$$\begin{tikzcd}
\mathbb{I}_K \arrow[r, "\Phi_K"] \arrow[d, dashed, "F"] & \mathrm{Gal}\left(K^{ab}/K\right) \\
\mathcal{J}_K \arrow[ur, dashed] &
\end{tikzcd}$$

$\mathcal{J}_K \leftarrow$ ideali frazionari)

$$F\left((\alpha_v)_v\right) \longmapsto \prod_{v \in M_0} \mathfrak{P}_v^{v(\alpha_v)}$$

K campo di numeri

$M_K = \{\text{posti di } K\} = M_\infty \cup M_0 \leftarrow$ n.a.

$\mathcal{J}_K = \{\text{ideali frazionari di } K\}$

Se $S \subseteq M_K$

$\mathcal{J}_K^S$ = sgp di $\mathcal{J}_K$ generato dai primi non in S

$= \{ \mathfrak{a} = \mathfrak{P}_1^{n_1} \cdots \mathfrak{P}_k^{n_k} \quad \mathfrak{P}_i \notin S \}$

$= \{ \sum_{v \notin S} n_v v \ / \ n_v$ quasi ovunque nulli $\}$.

$$K^S = \{ a \in K^* \ / \ v(a) = 0 \quad \forall v \text{ in } S \cap M_0 \}$$

$$i : K^S \longrightarrow \mathcal{J}^S$$
$$a \longmapsto a\mathcal{O}_K$$

Per es. se $K = \mathbb{Q}$ e $S = \{ p \mid p \mid N \}$

$\mathbb{Q}^S = \{ a/b \mid (N,a) = (N,b) = 1 \}$

$$\begin{array}{ccc} \mathbb{Q}^S & \longrightarrow & I^S \\ a/b & \longmapsto & \left(a/b\right) \\ & & \parallel \\ & & a/b\,\mathbb{Z} \end{array}$$

iniettiva con $\ker = \{\pm 1\}$

In generale c'è succ. esatta

$$1 \to U_K \to K^S \to I^S \to Cl(K) \to 0$$
$$U_K = \mathcal{O}_K^\times$$

GCFT in termini di ideali

Sia $S \subseteq M_K$ e supponiamo $M_\infty \subseteq S$.

e sia G gruppo ab. topologico.

Un omomorfismo $\varphi: \mathcal{I}^S \longrightarrow G$ si dice **ammissibile** se per ogni intorno N dell'identità in G esiste $\varepsilon > 0$ t.c. $\varphi((a)^S) \in N$ $\forall a \in K^\times$ t.c. $|a-1|_v < \varepsilon$ $\forall v \in S$.

(Se G discreto si può prendere $N = \{1\}$).

Proposizione

K, S come sopra, G gruppo top. abeliano completo.

A) Se $\varphi: \mathcal{I}^S \longrightarrow G$ è ammissibile allora esiste un unico omom. $\Phi: \mathbb{I}_K \longrightarrow G$ t.c.

(i) Φ continuo

(ii) $\Phi(K^*) = 1$

(iii) $\forall x \in \mathbb{I}_K^S \; \left((\alpha_v)_v \mid \alpha_v = 1 \text{ se } v \in S \right)$

si ha $\Psi((x)^S) = \Phi(x)$.

dove $(x)^S = \sum_{v \notin S} n_v v \in \mathcal{I}^S$.

B) Viceversa se

"G non ha sottogruppi piccoli" $(*)$

e Φ omom. continuo $\mathbb{I}_K \longrightarrow G$ t.c. $\Phi(K^*) = \{1\}$

allora $\exists S \; \exists \Psi : \mathcal{I}^S \longrightarrow G$ ammissibile t.c.

$$\Psi((x)^S) = \Phi(x).$$

dove "G non ha sottogruppi piccoli" se esiste un intorno aperto di 1 in G che non contiene sottogruppi non banali.

Es. G finito discreto,

$G = \mathbb{R}^*, \mathbb{C}^*$ non hanno sgp. piccoli

$\mathbb{Q}_p^*, \mathbb{Q}_p, \mathbb{I}_K$ hanno sottogruppi piccoli.

Quindi la legge di reciprocità globale è

Se L/K ab. finita e $S = M_\infty \cup \{$ primi che ramificano in $K\}$

la funzione

$$\psi_{L/K} : \mathcal{J}^S \longrightarrow Gal(L/K) = G$$
$$\sum_{v \notin S} n_v v \longmapsto \prod_{v \notin S} Frob_{L/K}(v)^{n_v}$$

è un omom. ammissibile.

G finito.

ammissibile $\Rightarrow \ker \psi_{L/K} \ni K^S \cdot (1 + \mathfrak{a})$

dove $\mathfrak{a}$ è un ideale con supporto in S

(cioè costruito a partire da primi non arch. in S)

+ condizioni ai primi archimedei.

Questo "ideale" si dice MODULO.

$\rightsquigarrow$ Le est. ab. di K sono descritte in termini di congruenze

(fino qui Cassels-Frölich)

Milne:

Def. Un modulo per K è una funzione

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

t.c.

1) $m(v) = 0$ per quasi tutti i v.

2) se $K_v = \mathbb{R}$ $\quad m(v) \in \{0, 1\}$

3) se $K_v = \mathbb{C}$ $\quad m(v) = 0$

Tradizionalmente $m = \sum_v m(v) v$

Diciamo che m_1 divide m_2 se

$m_1(v) \leq m_2(v)$ per ogni v.

v divide m se $m(v) > 0$.

$$m = \underbrace{\sum_{v \in \mathfrak{M}_0} m(v) v}_{\substack{\text{ideale} \\ \text{in } \mathcal{O}_K}} + \sum_{v \in \mathfrak{M}_\infty} m(v) v = m_0 + m_\infty$$

$\sum_{v \in \mathfrak{M}_\infty}$: sottoinsieme di posti arch. reali.

Poniamo

$$S(m) = \{ v \in \mathfrak{M}_K \mid v \text{ divide } m \}$$

supporto di m.

$$K_{m,1} = \{ a \in K^* \mid v(a-1) \geq m(v) \ \forall v \in \mathfrak{M}_0, \quad v(a) > 0 \quad \forall v \text{ reale } v \mid m \}$$

$$i : K^* \longrightarrow \mathcal{J}$$
$$a \longmapsto (a) = a\mathcal{O}_K$$

se $a \in K_{m,1}$ $\quad i(a) \in \mathcal{J}^{S(m)}$

Poniamo

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

RAY CLASS GROUP associato a m

Esempio

$$m = (2)^3 \cdot (17)^2 \cdot (13) \cdot \infty \quad \text{in } \mathbb{Q}$$

$$\mathbb{Q}_{m,1} \left\{ a \in \mathbb{Q} \;\middle|\; \begin{array}{l} a > 0 \\ \mathrm{ord}_2(a-1) \geq 3 \\ \mathrm{ord}_{17}(a-1) \geq 2 \\ \mathrm{ord}_{13}(a-1) \geq 1 \end{array} \right\}$$

Si vede facilmente che ogni classe in Cl_m è rappresentata da un ideale intero $\mathfrak{a} \subseteq \mathcal{O}_K$ e due ideali interi $\mathfrak{a}, \mathfrak{B}$ stanno nella stessa classe in Cl_m se $\exists\, a, b \in \mathcal{O}_K$ t.c. $a\mathfrak{a} = b\mathfrak{B}$ e

$a \equiv b \equiv 1 \mod m_0$

e a, b hanno lo stesso segno $\forall\, v$ reale t.c. $v \mid m$.

(per $m = 1$ $Cl_m = Cl(K)$).

Poniamo $K_m = \{ \alpha \in K^* \mid v(\alpha) = 0 \;\; \forall\, v \mid m_0 \}$

$$U_{m,1} = \mathcal{O}_K^* \cap K_{m,1}$$

c'è una succ. esatta

$$1 \longrightarrow U/U_{m,1} \longrightarrow K_m/K_{m,1} \longrightarrow Cl_m \longrightarrow Cl(K) \longrightarrow 1$$

$$\mathcal{J}^{S(m)} \longrightarrow \mathcal{J}$$

$$K_{m,1} = \left(\mathcal{O}_K/m_0\right)^{\times} \cdot \prod_{\substack{v \in m_\infty \\ v \mid m}} \{\pm 1\}$$

$\rightsquigarrow$ Cl_m è un gruppo finito di ordine

$$h_m = h\,[U : U_{m,1}]^{-1} \cdot 2^{r_0} N(m_0) \prod_{\wp \mid m_0} \left(1 - \frac{1}{N(\wp)}\right)$$

r_0 = posti reali di K.

(Milne)

<u>Esempi</u>

- se $m = 1$ $\quad Cl_m = Cl(K)$
- se m è il prodotto dei primi reali

C_m narrow class group e si ha

$$1 \longrightarrow U/U_+ \longrightarrow K^\times/K_+ \longrightarrow Cl_m \longrightarrow Cl \longrightarrow 1$$

$$K^\times/K_+ = \prod_{v \text{ reali}} \{\pm 1\}$$

$K_+ = \{$ elementi totalmente positivi di K (positivi in tutte le immersioni reali) $\}$

$U_+ = U \cap K_+$ unità tot. positive.

Quindi

$$\ker : Cl_m \longrightarrow Cl(K)$$

è l'insieme dei possibili segni modulo quelli che provengono dalle unità.

Es.

- Se $K = \mathbb{Q}$ il narrow class group è banale
- Se $K = \mathbb{Q}(\sqrt{d})$ $d > 0$

$U = \{\pm \varepsilon^m \mid m \in \mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

ε unità fondamentale

in questo caso

$$h_m = \begin{cases} 2h & \text{se } \varepsilon, \bar{\varepsilon} \ \overbrace{\text{hanno segni diversi}}^{N(\varepsilon) = -1} \\ h & \text{se } \varepsilon, \bar{\varepsilon} \ \underbrace{\text{hanno lo stesso segno}}_{N(\varepsilon) = 1} \end{cases}$$

Per es.

$d = 2, 5$ $\quad N(\varepsilon) = -1$

$d = 3, 6$ $\quad N(\varepsilon) = 1$

c) $K = \mathbb{Q}$ $\quad m = N \in \mathbb{Z}$

La successione diventa

$$1 \to \{\pm 1\} \to \left(\mathbb{Z}/N\mathbb{Z}\right)^* \to C_m \to 1$$

si ha $h_m = \dfrac{\varphi(N)}{2}$

c) $m = N\infty$

$$1 \to \{\pm 1\} \to \{\pm 1\} \times \left(\mathbb{Z}/N\mathbb{Z}\right)^* \to C_m \to 1$$

$$h_m = \varphi(N).$$

RAY CLASS FIELD

S insieme finito di primi di K

Un omomorfismo

$\varphi : \mathcal{J}^S \longrightarrow G$ ammette un modulo

se esiste un modulo m con $S(m) \supseteq S$

t.c. $\varphi(i(K_{m,1})) = 0$

cioè se φ fattorizza per Cl_m per qc.

m con $S \subseteq S(m)$.

La GRL dice che

se L/K ab. finito e

$S = M_\infty \cup \{v \mid v \text{ ramifica in } L\}$

$\rightsquigarrow$ la mappa di Artin $\varphi_{L/K} : \mathcal{J}^S \longrightarrow Gal(L/K)$

ammette un modulo m con $S \subseteq S(m)$

e definisce un isomorfismo

$$\frac{\mathcal{J}^{S(m)}}{K_{m,1} \, N(\mathcal{J}_L^{S(m)})} \xrightarrow{\sim} Gal(L/K)$$

m si dice modulo definente per L/K.

Teorema di esistenza (in termini di ideali)

Un sottogruppo $H \subseteq \mathcal{J}^{S(m)}$ si dice **sottogruppo di congruenza mod m** se contiene $i(K_{m,1})$

Th. esistenza: Per ogni sottogruppo di congruenza mod m esiste un'estensione ab. di L/K finita, non ramificata fuori da $S(m)$ e t.c. $H = i(K_{m,1})\, N_{L/K}(\mathcal{J}_L^{S(m)})$

$$\left(N_{L/K}\, \mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{p}}} \quad \text{se } \mathfrak{P} \mid \mathfrak{p} \right)$$