Sabores de la Teoría de Números
I. La Teoría Algebraica

Tim Gendron
Instituto de Matemáticas, Universidad Nacional Autónoma de México

26 junio 2017

Introducción

En 1900, en el Congreso Internacional de Matemáticas de Paris, En 1900, en el Congreso Internacional de Matemáticas de Paris, el matemático aleman David Hilbert presentó una lista de veintitrés problemas

Los Problemas de Hilbert

En 1900, en el Congreso Internacional de Matemáticas de Paris, el matemático aleman David Hilbert presentó una lista de veintitrés problemas que él consideró bien motivados, desafiantes y suficientemente abiertos para estimular investigación por un siglo.

En 1900, en el Congreso Internacional de Matemáticas de Paris, el matemático aleman David Hilbert presentó una lista de veintitrés problemas que él consideró bien motivados, desafiantes y suficientemente abiertos para estimular investigación por un siglo.

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert:

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**)

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea* K *un* **campo global**

El Duodécimo Problema

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea K un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q}$$

El Duodécimo Problema

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea* K *un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q} \quad o \quad K/\mathbb{F}(T)$$

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea K un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q} \quad \text{o} \quad K/\mathbb{F}(T)$$

donde

- $\mathbb{Q} =$ *es el campo de los racionales*

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea K un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q} \quad \text{o} \quad K/\mathbb{F}(T)$$

donde

- $\mathbb{Q} =$ *es el campo de los racionales y*
- $\mathbb{F}(T) =$ *el campo de funciones racionales sobre un campo finito* $\mathbb{F}$.

En este momento sólo quedan tres problemas abiertos en la lista de Hilbert: entre ellos el octavo (la **Hipótesis de Riemann**) y el duodécimo:

Duodécimo Problema de Hilbert. *Sea K un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q} \quad \text{o} \quad K/\mathbb{F}(T)$$

donde

- $\mathbb{Q} =$ *es el campo de los racionales y*
- $\mathbb{F}(T) =$ *el campo de funciones racionales sobre un campo finito* $\mathbb{F}$.

Da una descripción explícita de cada **campo de clase**

$$K^{\mathfrak{m}}/K.$$

Propósito del MiniCurso

El propósito de este mini-curso es explicar lo necesario de la teoría de números para entender las afirmaciones de

Propósito del MiniCurso

El propósito de este mini-curso es explicar lo necesario de la teoría de números para entender las afirmaciones de

1. El Duodécimo Problema de Hilbert.

Propósito del MiniCurso

El propósito de este mini-curso es explicar lo necesario de la teoría de números para entender las afirmaciones de

1. El Duodécimo Problema de Hilbert.
2. El Teorema de Weber-Fueter, que da una solución en el caso de $K/\mathbb{Q}$ cuadrática y compleja.

Propósito del MiniCurso

El propósito de este mini-curso es explicar lo necesario de la teoría de números para entender las afirmaciones de

1. El Duodécimo Problema de Hilbert.
2. El Teorema de Weber-Fueter, que da una solución en el caso de $K/\mathbb{Q}$ cuadrática y compleja.
3. Un teorema nuestro que da una solución en un nuevo caso: lo de $K/\mathbb{F}(T)$ cuadrática y real.

Propósito del MiniCurso

El propósito de este mini-curso es explicar lo necesario de la teoría de números para entender las afirmaciones de

1. El Duodécimo Problema de Hilbert.
2. El Teorema de Weber-Fueter, que da una solución en el caso de $K/\mathbb{Q}$ cuadrática y compleja.
3. Un teorema nuestro que da una solución en un nuevo caso: lo de $K/\mathbb{F}(T)$ cuadrática y real.

Este tarea nos conduce a explorar cuatro sabores de la teoría de números: lo algebraico, lo analítico lo geométrico y lo cuántico.

Campos y sus Extensiones

Sea K un campo.

Sea K un campo. Si $L \supset K$ es otro campo decimos que L es campo extensión

Extensiones

Sea K un campo. Si $L \supset K$ es otro campo decimos que L es campo extensión y escribimos

$$L/K \quad \text{o} \quad \begin{array}{c} L \\ | \\ K \end{array}$$

Sea K un campo. Si $L \supset K$ es otro campo decimos que L es campo extensión y escribimos

$$L/K \quad \text{o} \quad \begin{array}{c} L \\ | \\ K \end{array}$$

Si L/K, L es K-espacio vectorial.

Extensiones

Sea K un campo. Si $L \supset K$ es otro campo decimos que L es campo extensión y escribimos

$$L/K \quad \text{o} \quad \begin{array}{c} L \\ \Big| \\ K \end{array}$$

Si L/K, L es K-espacio vectorial. El **grado** es

$$[L : K] := \dim_K L.$$

Sea K un campo. Si $L \supset K$ es otro campo decimos que L es campo extensión y escribimos

$$L/K \quad \text{o} \quad \begin{array}{c} L \\ | \\ K \end{array}$$

Si L/K, L es K-espacio vectorial. El **grado** es

$$[L : K] := \dim_K L.$$

Si $[L : K] < \infty$ decimos que la extensión es **finita**.

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Ejemplo. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$.

Algebraicidad

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Ejemplo. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$.

Teorema de Lindemann-Weierstraß (1882, 1885)**.** π *no es algebraico sobre* $\mathbb{Q}$ *i.e. es* ***trascendente****.*

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Ejemplo. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$.

Teorema de Lindemann-Weierstraß (1882, 1885)**.** π *no es algebraico sobre* $\mathbb{Q}$ *i.e. es* **trascendente***.*

Si cada $\alpha \in L$ es algebraico sobre K decimos que L/K es algebraica.

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Ejemplo. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$.

Teorema de Lindemann-Weierstraß (1882, 1885). π *no es algebraico sobre* $\mathbb{Q}$ *i.e. es* **trascendente**.

Si cada $\alpha \in L$ es algebraico sobre K decimos que L/K es algebraica.

Teorema. *Si* L/K *es finita, es algebraica.*

Algebraicidad

Dada L/K, decimos que $\alpha \in L$ es **algebraico** sobre K si

$$f(\alpha) = 0 \text{ por algún polinomio } f(X) \in K[X].$$

Ejemplo. $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$.

Teorema de Lindemann-Weierstraß (1882, 1885)**.** *π no es algebraico sobre $\mathbb{Q}$ i.e. es* **trascendente***.*

Si cada $\alpha \in L$ es algebraico sobre K decimos que L/K es algebraica.

Teorema. *Si L/K es finita, es algebraica.*

La **Teoría de Números Algebraicos** es el estudio de la aritmética de extensiónes algebraicas de $\mathbb{Q}$, $\mathbb{F}(T)$ y sus **localizaciones** (completaciónes topológicas).

Un campo $\mathbb{C}$ es **algebraicamente cerrado**

Cerradura Algebraica

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado,

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} |\ \alpha \text{ es algebraica sobre } K\}.$$

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} |\ \alpha \text{ es algebraica sobre } K\}.$$

$\overline{K}$ es un campo extensión de K que es algebraica pero en general $[\overline{K} : K] = \infty$.

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} | \ \alpha \text{ es algebraica sobre } K\}.$$

$\overline{K}$ es un campo extensión de K que es algebraica pero en general $[\overline{K} : K] = \infty$. Es única salvo isomorfismo.

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} |\ \alpha \text{ es algebraica sobre } K\}.$$

$\overline{K}$ es un campo extensión de K que es algebraica pero en general $[\overline{K} : K] = \infty$. Es única salvo isomorfismo.
Si L/K y $L \subset \overline{K}$,

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. *$\mathbb{C}$ es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} |\ \alpha \text{ es algebraica sobre } K\}.$$

$\overline{K}$ es un campo extensión de K que es algebraica pero en general $[\overline{K} : K] = \infty$. Es única salvo isomorfismo.
Si L/K y $L \subset \overline{K}$, existe un conjunto $\{\alpha_\iota\}_{\iota \in I} \subset \overline{K}$ tal que

$$L = K(\alpha_\iota | \iota \in I),$$

Un campo $\mathbf{C}$ es **algebraicamente cerrado** si cada polinomio $f(X) \in \mathbf{C}[X]$ tiene solución en $\mathbf{C}$.

Teorema Fundamental de la Aritmética. $\mathbb{C}$ *es algebraicamente cerrado.*

Si $K \subset \mathbf{C}$ y $\mathbf{C}$ es algebraicamente cerrado, la **cerradura algebraica** de K en $\mathbf{C}$ es

$$\overline{K} = \{\alpha \in \mathbf{C} |\ \alpha \text{ es algebraica sobre } K\}.$$

$\overline{K}$ es un campo extensión de K que es algebraica pero en general $[\overline{K} : K] = \infty$. Es única salvo isomorfismo.
Si L/K y $L \subset \overline{K}$, existe un conjunto $\{\alpha_\iota\}_{\iota \in I} \subset \overline{K}$ tal que

$$L = K(\alpha_\iota | \iota \in I),$$

i.e. L es el **campo generado** por $\{\alpha_\iota\}_{\iota \in I}$.

Teoría de Galois

M/K, $M \subset \overline{K}$, es de **Galois**

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\text{Raices}(f(X)) \subset M \quad \text{o} \quad \text{Raices}(f(X)) \cap M = \emptyset.$$

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\text{Raices}(f(X)) \subset M \quad \text{o} \quad \text{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\text{Gal}(L/K) := \{\sigma \in \text{Aut}(L) |\ \sigma|_K = \text{id}\}.$$

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\text{Raices}(f(X)) \subset M \quad \text{o} \quad \text{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\text{Gal}(L/K) := \{\sigma \in \text{Aut}(L) |\ \sigma|_K = \text{id}\}.$$

Teorema. $\#\text{Gal}(L/K) = [L : K]$.

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\mathrm{Raices}(f(X)) \subset M \quad \text{o} \quad \mathrm{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\mathrm{Gal}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}\}.$$

Teorema. $\#\mathrm{Gal}(L/K) = [L : K]$.

Ejemplo. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ donde

$$\sigma(x + y\sqrt{2}) = x - y\sqrt{2}.$$

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\text{Raices}(f(X)) \subset M \quad \text{o} \quad \text{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\text{Gal}(L/K) := \{\sigma \in \text{Aut}(L) |\ \sigma|_K = \text{id}\}.$$

Teorema. $\#\text{Gal}(L/K) = [L : K]$.

Ejemplo. $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \sigma\}$ donde

$$\sigma(x + y\sqrt{2}) = x - y\sqrt{2}.$$

El grupo de Galois no es necesariamente abeliana

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\mathrm{Raices}(f(X)) \subset M \quad \text{o} \quad \mathrm{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\mathrm{Gal}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}\}.$$

Teorema. $\#\mathrm{Gal}(L/K) = [L : K]$.

Ejemplo. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ donde

$$\sigma(x + y\sqrt{2}) = x - y\sqrt{2}.$$

El grupo de Galois no es necesariamente abeliana e.g. $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$.

M/K, $M \subset \overline{K}$, es de **Galois** si para cada $f(X) \in K[X]$

$$\text{Raices}(f(X)) \subset M \quad \text{o} \quad \text{Raices}(f(X)) \cap M = \emptyset.$$

El **grupo de Galois** es

$$\text{Gal}(L/K) := \{\sigma \in \text{Aut}(L) | \ \sigma|_K = \text{id}\}.$$

Teorema. $\#\text{Gal}(L/K) = [L : K]$.

Ejemplo. $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \sigma\}$ donde

$$\sigma(x + y\sqrt{2}) = x - y\sqrt{2}.$$

El grupo de Galois no es necesariamente abeliana e.g. $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$. Cuando lo es decimos que L/K es **abeliana**.

Sea M/K de Galois.

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M |\ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M |\ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

es un campo intermedio: el **campo fijo** de H.

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M \mid \sigma(x) = x \text{ para todo } \sigma \in H\}$$

es un campo intermedio: el **campo fijo** de H.

- Reciprocamente, si

$$K \subset L \subset M,$$

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M|\ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

  es un campo intermedio: el **campo fijo** de H.
- Reciprocamente, si

$$K \subset L \subset M,$$

  la extensión M/L siempre es de Galois

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M | \ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

  es un campo intermedio: el **campo fijo** de H.
- Reciprocamente, si

$$K \subset L \subset M,$$

  la extensión M/L siempre es de Galois y define un subgrupo del grupo de $\mathrm{Gal}(M/K)$:

Sea M/K de Galois.

- Si $H < \text{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M | \ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

es un campo intermedio: el **campo fijo** de H.

- Reciprocamente, si

$$K \subset L \subset M,$$

la extensión M/L siempre es de Galois y define un subgrupo del grupo de $\text{Gal}(M/K)$:

$$H_L = \text{Gal}(M/L)$$

Sea M/K de Galois.

- Si $H < \mathrm{Gal}(M/K)$, el conjunto

$$L_H = \{x \in M | \ \sigma(x) = x \text{ para todo } \sigma \in H\}$$

es un campo intermedio: el **campo fijo** de H.

- Reciprocamente, si

$$K \subset L \subset M,$$

la extensión M/L siempre es de Galois y define un subgrupo del grupo de $\mathrm{Gal}(M/K)$:

$$H_L = \mathrm{Gal}(M/L) = \{\sigma \in \mathrm{Gal}(M/K) | \ \sigma|_L = \mathrm{id}\}.$$

Teorema Fundamental de la Teoría de Galois. *La asociación* $L \mapsto H_L$

Teorema Fundamental de la Teoría de Galois. *La asociación $L \mapsto H_L$ induce una biyección entre extensiónes de Galois intermedias L/K y subgrupos normales $N_L \lhd \mathrm{Gal}(M/K)$.*

Teorema Fundamental de la Teoría de Galois. *La asociación $L \mapsto H_L$ induce una biyección entre extensiónes de Galois intermedias L/K y subgrupos normales $N_L \lhd \mathsf{Gal}(M/K)$. Tenemos*

$$\mathsf{Gal}(L/K) \cong \mathsf{Gal}(M/K)/N_L.$$

Teorema Fundamental

Teorema Fundamental de la Teoría de Galois. *La asociación $L \mapsto H_L$ induce una biyección entre extensiónes de Galois intermedias L/K y subgrupos normales $N_L \lhd \mathrm{Gal}(M/K)$. Tenemos*

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K)/N_L.$$

$$\begin{tikzcd}
M \arrow[d, dash, "\circlearrowleft \mathrm{Gal}(M/L)=N_L"] \\
L \arrow[d, dash, "\circlearrowleft \mathrm{Gal}(L/K)\cong\mathrm{Gal}(M/K)/N_L"] \\
K
\end{tikzcd}$$

El Teorema Fundamental de la Teoría de Galois

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**:

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir “desde arriba hacia abajo”

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir “desde arriba hacia abajo” cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \text{Gal}(M/K)$ actuando en M.

Resumen

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \mathrm{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**:

Resumen

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \mathrm{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**: que sólo requiere conocimiento de K para construir "desde abajo hacia arriba" todas las extensiónes algebraicas de K.

Resumen

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \text{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**: que sólo requiere conocimiento de K para construir "desde abajo hacia arriba" todas las extensiónes algebraicas de K. Mas precisamente, buscamos un grupo intrínsico

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \mathrm{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**: que sólo requiere conocimiento de K para construir "desde abajo hacia arriba" todas las extensiónes algebraicas de K. Mas precisamente, buscamos un grupo intrínsico i.e. construido por el campo base K, El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \text{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**: que sólo requiere conocimiento de K para construir "desde abajo hacia arriba" todas las extensiónes algebraicas de K. Mas precisamente, buscamos un grupo intrínsico i.e. construido por el campo base K, cuyos subgrupos normales indexan las extensiones de Galois de K

El Teorema Fundamental de la Teoría de Galois es un ejemplo de un resultado basado en **conocimiento relativo**: dado conocimiento de una extensión de Galois M/K, podemos construir "desde arriba hacia abajo" cada campo extensión de Galois L/K contenida en M/K, como el campo fijo L_N de un subgrupo $N \lhd \mathrm{Gal}(M/K)$ actuando en M.

Problema Absoluto. Encontrar una versión del Teorema Fundamental basado en **conocimiento absoluto**: que sólo requiere conocimiento de K para construir "desde abajo hacia arriba" todas las extensiónes algebraicas de K. Mas precisamente, buscamos un grupo intrínsico i.e. construido por el campo base K, cuyos subgrupos normales indexan las extensiones de Galois de K y además, nos permite construirlas explícitamente.

Digresión: Grupo Fundamental

Sea X un espacio topológico.

Sea X un espacio topológico. Su **grupo fundamental** es

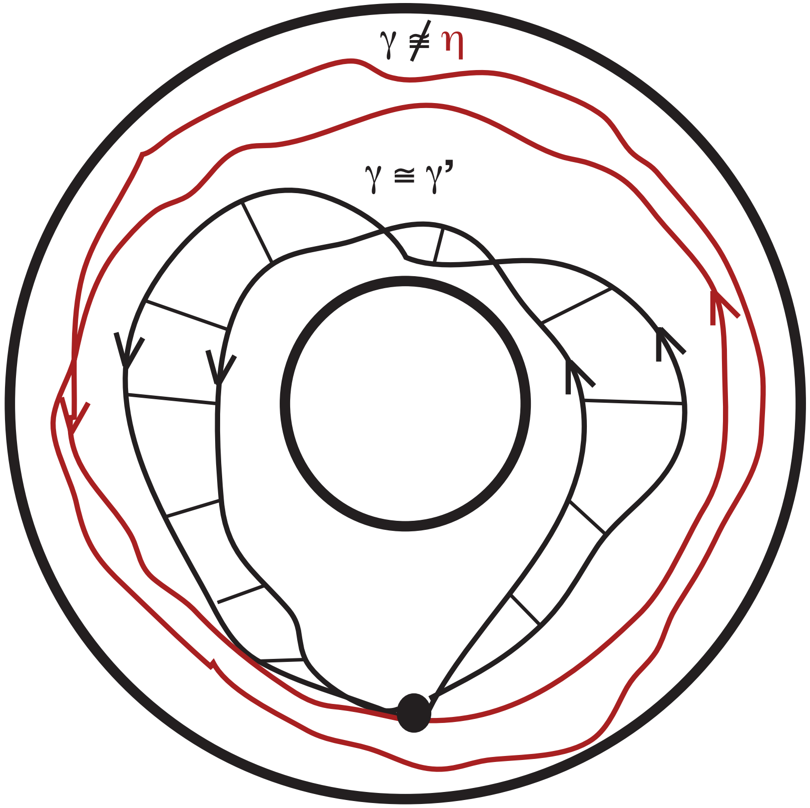
$$\pi_1 X = \{\text{lazos basados en un punto fijo } x_0 \in X\}/\text{homotopía.}$$

Grupo Fundamental

Sea X un espacio topológico. Su **grupo fundamental** es

$$\pi_1 X = \{\text{lazos basados en un punto fijo } x_0 \in X\}/\text{homotopía.}$$

Ejemplo. $\pi_1\mathbb{R} = 1, \pi_1\mathbb{S}^1 = \mathbb{Z}$.



$$\pi_1 X \cong \mathbb{Z}$$

Un **cubriente (no ramificado)**

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U.

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U. A veces escribimos

$$Y/X,$$

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U. A veces escribimos

$$Y/X,$$

y definimos el **grado** como $[Y : X] := \#\rho^{-1}(x)$, $x \in X$.

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U. A veces escribimos

$$Y/X,$$

y definimos el **grado** como $[Y : X] := \#\rho^{-1}(x)$, $x \in X$. Definimos

$$\mathrm{Aut}(Y/X) = \{\sigma \in \mathrm{Homeo}(Y) |\ \sigma \circ \rho = \rho\}.$$

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U. A veces escribimos

$$Y/X,$$

y definimos el **grado** como $[Y : X] := \#\rho^{-1}(x)$, $x \in X$. Definimos

$$\mathrm{Aut}(Y/X) = \{\sigma \in \mathrm{Homeo}(Y) | \ \sigma \circ \rho = \rho\}.$$

Si $\#\mathrm{Aut}(Y/X) = [Y : X]$ decimos que Y/X es de **Galois**

Un **cubriente (no ramificado)** es un mapeo suprayectivo

$$\rho : Y \to X$$

tal que para cada $x \in X$ existe una vecindad $U \ni x$ en la cual los componentes de $\rho^{-1}(U)$ mapean homeomorficamente sobre U. A veces escribimos

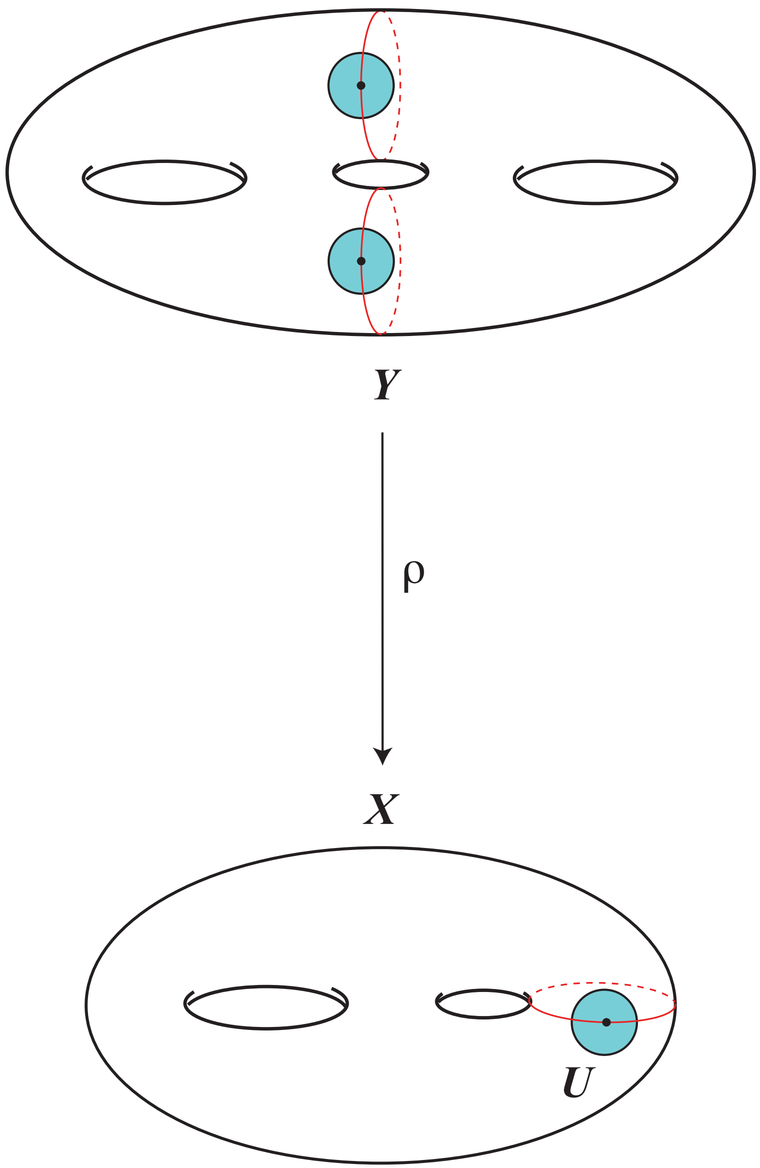
$$Y/X,$$

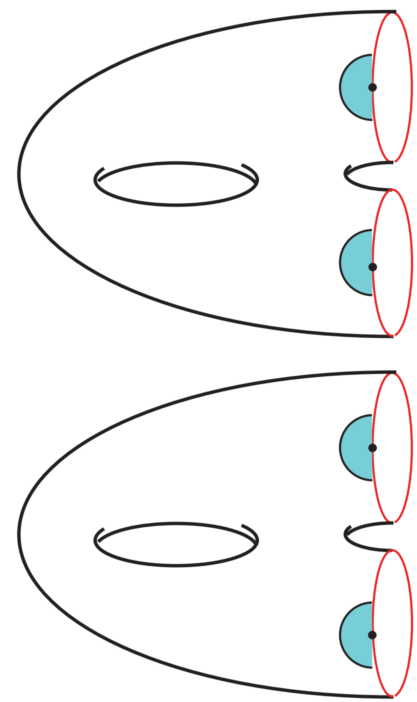
y definimos el **grado** como $[Y : X] := \#\rho^{-1}(x)$, $x \in X$. Definimos

$$\mathrm{Aut}(Y/X) = \{\sigma \in \mathrm{Homeo}(Y) | \ \sigma \circ \rho = \rho\}.$$

Si $\#\mathrm{Aut}(Y/X) = [Y : X]$ decimos que Y/X es de **Galois** y escribimos

$$\mathrm{Gal}(Y/X) := \mathrm{Aut}(Y/X).$$


Y
ρ
X
U



Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

$$K_\Sigma = \{f : \Sigma \to \mathbb{C} \text{ meromorfa}\}.$$

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

$$K_\Sigma = \{f : \Sigma \to \mathbb{C} \text{ meromorfa}\}.$$

Ejemplo. Sea $\Sigma = \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ la **esfera de Riemann**.

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

$$K_\Sigma = \{f : \Sigma \to \mathbb{C} \text{ meromorfa}\}.$$

Ejemplo. Sea $\Sigma = \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ la **esfera de Riemann**.

$$K_{\hat{\mathbb{C}}} = \mathbb{C}(X) = \{f(X)/g(X) | \ f(X), g(X) \in \mathbb{C}[X]\}.$$

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

$$K_\Sigma = \{f : \Sigma \to \mathbb{C} \text{ meromorfa}\}.$$

Ejemplo. Sea $\Sigma = \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ la **esfera de Riemann**.

$$K_{\hat{\mathbb{C}}} = \mathbb{C}(X) = \{f(X)/g(X) |\ f(X), g(X) \in \mathbb{C}[X]\}.$$

Teorema. Σ_1/Σ_2 *es de Galois* $\Leftrightarrow K_{\Sigma_1}/K_{\Sigma_2}$ *es de Galois*

Superficies de Riemann y Campos de Funciones

Una superficie Σ dotada con un atlas compleja cuyas transiciones son holomorfas se llama **superficie de Riemann**.
A cada superficie de Riemann se puede asociar su campo de funciones meromorfas

$$K_\Sigma = \{f : \Sigma \to \mathbb{C} \text{ meromorfa}\}.$$

Ejemplo. Sea $\Sigma = \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ la **esfera de Riemann**.

$$K_{\hat{\mathbb{C}}} = \mathbb{C}(X) = \{f(X)/g(X) |\ f(X), g(X) \in \mathbb{C}[X]\}.$$

Teorema. *Σ_1/Σ_2 es de Galois $\Leftrightarrow$ $K_{\Sigma_1}/K_{\Sigma_2}$ es de Galois y*

$$\mathrm{Gal}(\Sigma_1/\Sigma_2) \cong \mathrm{Gal}(K_{\Sigma_1}/K_{\Sigma_2}).$$

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado**

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$ tal que el mapeo

$$\rho : Y - \bigcup \rho^{-1}(x_i) \longrightarrow X - \bigcup x_i$$

es cubriente.

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$ tal que el mapeo

$$\rho : Y - \bigcup \rho^{-1}(x_i) \longrightarrow X - \bigcup x_i$$

es cubriente. Los puntos x_i son los **puntos de ramificación**.

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$ tal que el mapeo

$$\rho : Y - \bigcup \rho^{-1}(x_i) \longrightarrow X - \bigcup x_i$$

es cubriente. Los puntos x_i son los **puntos de ramificación**.

Ejemplo. El mapeo

$$\rho : \mathbb{C} \to \mathbb{C}, \quad \rho(z) = z^n$$

es cubriente con punto de ramificación $z = 0$.

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$ tal que el mapeo

$$\rho : Y - \bigcup \rho^{-1}(x_i) \longrightarrow X - \bigcup x_i$$

es cubriente. Los puntos x_i son los **puntos de ramificación**.

Ejemplo. El mapeo

$$\rho : \mathbb{C} \to \mathbb{C}, \quad \rho(z) = z^n$$

es cubriente con punto de ramificación $z = 0$. Cada superficie de Riemann compacta tiene un cubriente ramificado

$$\rho : \Sigma \longrightarrow \hat{\mathbb{C}}.$$

Cubrientes Ramificados

Un mapeo $\rho : Y \to X$ es un **cubriente ramificado** si existe un conjunto discreto de puntos $\{x_i\} \subset X$ tal que el mapeo

$$\rho : Y - \bigcup \rho^{-1}(x_i) \longrightarrow X - \bigcup x_i$$

es cubriente. Los puntos x_i son los **puntos de ramificación**.

Ejemplo. El mapeo

$$\rho : \mathbb{C} \to \mathbb{C}, \quad \rho(z) = z^n$$

es cubriente con punto de ramificación $z = 0$. Cada superficie de Riemann compacta tiene un cubriente ramificado

$$\rho : \Sigma \longrightarrow \hat{\mathbb{C}}.$$

Así que pensamos en $\hat{\mathbb{C}}$ como “superficie base”: el análogo de $\mathbb{Q}$.

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$,

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**.

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**. *Tenemos*

$$\mathrm{Gal}(\tilde{X}/X) \cong \pi_1 X.$$

Teorema Fundamental de Cubrientes

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**. *Tenemos*

$$\mathrm{Gal}(\tilde{X}/X) \cong \pi_1 X.$$

Teorema Fundamental de Cubrientes. *Hay una biyección*

$$\{N \lhd \pi_1 X\} \longleftrightarrow \{\textit{cubrientes de Galois } X_N \to X\}$$

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**. *Tenemos*

$$\mathrm{Gal}(\tilde{X}/X) \cong \pi_1 X.$$

Teorema Fundamental de Cubrientes. *Hay una biyección*

$$\{N \lhd \pi_1 X\} \longleftrightarrow \{\textit{cubrientes de Galois } X_N \to X\}$$

donde

$$X_N = \tilde{X}/N,$$

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**. *Tenemos*

$$\mathrm{Gal}(\tilde{X}/X) \cong \pi_1 X.$$

Teorema Fundamental de Cubrientes. *Hay una biyección*

$$\{N \lhd \pi_1 X\} \longleftrightarrow \{\textit{cubrientes de Galois } X_N \to X\}$$

donde

$$X_N = \tilde{X}/N, \quad \mathrm{Gal}(X_N/X) \cong \pi_1 X/N.$$

Teorema Fundamental de Cubrientes

Teorema. *Existe un cubriente de Galois* $\rho : \tilde{X} \longrightarrow X$ *con* $\pi_1 \tilde{X} = 1$, *llamado el* **cubriente universal**. *Tenemos*

$$\mathrm{Gal}(\tilde{X}/X) \cong \pi_1 X.$$

Teorema Fundamental de Cubrientes. *Hay una biyección*

$$\{N \lhd \pi_1 X\} \longleftrightarrow \{\text{cubrientes de Galois } X_N \to X\}$$

donde

$$X_N = \tilde{X}/N, \quad \mathrm{Gal}(X_N/X) \cong \pi_1 X/N.$$

Nota. Desafortunadamente, el Teorema Fundamental de Cubrientes sólo comprende los cubrientes no ramificados de K.

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación**

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann definimos

$$\pi_1 K := \pi_1 \Sigma$$

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann definimos

$$\pi_1 K := \pi_1 \Sigma$$

y por el diccionario entre extensiónes de Galois de K y cubrientes de Galois de Σ,

Motivación

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann definimos

$$\pi_1 K := \pi_1 \Sigma$$

y por el diccionario entre extensiónes de Galois de K y cubrientes de Galois de Σ, tenemos el analogo del Teorema Fundamental de Cubrientes.

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann definimos

$$\pi_1 K := \pi_1 \Sigma$$

y por el diccionario entre extensiónes de Galois de K y cubrientes de Galois de Σ, tenemos el analogo del Teorema Fundamental de Cubrientes.

El Ejemplo indica que una posible solución del **Problema Absoluto**

Idea. Buscar una noción de de grupo fundamental

$$\pi_1 K$$

para cada campo K y demostrar un análogo del Teorema Fundamental de Cubrientes **que admite ramificación** para soluciónar el **Problema Absoluto**.

Ejemplo. Si $K = K_\Sigma$ donde Σ es superficie de Riemann definimos

$$\pi_1 K := \pi_1 \Sigma$$

y por el diccionario entre extensiónes de Galois de K y cubrientes de Galois de Σ, tenemos el analogo del Teorema Fundamental de Cubrientes.

El Ejemplo indica que una posible solución del **Problema Absoluto** puede ser encontrado por una **geometrización** Σ_K del campo K.

Enteros

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**.

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico**

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \textit{ entero sobre } \mathbb{Q}\}$$

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ entero sobre } \mathbb{Q}\}$$

es un **dominio de Dedekind***:*

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ entero sobre } \mathbb{Q}\}$$

es un ***dominio de Dedekind****: un dominio entero que cuenta con factorisación única de ideales en ideales primos:*

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ entero sobre } \mathbb{Q}\}$$

es un **dominio de Dedekind***: un dominio entero que cuenta con factorisación única de ideales en ideales primos: para cada ideal* $\mathfrak{a} \subset \mathcal{O}_K$

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ entero sobre } \mathbb{Q}\}$$

es un **dominio de Dedekind***: un dominio entero que cuenta con factorisación única de ideales en ideales primos: para cada ideal* $\mathfrak{a} \subset \mathcal{O}_K$

$$\mathfrak{a} = \prod \mathfrak{p}_i^{n_i},$$

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ entero sobre } \mathbb{Q}\}$$

es un **dominio de Dedekind***: un dominio entero que cuenta con factorisación única de ideales en ideales primos: para cada ideal* $\mathfrak{a} \subset \mathcal{O}_K$

$$\mathfrak{a} = \prod \mathfrak{p}_i^{n_i},$$

donde los $\mathfrak{p}_i$ *son ideales primos.*

Sea $K/\mathbb{Q}$ una extensión finita i.e. un **campo numérico**. $\alpha \in K$ es **entero** sobre $\mathbb{Q}$ si existe $f(X) \in \mathbb{Z}[X]$ **mónico** tal que $f(\alpha) = 0$.

Teorema. *El conjunto*

$$\mathcal{O}_K = \{\alpha \in K \text{ \textit{entero sobre} } \mathbb{Q}\}$$

es un **dominio de Dedekind***: un dominio entero que cuenta con factorisación única de ideales en ideales primos: para cada ideal* $\mathfrak{a} \subset \mathcal{O}_K$

$$\mathfrak{a} = \prod \mathfrak{p}_i^{n_i},$$

donde los $\mathfrak{p}_i$ *son ideales primos.*

Así que existe una **aritmética** de ideales.

El **espectro** de $\mathcal{O}_K$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**:

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \mathfrak{p}|\mathfrak{a}\}$.

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_\mathfrak{a} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión,

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K),$$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_\mathfrak{a} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_\mathfrak{a} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

Para $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$,

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

Para $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$,

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}_i \in \rho^{-1}(\mathfrak{p})} \mathfrak{P}_i^{n_i}.$$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

Para $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$,

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}_i \in \rho^{-1}(\mathfrak{p})} \mathfrak{P}_i^{n_i}.$$

Escribimos $\mathfrak{P}_i|\mathfrak{p}$.

El **espectro** de $\mathcal{O}_K$ es

$$\operatorname{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \operatorname{Spec}(\mathcal{O}_L) \longrightarrow \operatorname{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

Para $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$,

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}_i \in \rho^{-1}(\mathfrak{p})} \mathfrak{P}_i^{n_i}.$$

Escribimos $\mathfrak{P}_i|\mathfrak{p}$. Decimos que L/K es **no ramificado** en $\mathfrak{p}$

El **espectro** de $\mathcal{O}_K$ es

$$\mathrm{Spec}(\mathcal{O}_K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ primo}\}$$

un espacio topológico con la **topología de Zariski**: generado por la base de cerrados $\mathcal{U}_{\mathfrak{a}} = \{\mathfrak{p} : \ \mathfrak{p}|\mathfrak{a}\}$. Si L/K es una extensión, $\mathcal{O}_K \subset \mathcal{O}_L$ y hay un mapeo sobre

$$\rho : \mathrm{Spec}(\mathcal{O}_L) \longrightarrow \mathrm{Spec}(\mathcal{O}_K), \quad \mathfrak{P} \mapsto \mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K.$$

Para $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$,

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}_i \in \rho^{-1}(\mathfrak{p})} \mathfrak{P}_i^{n_i}.$$

Escribimos $\mathfrak{P}_i|\mathfrak{p}$. Decimos que L/K es **no ramificado** en $\mathfrak{p}$ si $n_i = 1$ para todo $\mathfrak{P}_i|\mathfrak{p}$.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. El ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$ no es principal.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. El ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$ no es principal.

El conjunto de ideales forma un monoïde con identidad $(1) = \mathcal{O}_K$.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. El ideal $\mathfrak{a} = (2, 1 + \sqrt{-5})$ no es principal.

El conjunto de ideales forma un monoïde con identidad $(1) = \mathcal{O}_K$. Un **ideal fraccionario** es un $\mathcal{O}_K$ módulo

$$\mathfrak{a} \subset K$$

finitamente generado.

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. El ideal $\mathfrak{a} = (2, 1 + \sqrt{-5})$ no es principal.

El conjunto de ideales forma un monoïde con identidad $(1) = \mathcal{O}_K$. Un **ideal fraccionario** es un $\mathcal{O}_K$ módulo

$$\mathfrak{a} \subset K$$

finitamente generado. El producto de ideales fraccionarios es

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i \middle| \; a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

En general no es el caso que cada ideal $\mathfrak{a} \subset \mathcal{O}_K$ es principal.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$. Luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. El ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$ no es principal.

El conjunto de ideales forma un monoïde con identidad $(1) = \mathcal{O}_K$. Un **ideal fraccionario** es un $\mathcal{O}_K$ módulo

$$\mathfrak{a} \subset K$$

finitamente generado. El producto de ideales fraccionarios es

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i \middle| \ a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

y el inverso multiplicativo es

$$\mathfrak{a}^{-1} := \{x \in K | \ x\mathfrak{a} \subset \mathcal{O}_K\}.$$

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$.

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathsf{Cl}_K = \mathsf{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathsf{Cl}_K = \mathsf{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea* $K = \mathbb{Q}(\sqrt{D})$ *cuadrático.*

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea* $K = \mathbb{Q}(\sqrt{D})$ *cuadrático.*

- $h_K \to \infty$ *cuando* $D \to -\infty$.

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea* $K = \mathbb{Q}(\sqrt{D})$ *cuadrático.*

- $h_K \to \infty$ *cuando* $D \to -\infty$. *Heilbronn (1934).*

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea $K = \mathbb{Q}(\sqrt{D})$ cuadrático.*

- $h_K \to \infty$ *cuando* $D \to -\infty$. *Heilbronn (1934).*
- *Si* $D < 0$, $h_K = 1 \Leftrightarrow -D = 1, 2, 3, 7, 11, 19, 43, 67, 163$

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea $K = \mathbb{Q}(\sqrt{D})$ cuadrático.*

- $h_K \to \infty$ *cuando* $D \to -\infty$. *Heilbronn (1934).*
- *Si* $D < 0$, $h_K = 1 \Leftrightarrow -D = 1, 2, 3, 7, 11, 19, 43, 67, 163$
  Heegner (1952), Baker (1966), Stark (1967).

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea* $K = \mathbb{Q}(\sqrt{D})$ *cuadrático.*

- $h_K \to \infty$ *cuando* $D \to -\infty$. *Heilbronn (1934).*
- *Si* $D < 0$, $h_K = 1 \Leftrightarrow -D = 1, 2, 3, 7, 11, 19, 43, 67, 163$
  Heegner (1952), Baker (1966), Stark (1967).
- *Si* $D > 0$, *hay un número infinito de campos cuadráticos con* $h_K = 1$.

Así que el conjunto de ideales fraccionarios es un grupo multiplicativo $\mathcal{I}_{\mathcal{O}_K}$, con subgrupo de ideales principales fraccionarios $\mathcal{P}_{\mathcal{O}_K}$. El **grupo de clases de ideales** es

$$\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K} := \mathcal{I}_{\mathcal{O}_K} / \mathcal{P}_{\mathcal{O}_K}.$$

Teorema. Cl_K *es un grupo finito.*

La cardinalidad h_K de Cl_K se llama el **número de clase**.

El Problema del Numero de Clase Uno (Gauß 1801). *Sea $K = \mathbb{Q}(\sqrt{D})$ cuadrático.*

- *$h_K \to \infty$ cuando $D \to -\infty$. Heilbronn (1934).*
- *Si $D < 0$, $h_K = 1 \Leftrightarrow -D = 1, 2, 3, 7, 11, 19, 43, 67, 163$*
  Heegner (1952), Baker (1966), Stark (1967).
- *Si $D > 0$, hay un número infinito de campos cuadráticos con $h_K = 1$. Abierto*

Teoría de Campos de Clase

El **campo de clase de Hilbert**

$$H_K/K$$

El **campo de clase de Hilbert**

$$H_K/K$$

es la máxima extensión abeliana y no ramificada.

El **campo de clase de Hilbert**

$$H_K/K$$

es la máxima extensión abeliana y no ramificada.

Teorema (Hilbert). $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}_K.$

El **campo de clase de Hilbert**

$$H_K/K$$

es la máxima extensión abeliana y no ramificada.

Teorema (Hilbert)**.** $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}_K.$

Corolario. *Sólo hay un número finitos de L/K no ramificada.*

El **campo de clase de Hilbert**

$$H_K/K$$

es la máxima extensión abeliana y no ramificada.

Teorema (Hilbert)**.** $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}_K$.

Corolario. *Sólo hay un número finitos de L/K no ramificada.*

Nota. Para superficies de Riemann hay un número infinito de cubrientes no ramificados.

El **campo de clase de Hilbert**

$$H_K/K$$

es la máxima extensión abeliana y no ramificada.

Teorema (Hilbert)**.** $\mathsf{Gal}(H_K/K) \cong \mathsf{Cl}_K$.

Corolario. *Sólo hay un número finitos de L/K no ramificada.*

Nota. Para superficies de Riemann hay un número infinito de cubrientes no ramificados.

Idea. Cl_K deberia ser un cociente de un $\pi_1 K$ hipotético.

Hay una “versión abeliana” de π_1:

La Teoría de Campos de Clase en Resumen

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay una “versión abeliana” de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

La Teoría de Campos de Clase en Resumen

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathsf{Gal}(L/K)$$

La Teoría de Campos de Clase en Resumen

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathrm{Gal}(L/K)$$

con $\mathrm{Ker}(\phi_L) = N_L$

La Teoría de Campos de Clase en Resumen

Hay una “versión abeliana” de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathrm{Gal}(L/K)$$

con $\mathrm{Ker}(\phi_L) = N_L$ que induce un isomorfismo

$$C_K/N_L \cong \mathrm{Gal}(L/K).$$

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathrm{Gal}(L/K)$$

con $\mathrm{Ker}(\phi_L) = N_L$ que induce un isomorfismo

$$C_K/N_L \cong \mathrm{Gal}(L/K).$$

Para $L = H_K$,

La Teoría de Campos de Clase en Resumen

Hay una “versión abeliana” de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathrm{Gal}(L/K)$$

con $\mathrm{Ker}(\phi_L) = N_L$ que induce un isomorfismo

$$C_K/N_L \cong \mathrm{Gal}(L/K).$$

Para $L = H_K$, $C_K/N_{H_K} \cong \mathrm{Cl}_K$

La Teoría de Campos de Clase en Resumen

Hay una "versión abeliana" de π_1: el **grupo de clases de idèles**

$$C_K$$

y una correspondencia biyectiva

$$\{N_L < C_K\} \longleftrightarrow \{L/K \text{ abelianas}\}.$$

Hay un epimorfismo llamado **el mapeo de reciprocidad**

$$\phi_L : C_K \twoheadrightarrow \mathsf{Gal}(L/K)$$

con $\mathsf{Ker}(\phi_L) = N_L$ que induce un isomorfismo

$$C_K/N_L \cong \mathsf{Gal}(L/K).$$

Para $L = H_K$, $C_K/N_{H_K} \cong \mathsf{Cl}_K$ y ϕ_{H_K} induce el isomorfismo del Teorema de Hilbert.

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}}$$

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n}$$

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n} \quad \text{si } \mathfrak{p}^n|(x) \text{ pero } \mathfrak{p}^{n+1} \not|(x)$$

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n} \quad \text{si } \mathfrak{p}^n | (x) \text{ pero } \mathfrak{p}^{n+1} \not| (x)$$

donde $c > 1$ un constante.

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n} \quad \text{si } \mathfrak{p}^n | (x) \text{ pero } \mathfrak{p}^{n+1} \not| (x)$$

donde $c > 1$ un constante. La completación $\mathcal{O}_{\mathfrak{p}}$ es un anillo local

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n} \quad \text{si } \mathfrak{p}^n|(x) \text{ pero } \ \mathfrak{p}^{n+1} \ \not|(x)$$

donde $c > 1$ un constante. La completación $\mathcal{O}_{\mathfrak{p}}$ es un anillo local (sólo tiene un ideal primo, la completación $\overline{\mathfrak{p}}$ de $\mathfrak{p}$)

Si $\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_\mathfrak{p} = c^{-n} \quad \text{si } \mathfrak{p}^n|(x) \text{ pero } \mathfrak{p}^{n+1} \not|(x)$$

donde $c > 1$ un constante. La completación $\mathcal{O}_\mathfrak{p}$ es un anillo local (sólo tiene un ideal primo, la completación $\overline{\mathfrak{p}}$ de $\mathfrak{p}$) y su campo de fracciones

$$K_\mathfrak{p}$$

Si $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ y $x \in \mathcal{O}_K$ definimos un valor absolute

$$|x|_{\mathfrak{p}} = c^{-n} \quad \text{si } \mathfrak{p}^n | (x) \text{ pero } \ \mathfrak{p}^{n+1} \ \not| (x)$$

donde $c > 1$ un constante. La completación $\mathcal{O}_{\mathfrak{p}}$ es un anillo local (sólo tiene un ideal primo, la completación $\overline{\mathfrak{p}}$ de $\mathfrak{p}$) y su campo de fracciones

$$K_{\mathfrak{p}}$$

se llama la **completación $\mathfrak{p}$-adica** de K.

Supongamos $K/\mathbb{Q}$ es Galois de grado n.

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K$$

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

Grupo de Clases de Idèles

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in \mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} :$$

Grupo de Clases de Idèles

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p}\in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in \mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ para casi todo } \mathfrak{p}\}.$$

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} \;:\; x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ para casi todo } \mathfrak{p}\}.$$

donde $\mathcal{O}_{\mathfrak{p}}^{\times}$ es el grupo de unidades de $\mathcal{O}_{\mathfrak{p}}$

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ para casi todo } \mathfrak{p}\}.$$

donde $\mathcal{O}_{\mathfrak{p}}^{\times}$ es el grupo de unidades de $\mathcal{O}_{\mathfrak{p}}$ (enteros cuyos inversos son enteros).

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in \mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p}\in \mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in \mathrm{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ para casi todo } \mathfrak{p}\}.$$

  donde $\mathcal{O}_{\mathfrak{p}}^{\times}$ es el grupo de unidades de $\mathcal{O}_{\mathfrak{p}}$ (enteros cuyos inversos son enteros).

Hay un encaje diagonal $K^{\times} \hookrightarrow \mathbb{I}_K$.

Grupo de Clases de Idèles

Supongamos $K/\mathbb{Q}$ es Galois de grado n. El **grupo de idèles** es

$$\mathbb{I}_K := \mathbb{K}^n \times \widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$$

donde

- $\mathbb{K} = \mathbb{R}$ o $\mathbb{C}$ dependiente si $K \subset \mathbb{R}$ o no,
- $K_{\mathfrak{p}}^{\times} = (K_{\mathfrak{p}} - 0, \times)$ es el grupo multiplicativo de $K_{\mathfrak{p}}$.
- $\widetilde{\prod}_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times}$ es el grupo

$$\{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in\mathsf{Spec}(\mathcal{O}_K)} K_{\mathfrak{p}}^{\times} : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ para casi todo } \mathfrak{p}\}.$$

donde $\mathcal{O}_{\mathfrak{p}}^{\times}$ es el grupo de unidades de $\mathcal{O}_{\mathfrak{p}}$ (enteros cuyos inversos son enteros).

Hay un encaje diagonal $K^{\times} \hookrightarrow \mathbb{I}_K$. Luego $C_K = \mathbb{I}_K/K^{\times}$.

La Propuesta de una Teoría No Abeliana de Campos de Clase.

Construir desde K un grupo no abeliano

$$\mathfrak{C}_K$$

La Propuesta de una Teoría No Abeliana de Campos de Clase.
Construir desde K un grupo no abeliano

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K

La Propuesta de una Teoría No Abeliana de Campos de Clase. *Construir desde K un grupo no abeliano*

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathsf{Gal}(L/K),$$

La Propuesta de una Teoría No Abeliana de Campos de Clase.
Construir desde K un grupo no abeliano

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathsf{Gal}(L/K), \quad \mathsf{Ker}(\Phi_L) = \mathfrak{N}_L$$

La Propuesta de una Teoría No Abeliana de Campos de Clase.
Construir desde K un grupo no abeliano

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathsf{Gal}(L/K), \quad \mathsf{Ker}(\Phi_L) = \mathfrak{N}_L$$

con

$$\mathsf{Gal}(L/K) \cong \mathfrak{C}_K/\mathfrak{N}_K.$$

La Propuesta de una Teoría No Abeliana de Campos de Clase. *Construir desde K un grupo no abeliano*

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathsf{Gal}(L/K), \quad \mathsf{Ker}(\Phi_L) = \mathfrak{N}_L$$

con

$$\mathsf{Gal}(L/K) \cong \mathfrak{C}_K/\mathfrak{N}_K.$$

El Programa de Langlands. *Una reformulación de La Propuesta*

La Propuesta de una Teoría No Abeliana de Campos de Clase. *Construir desde K un grupo no abeliano*

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathrm{Gal}(L/K), \quad \mathrm{Ker}(\Phi_L) = \mathfrak{N}_L$$

con

$$\mathrm{Gal}(L/K) \cong \mathfrak{C}_K/\mathfrak{N}_K.$$

El Programa de Langlands. *Una reformulación de La Propuesta que concentra en el efecto de una teoría no abeliana en las* **funciones L** *de K:*

La Propuesta de una Teoría No Abeliana de Campos de Clase. *Construir desde K un grupo no abeliano*

$$\mathfrak{C}_K$$

cuyos subgrupos normales $\mathfrak{N}_L$ indexan extensiónes de Galois L/K y un epimorfismo

$$\Phi_L : \mathfrak{C}_K \longrightarrow \mathrm{Gal}(L/K), \quad \mathrm{Ker}(\Phi_L) = \mathfrak{N}_L$$

con

$$\mathrm{Gal}(L/K) \cong \mathfrak{C}_K/\mathfrak{N}_K.$$

El Programa de Langlands. *Una reformulación de La Propuesta que concentra en el efecto de una teoría no abeliana en las* **funciones L** *de K: generalizaciones de la función zeta de Riemann.*

El Teorema de Kronecker-Weber

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}}$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

El **grupo de clases de $\mathfrak{m}$ rayos** es

$$\mathrm{Cl}_K^{\mathfrak{m}}$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}^{\mathfrak{m}}_{\mathcal{O}_K} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}^{\mathfrak{m}}_{\mathcal{O}_K} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

El **grupo de clases de $\mathfrak{m}$ rayos** es

$$\mathrm{Cl}^{\mathfrak{m}}_K := \mathcal{I}^{\mathfrak{m}}_{\mathcal{O}_K} / \mathcal{P}^{\mathfrak{m}}_{\mathcal{O}_K}.$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

El **grupo de clases de $\mathfrak{m}$ rayos** es

$$\mathrm{Cl}_K^{\mathfrak{m}} := \mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} / \mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}}.$$

Llamamos a $\mathfrak{m}$ un **modulus** para L/K

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

El **grupo de clases de $\mathfrak{m}$ rayos** es

$$\mathrm{Cl}_K^{\mathfrak{m}} := \mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} / \mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}}.$$

Llamamos a $\mathfrak{m}$ un **modulus** para L/K si el mapeo de reciprocidad factorisa como

$$\psi_K : C_K \longrightarrow \mathrm{Cl}_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K).$$

Sea $\mathfrak{m} \subset \mathcal{O}_K$ un ideal y sea

$$\mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} := \{\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K} \mid (\mathfrak{a}, \mathfrak{m}) = 1\}.$$

El **subgrupo de $\mathfrak{m}$ rayos** es

$$\mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}} := \{(\alpha) \in \mathcal{P}_{\mathcal{O}_K} \mid \alpha \equiv 1 \mod \mathfrak{m}\}.$$

El **grupo de clases de $\mathfrak{m}$ rayos** es

$$\mathrm{Cl}_K^{\mathfrak{m}} := \mathcal{I}_{\mathcal{O}_K}^{\mathfrak{m}} / \mathcal{P}_{\mathcal{O}_K}^{\mathfrak{m}}.$$

Llamamos a $\mathfrak{m}$ un **modulus** para L/K si el mapeo de reciprocidad factorisa como

$$\psi_K : C_K \longrightarrow \mathrm{Cl}_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K).$$

El modulus mas pequeño para L/K se llama el **conductor**.

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$.

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$. Cuando $\mathfrak{m} = (1)$, $K^{(1)} = H_K$.

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$. Cuando $\mathfrak{m} = (1)$, $K^{(1)} = H_K$.

Teorema. $\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$.

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$. Cuando $\mathfrak{m} = (1)$, $K^{(1)} = H_K$.

Teorema. $\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$.

Notemos que cada extensión abeliana L/K está contenida en algún $K^{\mathfrak{m}}$.

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \not| \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$. Cuando $\mathfrak{m} = (1)$, $K^{(1)} = H_K$.

Teorema. $\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$.

Notemos que cada extensión abeliana L/K está contenida en algún $K^{\mathfrak{m}}$. En particular, la **máxima extensión abeliana** de K es

$$K^{\mathrm{ab}} = \bigcup K^{\mathfrak{m}}.$$

El **campo de clase de $\mathfrak{m}$ rayos**

$$K^{\mathfrak{m}}/K$$

es la máxima extensión abeliana no ramificada en primos $\mathfrak{p} \nmid \mathfrak{m}$ y cuyo conductor divide $\mathfrak{m}$. Cuando $\mathfrak{m} = (1)$, $K^{(1)} = H_K$.

Teorema. $\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}$.

Notemos que cada extensión abeliana L/K está contenida en algún $K^{\mathfrak{m}}$. En particular, la **máxima extensión abeliana** de K es

$$K^{\mathrm{ab}} = \bigcup K^{\mathfrak{m}}.$$

Colectivamente se refiere a los $K^{\mathfrak{m}}$ como **campos de clase**.

Duodécimo Problema de Hilbert. *Sea* K *un* **campo global** *i.e. una extensión finita de la forma*

$$K/\mathbb{Q} \quad \text{o} \quad K/\mathbb{F}(T)$$

donde

- $\mathbb{Q} =$ *es el campo de los racionales y*
- $\mathbb{F}(T) =$ *el campo de funciones racionales sobre un campo finito* $\mathbb{F}$.

Da una descripción explícita de cada **campo de clase**

$$K^{\mathfrak{m}}/K.$$

Una m-**ésima raíz de unidad**

Una **m-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$.

Una m**-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$. Cada tal ζ es de la forma

$$\zeta = \exp(2\pi i q), \quad q \in (m)^{-1} \mod \mathbb{Z}.$$

Una **m-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$. Cada tal ζ es de la forma

$$\zeta = \exp(2\pi i q), \quad q \in (m)^{-1} \mod \mathbb{Z}.$$

Las m-ésima raices de unidad forman un grupo multiplicativo cíclico:

Una m**-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$. Cada tal ζ es de la forma

$$\zeta = \exp(2\pi i q), \quad q \in (m)^{-1} \mod \mathbb{Z}.$$

Las m-ésima raices de unidad forman un grupo multiplicativo cíclico: un generador se llama **primitiva**.

Una **m-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$. Cada tal ζ es de la forma

$$\zeta = \exp(2\pi i q), \quad q \in (m)^{-1} \mod \mathbb{Z}.$$

Las m-ésima raices de unidad forman un grupo multiplicativo cíclico: un generador se llama **primitiva**. Una **extensión ciclotómica** de $\mathbb{Q}$ es una de la forma

$$\mathbb{Q}(\zeta_m)$$

Una **m-ésima raíz de unidad** es $\zeta \in \mathbb{C}$ con $\zeta^m = 1$. Cada tal ζ es de la forma

$$\zeta = \exp(2\pi i q), \quad q \in (m)^{-1} \mod \mathbb{Z}.$$

Las m-ésima raices de unidad forman un grupo multiplicativo cíclico: un generador se llama **primitiva**. Una **extensión ciclotómica** de $\mathbb{Q}$ es una de la forma

$$\mathbb{Q}(\zeta_m)$$

donde ζ_m es una m-ésima raíz de unidad primitiva.

El siguiente teorema da una solución del duodécimo problema para $K = \mathbb{Q}$.

El siguiente teorema da una solución del duodécimo problema para $K = \mathbb{Q}$.

Teorema de Kronecker-Weber. *Sea $(m) \subset \mathbb{Z}$ un ideal. Entonces*

$$\mathbb{Q}^{(m)} = \mathbb{Q}(\zeta_m).$$