Aalto University
School of Science

Equivalencia aritmética como un análogo al teorema de la isogenia

Guillermo Mantilla-Soler

Seminario LATeN, Agosto 6 2020.

Funciones zeta de cuerpos de números y equivalencia aritmética

Funciones zeta de cuerpos de números y equivalencia aritmética

La función *zeta de Dedekind* de un cuerpo de números K es la función compleja $\zeta_K(s) := \sum_{0 \neq I \leqslant O_K} \frac{1}{\|I\|^s}$ definida para $R(s) > 1$. La función $\zeta_K(s)$ es holomorfa y se extiende a una función meromorfa en $\mathbb{C}$ con un polo simple en $s = 1$.

Funciones zeta de cuerpos de números y equivalencia aritmética

La función *zeta de Dedekind* de un cuerpo de números K es la función compleja $\zeta_K(s) := \sum_{0 \neq I \leqslant O_K} \frac{1}{\|I\|^s}$ definida para $R(s) > 1$. La función $\zeta_K(s)$ es holomorfa y se extiende a una función meromorfa en $\mathbb{C}$ con un polo simple en $s = 1$.

Teorema (Producto de Euler)

$$\zeta_K(s) = \prod_{\mathfrak{P}} (1 - \|\mathfrak{P}\|^{-s})^{-1}$$

En otras palabras, el orden maximal O_K es un dominio de Dedekind residualmente finito.

Teorema (Class # formula)

El residuo de $\zeta_K(s)$ en el polo $s = 1$ es

$$\frac{2^{r_k}(2\pi)^{s_K} h_K R_K}{w(K)|d_K|^{1/2}}$$

Teorema (Class # formula)

El residuo de $\zeta_K(s)$ en el polo $s = 1$ es

$$\frac{2^{r_k}(2\pi)^{s_K} h_K R_K}{w(K)|d_K|^{1/2}}$$

- d_K es el discriminate de K
- r_k es el número de inmersiones reales y s_k el número de pares complejas.
- $w(K)$ es el tamaño de la torsión de O_K^*, i.e., el número de raíces de la unidad en K
- h_K es el tamaño del grupo de clases de K
- R_K es el regulador de K.

Teorema (Class # formula II)

La función $\zeta_K(s)$ tiene un cero de orden $r = r_K + s_K - 1$ en $s = 0$ y

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^r} = -\frac{h_K R_K}{w(K)}$$

En principio la fórmula de clases combina muchos invariantes artiméticos de K, entonces es natural preguntarse

Pregunta

¿qué información de K se puede obtener de su función zeta?

En principio la fórmula de clases combina muchos invariantes artiméticos de K, entonces es natural preguntarse

Pregunta

¿qué información de K se puede obtener de su función zeta?

Definición

Dos cuerpos de números K y L se llaman aritméticamente equivalentes si sus funciones zeta de Dedekind $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n(K)}{n^s}$ y $\zeta_L(s) = \sum_{n=1}^{\infty} \frac{a_n(L)}{n^s}$ coinciden.

$$a_n(K) = \#\{I \leqslant O_K \ : \|I\| = n\}.$$

Observación

Los cuerpos K y L son A.E si y sólo si $a_n(K) = a_n(L)$ para todo n. De hecho es suficiente verificar la igualdad para n potencia de primo

$$a_p(K), a_{p^2}(K), \ldots$$

Observación

Los cuerpos K y L son A.E si y sólo si $a_n(K) = a_n(L)$ para todo n. De hecho es suficiente verificar la igualdad para n potencia de primo

$$a_p(K), a_{p^2}(K), \ldots$$

La primera afirmación se sigue inductivamente; por ejemplo $a_1(K) = 1 = a_1(L)$ y

$$a_2(K) = \lim_{s\to\infty} 2^s \left(\zeta_K(s) - a_1(K)\right) = \lim_{s\to\infty} 2^s \left(\zeta_L(s) - a_1(L)\right) = a_2(L).$$

La segunda afirmación se tiene gracias a que la función

$$n \mapsto a_n(K)$$

es multiplicativa.

Observación

Para todo primo p se tiene que $a_p(K) \leqslant [K : \mathbb{Q}]$. Más aún, la igualdad se obtiene si y sólo si p se rompe completamente en K.

Observación

Para todo primo p se tiene que $a_p(K) \leqslant [K : \mathbb{Q}]$. Más aún, la igualdad se obtiene si y sólo si p se rompe completamente en K.

Las observaciones que tenemos hasta ahora nos permiten concluír:

Proposición

Si K y L son A.E entonces comparten grado, clausura de Galois, signatura, discriminante.

Si p se rompe en K, $[K : \mathbb{Q}] = a_p(K) = a_p(L) \leqslant [L : \mathbb{Q}]$.

recordemos

dos cuerpos de números tienen la misma clausura de Galois si y sólo si el conjunto de primos racionales que se rompen en ambos cuerpos es el mismo

Observación

Para todo primo p se tiene que $a_p(K) \leqslant [K : \mathbb{Q}]$. Más aún, la igualdad se obtiene si y sólo si p se rompe completamente en K.

Las observaciones que tenemos hasta ahora nos permiten concluír:

Proposición

Si K y L son A.E entonces comparten grado, clausura de Galois, signatura, discriminante.

Si p se rompe en K, $[K : \mathbb{Q}] = a_p(K) = a_p(L) \leqslant [L : \mathbb{Q}]$.

recordemos

dos cuerpos de números tienen la misma clausura de Galois si y sólo si el conjunto de primos racionales que se rompen en ambos cuerpos es el mismo

Un cuerpo de números K es llamado *solitario* o *aritméticamente solitario* si todo cuerpo aritméticamente equivalente a K es un conjugado de K.

En otras palabras K es solitario si $\zeta_K(s)$ es un invariante completo de K.

Corolario

Sea K un cuerpo de números de grado n y sea G el grupo de Galois sobre $\mathbb{Q}$ de su clausura de Galois. En cualquiera de los siguientes casos K es solitario.

- $n \leqslant 3$.
- $G \cong S_n$, $n \neq 6$.
- *El discriminante de K es fundamental.*

Lo anterior es sólo un caso particular de un resultado de Robert Perlis

En otras palabras K es solitario si $\zeta_K(s)$ es un invariante completo de K.

Corolario

Sea K un cuerpo de números de grado n y sea G el grupo de Galois sobre $\mathbb{Q}$ de su clausura de Galois. En cualquiera de los siguientes casos K es solitario.

- $n \leqslant 3$.
- $G \cong S_n$, $n \neq 6$.
- *El discriminante de K es fundamental.*

Lo anterior es sólo un caso particular de un resultado de Robert Perlis

Teorema (Perlis,73)

El cuerpo K es solitario para cada una de las siguientes situaciones

- $n \leqslant 6$.
- $G \cong S_n, A_n$.

Muchos de los invariantes que aparecen en la class # formula pueden ser obtenidos a partir del conocimiento de la función zeta.

Muchos de los invariantes que aparecen en la class # formula pueden ser obtenidos a partir del conocimiento de la función zeta.

Teorema (Perlis,73)

Si K y L son A.E,

1. $[K:\mathbb{Q}] = [L:\mathbb{Q}]$.
2. $\text{sign}(K) = \text{sign}(L)$.
3. $Disc(K) = Disc(L)$.
4. *K y L tiene la misma clausura de Galois.*
5. *K y L tienen el mismo Galois core (la maxima extension de Galois contenida en K.)*
6. $O_K^* \cong O_L^*$, *en particular* $w(K) = w(L)$.
7. $h(K)R(K) = h(L)R(L)$.

Definición

El K-tipo artimético de un primo racional p es la tupla

$$A_p(K) = (f_1, ..., f_g)$$

de grados residuales p in K, escritos en forma ascendente.

Definición

El K-tipo artimético de un primo racional p es la tupla

$$A_p(K) = (f_1, \ldots, f_g)$$

de grados residuales p in K, escritos en forma ascendente.

$$\sum_{n=1}^{\infty} \frac{a_n(K)}{n^s} = \zeta_K(s) = \prod_{\mathfrak{P}} (1 - \|\mathfrak{P}\|^{-s})^{-1} = \prod_{p} \prod_{i=1}^{g} (1 - p^{-sf_i})^{-1}.$$

Para un primo p fijo lo anterior se puede resumir en identidad combinatórica

$$\sum_{m=0}^{\infty} a_{p^m}(K) T^m = \prod_{i=1}^{g} \sum_{d=0}^{\infty} T^{df_i}.$$

Theorem (Perlis, 73)

Sea N el compositum de las clausuras de Galois de K y L, y sea $G = \mathrm{Gal}(N/\mathbb{Q})$. Las siguientes son equivalentes:

1. $\zeta_K(s) = \zeta_L(s)$
2. *Para casi todo primo p los tipos aritméticos*

$$A_K(p) = A_L(p)$$

3. *Los cuerpos K y L son A.E si y sólo si los subgrupos $H_1 := \mathrm{Gal}(N/K)$ y $H_2 := \mathrm{Gal}(N/L)$ son cuasiconjugados en of G, i.e., para toda clase de conjugación C of G*

$$\#(C \cap H_1) = \#(C \cap H_2).$$

Acá *para casi todo* quiere decir que la densidad del conjunto en que coinciden es 1.

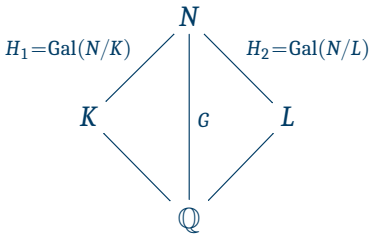
Sea p un primo racional y $D_p \leqslant G$ es su grupo de descomposición. La caracterización en términos de teoría de grupos se obtiene del teorema de densidad de Frobenius usando que

$$\#(H_1 \backslash G / D_p) = g$$

y que cada co-conjunto tiene tamaño $(\#H_1) f_i$.

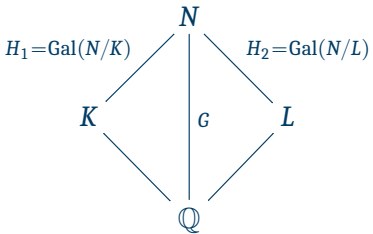
La condición grupo teórica de Perlis puede ser expresada en términos de equivalencias de representaciones ya que si χ_j es el caracter de la representación $\mathrm{Ind}_{H_i}^{G} 1_{H_i}$ entonces

$$\chi_j(C) = \#(C \cap H_i)\frac{\#G}{\#C\#H_i}.$$



La condición grupo teórica de Perlis puede ser expresada en términos de equivalencias de representaciones ya que si χ_j es el caracter de la representación $\mathrm{Ind}_{H_i}^{G} 1_{H_i}$ entonces

$$\chi_j(C) = \#(C \cap H_i)\frac{\#G}{\#C\#H_i}.$$



por tanto H_1 y H_2 son cuasiconjugados si y sólo si $\mathrm{Ind}_{H_1}^{G} 1_{H_1} \cong \mathrm{Ind}_{H_2}^{G} 1_{H_2}$.

Analogía con curvas racionales

Sea $E/\mathbb{Q}$ una curva elíptica, $L(E,s) = \sum_{n=0}^{\infty} \frac{a_n(E)}{n^s}$ su L-function y sea ℓ un primo. Sea $T_\ell(E) := \varprojlim_m E[\ell^m] \cong \mathbb{Z}_\ell^2$ el módulo de Tate ℓ-ádico y sea $\rho_{E,\ell} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ su correspondiente representación ℓ-ádica. El teorema de la isogenia implica que para todo par de curvas elípticas E, E_1

Analogía con curvas racionales

Sea $E/\mathbb{Q}$ una curva elíptica, $L(E,s) = \sum_{n=0}^{\infty} \frac{a_n(E)}{n^s}$ su L-function y sea ℓ un primo. Sea $T_\ell(E) := \varprojlim_m E[\ell^m] \cong \mathbb{Z}_\ell^2$ el módulo de Tate ℓ-ádico y sea $\rho_{E,\ell} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ su correspondiente representación ℓ-ádica. El teorema de la isogenia implica que para todo par de curvas elípticas E, E_1

(i) Para casi todo[a] primo ℓ las representaciones $\rho_{E,\ell}$ y $\rho_{E_1,\ell}$ son conjugadas.

(i) Para casi todo primo ℓ existe un $\mathbb{Z}_\ell$-isomorfismo $T_\ell(E) \cong T_\ell(E_1)$ de $\mathrm{G}_{\mathbb{Q}}$-módulos.

(ii) Para casi todo primo p, $a_p(E) = a_p(E_1)$.

(ii) Para casi todo primo p, las curvas E and E' tienen el mismo número de $\mathbb{F}_p$ puntos.

(ii) $L(E,s) = L(E_1,s)$.

[a] equivalentemente: existe un primo ℓ

¿ Cuál sería el enunciado análogo para la función zeta de Dedekind $\zeta_K(s)$?

¿ Cuál sería el enunciado análogo para la función zeta de Dedekind $\zeta_K(s)$?

¿ qué necesitamos?

- La función $\zeta_K(s)$ debería jugar el papel de la L-function de la curva.
- La representación $\rho_{E,\ell}$ debe corresponder a una representación ρ_K.
- El módulo ℓ-ádico de Tate debe corresponder an $\mathrm{G}_{\mathbb{Q}}$-module T_K.
- El número de $\mathbb{F}_p$ puntos sobre la curva E corresponde al número de $\mathbb{F}_p$ puntos sobre la curva $\mathrm{Spec}(O_K)$.

¿ Cuál sería el enunciado análogo para la función zeta de Dedekind $\zeta_K(s)$?

¿ qué necesitamos?

- La función $\zeta_K(s)$ debería jugar el papel de la L-function de la curva.
- La representación $\rho_{E,\ell}$ debe corresponder a una representación ρ_K.
- El módulo ℓ-ádico de Tate debe corresponder an $G_{\mathbb{Q}}$-module T_K.
- El número de $\mathbb{F}_p$ puntos sobre la curva E corresponde al número de $\mathbb{F}_p$ puntos sobre la curva $\mathrm{Spec}(O_K)$.

¿ qué queremos?

(i) Las representaciones ρ_K y ρ_L son conjugadas.

(i) Existe un isomorfismo $T_K \cong T_L$ de $G_{\mathbb{Q}}$-módulos.

(ii) Para casi todo primo p, $a_p(K) = a_p(L)$.

(ii) Para casi todo primo p, las curvas $\mathrm{Spec}(O_K)$ y $\mathrm{Spec}(O_L)$ tienen el mismo número de $\mathbb{F}_p$ puntos.

(ii) $\zeta_K(s) = \zeta_L(s)$.

Sea K un cuerpo de números de grado n y sea $\mathrm{Emb}(K)$ el conjunto de sus inmersiones complejas. El grupo absoluto de Galois $\mathrm{G}_{\mathbb{Q}}$ actúa continuamente sobre $\mathrm{Emb}(K)$ vía composición. Tal representación $\mathrm{G}_{\mathbb{Q}} : \pi_K \to S_n$, compuesta con la representación de permutación natural $\iota_n : S_n \to \mathrm{GL_n}(\mathbb{C})$, produce una representación de Galois n-dimensional

$$\rho_K : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL_n}(\mathbb{C}).$$

Sea K un cuerpo de números de grado n y sea $\mathrm{Emb}(K)$ el conjunto de sus inmersiones complejas. El grupo absoluto de Galois $\mathrm{G}_{\mathbb{Q}}$ actúa continuamente sobre $\mathrm{Emb}(K)$ vía composición. Tal representación $\mathrm{G}_{\mathbb{Q}} : \pi_K \to S_n$, compuesta con la representación de permutación natural $\iota_n : S_n \to \mathrm{GL_n}(\mathbb{C})$, produce una representación de Galois n-dimensional

$$\rho_K : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL_n}(\mathbb{C}).$$

En otras palabras, tenemos el $\mathrm{G}_{\mathbb{Q}}$-módulo $T_K := \bigoplus_{\sigma \in \mathrm{Emb}(K)} \mathbb{C}\sigma$ con la acción of $\mathrm{G}_{\mathbb{Q}}$ definida en cada elemento de la base como composición.

Teorema (El que queríamos)

Sean K, L dos cuerpos de números. Las siguientes son equivalentes:

(i) *Las representaciones ρ_K y ρ_L son conjugadas.*

(i) *Existe un $\mathbb{C}$-isomorfismo $T_K \cong T_L$ de $\mathrm{G}_{\mathbb{Q}}$-módulos.*

(ii) *Para casi todo primo p, $a_p(K) = a_p(L)$.*

(ii) *Para casi todo primo p, las curvas $\mathrm{Spec}(O_K)$ y $\mathrm{Spec}(O_L)$ tienen el mismo número de $\mathbb{F}_p$ puntos.*

(ii) $\zeta_K(s) = \zeta_L(s)$.

Teorema (El que queríamos)

Sean K, L dos cuerpos de números. Las siguientes son equivalentes:

(i) *Las representaciones ρ_K y ρ_L son conjugadas.*

(i) *Existe un $\mathbb{C}$-isomorfismo $T_K \cong T_L$ de $G_{\mathbb{Q}}$-módulos.*

(ii) *Para casi todo primo p, $a_p(K) = a_p(L)$.*

(ii) *Para casi todo primo p, las curvas $\mathrm{Spec}(O_K)$ y $\mathrm{Spec}(O_L)$ tienen el mismo número de $\mathbb{F}_p$ puntos.*

(ii) $\zeta_K(s) = \zeta_L(s)$.

Corolario

Dos cuerpos de números K y L son A.E si y sólo si para casi todo primo p

$$\#\{f \in A_K(p) \mid f = 1\} = \#\{f \in A_L(p) \mid f = 1\}.$$

El punto central detrás de la analogía es que tanto $\zeta_K(s)$ como $L(E,s)$ son L-funciones de representaciones de Galois de $G_{\mathbb{Q}}$

$$\zeta_K(s) = L(\rho_K, s) \text{ y } L(E,s) = L(\rho_{E,\ell}, s)$$

más aún

$$\mathrm{Trace}(\rho_K(\mathrm{Frob}_p)) = a_p(K) = \#\mathrm{Spec}(O_K)[\mathbb{F}_p]$$

$$\mathrm{Trace}(\rho_{E,\ell}(\mathrm{Frob}_p)) = a_p(E) = 1 + p - \#E(\mathbb{F}_p).$$

El punto central detrás de la analogía es que tanto $\zeta_K(s)$ como $L(E,s)$ son L-funciones de representaciones de Galois de $G_{\mathbb{Q}}$

$$\zeta_K(s) = L(\rho_K, s) \text{ y } L(E,s) = L(\rho_{E,\ell}, s)$$

más aún

$$\mathrm{Trace}(\rho_K(\mathrm{Frob}_p)) = a_p(K) = \#\mathrm{Spec}(O_K)[\mathbb{F}_p]$$
$$\mathrm{Trace}(\rho_{E,\ell}(\mathrm{Frob}_p)) = a_p(E) = 1 + p - \#E(\mathbb{F}_p).$$

$$\begin{aligned} \det(X - \rho_K(\mathrm{Frob}_p)) &= \prod_{i=1}^{g}(X^{f_i} - 1). \\ \det(X - \rho_{E,\ell}(\mathrm{Frob}_p)) &= X^2 - a_p(E)X + p. \end{aligned}$$

Los resultados acerca de A.E pueden ser expresados de manera cohesiva en términos de la representación ρ_K.

Los resultados acerca de A.E pueden ser expresados de manera cohesiva en términos de la representación ρ_K.

Invariantes de la representación ρ_K

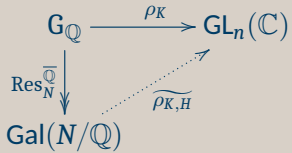
- $\deg(\rho_K) = [K : \mathbb{Q}]$
- $\text{Trace}\,(\rho_K(\tau)) = r_K$, donde $\tau \in G_{\mathbb{Q}}$ es conjugación compleja.
- $\text{Conductor}(\rho_K) = \text{Disc}(K)$
- $\overline{\mathbb{Q}}^{\text{Ker}(\rho_K)} = \widetilde{K}$, la clausura de Galois de K.

- Suponga que $N/\mathbb{Q}$ es de Galois con grupo de Galois G tal que $\widetilde{K} \leqslant N$, sea $H = \mathrm{Gal}(N/K)$ y $n = [K : \mathbb{Q}]$. Entonces si

$$\widetilde{\rho_{K,H}} : G \to \mathrm{GL}_n(\mathbb{C})$$

es la representación obtenida al restringir a N, i.e., $\mathrm{Res}_N^{\overline{\mathbb{Q}}} \circ \rho_K = \widetilde{\rho_{K,H}}$ entonces

$$\widetilde{\rho_{K,H}} \cong \mathrm{Ind}_H^G 1_H.$$



¿qué cosas nuevas podemos encontrar usando esta analogía?

Dada una representación de Artin $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, con L-función de Artin $L(\rho, s)$, su L-function completa se define como

$$\Lambda(\rho, s) := A(\rho)^{s/2} L_\infty(s, \rho) L(s, \rho),$$

donde $A(\rho)$ es el *conductor de Artin*, y $L_\infty(\rho, s)$ un factor que depende del valor de ρ en conjugación compleja.

¿qué cosas nuevas podemos encontrar usando esta analogía?

Dada una representación de Artin $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, con L-función de Artin $L(\rho, s)$, su L-function completa se define como

$$\Lambda(\rho, s) := A(\rho)^{s/2} L_\infty(s, \rho) L(s, \rho),$$

donde $A(\rho)$ es el *conductor de Artin*, y $L_\infty(\rho, s)$ un factor que depende del valor de ρ en conjugación compleja. La L-función completa satisface la ecuación funcional

$$\Lambda(\rho, s) = W(\rho)\Lambda(\rho^\vee, 1 - s),$$

donde $\rho^\vee$ es la representación dual y $W(\rho)$ es un complejo unitario llamado el *número de raíz de* ρ.

¿qué cosas nuevas podemos encontrar usando esta analogía?

Dada una representación de Artin $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, con L-función de Artin $L(\rho, s)$, su L-function completa se define como

$$\Lambda(\rho, s) := A(\rho)^{s/2} L_\infty(s, \rho) L(s, \rho),$$

donde $A(\rho)$ es el *conductor de Artin*, y $L_\infty(\rho, s)$ un factor que depende del valor de ρ en conjugación compleja. La L-función completa satisface la ecuación funcional

$$\Lambda(\rho, s) = W(\rho)\Lambda(\rho^\vee, 1 - s),$$

donde $\rho^\vee$ es la representación dual y $W(\rho)$ es un complejo unitario llamado el *número de raíz de* ρ. Gracias a Deligne el número de raíz puede ser escrito como un producto de *números de raíz locales* $W(\rho) = \prod_p W_p(\rho)$. Los números $W_p(\rho)$ son complejos de magnitud igual a 1, más aún $W_p(\rho) = 1$ si ρ es no ramificada en p.

En el caso de la representación ρ_K, asociada al cuerpo de números K, se tiene que

- $A(\rho_K) = |\mathrm{Disc}(K)|$
- $W(\rho_K) = 1$.
- $L_\infty(s, \rho_K) := \Gamma_{\mathbb{R}}^{r_1}(s)\Gamma_{\mathbb{C}}^{r_2}(s)$ donde $\Gamma_{\mathbb{R}} = (\pi)^{-s/2}\Gamma\left(\frac{s}{2}\right)$ and $\Gamma_{\mathbb{C}} = 2(2\pi)^{-s}\Gamma(s)$.
- $\rho_K = \rho_K^\vee$

Definición

Sea K un cuerpo de números y sea p un primo, incluyendo[a] $p = -1$. Llamamos a $W_p(\rho_K)$ el número de raíz local de K en p.

[a] J. Conway denotaba el primo infinito por $p = -1$.

Definición

Dos cuerpos de números K y L son llamados débilmente aritméticamente equivalentes si se cumplen las siguientes:

- *Comparten el grado y los primos que ramifican*
- *para todo primo p que ramifica en cualquiera de los cuerpos los p-factores de sus funciones zeta son iguales ,i.e.,*

$$L_p(\rho_K, s) = L_p(\rho_L, s).$$

Definición

Dos cuerpos de números K y L son llamados débilmente aritméticamente equivalentes si se cumplen las siguientes:

- *Comparten el grado y los primos que ramifican*
- *para todo primo p que ramifica en cualquiera de los cuerpos los p-factores de sus funciones zeta son iguales ,i.e.,*

$$L_p(\rho_K, s) = L_p(\rho_L, s).$$

Observación

La noción de D.A.E es mucho menos restrictiva que la de A.E. Por ejemplo, existen parejas de cuerpos de números D.A.E no conjugados que cumple cualquiera de las siguientes:

- *Extensiones de Galois de $\mathbb{Q}$.*
- *Tienen discriminante fundamental.*
- *Tienen grado menor a 7.*

Teorema (MS, 2015.)

Sean K, L cuerpos de números que son D.A.E y sin ramificación salvaje. Suponga que cualquiera de las siguientes es valida

(a) *Tienen discriminante fundamental.*

(b) *Extensiones de Galois de $\mathbb{Q}$.*

(c) *Tienen grado menor o igual a 3.*

Entonces, K y L tienen el mismo número local de raíz para todo primo p.

Teorema (MS, 2015.)

Sean K, L cuerpos de números que son D.A.E y sin ramificación salvaje. Suponga que cualquiera de las siguientes es valida

(a) *Tienen discriminante fundamental.*

(b) *Extensiones de Galois de $\mathbb{Q}$.*

(c) *Tienen grado menor o igual a 3.*

Entonces, K y L tienen el mismo número local de raíz para todo primo p.

Theorem (Rohrlich, 93)

Sean $E/\mathbb{Q}$, $E'/\mathbb{Q}$ dos curvas elípticas semistables con ramificación mala en el mismo conjunto de primos. Suponga que para todo primo malo p, los p-factores de $L(E, s)$ y $L(E', s)$ coinciden. Entonces, para todo primo p, E y E' tienen los mismos números locales de raíz

$$W_p(E) = W_p(E').$$

Sea K un cuerpo de números de grado n y sea $\pi_K : G_{\mathbb{Q}} \to s_n$ la representación de permutación sobre T_K Los morfismos estándar

$$\mathrm{i} : s_n \hookrightarrow \mathrm{GL}_n(\mathbb{C}) \text{ and } \mathrm{j} : s_n \hookrightarrow \mathrm{O}_n(\overline{\mathbb{Q}})$$

Sea K un cuerpo de números de grado n y sea $\pi_K : G_{\mathbb{Q}} \to s_n$ la representación de permutación sobre T_K Los morfismos estándar

$$\mathfrak{i} : s_n \hookrightarrow \mathrm{GL}_n(\mathbb{C}) \text{ and } \mathfrak{j} : s_n \hookrightarrow \mathrm{O}_n(\overline{\mathbb{Q}})$$

inducen mapeos $\mathfrak{i}^*$ and $\mathfrak{j}^*$

$$\begin{array}{ccc} \mathrm{H}^1(\mathbb{Q}, \mathrm{O}_n(\overline{\mathbb{Q}})) & & \\ \uparrow{\scriptstyle \mathfrak{j}^*} & & \\ \mathrm{H}^1(\mathbb{Q}, s_n) & \xrightarrow{\mathfrak{i}^*} & \mathrm{H}^1(\mathbb{Q}, \mathrm{GL}_n(\mathbb{C})) \end{array}$$

- La L-función de Artin asociada a $\rho_K = \mathfrak{j}^*(\pi_K)$ es $\zeta_K(s)$.

Sea K un cuerpo de números de grado n y sea $\pi_K : G_{\mathbb{Q}} \to s_n$ la representación de permutación sobre T_K Los morfismos estándar

$$\mathfrak{i} : s_n \hookrightarrow \mathrm{GL}_n(\mathbb{C}) \text{ and } \mathfrak{j} : s_n \hookrightarrow \mathrm{O}_n(\overline{\mathbb{Q}})$$

inducen mapeos $\mathfrak{i}^*$ and $\mathfrak{j}^*$

$$\begin{array}{ccc} \mathrm{H}^1(\mathbb{Q}, \mathrm{O}_n(\overline{\mathbb{Q}})) & & \\ \uparrow{\scriptstyle \mathfrak{j}^*} & & \\ \mathrm{H}^1(\mathbb{Q}, s_n) & \xrightarrow{\mathfrak{i}^*} & \mathrm{H}^1(\mathbb{Q}, \mathrm{GL}_n(\mathbb{C})) \end{array}$$

- La L-función de Artin asociada a $\rho_K = \mathfrak{j}^*(\pi_K)$ es $\zeta_K(s)$.
- La forma cuadrática racional asociada a $\mathfrak{i}^*(\pi_K)$ es la forma traza racional de K.

$$\begin{array}{rccc} \langle\ ,\ \rangle : & K \times K & \to & \mathbb{Q} \\ & (x, y) & \mapsto & \mathrm{Tr}_{K/\mathbb{Q}}(xy) \end{array}$$

Theorem (Perlis, 73)

Sean K y L dos cuerpos de números. Las siguientes son equivalentes:

1. $\zeta_K(s) = \zeta_L(s)$
2. *Para casi todo primo p, $A_K(p) = A_L(p)$.*

Theorem (Perlis, 73)

Sean K y L dos cuerpos de números. Las siguientes son equivalentes:

1. $\zeta_K(s) = \zeta_L(s)$
2. *Para casi todo primo p, $A_K(p) = A_L(p)$.*

Acá *para casi todo* quiere decir que la densidad del conjunto en que coinciden es 1.

Theorem (Perlis, 73)

Sean K y L dos cuerpos de números. Las siguientes son equivalentes:

1. $\zeta_K(s) = \zeta_L(s)$
2. *Para casi todo primo p, $A_K(p) = A_L(p)$.*

Acá *para casi todo* quiere decir que la densidad del conjunto en que coinciden es 1.

Theorem (MS, 2020)

Sean K y L dos cuerpos de números de grado n. Las siguientes son equivalentes:

1. $\zeta_K(s) = \zeta_L(s)$
2. *El conjunto de los primos p tales que $A_K(p) = A_L(p)$ tiene densidad mayor que $1 - \frac{1}{4n^2}$.*

¡Gracias!