Sabores de la Teoría de Números
III. La Teoría Geométrica

Tim Gendron

Instituto de Matemáticas, Universidad Nacional Autónoma de México

28 junio 2017

Introducción

Hay various temas que pueden reclamar la denominación "geométrica" en la teoría de números. Por ejemplo:

- La *Geometría de Números* de Minkowski, que consiste del estudio de anillos de enteros y sus ideales como retículas en espacio vectoriales.
- Campos de funciones sobre campos finitos $K/\mathbb{F}(T)$, estudiados geométricamente mediante las curvas asociadas.

En esta charla vamos a enfocarnos en el tema de *curvas elípticas*, que tiene una historia amplia y profunda en el desarrollo de la teoría de números, particularmente bien conocido por su contribución a la solución de la Conjetura de Fermat. Aquí vamos a discutir su uso en la solución del duodécimo problema de Hilbert en el caso de campos cuadráticos y complejos sobre $\mathbb{Q}$, por la teoría de *Multiplicación Compleja*.

Retículas y Toros

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$,

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu)$$

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle$$

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n \mid m, n \in \mathbb{Z}\}.$$

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{ m\mu + n | \ m, n \in \mathbb{Z} \}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**,

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n |\ m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n |\; m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie.

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n | \; m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie. $\mathbb{T}(\Lambda)$ es **isomorfo** a $\mathbb{T}(\Lambda')$

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n |\ m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie. $\mathbb{T}(\Lambda)$ es **isomorfo** a $\mathbb{T}(\Lambda')$ $\Leftrightarrow$ existe $c \in \mathbb{C}$ con $\Lambda' = c\Lambda$,

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n | \; m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie. $\mathbb{T}(\Lambda)$ es **isomorfo** a $\mathbb{T}(\Lambda')$ $\Leftrightarrow$ existe $c \in \mathbb{C}$ con $\Lambda' = c\Lambda$, el isomorfismo inducido por $z \mapsto cz$.

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n | \; m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie. $\mathbb{T}(\Lambda)$ es **isomorfo** a $\mathbb{T}(\Lambda')$ $\Leftrightarrow$ existe $c \in \mathbb{C}$ con $\Lambda' = c\Lambda$, el isomorfismo inducido por $z \mapsto cz$. En particular cada $\mathbb{T}(\Lambda)$ es isomorfo a un toro de la forma

$$\mathbb{T}(\mu)$$

Una **retícula** $\Lambda \subset \mathbb{C}$ es un grupo discreto $\cong \mathbb{Z}^2$.

Ejemplo. Si $\mu \in \mathbb{C} - \mathbb{R}$, podemos definir la retícula

$$\Lambda(\mu) := \langle \mu, 1 \rangle = \{m\mu + n | \ m, n \in \mathbb{Z}\}.$$

Si Λ es retícula, llamamos al cociente

$$\mathbb{T}(\Lambda) := \mathbb{C}/\Lambda$$

un **toro**, una superficie de Riemann de genero 1 que es además un grupo de Lie. $\mathbb{T}(\Lambda)$ es **isomorfo** a $\mathbb{T}(\Lambda')$ $\Leftrightarrow$ existe $c \in \mathbb{C}$ con $\Lambda' = c\Lambda$, el isomorfismo inducido por $z \mapsto cz$. En particular cada $\mathbb{T}(\Lambda)$ es isomorfo a un toro de la forma

$$\mathbb{T}(\mu) := \mathbb{C}/\Lambda(\mu), \quad \mu \in \mathbb{C} - \mathbb{R}.$$

Sea Λ una retícula.

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}},$$

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Para cada $\lambda \in \Lambda$,

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Para cada $\lambda \in \Lambda$, $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$,

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Para cada $\lambda \in \Lambda$, $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$, así que $\wp$ induce una función meromorfa

$$\wp_\Lambda : \mathbb{T}(\Lambda) \longrightarrow \hat{\mathbb{C}}.$$

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda-0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Para cada $\lambda \in \Lambda$, $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$, así que $\wp$ induce una función meromorfa

$$\wp_\Lambda : \mathbb{T}(\Lambda) \longrightarrow \hat{\mathbb{C}}.$$

La derivada

$$\wp'_\Lambda(z) = -2 \sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^3}$$

Sea Λ una retícula. La **función $\wp$ de Weierstraß** es

$$\wp_\Lambda : \mathbb{C} \longrightarrow \hat{\mathbb{C}}, \quad \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - 0} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\}.$$

Para cada $\lambda \in \Lambda$, $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$, así que $\wp$ induce una función meromorfa

$$\wp_\Lambda : \mathbb{T}(\Lambda) \longrightarrow \hat{\mathbb{C}}.$$

La derivada

$$\wp'_\Lambda(z) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

también induce una función meromorfa en $\mathbb{T}(\Lambda)$.

Para cada retícula Λ

Para cada retícula Λ y $n \in \mathbb{N}$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$,

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n)$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$.

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4)$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4),$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6)$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6) = 140 G_\Lambda(6).$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6) = 140 G_\Lambda(6).$$

La **eccuación de Weierstraß** asociada es

$$\mathsf{Eqn}_\Lambda :$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6) = 140 G_\Lambda(6).$$

La **eccuación de Weierstraß** asociada es

$$\text{Eqn}_\Lambda : \quad Y^2 = 4X^3 - g_\Lambda(4)X - g_\Lambda(6).$$

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6) = 140 G_\Lambda(6).$$

La **eccuación de Weierstraß** asociada es

$$\text{Eqn}_\Lambda : \quad Y^2 = 4X^3 - g_\Lambda(4)X - g_\Lambda(6).$$

Cuando $\Lambda = \Lambda(\mu)$ escribimos $G_\mu(n)$, *etc.*

Para cada retícula Λ y $n \in \mathbb{N}$ definimos una generalización bi-dimensional de $\zeta(s)$, la **serie de Eisenstein**

$$G_\Lambda(n) = \sum_{\lambda \in \Lambda - 0} \lambda^{-n}$$

que converge para $n \geq 4$. Escribimos

$$g_\Lambda(4) = 60 G_\Lambda(4), \quad g_\Lambda(6) = 140 G_\Lambda(6).$$

La **eccuación de Weierstraß** asociada es

$$\text{Eqn}_\Lambda : \quad Y^2 = 4X^3 - g_\Lambda(4)X - g_\Lambda(6).$$

Cuando $\Lambda = \Lambda(\mu)$ escribimos $G_\mu(n)$, *etc.* Omitimos completamente la retícula en la notación si no es importante.

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo.

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß es

$$Y^2 Z = 4X^3 - g(4)XZ^2 - g(6)Z^3 \tag{1}$$

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß es

$$Y^2 Z = 4X^3 - g(4)XZ^2 - g(6)Z^3 \tag{1}$$

y denotemos por

$$E \subset \mathbb{P}^2(\mathbb{C})$$

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß es

$$Y^2 Z = 4X^3 - g(4)XZ^2 - g(6)Z^3 \tag{1}$$

y denotemos por

$$E \subset \mathbb{P}^2(\mathbb{C})$$

la curva proyectiva definido por la eccuación (1).

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß es

$$Y^2 Z = 4X^3 - g(4)XZ^2 - g(6)Z^3 \tag{1}$$

y denotemos por

$$E \subset \mathbb{P}^2(\mathbb{C})$$

la curva proyectiva definido por la eccuación (1). E se llama una **curva elíptica**,

Sea

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - 0)/\mathbb{C}^*$$

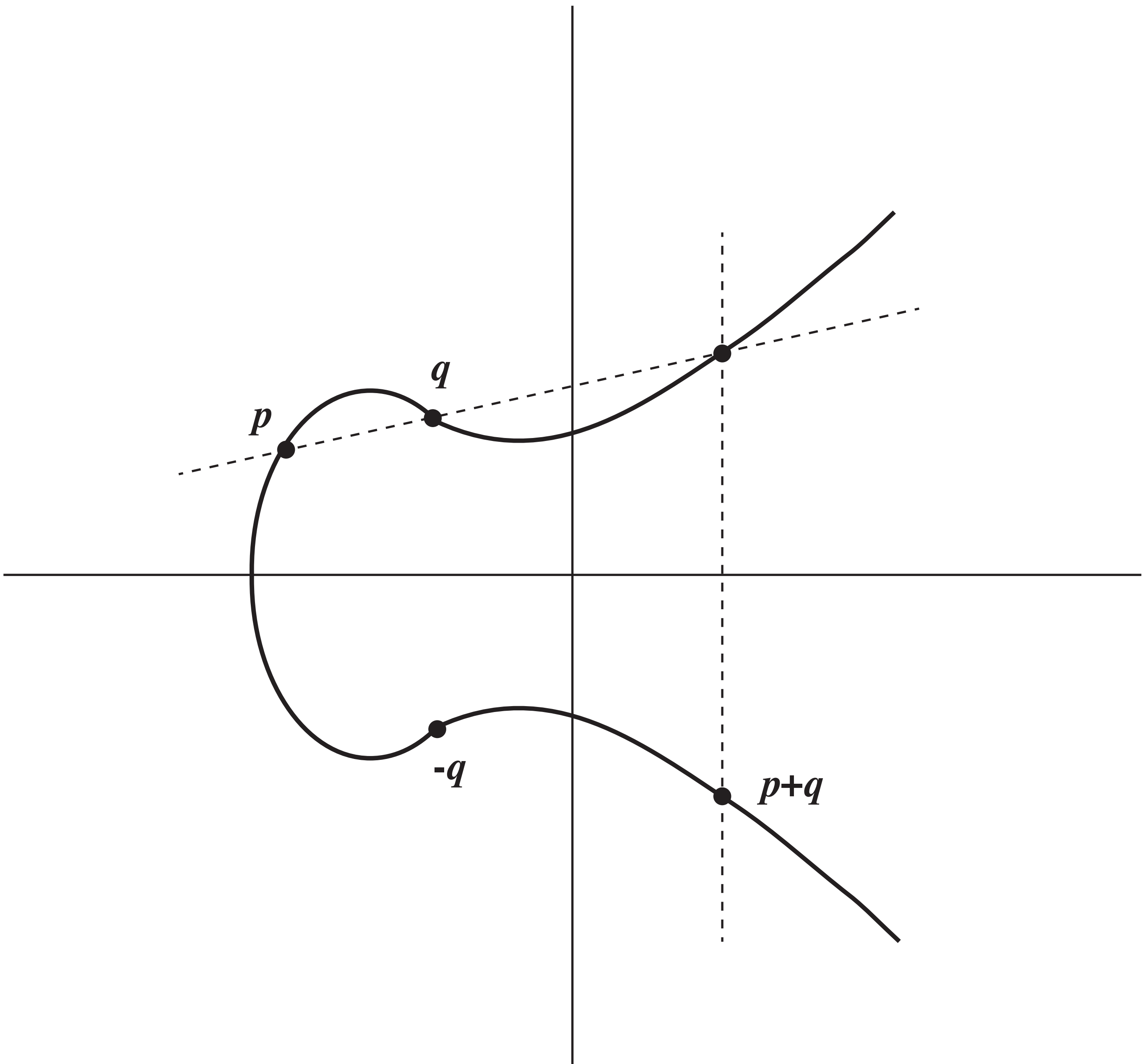
el espacio proyectivo. La versión homogénea de la eccuación de Weierstraß es

$$Y^2Z = 4X^3 - g(4)XZ^2 - g(6)Z^3 \tag{1}$$

y denotemos por

$$E \subset \mathbb{P}^2(\mathbb{C})$$

la curva proyectiva definido por la eccuación (1). E se llama una **curva elíptica**, un grupo c.r.a. la ley de cuerda-tangente:


q
p
-q
p+q

Teorema. *Cada curva proyectiva de genero* 1

Teorema. *Cada curva proyectiva de genero* 1 *es isomorfo a una curva eliptica* E *con eccuación (1),*

Teorema. *Cada curva proyectiva de genero 1 es isomorfo a una curva eliptica E con ecuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}),$$

Teorema. *Cada curva proyectiva de genero 1 es isomorfo a una curva eliptica E con ecuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

Teorema. *Cada curva proyectiva de genero* 1 *es isomorfo a una curva eliptica* E *con eccuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

define un isomorphismo $\mathbb{C}$*-analítico entre* $\mathbb{T}$ *y la curva elíptica* E *asociada a la ecuación de Weierstraß correspondiente.*

Teorema. *Cada curva proyectiva de genero* 1 *es isomorfo a una curva eliptica* E *con ecuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

define un isomorphismo $\mathbb{C}$*-analítico entre* $\mathbb{T}$ *y la curva elíptica* E *asociada a la ecuación de Weierstraß correspondiente. Si* $\mathbb{T}_1 \to \mathbb{T}_2$ *por* $z \mapsto cz$*,*

El Diccionario Analítico-Algebraico

Teorema. *Cada curva proyectiva de genero 1 es isomorfo a una curva eliptica E con eccuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

define un isomorphismo $\mathbb{C}$-analítico entre $\mathbb{T}$ y la curva elíptica E asociada a la eccuación de Weierstraß correspondiente. Si $\mathbb{T}_1 \to \mathbb{T}_2$ por $z \mapsto cz$, tenemos un diagrama conmutativo

$$\begin{tikzcd}
\mathbb{T}_1 \arrow[r, "c"] \arrow[d, "\varphi_1"', "\cong"] & \mathbb{T}_2 \arrow[d, "\varphi_2", "\cong"'] \\
E_1 \arrow[r, "f_c"'] & E_2
\end{tikzcd}$$

Teorema. *Cada curva proyectiva de genero 1 es isomorfo a una curva eliptica E con eccuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

define un isomorphismo $\mathbb{C}$-analítico entre $\mathbb{T}$ y la curva elíptica E asociada a la eccuación de Weierstraß correspondiente. Si $\mathbb{T}_1 \to \mathbb{T}_2$ por $z \mapsto cz$, tenemos un diagrama conmutativo

$$\begin{tikzcd}
\mathbb{T}_1 \arrow[r, "c"] \arrow[d, "\varphi_1"', "\cong"] & \mathbb{T}_2 \arrow[d, "\cong"', "\varphi_2"] \\
E_1 \arrow[r, "f_c"'] & E_2
\end{tikzcd}$$

donde f_c es un **morfismo de variedades**

Teorema. *Cada curva proyectiva de genero 1 es isomorfo a una curva eliptica E con eccuación (1), y el mapeo*

$$\varphi_\mu : \mathbb{T} \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

define un isomorphismo $\mathbb{C}$-analítico entre $\mathbb{T}$ y la curva elíptica E asociada a la eccuación de Weierstraß correspondiente. Si $\mathbb{T}_1 \to \mathbb{T}_2$ por $z \mapsto cz$, tenemos un diagrama conmutativo

$$\begin{tikzcd} \mathbb{T}_1 \arrow[r, "c"] \arrow[d, "\varphi_1"', "\cong"] & \mathbb{T}_2 \arrow[d, "\cong"', "\varphi_2"] \\ E_1 \arrow[r, "f_c"'] & E_2 \end{tikzcd}$$

donde f_c es un **morfismo de variedades** *i.e. un mapeo polinomio.*

Cuando queremos hacer operaciones

Cuando queremos hacer operaciones

Cuando queremos hacer operaciones

- analíticas,

Cuando queremos hacer operaciones

- analíticas, trabajaremos con $\mathbb{T} = \mathbb{C}/\Lambda$, etc.

Cuando queremos hacer operaciones

- analíticas, trabajaremos con $\mathbb{T} = \mathbb{C}/\Lambda$, etc.
- algebraicas,

Cuando queremos hacer operaciones

- analíticas, trabajaremos con $\mathbb{T} = \mathbb{C}/\Lambda$, etc.
- algebraicas, trabajaremos con $E \subset \mathbb{P}^2(\mathbb{C})$

Cuando queremos hacer operaciones

- analíticas, trabajaremos con $\mathbb{T} = \mathbb{C}/\Lambda$, etc.
- algebraicas, trabajaremos con $E \subset \mathbb{P}^2(\mathbb{C})$ y su eccuación de Weierstraß .

Cuando queremos hacer operaciones

- analíticas, trabajaremos con $\mathbb{T} = \mathbb{C}/\Lambda$, etc.
- algebraicas, trabajaremos con $E \subset \mathbb{P}^2(\mathbb{C})$ y su eccuación de Weierstraß .

En cualquier caso, usaremos el término *curva elíptica* para E o el toro $\mathbb{T}$.

Origen de la Terminología

El origen de la terminología viene del clásico tema de **integrales elípticas**.

El origen de la terminología viene del clásico tema de **integrales elípticas**. Los inversos de funciones $\mathbb{T} \to \hat{\mathbb{C}}$

El origen de la terminología viene del clásico tema de **integrales elípticas**. Los inversos de funciones $\mathbb{T} \to \hat{\mathbb{C}}$ son funciones multi-valuadas

El origen de la terminología viene del clásico tema de **integrales elípticas**. Los inversos de funciones $\mathbb{T} \to \hat{\mathbb{C}}$ son funciones multi-valuadas definidas por integrales de la forma

$$z \longmapsto \int_{z_0}^{z} \frac{dz}{\sqrt{(z-a)(z-b)(z-c)}};$$

El origen de la terminología viene del clásico tema de **integrales elípticas**. Los inversos de funciones $\mathbb{T} \to \hat{\mathbb{C}}$ son funciones multi-valuadas definidas por integrales de la forma

$$z \longmapsto \int_{z_0}^{z} \frac{dz}{\sqrt{(z-a)(z-b)(z-c)}};$$

llamadas elípticas porque la fórmula de la circunferencia de un elipse se da por una tal integral.

Origen de la Terminología

El origen de la terminología viene del clásico tema de **integrales elípticas**. Los inversos de funciones $\mathbb{T} \to \hat{\mathbb{C}}$ son funciones multi-valuadas definidas por integrales de la forma

$$z \longmapsto \int_{z_0}^{z} \frac{dz}{\sqrt{(z-a)(z-b)(z-c)}};$$

llamadas elípticas porque la fórmula de la circunferencia de un elipse se da por una tal integral.

Invariante Modular

Teorema. $\mathbb{T}(\mu) \cong \mathbb{T}(\nu)$

Teorema. $\mathbb{T}(\mu) \cong \mathbb{T}(\nu) \Leftrightarrow \mu \sim \nu$ *por* $\mathrm{GL}_2(\mathbb{Z})$*:*

Teorema. $\mathbb{T}(\mu) \cong \mathbb{T}(\nu) \Leftrightarrow \mu \sim \nu$ *por* $\mathrm{GL}_2(\mathbb{Z})$*: existe*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

Teorema. $\mathbb{T}(\mu) \cong \mathbb{T}(\nu) \Leftrightarrow \mu \sim \nu$ *por* $\mathrm{GL}_2(\mathbb{Z})$*: existe* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ *tal que*

$$\mu = \frac{a\nu + b}{c\nu + d}.$$

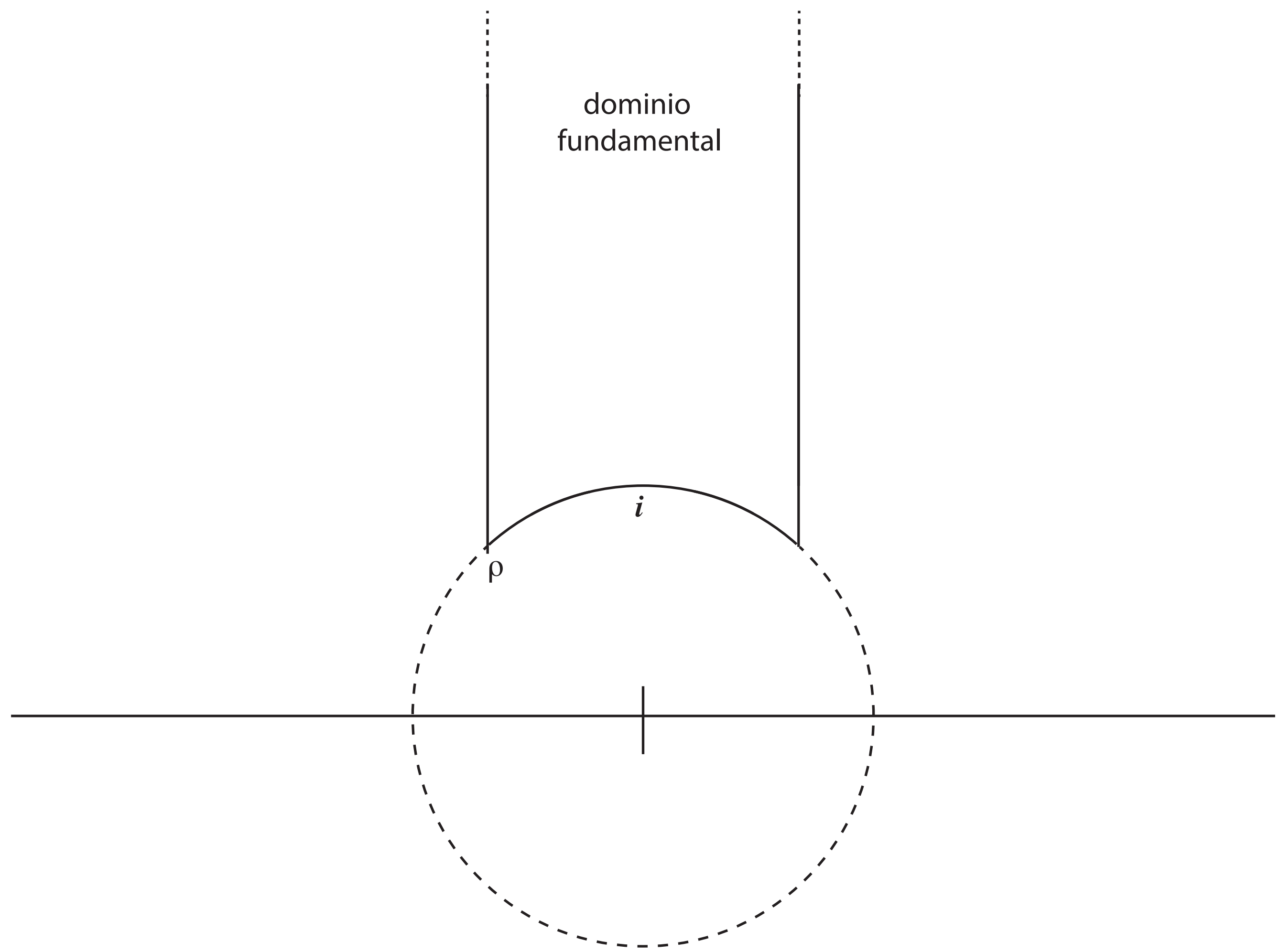
Teorema. $\mathbb{T}(\mu) \cong \mathbb{T}(\nu) \Leftrightarrow \mu \sim \nu$ *por* $\mathrm{GL}_2(\mathbb{Z})$*: existe* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ *tal que*

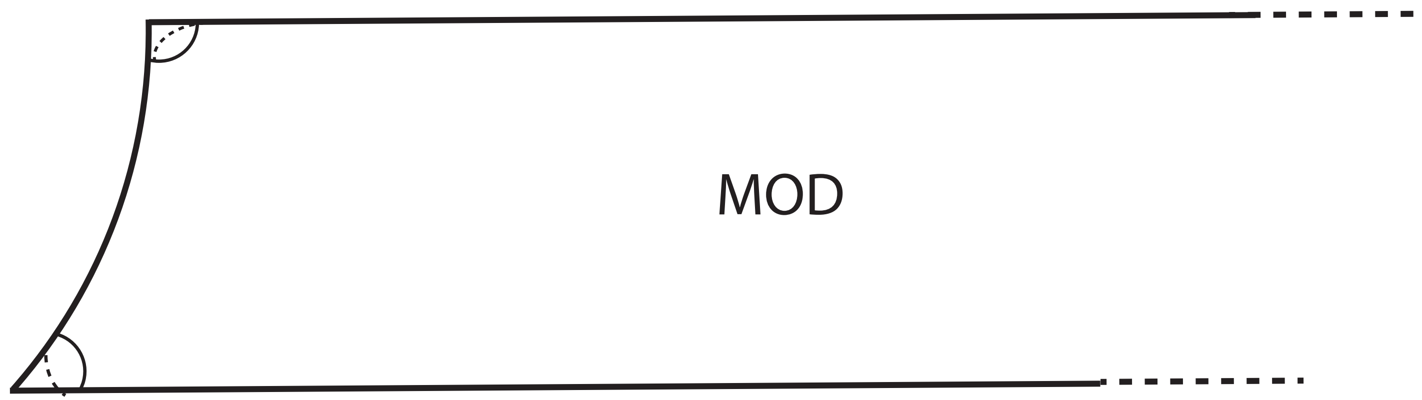
$$\mu = \frac{a\nu + b}{c\nu + d}.$$

Así que el **espacio de moduli** de curvas elípticas es

$$\mathrm{Mod} := (\mathbb{C} - \mathbb{R})/\mathrm{GL}_2(\mathbb{Z}).$$

Dominio Fundamental para Mod




MOD

Para cada n par,

Para cada n par, la función

$$\mu \mapsto G_\mu(n)$$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

Para cada n par, la función

$$\mu \mapsto G_{\mu}(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n:

Para cada n par, la función

$$\mu \mapsto G_{\mu}(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n)$$

Para cada n par, la función

$$\mu \mapsto G_{\mu}(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathsf{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_{\mu}(n),$$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_\mu(n), \quad A'(z) = \frac{1}{(cz+d)^2}.$$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_\mu(n), \quad A'(z) = \frac{1}{(cz+d)^2}.$$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_\mu(n), \quad A'(z) = \frac{1}{(cz+d)^2}.$$

Entonces el cociente

$$J(\mu) := \frac{G_\mu(6)^2}{G_\mu(4)^3}$$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_\mu(n), \quad A'(z) = \frac{1}{(cz+d)^2}.$$

Entonces el cociente

$$J(\mu) := \frac{G_\mu(6)^2}{G_\mu(4)^3}$$

es invariante c.r.a. la acción de $A \in \mathrm{GL}_2(\mathbb{Z})$

Para cada n par, la función

$$\mu \mapsto G_\mu(n) = \sum_{\lambda \in \Lambda(\mu) - 0} \lambda^{-n}$$

es una **forma modular** de peso n: para cada $A \in \mathrm{GL}_2(\mathbb{Z})$,

$$(A'(z))^n \cdot G_{A\mu}(n) = G_\mu(n), \quad A'(z) = \frac{1}{(cz+d)^2}.$$

Entonces el cociente

$$J(\mu) := \frac{G_\mu(6)^2}{G_\mu(4)^3}$$

es invariante c.r.a. la acción de $A \in \mathrm{GL}_2(\mathbb{Z})$ y define una función en Mod.

El **invariante modular** es

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente,

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente, si $\mathbb{T}(\mu)$ tiene ecuación de Weierstraß

$$Y^2 = 4X^3 - g_\mu(4)X - g_\mu(6)$$

El **invariante modular** es

$$j : \text{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente, si $\mathbb{T}(\mu)$ tiene ecuación de Weierstraß

$$Y^2 = 4X^3 - g_\mu(4)X - g_\mu(6)$$

con **discriminante** $\Delta_\mu = g_\mu(4)^3 - 27 g_\mu(6)^2$

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente, si $\mathbb{T}(\mu)$ tiene eccuación de Weierstraß

$$Y^2 = 4X^3 - g_\mu(4)X - g_\mu(6)$$

con **discriminante** $\Delta_\mu = g_\mu(4)^3 - 27 g_\mu(6)^2$ entonces

$$j(\mu) = \frac{12^3 g_\mu(4)^3}{\Delta_\mu}.$$

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente, si $\mathbb{T}(\mu)$ tiene ecuación de Weierstraß

$$Y^2 = 4X^3 - g_\mu(4)X - g_\mu(6)$$

con **discriminante** $\Delta_\mu = g_\mu(4)^3 - 27 g_\mu(6)^2$ entonces

$$j(\mu) = \frac{12^3 g_\mu(4)^3}{\Delta_\mu}.$$

Teorema. j *tiene un polo simple en* $i\infty$

El **invariante modular** es

$$j : \mathrm{Mod} \longrightarrow \mathbb{C}, \quad j(\mu) := \frac{12^3}{1 - \frac{49}{20} J(\mu)}.$$

Alternativamente, si $\mathbb{T}(\mu)$ tiene eccuación de Weierstraß

$$Y^2 = 4X^3 - g_\mu(4)X - g_\mu(6)$$

con **discriminante** $\Delta_\mu = g_\mu(4)^3 - 27 g_\mu(6)^2$ entonces

$$j(\mu) = \frac{12^3 g_\mu(4)^3}{\Delta_\mu}.$$

Teorema. *j tiene un polo simple en $i\infty$ y define un isomorfismo*

$$\mathrm{Mod} \cup \{\infty\} \cong \hat{\mathbb{C}}.$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z}$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El "nucleo" de este cambio de variable es

$$\{z \mapsto z + n\}$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\}$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El "nucleo" de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C},$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C}, \quad q = e^{2\pi i z} \longmapsto j(z),$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C}, \quad q = e^{2\pi i z} \longmapsto j(z),$$

con polo en $q = 0 \leftrightsquigarrow z = i\infty$.

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} | \ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C}, \quad q = e^{2\pi i z} \longmapsto j(z),$$

con polo en $q = 0 \leftrightsquigarrow z = i\infty$. Su expansión de Laurent en 0 es

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathsf{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C}, \quad q = e^{2\pi i z} \longmapsto j(z),$$

con polo en $q = 0 \leftrightsquigarrow z = i\infty$. Su expansión de Laurent en 0 es

$$j(q) = \frac{1}{q} + \sum_{i=1}^{\infty} a_i q^i$$

Consideremos el cambio de variable dado por

$$\mathbb{C} - \mathbb{R} \ni z \rightsquigarrow q = e^{2\pi i z} \in \mathbb{D}^* = \{z \in \mathbb{C} |\ |z| < 1\} - 0.$$

El “nucleo” de este cambio de variable es

$$\{z \mapsto z + n\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\} < \mathrm{GL}_2(\mathbb{Z}),$$

así que j define una función

$$j : \mathbb{D}^* \to \mathbb{C}, \quad q = e^{2\pi i z} \longmapsto j(z),$$

con polo en $q = 0 \leftrightsquigarrow z = i\infty$. Su expansión de Laurent en 0 es

$$j(q) = \frac{1}{q} + \sum_{i=1}^{\infty} a_i q^i = \frac{1}{q} + 744q + 196884q^2 + 21493760q^3 + \cdots .$$

Sea $\mathbb{M}$ el **grupo monstruo**:

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$,

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0,$$

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0, \;\; a_2 = r_2 + r_1 + r_0,$$

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0, \; a_2 = r_2 + r_1 + r_0, \; a_3 = r_3 + r_2 + 2r_1 + 2r_0, \ldots .$$

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \dots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0, \; a_2 = r_2 + r_1 + r_0, \; a_3 = r_3 + r_2 + 2r_1 + 2r_0, \dots .$$

Basado en esta, Conway y Norton conjeturaron que debería ser un módulo graduado sobre $\mathbb{M}$

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \approx 8\times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0,\ \ a_2 = r_2 + r_1 + r_0,\ \ a_3 = r_3 + r_2 + 2r_1 + 2r_0, \ldots.$$

Basado en esta, Conway y Norton conjeturaron que debería ser un módulo graduado sobre $\mathbb{M}$ cuya dimensión graduada se da por los coeficientes de j.

Paparrucha Monstruosa (Monstruous Moonshine)

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0,\ a_2 = r_2 + r_1 + r_0,\ a_3 = r_3 + r_2 + 2r_1 + 2r_0, \ldots.$$

Basado en esta, Conway y Norton conjeturaron que debería ser un módulo graduado sobre $\mathbb{M}$ cuya dimensión graduada se da por los coeficientes de j. Borcherds demostró esta conjetura en 1982

Sea $\mathbb{M}$ el **grupo monstruo**: el grupo simple sporadico mas grande, de orden

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}.$$

Si $r_0 = 1, r_1 < \ldots$ denotan las dimensiones de las representaciones irreducibles de $\mathbb{M}$, McKay observó que

$$a_1 = r_1 + r_0,\ a_2 = r_2 + r_1 + r_0,\ a_3 = r_3 + r_2 + 2r_1 + 2r_0, \ldots.$$

Basado en esta, Conway y Norton conjeturaron que debería ser un módulo graduado sobre $\mathbb{M}$ cuya dimensión graduada se da por los coeficientes de j. Borcherds demostró esta conjetura en 1982 y por este trabajo ganó una medalla de Fields.

Multiplicación Compleja

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$.*

Teorema. *Sea* $f : \mathbb{T} \to \mathbb{T}$ *un endomorfismo de la curva elíptica* $\mathbb{T} = \mathbb{C}/\Lambda$. *Existe* $c \in \mathbb{C}$ *tal que* f *se induce por el mapeo* $z \mapsto cz$,

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos.

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T})$

Teorema. *Sea* $f : \mathbb{T} \to \mathbb{T}$ *un endomorfismo de la curva elíptica* $\mathbb{T} = \mathbb{C}/\Lambda$. *Existe* $c \in \mathbb{C}$ *tal que* f *se induce por el mapeo* $z \mapsto cz$, *donde* $c\Lambda \subset \Lambda$.

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe* $\mu \in \mathbb{C} - \mathbb{R}$ *cuadrático*

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$.*

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo,

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe* $\mu \in \mathbb{C} - \mathbb{R}$ *cuadrático tal que* $\mathbb{T} \cong \mathbb{T}(\mu)$. *Decimos que* $\mathbb{T}$ *tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$.

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$. Entonces $\mathfrak{a}$ es retícula en $\mathbb{C}$

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. *$\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$. Entonces $\mathfrak{a}$ es retícula en $\mathbb{C}$ y la curva elíptica $\mathbb{T}_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$. Entonces $\mathfrak{a}$ es retícula en $\mathbb{C}$ y la curva elíptica $\mathbb{T}_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ satisface

$$\mathrm{End}(\mathbb{T}_{\mathfrak{a}}) = \mathcal{O}_K.$$

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$. Entonces $\mathfrak{a}$ es retícula en $\mathbb{C}$ y la curva elíptica $\mathbb{T}_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ satisface

$$\mathrm{End}(\mathbb{T}_{\mathfrak{a}}) = \mathcal{O}_K.$$

En general, si $\mathbb{T}$ tiene MC,

Teorema. *Sea $f : \mathbb{T} \to \mathbb{T}$ un endomorfismo de la curva elíptica $\mathbb{T} = \mathbb{C}/\Lambda$. Existe $c \in \mathbb{C}$ tal que f se induce por el mapeo $z \mapsto cz$, donde $c\Lambda \subset \Lambda$.*

Denotamos por $\mathrm{End}(\mathbb{T})$ el anillo de endomorfismos. Notemos que siempre tenemos $\mathbb{Z} \subset \mathrm{End}(\mathbb{T})$.

Teorema. $\mathbb{Z} \subsetneq \mathrm{End}(\mathbb{T}) \Leftrightarrow$ *existe $\mu \in \mathbb{C} - \mathbb{R}$ cuadrático tal que $\mathbb{T} \cong \mathbb{T}(\mu)$. Decimos que $\mathbb{T}$ tiene* **multiplicación compleja (MC)**.

Ejemplo. Sea $K = \mathbb{Q}(\mu)/\mathbb{Q}$ un campo cuadrático y complejo, $\mathfrak{a} \subset \mathcal{O}_K$. Entonces $\mathfrak{a}$ es retícula en $\mathbb{C}$ y la curva elíptica $\mathbb{T}_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ satisface

$$\mathrm{End}(\mathbb{T}_{\mathfrak{a}}) = \mathcal{O}_K.$$

En general, si $\mathbb{T}$ tiene MC, existe un $K/\mathbb{Q}$ tal que $\mathrm{End}(\mathbb{T}) \subset \mathcal{O}_K$.

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$.

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario,

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda$$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i |$$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i\lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i\lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. $\mathfrak{a}\Lambda$ *es retícula*

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. $\mathfrak{a}\Lambda$ *es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. *$\mathfrak{a}\Lambda$ es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. $\mathfrak{a}\Lambda$ *es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathsf{Ell}(\mathcal{O}_K)$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i\lambda_i | \ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. $\mathfrak{a}\Lambda$ *es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathrm{Ell}(\mathcal{O}_K) := \{\mathbb{T} | \ \mathrm{End}(\mathbb{T}) = \mathcal{O}_K\}/$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i\lambda_i | \ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. *$\mathfrak{a}\Lambda$ es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathrm{Ell}(\mathcal{O}_K) := \{\mathbb{T} | \ \mathrm{End}(\mathbb{T}) = \mathcal{O}_K\}/\cong$.

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i |\ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. $\mathfrak{a}\Lambda$ *es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathsf{Ell}(\mathcal{O}_K) := \{\mathbb{T} |\ \mathsf{End}(\mathbb{T}) = \mathcal{O}_K\}/\cong$.

Teorema. *La acción* $\mathbb{T} \mapsto \mathfrak{a}\mathbb{T}$

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \left\{\sum \alpha_i \lambda_i \middle| \, \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\right\}.$$

Teorema. *$\mathfrak{a}\Lambda$ es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathrm{Ell}(\mathcal{O}_K) := \{\mathbb{T} | \, \mathrm{End}(\mathbb{T}) = \mathcal{O}_K\}/\cong$.

Teorema. *La acción $\mathbb{T} \mapsto \mathfrak{a}\mathbb{T}$ induce una acción simple y transitiva de Cl_K en $\mathrm{Ell}(\mathcal{O}_K)$.*

Sea $\mathbb{T} = \mathbb{C}/\Lambda$ una curva elíptica con MC por $\mathcal{O}_K$. Si $\mathfrak{a} \in \mathcal{I}_{\mathcal{O}_K}$ es ideal fraccionario, definimos

$$\mathfrak{a}\Lambda := \{\sum \alpha_i \lambda_i | \ \alpha_i \in \mathfrak{a}, \lambda \in \Lambda_i\}.$$

Teorema. *$\mathfrak{a}\Lambda$ es retícula y la curva elítica*

$$\mathfrak{a}\mathbb{T} := \mathbb{C}/\mathfrak{a}\Lambda$$

tiene MC por $\mathcal{O}_K$.

Sea $\mathrm{Ell}(\mathcal{O}_K) := \{\mathbb{T}| \ \mathrm{End}(\mathbb{T}) = \mathcal{O}_K\}/\cong$.

Teorema. *La acción $\mathbb{T} \mapsto \mathfrak{a}\mathbb{T}$ induce una acción simple y transitiva de Cl_K en $\mathrm{Ell}(\mathcal{O}_K)$. En particular,*

$$\#\mathrm{Ell}(\mathcal{O}_K) = h_K < \infty.$$

En lo que sigue usamos la notacion

$$x^{\sigma}$$

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x),$$

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois,

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathrm{Aut}(\mathbb{C})$.

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$.
Sea E una curva elíptica con MC por $\mathcal{O}_K$,

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

Eqn :

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathsf{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathrm{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathrm{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathrm{Aut}(\mathbb{C})$,

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathsf{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathsf{Aut}(\mathbb{C})$, definimos E^σ

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathsf{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathsf{Aut}(\mathbb{C})$, definimos E^σ por

$$\mathsf{Eqn}^\sigma$$

En lo que sigue usamos la notacion

$$x^{\sigma} = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathsf{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathsf{Aut}(\mathbb{C})$, definimos E^{σ} por

$$\mathsf{Eqn}^{\sigma} := Y^2 = 4X^3 - g(4)^{\sigma}X - g(6)^{\sigma}.$$

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathrm{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathrm{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathrm{Aut}(\mathbb{C})$, definimos E^σ por

$$\mathrm{Eqn}^\sigma := Y^2 = 4X^3 - g(4)^\sigma X - g(6)^\sigma.$$

Tenemos que $\mathrm{Aut}(\mathbb{C})$ actúa en $\mathrm{Ell}(\mathcal{O}_K)$ también

Acción Algebraica por $\mathsf{Aut}(\mathbb{C})$

En lo que sigue usamos la notacion

$$x^\sigma = \sigma(x), \quad \sigma \in \mathsf{Aut}(\mathbb{C}).$$

Si σ es automorfismo de Galois, define un elemento de $\mathsf{Aut}(\mathbb{C})$. Sea E una curva elíptica con MC por $\mathcal{O}_K$, dada por

$$\mathsf{Eqn}: \quad Y^2 = 4X^3 - g(4)X - g(6).$$

Si $\sigma \in \mathsf{Aut}(\mathbb{C})$, definimos E^σ por

$$\mathsf{Eqn}^\sigma := Y^2 = 4X^3 - g(4)^\sigma X - g(6)^\sigma.$$

Tenemos que $\mathsf{Aut}(\mathbb{C})$ actúa en $\mathsf{Ell}(\mathcal{O}_K)$ también ya que

$$\mathsf{End}(E) \cong \mathsf{End}(E^\sigma), \quad f \longmapsto f^\sigma.$$

Teorema Fundamental de Multiplicación Compleja. *Si*

$$\mathrm{Cl}_K \ni \mathfrak{a} \leftrightsquigarrow \sigma_{\mathfrak{a}} \in \mathrm{Gal}(H_K/K)$$

por reciprocidad

Teorema Fundamental de Multiplicación Compleja. *Si*

$$\mathsf{Cl}_K \ni \mathfrak{a} \leftrightsquigarrow \sigma_{\mathfrak{a}} \in \mathsf{Gal}(H_K/K)$$

por reciprocidad y $\mathbb{T} \leftrightsquigarrow E$

Teorema Fundamental de Multiplicación Compleja. *Si*

$$\mathsf{Cl}_K \ni \mathfrak{a} \leftrightsquigarrow \sigma_{\mathfrak{a}} \in \mathsf{Gal}(H_K/K)$$

por reciprocidad y $\mathbb{T} \leftrightsquigarrow E$

$$E^{\sigma_{\mathfrak{a}}} \cong \mathfrak{a}^{-1}\mathbb{T}.$$

Weber-Fueter

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$.

Módulo de Torsión. Funciones de Weber

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión**

Módulo de Torsión. Funciones de Weber

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión** si

$$\alpha \cdot x = 0 \quad \text{para todo } \alpha \in \mathfrak{m}.$$

Módulo de Torsión. Funciones de Weber

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión** si

$$\alpha \cdot x = 0 \quad \text{para todo } \alpha \in \mathfrak{m}.$$

Los puntos de $\mathfrak{m}$ torsión forman un sub $\mathcal{O}_K$ modulo

$$\mathbb{T}[\mathfrak{m}] \subset \mathbb{T}.$$

Módulo de Torsión. Funciones de Weber

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión** si

$$\alpha \cdot x = 0 \quad \text{para todo } \alpha \in \mathfrak{m}.$$

Los puntos de $\mathfrak{m}$ torsión forman un sub $\mathcal{O}_K$ modulo

$$\mathbb{T}[\mathfrak{m}] \subset \mathbb{T}.$$

La **funcion de Weber** es

Módulo de Torsión. Funciones de Weber

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión** si

$$\alpha \cdot x = 0 \quad \text{para todo } \alpha \in \mathfrak{m}.$$

Los puntos de $\mathfrak{m}$ torsión forman un sub $\mathcal{O}_K$ modulo

$$\mathbb{T}[\mathfrak{m}] \subset \mathbb{T}.$$

La **funcion de Weber** es

$$\varpi : \mathbb{T} \to \hat{\mathbb{C}},$$

Sea $\mathbb{T}$ una curva elíptica con MC por $\mathcal{O}_K$. Llamamos a $x \in \mathbb{T}$ un **punto de $\mathfrak{m}$ torsión** si

$$\alpha \cdot x = 0 \quad \text{para todo } \alpha \in \mathfrak{m}.$$

Los puntos de $\mathfrak{m}$ torsión forman un sub $\mathcal{O}_K$ modulo

$$\mathbb{T}[\mathfrak{m}] \subset \mathbb{T}.$$

La **funcion de Weber** es

$$\varpi : \mathbb{T} \to \hat{\mathbb{C}}, \quad \varpi(z) = \begin{cases} \frac{g_4(\Lambda)g_6(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z) & \text{si } j(\mathbb{T}) \neq 0, 1728 \\ \frac{g_4(\Lambda)^2}{\Delta(\Lambda)}\wp_\Lambda(z)^2 & \text{si } j(\mathbb{T}) = 1728 \\ \frac{g_6(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z)^3 & \text{si } j(\mathbb{T}) = 0. \end{cases}$$

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

$$H_K = K(j(\mu)).$$

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

$$H_K = K(j(\mu)).$$

2. *Sea $\mathfrak{m} \subset \mathcal{O}_K$*

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

$$H_K = K(j(\mu)).$$

2. *Sea $\mathfrak{m} \subset \mathcal{O}_K$ y supongamos que $\mathbb{T}(\mu)$ tiene MC por $\mathcal{O}_K$*

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

$$H_K = K(j(\mu)).$$

2. *Sea $\mathfrak{m} \subset \mathcal{O}_K$ y supongamos que $\mathbb{T}(\mu)$ tiene MC por $\mathcal{O}_K$ (siempre existe un tal $\mu \in K - \mathbb{Q}$).*

Teorema de Weber-Fueter. *Sea $K/\mathbb{Q}$ cuadrática y compleja.*

1. *Para cada $\mu \in K - \mathbb{Q}$,*

$$H_K = K(j(\mu)).$$

2. *Sea $\mathfrak{m} \subset \mathcal{O}_K$ y supongamos que $\mathbb{T}(\mu)$ tiene MC por $\mathcal{O}_K$ (siempre existe un tal $\mu \in K - \mathbb{Q}$). Entonces*

$$K^{\mathfrak{m}} = H_K(\varpi(\mathbb{T}[\mathfrak{m}])).$$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^{\sigma}$$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^\sigma = \left(\frac{g_\mu(4)^3}{g_\mu(4)^3 - 27\Delta_\mu} \right)^\sigma$$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^\sigma = \left(\frac{g_\mu(4)^3}{g_\mu(4)^3 - 27\Delta_\mu}\right)^\sigma = j(E^\sigma).$$

Sigue que $\mathrm{Aut}(\mathbb{C})$ actúa en el conjunto

$$j(\mathrm{Ell}(\mathcal{O}_K))$$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^\sigma = \left(\frac{g_\mu(4)^3}{g_\mu(4)^3 - 27\Delta_\mu}\right)^\sigma = j(E^\sigma).$$

Sigue que $\mathrm{Aut}(\mathbb{C})$ actúa en el conjunto

$$j(\mathrm{Ell}(\mathcal{O}_K)) := \{j(E') | E' \in \mathrm{Ell}(\mathcal{O}_K)\}.$$

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^\sigma = \left(\frac{g_\mu(4)^3}{g_\mu(4)^3 - 27\Delta_\mu} \right)^\sigma = j(E^\sigma).$$

Sigue que $\mathrm{Aut}(\mathbb{C})$ actúa en el conjunto

$$j(\mathrm{Ell}(\mathcal{O}_K)) := \{j(E')|E' \in \mathrm{Ell}(\mathcal{O}_K)\}.$$

O sea, la orbita de $j(E)$ por $\mathrm{Aut}(\mathbb{C})$ es finita.

Para cada $\sigma \in \mathrm{Aut}(\mathbb{C})$ tenemos

$$j(E)^\sigma = \left(\frac{g_\mu(4)^3}{g_\mu(4)^3 - 27\Delta_\mu}\right)^\sigma = j(E^\sigma).$$

Sigue que $\mathrm{Aut}(\mathbb{C})$ actúa en el conjunto

$$j(\mathsf{Ell}(\mathcal{O}_K)) := \{j(E')|E' \in \mathsf{Ell}(\mathcal{O}_K)\}.$$

O sea, la orbita de $j(E)$ por $\mathrm{Aut}(\mathbb{C})$ es finita. Pero esto implica que $j(E) \in \overline{\mathbb{Q}}$.

“La teoría de Multiplicación Compleja, que forma una vinculación poderosa entre la teoría de números y análisis,

"La teoría de Multiplicación Compleja, que forma una vinculación poderosa entre la teoría de números y análisis, no es solamente la parte más hermosa de las matemáticas

"La teoría de Multiplicación Compleja, que forma una vinculación poderosa entre la teoría de números y análisis, no es solamente la parte más hermosa de las matemáticas sino la parte más hermosa de toda ciencia."

“La teoría de Multiplicación Compleja, que forma una vinculación poderosa entre la teoría de números y análisis, no es solamente la parte más hermosa de las matemáticas sino la parte más hermosa de toda ciencia.”

– David Hilbert, Zürich, 1933