Esempio di estensioni locali tot. ram. con composto non tot. ramificato

p dispari, $p \not\equiv 1 \mod 4$

$$\mathbb{Q}_p(\sqrt{p}) \qquad \mathbb{Q}_p(\sqrt{-p})$$

estensioni quadratiche di $\mathbb{Q}_p$ tot. ramificate.

$$\mathbb{Q}_p(\sqrt{p}, \sqrt{-p}) = \mathbb{Q}_p(\sqrt{p}, \sqrt{-1}) = K$$

$$\mathbb{Q}_p(\sqrt{-1}) \subseteq K$$

↳ quadratica, non ramificata perché $\mathbb{F}_p(\sqrt{-1}) = \mathbb{F}_{p^2}$ ha grado 2 su $\mathbb{F}_p$.

CAMPI GLOBALI (campi di numeri)

$K/\mathbb{Q}$ finita. $[K:\mathbb{Q}] = d$

$\alpha \in K$ è **intero** se $f(\alpha) = 0$ $f \in \mathbb{Z}[x]$ monico ($\Leftrightarrow$ il pol. minimo di α su $\mathbb{Q}$ ha coeff. interi).

$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ interi}\}$ è un anello, è uno $\mathbb{Z}$-mod. libero di rg d.

$\mathcal{O}_K \cong \mathbb{Z}^d$ come gruppo additivo.

Esempi

- campi quadratici $K = \mathbb{Q}(\sqrt{d})$ $d \in \mathbb{Z}$ d squarefree

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \quad \text{se } d \equiv 2, 3 \mod (4)$$
$$= \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} \quad \text{se } d \equiv 1 \mod 4$$

- campi ciclotomici
  $K = \mathbb{Q}(\xi)$ $\qquad \mathcal{O}_K = \mathbb{Z}[\xi]$
- In generale non è detto che $\mathcal{O}_K$ sia **monogenico**, cioè che $\mathcal{O}_K = \mathbb{Z}[\alpha]$

Aritmetica di K = studio di $\mathcal{O}_K$.
$\mathcal{O}_K$ in generale non è un PID
In $\mathbb{Q}(\sqrt{-5})$
$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$
doppia fattorizzazione in irriducibili non associati $\rightsquigarrow \mathbb{Z}[\sqrt{-5}]$ non UFD $\Rightarrow$ non è PID.

Risulta: $\mathcal{O}_K$ **dominio di Dedekind.**
Def.
Un anello A è un d. di Dedekind se
è - un dominio
- integralmente chiuso
- noetheriano

- $\dim_{Krull}(A) = 1$ cioè ogni primo non nullo è massimale.

Integralmente chiuso: se $\alpha \in K = \mathrm{Frac}(A)$ e α radice di $f(x)$ monico in $A[x] \Rightarrow \alpha \in A$.

$\mathcal{O}_K$ è di Dedekind.

① A Dedekind $\Leftrightarrow$ $\forall \mathfrak{P}$ primo di A $A_{(\mathfrak{P})}$ è un DVR

② Ideale frazionario: I sotto $\mathcal{O}_K$-modulo di K t.c. esiste $\alpha \in K$ t.c. $\alpha I \subseteq \mathcal{O}_K$.

Prop. Se A di Dedekind, ogni ideale frazionario non nullo si decompone in modo unico come prodotto di potenze di primi $I = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$ $\mathfrak{P}_i$ primi di A e $e_1, \ldots, e_k \in \mathbb{Z}$

$(\mathfrak{P}^{-1} = \{\alpha \in K \mid \alpha\mathfrak{P} \subseteq \mathcal{O}_K\})$

Se $\alpha \in K^*$

$\alpha\mathcal{O}_K$ ideale frazionario principale

$\mathcal{O}_K$ pid $\Rightarrow$ Tutti gli id. frazionari sono principali

$\mathcal{I}_K =$ gruppo degli ideali frazionari di K

$\mathcal{P}_K =$ sottogruppo degli id. frat principali.

$$Cl(K) = \mathcal{I}_K / \mathcal{P}_K$$ gruppo delle classi di K.

Teorema: se K campo di numeri $Cl(K)$ è finito.

$K \quad \sigma_1, \dots, \sigma_d : K \hookrightarrow \overline{\mathbb{Q}} \subseteq \mathbb{C}$

Teorema delle unità (Dirichlet)

$\mathcal{O}_K^*$ elem. invertibili di $\mathcal{O}_K$.

$\mathcal{O}_K^*$ è f.g.

$$\mathcal{O}_K^* = G \times \mathbb{Z}^r$$

$G = \{$ radici dell'unità in $K \}$

$r = r_1 + r_2 - 1$ dove

$r_1 = |\{\sigma_i \mid \sigma_i : K \longrightarrow \mathbb{R}\}|$

$2r_2 = |\{\sigma_i \mid \sigma_i : K \longrightarrow \mathbb{C} \text{ e } \sigma_i(K) \not\subseteq \mathbb{R}\}|$

$r_1 + 2r_2 = d.$

Decomposizione degli ideali primi nei campi di numeri

L/K estensione di campi di numeri.

$\mathfrak{p}$ primo di K

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ $\quad \mathfrak{P}_i$ primi di $\mathcal{O}_L$

i $\mathfrak{P}_i$ sono e esattamente i primi di $\mathcal{O}_L$ che si restringono a $\mathfrak{p}$ in $\mathcal{O}_K$ cioè

$$\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$$

Diremo che

- $\mathfrak{p}$ è **inerte** se $g=1$ $\quad e_1 = 1$ $\quad \mathfrak{p}\mathcal{O}_L = \mathfrak{P}$
- $\mathfrak{p}$ **ramifica** se $e_i > 1$ per qualche i.
- $\mathfrak{p}$ **si decompone** se $g \geq 2$.

e_i = **indice di ramificazione** di $\mathfrak{p}$ a $\mathfrak{P}_i$

$e_i(\mathfrak{P}_i | \mathfrak{p})$

$$\underbrace{\mathcal{O}_L / \mathfrak{P}_i}_{= k_i} \text{ campo } \supseteq \underbrace{\mathcal{O}_K / \mathfrak{p}}_{= k}$$

$\rightsquigarrow$ $[k_i : k] = f_i < \infty$ **grado residuo** a $\mathfrak{P}_i$

Risulta

$$\sum_i e_i f_i = d$$

$$\mathcal{O}_L/\mathfrak{p} = \prod_{i=1}^{g} \underbrace{\mathcal{O}_L/\mathfrak{P}_i^{e_i}}$$

$$\left|\mathcal{O}_L/\mathfrak{P}_i^{e_i}\right| = \left|\mathcal{O}_L/\mathfrak{P}_i\right|^{e_i} = \left|\mathcal{O}_K/\mathfrak{p}\right|^{f_i e_i}$$

VALUTAZIONI SU K GLOBALE

① Archimedee

Ci sono $d = [K:\mathbb{Q}]$ immersioni $K \hookrightarrow \mathbb{C}$

$\sigma_1, \dots, \sigma_{r_1}, \tau_1, \dots, \tau_{r_2}, \bar{\tau}_1, \dots, \bar{\tau}_{r_2}$

Ognuna determina un v.a. arch. su K

$|x|_{\sigma_i} = |\sigma_i(x)|$

$|x|_{\tau_i} = |\tau_i(x)| = |\bar{\tau}_i(x)|$

dove $|\ |$ è il valore ass. su $\mathbb{C}$.

Sono tutte e sole le val. arch. su K.

② Non archimedee

$\mathfrak{P}$ primo di $\mathcal{O}_K$ $\rightsquigarrow$ $v_\mathfrak{P}$ val. discreta su K

$x \in K$ $\quad x\mathcal{O}_K = \prod_{\mathfrak{P}} \mathfrak{P}^{v_\mathfrak{P}(x)}$

↳ funzionano

Se $\mathfrak{P} \cap \mathbb{Z} = (p)$

$p\mathcal{O}_K = \mathfrak{P}^e \dots\dots$

$v_\mathfrak{P}(p) = e > 0$

$\mathfrak{P}$ una valutazione su K che estende la valutazione p-adica su $\mathbb{Q}$.

Normalizzandola opportunamente

$\left(v'_{\mathfrak{P}} = \frac{v_{\mathfrak{P}}}{e}\right)$ una v. ass. $|\ |_{\mathfrak{P}}$ che

estende a K il valore ass $|\ |_p$.

Ostrowski: Le $|\ |_{\mathfrak{P}}$ sono (a meno di eq.za).

tutti e soli i v. ass. n. arch. di K.

$M_K = \{$**posti** di $K\}$

$\hookrightarrow$ rappres. di valori ass. arch. e n.a.

$M_K^0 = \{$posti non archimedei$\}$

Completamenti

$v \in M_K$ una completamento K_v

$K_v = \mathbb{R}, \mathbb{C}$ se v archimedea

$=$ estensione finita di $\mathbb{Q}_p$ se v. non arch.

$$\begin{tikzcd}
 & K_v \arrow[d, dash, "d_v"] \\
K \arrow[ur, dash] \arrow[d, dash, "d"'] & \mathbb{Q}_p \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}$$

$\boxed{v \mid p}$

$v = v_{\mathfrak{P}} \qquad \mathfrak{P} \cap \mathbb{Z} = p$

$$d_v = [K_v : \mathbb{Q}_p] \leq d = [K : \mathbb{Q}]$$

$\mathcal{O}_K \hookrightarrow \mathcal{O}_v$ immersione densa

$\mathfrak{P}$ primo $\rightsquigarrow$ $|\ |_{\mathfrak{P}}$ $\rightsquigarrow$ immersione $K \to \bar{\mathbb{Q}}_p$

Viceversa diverse immersioni da $K \hookrightarrow \bar{\mathbb{Q}}$

possono determinare lo stesso primo

$$K \hookrightarrow \bar{\mathbb{Q}}_p \xrightarrow{\text{autom}} \bar{\mathbb{Q}}$$

Precisamente: ci sono esattamente $d_v = [K_v : \mathbb{Q}_p]$ $(v|p)$ immersioni $K \hookrightarrow \bar{\mathbb{Q}}_p$ che determinano lo stesso primo $\mathfrak{P}$ di K (e quindi lo stesso v. ass.). Quindi se $x \neq 0$

$$\prod_{v|p} |x|_v^{d_v} = \prod_{\sigma: K \hookrightarrow \bar{\mathbb{Q}}_p} |\sigma(x)|_{v_\sigma} = |N_{K/\mathbb{Q}}(x)|_p$$

$$\Big| \prod_{\sigma} \sigma(x) \Big|_p$$

$$\prod_{v \in M_K} |x|_v^{d_v} = \prod_{v \in M_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(x)|_p = 1$$

FORMULA DEL PRODOTTO: $\prod_{v \in M_K} |x|_v^{d_v} = 1$

Oss.

L/K estensioni di campi globali

$\mathfrak{p}$ primo di K $\quad \mathfrak{P}|\mathfrak{p}$ primo di $\mathcal{O}_L$

"Globale" $\quad \mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e \ldots\ldots$

$e = e(\mathfrak{P}|\mathfrak{p})$ indice di ramif.

$f = \left[\mathcal{O}/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p} \right]$ grado residuo.

"locale" completando

$L_\mathfrak{P}/K_\mathfrak{p}$ $\qquad \mathcal{O}_{L_\mathfrak{P}} \rightsquigarrow$ id max $\mathfrak{P}\mathcal{O}_{L_\mathfrak{P}}$

$\qquad \mathcal{O}_{K_\mathfrak{p}} \rightsquigarrow$ " $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$

$\downarrow$

l'indice di ramificazione e il grado residuo locale di queste estensione coincidono con quelli globali.

Supponiamo L/K Galois $\mathfrak{p}$ primo di $\mathcal{O}_K$

$Gal(L/K)$ agisce transitivamente su

$$\{\mathfrak{P} / \mathfrak{P} | \mathfrak{p}\}$$

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$

Applicando $Gal(L/K)$ vediamo che $e_i = e \ \forall i$

$f_i = f$

$\sum_i e_i f_i = d \rightsquigarrow gef = d$

$$\begin{tikzcd}
L \arrow[r, no head] \arrow[d, no head, "d"] & L_\mathfrak{P} \arrow[d, no head, "d_0 = ef"] & \\
K \arrow[r, no head] & K_\mathfrak{p} \arrow[r] & \text{galois}
\end{tikzcd}$$

$$\mathrm{Gal}\left(L_{\mathfrak{P}}/K_{\mathfrak{p}}\right) \xleftrightarrow{\mathrm{Res}} \mathrm{Gal}\left(L/K\right)$$