

# Pruebas de Independencia: ¿Qué son y para qué sirven?

David Fernández Bretón

`dfernandezb@ipn.mx`

`https://dfernandezb.web.app/espanol.html`

Seminario del Departamento de Matemáticas  
ESFM, IPN  
10 de noviembre de 2021



**Instituto  
Politécnico  
Nacional**

En lógica, un **lenguaje** tiene como ingredientes:



En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$



**Instituto  
Politécnico  
Nacional**

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$



**Instituto  
Politécnico  
Nacional**

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$



**Instituto  
Politécnico  
Nacional**

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$



Instituto  
Politécnico  
Nacional

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).



Instituto  
Politécnico  
Nacional

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además



Instituto  
Politécnico  
Nacional



En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e,$



Instituto  
Politécnico  
Nacional

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e,$
- y un *símbolo de relación binaria*  $*$ .



Instituto  
Politécnico  
Nacional

En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e,$
- y un *símbolo de relación binaria*  $*$ .

Los **axiomas de la teoría de grupos** son los siguientes:



En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e,$
- y un *símbolo de relación binaria*  $*$ .

Los **axiomas de la teoría de grupos** son los siguientes:

- 1  $(\forall x)(\forall y)(\forall z)((x * y) * z = x * (y * z)),$



En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots,$
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow,$
- cuantificadores  $\forall, \exists,$
- y el símbolo de igualdad  $=,$
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e,$
- y un *símbolo de relación binaria*  $*$ .

Los **axiomas de la teoría de grupos** son los siguientes:

- 1  $(\forall x)(\forall y)(\forall z)((x * y) * z = x * (y * z)),$
- 2  $(\forall x)(x * e = x \wedge e * x = x),$



En lógica, un **lenguaje** tiene como ingredientes:

- variables,  $x, y, z, \dots, x_1, x_2, \dots, \alpha, \beta, \dots$ ,
- conectivas lógicas  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ ,
- cuantificadores  $\forall, \exists$ ,
- y el símbolo de igualdad  $=$ ,
- (y paréntesis).

El **lenguaje de la teoría de grupos** incluye además

- un *símbolo de constante*  $e$ ,
- y un *símbolo de relación binaria*  $*$ .

Los **axiomas de la teoría de grupos** son los siguientes:

- 1  $(\forall x)(\forall y)(\forall z)((x * y) * z = x * (y * z))$ ,
- 2  $(\forall x)(x * e = x \wedge e * x = x)$ ,
- 3  $(\forall x)(\exists y)(y * x = e \wedge x * y = e)$ .



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$



**Instituto  
Politécnico  
Nacional**

Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,





Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ ,



**Instituto  
Politécnico  
Nacional**

Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ ,



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien se *sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ )



Instituto  
Politécnico  
Nacional

Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$  es una fórmula  $\varphi$  para la cual existe una demostración a partir de los axiomas  $\Sigma$ .



Instituto  
Politécnico  
Nacional

Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$  es una fórmula  $\varphi$  para la cual existe una demostración a partir de los axiomas  $\Sigma$ . Se escribe  $\Sigma \vdash \varphi$ .



Instituto  
Politécnico  
Nacional

Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$  es una fórmula  $\varphi$  para la cual existe una demostración a partir de los axiomas  $\Sigma$ . Se escribe  $\Sigma \vdash \varphi$ .

**Por ejemplo:**



Instituto  
Politécnico  
Nacional



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *se sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$  es una fórmula  $\varphi$  para la cual existe una demostración a partir de los axiomas  $\Sigma$ . Se escribe  $\Sigma \vdash \varphi$ .

### Por ejemplo:

La fórmula  $(\forall z)((\exists x)(x * z = x) \Rightarrow z = e)$  es un teorema de los axiomas de la teoría de grupos



Una **demostración** de una fórmula  $\varphi$  a partir de los axiomas  $\Sigma$  es una sucesión finita de fórmulas,  $\varphi_1, \dots, \varphi_n$ , tal que  $\varphi_n$  es  $\varphi$ , y cada  $\varphi_i$  es o bien un axioma, o bien *sigue lógicamente* de algunas  $\varphi_j$  ( $j < i$ ) (reglas de inferencia, puramente sintácticas, completamente formalizadas).

Un **teorema** de  $\Sigma$  es una fórmula  $\varphi$  para la cual existe una demostración a partir de los axiomas  $\Sigma$ . Se escribe  $\Sigma \vdash \varphi$ .

### Por ejemplo:

La fórmula  $(\forall z)((\exists x)(x * z = x) \Rightarrow z = e)$  es un teorema de los axiomas de la teoría de grupos (intuitivamente, se sigue de los axiomas de la teoría de grupos que el elemento identidad es único).



## Ejemplo:



## Ejemplo:

- Sea  $z$  arbitrario,



**Instituto  
Politécnico  
Nacional**

## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,



Instituto  
Politécnico  
Nacional

## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ ,



Instituto  
Politécnico  
Nacional

## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ ,





## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,
  - entonces  $(y * x) * z = e$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,
  - entonces  $(y * x) * z = e$ ,
  - entonces  $e * z = e$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,
  - entonces  $(y * x) * z = e$ ,
  - entonces  $e * z = e$ ,
  - entonces  $z = e$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,
  - entonces  $(y * x) * z = e$ ,
  - entonces  $e * z = e$ ,
  - entonces  $z = e$ ,
- por lo tanto,  $(\exists x)(x * z = x) \Rightarrow z = e$ ,



## Ejemplo:

- Sea  $z$  arbitrario,
  - supongamos que  $(\exists x)(x * z = x)$ ,
  - entonces  $x * z = x$ , (más adelante no podemos poner  $(\forall x)$ ),
  - sea  $y$  tal que  $y * x = e \wedge x * y = e$ , (más adelante no podemos poner  $(\forall y)$ ),
  - entonces  $y * x = e$ ,
  - entonces  $y * (x * z) = y * x$ ,
  - entonces  $(y * x) * z = e$ ,
  - entonces  $e * z = e$ ,
  - entonces  $z = e$ ,
- por lo tanto,  $(\exists x)(x * z = x) \Rightarrow z = e$ ,
- por lo tanto,  $(\forall z)((\exists x)(x * z = x) \Rightarrow z = e)$ .



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**

La fórmula  $\varphi \equiv (\forall x)(\forall y)(x * y = y * x)$  no se puede demostrar desde los axiomas de teoría de grupos.



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**

La fórmula  $\varphi \equiv (\forall x)(\forall y)(x * y = y * x)$  no se puede demostrar desde los axiomas de teoría de grupos.

Ya que (por ejemplo)  $\left( \text{GL}_n(\mathbb{R}), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \cdot \right)$  es un *modelo* de los axiomas de la teoría de grupos,



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**

La fórmula  $\varphi \equiv (\forall x)(\forall y)(x * y = y * x)$  no se puede demostrar desde los axiomas de teoría de grupos.

Ya que (por ejemplo)  $\left( \text{GL}_n(\mathbb{R}), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \cdot \right)$  es un *modelo* de los axiomas de la teoría de grupos, pero este modelo **no** satisface  $\varphi$ .



Instituto  
Politécnico  
Nacional

¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**

La fórmula  $\varphi \equiv (\forall x)(\forall y)(x * y = y * x)$  no se puede demostrar desde los axiomas de teoría de grupos.

Ya que (por ejemplo)  $\left( \text{GL}_n(\mathbb{R}), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \cdot \right)$  es un *modelo* de los axiomas de la teoría de grupos, pero este modelo **no** satisface  $\varphi$ .

Teoría de grupos  $\not\models$  Conmutatividad.



¿Qué pasa cuando  $\Sigma \not\models \varphi$ ?

Para verificar tal cosa, tendríamos que encontrar un *modelo* que *satisfaga* los axiomas  $\Sigma$  pero no satisfaga  $\varphi$ .

**Por ejemplo:**

La fórmula  $\varphi \equiv (\forall x)(\forall y)(x * y = y * x)$  no se puede demostrar desde los axiomas de teoría de grupos.

Ya que (por ejemplo)  $\left( \text{GL}_n(\mathbb{R}), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \cdot \right)$  es un *modelo* de los axiomas de la teoría de grupos, pero este modelo **no** satisface  $\varphi$ .

Teoría de grupos  $\not\models$  Conmutatividad.

(La conmutatividad es *independiente* de los axiomas de Teoría de Grupos.)





Por otra parte, pasa lo mismo con la negación de la conmutatividad.



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos,



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos, y también satisface  $(\forall x)(\forall y)(x * y = y * x)$ .



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos, y también satisface  $(\forall x)(\forall y)(x * y = y * x)$ .

Teoría de grupos  $\not\models \neg(\text{Conmutatividad})$ .



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos, y también satisface  $(\forall x)(\forall y)(x * y = y * x)$ .

Teoría de grupos  $\not\models \neg(\text{Conmutatividad})$ .

(La conmutatividad es *consistente* con los axiomas de Teoría de Grupos.)



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos, y también satisface  $(\forall x)(\forall y)(x * y = y * x)$ .

Teoría de grupos  $\not\vdash \neg(\text{Conmutatividad})$ .

(La conmutatividad es *consistente* con los axiomas de Teoría de Grupos.)

Por lo tanto, la conmutatividad es *indecidable* desde los axiomas de la Teoría de Grupos



Por otra parte, pasa lo mismo con la negación de la conmutatividad.

Ya que (por ejemplo)  $(\mathbb{R}, 0, +)$  satisface los axiomas de la teoría de grupos, y también satisface  $(\forall x)(\forall y)(x * y = y * x)$ .

Teoría de grupos  $\not\vdash \neg(\text{Conmutatividad})$ .

(La conmutatividad es *consistente* con los axiomas de Teoría de Grupos.)

Por lo tanto, la conmutatividad es *indecidable* desde los axiomas de la Teoría de Grupos (ni ella ni su negación se puede demostrar).



En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:





En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...



**Instituto  
Politécnico  
Nacional**

En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...



Instituto  
Politécnico  
Nacional

En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...
- Un espacio vectorial es un **conjunto**  $V$  equipado con una relación binaria  $+$  :  $V \times V \longrightarrow V$ , y un campo  $k$ , y una acción de  $k^*$  en el conjunto  $V$ , tal que...



Instituto  
Politécnico  
Nacional

En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...
- Un espacio vectorial es un **conjunto**  $V$  equipado con una relación binaria  $+$  :  $V \times V \longrightarrow V$ , y un campo  $k$ , y una acción de  $k^*$  en el conjunto  $V$ , tal que...
- Un campo es un **conjunto**  $k$  equipado con operaciones binarias  $+$  :  $k \times k \longrightarrow k$  y  $\cdot$  :  $k \times k \longrightarrow k$  tales que...



En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...
- Un espacio vectorial es un **conjunto**  $V$  equipado con una relación binaria  $+$  :  $V \times V \longrightarrow V$ , y un campo  $k$ , y una acción de  $k^*$  en el conjunto  $V$ , tal que...
- Un campo es un **conjunto**  $k$  equipado con operaciones binarias  $+$  :  $k \times k \longrightarrow k$  y  $\cdot$  :  $k \times k \longrightarrow k$  tales que...
- Una función  $f : X \longrightarrow Y$  es un **subconjunto**  $f \subseteq X \times Y$  tal que...



En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...
- Un espacio vectorial es un **conjunto**  $V$  equipado con una relación binaria  $+$  :  $V \times V \longrightarrow V$ , y un campo  $k$ , y una acción de  $k^*$  en el conjunto  $V$ , tal que...
- Un campo es un **conjunto**  $k$  equipado con operaciones binarias  $+$  :  $k \times k \longrightarrow k$  y  $\cdot$  :  $k \times k \longrightarrow k$  tales que...
- Una función  $f : X \longrightarrow Y$  es un **subconjunto**  $f \subseteq X \times Y$  tal que...
- Un par ordenado  $(x, y)$  es el **conjunto**  $\{\{x\}, \{x, y\}\}$ ...



En matemáticas, básicamente cualquier estructura se define en términos de conjuntos:

- Un grupo es un **conjunto**  $X$  equipado con una operación binaria  $\cdot : X \times X \longrightarrow X$  tal que...
- Un espacio métrico es un **conjunto**  $X$  equipado con una función  $d : X \times X \longrightarrow [0, \infty)$  tal que...
- Un espacio vectorial es un **conjunto**  $V$  equipado con una relación binaria  $+$  :  $V \times V \longrightarrow V$ , y un campo  $k$ , y una acción de  $k^*$  en el conjunto  $V$ , tal que...
- Un campo es un **conjunto**  $k$  equipado con operaciones binarias  $+$  :  $k \times k \longrightarrow k$  y  $\cdot$  :  $k \times k \longrightarrow k$  tales que...
- Una función  $f : X \longrightarrow Y$  es un **subconjunto**  $f \subseteq X \times Y$  tal que...
- Un par ordenado  $(x, y)$  es el **conjunto**  $\{\{x\}, \{x, y\}\}$ ...
- (También se pueden construir  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , etc., como conjuntos...)



# Moraleja:





**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**,



**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**, implícitamente está diciendo que  $\varphi$  es un teorema desde los axiomas de la Teoría de Conjuntos.



**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**, implícitamente está diciendo que  $\varphi$  es un teorema desde los axiomas de la Teoría de Conjuntos. (¡Aún cuando no sepa con exactitud cuáles son esos axiomas!)



**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**, implícitamente está diciendo que  $\varphi$  es un teorema desde los axiomas de la Teoría de Conjuntos. (¡Aún cuando no sepa con exactitud cuáles son esos axiomas!)

*[...] most mathematicians “do not know” of ZFC just as Monsieur Jourdain in Molière’s Bourgeois Gentilhomme “did not know” he was speaking in prose; [...] because we do not even notice that we are using it.*



**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**, implícitamente está diciendo que  $\varphi$  es un teorema desde los axiomas de la Teoría de Conjuntos. (¡Aún cuando no sepa con exactitud cuáles son esos axiomas!)

*[...] most mathematicians “do not know” of ZFC just as Monsieur Jourdain in Molière’s Bourgeois Gentleman “did not know” he was speaking in prose; [...] because we do not even notice that we are using it.*

*[...] The best framework, the best foundation, is the one that governs you least; that is you do not notice its restrictions (except when really necessary, like arriving at a contradiction).*



**Moraleja:** Cuando un matemático dice que  $\varphi$  es un **teorema**, implícitamente está diciendo que  $\varphi$  es un teorema desde los axiomas de la Teoría de Conjuntos. (¡Aún cuando no sepa con exactitud cuáles son esos axiomas!)

*[...] most mathematicians “do not know” of ZFC just as Monsieur Jourdain in Molière’s Bourgeois Gentleman “did not know” he was speaking in prose; [...] because we do not even notice that we are using it.*

*[...] The best framework, the best foundation, is the one that governs you least; that is you do not notice its restrictions (except when really necessary, like arriving at a contradiction).*

Saharon Shelah, *Logical dreams*. Bull. Amer. Math. Soc. **40** (2003), 203–228.



**Instituto  
Politécnico  
Nacional**

El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis)





El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,
- $A \subseteq B$  puede pensarse como una “abreviación” de  $(\forall x)(x \in A \Rightarrow x \in B)$ ,



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,
- $A \subseteq B$  puede pensarse como una “abreviación” de  $(\forall x)(x \in A \Rightarrow x \in B)$ ,
- “ $x = (a, b)$ ”



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,
- $A \subseteq B$  puede pensarse como una “abreviación” de  $(\forall x)(x \in A \Rightarrow x \in B)$ ,
- “ $x = (a, b)$ ” (que significa  $x = \{\{a\}, \{a, b\}\}$ )



El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,
- $A \subseteq B$  puede pensarse como una “abreviación” de  $(\forall x)(x \in A \Rightarrow x \in B)$ ,
- “ $x = (a, b)$ ” (que significa  $x = \{\{a\}, \{a, b\}\}$ ) puede pensarse como una “abreviación” de  $(\forall z)(z \in x \iff (\forall y)(y \in z \iff y = a) \vee ((\forall y)(y \in z \iff (y = a \wedge y = b))))$ ,





El **lenguaje de la Teoría de Conjuntos** es aquél cuyo alfabeto consta (además de conectivas, cuantificadores, variables, signo de igualdad y paréntesis) de un símbolo de relación binaria  $\in$ .

Así, fórmulas típicas en el lenguaje de la Teoría de Conjuntos serían, por ejemplo,  $(\forall x)(\exists y)(z = x \wedge y \in z)$ , o  $(\exists z)(\forall x)(x \in z \Rightarrow x = y)$ .

Por ejemplo,

- $x \notin y$  puede pensarse como una “abreviación” de  $\neg(x \in y)$ ,
- $x = \emptyset$  puede pensarse como una “abreviación” de  $(\forall y)(y \notin x)$ ,
- $A \subseteq B$  puede pensarse como una “abreviación” de  $(\forall x)(x \in A \Rightarrow x \in B)$ ,
- “ $x = (a, b)$ ” (que significa  $x = \{\{a\}, \{a, b\}\}$ ) puede pensarse como una “abreviación” de  $(\forall z)(z \in x \iff (\forall y)(y \in z \iff y = a) \vee ((\forall y)(y \in z \iff (y = a \wedge y = b))))$ ,
- etc...



# Los axiomas



# Los axiomas (de Zermelo–Fränkel con Elección,



**Instituto  
Politécnico  
Nacional**

# Los axiomas (de Zermelo–Fränkel con Elección, o ZFE):



## Los axiomas (de Zermelo–Fränkel con Elección, o ZFE):

- 1 **Existencia:**  $(\exists x)(x = x)$  (existe un conjunto).
- 1 **Extensionalidad:**  $(\forall x)(\forall y)(x = y \Leftrightarrow (\forall z)(z \in x \Leftrightarrow z \in y))$  (un conjunto está completamente determinado por sus elementos).
- 2 **Comprensión:** Para cada fórmula  $\varphi$  con una variable libre,  $(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow z \in x \wedge \varphi(z))$  (para cada propiedad  $\varphi$  y para cada conjunto  $x$ , existe el conjunto  $\{z \in x \mid \varphi(z)\}$ ).
- 3 **Par:**  $(\forall x)(\forall y)(\exists z)(\forall w)(w \in z \Leftrightarrow (w = x \vee w = y))$  (para cualesquiera dos conjuntos  $x, y$ , existe el conjunto  $\{x, y\}$ ).
- 4 **Unión:**  $(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\exists w \in x)(z \in w))$  (para toda familia de conjuntos  $x$ , existe su unión  $\bigcup_{w \in x} w$ ).
- 5 **Conjunto Potencia:**  $(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow z \subseteq x)$  (para todo conjunto  $x$ , existe su conjunto potencia  $\wp(x)$ ).
- 6 **Axioma de Infinitud:**  $(\exists x)(\emptyset \in x \wedge (\forall y \in x)(y \cup \{y\} \in x))$ . (existe un conjunto infinito).
- 7 **Reemplazo:** Para cada fórmula  $\varphi$  con dos variables libres,  $(\forall x)(\exists! y)(\varphi(x, y)) \Rightarrow (\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (\exists w \in x)(\varphi(w, z)))$  (si la fórmula  $\varphi$  se comporta como una función  $F$ , entonces para todo conjunto  $x$ , la imagen directa  $F[x]$  también es un conjunto).
- 8 **Fundación:**  $(\forall x)(x \neq \emptyset \Rightarrow (\exists y \in x)(\forall z \in x)(z \notin y))$  (la relación  $\in$  de pertenencia es bien fundada).
- 9 **Elección:**  $(\forall x)((\forall y \in x)(y \neq \emptyset) \Rightarrow (\exists z)(\forall y \in x)(\exists! w)(w \in z \wedge w \in y))$  (si  $x$  es una familia de conjuntos no vacíos, entonces se puede escoger un elemento de cada miembro de  $x$ ).



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real”)



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):





A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

**El universo constructible de Gödel,**



**Instituto  
Politécnico  
Nacional**

A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

**El universo constructible de Gödel,  $L \subseteq V$**



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

## El universo constructible de Gödel, $L \subseteq V$

más tarde, la teoría de los modelos internos y los modelos núcleo;



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiéndolo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

## **El universo constructible de Gödel, $L \subseteq V$**

más tarde, la teoría de los modelos internos y los modelos núcleo;

## **La técnica del forzamiento de Cohen,**



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiendo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

### **El universo constructible de Gödel, $L \subseteq V$**

más tarde, la teoría de los modelos internos y los modelos núcleo;

### **La técnica del forzamiento de Cohen, $V[G] \supseteq V$ ;**



A partir de los años 30, se han desarrollado diversas técnicas para construir modelos de ZFE (ya sea encogiéndolo o ensanchando el “mundo real” –el modelo de ZFE en el que se supone que realizamos nuestras matemáticas–):

### **El universo constructible de Gödel, $L \subseteq V$**

más tarde, la teoría de los modelos internos y los modelos núcleo;

### **La técnica del forzamiento de Cohen, $V[G] \supseteq V$ ;**

después, forzamiento iterado, forzamiento apropiado, matrices de iteración, forzamiento con clases, forzamiento con submodelos elementales, iteraciones de Asperó–Mota, ...



# Cardinalidad:



## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:





## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*:



## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ ,



## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $c$ ;



**Instituto  
Politécnico  
Nacional**

## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $c$ ;

La *aritmética*:



## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $c$ ;

La *aritmética*: contar, contar y contar,



**Instituto  
Politécnico  
Nacional**

## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $\mathfrak{c}$ ;

La *aritmética*: contar, contar y contar, al infinito y más allá...



## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $\mathfrak{c}$ ;

La *aritmética*: contar, contar y contar, al infinito y más allá...

$$0, 1, 2, \dots, \aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots,$$



Instituto  
Politécnico  
Nacional

## Cardinalidad:

Al pensar en cardinalidades infinitas, hay dos intuiciones que se contraponen:

La *geométrica*: la recta real,  $\mathbb{R}$ , de cardinalidad  $\mathfrak{c}$ ;

La *aritmética*: contar, contar y contar, al infinito y más allá...

$$0, 1, 2, \dots, \aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots,$$

### Teorema (Cantor)

$$\aleph_1 \leq \mathfrak{c} = |\mathbb{R}|$$





Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis)



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $c$ .



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $c$ . Por ello, Cantor conjeturó



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $\mathfrak{c}$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $\mathfrak{c} = \aleph_1$ .



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $\mathfrak{c}$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $\mathfrak{c} = \aleph_1$ .

(*Primer Problema de Hilbert*: demostrar (o refutar) CH).



Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $c$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $c = \aleph_1$ .

(*Primer Problema de Hilbert*: demostrar (o refutar) CH).

**Teorema (Gödel 1939)**

CH es consistente con ZFE.



Instituto  
Politécnico  
Nacional

Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $c$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $c = \aleph_1$ .

(*Primer Problema de Hilbert*: demostrar (o refutar) CH).

**Teorema (Gödel 1939)**

CH es consistente con ZFE. (*El universo constructible de Gödel.*)





Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $\mathfrak{c}$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $\mathfrak{c} = \aleph_1$ .

(*Primer Problema de Hilbert*: demostrar (o refutar) CH).

**Teorema (Gödel 1939)**

CH es consistente con ZFE. (*El universo constructible de Gödel.*)

**Teorema (Cohen 1960)**

CH es independiente de ZFE.



Instituto  
Politécnico  
Nacional

Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $\mathfrak{c}$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $\mathfrak{c} = \aleph_1$ .

(*Primer Problema de Hilbert: demostrar (o refutar) CH.*)

**Teorema (Gödel 1939)**

CH es consistente con ZFE. (*El universo constructible de Gödel.*)

**Teorema (Cohen 1960)**

CH es independiente de ZFE. (*Método del forzamiento.*)



**Instituto  
Politécnico  
Nacional**

Resulta bastante sospechoso que prácticamente todos los conjuntos infinitos que surgen de manera natural (e.g. mientras hacemos análisis) son todos o bien numerables, o bien de cardinalidad  $c$ . Por ello, Cantor conjeturó

**La Hipótesis del Continuo (CH):**  $c = \aleph_1$ .

(*Primer Problema de Hilbert*: demostrar (o refutar) CH).

**Teorema (Gödel 1939)**

CH es consistente con ZFE. (*El universo constructible de Gödel.*)

**Teorema (Cohen 1960)**

CH es independiente de ZFE. (*Método del forzamiento.*)

En conclusión, la CH es indecidible desde los axiomas de ZFE.



Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si



**Instituto  
Politécnico  
Nacional**

Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que



Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

$$\sum_{n=1}^{\infty} \ell(I_n) < \varepsilon$$

y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n.$$



Instituto  
Politécnico  
Nacional

Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

$$\sum_{n=1}^{\infty} \ell(I_n) < \varepsilon$$

y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n.$$

### Definition

Un conjunto  $X \subseteq \mathbb{R}$  tiene **medida fuertemente cero**

Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

$$\sum_{n=1}^{\infty} \ell(I_n) < \varepsilon$$

y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n.$$

### Definition

Un conjunto  $X \subseteq \mathbb{R}$  tiene **medida fuertemente cero** si para cada sucesión  $\varepsilon_n$ ,  $n \in \mathbb{N}$ ,



Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

$$\sum_{n=1}^{\infty} \ell(I_n) < \varepsilon$$

y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n.$$

### Definition

Un conjunto  $X \subseteq \mathbb{R}$  tiene **medida fuertemente cero** si para cada sucesión  $\varepsilon_n$ ,  $n \in \mathbb{N}$ , existen intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

Recordemos que un conjunto  $X \subseteq \mathbb{R}$  tiene **medida cero** si para todo  $\varepsilon > 0$  hay intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que

$$\sum_{n=1}^{\infty} \ell(I_n) < \varepsilon$$

y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n.$$

### Definition

Un conjunto  $X \subseteq \mathbb{R}$  tiene **medida fuertemente cero** si para cada sucesión  $\varepsilon_n$ ,  $n \in \mathbb{N}$ , existen intervalos  $I_n$ ,  $n \in \mathbb{N}$ , tales que  $\ell(I_n) < \varepsilon_n$  y

$$X \subseteq \bigcup_{n=1}^{\infty} I_n$$

Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

## La **conjetura de Borel**



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC**



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.

**Teorema (Sierpiński 1928)**

*CH implica que existe un conjunto no numerable de medida fuertemente cero.*



**Instituto  
Politécnico  
Nacional**

Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.

### Teorema (Sierpiński 1928)

*CH implica que existe un conjunto no numerable de medida fuertemente cero. En particular, BC es independiente de ZFE.*



**Instituto  
Politécnico  
Nacional**



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.

### Teorema (Sierpiński 1928)

*CH implica que existe un conjunto no numerable de medida fuertemente cero. En particular, BC es independiente de ZFE.*

### Teorema (Laver 1976)

*BC es consistente con ZFE.*



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.

### Teorema (Sierpiński 1928)

*CH implica que existe un conjunto no numerable de medida fuertemente cero. En particular, BC es independiente de ZFE.*

### Teorema (Laver 1976)

*BC es consistente con ZFE. (Iteración con soporte numerable de forzamientos apropiados.)*



Note que si  $X \subseteq \mathbb{R}$  es numerable, entonces  $X$  tiene medida fuertemente cero.

La **conjetura de Borel BC** es la afirmación “todo conjunto de medida fuertemente cero es numerable”.

### Teorema (Sierpiński 1928)

*CH implica que existe un conjunto no numerable de medida fuertemente cero. En particular, BC es independiente de ZFE.*

### Teorema (Laver 1976)

*BC es consistente con ZFE. (Iteración con soporte numerable de forzamientos apropiados.)*

En conclusión, la BC es indecidible desde los axiomas de ZFE.





**Instituto  
Politécnico  
Nacional**

Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ?



**Instituto  
Politécnico  
Nacional**

Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ .





Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$  que codifica las posibilidades para  $G$ , hasta isomorfismo



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$  que codifica las posibilidades para  $G$ , hasta isomorfismo (que respete a la sucesión exacta corta).



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$  que codifica las posibilidades para  $G$ , hasta isomorfismo (que respete a la sucesión exacta corta). (El elemento identidad de  $\text{Ext}(B, A)$  es justamente  $A \oplus B$ ).



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$  que codifica las posibilidades para  $G$ , hasta isomorfismo (que respete a la sucesión exacta corta). (El elemento identidad de  $\text{Ext}(B, A)$  es justamente  $A \oplus B$ ).

### Definición

*Un grupo abeliano  $A$  es un **W-grupo***



Considere la siguiente sucesión exacta corta en la categoría de grupos abelianos:

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0$$

Dados  $A$  y  $B$ , ¿quién puede ser  $G$ ? Una posibilidad obvia es  $G = A \oplus B$ . Existe un grupo abeliano  $\text{Ext}(B, A)$  que codifica las posibilidades para  $G$ , hasta isomorfismo (que respete a la sucesión exacta corta). (El elemento identidad de  $\text{Ext}(B, A)$  es justamente  $A \oplus B$ ).

### Definición

*Un grupo abeliano  $A$  es un **W-grupo** si  $\text{Ext}(A, \mathbb{Z})$  es trivial.*



Resulta que todo grupo abeliano libre es un W-grupo.



Resulta que todo grupo abeliano libre es un W-grupo.

El **problema de Whitehead** es la pregunta





Resulta que todo grupo abeliano libre es un W-grupo.

El **problema de Whitehead** es la pregunta “¿Ser W-grupo implica ser libre abeliano?”



Resulta que todo grupo abeliano libre es un  $W$ -grupo.

El **problema de Whitehead** es la pregunta “¿Ser  $W$ -grupo implica ser libre abeliano?”

### Teorema (Pontryagin)

*Todo  $W$ -grupo numerable es libre abeliano.*



Instituto  
Politécnico  
Nacional

Resulta que todo grupo abeliano libre es un  $W$ -grupo.

El **problema de Whitehead** es la pregunta “¿Ser  $W$ -grupo implica ser libre abeliano?”

### Teorema (Pontryagin)

*Todo  $W$ -grupo numerable es libre abeliano.*

Por lo tanto, el problema de Whitehead es fundamentalmente un problema acerca de grupos no numerables.



Instituto  
Politécnico  
Nacional

## Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano.*



**Instituto  
Politécnico  
Nacional**

## Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*



**Instituto  
Politécnico  
Nacional**

### Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*

### Teorema (Shelah 1974)

*Es consistente con ZFE que existe un  $W$ -grupo  $G$  que no es abeliano libre.*



**Instituto  
Politécnico  
Nacional**

### Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*

### Teorema (Shelah 1974)

*Es consistente con ZFE que existe un  $W$ -grupo  $G$  que no es abeliano libre. ( $|G| = \aleph_1$ )*



### Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*

### Teorema (Shelah 1974)

*Es consistente con ZFE que existe un  $W$ -grupo  $G$  que no es abeliano libre. ( $|G| = \aleph_1$ ) (Consecuencia del Axioma de Martin)*



**Instituto  
Politécnico  
Nacional**



### Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*

### Teorema (Shelah 1974)

*Es consistente con ZFE que existe un  $W$ -grupo  $G$  que no es abeliano libre. ( $|G| = \aleph_1$ ) (Consecuencia del Axioma de Martin –esencialmente, una iteración con soporte finito de forzamientos c.c.c.–)*



**Instituto  
Politécnico  
Nacional**

### Teorema (Shelah 1974)

*Es consistente con ZFE que todo  $W$ -grupo es libre abeliano. (En el universo constructible de Gödel.)*

### Teorema (Shelah 1974)

*Es consistente con ZFE que existe un  $W$ -grupo  $G$  que no es abeliano libre. ( $|G| = \aleph_1$ ) (Consecuencia del Axioma de Martin –esencialmente, una iteración con soporte finito de forzamientos c.c.c.–)*

En conclusión, el problema de Whitehead es indecidible desde los axiomas de ZFE.



Instituto  
Politécnico  
Nacional



**Instituto  
Politécnico  
Nacional**

Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).



Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).

### Definición

La **dimensión proyectiva** de  $M$ , denotada  $\text{pd}(M)$ , es el mínimo  $n$  tal que existe una sucesión exacta

$$\cdots \longrightarrow P_m \xrightarrow{f_m} P_{m-1} \xrightarrow{f_{m-1}} \cdots \longrightarrow P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$



Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).

### Definición

La **dimensión proyectiva** de  $M$ , denotada  $\text{pd}(M)$ , es el mínimo  $n$  tal que existe una sucesión exacta

$$\cdots \longrightarrow P_m \xrightarrow{f_m} P_{m-1} \xrightarrow{f_{m-1}} \cdots \longrightarrow P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

en donde cada  $P_i$  es proyectivo



Instituto  
Politécnico  
Nacional

Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).

### Definición

La **dimensión proyectiva** de  $M$ , denotada  $\text{pd}(M)$ , es el mínimo  $n$  tal que existe una sucesión exacta

$$\cdots \longrightarrow P_m \xrightarrow{f_m} P_{m-1} \xrightarrow{f_{m-1}} \cdots \longrightarrow P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

en donde cada  $P_i$  es proyectivo (toda sucesión exacta corta

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0 \text{ se escinde})$$



Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).

### Definición

La **dimensión proyectiva** de  $M$ , denotada  $\text{pd}(M)$ , es el mínimo  $n$  tal que existe una sucesión exacta

$$\cdots \longrightarrow P_m \xrightarrow{f_m} P_{m-1} \xrightarrow{f_{m-1}} \cdots \longrightarrow P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

en donde cada  $P_i$  es proyectivo (toda sucesión exacta corta

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0 \text{ se escinde}) \text{ y } \ker(f_{n-1}) = 0.$$





Sea  $R$  un anillo, y sea  $M$  un  $R$ -módulo (derecho).

### Definición

La **dimensión proyectiva** de  $M$ , denotada  $\text{pd}(M)$ , es el mínimo  $n$  tal que existe una sucesión exacta

$$\dots \longrightarrow P_m \xrightarrow{f_m} P_{m-1} \xrightarrow{f_{m-1}} \dots \longrightarrow P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

en donde cada  $P_i$  es proyectivo (toda sucesión exacta corta

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0 \text{ se escinde) y } \ker(f_{n-1}) = 0.$$

### Definición

La **dimensión proyectiva** del anillo  $R$  se define como

$$\text{pd}(R) = \sup\{\text{pd}(M) \mid M \text{ es un } R\text{-módulo}\}.$$

# Pregunta:



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ?



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

Teorema (Osofski, 1968)



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

**Teorema (Osofski, 1968)**

$$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3.$$



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

**Teorema (Osofski, 1968)**

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

**Teorema (Osofski, 1968)**

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:

1  $\text{pd}(\mathbb{R}(x, y, z)) = 2,$



**Instituto  
Politécnico  
Nacional**



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

**Teorema (Osofski, 1968)**

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:

- 1  $\text{pd}(\mathbb{R}(x, y, z)) = 2$ ,
- 2  $\text{pd}(\mathbb{Q}(x, y, z)) = 2$ ,



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

### Teorema (Osofski, 1968)

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:

- 1  $\text{pd}(\mathbb{R}(x, y, z)) = 2$ ,
- 2  $\text{pd}(\mathbb{Q}(x, y, z)) = 2$ ,
- 3 CH.



Instituto  
Politécnico  
Nacional

**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

### Teorema (Osofski, 1968)

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:

- 1  $\text{pd}(\mathbb{R}(x, y, z)) = 2$ ,
- 2  $\text{pd}(\mathbb{Q}(x, y, z)) = 2$ ,
- 3 CH.

En particular, los valores exactos de  $\text{pd}(\mathbb{R}(x, y, z))$  y  $\text{pd}(\mathbb{Q}(x, y, z))$  son indecidibles desde los axiomas de ZFE.



**Pregunta:** ¿Cuál es la dimensión proyectiva de  $\mathbb{R}(x, y, z)$ ? ¿Cuál es la dimensión proyectiva de  $\mathbb{Q}(x, y, z)$ ?

### Teorema (Osofski, 1968)

$2 \leq \text{pd}(\mathbb{R}(x, y, z)) = \text{pd}(\mathbb{Q}(x, y, z)) \leq 3$ . Además, las siguientes condiciones son equivalentes:

- 1  $\text{pd}(\mathbb{R}(x, y, z)) = 2$ ,
- 2  $\text{pd}(\mathbb{Q}(x, y, z)) = 2$ ,
- 3 CH.

En particular, los valores exactos de  $\text{pd}(\mathbb{R}(x, y, z))$  y  $\text{pd}(\mathbb{Q}(x, y, z))$  son indecidibles desde los axiomas de ZFE.

### Teorema (Osofski, 1968)

En general, si  $c = \aleph_\ell$ , entonces  $\text{pd}(\mathbb{C}(x_1, \dots, x_n)) = \min\{n, \ell + 1\}$ .



**Instituto  
Politécnico  
Nacional**

Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita.



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ ,



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos





Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).

### Definición

*El álgebra de Calkin es el álgebra cociente  $\mathcal{C}(\mathbb{H}) := \mathcal{B}(\mathbb{H})/\mathcal{K}(\mathbb{H})$ .*



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).

### Definición

*El álgebra de Calkin es el álgebra cociente  $\mathcal{C}(\mathbb{H}) := \mathcal{B}(\mathbb{H})/\mathcal{K}(\mathbb{H})$ .*

Miramos el grupo de automorfismos de  $\mathcal{C}(\mathbb{H})$ .



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).

### Definición

*El álgebra de Calkin es el álgebra cociente  $\mathcal{C}(\mathbb{H}) := \mathcal{B}(\mathbb{H})/\mathcal{K}(\mathbb{H})$ .*

Miramos el grupo de automorfismos de  $\mathcal{C}(\mathbb{H})$ . Un automorfismo de la forma  $x \mapsto u^*xu$ , en donde  $u \in \mathcal{C}(\mathbb{H})$  es unitario, se llama un **automorfismo interno**.



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).

### Definición

*El álgebra de Calkin es el álgebra cociente  $\mathcal{C}(\mathbb{H}) := \mathcal{B}(\mathbb{H})/\mathcal{K}(\mathbb{H})$ .*

Miramos el grupo de automorfismos de  $\mathcal{C}(\mathbb{H})$ . Un automorfismo de la forma  $x \mapsto u^*xu$ , en donde  $u \in \mathcal{C}(\mathbb{H})$  es unitario, se llama un **automorfismo interno**. Un automorfismo que no es interno se llama **automorfismo externo**.



Sea  $\mathbb{H}$  un espacio de Hilbert separable de dimensión infinita. Sea  $\mathcal{B}(\mathbb{H})$  el álgebra  $C^*$  de operadores acotados en  $\mathbb{H}$ , y sea  $\mathcal{K}(\mathbb{H}) \subseteq \mathcal{B}(\mathbb{H})$  el ideal de operadores compactos (que mandan conjuntos acotados en conjuntos totalmente acotados).

### Definición

*El álgebra de Calkin es el álgebra cociente  $\mathcal{C}(\mathbb{H}) := \mathcal{B}(\mathbb{H})/\mathcal{K}(\mathbb{H})$ .*

Miramos el grupo de automorfismos de  $\mathcal{C}(\mathbb{H})$ . Un automorfismo de la forma  $x \mapsto u^*xu$ , en donde  $u \in \mathcal{C}(\mathbb{H})$  es unitario, se llama un **automorfismo interno**. Un automorfismo que no es interno se llama **automorfismo externo**.

**Pregunta:** ¿Cuántos, y cuáles, automorfismos externos existen?



## Teorema (Phillips–Weaver, 2006)

*CH implica que existe un automorfismo externo de  $C(\mathbb{H})$ .*



**Instituto  
Politécnico  
Nacional**

## Teorema (Phillips–Weaver, 2006)

*CH implica que existe un automorfismo externo de  $C(\mathbb{H})$ . En particular, la existencia de un automorfismo externo es consistente con ZFE.*



**Instituto  
Politécnico  
Nacional**



### Teorema (Phillips–Weaver, 2006)

*$CH$  implica que existe un automorfismo externo de  $C(\mathbb{H})$ . En particular, la existencia de un automorfismo externo es consistente con ZFE.*

### Teorema (Farah, 2011)

*El enunciado “todo automorfismo de  $C(\mathbb{H})$  es interno” es consistente con ZFE.*



### Teorema (Phillips–Weaver, 2006)

*CH implica que existe un automorfismo externo de  $C(\mathbb{H})$ . En particular, la existencia de un automorfismo externo es consistente con ZFE.*

### Teorema (Farah, 2011)

*El enunciado “todo automorfismo de  $C(\mathbb{H})$  es interno” es consistente con ZFE. (Es consecuencia del Axioma del Forzamiento Apropriado, o incluso del Axioma del Grafo Abierto.)*



### Teorema (Phillips–Weaver, 2006)

*$\mathcal{CH}$  implica que existe un automorfismo externo de  $C(\mathbb{H})$ . En particular, la existencia de un automorfismo externo es consistente con ZFE.*

### Teorema (Farah, 2011)

*El enunciado “todo automorfismo de  $C(\mathbb{H})$  es interno” es consistente con ZFE. (Es consecuencia del Axioma del Forzamiento Apropriado, o incluso del Axioma del Grafo Abierto.)*

En conclusión, la existencia de automorfismos externos de  $C(\mathbb{H})$  es indecidible de los axiomas de ZFE.





**Instituto  
Politécnico  
Nacional**

**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ ,



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).

**La Conjetura de Schanuel:**





**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).

**La Conjetura de Schanuel:** Dados  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  linealmente independientes sobre  $\mathbb{Q}$ , se cumple que

$$\text{trdg}(\mathbb{Q}(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n.$$



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).

**La Conjetura de Schanuel:** Dados  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  linealmente independientes sobre  $\mathbb{Q}$ , se cumple que

$$\text{trdg}(\mathbb{Q}(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n.$$

(El caso particular cuando los  $\lambda_1, \dots, \lambda_n$  son todos algebraicos se conoce como el **Teorema de Lindemann–Weierstraß**.)



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).

**La Conjetura de Schanuel:** Dados  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  linealmente independientes sobre  $\mathbb{Q}$ , se cumple que

$$\text{trdg}(\mathbb{Q}(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n.$$

(El caso particular cuando los  $\lambda_1, \dots, \lambda_n$  son todos algebraicos se conoce como el **Teorema de Lindemann–Weierstraß**.) Una demostración de esta conjetura tendría muchas consecuencias interesantes,



**Recordemos:** El **grado de trascendencia** de una extensión de campos  $F/k$ , denotado  $\text{trdg}(F/k)$ , es la cardinalidad de una *base de trascendencia* de  $F$  sobre  $k$  (es decir, de un  $S \subseteq F$  que es algebraicamente independiente sobre  $k$  y tal que  $k(S)/k$  es una extensión algebraica).

**La Conjetura de Schanuel:** Dados  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  linealmente independientes sobre  $\mathbb{Q}$ , se cumple que

$$\text{trdg}(\mathbb{Q}(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n.$$

(El caso particular cuando los  $\lambda_1, \dots, \lambda_n$  son todos algebraicos se conoce como el **Teorema de Lindemann–Weierstraß**.) Una demostración de esta conjetura tendría muchas consecuencias interesantes, por ejemplo, que  $e$  y  $\pi$  son algebraicamente independientes.



Una *forma débil* de la conjetura de Schanuel sería la siguiente:



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*



Instituto  
Politécnico  
Nacional

Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

**Demostración del teorema anterior por Viale:**



Instituto  
Politécnico  
Nacional

Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento



Instituto  
Politécnico  
Nacional



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy)



Instituto  
Politécnico  
Nacional

Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $V[G] \supseteq V$  tal que  $k := \mathbb{C} \cap V$  es numerable.



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).
- 4 Por lo tanto, el enunciado del teorema de Wilkie y Kirby es consistente con ZFE.



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

### Teorema (Wilkie, Kirby)

*Existe un campo  $k \subseteq \mathbb{C}$  numerable, algebraica y exponencialmente cerrado, tal que  $\text{trdg}(k(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})) \geq n$  siempre que  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  son linealmente independientes sobre  $\mathbb{Q}$ .*

### Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).
- 4 Por lo tanto, el enunciado del teorema de Wilkie y Kirby es consistente con ZFE.
- 5 Pero dicho enunciado tiene una complejidad baja,



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

## Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).
- 4 Por lo tanto, el enunciado del teorema de Wilkie y Kirby es consistente con ZFE.
- 5 Pero dicho enunciado tiene una complejidad baja, y por lo tanto, por el *teorema de absoluteness de Schoenfield*, es *absoluto*



Una *forma débil* de la conjetura de Schanuel sería la siguiente:

## Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).
- 4 Por lo tanto, el enunciado del teorema de Wilkie y Kirby es consistente con ZFE.
- 5 Pero dicho enunciado tiene una complejidad baja, y por lo tanto, por el *teorema de absolutez de Schoenfield*, es *absoluto* (si es consistente con ZFE entonces es un teorema de ZFE).





Una *forma débil* de la conjetura de Schanuel sería la siguiente:

## Demostración del teorema anterior por Viale:

- 1 Realizar una construcción de forzamiento (colapso de Lévy) para obtener  $\mathbb{V}[G] \supseteq \mathbb{V}$  tal que  $k := \mathbb{C} \cap \mathbb{V}$  es numerable.
- 2 En  $\mathbb{V}[G]$ , tenemos que  $k$  es numerable, algebraica y exponencialmente cerrado.
- 3 Además, se satisface la conjetura de Schanuel sobre  $k$  (básicamente, todo elemento de  $\mathbb{C} \setminus k$  es muy, muy indescriptible en términos de  $k$ ).
- 4 Por lo tanto, el enunciado del teorema de Wilkie y Kirby es consistente con ZFE.
- 5 Pero dicho enunciado tiene una complejidad baja, y por lo tanto, por el *teorema de absoluteness de Schoenfield*, es *absoluto* (si es consistente con ZFE entonces es un teorema de ZFE).
- 6 Por lo tanto, el enunciado es un teorema de ZFE.



# En conclusión...



## En conclusión...



Hacer Matemáticas sin saber  
Teoría de Conjuntos



Hacer Matemáticas utilizando  
herramientas conjuntistas



Instituto  
Politécnico  
Nacional

## En conclusión...



Hacer Matemáticas sin saber  
Teoría de Conjuntos



Hacer Matemáticas utilizando  
herramientas conjuntistas

**!!!Muchísimas gracias!!!**



Instituto  
Politécnico  
Nacional