Modulo $m$: $M_K \longrightarrow \mathbb{N}$

"ideale generalizzato"

$$K_{m,1} = \{ a \in K^\times \,/\, v(a-1) \geq m(v) \quad \forall v \in M_0,\ v|m$$
$$v(a) \geq 0 \quad \forall v \text{ reale } v|m \}$$

$S(m)$ supporto di $m$

Ray class group associato a $m$:

$$Cl_m = \frac{J^{S(m)}}{K_{m,1}}$$

$$Cl_m \longrightarrow Cl(K) \qquad S = M_\infty \cup \{ v \,/\, v \text{ ramifica in } L \}$$

finito.

$\forall\ L/K$ abeliana la mappa di Artin

$$\psi_{L/K} : J^S \longrightarrow Gal(L/K)$$
$$\mathfrak{p} \longmapsto Frob_{\mathfrak{p}}$$

ammette un modulo $m$ t.c. $S(m) \supseteq S$

cioè fattorizza per $Cl_m$

(cioè il nucleo contiene $K_{m,1}$ cioè è un sottogruppo di congruenza)

Il Teorema di esistenza afferma che

per ogni sgp di congruenza $H$ (di $J_K$ mod $m$) $\exists$

est. ab. finita $L/K$ n.r. fuori da $S(m)$ e t.c. $H = i(K_{m,1}) N_{L/K}(J_L^m)$

Il minimo modulo $m$ per cui questo accade.
si dice conduttore dell'estensione.
(Analogia con il caso $\mathbb{Q}$).

Esempio

$m = 1$

Il ray class group associato è
$$Cl_1 = Cl(K)$$
a cui è associato il ray class field $L_m$,
detto in questo caso campo di Hilbert di $K$
per def. è la max estensione di $K$ n.r.
a tutti i primi, inclusi i primi reali (cioè
i primi reali di $K$ restano reali in $L$)

- Il corpo di classe di Hilbert di $\mathbb{Q}$ è $\mathbb{Q}$.
- $K = \mathbb{Q}(\sqrt{5})$

  $H = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$

In

$\mathbb{Q}(\sqrt{-5})$ ramificano 2, 5

ma solo 2 ramifica in $\mathbb{Q}(i)/\mathbb{Q}$

5 ramifica in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$

$\rightsquigarrow$ $H/K$ è non ramificato.

## Teorema dell'ideale principale

Poiché $Cl(K)$ è finito, $\exists$ un'estensione finita $L/K$ in cui tutti gli ideali di $K$ diventano principali

$C_1, \dots, C_h$ classi di ideali

$a_1, \dots, a_h$

$$a_i^{h} = (\alpha_i)$$

$$L = K(\sqrt[h]{\alpha_1}, \dots, \sqrt[h]{\alpha_h}, \mu_h)$$

Il corpo di Hilbert di $K$ è la minima estensione di $K$ in cui gli ideali di $K$ diventano principali.

## Teorema di densità di Chebotarev

Dirichlet. dato $m$, e $a$ t.c. $(a, m) = 1$ esistono infiniti primi $p \equiv a \mod m$.

$L/K$ abeliana

$\Psi_{L/K}$ induce un omom. $Cl_m \longrightarrow Gal(L/K)$

per qualche modulo $m$

$$\mathcal{J}^{S(m)} \longrightarrow Gal(L/K)$$

I primi sono equidistribuiti nelle classi di $Cl_m$

$\rightsquigarrow$ per ogni $\sigma \in Gal(L/K)$ esistono infiniti primi $\mathfrak{p}$ di $O_K$ che non ramificano in $L$ e t.c. $\sigma = Frob_{L/K}(\mathfrak{p})$

## Teorema di Chebotarev

Sia $L/K$ finita di campi di numeri

$G = Gal(L/K)$

Sia $C$ una classe di coniugio in $G$.

(un elem. se $G$ abeliano).

L'insieme

$$X_C = \{\mathfrak{p} \text{ primo di } O_K \mid \exists \mathfrak{P} \subseteq O_L \ \ \mathfrak{P} \mid \mathfrak{p} \text{ e } Frob_{\mathfrak{P}} \in C\}$$

ha densità $|C|/|G|$ nell'insieme degli ideali primi di $K$.

($|C| = 1$ se $G$ abeliano)

### Corollario

Se un polinomio $f(x) \in O_K[x]$ si spezza in fattori lineari mod $\mathfrak{p}$ per tutti i primi

$\mathfrak{p}$ di $\mathcal{O}_K$ salvo un numero finito, allora si spezza in fattori lineari in $K$.

<u>Dim.</u>

$L$ campo di spezzam. di $f(x)$.

$f(x)$ si spezza in fatt. lineari mod $\mathfrak{p}$ $\Leftrightarrow$ $\mathrm{Frob}_{\mathfrak{P}}$ è banale $\forall \mathfrak{P} | \mathfrak{p}$.

$\Rightarrow$ $L/K$ banale. ■

---

## Caso non abeliano

<u>CFT</u>

- locale

$$\begin{array}{ccc} K^* & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow \\ K^*/NL^* & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \end{array} \quad \forall \text{ est. finita ab. } L/K$$

- globale

$$\begin{array}{ccc} C_K & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow \\ C_K/NC_L & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \end{array} \quad \forall \text{ est. finita ab. } L/K.$$

$\leadsto$ per il caso non ab.

$K \leadsto G(K)$ non. ab. $\nearrow$ sottoinsieme

con mappe $G(K) \longrightarrow \mathrm{Gal}(\bar{K}/K)$

in modo t.c. $\forall\ L/K$ finito

$$\frac{G(K)}{N_{L/K}(G(L))} \simeq Gal(L/K)$$

normale.

Situazione più chiara considerando i gruppi duali.

$G$ gruppo loc. compatto.

Si può considerare l'insieme dei caratteri

$\hat{G} = \{$ omo continui $G \longrightarrow S^1 \}$ GRUPPO DUALE

Se $G$ abeliano esiste iso

$\hat{\hat{G}} \simeq G$ (Pontryagin).

Nel caso abeliano

$\omega : C_K \longrightarrow S^1$ caratteri di Hecke o grossencharacter

$\chi : Gal(K^{ab}/K) \longrightarrow S^1$

$\hookrightarrow$ rappres 1-dimensionali di $Gal(\bar{K}/K)$ rappresentazioni Galoisiane

Se $\chi : Gal(K^{ab}/K) \longrightarrow S^1$, componendo $\chi$ con $\phi_{L/K} : C_K \longrightarrow Gal(K^{ab}/K)$

otteniamo $\omega = \chi \circ \phi_{L/K}$ grossencharacter.

Mappa unitaria

$$\left\{\begin{matrix}\text{Rappres.}\\ \text{1-dim. di } G_K\end{matrix}\right\} \leftrightsquigarrow \left\{\begin{matrix}\text{caratteri di}\\ \text{Hecke di}\\ C_K\end{matrix}\right\}$$

$G_K = Gal(\bar{K}/K)$

L'immagine è data dai caratteri di Hecke di ordine finito (cioè fattorizzano per un gruppo finito)

Oss. $S^1$ non ha sottogruppi piccoli

$$\omega : Gal(\bar{K}/K) \longrightarrow S^1$$

fattorizza per un quoziente finito: se $U$ aperto in $S^1$ non contiene sgp, allora $\omega^{-1}(U)$ aperto di $G_K$, quindi contiene un sgp aperto $H = Gal(\bar{K}/L)$ con $L/K$ finito $\rightsquigarrow \omega(H) = 1 \rightsquigarrow \omega$ ha imm. finita.

(Oss. possono esistere caratteri di $Gal(\bar{K}/K) \to L^*$ di ordine infinito se $L/\mathbb{Q}_p$ è per es. un estensione finita: per es. il carattere ciclotomico

$$\omega : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^{\times}$$

che descrive l'azione di $G_{\mathbb{Q}}$ su $\mathbb{Q}(\mu_{p^\infty})$).

Domanda: $F = \mathbb{C}, \mathbb{Q}_p, L/\mathbb{Q}_p$

$$\left\{\begin{matrix}\text{analogo}\\ \text{dei caratteri}\\ \text{di } C_K \text{ di}\\ \text{ordine finito}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{rappres. n-dim.}\\ G_K \longrightarrow GL_n(F)\end{matrix}\right\}$$

$\updownarrow$

$\left\{ \begin{array}{l} \text{rappresentazioni} \\ \text{automorfe di} \\ GL_n(\mathbb{A}_K) \end{array} \right\}$

basate su $GL_n(K)$

(CONGETTURA DI LANGLANDS GLOBALE)

Rappres. automorfe di un gruppo localm. compatto $G$ è una rappres. irriducibile di $G$ su $L^2(G)$ (funzioni square-integrable $G \to \mathbb{C}$ dove $G$ agisce per moltiplicazione a dx

$$g, f \longmapsto f(\cdot\, g)$$

Rappres. regolare dx di $G$.

si decompone in rappres. irriducibili

$\leadsto$ rappres. automorfe di $G$.

Si realizzano su spazi di forme automorfe.

"modulari"

funzioni $GL_n(\mathbb{A}) \to \mathbb{C}$

$\pi$ rappresentazione automorfe $\leadsto$

$$\pi = \bigotimes_v \pi_v \qquad \pi_v \text{ rappres. di } GL_n(K_v)$$

Congettura di Langlands locale

{esiste corrisp. biunivoca}

$\left\{ \begin{array}{l} \text{classi di isom.} \\ \text{di rappres. irrid.} \\ \text{"ammissibili" di } GL_n(K_v) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{classi di isom.} \\ \text{di rappres. n. dim.} \\ \text{galoisiane di } Gal(\bar{K}_v/K_v) \end{array} \right\}$

$\uparrow$ imprecisio

su cui Frob agisce in modo semisemplice.

Dimostrata da Kutzko nel 1980

Dimostrato nel 2001 per n arbitrario
(Harris-Taylor)

---

La corrispondenza è espressa in termini di funzioni L.

A ogni oggetto $\rightsquigarrow$ rappres. autom. di $GL_n(\mathbb{A}_K)$

$\rightsquigarrow$ rappres. di $G_K$ ($K$ locale o globale)

è possibile associare una funzione L

$L(\pi, s)$ $\quad$ $L(\rho, s)$ $\quad$ $L(\pi_v, s)$

s variabile complessa

- $L(\pi, \cdot)$, $L(\rho, \cdot)$ meromorfe
- soddisfa un'eq. funzionale
- si decompone in un prodotto di Eulero

$$L(\pi, s) = \prod_{p \text{ primi } O_K} \left( \frac{\quad}{p} \right)$$

Langlands

$\pi$ di $GL_n(\mathbb{A}) \longleftrightarrow \rho : G_K \to GL_n(F)$

$L(\pi, s) \longleftrightarrow L(\rho, s)$