

Una nueva generalización de la constante de Hermite¹

Emilio Lauret
Universidad Nacional de Córdoba

Seminario del IMAL “*Carlos Segovia Fernandez*”

21 de Octubre de 2011

¹Trabajo conjunto con W.K. Chan (Wesleyan University) y M.I. Icaza (Universidad de Talca)

Contenidos

- 1 Constante de Hermite clásica
 - Formas cuadráticas definidas positivas
 - Mínimo canónico
 - Constante de Hermite
 - Relación con lattices
- 2 Constantes de Hermite hermíticas
 - Formas binarias hermíticas
 - Constante de Hermite clásica
 - Constante de Hermite proyectiva
 - Resultados conocidos
- 3 Cálculo de la constante proyectiva
 - Correspondencias
 - Cálculo geométrico
 - Resultados

Contenidos

- 1 Constante de Hermite clásica
 - Formas cuadráticas definidas positivas
 - Mínimo canónico
 - Constante de Hermite
 - Relación con lattices
- 2 Constantes de Hermite hermíticas
 - Formas binarias hermíticas
 - Constante de Hermite clásica
 - Constante de Hermite proyectiva
 - Resultados conocidos
- 3 Cálculo de la constante proyectiva
 - Correspondencias
 - Cálculo geométrico
 - Resultados

Contenidos

- 1 Constante de Hermite clásica
 - Formas cuadráticas definidas positivas
 - Mínimo canónico
 - Constante de Hermite
 - Relación con lattices
- 2 Constantes de Hermite hermíticas
 - Formas binarias hermíticas
 - Constante de Hermite clásica
 - Constante de Hermite proyectiva
 - Resultados conocidos
- 3 Cálculo de la constante proyectiva
 - Correspondencias
 - Cálculo geométrico
 - Resultados

Formas cuadráticas definidas positivas

Una **forma cuadrática de rango n** es de la forma

$$S[x] = x^t S x \quad (x \in \mathbb{R}^n),$$

donde $S \in M_n(\mathbb{R})$ tal que $S^t = S$.

La forma S es definida positiva ($S > 0$) si $S[x] > 0$ para todo $x \neq 0$; equivalentemente si S tiene todos sus autovalores positivos.

Formas cuadráticas definidas positivas

Una **forma cuadrática de rango n** es de la forma

$$S[x] = x^t S x \quad (x \in \mathbb{R}^n),$$

donde $S \in M_n(\mathbb{R})$ tal que $S^t = S$.

La forma S es definida positiva ($S > 0$) si $S[x] > 0$ para todo $x \neq 0$; equivalentemente si S tiene todos sus autovalores positivos.

Formas cuadráticas definidas positivas

Una **forma cuadrática de rango n** es de la forma

$$S[x] = x^t S x \quad (x \in \mathbb{R}^n),$$

donde $S \in M_n(\mathbb{R})$ tal que $S^t = S$.

La forma S es definida positiva ($S > 0$) si $S[x] > 0$ para todo $x \neq 0$; equivalentemente si S tiene todos sus autovalores positivos.

Formas cuadráticas definidas positivas

Una **forma cuadrática de rango n** es de la forma

$$S[x] = x^t S x \quad (x \in \mathbb{R}^n),$$

donde $S \in M_n(\mathbb{R})$ tal que $S^t = S$.

La forma S es definida positiva ($S > 0$) si $S[x] > 0$ para todo $x \neq 0$; equivalentemente si S tiene todos sus autovalores positivos.

Mínimo canónico

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x].$$

Si $t > 0$ entonces $\mu(t \cdot S) = t \mu(S)$. Es razonable comparar $\mu(S)$ con $\det(S)^{1/n}$.

Teorema [Hermite]

Si $S > 0$ de rango n , entonces

$$\mu(S) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(S)^{\frac{1}{n}}.$$

Mínimo canónico

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x].$$

Si $t > 0$ entonces $\mu(t \cdot S) = t \mu(S)$. Es razonable comparar $\mu(S)$ con $\det(S)^{1/n}$.

Teorema [Hermite]

Si $S > 0$ de rango n , entonces

$$\mu(S) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(S)^{\frac{1}{n}}.$$

Mínimo canónico

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x].$$

Si $t > 0$ entonces $\mu(t \cdot S) = t \mu(S)$. Es razonable comparar $\mu(S)$ con $\det(S)^{1/n}$.

Teorema [Hermite]

Si $S > 0$ de rango n , entonces

$$\mu(S) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(S)^{\frac{1}{n}}.$$

Mínimo canónico

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x].$$

Si $t > 0$ entonces $\mu(t \cdot S) = t \mu(S)$. **Es razonable comparar $\mu(S)$ con $\det(S)^{1/n}$.**

Teorema [Hermite]

Si $S > 0$ de rango n , entonces

$$\mu(S) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(S)^{\frac{1}{n}}.$$

Mínimo canónico

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x].$$

Si $t > 0$ entonces $\mu(t \cdot S) = t \mu(S)$. **Es razonable comparar $\mu(S)$ con $\det(S)^{1/n}$.**

Teorema [Hermite]

Si $S > 0$ de rango n , entonces

$$\mu(S) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(S)^{\frac{1}{n}}.$$

Constante de Hermite Clásica

Definición

La **constante de Hermite clásica** de dimensión n se define como

$$\gamma_n = \max_S \frac{\mu(S)}{(\det(S))^{1/n}} = \max_S \min_{0 \neq x \in \mathbb{Z}^n} \frac{S[x]}{(\det(S))^{1/n}},$$

donde S recorre todas las formas cuadráticas definidas positivas de rango n .

Es inmediato que $\gamma_n \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$. En particular $\gamma_2 = \sqrt{\frac{4}{3}}$, pues el máximo se realiza en la forma S_1 .

Constante de Hermite Clásica

Definición

La **constante de Hermite clásica** de dimensión n se define como

$$\gamma_n = \max_S \frac{\mu(S)}{(\det(S))^{1/n}} = \max_S \min_{0 \neq x \in \mathbb{Z}^n} \frac{S[x]}{(\det(S))^{1/n}},$$

donde S recorre todas las formas cuadráticas definidas positivas de rango n .

Es inmediato que $\gamma_n \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$. En particular $\gamma_2 = \sqrt{\frac{4}{3}}$, pues el máximo se realiza en la forma S_1 .

Constante de Hermite Clásica

Definición

La **constante de Hermite clásica** de dimensión n se define como

$$\gamma_n = \max_S \frac{\mu(S)}{(\det(S))^{1/n}} = \max_S \min_{0 \neq x \in \mathbb{Z}^n} \frac{S[x]}{(\det(S))^{1/n}},$$

donde S recorre todas las formas cuadráticas definidas positivas de rango n .

Es inmediato que $\gamma_n \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$. En particular $\gamma_2 = \sqrt{\frac{4}{3}}$, pues el máximo se realiza en la forma S_1 .

Constante de Hermite Clásica

Definición

La **constante de Hermite clásica** de dimensión n se define como

$$\gamma_n = \max_S \frac{\mu(S)}{(\det(S))^{1/n}} = \max_S \min_{0 \neq x \in \mathbb{Z}^n} \frac{S[x]}{(\det(S))^{1/n}},$$

donde S recorre todas las formas cuadráticas definidas positivas de rango n .

Es inmediato que $\gamma_n \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$. En particular $\gamma_2 = \sqrt{\frac{4}{3}}$, pues el máximo se realiza en la forma S_1 .

Relación con lattices

Un **retículo** o **lattice** Λ en $\mathbb{R}^n$ es el conjunto de combinaciones lineales enteras de n vectores linealmente independientes en $\mathbb{R}^n$, en símbolos

$$\Lambda = \sum_{i=1}^n m_i v_i \quad \text{donde } m_i \in \mathbb{Z}.$$

Relación con lattices

Un **retículo** o **lattice** Λ en $\mathbb{R}^n$ es el conjunto de combinaciones lineales enteras de n vectores linealmente independientes en $\mathbb{R}^n$, en símbolos

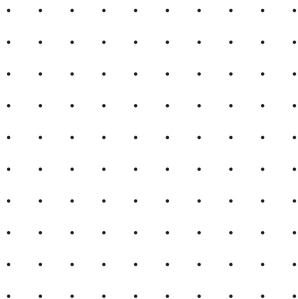
$$\Lambda = \sum_{i=1}^n m_i v_i \quad \text{donde } m_i \in \mathbb{Z}.$$

Relación con lattices

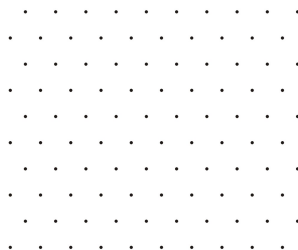
Un **retículo** o **lattice** Λ en $\mathbb{R}^n$ es el conjunto de combinaciones lineales enteras de n vectores linealmente independientes en $\mathbb{R}^n$, en símbolos

$$\Lambda = \sum_{i=1}^n m_i v_i \quad \text{donde } m_i \in \mathbb{Z}.$$

Ejemplos:



$\mathbb{Z}^2$



Lattice hexagonal

Existe una identificación entre formas cuadráticas definidas positivas y lattices, donde a formas cuadráticas ‘equivalentes’ le corresponden lattices ‘equivalentes’.

Si $S > 0$ existe M tal que $S = MM^t$. Denotemos $v_1, \dots, v_n$ las filas de M .

$$S = MM^t \iff \Lambda = \sum \mathbb{Z} \cdot v_i.$$

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x] = \min_{0 \neq v \in \Lambda} \|v\|^2.$$

Entonces

$$\gamma_n = \max_S \frac{\mu(S)}{\det(S)^{1/n}} = \max_{\Lambda} \frac{\min_{0 \neq v \in \Lambda} \|v\|^2}{\det(\Lambda)^{1/n}}.$$

Existe una identificación entre formas cuadráticas definidas positivas y lattices, donde a formas cuadráticas ‘equivalentes’ le corresponden lattices ‘equivalentes’.

Si $S > 0$ existe M tal que $S = MM^t$. Denotemos $v_1, \dots, v_n$ las filas de M .

$$S = MM^t \quad \longleftrightarrow \quad \Lambda = \sum \mathbb{Z} \cdot v_i.$$

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x] = \min_{0 \neq v \in \Lambda} \|v\|^2.$$

Entonces

$$\gamma_n = \max_S \frac{\mu(S)}{\det(S)^{1/n}} = \max_{\Lambda} \frac{\min_{0 \neq v \in \Lambda} \|v\|^2}{\det(\Lambda)^{1/n}}.$$

Existe una identificación entre formas cuadráticas definidas positivas y lattices, donde a formas cuadráticas ‘equivalentes’ le corresponden lattices ‘equivalentes’.

Si $S > 0$ existe M tal que $S = MM^t$. Denotemos $v_1, \dots, v_n$ las filas de M .

$$S = MM^t \quad \longleftrightarrow \quad \Lambda = \sum \mathbb{Z} \cdot v_i.$$

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x] = \min_{0 \neq v \in \Lambda} \|v\|^2.$$

Entonces

$$\gamma_n = \max_S \frac{\mu(S)}{\det(S)^{1/n}} = \max_{\Lambda} \frac{\min_{0 \neq v \in \Lambda} \|v\|^2}{\det(\Lambda)^{1/n}}.$$

Existe una identificación entre formas cuadráticas definidas positivas y lattices, donde a formas cuadráticas ‘equivalentes’ le corresponden lattices ‘equivalentes’.

Si $S > 0$ existe M tal que $S = MM^t$. Denotemos $v_1, \dots, v_n$ las filas de M .

$$S = MM^t \quad \longleftrightarrow \quad \Lambda = \sum \mathbb{Z} \cdot v_i.$$

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x] = \min_{0 \neq v \in \Lambda} \|v\|^2.$$

Entonces

$$\gamma_n = \max_S \frac{\mu(S)}{\det(S)^{1/n}} = \max_{\Lambda} \frac{\min_{0 \neq v \in \Lambda} \|v\|^2}{\det(\Lambda)^{1/n}}.$$

Existe una identificación entre formas cuadráticas definidas positivas y lattices, donde a formas cuadráticas ‘equivalentes’ le corresponden lattices ‘equivalentes’.

Si $S > 0$ existe M tal que $S = MM^t$. Denotemos $v_1, \dots, v_n$ las filas de M .

$$S = MM^t \quad \longleftrightarrow \quad \Lambda = \sum \mathbb{Z} \cdot v_i.$$

$$\mu(S) = \min_{0 \neq x \in \mathbb{Z}^n} S[x] = \min_{0 \neq v \in \Lambda} \|v\|^2.$$

Entonces

$$\gamma_n = \max_S \frac{\mu(S)}{\det(S)^{1/n}} = \max_{\Lambda} \frac{\min_{0 \neq v \in \Lambda} \|v\|^2}{\det(\Lambda)^{1/n}}.$$

Dado un lattice $\Lambda = \sum \mathbb{Z} \cdot v_i$, el conjunto

$$P = \left\{ \sum_{i=1}^n t_i v_i : 0 \leq t \leq 1 \right\}$$

es un dominio fundamental del lattice de traslaciones inducido por Λ . Llamamos **volumen** de Λ al volumen de P .

Se cumple que

$$\det(S) = \det(\Lambda) = \text{vol}(\Lambda)^2.$$

Dado un lattice $\Lambda = \sum \mathbb{Z} \cdot v_i$, el conjunto

$$P = \left\{ \sum_{i=1}^n t_i v_i : 0 \leq t_i \leq 1 \right\}$$

es un dominio fundamental del lattice de traslaciones inducido por Λ . Llamamos **volumen** de Λ al volumen de P .

Se cumple que

$$\det(S) = \det(\Lambda) = \text{vol}(\Lambda)^2.$$

Dado un lattice $\Lambda = \sum \mathbb{Z} \cdot v_i$, el conjunto

$$P = \left\{ \sum_{i=1}^n t_i v_i : 0 \leq t_i \leq 1 \right\}$$

es un dominio fundamental del lattice de traslaciones inducido por Λ . Llamamos **volumen** de Λ al volumen de P .

Se cumple que

$$\det(S) = \det(\Lambda) = \text{vol}(\Lambda)^2.$$

Empaquetamiento de esferas

Dado Λ un lattice, hay una distancia mínima entre sus puntos, que es igual a

$$r = \min_{0 \neq v \in \Lambda} \|v\|.$$

Entonces Λ induce un empaquetamiento de esferas de radio $r/2$ centradas en cada punto del lattice.

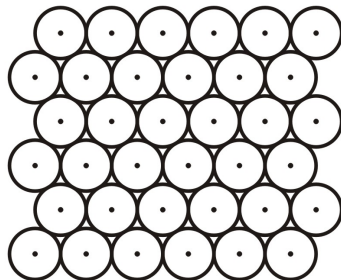
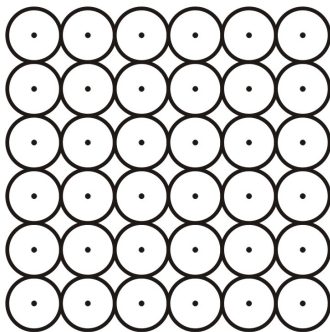
Empaquetamiento de esferas

Dado Λ un lattice, hay una distancia mínima entre sus puntos, que es igual a

$$r = \min_{0 \neq v \in \Lambda} \|v\|.$$

Entonces Λ induce un empaquetamiento de esferas de radio $r/2$ centradas en cada punto del lattice.

Ejemplos:

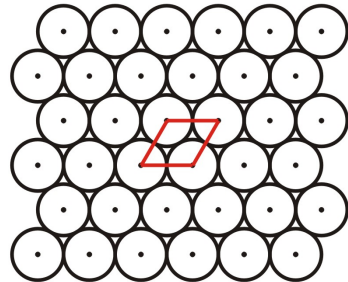
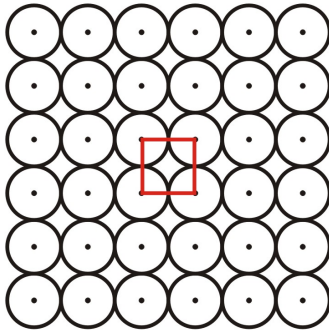


Definición

La **densidad** de un lattice Λ es

$$\delta(\Lambda) = \frac{\text{volumen de una bola}}{\text{volumen del lattice}}.$$

Ejemplos:



$$\delta(\Lambda) = \frac{\text{volumen de una bola}}{\text{volumen del lattice}}.$$

$$\Rightarrow \delta(\Lambda) = \frac{c_n r^n}{\det(\Lambda)^{1/2}} = c_n \left(\frac{r^2}{\det(\Lambda)^{1/n}} \right)^{n/2}.$$

$$\delta(\Lambda) = \frac{\text{volumen de una bola}}{\text{volumen del lattice}}.$$

$$\Rightarrow \delta(\Lambda) = \frac{c_n r^n}{\det(\Lambda)^{1/2}} = c_n \left(\frac{r^2}{\det(\Lambda)^{1/n}} \right)^{n/2}.$$

Formas binarias Hermíticas

Nos restringiremos al caso binario ($n = 2$).

Una **forma hermítica binaria** es de la forma

$$\begin{aligned} S[x] &= x^* S x = (\bar{x}_1 \quad \bar{x}_2) \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= a|x_1|^2 + b\bar{x}_1 x_2 + \bar{b}x_1 \bar{x}_2 + c|x_2|^2 \quad (x \in \mathbb{C}^2). \end{aligned}$$

En este caso $S^* = S \in M_2(\mathbb{C})$ (por lo tanto $a, c \in \mathbb{R}$).

$$S > 0 \iff \det(S) > 0 \quad \text{y} \quad a > 0.$$

Formas binarias Hermíticas

Nos restringiremos al caso binario ($n = 2$).

Una **forma hermítica binaria** es de la forma

$$\begin{aligned} S[x] &= x^* S x = (\bar{x}_1 \quad \bar{x}_2) \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= a|x_1|^2 + b\bar{x}_1 x_2 + \bar{b}x_1 \bar{x}_2 + c|x_2|^2 \quad (x \in \mathbb{C}^2). \end{aligned}$$

En este caso $S^* = S \in M_2(\mathbb{C})$ (por lo tanto $a, c \in \mathbb{R}$).

$$S > 0 \iff \det(S) > 0 \quad \text{y} \quad a > 0.$$

Formas binarias Hermíticas

Nos restringiremos al caso binario ($n = 2$).

Una **forma hermítica binaria** es de la forma

$$\begin{aligned} S[x] &= x^* S x = (\bar{x}_1 \quad \bar{x}_2) \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= a|x_1|^2 + b\bar{x}_1 x_2 + \bar{b}x_1 \bar{x}_2 + c|x_2|^2 \quad (x \in \mathbb{C}^2). \end{aligned}$$

En este caso $S^* = S \in M_2(\mathbb{C})$ (por lo tanto $a, c \in \mathbb{R}$).

$$S > 0 \iff \det(S) > 0 \quad \text{y} \quad a > 0.$$

Formas binarias Hermíticas

Nos restringiremos al caso binario ($n = 2$).

Una **forma hermítica binaria** es de la forma

$$\begin{aligned} S[x] &= x^* S x = (\bar{x}_1 \quad \bar{x}_2) \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= a|x_1|^2 + b\bar{x}_1 x_2 + \bar{b}x_1 \bar{x}_2 + c|x_2|^2 \quad (x \in \mathbb{C}^2). \end{aligned}$$

En este caso $S^* = S \in M_2(\mathbb{C})$ (por lo tanto $a, c \in \mathbb{R}$).

$$S > 0 \iff \det(S) > 0 \quad \text{y} \quad a > 0.$$

Constante de Hermite hermítica clásica

Para definir el mínimo de una forma hermítica binaria nos hacen falta **enteros** en donde evaluar la forma.

Fijemos K una extensión cuadrática imaginaria de $\mathbb{Q}$, esto es un cuerpo $K \subset \mathbb{C}$ tal que $\dim_{\mathbb{Q}}(K) = 2$ y $K \not\subset \mathbb{R}$.

Están parametrizadas por

$$K = \mathbb{Q}(\sqrt{-D}) \quad D \in \mathbb{N} \text{ libre de cuadrados.}$$

Constante de Hermite hermítica clásica

Para definir el mínimo de una forma hermítica binaria nos hacen falta **enteros** en donde evaluar la forma.

Fijemos K una extensión cuadrática imaginaria de $\mathbb{Q}$, esto es un cuerpo $K \subset \mathbb{C}$ tal que $\dim_{\mathbb{Q}}(K) = 2$ y $K \not\subset \mathbb{R}$.

Están parametrizadas por

$$K = \mathbb{Q}(\sqrt{-D}) \quad D \in \mathbb{N} \text{ libre de cuadrados.}$$

Constante de Hermite hermítica clásica

Para definir el mínimo de una forma hermítica binaria nos hacen falta **enteros** en donde evaluar la forma.

Fijemos K una extensión cuadrática imaginaria de $\mathbb{Q}$, esto es un cuerpo $K \subset \mathbb{C}$ tal que $\dim_{\mathbb{Q}}(K) = 2$ y $K \not\subset \mathbb{R}$.

Están parametrizadas por

$$K = \mathbb{Q}(\sqrt{-D}) \quad D \in \mathbb{N} \text{ libre de cuadrados.}$$

Constante de Hermite hermítica clásica

Para definir el mínimo de una forma hermítica binaria nos hacen falta **enteros** en donde evaluar la forma.

Fijemos K una extensión cuadrática imaginaria de $\mathbb{Q}$, esto es un cuerpo $K \subset \mathbb{C}$ tal que $\dim_{\mathbb{Q}}(K) = 2$ y $K \not\subset \mathbb{R}$.

Están parametrizadas por

$$K = \mathbb{Q}(\sqrt{-D}) \quad D \in \mathbb{N} \text{ libre de cuadrados.}$$

Constante de Hermite hermítica clásica

Para definir el mínimo de una forma hermítica binaria nos hacen falta **enteros** en donde evaluar la forma.

Fijemos K una extensión cuadrática imaginaria de $\mathbb{Q}$, esto es un cuerpo $K \subset \mathbb{C}$ tal que $\dim_{\mathbb{Q}}(K) = 2$ y $K \not\subset \mathbb{R}$.

Están parametrizadas por

$$K = \mathbb{Q}(\sqrt{-D}) \quad D \in \mathbb{N} \text{ libre de cuadrados.}$$

Sea $\mathcal{O}$ el anillo de enteros de $K = \mathbb{Q}(\sqrt{-D})$, esto es

$$\mathcal{O} = \mathbb{Z}[\omega] \quad \text{donde} \quad \omega = \begin{cases} \sqrt{-D} & \text{si } D \equiv 1, 2 \pmod{4}, \\ \frac{1 + \sqrt{-D}}{2} & \text{si } D \equiv 3 \pmod{4}. \end{cases}$$

Ejemplos:

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$ (enteros de Gauss),
- $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$,
- $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (enteros de Eisenstein).

Sea $\mathcal{O}$ el anillo de enteros de $K = \mathbb{Q}(\sqrt{-D})$, esto es

$$\mathcal{O} = \mathbb{Z}[\omega] \quad \text{donde} \quad \omega = \begin{cases} \sqrt{-D} & \text{si } D \equiv 1, 2 \pmod{4}, \\ \frac{1 + \sqrt{-D}}{2} & \text{si } D \equiv 3 \pmod{4}. \end{cases}$$

Ejemplos:

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$ (enteros de Gauss),
- $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$,
- $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (enteros de Eisenstein).

Sea $\mathcal{O}$ el anillo de enteros de $K = \mathbb{Q}(\sqrt{-D})$, esto es

$$\mathcal{O} = \mathbb{Z}[\omega] \quad \text{donde} \quad \omega = \begin{cases} \sqrt{-D} & \text{si } D \equiv 1, 2 \pmod{4}, \\ \frac{1 + \sqrt{-D}}{2} & \text{si } D \equiv 3 \pmod{4}. \end{cases}$$

Ejemplos:

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$ (enteros de Gauss),
- $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$,
- $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (enteros de Eisenstein).

Sea $\mathcal{O}$ el anillo de enteros de $K = \mathbb{Q}(\sqrt{-D})$, esto es

$$\mathcal{O} = \mathbb{Z}[\omega] \quad \text{donde} \quad \omega = \begin{cases} \sqrt{-D} & \text{si } D \equiv 1, 2 \pmod{4}, \\ \frac{1 + \sqrt{-D}}{2} & \text{si } D \equiv 3 \pmod{4}. \end{cases}$$

Ejemplos:

- $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$ (enteros de Gauss),
- $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$,
- $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (enteros de Eisenstein).

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathcal{O}^2} S[x].$$

Definición

La **constante de Hermite clásica** está dada por

$$\gamma_{K,2} = \max_S \frac{\mu(S)}{(\det(S))^{1/2}},$$

donde S recorre todas las formas binarias hermíticas definidas positivas.

Definición

El **mínimo canónico** de $S > 0$ está dado por

$$\mu(S) = \min_{0 \neq x \in \mathcal{O}^2} S[x].$$

Definición

La **constante de Hermite clásica** está dada por

$$\gamma_{K,2} = \max_S \frac{\mu(S)}{(\det(S))^{1/2}},$$

donde S recorre todas las formas binarias hermíticas definidas positivas.

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

Constante de Hermite proyectiva

Sea $x = (\alpha, \beta)^t \in \mathcal{O}^2$.

- Denotamos $\langle \alpha, \beta \rangle = \alpha\mathcal{O} + \beta\mathcal{O} \subseteq \mathcal{O}$ al ideal en $\mathcal{O}$ generado por α y β .
- Denotamos $N(\langle \alpha, \beta \rangle) = \#(\mathcal{O}/\langle \alpha, \beta \rangle) \in \mathbb{N}$ a la norma del ideal $\langle \alpha, \beta \rangle$.

En el caso real: si $x = (\alpha, \beta)^t \in \mathbb{Z}^2$ entonces

$$\langle \alpha, \beta \rangle = \text{mcd}(\alpha, \beta) \cdot \mathbb{Z} \quad \text{y} \quad N(\langle \alpha, \beta \rangle) = \text{mcd}(\alpha, \beta).$$

En el caso real: supongamos que

$$S[x] = \mu(S) \quad (x \in \mathbb{Z}^n \text{ realiza el mínimo de } S),$$

$$\Rightarrow \text{mcd}(x_1, \dots, x_n) = 1,$$

$$\Rightarrow \langle x \rangle = \mathbb{Z} \iff N(\langle x \rangle) = 1 \quad (x \text{ es unimodular}).$$

Esto NO vale en general en el caso hermítico. Más precisamente, para algunos K existen $S > 0$ y $x \in \mathcal{O}^2$ tales que

$$S[x] = \mu(S) \quad \text{y} \quad N(\langle x \rangle) > 1.$$

En el caso real: supongamos que

$$S[x] = \mu(S) \quad (x \in \mathbb{Z}^n \text{ realiza el mínimo de } S),$$

$$\Rightarrow \text{mcd}(x_1, \dots, x_n) = 1,$$

$$\Rightarrow \langle x \rangle = \mathbb{Z} \iff N(\langle x \rangle) = 1 \quad (x \text{ es unimodular}).$$

Esto NO vale en general en el caso hermítico. Más precisamente, para algunos K existen $S > 0$ y $x \in \mathcal{O}^2$ tales que

$$S[x] = \mu(S) \quad \text{y} \quad N(\langle x \rangle) > 1.$$

En el caso real: supongamos que

$$S[x] = \mu(S) \quad (x \in \mathbb{Z}^n \text{ realiza el mínimo de } S),$$

$$\Rightarrow \text{mcd}(x_1, \dots, x_n) = 1,$$

$$\Rightarrow \langle x \rangle = \mathbb{Z} \iff N(\langle x \rangle) = 1 \quad (x \text{ es unimodular}).$$

Esto NO vale en general en el caso hermítico. Más precisamente, para algunos K existen $S > 0$ y $x \in \mathcal{O}^2$ tales que

$$S[x] = \mu(S) \quad \text{y} \quad N(\langle x \rangle) > 1.$$

En el caso real: supongamos que

$$S[x] = \mu(S) \quad (x \in \mathbb{Z}^n \text{ realiza el mínimo de } S),$$

$$\Rightarrow \text{mcd}(x_1, \dots, x_n) = 1,$$

$$\Rightarrow \langle x \rangle = \mathbb{Z} \iff N(\langle x \rangle) = 1 \quad (x \text{ es unimodular}).$$

Esto NO vale en general en el caso hermítico. Más precisamente,
para algunos K existen $S > 0$ y $x \in \mathcal{O}^2$ tales que

$$S[x] = \mu(S) \quad \text{y} \quad N(\langle x \rangle) > 1.$$

En el caso real: supongamos que

$$S[x] = \mu(S) \quad (x \in \mathbb{Z}^n \text{ realiza el mínimo de } S),$$

$$\Rightarrow \text{mcd}(x_1, \dots, x_n) = 1,$$

$$\Rightarrow \langle x \rangle = \mathbb{Z} \iff N(\langle x \rangle) = 1 \quad (x \text{ es unimodular}).$$

Esto NO vale en general en el caso hermítico. Más precisamente, para algunos K existen $S > 0$ y $x \in \mathcal{O}^2$ tales que

$$S[x] = \mu(S) \quad \text{y} \quad N(\langle x \rangle) > 1.$$

El **número de clase** de una extensión cuadrática imaginaria K está dado por

$$h_K = \# \left(\frac{\{\text{ideales fraccionarios en } K\}}{\{\text{ideales principales en } K\}} \right).$$

$\mathcal{O}$ es DFU si y sólo si es DIP.

$h_K = 1$ si y sólo si $\mathcal{O}$ es DFU.

Mientras más grande es h_K "menos DFU" es $\mathcal{O}$.

Si $K = \mathbb{Q}(\sqrt{-D})$ con $D > 0$ libre de cuadrados, entonces

$$h_K = 1 \iff D = 1, 2, 3, 7, 11, 19, 43, 163.$$

El **número de clase** de una extensión cuadrática imaginaria K está dado por

$$h_K = \# \left(\frac{\{\text{ideales fraccionarios en } K\}}{\{\text{ideales principales en } K\}} \right).$$

$\mathcal{O}$ es DFU si y sólo si es DIP.

$h_K = 1$ si y sólo si $\mathcal{O}$ es DFU.

Mientras más grande es h_K “menos DFU” es $\mathcal{O}$.

Si $K = \mathbb{Q}(\sqrt{-D})$ con $D > 0$ libre de cuadrados, entonces

$$h_K = 1 \iff D = 1, 2, 3, 7, 11, 19, 43, 163.$$

El **número de clase** de una extensión cuadrática imaginaria K está dado por

$$h_K = \# \left(\frac{\{\text{ideales fraccionarios en } K\}}{\{\text{ideales principales en } K\}} \right).$$

$\mathcal{O}$ es DFU si y sólo si es DIP.

$h_K = 1$ si y sólo si $\mathcal{O}$ es DFU.

Mientras más grande es h_K "menos DFU" es $\mathcal{O}$.

Si $K = \mathbb{Q}(\sqrt{-D})$ con $D > 0$ libre de cuadrados, entonces

$$h_K = 1 \iff D = 1, 2, 3, 7, 11, 19, 43, 163.$$

El **número de clase** de una extensión cuadrática imaginaria K está dado por

$$h_K = \# \left(\frac{\{\text{ideales fraccionarios en } K\}}{\{\text{ideales principales en } K\}} \right).$$

$\mathcal{O}$ es DFU si y sólo si es DIP.

$h_K = 1$ si y sólo si $\mathcal{O}$ es DFU.

Mientras más grande es h_K “menos DFU” es $\mathcal{O}$.

Si $K = \mathbb{Q}(\sqrt{-D})$ con $D > 0$ libre de cuadrados, entonces

$$h_K = 1 \quad \Longleftrightarrow \quad D = 1, 2, 3, 7, 11, 19, 43, 163.$$

El **número de clase** de una extensión cuadrática imaginaria K está dado por

$$h_K = \# \left(\frac{\{\text{ideales fraccionarios en } K\}}{\{\text{ideales principales en } K\}} \right).$$

$\mathcal{O}$ es DFU si y sólo si es DIP.

$h_K = 1$ si y sólo si $\mathcal{O}$ es DFU.

Mientras más grande es h_K “menos DFU” es $\mathcal{O}$.

Si $K = \mathbb{Q}(\sqrt{-D})$ con $D > 0$ libre de cuadrados, entonces

$$h_K = 1 \quad \Longleftrightarrow \quad D = 1, 2, 3, 7, 11, 19, 43, 163.$$

Recordemos que escribimos $x = (\alpha, \beta)^t$.

Definición

Definimos el **mínimo proyectivo** como

$$\mu^P(S) = \min_{0 \neq x \in \mathcal{O}^2} \frac{S[x]}{N(\langle \alpha, \beta \rangle)}.$$

Es claro que

$$\mu^P(S) \leq \mu(S).$$

Si $h_K = 1$ entonces $S[x] = \mu(S)$ implica x es unimodular, por lo tanto

$$\mu(S) = \mu^P(S).$$

Recordemos que escribimos $x = (\alpha, \beta)^t$.

Definición

Definimos el **mínimo proyectivo** como

$$\mu^P(S) = \min_{0 \neq x \in \mathcal{O}^2} \frac{S[x]}{N(\langle \alpha, \beta \rangle)}.$$

Es claro que

$$\mu^P(S) \leq \mu(S).$$

Si $h_K = 1$ entonces $S[x] = \mu(S)$ implica x es unimodular, por lo tanto

$$\mu(S) = \mu^P(S).$$

Recordemos que escribimos $x = (\alpha, \beta)^t$.

Definición

Definimos el **mínimo proyectivo** como

$$\mu^P(S) = \min_{0 \neq x \in \mathcal{O}^2} \frac{S[x]}{N(\langle \alpha, \beta \rangle)}.$$

Es claro que

$$\mu^P(S) \leq \mu(S).$$

Si $h_K = 1$ entonces $S[x] = \mu(S)$ implica x es unimodular, por lo tanto

$$\mu(S) = \mu^P(S).$$

Recordemos que escribimos $x = (\alpha, \beta)^t$.

Definición

Definimos el **mínimo proyectivo** como

$$\mu^P(S) = \min_{0 \neq x \in \mathcal{O}^2} \frac{S[x]}{N(\langle \alpha, \beta \rangle)}.$$

Es claro que

$$\mu^P(S) \leq \mu(S).$$

Si $h_K = 1$ entonces $S[x] = \mu(S)$ implica x es unimodular, por lo tanto

$$\mu(S) = \mu^P(S).$$

Definición

Definimos la **constante de Hermite proyectiva** como

$$\gamma_{K,2}^p = \max_S \frac{\mu^p(S)}{(\det(S))^{1/2}},$$

donde S recorre todas las formas binarias hermíticas definidas positivas.

Es claro que

$$\gamma_{K,2}^p \leq \gamma_{K,2},$$

y ellos coinciden si $h_K = 1$.

Definición

Definimos la **constante de Hermite proyectiva** como

$$\gamma_{K,2}^p = \max_S \frac{\mu^p(S)}{(\det(S))^{1/2}},$$

donde S recorre todas las formas binarias hermíticas definidas positivas.

Es claro que

$$\gamma_{K,2}^p \leq \gamma_{K,2},$$

y ellos coinciden si $h_K = 1$.

Resultados conocidos

Para $K = \mathbb{Q}$:

- $n = 2, 3, 4, 5, 6, 7, 8$.
- $n = 24$ (Leech lattice).

Para $K = \mathbb{Q}(\sqrt{-D})$ y $n = 2$:

- $D = 1$, Speiser (1932).
- $D = 1, 2, 3, 7, 11, 19$, Perron (1933).
- Oberseider completó los casos con número de clase 1 ($D = 43, 67, 163$) y calculó $\gamma_{K,2}$ (constante clásica) para los casos $D = 5, 6, 10, 13, 15$ (1934).
- Oppenheim mostró que

$$\gamma_{K,2} \leq \frac{|d_K|}{2},$$

y que la igualdad vale si y sólo si $x^2 \equiv -2 \pmod{D}$ tiene solución (1934).

Resultados conocidos

Para $K = \mathbb{Q}$:

- $n = 2, 3, 4, 5, 6, 7, 8$.
- $n = 24$ (Leech lattice).

Para $K = \mathbb{Q}(\sqrt{-D})$ y $n = 2$:

- $D = 1$, Speiser (1932).
- $D = 1, 2, 3, 7, 11, 19$, Perron (1933).
- Oberseider completó los casos con número de clase 1 ($D = 43, 67, 163$) y calculó $\gamma_{K,2}$ (constante clásica) para los casos $D = 5, 6, 10, 13, 15$ (1934).
- Oppenheim mostró que

$$\gamma_{K,2} \leq \frac{|d_K|}{2},$$

y que la igualdad vale si y sólo si $x^2 \equiv -2 \pmod{D}$ tiene solución (1934).

Resultados conocidos

Para $K = \mathbb{Q}$:

- $n = 2, 3, 4, 5, 6, 7, 8$.
- $n = 24$ (Leech lattice).

Para $K = \mathbb{Q}(\sqrt{-D})$ y $n = 2$:

- $D = 1$, Speiser (1932).
- $D = 1, 2, 3, 7, 11, 19$, Perron (1933).
- Oberseider completó los casos con número de clase 1 ($D = 43, 67, 163$) y calculó $\gamma_{K,2}$ (constante clásica) para los casos $D = 5, 6, 10, 13, 15$ (1934).
- Oppenheim mostró que

$$\gamma_{K,2} \leq \frac{|d_K|}{2},$$

y que la igualdad vale si y sólo si $x^2 \equiv -2 \pmod{D}$ tiene solución (1934).

Resultados conocidos

Para $K = \mathbb{Q}$:

- $n = 2, 3, 4, 5, 6, 7, 8$.
- $n = 24$ (Leech lattice).

Para $K = \mathbb{Q}(\sqrt{-D})$ y $n = 2$:

- $D = 1$, Speiser (1932).
- $D = 1, 2, 3, 7, 11, 19$, Perron (1933).
- Oberseider completó los casos con número de clase 1 ($D = 43, 67, 163$) y calculó $\gamma_{K,2}$ (constante clásica) para los casos $D = 5, 6, 10, 13, 15$ (1934).
- Oppenheim mostró que

$$\gamma_{K,2} \leq \frac{|d_K|}{2},$$

y que la igualdad vale si y sólo si $x^2 \equiv -2 \pmod{D}$ tiene solución (1934).

Nuestro método

Todas las formas hermíticas binarias sobre $K = \mathbb{Q}(\sqrt{-D})$ son:

$$\mathcal{P}_{K,2} = \left\{ \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \in M_2(\mathbb{C}) : ac - |b|^2 > 0, c > 0 \right\}.$$

$$\mathcal{P}_{K,2}(\Delta) = \{S \in \mathcal{P}_{K,2} : \det(S) = \Delta\}.$$

El modelo del semiespacio superior del espacio hiperbólico tridimensional es:

$$\mathbb{H}^3 = \{(z, \zeta) \in \mathbb{C} \times \mathbb{R} : \zeta > 0\}.$$

Nuestro método

Todas las formas hermíticas binarias sobre $K = \mathbb{Q}(\sqrt{-D})$ son:

$$\mathcal{P}_{K,2} = \left\{ \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \in M_2(\mathbb{C}) : ac - |b|^2 > 0, c > 0 \right\}.$$

$$\mathcal{P}_{K,2}(\Delta) = \{S \in \mathcal{P}_{K,2} : \det(S) = \Delta\}.$$

El modelo del semiespacio superior del espacio hiperbólico tridimensional es:

$$H^3 = \{(z, \zeta) \in \mathbb{C} \times \mathbb{R} : \zeta > 0\}.$$

El grupo $GL_2(\mathbb{C})$ actúa en ambos conjuntos por:

$$g \cdot S = |\det(S)|(g^{-1})^* S(g^{-1}),$$

$$g \cdot (z, \zeta) = \left(\frac{(az + b)\overline{(cz + d)} + a\bar{c}\zeta^2}{|cz + d|^2 + |c|^2\zeta^2}, \frac{|\det g| \zeta}{|cz + d|^2 + |c|^2\zeta^2} \right).$$

El grupo $GL_2(\mathbb{C})$ actúa en ambos conjuntos por:

$$g \cdot S = |\det(S)|(g^{-1})^* S (g^{-1}),$$

$$g \cdot (z, \zeta) = \left(\frac{(az + b)\overline{(cz + d)} + a\bar{c}\zeta^2}{|cz + d|^2 + |c|^2\zeta^2}, \frac{|\det g| \zeta}{|cz + d|^2 + |c|^2\zeta^2} \right).$$

El mapeo $\Phi : \mathcal{P}_{K,2} \rightarrow H^3$ definido por

$$\Phi \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} = \left(\frac{-b}{a}, \frac{\sqrt{ac - |b|^2}}{a} \right),$$

es $GL_2(\mathbb{C})$ -equivariante, y $\Phi_\Delta := \Phi|_{\mathcal{P}_{K,2}(\Delta)} : \mathcal{P}_{K,2}(\Delta) \rightarrow H^3$ es una biyección para todo $\Delta > 0$.

Se llaman **cúspides** a los elementos λ de $\mathbb{P}^1(K)$, i.e.

$$\lambda \in K \subset \mathbb{C} \quad \text{o} \quad \lambda = \infty.$$

Notación:

- Si $\lambda \in K$ escribimos $\lambda = \alpha/\beta$ con $\alpha, \beta \in \mathcal{O}$.
- Si $\lambda = \infty$ escribimos $\lambda = 1/0$.

Se llaman **cúspides** a los elementos λ de $\mathbb{P}^1(K)$, i.e.

$$\lambda \in K \subset \mathbb{C} \quad \text{o} \quad \lambda = \infty.$$

Notación:

- Si $\lambda \in K$ escribimos $\lambda = \alpha/\beta$ con $\alpha, \beta \in \mathcal{O}$.
- Si $\lambda = \infty$ escribimos $\lambda = 1/0$.

Correspondencias

$$\mathcal{P}_{K,2}(\Delta) \longleftrightarrow H^3$$

$$S = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \longrightarrow P_S = \left(\frac{-b}{a}, \frac{\sqrt{ac - |b|^2}}{a} \right)$$

$$S_P = \frac{\sqrt{\Delta}}{\zeta} \begin{pmatrix} 1 & -z \\ -\bar{z} & |z|^2 + \zeta^2 \end{pmatrix} \longleftarrow P = (z, \zeta)$$

$$x = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathcal{O}_K^2 \longrightarrow \lambda = \frac{\alpha}{\beta} \in \mathbb{P}^1(K)$$

$$S[x] = x^* S x \longleftrightarrow ?$$

Distancia

La distancia entre un punto $P = (z, \zeta) \in \mathbb{H}^3$ y una cúspide $\lambda = \alpha/\beta$ está dada por

$$d(P, \lambda) = \frac{|\beta z - \alpha|^2 + |\beta|^2 \zeta^2}{\zeta N(\alpha, \beta)}.$$

Uno puede chequear que

$$d(P, \lambda) = \frac{S[x]}{\sqrt{\Delta} N(\alpha, \beta)}.$$

Entonces

$$\gamma_{K,2}^P = \max_{P \in \mathbb{H}^3} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda).$$

Esto convierte nuestro problema *aritmético* en un problema *geométrico*.

Distancia

La **distancia entre un punto** $P = (z, \zeta) \in \mathbb{H}^3$ **y una cúspide** $\lambda = \alpha/\beta$ **está dada por**

$$d(P, \lambda) = \frac{|\beta z - \alpha|^2 + |\beta|^2 \zeta^2}{\zeta N(\alpha, \beta)}.$$

Uno puede chequear que

$$d(P, \lambda) = \frac{S[x]}{\sqrt{\Delta} N(\alpha, \beta)}.$$

Entonces

$$\gamma_{K,2}^P = \max_{P \in \mathbb{H}^3} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda).$$

Esto convierte nuestro problema aritmético en un problema geométrico.

Distancia

La **distancia entre un punto** $P = (z, \zeta) \in \mathbb{H}^3$ **y una cúspide** $\lambda = \alpha/\beta$ **está dada por**

$$d(P, \lambda) = \frac{|\beta z - \alpha|^2 + |\beta|^2 \zeta^2}{\zeta N(\alpha, \beta)}.$$

Uno puede chequear que

$$d(P, \lambda) = \frac{S[x]}{\sqrt{\Delta} N(\alpha, \beta)}.$$

Entonces

$$\gamma_{K,2}^P = \max_{P \in \mathbb{H}^3} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda).$$

*Esto convierte nuestro problema **aritmético** en un problema **geométrico**.*

Distancia

La **distancia entre un punto** $P = (z, \zeta) \in \mathbb{H}^3$ **y una cúspide** $\lambda = \alpha/\beta$ está dada por

$$d(P, \lambda) = \frac{|\beta z - \alpha|^2 + |\beta|^2 \zeta^2}{\zeta N(\alpha, \beta)}.$$

Uno puede chequear que

$$d(P, \lambda) = \frac{S[x]}{\sqrt{\Delta} N(\alpha, \beta)}.$$

Entonces

$$\gamma_{K,2}^P = \max_{P \in \mathbb{H}^3} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda).$$

*Esto convierte nuestro problema **aritmético** en un problema **geométrico**.*

Distancia

La **distancia entre un punto** $P = (z, \zeta) \in \mathbb{H}^3$ **y una cúspide** $\lambda = \alpha/\beta$ está dada por

$$d(P, \lambda) = \frac{|\beta z - \alpha|^2 + |\beta|^2 \zeta^2}{\zeta N(\alpha, \beta)}.$$

Uno puede chequear que

$$d(P, \lambda) = \frac{S[x]}{\sqrt{\Delta} N(\alpha, \beta)}.$$

Entonces

$$\gamma_{K,2}^P = \max_{P \in \mathbb{H}^3} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda).$$

*Esto convierte nuestro problema **aritmético** en un problema **geométrico**.*

Cálculo geométrico de $\gamma_{K,2}^p$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Cálculo geométrico de $\gamma_{K,2}^p$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Cálculo geométrico de $\gamma_{K,2}^p$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Cálculo geométrico de $\gamma_{K,2}^p$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Cálculo geométrico de $\gamma_{K,2}^p$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Cálculo geométrico de $\gamma_{K,2}^P$

Observaciones:

Para $P = (z, \zeta) \in \mathbb{H}^3$ y $\lambda = \alpha/\beta \neq \infty$, se puede chequear que

$$d(P, \infty) = \frac{1}{\zeta}, \quad d(P, \lambda) = \frac{|P - \lambda|^2}{\zeta N_\lambda} \quad \left(N_\lambda = \frac{N\langle \alpha, \beta \rangle}{|\beta|^2} \right).$$

El conjunto

$$S(\lambda, \mu) := \{P \in \mathbb{H}^3 : d(P, \lambda) = d(P, \mu)\}$$

es una semiesfera o un plano, perpendicular al borde $\mathbb{C}$.

$S(\lambda, \infty)$ es una semiesfera centrada en λ con radio $\sqrt{N_\lambda}$.

Llamemos **conjunto minimal** asociado a una cúspide λ a

$$H(\lambda) = \{P \in H^3 : d(P, \lambda) \leq d(P, \mu) \text{ for all } \mu \neq \lambda\}.$$

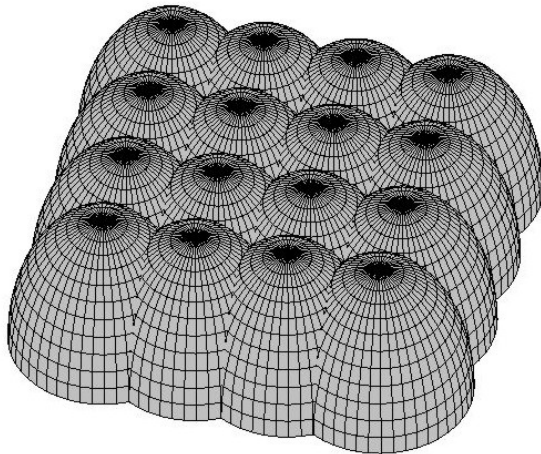
Claramente, si $P \in H(\lambda)$ entonces $\min_{\mu \in \mathbb{P}^1(K)} d(P, \mu) = d(P, \lambda)$.

Llamemos **conjunto minimal** asociado a una cúspide λ a

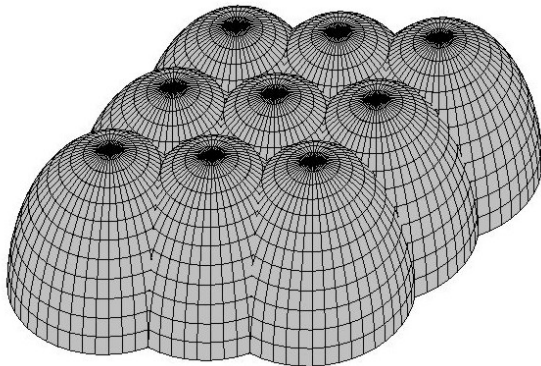
$$H(\lambda) = \{P \in \mathbb{H}^3 : d(P, \lambda) \leq d(P, \mu) \text{ for all } \mu \neq \lambda\}.$$

Claramente, si $P \in H(\lambda)$ entonces $\min_{\mu \in \mathbb{P}^1(K)} d(P, \mu) = d(P, \lambda)$.

Por ejemplo: $H(\infty)$ por $K = \mathbb{Q}(\sqrt{-1})$,



Por ejemplo: $H(\infty)$ por $K = \mathbb{Q}(\sqrt{-3})$,



Denotemos $\Gamma = \mathrm{SL}_2(\mathcal{O})$ al grupo de Bianchi asociado a K .

$d(\cdot, \cdot)$ es invariante bajo la acción de Γ , i.e.

$$d(g \cdot P, g \cdot \lambda) = d(P, \lambda) \quad \forall g \in \Gamma.$$

Consideremos

$$\Gamma(\lambda) = \{g \in \Gamma : g \cdot \lambda = \lambda\}.$$

Entonces $\Gamma(\lambda)$ deja estable a $H(\lambda)$ y a su frontera $\partial H(\lambda)$.

Denotemos $\Gamma = \mathrm{SL}_2(\mathcal{O})$ al grupo de Bianchi asociado a K .

$d(\cdot, \cdot)$ es invariante bajo la acción de Γ , i.e.

$$d(g \cdot P, g \cdot \lambda) = d(P, \lambda) \quad \forall g \in \Gamma.$$

Consideremos

$$\Gamma(\lambda) = \{g \in \Gamma : g \cdot \lambda = \lambda\}.$$

Entonces $\Gamma(\lambda)$ deja estable a $H(\lambda)$ y a su frontera $\partial H(\lambda)$.

Denotemos $\Gamma = \mathrm{SL}_2(\mathcal{O})$ al grupo de Bianchi asociado a K .

$d(\cdot, \cdot)$ es invariante bajo la acción de Γ , i.e.

$$d(g \cdot P, g \cdot \lambda) = d(P, \lambda) \quad \forall g \in \Gamma.$$

Consideremos

$$\Gamma(\lambda) = \{g \in \Gamma : g \cdot \lambda = \lambda\}.$$

Entonces $\Gamma(\lambda)$ deja estable a $H(\lambda)$ y a su frontera $\partial H(\lambda)$.

Teorema [Mendoza]

$$\begin{aligned}\gamma_{K,2}^P &= \max_{P \in \bigcup_{\lambda} \partial H(\lambda)} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda) \\ &= \max_{1 \leq i \leq h} \max_{P \in \partial H(\lambda_i)} d(P, \lambda_i) \\ &= \max_{1 \leq i \leq h} \max_{P \in \tilde{T}_i} d(P, \lambda_i),\end{aligned}$$

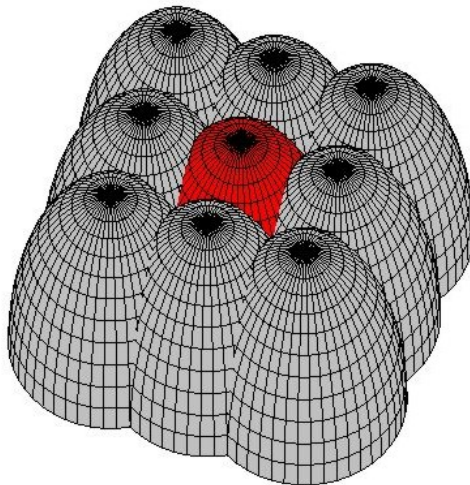
donde $\tilde{T}_i$ denota un dominio fundamental de $\partial H(\lambda_i)$ bajo la acción de $\Gamma(\lambda_i)$.

Teorema [Mendoza]

$$\begin{aligned}\gamma_{K,2}^p &= \max_{P \in \bigcup_{\lambda} \partial H(\lambda)} \min_{\lambda \in \mathbb{P}^1(K)} d(P, \lambda) \\ &= \max_{1 \leq i \leq h} \max_{P \in \partial H(\lambda_i)} d(P, \lambda_i) \\ &= \max_{1 \leq i \leq h} \max_{P \in \tilde{T}_i} d(P, \lambda_i),\end{aligned}$$

donde $\tilde{T}_i$ denota un dominio fundamental de $\partial H(\lambda_i)$ bajo la acción de $\Gamma(\lambda_i)$.

Ejemplo: $\tilde{T}_1 = \partial H(\infty)/\Gamma(\infty)$ para $K = \mathbb{Q}(\sqrt{-1})$ ($h_K = 1$),



Ejemplo: $\tilde{T}_1 = \partial H(\infty)/\Gamma(\infty)$ para $K = \mathbb{Q}(\sqrt{-39})$ ($h_K = 4$),

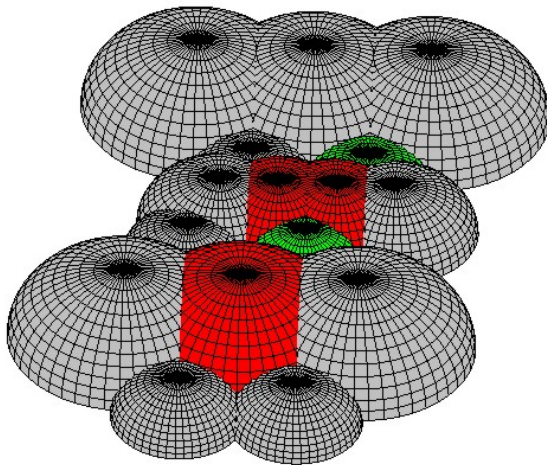


Tabla de resultados

Calculamos $\gamma_{K,2}^p$ para K para $|d_K| < 70$.

$-d_K$	D	$\gamma_{K,2}^p$	$\gamma_{K,2}$	h_K
3	3	3/2	3/2	1
4	1	2	2	1
7	7	7/3	7/3	1
8	2	4	4	1
11	11	11/2	11/2	1
15	15	3	20/3	2
19	19	19/2	19/2	1
20	5	5	80/11	2
23	23	23/5		3
24	6	12	12	2

$-d_K$	D	$\gamma_{K,2}^p$	$\gamma_{K,2}$	h_K
31	31	31/3		2
35	35	7		2
39	39	13		4
40	10	180/13	640/39	2
43	43	43/2	43/2	1
47	47	47/5		5
51	51	51/2	51/2	2
52	13	52/3	832/35	2
55	55	176/19		4
56	14	28/3	896/41	4
59	59	59/2	59/2	3
67	67	67/2	67/2	1
68	17	34	34	4
163	163	163/2	163/2	1