$$\phi_K : K^* \longrightarrow Gal\left(K^{ab}/K\right)$$

$\forall$ estensione finita L/K abeliana indice isom.

$$\phi_{L/K} : \frac{K^*}{N(L^*)} \longrightarrow Gal\left(L/K\right)$$

Sgp. di norme $\Leftrightarrow$ aperti di indice finito.

$$\underbrace{\langle \pi^m \rangle \cdot U_K^{(i)}}$$

$U_K^{(i)} = U_K$ se $i=0$
$= 1+\mathfrak{p}^i$ se $i>0$

Conduttore di L/K = $\min\{i \mid U_K^{(i)} \subseteq N_{L/K}(L^*)\}$

(1) se L/K n.r. $\Rightarrow$ $\text{cond}(L/K) = 0$

cioè $U_K \subseteq N(L^*)$.

Infatti $\phi_{L/K}(\pi) = \text{Frob}_{L/K}$, $\forall \pi$ unif. di K

$\Rightarrow \phi_{L/K}(U_K) = \text{id}$.

(2) Se $\text{cond}(L/K) = 0$

$K^* = \langle \pi \rangle \cdot U_K \leadsto N(L^*) = \langle \pi^m \rangle = N(L_1^*)$

dove L_1 è n.r. di grado m. $\Rightarrow L = L_1$.

(3) Si ha $\phi_{L/K}(U_K) = I_{L/K}$ infatti se

$L_0 = L^{\phi(U_K)}$, allora L_0 è la massima

sottoestensione di L/K t.c.

$U_K \subseteq \ker \phi_{L_0/K} = N(L_0^*) \Rightarrow L_0/K$ è la

max estensione n.r. di $L/K \leadsto L_0 = L^{nr}$

$\rightsquigarrow \Phi_{L/K}(U_K) = Gal(L/L^{nr}) = I(L/K)$

(4) Se $cond(L/K) = 1$

$U_K^{(1)} \subseteq N_{L/K}(L^\times)$.

$$\begin{tikzcd} U_K \arrow[r, "\Phi_{L/K}"] \arrow[d] & I_{L/K} \\ U_K/U_K^{(1)} \arrow[ur] & \end{tikzcd}$$

ordine coprimo con p $\Rightarrow p \nmid e \rightsquigarrow L/K$ tame ram.

(Viceversa se $cond(L/K) = i > 1$
la mappa $\Phi_{L/K}$ non fattorizza per $U_K/U_K^{(1)}$
$\rightsquigarrow I_{L/K}$ ha un p-sottogruppo non banale
$p \mid e \rightsquigarrow L/K$ wild.

$$K^\times = \langle \pi \rangle \cdot U_K$$

$$K^{ab} = \underset{\displaystyle K_\pi}{\overset{\shortparallel}{K^{ab,\langle \pi \rangle}}} \cdot \underbrace{K^{ab \cdot U_K}}_{\displaystyle \shortparallel \atop \displaystyle K^{nr}}$$

<u>Teorema di Lubin-Tate</u>: costruzione esplicita dei campi K_π.

Gruppo formale: serie di potenze $F(x,y)$
$F(x, F(y,z)) = F(F(x,y), z)$ . . .
$F(x,y) \in K[[x,y]]$.

$\rightsquigarrow$ $\forall \pi$ F_π gruppo formale

F_π $\rightsquigarrow$ valutare in $\mathfrak{M}_{\bar{K}}$ $\rightsquigarrow$ Γ_π gruppo

Azione di $\underbrace{Gal(\bar{K}/K) \text{ su } \Gamma_\pi}$

Γ_π^{tors} punti di torsione di Γ_π

$K(\Gamma_\pi^{tors}) = K_\pi$

$K_\pi \cdot K^{nr} = \boxed{K^{LT} \subseteq K^{ab}}$

$\uparrow$

non dipende da π.

Teorema di K.W. globale

non banali)

<u>Fatto</u> non ci sono estensioni di $\mathbb{Q}$ ovunque n.r.

<u>Teorema</u> (Hermite-Minkowski)

Se $K/\mathbb{Q}$ est. finita di grado n

$$\sqrt{\Delta_{K/\mathbb{Q}}} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$$

$$\Delta_{K/\mathbb{Q}} = 1 \implies n = 1 \rightsquigarrow K = \mathbb{Q}$$

Lemma

Se $L/\mathbb{Q}$ Galois finito,
$Gal(L/\mathbb{Q})$ è generato da $I_\mathfrak{P}$ mentre
al variare dei $\mathfrak{P}$ primi di K che ramificano.

Dim.

Sia $H = \langle I_\mathfrak{P} \mid \mathfrak{P}$ ramifica $\rangle$

L^H è non ram. ad ogni $\mathfrak{P}$ $\Rightarrow$ $L^H = \mathbb{Q}$. $\blacksquare$

Dim K.W.

$K/\mathbb{Q}$ abeliana.

$\forall \mathfrak{P}$ primo di K $\qquad \mathfrak{P} \mid p$

$Gal(K_\mathfrak{P}/\mathbb{Q}_p) \leq Gal(K/\mathbb{Q}) \Rightarrow K_\mathfrak{P}/\mathbb{Q}_p$ abeliana

$K_\mathfrak{P} \leq \mathbb{Q}_p(\mu_p, \nu_p)$ dove μ_p radice p^{s_p}-esima di 1, ν_p radice di ordine primo con p di 1.

dipendono solo da p
perché $Gal(K/\mathbb{Q})$ agisce trans. sui $\mathfrak{P} \mid p$.

Sia $K' = K(\mu_p,\ p$ ramifica in $K)$

$\Rightarrow K'$ abeliana. $\qquad L = \mathbb{Q}(\mu_p \mid p$ ramifica in $K)$

$$[K':\mathbb{Q}] \geq [L:\mathbb{Q}] = \prod_p \varphi(p^{s_p})$$

Siccome $K'/\mathbb{Q}$ ab. $\forall \mathfrak{P}$ di K' $I(\mathfrak{P})$ dipende solo da p. $K'_{\mathfrak{P}} \subseteq \underline{\mathbb{Q}_p(\mu_p, \nu_p)}$

$|I(\mathfrak{P})| \leq \varphi(p^{s_p})$

Per il lemma c'è una mappa suriettiva

$$\prod_{\mathfrak{P}\text{ ram.}} I(\mathfrak{P}) \longrightarrow Gal\left(K'/\mathbb{Q}\right)$$

Quindi $\left|Gal\left(K'/\mathbb{Q}\right)\right| \leq \prod_{\mathfrak{P}} |I(\mathfrak{P})| \leq \prod_p \varphi(p^{s_p})$

$$\left|Gal\left(K'/\mathbb{Q}\right)\right| = \prod_p \varphi(p^{s_p})$$

$K' = L$. $\blacksquare$

Coomologia dei gruppi (finiti)

G gruppo finito
M gruppo ab.

G-modulo M

$Hom_G(M,N) = \{$omo di G-mo.

$$\begin{aligned} G \times M &\longrightarrow M \\ (g, m) &\longmapsto m^g \end{aligned}$$ azione

$\forall g \quad \varphi_g : M \longrightarrow M$, $m \longmapsto m^g$ automorfismo

$\mathbb{Z}[G]$ algebra gruppo di G
$= \{ \sum_g m_g g \mid m_g \in \mathbb{Z} \}$

M G-modulo $\iff$ M $\mathbb{Z}[G]$-modulo
Mod_G categoria abeliana
$\mathrm{Hom}_{\mathbb{Z}}(M, N)$ ha strutt. di G-modulo
ponendo $\forall \varphi$ $\quad \varphi^g(m) = \varphi(m^{g^{-1}})^g$

Se $H \leq G$ e M è un H-modulo
$\mathrm{Ind}_H^G(M) = \{ \varphi : G \to M \mid \varphi(hg) = \varphi(g)^h \ \forall h \in H \}$
è un G-modulo con
$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$
$\varphi^g(x) = \varphi(xg)$
Un morfismo $\alpha : M \longrightarrow M'$ di H-moduli
induce un morfismo (composizione per α)
$$\mathrm{Ind}_H^G(M) \longrightarrow \mathrm{Ind}_H^G(M')$$
$$\varphi \longmapsto \alpha \circ \varphi.$$
$\mathrm{Ind}_H^G(M)$ modulo indotto di M da H a G.

Un G-modulo M si dice iniettivo se per ogni inclusione $A \hookrightarrow B$ di G-moduli e ogni morfismo $\phi : A \longrightarrow M$ esiste $\psi : B \longrightarrow M$ che estende ϕ

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, "\phi"'] & B \arrow[dl, dotted, "\psi"] \\ M & \end{tikzcd}$$

<u>Lemma</u>: La categoria dei G-moduli "ha abbastanza iniettivi" cioè ogni modulo si immerge in un modulo iniettivo..

In particolare ogni G-modulo ha una risoluzione iniettiva

$$0 \longrightarrow M \longrightarrow I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} \ldots \ldots$$

con I_i iniettivi $\forall i \geq 0$

esatta cioè $\ker d_i = \operatorname{im} d_{i-1}$ $\forall i > 1$.

$\forall$ G mod M consideriamo

$$M^G = \{ m \in M \mid m^g = m \}$$

G-invarianti di M.

$M \longmapsto M^G$ funtore

$\mathrm{Mod}_G \longrightarrow \mathrm{Ab.grp.}$

è esatto a sinistra ma non a destra
cioè se $0 \to M_1 \to M_2 \xrightarrow{\varphi} M_3 \to 0$
ses di G-moduli allora
$$0 \longrightarrow M_1^G \longrightarrow M_2^G \longrightarrow M_3^G$$
(non è detto che $\varphi : M_2^G \to M_3^G$ sia suriettiva)
Dato un G-mod M, e una sua risoluz. iniettiva, prendiamo
$$0 \to I_0^G \xrightarrow{d_0} I_1^G \xrightarrow{d_1} \cdots \longrightarrow I_n^G$$
è un complesso di G-moduli cioè
$$d_{i+1} \circ d_i = 0 \qquad \operatorname{im} d_i \subseteq \ker d_{i+1}$$
Poniamo
$$H^i(G, M) = \frac{\ker(d_{i+1})}{\operatorname{im}(d_i)}$$
i-esimo gruppo di coom. di M.

(per convenzione $d_{-1} : 0 \longrightarrow I_0^G$ è nulla)
$$H^0(G, M) = M^G.$$

Se $f : M \longrightarrow N$ è un morfismo di G-moduli e
$$0 \to N \to J_0 \to J_1 \to J_2 \cdots \quad \text{ris. iniettiva}$$
Si ottiene un diagramma commutativo

$$\begin{array}{ccccccc} 0 \to & M & \to & I_0 & \to & I_1 & \cdots \\ & \downarrow f & & \downarrow f_0 & & \downarrow f_1 & \\ 0 \to & N & \to & J_0 & \to & J_1 & \cdots \end{array}$$

prendendo i G. invarianti si ottiene morfismo
$H^i(f): H^i(G,M) \longrightarrow H^i(G,N)$.

Si può provare che $H^i(f)$ non dipende dalle risoluzioni scelte. (costruzione di omotopie).

<u>Proprietà fondamentale</u>

Data una ses di G. moduli

$$0 \to M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

esiste una l.e.s in coomologia

$$0 \longrightarrow H^0(G,M_1) \longrightarrow H^0(G,M_2) \cdots\cdots$$
$$\longrightarrow H^i(G,M_3) \xrightarrow{\delta} H^{i+1}(G,M_1) \to H^{i+1}(G,M_2)$$
$$\to H^{i+1}(G,M_3) \cdots\cdots$$

δ omomorfismi di connessione.

In particolare se $H^1(G,M_1)=0$ allora

$0 \to M_1^G \to M_2^G \longrightarrow M_3^G \to 0$ è esatto.

Più in generale se $H^i(G,M)=0$ $\forall i>0$ allora δ dà un isomorfismo

$$H^i(G,M_3) \underset{\sim}{\xrightarrow{\delta}} H^{i+1}(G,M_1) \quad \forall i>0$$

(~~surietiva~~ solo per $i=0$)

Questo può essere utilizzato per trasferire proprietà da H^i a H^{i+1} $\rightsquigarrow$ dimension shifting.

2) Se M è iniettivo ho come risol. iniettiva

$$0 \to M \to M \to 0 \quad \dots \rightsquigarrow H^i(G,M)=0 \quad \forall i>0.$$

3) Se $H^i(G,M)=0 \ \forall i>0 \rightsquigarrow M$ aciclico

iniettivo $\Rightarrow$ aciclico

Usando il dim. shifting si può provare che la coom. di M si può definire usando una risoluzione aciclica invece di una risoluzione iniettiva.

<u>Oss</u>

Se $H \leq G$ e M è H-modulo

$$\mathrm{Ind}_H^G M \simeq M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$$

$$\phi_{m,g} \rightsquigarrow m \otimes g$$

dove $\phi_{m,g}(g') = \begin{cases} m^{gg'} & \text{se } gg' \in H \\ 0 & \text{altrimenti} \end{cases}$

<u>Lemma di Shapiro</u>

Esiste un iso canonico

$$H^i(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H^i(H, M)$$

In particolare M aciclico $\iff$ $\mathrm{Ind}_H^G M$ aciclico.
(dim Kedlaya p. 36)