Cuerpo de clases de Hilbert y simbolo de Artin

Matías Alvarado

Junio 2020

Algunas definiciones

En todo lo que sigue L y K serán cuerpos de números.

Definición

Decimos que una extension de cuerpos L/K es abeliana si es una extension de Galois y además $Gal(L/K)$ es un grupo abeliano

Algunas definiciones

En todo lo que sigue L y K serán cuerpos de números.

Definición

Decimos que una extension de cuerpos L/K es abeliana si es una extension de Galois y además $Gal(L/K)$ es un grupo abeliano

Definición

Un lugar (o primo) al infinito σ de K, es una incrustación

$$\sigma : K \hookrightarrow \mathbb{C}$$

Algunas definiciones

En todo lo que sigue L y K serán cuerpos de números.

Definición

Decimos que una extension de cuerpos L/K es abeliana si es una extension de Galois y además $Gal(L/K)$ es un grupo abeliano

Definición

Un lugar (o primo) al infinito σ de K, es una incrustación

$$\sigma : K \hookrightarrow \mathbb{C}$$

Definición

Si L/K es una extensión y σ lugar al infinito de K. Diremos que σ ramifica en L si σ es real y tiene alguna extensión a L que no sea real.

Ejemplos de (no)ramificación al infinito

Ejemplos de (no)ramificación al infinito

- $\mathbb{Q}(i)/\mathbb{Q}$ ramifica en ∞

Ejemplos de (no)ramificación al infinito

- $\mathbb{Q}(i)/\mathbb{Q}$ ramifica en ∞
- $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ es no ramificado en ∞

Ejemplos de (no)ramificación al infinito

- $\mathbb{Q}(i)/\mathbb{Q}$ ramifica en ∞
- $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ es no ramificado en ∞
- Si ζ es una raíz primitiva n-ésima de la unidad, con $n > 2$. $\mathbb{Q}(\zeta + \zeta^{-1})$ es un cuerpo totalmente real y $\mathbb{Q}(\zeta)$ es totalmente imaginario. De este modo $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$ ramifica en cada lugar infinito σ de $\mathbb{Q}(\zeta + \zeta^{-1})$

Cuerpo de clase de Hilbert

Definición

Sea K un cuerpo de números, el **cuerpo de clases de Hilbert** *de K se define como la extensión finita L/K tal que:*

(i) *L/K es abeliana y no ramificada*

(ii) *Cualquier extensión abeliana no ramifica de K es una subextensión de L/K.*

Cuerpo de clase de Hilbert

Definición

Sea K un cuerpo de números, el **cuerpo de clases de Hilbert** *de K se define como la extensión finita L/K tal que:*

(i) *L/K es abeliana y no ramificada*

(ii) *Cualquier extensión abeliana no ramifica de K es una subextensión de L/K.*

Ejemplo

El cuerpo de clases de Hilbert de $\mathbb{Q}$ es $\mathbb{Q}$

Cuerpo de clase de Hilbert

Definición

Sea K un cuerpo de números, el **cuerpo de clases de Hilbert** *de K se define como la extensión finita L/K tal que:*

(i) *L/K es abeliana y no ramificada*

(ii) *Cualquier extensión abeliana no ramifica de K es una subextensión de L/K.*

Ejemplo

El cuerpo de clases de Hilbert de $\mathbb{Q}$ es $\mathbb{Q}$

¿Algún otro ejemplo mas interesante?

Cuerpo de clase de Hilbert

Definición

Sea K un cuerpo de números, el **cuerpo de clases de Hilbert** *de K se define como la extensión finita L/K tal que:*

(i) *L/K es abeliana y no ramificada*

(ii) *Cualquier extensión abeliana no ramifica de K es una subextensión de L/K.*

Ejemplo

El cuerpo de clases de Hilbert de $\mathbb{Q}$ es $\mathbb{Q}$

¿Algún otro ejemplo mas interesante?
¡No por ahora!

Lema

Sea L/K Galois, y $\mathfrak{p}$ un primo de $\mathcal{O}_K$ no ramificado en L. Si $\mathfrak{P}$ es un primo de L sobre $\mathfrak{p}$, entonces existe un único elemento $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P}$$

Lema

Sea L/K Galois, y $\mathfrak{p}$ un primo de $\mathcal{O}_K$ no ramificado en L. Si $\mathfrak{P}$ es un primo de L sobre $\mathfrak{p}$, entonces existe un único elemento $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P}$$

Demostración: En general tenemos la sucesión exacta

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \to 1$$

En nuestro caso $\mathfrak{p}$ no ramifica en L, por lo tanto $I_{\mathfrak{P}}$ es trivial. Asi

$$D_{\mathfrak{P}} \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$$

De este modo elegimos $\sigma \in D_{\mathfrak{P}}$ como la preimagen de $Frob \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, donde $Frob$ mapea $x \mapsto x^{N(\mathfrak{p})}$. De este modo concluimos que $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P},$ para $\alpha \in \mathcal{O}_L$.

Lema

Sea L/K Galois, y $\mathfrak{p}$ un primo de $\mathcal{O}_K$ no ramificado en L. Si $\mathfrak{P}$ es un primo de L sobre $\mathfrak{p}$, entonces existe un único elemento $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P}$$

Definición

El elemento σ del lema anterior se llama el **simbolo de Artin** *y se denota por* $\left(\frac{L/K}{\mathfrak{P}}\right)$

Ejemplo de simbolo de Artin

Sean p, q primos impares diferentes, y sea $\mathfrak{p}$ un primo de $\mathbb{Q}(\sqrt{q})$. Estudiemos el simbolo de Artin para la extensión $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$

- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = Id$, entonces $\sqrt{q} \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Luego $\sqrt{q} \in \mathbb{F}_p$ por ser invariante por la acción del Frobenius. Concluimos que q es un cuadrado módulo p.

Ejemplo de simbolo de Artin

Sean p, q primos impares diferentes, y sea $\mathfrak{p}$ un primo de $\mathbb{Q}(\sqrt{q})$. Estudiemos el simbolo de Artin para la extensión $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$

- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = Id$, entonces $\sqrt{q} \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Luego $\sqrt{q} \in \mathbb{F}_p$ por ser invariante por la acción del Frobenius. Concluimos que q es un cuadrado módulo p.
- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right)$ es el elemento no trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ entonces $-\sqrt{q} = \left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right)(\sqrt{q}) \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Por lo tanto $\sqrt{q} \notin \mathbb{F}_p$, es decir q no es cuadrado módulo p.
  Concluimos que el simbolo de Artin coincide con el simbolo de Legendre

$$\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = \left(\frac{q}{p}\right)$$

Ejemplo de simbolo de Artin

Sean p, q primos impares diferentes, y sea $\mathfrak{p}$ un primo de $\mathbb{Q}(\sqrt{q})$. Estudiemos el simbolo de Artin para la extensión $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$

- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = Id$, entonces $\sqrt{q} \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Luego $\sqrt{q} \in \mathbb{F}_p$ por ser invariante por la acción del Frobenius. Concluimos que q es un cuadrado módulo p.
- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right)$ es el elemento no trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ entonces $-\sqrt{q} = \left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right)(\sqrt{q}) \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Por lo tanto $\sqrt{q} \notin \mathbb{F}_p$, es decir q no es cuadrado módulo p.
  Concluimos que el simbolo de Artin coincide con el simbolo de Legendre

$$\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = \left(\frac{q}{p}\right) = \left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{p}\right)$$

Propiedades del simbolo de Artin

Proposición

Sea L/K Galois, $\mathfrak{p}$ lugar de K no ramificado y $\mathfrak{P}$ un lugar de L sobre $\mathfrak{p}$:

(i) *Si $\sigma \in Gal(L/K)$, entonces*

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$

(ii) *El orden de $\left(\frac{L/K}{\mathfrak{P}}\right)$ en $Gal(L/K)$ es el grado de inercia de L/K*

(iii) *$\mathfrak{p}$ escinde completamente en L si y solo si $\left(\frac{L/K}{\mathfrak{P}}\right)$ es la identidad.*

(i) Si $\sigma \in \mathrm{Gal}(L/K)$, entonces

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$$

Demostración:

$$\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) - \sigma^{-1}(\alpha)^{N(\mathfrak{p})} = x \in \mathfrak{P}$$

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) - \sigma\sigma^{-1}(\alpha)^{N(\mathfrak{p})} = \sigma(x) \in \sigma(\mathfrak{P})$$

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) - \alpha^{N(\mathfrak{p})} = \sigma(x) \in \sigma(\mathfrak{P}) \ \forall \alpha \in \mathcal{O}_L$$

Por la unicidad del simbolo de Artin se concluye la igualdad

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$$

(ii) El orden de $\left(\frac{L/K}{\mathfrak{P}}\right)$ en $\mathrm{Gal}(L/K)$ es el grado de inercia de L/K

Demostración: El simbolo de Artin tiene el mismo orden que el Frobenius (generador de la extensión residual), luego su orden es igual al grado de inercia.

(iii) $\mathfrak{p}$ escinde completamente en L si y solo si $\left(\frac{L/K}{\mathfrak{P}}\right)$ es la identidad.

Demostración: Sea $n = \deg(L/K)$. $\mathfrak{p}$ escinde completamente ssi descompone en n primos diferentes en L. Luego por la formula "$n = efg$" se tiene que $f = 1$ y se concluye por (ii).

Caso abeliano

Sea L/K abeliana, $\mathfrak{p}$ primo de K y $\mathfrak{P}, \mathfrak{P}'$ primos de L sobre $\mathfrak{p}$

- $\mathrm{Gal}(L/K)$ actúa de forma transitiva en los lugares de L sobre $\mathfrak{p}$
- Supongamos que $\sigma \in \mathrm{Gal}(L/K)$ es tal $\mathfrak{P}' = \sigma(\mathfrak{P})$
- $$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$
- $\left(\frac{L/K}{\mathfrak{P}}\right)$ depende solo de $\mathfrak{p}$

En el caso abeliano podemos escribir simplemente $\left(\frac{L/K}{\mathfrak{p}}\right)$

Mapa de Artin

Sea L/K una extensión abeliana y no ramificada. I_K el grupo de ideales fraccionario de K, y $\mathfrak{a} \in I_K$. Por factorización única en ideales tenemos

$$\mathfrak{a} = \prod_{1 \leq i \leq r} \mathfrak{p}_i^{r_i}, \qquad r_i \in \mathbb{Z}$$

De este modo definimos el simbolo de Artin para el ideal $\mathfrak{a}$ como,

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{1 \leq i \leq r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

Mapa de Artin

Sea L/K una extensión abeliana y no ramificada. I_K el grupo de ideales fraccionario de K, y $\mathfrak{a} \in I_K$. Por factorización única en ideales tenemos

$$\mathfrak{a} = \prod_{1 \leq i \leq r} \mathfrak{p}_i^{r_i}, \qquad r_i \in \mathbb{Z}$$

De este modo definimos el simbolo de Artin para el ideal $\mathfrak{a}$ como,

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{1 \leq i \leq r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

Observación

El simbolo de Artin se define en los generadores de I_K y luego se extiende por "linealidad" a todo I_K. Por lo tanto, el simbolo de Artin define un homomorfismo de grupo.

Mapa de Artin

Definición

El mapa de Artin es el homomorfismo

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K)$$

definido antes

Mapa de Artin

Definición

El mapa de Artin es el homomorfismo

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K)$$

definido antes

Teorema

Si L es el cuerpo de clase de Hilbert de K, entonces el mapa de Artin induce un isomorfismo entre $C(\mathcal{O}_K)$ y $Gal(L/K)$.

Mapa de Artin

Definición

El mapa de Artin es el homomorfismo

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K)$$

definido antes

Teorema

Si L es el cuerpo de clase de Hilbert de K, entonces el mapa de Artin induce un isomorfismo entre $C(\mathcal{O}_K)$ y $Gal(L/K)$.

Corolario

Existe una biyección entre las extensiones abelianas no ramificadas M/K y subgrupos H de $C(\mathcal{O}_K)$. Además el mapa de Artin induce el isomorfismo

$$C(\mathcal{O}_K)/H \simeq Gal(M/K)$$

Corolario

Sea L el cuerpo de Hilbert de K, y sea $\mathfrak{p}$ un ideal primo de K. Entonces

$$\mathfrak{p} \textit{ escinde completamente en } L \iff \mathfrak{p} \textit{ es principal}$$

Demostración.

$$\begin{aligned} \mathfrak{p} \text{ escinde completamente en } L &\Leftrightarrow \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \\ &\Leftrightarrow \mathfrak{p} \text{ determina la clase trivial en } C(\mathcal{O}_K) \\ &\Leftrightarrow \mathfrak{p} \text{ es principal} \end{aligned}$$

Ejemplo

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

Ejemplo

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

Ejemplo

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

- $d_K = -20$

Ejemplo

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

- $d_K = -20$
- $h(-20) = 2$, de hecho $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$

Ejemplo

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

- $d_K = -20$
- $h(-20) = 2$, de hecho $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$
- $[H(K) : K] = 2$

Ejemplo

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

- $d_K = -20$
- $h(-20) = 2$, de hecho $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$
- $[H(K) : K] = 2$
- Estudiemos $\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(\sqrt{-5})$

Ejemplo

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

- $d_K = -20$
- $h(-20) = 2$, de hecho $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$
- $[H(K) : K] = 2$
- Estudiemos $\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(\sqrt{-5})$