G&HG 25-03-21

An introduction to Galois module structure. The case of tame extensions (I. Del Corso)

1. Definizioni di base: G-moduli, basi normali (intere), reticoli, modulo indice, discriminante. Estensioni linearmente e aritmeticamente disgiunte

2. L/K ammette NIB $\Rightarrow$ L/K è tame

   L/K tame $\Leftrightarrow$ $Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$

3. Il teorema di Hilbert-Speiser: $L/\mathbb{Q}$ tame + abeliana $\Rightarrow$ $L/\mathbb{Q}$ ammette NIB

4. Il caso dei campi p-adici: L/K tame + Galois $\Updownarrow$ L/K ammette NIB.

Ref:

H. Johnston: Notes on Galois modules (personal web page)

G gruppo, M gruppo abeliano.

M si dice G-modulo se c'è un'azione di G su M per endom.

cioè se $\exists\ \varphi\ G \longrightarrow \mathrm{End}\, M$ omomorfismo

Equiv., posto $\quad \mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z} \right\}$

$$G\text{-modulo} = \mathbb{Z}[G]\text{-modulo}$$

M è un modulo di Galois se $G = \mathrm{Gal}(L/K)$ e l'azione di G è quella di Galois

Esempi: L/K di Galois $\quad G = \mathrm{Gal}(L/K)$

- L è un $K[G]$-modulo
- $\mathcal{O}_L$ è $\mathcal{O}_K[G]$-modulo
- $Cl(K)$ è $\mathcal{O}_K[G]$-modulo
- $\mathcal{O}_L^\times$ $\mathbb{Z}[G]$-modulo

Teorema della base normale

$L/K \quad \mathrm{Gal}(L/K) = G \Rightarrow L$ è un $K[G]$-modulo libero di rk 1

$L = K[G]\,w \qquad \{\sigma(w)\}_{\sigma \in G}$ è una K-base di L

$\hookrightarrow$ BASE NORMALE

Se L/K sono NF o p-adici. $\mathcal{O}_L$ è $\mathcal{O}_K[G]$ modulo

$\mathcal{O}_L$ è un $\mathcal{O}_K[G]$ modulo LIBERO?

$\sim$ $\exists\, \alpha \in \mathcal{O}_L$ tale che $\mathcal{O}_L = \mathcal{O}_K[G]\alpha$, $\{\sigma\alpha\}_{\sigma\in G}$ base normale intera NIB

In generale la risposta è **NO**

$\mathcal{O}_L$ non è necessariamente libero su $\mathcal{O}_K$

E se $\mathcal{O}_K$ è PID? non basta!

Esempi: ① $K = \mathbb{Q}(i)$ $\quad \mathbb{Z}[i]$ non ha NIB su $\mathbb{Z}$.

$G = \{id, \sigma\}$ $\quad \sigma w = \overline{w}$ $\quad\quad w = a + ib$

$\mathbb{Z}[G]w = \{\lambda(a+ib) + \mu(a-ib) \mid \lambda, \mu \in \mathbb{Z}\}$

$$1 \in \mathbb{Z}[G]w \iff \begin{cases} (\lambda+\mu)a = 1 \\ (\lambda-\mu)b = 0 \end{cases} \Rightarrow b = 0 \vee \lambda = \mu$$

$\mathbb{Z}[G]w = \mathbb{Z}[G]a = \mathbb{Z}$

$2\lambda a = 1$ no sol in $\mathbb{Z}$.

② $K = \mathbb{Q}(\sqrt{5})$ $\quad \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, $\quad \mathcal{O}_K = \mathbb{Z}[G]\frac{1+\sqrt{5}}{2}$

Quando $\mathcal{O}_L$ è libero su $\mathcal{O}_K[G]$?

Se sì, riesco a determinarne un generatore?

Reticoli. R dominio noetheriano, K campo di quozienti $R \neq K$

V K spazio vettoriale di dim finita

$M \subset V$ R-modulo si dice <u>R-reticolo</u> (R-lattice) di V
(si dice libero se lo è come R-modulo.)

se $KM = \text{span}_K M = V$ ($\Leftrightarrow$ M contiene una K-base di V)

Esempi: $L|K$ NF. $\mathcal{O}_L$ è un $\mathcal{O}_K$-reticolo, non necessariam libero

Notazione: K NF $\mathcal{O}_K$, $P \subset \mathcal{O}_K$ max

K_P, $\mathcal{O}_P$ completamenti rispetto alla val P-adica

M $\mathcal{O}_K$-modulo $\Rightarrow$ $M_P \doteq M \otimes_{\mathcal{O}_K} \mathcal{O}_P$

V K-sp. vett $\Rightarrow$ $V_P = V \otimes_K K_P$

Lemma: M, N reticoli in $V \Rightarrow M_P = N_P$ per quasi tutti i P.

Modulo indice e discriminante.

M N $\mathcal{O}$-Reticoli di V liberi

$\mathcal{B}_M = \{\alpha_1, \dots, \alpha_n\}$ $\qquad$ $\mathcal{B}_N = \{\beta_1 \dots \beta_n\}$

$[M:N] = \det[\alpha]$ $\qquad$ α $\quad$ $V \longrightarrow V$

$\alpha_i \longrightarrow \beta_i = \sum a_{ij} \alpha_j$

$A = \{a_{ij}\}$

$b \quad V \times V \longrightarrow K \qquad V = L$.

$\delta(M) = \operatorname{disc} M = \det(\{b(\alpha_i, \alpha_j)\}) \qquad Tr\ (x,y) \to Tr_{L/K}(xy)$

$$\boxed{\delta(N) = [M:N]^2\, \delta(M)} \quad *$$

Se M e N non sono liberi $\longrightarrow M_p \ N_p \qquad \mathcal{O}_p$ DVR.

$\delta(N_p) \qquad \delta(M_p) \qquad [M_p : N_p]$

$\delta(M) =$ l'unico ideale frazionario di $\mathcal{O}$ tale che

$\delta(M)_p = \delta(M_p) \qquad$ ($\exists$ perché $\delta(M_p) = \mathcal{O}_p$ per quasi tutti i p)

$[M:N] =$ l'unico id fraz di $\mathcal{O}$ tale che

$[M:N]_p = [M_p : N_p]$

La formula $*$ è vera in generale

Teorema: L/K e. di numeri o p-adica

$p \subset \mathcal{O}_K$ ramifica in $\mathcal{O}_L \iff p \mid \delta(L/K) = \underset{Tr}{\delta(\mathcal{O}_L)}$

Def: L, K estensioni finite di $F \qquad L, K \subset \Omega(F)$)

$$\begin{tikzcd}
 & LK \arrow[dl, dash, "n"'] \arrow[dr, dash] \arrow[dd, dash, "v_i w_j"] & \\
L \arrow[dr, dash, "\{v_i\}"'] & & K \arrow[dl, dash, "n\ \{w_j\}"] \\
 & F &
\end{tikzcd}$$

L e K si dicono linearmente disgiunti se $L \otimes_F K \cong LK$

$x \otimes y \longrightarrow xy$

$$K = F(\alpha) \cong \frac{F[x]}{(\mu_F(x))} \qquad LK = L(\alpha) \cong \frac{L[x]}{(\mu_L(x))} \qquad \mu_L \mid \mu_F$$

$$L \otimes_F K \cong \frac{L[x]}{(\mu_F(x))} \cong \bigoplus \frac{L[x]}{(\mu_i(x))} \qquad \mu_L = \mu_F$$

L e K sono l. disgiunti su F $\iff$ μ_F resta irrid. in L

$$\iff [LK:F] = \underbrace{[LK:L]}_{= [K:F]}[L:F] = [K:F][L:F]$$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, no head] & & \mathbb{Q}(\zeta_3 \sqrt[3]{2}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

non sono l. disgiunti

Def: L, K sono aritmeticamente disgiunti su F

se (1) sono l. disgiunti

(2) $(\delta(L/F), \delta(K/F)) = 1$

TEOREMA

F NF o p-adico, L, K aritm. disg su F

$$\Rightarrow \mathcal{O}_{LK} \cong \mathcal{O}_L \otimes_{\mathcal{O}_F} \mathcal{O}_K \cong \mathcal{O}_L \mathcal{O}_K$$

$$\begin{tikzcd}
 & LK \arrow[dl, no head] \arrow[dr, no head, "\delta"] & \\
L \arrow[dr, no head, "\delta"'] & & K \arrow[dl, no head] \\
 & F &
\end{tikzcd}$$

Dim $\mathcal{O}_L \mathcal{O}_K \subseteq \mathcal{O}_{LK}$

Per mostrare $l' =$ basta vedere $[\mathcal{O}_{LK} : \mathcal{O}_L \mathcal{O}_K] = \mathcal{O}_K$

Se per assurdo $p \subset \mathcal{O}_K$ $\quad p \mid [\mathcal{O}_{LK} : \mathcal{O}_L \mathcal{O}_K]$

$$[\mathcal{O}_{LK} : \mathcal{O}_L \otimes \mathcal{O}_K]^2 = \delta_{LK/K}(LK/K)^{-1} \, \delta_{LK/K}(\underbrace{\mathcal{O}_L \otimes \mathcal{O}_K}_{\mathcal{O}_L \mathcal{O}_K})$$

$$Tr_{L/F} \otimes \mathrm{id}$$

$$\delta_{L/F}(\mathcal{O}_L)\, \mathcal{O}_K$$

$(\delta(L/F), \delta(K/F)) = 1$ posso supporre che

$p \nmid \delta(L/F)$

$$p \mid [\mathcal{O}_{LK} : \mathcal{O}_L \otimes \mathcal{O}_K]^2 = \delta(LK/K)^{-1} \, \delta_{L/F}(\mathcal{O}_L)\, \mathcal{O}_K$$

$$\Longleftrightarrow \quad p \mid \delta(L/F)$$

Oss: F p-adico L, K campi disgiunti:

(1) Uno tra L/F e K/F è non ramificato (L)

(2) $([L : F], [K^{unram} : F]) = \mathcal{O}_F$

Teorema

F c. di n. a p-adica

(1) L e K lin disgiunti su F

(2) L/F di Galois G

(3) $\mathcal{O}_L \cong \mathcal{O}_F[G]\alpha$

$\Rightarrow \mathcal{O}_{LK} = \mathcal{O}_K[G]\alpha$

(4) K/F è di Galois H

$\mathcal{O}_K = \mathcal{O}_F[H]\beta$

$$\begin{tikzcd}
 & LK \arrow[dl, dash, "H\ \beta"'] \arrow[dr, dash, "G\ \alpha"] \arrow[dd, dash, "H\times G\ \alpha\beta"] & \\
L \arrow[dr, dash, "NIB\ \alpha\ G"'] & & K \arrow[dl, dash, "NIB\ \beta\ H"] \\
 & F &
\end{tikzcd}$$

Proposizione: L/F NF o p-adici di Galois.

K campo intermedio di Galois su F

α genera una NIB di $L/F \Rightarrow Tr_{L/K}(\alpha)$ genera base intera di K/F

Dim: $G = Gal(L/F)$ $\quad K = L^H$ $\quad H \trianglelefteq G$ $\quad Gal(K/F) \cong G/H$

$$\begin{tikzcd}
L \arrow[d, dash, "H \trianglelefteq G"] \arrow[dd, dash, bend right, "G"', "\text{NIB } \alpha"] \\
K = L^H \arrow[d, dash, "Tr_{L/K}(\alpha)\ \text{NIB}"] \\
F
\end{tikzcd}$$

$$\mathcal{O}_L = \mathcal{O}_F[G]\alpha$$

$$\forall x \in \mathcal{O}_L \qquad x = \sum_{g \in G} a_g\, g(\alpha) \qquad a_g \in \mathcal{O}_F$$

$$x \in \mathcal{O}_K \iff hx = x \quad \forall h \in H$$

$$hx = \sum_{g \in G} a_g\, hg(\alpha) = \sum_{g \in G} a_{h^{-1}g}\, g(\alpha) = x = \sum_{g \in G} a_g\, g(\alpha)$$

$\{g(\alpha)\}$ $\mathcal{O}_F$-base $\;=\;$ vale $\iff$ $a_g = a_{h^{-1}g} \quad \forall h$

$\iff$ i coeff di x sono costanti sulle classi laterali ($H\sigma$) di H in G

$$x = \sum_{\sigma \in G/H} a_\sigma \sum_{h \in H} h\sigma(\alpha) \underset{\substack{\checkmark \\ H \trianglelefteq G}}{=} \sum_{\sigma \in G/H} a_\sigma\, \sigma \sum_{h \in H} h(\alpha) = \sum_\sigma a_\sigma\, \sigma\, Tr_{L/K}(\alpha)$$

$$\Rightarrow \mathcal{O}_K = \mathcal{O}_F[G/H]\, Tr_{L/K}(\alpha)$$

$\square$

Corollario Se L/F ha NIB $\Rightarrow Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}_K \quad \forall K$
$F \subset K \subset L$

In particolare $Tr_{L/F}(\mathcal{O}_L) = \mathcal{O}_F$

Dim $Tr_{F/F}(\mathcal{O}_L) \subset \mathcal{O}_K \qquad K = L^H \qquad H \leq G$

$$x \in \mathcal{O}_K \qquad x = \sum_{\sigma \in G/H} a_\sigma \sum_h h\sigma(\alpha) = \sum_{\sigma \in G/H} a_\sigma Tr_{L/K}(\sigma(\alpha))$$

$$= Tr_{L/K}\Big(\sum_\sigma a_\sigma \sigma(\alpha)\Big) \in Tr_{L/K}(\mathcal{O}_L)$$

$a_\sigma \in \mathcal{O}_F$

L/F CdN $\qquad P \subset \mathcal{O}_F$ ha ramific. TAME in L

se $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r} \qquad \left(e_i, \operatorname{char} \frac{\mathcal{O}_F}{P}\right) = 1$

L/F è Tame se $\forall P \subset \mathcal{O}_F$ P ha ramific. Tame in L.

Teorema L/K di Galois di CdN o p-adici

$$L/K \text{ è Tame} \iff Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$$

Dim! $Tr_{L/K}(\mathcal{O}_L)$ è un ideale di $\mathcal{O}_K$

- mostriamo che $P \subset \mathcal{O}_K$ $P \mid Tr_{L/K}(\mathcal{O}_L) \iff P$ ha ramific wild in L.

$$P\mathcal{O}_L = (Q_1 \cdots Q_r)^e \qquad k = \frac{\mathcal{O}_K}{P} \qquad \ell_i = \frac{\mathcal{O}_L}{Q_i}$$

$$Tr_{L/K}(\alpha) = e \sum_{i=1}^r Tr_{\ell_i/k}(\bar{\alpha}) \quad \text{alg lin}$$

P wild $\iff p \mid e \Rightarrow \forall \alpha \in \mathcal{O}_L \; Tr_{L/K}(\alpha) \equiv 0 \; (P) \quad P \mid Tr_{L/K}(\mathcal{O}_L)$

Viceversa $Tr_{L/K}(\mathcal{O}_L) \subset P$

$Tr_{e_i/k}$ è suriettiva. $\exists\ \beta_1 \in \mathcal{O}_L$ t.c. $Tr_{e_1/k}(\bar\beta_1) \not\equiv 0$

$\beta \in \mathcal{O}$ $\begin{cases} \beta \equiv \beta_1 & (\mathfrak{Q}_1) \\ \beta \equiv 0 & (\mathfrak{Q}_i) \quad \forall\, 2 \le i \le r \end{cases}$

$Tr_{L/k}(\beta) \equiv e\, Tr_{e_1/k}(\bar\beta_1) \equiv 0 \ (P) \Rightarrow e \equiv 0 \ (p)$ wild.

Corollario

Se L/K ammette una NIB $\Rightarrow L/K$ Tame.

Il teorema di Hilbert-Speiser

Proposizione.

n libero da quadrati e sia $K \subset \mathbb{Q}(\zeta_n)$

Allora $K/\mathbb{Q}$ ha una NIB e $Tr_{\mathbb{Q}(\zeta_n)/k}(\zeta_n)$ è un gen.

Dim:

- Basta mostrare che ζ_n è un generatore per una NIB di $\mathbb{Q}(\zeta_n)$

$n = p_1 \cdots p_r$ per induzione su r

$$\zeta \quad \begin{array}{c} \mathbb{Q}(\zeta_n) \\ | \\ K \\ |\ Tr(\zeta) \\ \mathbb{Q} \end{array}$$

$n = p$ primo ζ_p genera NIB per $\mathbb{Q}(\zeta_p)$

$\mathbb{Z}[\zeta_p]$ $1, \zeta, \dots, \zeta^{p-2}, \zeta$ unità $\Rightarrow$

$\{\sigma\zeta\} = \{\zeta, \zeta^2, \dots \zeta^{p-1}\}$ $\mathbb{Z}$-base $\mathbb{Z}[\zeta_p]$

$n = pm \qquad (m,p) = 1$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_n) \arrow[dd, dash, "\zeta_p\zeta_m"] & \\
\mathbb{Q}(\zeta_p) \arrow[ur, dash] & & \mathbb{Q}(\zeta_m) \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash, "\zeta_p"] \arrow[ur, dash, "\zeta_m"'] &
\end{tikzcd}$$

- $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_m)$ sono aritm disgiunti

$\Rightarrow \zeta_p \zeta_m$ è un generatore di un NIB

$\uparrow$ radice n-esima primitiva di 1

Teorema di Hilbert-Speiser

Ogni estensione abeliana tame di $\mathbb{Q}$ ammette una NIB

Dim.

- $K/\mathbb{Q}$ abeliana TAME $\xRightarrow{K-W}$ K è contenuto in una estensione ciclotomica tame di $\mathbb{Q}$
- $\mathbb{Q}(\zeta_n)$ è tame $\Leftrightarrow$ n è libero da $\square$
- $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta)$ è un generatore di una NIB di $K/\mathbb{Q}$

Teorema (GRRS 99) $\mathbb{Q}$ è l'unico c.d. numeri per il quale vale H.S.

MARTINET 70 $\qquad G = D_p$ "$Gal(L/\mathbb{Q})$" $\qquad p$ primo $p \neq 2 \Rightarrow L/\mathbb{Q}$ NIB

MARTINET 71 $\qquad F = \mathbb{Q}(\sqrt{5}, \sqrt{21}) \qquad L_1 = F(\sqrt{m})$ NIB

$m = \frac{5+\sqrt{5}}{2} \cdot \frac{21+\sqrt{21}}{2} \qquad L_2 = F(\sqrt{-3m})$ NO NIB

$Gal(L_i/\mathbb{Q}) \cong Q_8$

Estensioni tame di campi p-adici

Estensioni non ramificate:

L/K finita e non ramificata p-adica $\Rightarrow$ L/K ammette NIB.

Dim $P\mathcal{O}_L = \mathfrak{Q}$ $\quad [L:K] = [k_L : k_K]$

L/K è di Galois $G = Gal(L/K) \cong Gal(k_L/k_K) = \bar{G}$

Per il T della base normale $k_L = k_K[\bar{G}]\bar{\alpha}$

Claim $\mathcal{O}_L \underset{\supset}{=} \mathcal{O}_K[G]\alpha = M$

$$\frac{M}{PM} = k_K[\bar{G}][\bar{\alpha}] = k_L = \frac{\mathcal{O}_L}{\mathfrak{Q}} = \frac{\mathcal{O}_L}{P\mathcal{O}_L}$$

$$\mathcal{O}_L = M + P\mathcal{O}_L \overset{Nak}{\Rightarrow} \mathcal{O}_L = M$$

Estensioni totalmente ramificate Tame

L/K di Galois di grado e Tot ram Tame $\Rightarrow$ L/K ammette NIB

Più precisamente, sia $\pi_L \in L$ uniformizzante t.c.
$\pi_L^e = \pi_K$ unif. di K. Allora $\forall$ scelta di $u_0, \dots, u_{e-1} \in \mathcal{O}_K^*$

$$\alpha = \sum_{i=0}^{e-1} u_i \pi_L^i$$

genera una NIB di L/K

Sappiamo che ogni est tot ramificata e Tame è del tipo $\qquad L = K(\sqrt[e]{\pi_K})$ $\qquad$ per un opportuno unif. π_K di K

$e \not\equiv 0 \ (p)$ $\qquad x^e - \pi_K$

L/K di Galois $\iff K \ni \zeta_e$ e $Gal(L/K)$ è ciclico

$\pi_L = \sqrt[e]{\pi_K} \qquad \pi_L \in L \qquad v(\pi_L) = \frac{1}{e}$

$\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L] \qquad 1, \pi_L, \dots, \pi_L^{e-1}$ base intera.

Per dire che $\{g(\alpha)\}_{g \in G}$ è una NIB

basta dimostrare che è una base

$$\langle \{g(\alpha)\} \rangle_{\mathcal{O}_K} \subseteq \langle \pi_L^i \rangle_{\mathcal{O}_K}$$

$$[\mathcal{O}_L : \langle \{g(\alpha)\} \rangle_{\mathcal{O}_K}] = \mathcal{O}_K$$

$\{\pi^i\} \longrightarrow \{g(\alpha)\}$ applicazione K-lineare è invertibile in $\mathcal{O}_K$

$Gal(L/K) = \langle \sigma \rangle \qquad \sigma\pi_L = \zeta \pi_L$

$$\sigma^j(\alpha) = \sum_{i=0}^{e-1} u_i \, \sigma^j(\pi_L)^i = \sum_{i=0}^{e-1} \underbrace{u_i \zeta^{ij}} \pi_L^i$$

$A = \{u_i \zeta^{ij}\} \leftarrow$ è invertibile in $\mathcal{O}_K$

$$\det A = \prod u_i \underbrace{\det\{\zeta^{ij}\}}_{\text{Vandermonde}} = \prod u_i \underbrace{\prod (\zeta^i - \zeta^j)}_{\in \mathcal{O}_K^*} \qquad \square$$

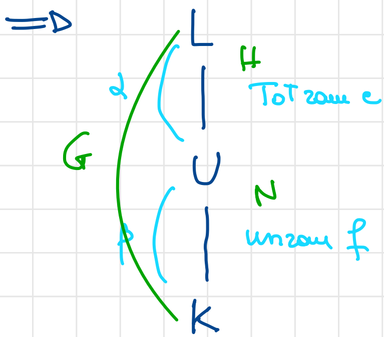
Caso generale

L/K finite di Galois di campi p-adici

L/K ammette NIB $\iff$ L/K è Tame.

Dim: ($\Leftarrow$) già visto

$\Longrightarrow$



$$\vartheta_L = \vartheta_U[H]\,\alpha =$$
$$= \bigoplus_{\sigma} \vartheta_U\, \sigma(\alpha)$$
$$= \bigoplus_{\sigma} \bigoplus_{\eta} \vartheta_K\, \eta(\beta)\, \sigma(\alpha)$$