E/F galois $\xrightarrow{\text{Galois}}$ $\mathrm{Gal}\left(\frac{E}{F}\right) = \varprojlim \mathrm{Gal}\left(\frac{K_i}{F}\right)$

(K_i/F estensioni finite contenute in E)

→ gruppo profinito con topologia di Krull

Corrispondenza di Galois

$$\left\{\begin{array}{l}\text{estensioni}\\ F \subseteq K \subseteq E\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{sottogruppi}\\ \text{chiusi di } \mathrm{Gal}\left(\frac{E}{F}\right)\end{array}\right\}$$

$$K \longrightarrow \mathrm{Gal}\left(\frac{E}{K}\right)$$

$$E^H \longleftarrow H$$

$$\pi_i^j(x_j) = x_i \qquad \forall j > i$$

K campo di numeri (est. finita di $\mathbb{Q}$)

$\bar{K}$ chiusura alg.

$$\mathrm{Gal}\left(\frac{\bar{K}}{K}\right) = G_K$$

$$\overline{\langle \text{commutori} \rangle} = H$$

$$\mathrm{Gal}\left(\frac{\bar{K}}{K}\right) \Big/ H = \boxed{\mathrm{Gal}\left(\frac{\bar{K}}{K}\right)^{ab}} = \mathrm{Gal}\left(\frac{K^{ab}}{K}\right)$$

K^{ab} = composto di tutte le est. ab. di K

$K = \mathbb{Q}$

$\mathbb{Q}^{cyc} = \mathbb{Q}(\zeta_m \mid m \in \mathbb{N})$

$Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \xrightarrow{\sim} Gal(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times = \hat{\mathbb{Z}}^\times$ (Kronecker Weber).

Numeri p-adici e valutazioni

p primo

$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$

$x \in \mathbb{Q}^\times \quad x = p^n y \quad n \in \mathbb{Z} \quad y = \frac{a}{b} \quad p \nmid a, p \nmid b$

$v_p(x) = n$

$v_p(0) = \infty$

1) $v_p(x) = \infty \iff x = 0$
2) $v_p(ab) = v_p(a) + v_p(b)$
3) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

Fissato $x \in (0,1)$

$|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}$

$a \longmapsto x^{v_p(a)}$ (di solito si prende $x = \frac{1}{p}$)

$|\ |_p$ è una norma su $\mathbb{Q}$.

1) $|a|_p = 0 \iff a = 0$
2) $|ab|_p = |a|_p |b|_p$
3) $|a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b_p|$

↳ disuguaglianza ultrametrica

Norme "equivalenti" se def. la stessa topologia,
la topologia def da $|\ |_p$ non dipende da x
ma dipende da p.

$|\ |_\infty$ valore assoluto standard.

Teorema di Ostrowski

Ogni norma su $\mathbb{Q}$ è equivalente a $|\ |_\infty$ o a $|\ |_p$
per qualche p.

$|\ |_\infty$ archimedea
$|\ |_p$ non archimedee.

$M_{\mathbb{Q}} = \{$ insieme completo
di rappres delle classi di eq.za di
norme su $\mathbb{Q}\}$ POSTI DI $\mathbb{Q}$

$= \{p, \infty \mid p \text{ primo}\}$.

Se $|\cdot|_p = \frac{1}{p^{v_p(\cdot)}}$ allora vale la

FORMULA DEL PRODOTTO

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1 \quad \text{se} \quad x \neq 0$$

infatti se $a \in \mathbb{Q}$ $\quad a = \pm p_i^{n_i} \quad n_i \in \mathbb{Z}$

$|a|_{p_i} = p_i^{-n_i} \qquad |a|_\infty = p_i^{n_i}$ ☒

Norma ma metrica ma completamento

(X, d) spazio metrico

esiste $(\tilde{X}, \tilde{d})$ t.c. $\tilde{X} \supseteq X$ $\tilde{d}|_X = d$

$\tilde{X}$ completo (tutte le succ. di Cauchy convergono)

e X denso in $\tilde{X}$.

$\tilde{X}$ unico a meno di eq.za metrica

$\Rightarrow \tilde{X}$ **completamento** di X

$\mathbb{Q}_p$ = completamento di $\mathbb{Q}$ rispetto a $|\ |_p$

$\mathbb{Q}_p$ è un campo contenente $\mathbb{Q}$.

Gli elementi di $\mathbb{Q}_p$ si possono rappresentare come $\sum_{n \geq n_0} a_n p^n$ $\quad a_n \in \{0, \dots, p-1\}$

la valutazione v_p si estende per continuità a $\mathbb{Q}_p$: $\tilde{v}_p : \mathbb{Q}_p \longrightarrow \mathbb{Z}$

e $|a|_p = \frac{1}{p^{\tilde{v}_p(a)}}$ $\forall a \in \mathbb{Q}_p$.

ANELLO DEGLI INTERI P-ADICI

$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ aperto chiuso in $\mathbb{Q}_p$

$v_p(x) \geq 0$

> -1

sottoanello di $\mathbb{Q}_p$

$\mathbb{Z} \subseteq \mathbb{Z}_p$ ed è denso in $\mathbb{Z}_p$.

Infatti se $a \in \mathbb{Z}_p$, possiamo supporre $|a|_p = 1$

esiste una successione $(q_n)_n$ $q_n \in \mathbb{Q}$

$q_n \xrightarrow{p} a$ $\quad |q_n| = 1$ $\quad q_n = \frac{a_n}{b_n}$ $\quad p \nmid a_n$, $p \nmid b_n$

$\frac{a}{b}$ $\quad p^k$

$\exists c$ t.c. $v_p\left(\frac{a}{b} - c\right) \geq k$

$\forall n, \forall k \; \exists c_n \in \mathbb{Z}$ t.c. $|q_n - c_n| \leq \frac{1}{p^k}$

$c_n \to a$ $\quad c_n \in \mathbb{Z}$.

Ogni $x \in \mathbb{Q}_p^*$ $\quad x = p^n u$ $\quad (u \in \mathbb{Z}$ t.c. $v_p(u) = 0$

in particolare $x \in \mathbb{Z}_p \setminus \{0\}$ $\quad x = p^n u$ $\quad v_p(u) = 0$ e $n \geq 0$

$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p \mid v_p(x) = 0\}$

$(v_p(x^{-1}) = -v_p(x))$

$\mathbb{Z}_p$ ha un unico ideale massimale (p) e tutti gli ideali sono del tipo (p^n) $n \geq 0$

in particolare $\mathbb{Z}_p$ è un PID.

$\forall n \geq 0$ $\exists$ biezione

$$\frac{\mathbb{Z}}{p^n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \quad \text{(suriettiva per densità)}$$

$$\frac{\mathbb{Z}}{p^n\mathbb{Z}} \longleftarrow \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}$$

$$\mathbb{Z}_p \longrightarrow \frac{\mathbb{Z}}{p^n\mathbb{Z}} \quad \forall n$$

$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$

Fatto: è un isom.

Lemma di Hensel

$\mathbb{Z}_p \quad (p)$

$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ → campo residuo

$f(x) \in \mathbb{Z}_p[x]$

$a \in \mathbb{Z}_p$ t.c. $f(a) \equiv 0 \mod p$

e $f'(a) \not\equiv 0 \mod p$

Allora esiste $\tilde{a} \in \mathbb{Z}_p$ t.c. $f(\tilde{a}) = 0$ e $\tilde{a} \equiv a \ (p)$.

Dim

Costruiamo successione $a_n \in \mathbb{Z}_p$ t.c. $f(a_n) \equiv 0 \mod p^n$

e $a_n \equiv a_{n-1} \mod p^{n-1}$

$a_0 = a$

Costruito a_{n-1} cerchiamo $a_n = a_{n-1} + p^{n-1} u$

$$\underbrace{f(a_n) - f(a_{n-1})}_{\text{divisibile per } p^{n-1}} \equiv f'(a_{n-1}) p^{n-1} u \mod p^n$$

$$\frac{f(a_n) - f(a_{n-1})}{p^{n-1}} \equiv f'(a) u \mod p$$

Si determina u richiedendo $f'(a) \not\equiv 0 \mod p$.

$\tilde{a} = \lim a_n \qquad f(a_n) \equiv 0 \mod p^n$

$f(\tilde{a}) = 0$ in $\mathbb{Z}_p$ ∎

Applicazione

$\mu_{p-1} = \{ \alpha \in \overline{\mathbb{Q}}_p \mid \alpha^{p-1} = 1 \}$

$f(x) = X^{p-1} - 1 \qquad f'(x) = (p-1)X^{p-2}$

Ha tutte le radici in $\mathbb{F}_p^\times$

Ogni radice si solleva a una radice in $\mathbb{Z}_p$

$$\boxed{\mu_{p-1} \subseteq \mathbb{Z}_p}$$

K campo

$v: K \longrightarrow \mathbb{R} \cup \{\infty\}$

1) $v(0) = \infty$
2) $v(ab) = v(a) + v(b)$
3) $v(a+b) \geq \min\{v(a), v(b)\}$

una $|\ |_v$ valore ass. non archimedeo su K.

Teorema di approssimazione (generalizza il TCR)

$|\ |_1, \dots, |\ |_n$ valori ass. non eq.ti su K

$a_1, \dots a_n \in K$

$\forall \varepsilon \quad \exists x \in K$ t.c.

$|x - a_i|_i < \varepsilon$.

$\mathcal{O} = \{x \in K \mid v(a) \geq 0\}$ ANELLO DI VALUTAZIONE

$\mathcal{O}^\times = \{x \in K \mid v(a) = 0\}$

↳ locale con massimale

$\mathcal{P} = \{x \in K \mid v(a) > 0\}$

v discreta se $v(K^\times)$ sottogruppo discreto di $\mathbb{R}$

$v(K^\times) = s\mathbb{Z} \quad s>0$

v normalizzata se $s=1$.

Se v normalizzata esiste $\pi \in K$ t.c. $v(\pi)=1$

↳ UNIFORMIZZANTE di K.

Ogni $x \in K$ si scrive $x = \pi^n u \quad n \in \mathbb{Z} \quad u \in \mathcal{O}^\times$

Se v discreta $\mathcal{O}$ è PID

$\mathfrak{P} = (\pi)$

tutti gli ideali (NON NULLI) di $\mathcal{O}$ hanno la forma $(\pi^n) = \mathfrak{P}^n \quad n \geq 0$

$$\mathfrak{P}^n = \{ x \in \mathcal{O} \mid v(x) \geq n \}$$

$$\frac{\mathfrak{P}^n}{\mathfrak{P}^{n+1}} = \frac{\pi^n \mathcal{O}}{\pi^{n+1}\mathcal{O}} \simeq \frac{\mathcal{O}}{\pi \mathcal{O}} \xrightarrow{\sim} \mathcal{O}/\mathfrak{P}$$

CAMPO RESIDUO

$$\mathcal{O} \supseteq \underbrace{\mathfrak{P} \supseteq \mathfrak{P}^2 \supseteq \dots}_{\mathcal{O}/\mathfrak{P}}$$

$\mathcal{O}$ aperto e chiuso

$\mathfrak{P}^n = \pi^n \mathcal{O} \simeq \mathcal{O}$ aperti e chiusi

i $\mathfrak{P}^n$ sono una base di intorni aperti di 0 in K.

$\mathcal{O}^\times$

$$1 \longrightarrow 1+\mathfrak{P} \longrightarrow \mathcal{O}^\times \longrightarrow k^\times \longrightarrow 1$$

$\| ?$

$\mathfrak{P}$

Catena discendente

$$\underset{U^{(0)}}{\mathcal{O}^\times} \supseteq \underset{U^{(1)}}{1+\mathfrak{P}} \supseteq \underset{U^{(2)}}{1+\mathfrak{P}^2} \supseteq \dots$$

con $U^{(n)} = \{ \alpha \mid \alpha \equiv 1 \mod \mathfrak{p}^n \}$

$$\frac{U^{(0)}}{U^{(1)}} \simeq \left(\frac{\mathcal{O}}{\mathfrak{p}}\right)^{\times} \simeq k^{\times}$$

$$\frac{U^{(n)}}{U^{(n+1)}} \simeq \frac{1+\mathfrak{p}^n}{1+\mathfrak{p}^{n+1}} \simeq \frac{\mathfrak{p}^n}{\mathfrak{p}^{n+1}} \simeq k \quad \forall n \geq 1$$

Completamento rms $(\tilde{K}, \tilde{v})$ $\tilde{v}$ discreta $v(K) = \tilde{v}(\tilde{K})$.

$$\frac{\mathcal{O}}{\mathfrak{p}^n} \longrightarrow \frac{\tilde{\mathcal{O}}}{\tilde{\mathfrak{p}}^n} \qquad \forall n \geq 1$$

$k = \frac{\mathcal{O}}{\mathfrak{p}}$ campo residuo

Se π uniformizzante ogni elem. di $\tilde{K}$ si scrive come serie di Laurent

$$\sum_{n \geq n_0} a_n \pi^n \qquad a_n \in \{ \text{insieme di rappres. in } \tilde{\mathcal{O}} \text{ di } \tilde{\mathcal{O}}/\tilde{\mathfrak{p}} \}$$

$$\tilde{\mathcal{O}} = \varprojlim \frac{\mathcal{O}}{\mathfrak{p}^n} \qquad \tilde{\mathcal{O}}^{\times} = \varprojlim \frac{\mathcal{O}^{\times}}{U^{(n)}}$$

Lemma di Hensel

K completo rispetto a v

$f \in \mathcal{O}[x]$ primitivo (gcd coefficienti $= 1$)

e $f(x) = g(x) h(x) \mod \mathfrak{p}$ con $g(x), h(x)$ coprimi mod $\mathfrak{p}$.

Allora esistono $\tilde{g}(x), \tilde{h}(x) \in \mathcal{O}[x]$

con $f(x) = \tilde{g}(x) \tilde{h}(x)$

$\deg g = \deg \tilde{g}$, $\deg h = \deg \tilde{h}$

$g \equiv \tilde{g}$, $h \equiv \tilde{h} \mod \mathcal{P}$ $\quad \tilde{g}, \tilde{h}$ comuni.

K, v val discreto

K completo.

L/K estensione finita.

v si estende in modo unico a una valutazione su L.

Presumibilmente il valore assoluto su L risulta essere $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ $\quad [L:K] = n$