. Unió: Donat X existeix $Y = \bigcup_{x \in X} x$.
6. Potència: donat A existeix el conjunt dels subconjunts de A. Exercici (Cantor): $|P(A)| > |A|$
7. Infinit: existeix un conjunt infinit.
8. Regularitat: donat A hi ha un conjunt minimal per $\in$ començant en A.

Exercici: escriure els axiomes en lògica de primer ordre.

Podem fer mates només amb això?

Podem fer mates només amb això?

- Parells ordenats: $(x, y) = \{\{x\}, \{x, y\}\}$ (Exercici: tripletes ordenades)

Podem fer mates només amb això?

- Parells ordenats: $(x, y) = \{\{x\}, \{x, y\}\}$ (Exercici: tripletes ordenades)
- Funcions $F : X \to Y := \{(x, F(x)) | x \in X\}$

Podem fer mates només amb això?

- Parells ordenats: $(x, y) = \{\{x\}, \{x, y\}\}$ (Exercici: tripletes ordenades)
- Funcions $F : X \to Y := \{(x, F(x)) | x \in X\}$
- Naturals:

$$
\begin{gathered}
0 := \emptyset \\
1 := \{0\} \\
2 := \{0, 1\} \\
3 := \{0, 1, 2\} \\
4 := \{0, 1, 2, 3\} \\
\ldots
\end{gathered}
$$

Volem afegir algo més?

Preguntes: tot espai vectorial de dimensió finita té una base. Es veritat per dimensió infinita?
Que els naturals estiguin ordenats ens deixa fer inducció: podem ordenar tot conjunt?
Solucions de $f : \mathbb{R} \to \mathbb{R}, f(x+y) = f(x) + f(y)$?

Volem afegir algo més?

Preguntes: tot espai vectorial de dimensió finita té una base. Es veritat per dimensió infinita?
Que els naturals estiguin ordenats ens deixa fer inducció: podem ordenar tot conjunt?
Solucions de $f : \mathbb{R} \to \mathbb{R}, f(x+y) = f(x) + f(y)$?

Axioma de l'elecció

Per tota família $(X_i)_{i \in I}$ existeix f tal que $f(X_i) = x_i$ amb $x_i \in X_i$.

Volem afegir algo més?

Preguntes: tot espai vectorial de dimensió finita té una base. Es veritat per dimensió infinita?
Que els naturals estiguin ordenats ens deixa fer inducció: podem ordenar tot conjunt?
Solucions de $f : \mathbb{R} \to \mathbb{R}, f(x+y) = f(x) + f(y)$?

Axioma de l'elecció

Per tota família $(X_i)_{i \in I}$ existeix f tal que $f(X_i) = x_i$ amb $x_i \in X_i$.

Bon ordre

Tot conjunt admet una relació $<$ que és un ordre estricte i total.

Volem afegir algo més?

Preguntes: tot espai vectorial de dimensió finita té una base. Es veritat per dimensió infinita?
Que els naturals estiguin ordenats ens deixa fer inducció: podem ordenar tot conjunt?
Solucions de $f : \mathbb{R} \to \mathbb{R}, f(x+y) = f(x) + f(y)$?

Axioma de l'elecció

Per tota família $(X_i)_{i \in I}$ existeix f tal que $f(X_i) = x_i$ amb $x_i \in X_i$.

Bon ordre

Tot conjunt admet una relació $<$ que és un ordre estricte i total.

Lema de Zorn

Sigui S un conjunt parcialment ordenat tal que per a tota cadena (subconjunt totalment ordenat) hi ha una cota superior. Llavors S té un element maximal.

Podriem afegir més!

Hipòtesi del continu

No hi ha cap cardinalitat entre la dels enters i els reals (parts dels enters)

Teorema (Cohen 1963)

La hipòtesi del continu és independent de ZFC.

Que volem de un sistema lògic?

Tenir els naturals com a conjunt i poder fer aritmètica bàsica.

- ZF (o ZFC)
- Peano:
  - $0 \in \mathbb{N}$
  - $=$ ben definit
  - Si n natural $S(n)$ natural
  - $S(m) = S(n) \iff m = n$
  - No existeix n tq $S(n) = 0$
  - Si $0 \in K$ i $n \in K \implies S(n) \in K$ llavors $K = \mathbb{N}$ (axioma de inducció)

Exercici: definir la suma $(+)$ de manera recursiva a ZF o a Peano.

Però que volem de veritat?

Però que volem de veritat?

- Completesa: tot el que és cert es pot provar.

Però que volem de veritat?

- Completesa: tot el que és cert es pot provar.
- Consistència: no hi ha proposicions contradictòries. Principi d'explosió.

Però que volem de veritat?

- Completesa: tot el que és cert es pot provar.
- Consistència: no hi ha proposicions contradictòries. Principi d'explosió.
- Decidibilitat: donat una proposició és pot decidir (mitjançant un algorisme) si aquesta és certa.

Una mica d'història

- 1870: Cantor i Dedekind intenten axiomatitzar la teoria de conjunts.
- 1908-1921: Zermelo i Fraenkel axiomatitzen la teoria de conjunts.
- Principis XX: Hilbert intenta trobar una manera de axiomatitzar les bases de les matemàtiques.
- 1931: Gödel demostra que no és possible el que vol Hilbert.
- 1936: Turing fica les bases de la computació

Primer teorema de Gödel

Teorema (1931)

Tot sistema lògic consistent capaç de fer aritmètica bàsica (amb el enters) és incomplet.

Interpretació

$\mathbb{R}$ o $\mathbb{C}$ sí que es poden definir de forma completa.
Podem incloure altres axiomes per a que el nostre conjunt de axiomes original sigui complet, però no ho serà el nou sistema.

Segon teorema de Gödel

Teorema (1931)

Cap sistema lògic consistent capaç de fer aritmètica bàsica és capaç de provar la seva pròpia consistència.