§1

Lemma 1 Sia G un gruppo finito di ordine n.
$H^q(G,A) \xrightarrow{n} H^q(G,A)$ è la mappa 0 $\forall q>0$

Dim $\{e\} \leq G$ ha indice n

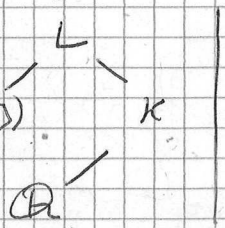
$$H^q(G,A) \xrightarrow{\text{Res}} H^q(\{e\},A) \xrightarrow{\text{cor}} H^q(G,A)$$
$$\overset{0}{\rightarrow} \qquad\qquad [G:\{e\}]=n$$

Cor Sia A finito, $(|G|,|A|)=1$. Allora $H^k(G,A)=0 \ \forall k>0$

Dim Per Bézout $\exists a,b \in \mathbb{Z}$: $a|A| + b|G| = 1$
WLOG $a<0$
La molt. per $|A|$ è 0 (perché annulla tutto in A)
La molt. per $a|A|$ è $\left(\underbrace{-a}_{>0}[\cdot 1]\,|A|\right.$, che è$\left.\right)$ 0
↑ Non serve!
La molt. per $|G|$ è 0 per il lemma prec.
Allora Id = molt. per 1 = molt. per 0 + molt. per 0 = mappa 0
$\Rightarrow H^k(G,A)=0$

---

§2 Setting: $E/\mathbb{Q}$, K, N come al solito, p di buona riduzione
Assumiamo $\text{disc}(K/\mathbb{Q})$ coprima con Np
e $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq GL_2(\mathbb{F}_n)$ via l'azione su $E[n]$ per permutazioni.



$L := K(E[n])$
$L/\mathbb{Q}$ Galois perché composto di Galois

L'ipotesi $(\text{disc}(L/K), Np)=1$ dice $\mathbb{Q}(E[n]) \cap K = \mathbb{Q}$
perché in ~~$\mathbb{Q}(E[n])/\mathbb{Q}$~~ c'è ~~almeno~~ un primo ~~ramificato~~,

- In $\mathbb{Q}(E[n])/\mathbb{Q}$ ramificano al più n e i primi di cattiva riduzione, che dividono N
- In $K/\mathbb{Q}$ nessuno di essi ramifica

Se $K \cap \mathbb{Q}(E[n]) \neq \mathbb{Q}$, avrebbe un primo ramificato, che ramificherebbe in entrambi.

Quindi la restrizione a $\mathbb{Q}(E[\pi])$: $Gal(L/K) \longrightarrow Gal(\mathbb{Q}(E[\pi])/\mathbb{Q})$ è un isomorfismo

Prop 1 $H^1(G_K, E[\pi]) \xrightarrow{Res} H^1(G_L, E[\pi])^{G_K} = Hom_{G_K}(G_L, E[\pi])$ è un isomorfismo di $G_{\mathbb{Q}}$-moduli

Dim Successione esatta di inflazione-restrizione:

$$0 \to H^1(Gal(L/K), E[\pi]) \xrightarrow{Inf} H^1(G_K, E[\pi]) \xrightarrow{Res} H^1(G_L, E[\pi])^{G_K} \to$$

$$\to H^2(Gal(L/K), E[\pi])$$

Oss A priori sarebbe solo di G_K-moduli, ma è di $G_{\mathbb{Q}}$-moduli perché $G_{\mathbb{Q}}$ agisce su G_K per coniugio e l'azione manda G_L in sé perché $L/\mathbb{Q}$ è Galois.

Oss La successione è quella perché $E[\pi]$ è fissato da G_L

In $Gal(L/K) =: \mathcal{G}$ c'è il sottogruppo dei multipli dell'identità, che è normale e isomorfo a $\mathbb{F}_\pi^*$

Ho un'altra successione di inflazione e restrizione

$$0 \to H^1(\mathcal{G}/\mathbb{F}_\pi^*, E[\pi]^{\mathbb{F}_\pi^*}) \to H^1(\mathcal{G}, E[\pi]) \to H^1(\mathbb{F}_\pi^*, E[\pi]) \to$$

$$\to H^2(\mathcal{G}/\mathbb{F}_\pi^*, E[\pi]^{\mathbb{F}_\pi^*})$$

Ora, $E[\pi]^{\mathbb{F}_\pi^*} = \{0\}$, $H^q(\mathbb{F}_\pi^*, E[\pi]) = 0$ $\forall q \geq 0$ per il corollario

In particolare, possiamo fare inflazione-restrizione anche in grado più alto proprio perché questi H^q sono 0, cioè abbiamo anche successioni esatte

$$0 \to H^{q+1}(\mathcal{G}/\mathbb{F}_\pi^*, E[\pi]^{\mathbb{F}_\pi^*}) \to H^{q+1}(\mathcal{G}, E[\pi]) \to H^{q+1}(\mathbb{F}_\pi^*, E[\pi])$$

che ci dicono $H^k(\mathcal{G}, E[\pi]) = 0$ $\forall k \geq 1$

Allora la prima successione inf-res dà la tesi.

Nel seguito ci farà comodo ricordare esplicitamente l'azione sui cocicli:

G profinito, $H \trianglelefteq G$ normale aperto di indice finito

↑ cioè G vi agisce legalmente per coniugio

A G-modulo discreto

$\varphi \in H^1(H, A)$, $\sigma \in G$

$(\sigma \cdot \varphi)(h) = \sigma \cdot \varphi(\sigma^{-1} \cdot h) = \sigma \varphi(\sigma^{-1} h \sigma)$

(azione in A ; azione in H)

Questo isomorfismo, che chiamiamo Ξ, dà un accoppiamento

$$[\ ,\ ] : H^1(G_K, E[\pi]) \times G_L \longrightarrow E[\pi]$$

$$(\varphi \ , \ g] \longmapsto \Xi(\varphi)(g) = \varphi(g)$$

(Ξ è la restrizione...)

E' non-degenere a sinistra nel seguente senso:
se $\forall g \in G_L \quad [\varphi, g] = 0$ allora $\varphi = 0$

Inoltre, soddisfa $\forall \sigma \in G_{\mathbb{Q}}$

$$[\sigma \cdot \varphi, g] = \sigma \cdot [\varphi, \sigma^{-1} \cdot g] = \sigma [\varphi, \sigma^{-1} g \sigma]$$

Inoltre, se $\sigma \in G_K$,

$[\sigma \cdot \varphi, g] = [\varphi, g]$ perché $\Xi(\varphi) \in \mathrm{Hom}(G_L, E[\pi])^{G_K}$

e quindi

$$\sigma [\varphi, g) = \sigma [\varphi, \sigma^{-1} \cdot \sigma \cdot g] = [\sigma \cdot \varphi) \sigma \cdot g] = [\varphi, \sigma \cdot g]$$

~~Proposizione 2~~

Def Se $S < H^1(G_K, E[\pi]) = \mathrm{Hom}(G_L, E[\pi])^{G_K}$ ed è finito

(azione di G_K banale)

quindi S è un sotto-G_K-modulo in realtà

$$G_S := \{ \varphi \in G_L \mid \forall s \in S \quad [s, \varphi] = 0 \}$$

Oss $G_S \trianglelefteq G_L$. Inoltre, se S è un sotto-$G_{\mathbb{Q}}$-modulo di $H^1(G_K, E[\pi])$ allora G_S è un sotto-$G_{\mathbb{Q}}$-modulo di G_L stabile per azione di $G_{\mathbb{Q}}$

Dim $\forall s \in S \ [s, \varphi] = 0 \iff \forall s \in S \ \forall \sigma \in \left\langle G_L, G_{\mathbb{Q}} \right\rangle \ [\sigma \cdot s, \varphi] = 0$

Però $0 = [\sigma \cdot s, \varphi] = \sigma [s, \sigma^{-1} \cdot \varphi] \Rightarrow [s, \sigma^{-1} \varphi] = 0$

Quindi otteniamo $\sigma^{-1} \varphi \in G_S$

Ma avevo il $\forall s$, quindi $\square$

Oss Il pairing indotto $[\cdot,\cdot] : S \times G_L/G_S \longrightarrow E[n]$ è non-degenere

Dim A sinistra: ovvio

A destra: se $\forall s \in S \ [s,\sigma] = 0$ allora $\sigma \in G_S$

Def L_S è il campo fisso di G_S

Oss L_S/L è di Galois con gruppo $G_L/G_S =: H$

Se inoltre S è un ~~sotto $G_{\mathbb{Q}}$-modulo di G_K~~ stabile per azione di $G_{\mathbb{Q}}$ allora

$L_S/\mathbb{Q}$ è di Galois

Dim Sia $\sigma : L_S \hookrightarrow \bar{\mathbb{Q}}$ che fissa $\mathbb{Q}$

$L/\mathbb{Q}$ è normale, quindi

$$\begin{array}{ccc} L_S & \xrightarrow{\sigma} & \sigma(L_S) \\ | H & & | \ \sigma H \sigma^{-1} \\ L & \longrightarrow & L = \sigma(L) \\ | & & | \\ \mathbb{Q} & \longrightarrow & \mathbb{Q} = \sigma(\mathbb{Q}) \end{array}$$

Ma so che H è stabile per azione di $G_{\mathbb{Q}}$, quindi

$\sigma H \sigma^{-1} = H$ e $\sigma(L_S) = L_S$

Proposizione 2 Il pairing indotto $[\cdot,\cdot]$ dà isomorfismi

$$H \xrightarrow{\sim} \mathrm{Hom}(S, E[n])$$
$$S \xrightarrow{\sim} \mathrm{Hom}_{G_K}(H, E[n])$$

che sono di G_K-moduli.

Se inoltre S è un sotto-$G_{\mathbb{Q}}$-modulo di $H^\vee$ sono di $G_{\mathbb{Q}}$-moduli

Dim Che ci siano $\hookrightarrow$ di gruppi abeliani e loro non-degenerità di $[\cdot,\cdot]$.

Vediamo che quelle mappe commutano con l'azione di $G_{\mathbb{Q}}$ (quindi, in particolare, se S è stabile per azione di G_K sono mappe di G_K-moduli e se è stabile per azione di $G_{\mathbb{Q}}$ sono mappe di $G_{\mathbb{Q}}$-moduli)

$$h \longmapsto \varphi_h : s \longmapsto [s,h]$$

$$(\sigma \cdot \varphi_h)(s) \overset{\text{azione su Hom}}{=} \sigma[\sigma^{-1}s, h] = \sigma\sigma^{-1}[s, \sigma h] = \varphi_{\sigma h}(s)$$

$$(\sigma \cdot \varphi_h)(s) = \sigma \varphi_h(\sigma^{-1} \cdot s)$$

$$s \longmapsto \varphi_s : h \longmapsto [s, h]$$

$$(\sigma \cdot \varphi_s)(h) = \sigma\, \varphi_s(\sigma^{-1} \cdot h) = \sigma [s, \sigma^{-1} h] = [\sigma s, h] = \varphi_{\sigma s}(h)$$

Ora, $E[\pi]$ è un G_K-modulo semplice (G_K agisce in modo transitivo su $E[\pi] - \{0\}$, appena ha un elemento non banale il sotto-G_K-modulo generato è tutto $E[\pi]$)

$S \hookrightarrow \mathrm{Hom}(H, E[\pi])$, quindi è un $\mathbb{F}_\pi$-spazio vettoriale.
Inoltre, $S \subseteq H^1(G_K, E[\pi]) \simeq H^1(G_L, E[\pi]) = \mathrm{Hom}_{G_K}(G_L, E[\pi])$
che ha azione di G_K banale
Con $\mathbb{F}_\pi$ intendo anche che la struttura di modulo di Galois è banale.
S finito, quindi $S = \mathbb{F}_\pi^r$ (G_K-moduli)

Tutto annullato dalla molt. per π ($\mathrm{Hom}_{\mathbb{Z}} = \mathrm{Hom}_{\mathbb{F}_\pi}$)

perché l'azione su $\mathbb{F}_\pi$ è banale e allora l'azione su Hom è solo in arrivo

$$\mathrm{Hom}(S, E[\pi]) \simeq \mathrm{Hom}(\mathbb{F}_\pi^r, E[\pi]) = \mathrm{Hom}_{\mathbb{F}_\pi}(\mathbb{F}_\pi^r, E[\pi]) \simeq E[\pi]^r$$

(tutti isomorfismi di G_K-moduli). $H \hookrightarrow E[\pi]^r \Rightarrow (H = E[\pi]^s$ perché $E[\pi]^r$ semisemplice, $s \le r$

Allora $S \hookrightarrow \mathrm{Hom}_{G_K}(E[\pi]^s, E[\pi]) = \mathrm{Hom}_{G_K}(E[\pi], E[\pi])^s$

Però $\mathrm{Hom}_{G_K}(E[\pi], E[\pi]) = \mathbb{F}_\pi$ perché

- $\mathrm{Hom}_{G_K}(\cdots) = \mathrm{Hom}(\cdots)^{G_K}$ ha G_K-azione banale
- Tutti gli unici elementi del G-L che commutano con tutto il G-L sono i multipli dell'identità.

Resta $S \hookrightarrow \mathrm{Hom}(H, E[\pi]) \simeq \mathrm{Hom}$ (G_K-moduli)

$E[\pi]^r = S \hookrightarrow E \quad \mathbb{F}_\pi^r = S \hookrightarrow \mathbb{F}_\pi^s \Rightarrow s \le r \Rightarrow s = r \Rightarrow \square$

3: Applichiamo a $Sel_\pi(E/\chi)$

Poniamo $S = Sel_\pi(E/\chi)$.
Verifichiamo che è un sotto-$G_{\mathbb{Q}}$-modulo di $H^1(G_K, E[\pi])$
Fatto questo, denotiamo $M := L_S$ e abbiamo $M/\mathbb{Q}$ Galois

$$0 \to \frac{E(K)}{\pi E(K)} \to H^1(G_K, E[\pi]) \to H^1(G_K, E)[\pi] \to 0$$

$$0 \to \prod_{v \in S(E)} \frac{E(K_v)}{\pi E(K_v)} \to \prod_{v \in S(E)} H^1(G_{K_v}, E[\pi]) \to \prod_{v \in G_K} H^1(G_{K_v}, E)[\pi] \to 0$$

Se dico che è di $G_{\mathbb{Q}}$-moduli sono a posto.

$Sel_n(E/K)$ è un sotto-G_K-modulo di $H^1(G_K, E[n])$?

$$\begin{array}{ccc} E(K)/nE(K) & \longrightarrow & H^1(G_K, E[n]) \\ \downarrow & & \downarrow \text{Res} \\ E(K_\mathfrak{P})/nE(K_\mathfrak{P}) & \longrightarrow & H^1(G_{K_\mathfrak{P}}, E[n]) \end{array}$$

Dico che, dopo aver agito con $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$

$$\begin{array}{ccc} E(K)/nE(K) & \longrightarrow & H^1(G_K, E[n]) \\ x & \longmapsto & \varphi_x : g \to \varphi_x(g) \\ \sigma \cdot x & \longmapsto & g \to \sigma(\varphi_x(\sigma^{-1} g \sigma)) \end{array}$$

La restrizione di $\sigma \cdot \varphi_x$ a $\sigma G_{K_\mathfrak{P}} \sigma^{-1} = G_{K_{\sigma(\mathfrak{P})}}$

sta ancora nell'immagine della mappa di bordo?

$$\begin{array}{ccc} E(K) & \longrightarrow & H^1(G_K, E[n]) \\ \sigma \cdot x \mapsto & & \sigma \cdot \varphi_x \\ \downarrow \sigma \cdot x & & \downarrow \text{Res} \\ E(K_{\sigma(\mathfrak{P})}) & \longrightarrow & H^1(G_{K_{\sigma(\mathfrak{P})}}, E[n]) \end{array}$$

$$(\sigma \cdot \varphi_x)(\underbrace{\sigma g \sigma^{-1}}_{\in G_{K_{\sigma(\mathfrak{P})}}}) = \sigma \cdot \varphi_x(\sigma) \in E[n]$$

$\sigma \cdot x$ dove va via la mappa di bordo?

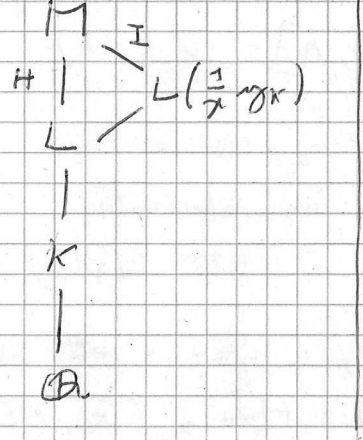
Sia sopra che sotto la mappa di bordo è, fissato un qualunque $\frac{1}{n}x$, $g \to \sigma(\frac{1}{n}x) - \frac{1}{n}x$

sia sopra $(\forall g \in G_K)$ che sotto $(\forall g \in G_{K_{\sigma(\mathfrak{P})}})$

Quindi il diagramma commuta (quel che ho fatto è correggere il disegno sotto)

Ma $G_{\mathbb{Q}}$ agisce transitivamente sui $\mathfrak{P}$ sopra uno stesso primo di $\mathbb{Q}$, quindi visto che la condizione di stare nell'immagine del bordo sotto per tutti i places continua ad averla anche dopo aver agito con σ, quindi è un sottogruppo sotto-$G_{\mathbb{Q}}$-modulo

Com'è fatta $M/\mathbb{Q}$? y_K punto di Heegner. Scelgo $\frac{1}{p} y_K$



$y_K \in E(K)$, $L(\frac{1}{p} y_K)/L$ è di Galois perché ha tutti gli $x \in E$: $p^x = y_K$ in quanto $E(L) \supseteq E[p]$

La mappa di bordo della succ. di Kummer

$$y_K \longmapsto \varphi_{y_K} \in Sel_p(E/K)$$

$$G_K \ni \sigma \longmapsto \sigma\left(\frac{1}{p} y_K\right) - \frac{1}{p} y_K \in E[p]$$

Assumiamo che p non divida y_K in $E(K)$, in modo che $y_K \not\mapsto 0$ in $Sel_p(E/K)$

Abbiamo $H \xrightarrow{\sim} Hom(\Sigma, E[p])$ iso di $G_{\mathbb{Q}}$-moduli dato da $[,]$

Considero la valutazione $Hom(\Sigma, E[p]) \xrightarrow{ev_{y_K}} E[p]$

È un omomorfismo di $G_{\mathbb{Q}}$-moduli, chiamo Σ il suo kernel.

Questo dà $H/I \hookrightarrow E[p]$ come $G_{\mathbb{Q}}$-moduli.

Diamo una caratterizzazione più esplicita di I

$\sigma \in I \iff \sigma\left(\frac{1}{p} y_K\right) - \frac{1}{p} y_K = 0 \iff \sigma$ fissa $\frac{1}{p} y_K$

Tra l'altro, questo dice $L(\frac{1}{p} y_K) \subseteq M$ ed è il sottocampo fissato da I, che è essere normale su L perché $I \trianglelefteq H$

(in realtà, I è un sotto-$G_{\mathbb{Q}}$-modulo di H, quindi $L(\frac{1}{p} y_K)/\mathbb{Q}$ è ancora Galois).

L'ipotesi $y_K \not\mapsto 0$ garantisce che I non sia tutto (cioè $= H$) quindi $H/\Sigma \neq \{0\}$ quindi, poiché $E[p]$ è un $G_{\mathbb{Q}}$-modulo semplice, $H/I \simeq E[p]$ via valutazione nella classe di y_K nel Selmer.

Proposizione Lemma Sia $\tau \in Gal(M/\mathbb{Q})$ una scelta di coniugio complesso. $\{(\tau h)^2 \mid h \in H\}$ coincide con $H^+ := \{h \in H \mid \tau h \tau^{-1} = h\}$ (autospazio di autovalore 1 di τ)

$I^+ := \{j \in \Sigma \mid \tau j \tau^{-1} = j\}$ coincide con $\{(\tau j)^2 \mid j \in I\}$

e $H^+/I^+ \simeq$ ($\mathbb{F}_p$ spazio vettoriale) come gruppi abeliani

Dim H è un p-gruppo con $p \neq 2$ $\Rightarrow$ elevare al quadrato è iso (o moltiplicare per 2, in notazione additiva)

Se $h \in H^+$, sia $g \in H \mid g^2 = h$ $(\exists!)$

$(\tau g)(\tau g) = (\tau g \tau) g \in H$

H abeliano

$(\tau g \tau g)^2 = (\tau g \tau) g (\tau g \tau) g \overset{\Downarrow}{=} (\tau g \tau)^2 g^2 = (\tau g^2 \tau) g^2$

$= (\tau h \tau) h = h^2$

Questo dice $(\tau g \tau)^2 h h^{-1} = h^2 h^{-1} = h \Rightarrow \tau g \tau = g$

E allora $\tau g \tau g = g^2 = h$

Per l'altra inclusione,

H abeliano

$\tau (\tau g \tau g) \tau = g (\tau g \tau) \overset{\Downarrow}{=} (\tau g \tau) g$

Per I è analogo

Allora $H^+ / I^+ = H^+ / I \cap H^+ = (H/I)^+ \simeq E[\pi]^+$

Per concludere mi basta dire che $E[\pi]$ ha due autospazi, uno di autovalore 1 e uno di autovalore -1, per il coniugio (inteso per l'azione di τ).

τ soddisfa $\tau^2 = Id$, cioè $\tau^2 - Id = 0$, quindi i suoi autovalori sono al più 1 e -1

Il Weil pairing è Galois-compatibile, quindi

$E[\pi] \times E[\pi] \longrightarrow \mu_p$ ci dice che (poiché $p \neq 2$)

$E[\pi]$ non è tutto invariante per τ e che analogamente non è tutto nell'autospazio di autovalore -1. Questo dà la tesi poiché $E[\pi]$ ha dimensione 2 su $\mathbb{F}_p$.

Proposizione 3 (Gross 9.5)
Sia $\sigma \in S^{\pm}$. TFAE

(1) $[\sigma, \rho] = 0 \quad \forall \rho \in H$

(2) $[\sigma, \rho] = 0 \quad \forall \rho \in H^+$

(3) $[\sigma, \rho] = 0 \quad \forall \rho \in H^+, I^+$

(4) $\sigma = 0$

Dim $4 \Rightarrow 1 \Rightarrow 2 \Rightarrow 3$ ovvio. Vediamo $3 \Rightarrow 4$.
Poiché non dobbiamo: $4 \Leftrightarrow 1$. Facciamo $3 \Rightarrow 1$

Per il lemma $I^+ \subsetneq H^+$, però sia Σ^+ che H^+ sono $\mathbb{F}_\pi$ - s.v. di dim. finita. $|H^+ : \Sigma^+| = \pi^b - \pi^{b-1}$ con $|H^+| = \pi^b$
Però $\pi^{b-1}(\pi - 1) > \pi^{b-1}$ (perché $\pi \neq 2$) e quindi
σ, che si deve annullare su un $\mathbb{F}_\pi$ - s.v., per cardinalità si annulla su tutto H^+
Se $\sigma \in S^+$, $[\sigma, \cdot] : H^+ \to E[\pi]^+$, $H^- \to E[\pi]^-$
perché $\tau[\sigma, \rho] = [\tau\sigma, \tau^{-1}\rho] = [\tau\sigma, \tau\rho] = [\sigma, \tau\rho]$
(τ la coniug. $\in S^+$) → $[\sigma, \rho]$ $\rho \in H^+$; → $[\sigma, \rho]$ $\rho \in H^-$

Analogamente, $\sigma \in S^- : H^{\pm} \to E[\pi]^{\pm}$

Però $\sigma(H) = \mathrm{Im}\, ev_\sigma$ è un sotto - $G_{\mathbb{Q}}$ - modulo di $E[\pi]$

$$ev_\sigma : \underbrace{\mathrm{Hom}(S, E[\pi])}_{\cong H} \to E[\pi]$$

$H = H^+ \oplus H^-$ e quindi $\sigma(H) \subseteq E[\pi]^{\mp} \subsetneq E[\pi]$
Ma $E[\pi]$ è semplice e quindi deve $\sigma(H) = \{0\}$.

Lemma Sia λ un primo di $\mathcal{O}_K$ che non divide $N\pi$.
λ è non - ramificato in M/K

Dim Step 1 E non - ramificato in L/K

$L = K(E[\pi])$ / $\mathbb{Q}(E[\pi])$ — K / $\mathbb{Q}$

Nel nostro setting, la restrizione a $\mathbb{Q}(E[\pi])$ dà un isomorfismo $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(E[\pi])/\mathbb{Q})$
Sia $\sigma \in I(\tilde{\lambda} | \lambda)$ con $\tilde{\lambda}$ primo di M sopra λ
(gruppo d'inerzia, E è già la curva)

$\forall x \in \mathcal{O}_{*M} \quad \sigma x - x \in \tilde{\lambda}$

$\forall x \in \mathcal{O}_{\mathbb{Q}(E[\pi])} \quad \sigma x - x \in \tilde{\lambda}$

$\forall x \in \mathcal{O}_{\mathcal{O}(E[\pi])} \quad \sigma x - x \in \tilde{\lambda} \cap \mathcal{O}_{\mathbb{Q}(E[\pi])}$

$\ell := \text{primo } \lambda \cap \mathbb{Z}$

$\tilde{\lambda} \cap \mathcal{O}_{\mathbb{Q}(E[\pi])} =: \tilde{\ell}$ è sopra ℓ

E allora $\sigma \in I(\tilde{\ell} \mid \ell)$

Ma gli ℓ che non dividono Np non ramificano in $\mathbb{Q}(E[\pi])/\mathbb{Q}$

Quindi $\sigma = Id$ (poiché Res è iso)

Step 2 Non-ramificazione in M/L

Usiamo il seguente Teorema (Silverman, X, 4.4)

$Sel_p(E/K)$ è (sottogruppo) non-ramificato fuori da p e dai primi di cattiva riduzione, cioè

$$\begin{array}{ccc} Sel_p(E/K) & \hookrightarrow & H^1(G_K, E[\pi]) \\ \downarrow & \circlearrowright & \downarrow \\ Sel_p(E/K_\lambda) & \hookrightarrow & H^1(G_{K_\lambda}, E[\pi]) \end{array}$$

e quello sotto è non-ramificato $\forall \lambda \nmid p$ - primo cattivi

Rmk Tutti i primi di cattiva riduzione dividono N

Si ha un diagramma commutativo

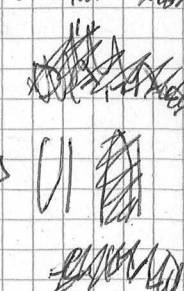
$$\begin{array}{ccccc} Sel_p(E/K) & \subseteq H^1(G_K, E[\pi]) & \xrightarrow[\sim]{Res} & H^1(G_L, E[\pi]) & \cong \prod_{G_K/G_L} H^1(G_{L_\lambda}, E[\pi]) \\ \downarrow & & & \downarrow & \\ Sel_p(E/K_\lambda) & \subseteq H^1(G_{K_\lambda}, E[\pi]) & \xrightarrow{Res} & H^1(G_{L_\lambda}, E[\pi]) & \cong \prod_{G_{K_\lambda}/G_{L_\lambda}} H^1(G_{L_\lambda}, E[\pi]) \end{array}$$

dove quella sotto è una scelta di primi che si restringono.

$$\begin{array}{ccc} M & \lambda_M & \\ | & & \\ L & \lambda_L & \\ | & & \\ K & \lambda & \end{array}$$

(La riga in basso è Inf-res sui completati e $\times$ è la valutazione)

$Gal(M_{\lambda_M}/L_{\lambda_L}) \times E[\pi] \cong D(\lambda_M \mid \lambda_L)$



QED

Però per il Teorema appena invocato, se $\sigma \in I(\lambda_M | \lambda_L)$ si ha (per commutatività del diagramma) che $[\cdot, \sigma] = 0$
Ma il pairing è non-degenere e quindi $\sigma = e$.

ev_σ annulla tutti i cocicli di $\text{Hom}_{G_{K_\lambda}}(G_{L_{\lambda_L}}, E[\pi]) = H^1(G_{K_\lambda}, E[\pi])$ □

Proposizione 4 (Gross 9.6) Sia λ primo di K che non ramifica completamente N_π e che in M/K non è completamente spezzato in L
Sia $Fr(\lambda_M | \lambda_M)$ il Frobenius di λ_M in M/K
(legale: λ_L lì è non-ramificato) e sia $Frob(\lambda)$ la sua orbita sotto $Gal(M/K)$, che agisce per coniugio
TFAE per $s \in Sel_\pi(E/K)$
(1) $[s, Fr(\lambda_M | \lambda_M)] = 0$
(2) $[s, \varphi] = 0 \quad \forall \varphi \in Frob(\lambda)$
(3) $s_\lambda = 0$ in $H^1(G_{K_\lambda}, E[\pi])$

Dim (1) $\Leftrightarrow$ (2): $\forall \sigma \in G_K \; \sigma \cdot [s, \varphi] = [s, \sigma \cdot \varphi]$
Resta da fare l'equivalenza con (3)

$$\begin{array}{ccc} s \in Sel_\pi(E/K) & \subseteq & H^1(G_K, E[\pi]) \\ \downarrow & & \downarrow \text{Res} \\ s_\lambda \in Sel_\pi(E/K_\lambda) & \subseteq & H^1(G_{K_\lambda}, E[\pi]) \\ \| & & \\ [P_\lambda] & & \end{array}$$

$E(K_\lambda) \xrightarrow{s/t} \pi E(K_\lambda)$

Più facile: prendo σ che fissa M_{λ_M} e uso che $[\cdot,\cdot]$ con G_S fanno $0 \Rightarrow \frac{1}{\pi} P_\lambda \in E(M_{\lambda_M})$ perché $D(\lambda_M | \lambda) \subseteq Gal(M_L)$

Dico che $\frac{1}{\pi} P_\lambda$ è razionale su M_{λ_M}

Sia $\sigma \in G_{L_{\lambda_L}}$ che estende $Fr(\lambda_M | \lambda_M)$. Scelgo $\frac{1}{\pi} P_\lambda$ fissato

$\sigma(\frac{1}{\pi} P_\lambda) - \frac{1}{\pi} P_\lambda =: T \in E[\pi]$ (è la valutazione di $\delta(P_\lambda)$ in σ)

σ fissa $E[\pi]$ perché $\mathbb{Q}(E[\pi]) \subseteq L \subseteq L_{\lambda_L}$

Quindi $\sigma^\pi(\frac{1}{\pi} P_\lambda) = \sigma^{\pi-1}(\frac{1}{\pi} P_\lambda + T) = \sigma^{\pi-1}(\frac{1}{\pi} P_\lambda) + T$

$= \dots = \frac{1}{\pi} P_\lambda + \pi T = \frac{1}{\pi} P_\lambda$

$\Rightarrow \frac{1}{\pi} P_\lambda \in E(\overline{L}^{\langle \sigma^\pi \rangle})$

11

(Però avevamo $L \subsetneq M$) e $\mathrm{Gal}(M/L)$ $\mathbb{F}_\lambda$-s.v.

Abbiamo $D(\lambda_M|\lambda) \subseteq \mathrm{Gal}(M/L)$ perché λ è split in L

$\Rightarrow$ $D(\lambda_M|\lambda)$ è un $\mathbb{F}_\lambda$-s.v., diciamo di cardinalità λ^b.

- Se $b=0$, prima potevo scegliere $\sigma = \mathrm{Id}_{\overline{K}_\lambda}$ e non c'è niente da fare
- Se $b>1$,

$$M_{\lambda_M} = \overline{K}_\lambda^{\langle \sigma^{\lambda^b} \rangle} \supseteq \overline{K}_\lambda^{\langle \sigma^\lambda \rangle}$$

Finito a qua posso anche non dirlo

e quindi $\frac{1}{\lambda} P_\lambda \in E(M_{\lambda_M})$. Allora $\sigma\left(\frac{1}{\lambda} P_\lambda\right) - \frac{1}{\lambda} P_\lambda$ non dipende da σ.

Rem Per primi β di buona riduzione e coprimi con γ la riduzione modulo β è iniettiva sulla γ-torsione

Indicando con le barre le proiezioni a quozienti su λ_M:

$$[\xi, F_r(\lambda_M|\lambda)] = 0 \iff \overline{[\xi, F_r(\lambda_M|\lambda)]} = 0 \in E\left(\mathcal{O}_M / \lambda_M \mathcal{O}_M\right)$$

$$\Updownarrow$$

$$\overline{[\xi, F_r(\lambda_M|\lambda)]} = 0 \in E\left(\mathcal{O}_{M_{\lambda_M}} / \lambda_M \mathcal{O}_{M_{\lambda_M}}\right)$$

$$\Updownarrow$$

$$\overline{s_\lambda(F_r(\lambda_M|\lambda))} = 0 \in E\left(\mathcal{O}_{M_{\lambda_M}} / \lambda_M \mathcal{O}_{M_{\lambda_M}}\right)$$

$$\Updownarrow$$

$$s_\lambda(\overline{F_r(\lambda_M|\lambda)}) = 0 \in E\left(M_{\lambda_M}\right)$$

$$\Updownarrow$$

$$F_r(\mathrm{Ma}_{\lambda_M}|M)\left(\tfrac{1}{\lambda} P_\lambda\right) - \tfrac{1}{\lambda} P_\lambda = 0$$

$$\Updownarrow$$

$$s_\lambda = 0 \iff \gamma\, \tfrac{1}{\lambda} P_\lambda - \tfrac{1}{\lambda} P_\lambda = 0 \quad \forall \gamma \in \mathrm{Gal}(M_{\lambda_M}/K_M)$$

□