Teoria algebrica dei numeri

Corso Dottorato 23-24

Teoria del corpo di classe

Descrivere delle estensioni abeliane di $\mathbb{Q}$

$K/\mathbb{Q}$ di Galois con $\mathrm{Gal}(K/\mathbb{Q})$ abeliano.

- leggi di reciprocità
- Teorema di Kronecker-Weber ($\sim$ 1850)
- Introduzione al programma di Langlands:

$$\left\{\begin{array}{l}\text{Rappres. di}\\ \text{gruppi di Galois}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Rappres di}\\ \text{gruppi algebrici}\\ GL_2\end{array}\right\}$$

Prerequisiti

A) CAMPI DI NUMERI E ANELLI DI INTERI, ARITMETICA

B) CAMPI LOCALI

C) TEORIA DI GALOIS INFINITA.

Bibliografia

- Kedlaya (note online)
- Milne (CFT)
- Cassels-Fröhlich (ANT)
- Lang
- Neukirch

- Serre Local fields (per la LCFT)

Teoria di Galois

L/K $K \subseteq L$ estensione

L K-spazio vett.

L/K finita se $\dim_K L = [L:K]$ è finito.

Ogni $\alpha \in L$ è algebrico su K

$\exists f(x) \in K[x]$ di grado minimo non nullo t.c. $f(\alpha)=0$. $\rightsquigarrow$ POLINOMIO MINIMO DI α su K.

Se L/K è algebrica $\forall \alpha \in L$ si ha $[K(\alpha):K]<\infty$.

Dato K consideriamo $\bar{K}$ chiusura algebrica di K.

(esiste sempre ed è unica a meno di K-isomorfismi)

$L/K \rightsquigarrow L \subseteq \bar{K}$

Se L/K estensione algebrica finita di grado n $\Leftrightarrow$ esistono al più n K-immersioni $L \to \bar{K}$

Se ce ne sono esattamente n, L/K si dice separabile.

$K = \mathbb{F}_p(x)$ $\quad L = K(\sqrt[p]{x})$ (α)

il pol. minimo di α su K è $Y^p - X$ irid. con derivata nulla

$\rightsquigarrow$ ha una sola radice in $\bar{K}$
c'è una sola K. immersione di L in $\bar{K}$.

Campo perfetto: tutte le sue estensioni finite sono separabili.

Se $\mathrm{char}(K)=0$ o K finito $\Rightarrow$ K perfetto.

L/K separabile

Se tutte le K. immersioni $L \to \bar{K}$ hanno L come immagine (sono autom. di L)

L/K si dice **normale**

L/K separabile + normale $=$ **galois.**

$\mathrm{Gal}(L/K) = \{$K. autom. di L$\}$ **gruppo di Galois di** L/K

Corrispondenza di Galois

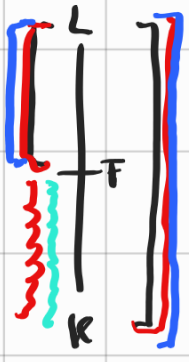
1) C'è una corrispondenza biunivoca

$$\{\text{campi intermedi } K \subseteq F \subseteq L\} \rightsquigarrow \{\text{Sottogruppi di } \mathrm{Gal}(L/K)\}$$

$$F \longmapsto \mathrm{Gal}(L/F)$$

$$L^H \longleftarrow H$$

$$L^H = \{\alpha \in L \mid \sigma(\alpha)=\alpha \ \ \forall \sigma \in H\}$$



2) F/K è normale $\iff Gal\left(\frac{L}{F}\right) \lhd Gal\left(\frac{L}{K}\right)$

In questo caso

$$Gal\left(\frac{L}{K}\right) \xrightarrow{\text{Res}} Gal\left(\frac{F}{K}\right)$$

induce un isomorfismo

$$\frac{Gal\left(\frac{L}{K}\right)}{Gal\left(\frac{L}{F}\right)} \xrightarrow{\sim} Gal\left(\frac{F}{K}\right)$$

Esempi notevoli

1) Estensioni quadratiche

$L = K(\beta)$ $\quad \beta^2 \in K,\ \beta \notin K$

$x^2 - \beta^2$ $\quad L/K$ Galois

Attenzione $\mathbb{Z}_n$ non si deve più usare !!!

invece $\mathbb{Z}/n\mathbb{Z}$

$$Gal\left(\frac{L}{K}\right) \cong \mathbb{Z}/2\mathbb{Z}$$

2) $K = \mathbb{Q}$ $\quad L = \mathbb{Q}(\zeta_N)$ $\quad \zeta_N$ radice prim. N-esima di 1

$[L : \mathbb{Q}] = \varphi(N)$ funzione φ di Eulero

$L/\mathbb{Q}$ è Galois.

$$\begin{array}{ccc} Gal\left(L/\mathbb{Q}\right) & \longrightarrow & \left(\mathbb{Z}/N\mathbb{Z}\right)^{\times} \\ \sigma & \longmapsto & k \end{array} \qquad \text{isomorfismo} \qquad \sigma(\xi) = \xi^{k}$$

Estensione abeliana : Gal è abeliano.

Ciclotomico $\Rightarrow$ abeliano

KW: $L/\mathbb{Q}$ abeliana $\Rightarrow \exists N$ t.c. $L \subseteq \mathbb{Q}(\xi_N)$

3) Estensioni radicali : $\mathrm{char}(K) = 0$ o $\mathrm{char} K \nmid n$.

K contenga μ_n = radici n-esime dell'unità

L/K finita è ciclica di ordine $m \mid n \iff$

$L = K(\beta)$ con $\beta^m \in K$.

- L_1, L_2 estensioni di K in $\bar{K}$

$L_1 L_2$ composto : più piccolo sottocampo di $\bar{K}$ contenente L_1 e L_2

se L_1/K, L_2/K Galois

$L_1 L_2/K$ è Galois e

$$Gal\left(L_1 L_2/K\right) \hookrightarrow Gal\left(L_1/K\right) \times Gal\left(L_2/K\right)$$

è un isom. se $L_1 \cap L_2 = K$ (L_1, L_2 linearmente disgiunti su K).

Campi finiti

K campo finito $|K| = p^t$ p primo

$\forall q = p^t$ $\exists$ K finito t.c. $|K| = p^t$

unico a meno di isomorfismo.

$\mathbb{F}_p$ $\quad$ $\overline{\mathbb{F}}_p$

esiste in $\overline{\mathbb{F}}_p$ un unico campo $\mathbb{F}_q$ con q elem. che è il campo di spezzamento di $X^q - X$

ma tutte le estensioni finite di $\mathbb{F}_p$ sono Galois.

Automorfismo di Frobenius:

$$\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$$
$$x \longmapsto x^p$$

$\varphi^t(x) = x^{p^t} = x$ $\quad$ ma $\quad$ $\varphi^t = id$ su $\mathbb{F}_q$

$$Gal\left(\mathbb{F}_q / \mathbb{F}_p\right) = \langle \varphi \rangle \simeq \mathbb{Z}/t\mathbb{Z}$$

In generale $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^t} \iff r \mid t$

e $\mathrm{Gal}\left(\frac{\mathbb{F}_{p^t}}{\mathbb{F}_{p^r}}\right) = \langle \varphi^r \rangle \simeq \frac{\mathbb{Z}}{(t-r)\mathbb{Z}}$

$\Rightarrow$ tutte le estensioni finite di campi finiti sono cicliche.

TEORIA DI GALOIS PER ESTENSIONI INFINITE

Sistemi proiettivi (o inversi)

$(I, \leq)$ sistema diretto

se

- $\leq$ riflessiva e transitiva
- $\forall\, i_1, i_2 \in I \quad \exists\, i \in I$ t.c. $i_1, i_2 \leq i$.

Sia $(G^i)_{i \in I}$ una famiglia di gruppi topologici indicizzati da I.

$\left(I, \{G^i\}, \{\pi_i^j\}_{j \geq i}\right)$ si dice sistema inverso se

- $\pi_i^j : G^j \longrightarrow G^i$ morfismo continuo

t.c.

$\pi_i^i = \mathrm{id} : G^i \longrightarrow G^i \quad \forall i$

e inoltre se $k \geq j \geq i$

$\pi_i^k = \pi_i^j \circ \pi_j^k$

Esempio: $I = \mathbb{N}$ con $N \leq M$ se $N \mid M$

$\pi_N^M : \frac{\mathbb{Z}}{M\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{N\mathbb{Z}}$ (top. discreta).

$\left(\mathbb{N}, \left\{\frac{\mathbb{Z}}{N\mathbb{Z}}\right\}_N, \{\pi_N^M\}\right)$ sistema inverso.

Dato $(I, \{G^i\}, \{\pi_i^j\})$ sistema inverso, cons. $\prod_{i\in I} G^i$ $(x_i)_{i\in I}$ suo elemento.

e il sottogruppo

$$\hat{G} = \{ (x_i)_{i\in I} \mid \forall j \geq i \quad \pi_i^j(x_j) = x_i \}$$

(con la top. indotta dalla top. prodotto)

quindi $\forall i \in I$ $\pi_i : \hat{G} \longrightarrow G^i$ è continua
$(x_i)_i \mapsto x_i$

$\hat{G}$ si dice **limite proiettivo (o inverso)** del sistema precedente,

$$\hat{G} = \varprojlim G^i$$

I triangoli

$$\begin{array}{ccc} \hat{G} & \xrightarrow{\pi_j} & G^j \\ & \searrow^{\pi_i} & \downarrow \pi_i^j \\ & & G_i \end{array}$$

commutano $\forall j \geq i$

Proprietà universale del limite proiettivo

$\forall H$ gruppo topologico per il quale esistono omom. continui $\varphi_i : H \longrightarrow G^i$ con indici che commutato

$$\begin{array}{ccc} H & \xrightarrow{\varphi^j} & G^j \\ & \searrow^{\varphi_i} & \downarrow \pi_i^j \\ & & G^i \end{array} \qquad \forall j \geq i$$

allora esiste un unico omom. continuo

$\varphi : H \longrightarrow \hat{G}$

t.c.

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \hat{G} \\ & \searrow^{\varphi_i} & \downarrow \pi_i \\ & & G^i \end{array}$$

commutano. $\forall i$

GRUPPO PROFINITO = limite proiettivo di gruppi finiti con la topologia discreta.

Esempio

$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ è profinito

G^i compatti $\forall i \Rightarrow \varprojlim G^i$ è compatto

(chiuso in un compatto)

Gruppi profiniti sono compatti

Sono totalmente sconnessi.

Caratterizzazione topologica dei gruppi profiniti:

G profinito $\iff$ compatto e totalmente sconnesso

Esempi notevoli

1) Gruppi finiti
2) $\hat{\mathbb{Z}}$
3) $\left(\left(\frac{\mathbb{Z}}{p^m\mathbb{Z}} \right)_m, (\pi_m^n) \right)$ $\qquad \pi_m^n : \frac{\mathbb{Z}}{p^n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{p^m\mathbb{Z}}$ se $n \geq m$

$$\varprojlim \frac{\mathbb{Z}}{p^n\mathbb{Z}} = \mathbb{Z}_p$$

Se $N = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$

$$\frac{\mathbb{Z}}{N\mathbb{Z}} = \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}$$

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

Altri gruppi profiniti:

$$\left(\frac{\mathbb{Z}}{M\mathbb{Z}} \right)^\times \longrightarrow \left(\frac{\mathbb{Z}}{N\mathbb{Z}} \right)^\times \qquad N \mid M$$

$$\rightsquigarrow \varprojlim \left(\frac{\mathbb{Z}}{M\mathbb{Z}} \right)^\times \simeq \hat{\mathbb{Z}}^\times$$

Analogamente $\varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}} \right)^\times \simeq \mathbb{Z}_p^\times$

E/F estensione di Galois (algebrica, separabile, normale)

$(K_i \mid i \in I)$ famiglia di tutte le estensioni di Galois K_i/F finite con $F \subseteq K_i \subseteq E$.

Allora $E = \bigcup_{i \in I} K_i$

Se

$K_i \subseteq K_j$ allora la restrizione dà un omom.

$$\pi_i^j : Gal\left(\frac{K_j}{F}\right) \longrightarrow Gal\left(\frac{K_i}{F}\right)$$

inoltre dati K_i, K_j il composto $K_i K_j \supseteq K_i, K_j$

(K_i) sistema diretto

e i $G_i = Gal\left(\frac{K_i}{F}\right)$ formano un sistema inverso. Proprietà universale fornisce mappa

$$Gal\left(\frac{E}{F}\right) \longrightarrow \varprojlim G_i$$

che si verifica essere un isomorfismo.

$Gal\left(\frac{E}{F}\right)$ eredita topologia $\rightsquigarrow$ topologia di Krull.

(un sistema fond. di intorni dell'identità sono i $Gal\left(\frac{E}{K_i}\right)$)

Corrispondenza di Galois.

1) esiste biiezione

$\{$campi intermedi $F \subseteq L \subseteq E\}$ $\longleftrightarrow$ $\{$sottogruppi chiusi di $Gal(E/F)\}$

$$L \longmapsto Gal(E/L)$$

$$E^H \longleftarrow H$$

2) L/F Galois $\iff Gal(E/L) \lhd Gal(E/F)$

la restrizione dà

isom. + omeo

$$Gal(E/F)\Big/Gal(E/L) \xrightarrow{\sim} Gal(L/F)$$

$$E = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_n \mathbb{Q}(\mu_{p^n})$$

$$Gal(E/\mathbb{Q}) = \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times$$

$$Gal\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) = \hat{\mathbb{Z}}$$

$\mathbb{Z} \subseteq \hat{\mathbb{Z}}$ ma non è chiuso

esercizio: provare che $\mathbb{Z}$ è denso dentro a $\hat{\mathbb{Z}}$

$$\boxed{\overline{\mathbb{F}_p}^{\mathbb{Z}} = \overline{\mathbb{F}_p}^{\hat{\mathbb{Z}}} = \mathbb{F}_p}$$