Oss.

$$\mathbb{I}_{\mathbb{Q}} \simeq \mathbb{Q}^* \, \mathbb{R}^*_{>0} \prod_p \mathbb{Z}_p^* = \mathbb{Q}^* \, \mathbb{R}^*_{>0} \, \hat{\mathbb{Z}}$$

infatti dato $\alpha = (\alpha_p)_p \in \mathbb{I}_{\mathbb{Q}}$

se $\lambda = \prod_p p^{v_p(\alpha_p)} \cdot sg(\alpha_\infty)$

allora

$$\lambda^{-1} \alpha \in \mathbb{R}^*_{>0} \cdot \prod_p \mathbb{Z}_p^*$$

Oss. vale solo per $K = \mathbb{Q}$.

Estensioni locali non ramificate

K campo locale $\mathcal{O}_K, \mathcal{P}_K, k$ finito.

$\bar{K}, \bar{k}$ chiusure algebriche di K, k risp

C'è una corrispondenza biunivoca

$$\left\{ \begin{array}{l} \text{estensioni finite} \\ \text{non ramificate di } K \\ \text{contenute in } \bar{K} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{estensioni finite} \\ \text{di } k \text{ in } \bar{k} \end{array} \right\}$$

$$L/K \longmapsto k_L/k$$

L'inversa si ottiene considerando k'/k, $k' = k(\alpha)$

$f(x)$ pol. minimo di α su k, $\tilde{f}(x)$ solleviamo

a un polinomio monico in $K[x]$, $\tilde{\alpha}$ radice. $L = K(\tilde{\alpha})$

Hensel mostra che L dipende solo da k'.

Si ha $[L:K] = [k_L : k]$

In particolare ogni L/K non ramificato è di Galois ($\sigma(L) = L$ $\forall \sigma$ K-immersione) e la mappa
$$\mathrm{Gal}\left(L/K\right) \longrightarrow \mathrm{Gal}\left(k_L/k\right) \text{ è un isomorfismo}$$
Se $|k| = q$ sappiamo che $\mathrm{Gal}\left(k_L/k\right)$ è ciclico generato da Frobenius: $\alpha \longmapsto \alpha^q$. Poniamo $\mathrm{Frob}_K \in \mathrm{Gal}\left(L/K\right)$ la controimmagine di Frobenius.
$$\mathrm{Frob}_K(\alpha) \equiv \alpha^q \mod \mathfrak{P}_L \quad \forall \alpha \in L.$$
Sia K^{nr} la massima estensione n.r. di K in $\overline{K}$ la valutazione $v: K \longrightarrow \mathbb{Z}$ si estende a una valutazione discreta di $K^{nr} \longrightarrow \mathbb{Z}$.

Quindi K^{nr} è un campo a val. discreta.

Il campo residuo è $\overline{k}$ (infinito)

K^{nr}/K è Galois e $\mathrm{Gal}\left(K^{nr}/K\right) \simeq \mathrm{Gal}\left(\overline{k}/k\right) \simeq \hat{\mathbb{Z}}$. (procicliclo)

L'elemento $\mathrm{Frob}_K \in \mathrm{Gal}\left(K^{nr}/K\right)$ che solleva il Frob su $\overline{k}$ è un generatore topologico di $\mathrm{Gal}\left(K^{nr}/K\right)$.

Sia ora K globale, L/K Galois n.r. a $\mathfrak{p}$ primo di K
$\forall \mathfrak{P} | \mathfrak{p}$ $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ è non ramificato, $\mathrm{Gal}\left(L_{\mathfrak{P}}/K_{\mathfrak{p}}\right) = \langle \mathrm{Frob}_{\mathfrak{P}} \rangle$

Se $\mathfrak{P}_1, \mathfrak{P}_2 | \mathfrak{p}$, $\mathrm{Frob}_{\mathfrak{P}_1}$ e $\mathrm{Frob}_{\mathfrak{P}_2}$ sono coniugati

Proprietà delle estensioni abeliane

Se L/K abeliana Galois (globale), $\mathfrak{p}$ primo di K, $\mathfrak{P}$ primo di L

$\mathfrak{P} | \mathfrak{p}$ e $G_{\mathfrak{P}}$ gruppo di decomposizione e $\mathfrak{P}$, $I_{\mathfrak{P}} \leq G_{\mathfrak{P}}$ inerzia

$G_{\mathfrak{P}} = \{ \sigma \in Gal(L/K) \,/\, \sigma(\mathfrak{P}) \subseteq \mathfrak{P} \}$

Se $\mathfrak{P}'$ è un altro primo sopra a $\mathfrak{p}$, $\exists \sigma$ t.c. $\sigma(\mathfrak{P}') = \mathfrak{P}$

$G_{\mathfrak{P}'} = \sigma^{-1} G_{\mathfrak{P}} \sigma \Rightarrow$ i gruppi di decomposizione sono coniugati.

Se L/K abeliana $\Rightarrow G_{\mathfrak{P}'} = G_{\mathfrak{P}}$, $I_{\mathfrak{P}'} = I_{\mathfrak{P}}$, $Frob_{\mathfrak{P}'} = Frob_{\mathfrak{P}}$

dipendono solo dal primo $\mathfrak{p}$; possiamo scrivere

$Frob_{\mathfrak{p}}$, ...

Decomposizione degli ideali primi nei campi ciclotomici

m intero, ζ radice primitiva m-esima di 1.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$

$\mathcal{O}_K = \mathbb{Z}[\zeta]$

p ramifica in $K \iff p \mid m$

In part. se $m = p^n$ allora p ramifica totalmente in K: c'è un unico primo $\mathfrak{P}$ sopra a p con $e = \varphi(p^n)$

Il polinomio minimo di ζ su $\mathbb{Q}$ è

$$\frac{X^{p^n}-1}{X^{p^{n-1}}-1} = X^{p^{n-1}(p-1)} + \dots + X^{p^{n-1}} + 1 = \varphi(x)$$

si ha $\varphi(1) = p = \prod_{(p \nmid k)} (1-\zeta^k) \rightsquigarrow p\mathcal{O}_K = (1-\zeta)$

e $N(1-\zeta) = p$.

• se $q \nmid m$ allora $\varphi(m) = g f$ dove f è il periodo di q in $\mathbb{Z}/m^\times$.

(Per vederlo si osserva che se Q primo sopra a q allora $K_Q/\mathbb{Q}_q \rightsquigarrow \mathbb{F}/\mathbb{F}_q$ con $\mathbb{F} = \mathbb{F}_q(\zeta)$ e $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) = \langle x \mapsto x^q \rangle$

In particolare $\mathrm{Frob}_Q(\zeta) = \zeta^q \quad \forall Q \mid q$. $q \nmid m$.

La legge di reciprocità quadratica.

Sia $K = \mathbb{Q}(\zeta)$ ζ radice primitiva q-esima di 1

$Gal\left(K/\mathbb{Q}\right) \simeq \mathbb{F}_q^*$ ciclico di ordine $q-1$, (pari)

Quindi $\exists!\ H \leq Gal\left(K/\mathbb{Q}\right)$ t.c. $[\mathbb{F}_q^* : H] = 2$

$H = \mathbb{F}_q^{*,2}$.

Galois $\leadsto$ K contiene un unico campo quadratico F.

$Disc(K) = q^{q-2}$ $\leadsto$ q è l'unico primo che ramifica in K $\leadsto$ $F = \mathbb{Q}(\sqrt{q})$ o $F = \mathbb{Q}(\sqrt{-q})$

Se $q \equiv 1 \mod 4$ $\leadsto$ $F = \mathbb{Q}(\sqrt{q})$

Se $q \equiv 2,3 \mod 4$ $\leadsto$ $F = \mathbb{Q}(\sqrt{-q})$

Posto $q^* = (-1)^{\frac{q-1}{2}}$ si ha $F = \mathbb{Q}(\sqrt{q^*})$.

Ora sia p primo $p \neq q$.

Oss. $\mathbb{Q}_p(\zeta)$ ha ordine p $\overset{(P)}{\equiv} 1 \mod q$ è non ramificato

Sia $\sigma \in Gal\left(K/\mathbb{Q}\right)$ il Frobenius a p, è:

$\sigma|_F$ è il Frobenius su F; è

- banale se $\sigma \in H = \mathbb{F}_q^{*,2}$ cioè se $\left(\sigma(\zeta) = \zeta^p\right)$ p è un quadrato in F

Quindi identificando $Gal\left(K/\mathbb{Q}\right)$ a $\{\pm 1\}$

Si ha $\sigma|_F = \left(\frac{p}{q}\right)$ (vedendo σ come la restrizione di Frob)

D'altra parte vedendo σ come il $Frob_p$ di un'est. quadr.

si ha $\mathfrak{P}$ banale se p si decompone in K quindi

se $(K_{\mathfrak{P}} : \mathbb{Q}_p) = 1 \quad \forall \mathfrak{P} | p \iff \left(\frac{q^*}{p}\right) = 1$.

Da cui

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

(argom. analogo nel caso $q = 2$)

Quindi (LQR si può vedere come l'affermazione che) l'insieme dei primi che spaccano in $\mathbb{Q}(\sqrt{q^*})$ è descritto in termine di una congruenza mod q.

Ora supponiamo per un attimo il teorema di K.W

sia $K/\mathbb{Q}$ un'estensione abeliana

Chiamiamo conduttore di $K/\mathbb{Q}$ il minimo m t.c.

$K \subseteq \mathbb{Q}(\zeta_m)$

Quindi c'è omom. suriettivo

$$\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \simeq Gal\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right) \longrightarrow Gal\left(K/\mathbb{Q}\right)$$

se $p \nmid m$ $\quad K/\mathbb{Q}$ è n.r. a p.

Sia G_p il gruppo di decomposizione (I_p banale)

$G_p = \langle \mathrm{Frob}_p \rangle$ t.c. $\mathrm{Frob}_p(x) \equiv x^p \mod \mathfrak{P} \ \forall \mathfrak{P} | p.$,

Mappa di Artin

Sia S_m il sottogruppo di $\mathbb{Q}^*$ generato dai primi che non dividono m, e definiamo mappa

$$\begin{array}{ccc} S_m & \longrightarrow & Gal\left(K/\mathbb{Q}\right) \\ p & \longmapsto & \mathrm{Frob}_p \end{array}$$

Il punto importante è esiste un diagramma commutativo

$$\begin{tikzcd} S_m \arrow[r] \arrow[d] & Gal\left(K/\mathbb{Q}\right) \\ \left(\mathbb{Z}/m\mathbb{Z}\right)^* \arrow[ur] & \end{tikzcd}$$

La mappa di Artin può essere formulata idelica-mente:

$$\psi_{K/\mathbb{Q}} : \ \mathbb{Q}^* \backslash \overline{\prod} \mathbb{Q} \longrightarrow Gal\left(K/\mathbb{Q}\right)$$

$$(1 \ldots \mathfrak{P} \ldots) \dashrightarrow \ \prod \mathrm{Frob}_p^{v(\mathfrak{P}_p)}$$

posso sempre modificare un idèle di $\mathbb{Q}$ per un (unico) elemento di $\mathbb{Q}^*$ in modo che abbia com-ponenti invertibili ai posti che dividono m

Si ha $\ker \psi_{K/\mathbb{Q}} = \mathbb{R}^*_{>0} \times U$ U sgp aperto di $\hat{\mathbb{Z}}^*$ contenente $1 + m\hat{\mathbb{Z}}$

Quindi p spacca in $K/\mathbb{Q} \iff \mathrm{Frob}_p = 1$
$\iff (1 \dots 1\ p \dots 1) \in \ker \psi_{K/\mathbb{Q}} \iff$ c'è una congruenza modulo U.

La legge di reciprocità di Artin asserisce che un fenomeno simile avviene per ogni estensione abeliana L/K, cioè che $\mathrm{Gal}(L/K)$ è un quoziente di $\mathbb{I}_{K}$ e quindi che $\exists$ mappa di Artin

$$\psi_K : \mathbb{I}_K / K^* \longrightarrow \mathrm{Gal}\left(K^{ab}/K\right)$$

In particolare l'insieme dei primi che spaccano completamente in $\mathrm{Gal}\left(L/K\right)$ (L abeliana) è descritto mediante il ker di

$\psi_{L/K}$ (sottogruppo di C_K)
quindi "essenzialmente" una congruenza.

La mappa di Artin risulterà essere il prodotto sui $v \in M_K$ di mappe di Artin locali.