SEMINARIO KOLYVAGIN: TEOREMA DI HASSE E DUALITÀ TRA CICLI DI HEEGNER E GRUPPI DI SELMER

ANDREA BANDINI

Abstract. Il Teorema di Hasse per il gruppo di Brauer di un campo di numeri e l'applicazione alla sezione 8 di [1]

1. Notazioni

Nel seguito useremo le notazioni:

- per ogni campo di numeri K, $\mathcal{P}_K$ è l'insieme dei posti di K (finiti e infiniti);
- per ogni $\mathfrak{p} \in \mathcal{P}_K$, $K_\mathfrak{p}$ è il completamento di K in $\mathfrak{p}$;
- per ogni estensione di Galois L/K, $G_{L/K} := \mathrm{Gal}(L/K)$ (analoga notazione per estensioni di campi locali);
- per ogni $G_{L/K}$-modulo A, denotiamo con $H^q(L/K, A)$ il q-esimo gruppo di coomologia di Tate di A, se $L = \overline{K}$, scriviamo semplicemente $G_{\overline{K}/K} := G_K$ e $H^q(\overline{K}/K, A) := H^q(K, A)$;

tutte le estensioni (locali e globali) saranno estensioni di Galois.
Tutti i gruppi di coomologia saranno in coomologia di Tate, in particolare

$$H^0(L/K, A) = A^{G_{L/K}}/N_K^L(A) \quad \text{e} \quad H^{-1}(L/K, A) = \mathrm{Ker}(N_K^L)/\mathrm{Aug}_{L/K}A,$$

dove N_K^L è la norma associata a $G_{L/K}$ e $\mathrm{Aug}_{L/K} = (\sigma - 1, \sigma \in G_{L/K})$ è l'augmentazione di $G_{L/K}$.
In particolare, se $G_{L/K}$ è ciclico, allora

$$H^0(L/K, A) \simeq H^{2q}(L/K, A) \quad \text{e} \quad H^{-1}(L/K, A) \simeq H^{2q+1}(L/K, A)$$

per ogni $q \in \mathbb{Z}$ ([2, Part I, §6]).
Strategia e dimostrazioni complete (e corrette...) si possono trovare per esempio in [2] e [3].

2. Goal 1: il Teorema di Hasse

Teorema 2.1. *Sia K un campo di numeri, allora si ha una successione esatta canonica*

$$\mathrm{Br}(K) \xhookrightarrow{\ \mathrm{res}\ } \bigoplus_{\mathfrak{p} \in \mathcal{P}_K} \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\ \mathrm{inv}_K\ } \mathbb{Q}/\mathbb{Z}$$

dove res *è il prodotto delle restrizioni* $\mathrm{res}_\mathfrak{p} : \mathrm{Br}(K) = H^2(K, \overline{K}^*) \longrightarrow \mathrm{Br}(K_\mathfrak{p}) = H^2(K_\mathfrak{p}, \overline{K_\mathfrak{p}}^*)$ *e* inv_K *è definita da* $\mathrm{inv}_K((a_\mathfrak{p})_{\mathfrak{p} \in \mathcal{P}_K}) = \sum_{\mathfrak{p} \in \mathcal{P}_K} \mathrm{inv}_{K_\mathfrak{p}}(a_\mathfrak{p})$ *(la somma delle mappe invarianti locali).*

In realtà dimostreremo solo che $\mathrm{inv}_K \circ \mathrm{res} = 0$ e, per farlo, seguiremo la strategia seguente:

1. calcolo di $\bigoplus_{\mathfrak{p} \in \mathcal{P}_K} \mathrm{Br}(K_\mathfrak{p})$ tramite la coomologia degli ideli;
2. calcolo della coomologia degli ideli come limite diretto della coomologia sulle estensioni cicliche ciclotomiche (i.e. estensioni cicliche L/K tale che $L \subseteq K(\zeta_n)$ per qualche $n \in \mathbb{N}$);
3. dimostrazione dell'esattezza delle successioni

$$H^2(L/K, L^*) \xhookrightarrow{\ \mathrm{res}\ } \bigoplus_{\mathfrak{p} \in \mathcal{P}_K} H^2(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*) \xrightarrow{\ \mathrm{inv}_{L/K}\ } \mathbb{Z}/([L : K]) \tag{1}$$

(dove $\mathfrak{P}$ è un primo di L sopra $\mathfrak{p}$) per ogni estensione ciclica ciclotomica L/K.
L'enunciato segue prendendo il limite diretto dell'ultima successione rispetto alle estensioni L (una volta verificato che le mappe del limite diretto sono compatibili con res e inv).

2.1. **Coomologia degli ideli.**

Definizione 2.2. *Per ogni S sottoinsieme finito di $\mathcal{P}_K$, gli S-ideli di K sono*

$$\mathbb{I}_K^S := \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \subset \prod_{\mathfrak{p}\in\mathcal{P}_K} K_\mathfrak{p}^*$$

(dove $U_\mathfrak{p}$ sono le unità dell'anello degli interi di $K_\mathfrak{p}$).
Gli ideli di K sono l'insieme

$$\mathbb{I}_K := \bigcup_S \mathbb{I}_K^S.$$

Consideriamo K^* immerso in $\mathbb{I}_K$ diagonalmente, allora il gruppo delle classi degli ideli di K è $C_K := \mathbb{I}_K/K^*$.

Sia L/K un'estensione di Galois; è facile verificare che $\mathbb{I}_K = \mathbb{I}_L^{G_{L/K}}$ (cf. [2, Proposition III.2.5]). Sia $S \subset \mathcal{P}_K$ un insieme finito e sia $S_L \subset \mathcal{P}_L$ l'insieme dei primi di L sopra i primi di S. Possiamo scrivere

$$\begin{aligned}\mathbb{I}_L^{S_L} &= \prod_{\mathfrak{P}\in S_L} L_\mathfrak{P}^* \times \prod_{\mathfrak{P}\notin S_L} U_\mathfrak{P} \\ &= \prod_{\mathfrak{p}\in S}\prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}^* \times \prod_{\mathfrak{p}\notin S}\prod_{\mathfrak{P}|\mathfrak{p}} U_\mathfrak{P} \\ &:= \prod_{\mathfrak{p}\in S} \mathbb{I}_L^\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} \mathbb{U}_L^\mathfrak{p}. \qquad (2)\end{aligned}$$

Dato che $G_{L/K}$ permuta i primi di L sopra un singolo $\mathfrak{p}$, i sottogruppi $\mathbb{I}_L^\mathfrak{p}$ e $\mathbb{U}_L^\mathfrak{p}$ (immersi in $\mathbb{I}_L$ con coordinate 1 fuori dai posti sopra $\mathfrak{p}$) sono $G_{L/K}$-moduli. La decomposizione di (2) induce isomorfismi tra i gruppi di coomologia

$$H^q(L/K, \mathbb{I}_L^{S_L}) \simeq \prod_{\mathfrak{p}\in S} H^q(L/K, \mathbb{I}_L^\mathfrak{p}) \times \prod_{\mathfrak{p}\notin S} H^q(L/K, \mathbb{U}_L^\mathfrak{p}). \qquad (3)$$

Proposizione 2.3. *Sia $\mathfrak{P}$ un primo di L sopra $\mathfrak{p}$, allora*

$$H^q(L/K, \mathbb{I}_L^\mathfrak{p}) \simeq H^q(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*) \quad e \quad H^q(L/K, \mathbb{U}_L^\mathfrak{p}) \simeq H^q(L_\mathfrak{P}/K_\mathfrak{p}, U_\mathfrak{P}).$$

Dimostrazione. Vediamo solo $\mathbb{I}_L^\mathfrak{p}$ (l'altro è analogo). Il gruppo $G_{L_\mathfrak{P}/K_\mathfrak{p}}$ è il gruppo di decomposizione di $\mathfrak{P}$ su $\mathfrak{p}$ e possiamo scrivere

$$\mathbb{I}_L^\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}^* = \prod_{\sigma\in\mathcal{R}_\mathfrak{P}} L_{\sigma\mathfrak{P}}^* = \prod_{\sigma\in\mathcal{R}_\mathfrak{P}} \sigma L_\mathfrak{P}^*,$$

dove $\mathcal{R}_\mathfrak{P}$ è un insieme di rappresentanti per $G_{L_\mathfrak{P}/K_\mathfrak{p}}$ in $G_{L/K}$. Dunque $\mathbb{I}_L^\mathfrak{p}$ è un G-modulo indotto (da $G_{L_\mathfrak{P}/K_\mathfrak{p}}$) e il Lemma di Shapiro (cf. [2, Theorem I.4.19]) implica

$$H^q(L/K, \mathbb{I}_L^\mathfrak{p}) \simeq H^q(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*). \qquad \square$$

Osservazione 2.4. *L'isomorfismo esplicito nel lemma precedente (ameno per gli H^0) si ottiene dalle seguenti mappe. Consideriamo la composizione*

$$H^q(L/K, \mathbb{I}_L^\mathfrak{p}) \xrightarrow{\text{res}} H^q(L_\mathfrak{P}/K_\mathfrak{p}, \mathbb{I}_L^\mathfrak{p}) \xrightarrow{\pi_\mathfrak{P}} H^q(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*),$$

dove $\pi_\mathfrak{P}$ è indotta dalla proiezione naturale sulla $\mathfrak{P}$-esima componente $\mathbb{I}_L^\mathfrak{p} \twoheadrightarrow L_\mathfrak{P}^*$.

Ricordiamo che per $q = 0$ si ha $H^0(L/K, A) = A^{G_{L/K}}/N_K^L(A)$, per cui l'omomorfismo precedente fornisce

$$(\mathbb{I}_L^{\mathfrak{p}})^{G_{L/K}}/N_K^L(\mathbb{I}_L^{\mathfrak{p}}) \xrightarrow{\text{res}} (\mathbb{I}_L^{\mathfrak{p}})^{G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}}/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(\mathbb{I}_L^{\mathfrak{p}}) \xrightarrow{\pi_{\mathfrak{P}}} (L_{\mathfrak{P}}^*)^{G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}}/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*) = K_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*).$$

Definiamo

$$\eta : K_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*) \longrightarrow (\mathbb{I}_L^{\mathfrak{p}})^{G_{L/K}}/N_K^L(\mathbb{I}_L^{\mathfrak{p}})$$
$$\eta(\overline{a}) = (\sigma(a))_{\sigma\in\mathcal{R}_{\mathfrak{P}}} + N_K^L(\mathbb{I}_L^{\mathfrak{p}})$$

(dove $a \in K_{\mathfrak{p}}^*$ è un qualsiasi rappresentante di $\overline{a} \in K_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*)$). È facile verificare che $\eta\circ(\pi_{\mathfrak{P}}\circ\text{res})$ (risp. $(\pi_{\mathfrak{P}}\circ\text{res})\circ\eta$) sono l'identità su $(\mathbb{I}_L^{\mathfrak{p}})^{G_{L/K}}/N_K^L(\mathbb{I}_L^{\mathfrak{p}})$ (risp. $K_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*)$) [1]*. Dunque otteniamo l'isomorfismo richiesto per $q = 0$. Il dimension shifting fornisce l'isomorfismo per ogni q.*

Corollario 2.5. [Hilbert 90] $H^1(L/K, \mathbb{I}_L^{\mathfrak{p}}) = 1$.

Ricordiamo che per le estensioni locali non ramificate la norma è surgettiva sulle unità quindi $H^0(L_{\mathfrak{P}}/K_{\mathfrak{p}}, U_{\mathfrak{P}}) = U_{\mathfrak{p}}/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(U_{\mathfrak{P}}) = 1$. Inoltre $G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ è ciclico e quindi per conoscere l'intera coomologia è sufficiente calcolare $H^1(L_{\mathfrak{P}}/K_{\mathfrak{p}}, U_{\mathfrak{P}}) = 0$. Per ogni estensione non ramificata di campi locali si ha

$$H^q(L_{\mathfrak{P}}/K_{\mathfrak{p}}, U_{\mathfrak{P}}) = 1$$

(cf. [2, Theorem II.4.3]). La dimostrazione utilizza local class field theory e la filtrazione delle unità data dai gruppi $U_{\mathfrak{P}}^{(n)} = \{u \in U_{\mathfrak{P}} : u \equiv 1 \pmod{\mathfrak{P}^n}\}$ con $U_{\mathfrak{P}}/U_{\mathfrak{P}}^{(1)} \simeq l_{\mathfrak{P}}^+$ (dove $l_{\mathfrak{P}}$ il campo residuo in $\mathfrak{P}$, che ha coomologia banale per [2, Theorem 2.1]) e $U_{\mathfrak{P}}^{(n+1)}/U_{\mathfrak{P}}^{(n)} \simeq l_{\mathfrak{P}}^*$ per ogni $n \geqslant 1$ (che ha H^1 banale per Hilbert 90).

Se $S \subset \mathcal{P}_K$ è finito e contiene tutti i posti ramificati in L, allora, dalla Proposizione 2.3 otteniamo

$$H^q(L/K, \mathbb{I}_L^S) \simeq \prod_{\mathfrak{p}\in S} H^q(L/K, \mathbb{I}_L^{\mathfrak{p}}) \simeq H^q(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*)$$

per un fissato $\mathfrak{P} \mid \mathfrak{p}$.
Dato che $\mathbb{I}_L = \bigcup_{S_L} \mathbb{I}_L^{S_L}$, passando al limite diretto sugli S_L contenenti i posti ramificati si ottiene

$$H^q(L/K, \mathbb{I}_L) \simeq \varinjlim_{S_L} \prod_{\mathfrak{p}\in S} H^q(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*) \simeq \bigoplus_{\mathfrak{p}\in\mathcal{P}_K} H^q(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*),$$

che, per $q = 2$, è la parte centrale della successione in (1).

2.2. **Estensioni cicliche ciclotomiche.** Ricordiamo brevemente il calcolo della coomologia dei campi locali, in particolare

$$\text{Br}(K_{\mathfrak{p}}) = H^2(K_{\mathfrak{p}}, \overline{K_{\mathfrak{p}}}^*) = \bigcup_{L_{\mathfrak{P}}/K_{\mathfrak{p}} \text{ ciclica}} H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*).$$

Sono sufficienti le estensioni cicliche grazie al seguente

Lemma 2.6. *Sia $M_{\mathfrak{q}}/K_{\mathfrak{p}}$ un'estensione qualsiasi e sia $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ l'estensione non ramificata tale che $[M_{\mathfrak{q}} : K_{\mathfrak{p}}] = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. Allora*

$$H^2(M_{\mathfrak{q}}/K_{\mathfrak{p}}, M_{\mathfrak{q}}^*) = H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*).$$

Tralasciamo la dimostrazione che è (in gran parte) analoga a quella della Proposizione 2.12 che fornirà il corrispondente per la coomologia globale.

[1] In particolare una dimostrazione analoga a [2, Proposizione III.2.5] mostra che $(\mathbb{I}_L^{\mathfrak{p}})^{G_{L/K}} = \prod_{\mathfrak{P}\mid\mathfrak{p}} K_{\mathfrak{p}}^*$

Lemma 2.7. *Sia $S \subset \mathcal{P}_K$ finito e sia $m \in \mathbb{N}$, allora esiste L/K estensione ciclica ciclotomica (i.e. L/K ciclica e $L \subseteq K(\zeta_n)$ per qualche n) tale che*

- $m \mid [L_\mathfrak{P} : K_\mathfrak{p}]$ *per ogni* $\mathfrak{p} \in S$, $\mathfrak{p} \nmid \infty$;
- $[L_\mathfrak{P} : K_\mathfrak{p}] = 2$ *per ogni* $\mathfrak{p} \in S$, $\mathfrak{p} \mid \infty$ *and* $\mathfrak{p}$ *real.*

Dimostrazione. Per l'arbitrarietà di m, è sufficiente dimostrarlo per $K = \mathbb{Q}$. Trovata una ciclica ciclotomica $M/\mathbb{Q}$ che verifica le richieste per ogni primo di $\mathbb{Z}$ che giace sotto un primo di S e per $m' = [K : \mathbb{Q}] \cdot m$, è sufficiente considerare MK/K.
Per $K = \mathbb{Q}$, si considera $m = p_1^{e_1} \cdots p_r^{e_r}$ e si prendono le estensioni cicliche ciclotomiche:

- $L_i = \mathbb{Q}(\zeta_{p_i^{n_i}})^{(\mathbb{Z}/(p_i))^*}$ per $p_i \neq 2$ (interpretando $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{n_i}})/\mathbb{Q}) \simeq (\mathbb{Z}/(p_i^{n_i}))^* \simeq (\mathbb{Z}/(p_i))^* \times \mathbb{Z}/(p^{n_i - 1}))$;
- $L_i = \mathbb{Q}(\zeta_{2^{n_i}}) \bigcap \mathbb{R}$ per $p_i = 2$.

Prendendo ogni $n_i \gg 0$, la composizione $\prod_i L_i = L$ verifica le richieste. □

2.2.1. *Definizione di* inv *locale.* Sia $L_\mathfrak{P}/K_\mathfrak{p}$ un'estensione non ramificata; è sufficiente definire la mappa invariante per tali estensioni grazie al Lemma 2.6.
La successione esatta

$$U_\mathfrak{P} \hookrightarrow L_\mathfrak{P}^* \xrightarrow{v_\mathfrak{P}} \mathbb{Z}$$

(dove $v_\mathfrak{P}$ è la valutazione $\mathfrak{P}$-adica) e la coomologia banale di $U_\mathfrak{P}$ forniscono un isomorfismo

$$\overline{v}_\mathfrak{P} : H^2(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*) \longrightarrow H^2(L_\mathfrak{P}/K_\mathfrak{p}, \mathbb{Z}).$$

La successione esatta

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}$$

e la coomologia banale di $\mathbb{Q}$ (che è un gruppo divisibile) forniscono un isomorfismo

$$\delta : H^1(L_\mathfrak{P}/K_\mathfrak{p}, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(L_\mathfrak{P}/K_\mathfrak{p}, \mathbb{Z}).$$

Infine dato che l'azione su $\mathbb{Q}/\mathbb{Z}$ è banale, $H^1(L_\mathfrak{P}/K_\mathfrak{p}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L_\mathfrak{P}/K_\mathfrak{p}}, \mathbb{Q}/\mathbb{Z})$ è il duale di Pontrjagin di $G_{L_\mathfrak{P}/K_\mathfrak{p}}$ (indicato con $G^\vee_{L_\mathfrak{P}/K_\mathfrak{p}}$). Dato che $G_{L_\mathfrak{P}/K_\mathfrak{p}}$ è un gruppo ciclico con un generatore canonico $\mathrm{Frob}_\mathfrak{p}$, possiamo definire un isomorfismo

$$\varphi_\mathfrak{P} : \mathrm{Hom}(G_{L_\mathfrak{P}/K_\mathfrak{p}}, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Z}/([L_\mathfrak{P} : K_\mathfrak{p}])$$
$$\varphi_\mathfrak{P}(\chi) = \chi(\mathrm{Frob}_\mathfrak{p}).$$

Definizione 2.8. *La mappa invariante locale* $\mathrm{inv}_{L_\mathfrak{P}/K_\mathfrak{p}}$ *è un isomorfismo definito da*

$$\mathrm{inv}_{L_\mathfrak{P}/K_\mathfrak{p}} : H^2(L_\mathfrak{P}/K_\mathfrak{p}, L_\mathfrak{P}^*) \longrightarrow \mathbb{Z}/([L_\mathfrak{P} : K_\mathfrak{p}])$$
$$\mathrm{inv}_{L_\mathfrak{P}/K_\mathfrak{p}}(c) = (\varphi_\mathfrak{P} \circ \delta^{-1} \circ \overline{v}_\mathfrak{P})(c).$$

Osservazione 2.9. *Se $M_\mathfrak{q}/K_\mathfrak{p}$ è una qualsiasi estensione di campi locali allora la mappa* $\mathrm{inv}_{M_\mathfrak{q}/K_\mathfrak{p}}$ *si definisce come* $\mathrm{inv}_{L_\mathfrak{P}/K_\mathfrak{p}}$*, dove $L_\mathfrak{P}/K_\mathfrak{p}$ è l'unica estensione non ramificata di $K_\mathfrak{p}$ che verifica $[L_\mathfrak{P} : K_\mathfrak{p}] = [M_\mathfrak{q} : K_\mathfrak{p}]$.*

Definizione 2.10. *La mappa di reciprocità di Artin è un isomorfismo (indotto dal cup product)*

$$\theta : G_{L_\mathfrak{P}/K_\mathfrak{p}} \simeq H^{-2}(G_{L_\mathfrak{P}/K_\mathfrak{p}}, \mathbb{Z}) \longrightarrow H^0(G_{L_\mathfrak{P}/K_\mathfrak{p}}, L_\mathfrak{P}^*) = K_\mathfrak{p}^*/N_{K_\mathfrak{p}}^{L_\mathfrak{P}}(L_\mathfrak{P}^*).$$

Indichiamo la mappa inversa con $(\bullet, L_\mathfrak{P}/K_\mathfrak{p})$ e la definiamo norm residue symbol.
In particolare, per un'estensione non ramificata $L_\mathfrak{P}/K_\mathfrak{p}$, per ogni $\overline{a} \in K_\mathfrak{p}^*/N_{K_\mathfrak{p}}^{L_\mathfrak{P}}(L_\mathfrak{P}^*)$ si ha

$$(\overline{a}, L_\mathfrak{P}/K_\mathfrak{p}) = \mathrm{Frob}_\mathfrak{p}^{v_\mathfrak{P}(a)} = \mathrm{Frob}_\mathfrak{p}^{v_\mathfrak{p}(a)},$$

dove $a \in K_\mathfrak{p}^*$ è un qualsiasi rappresentante di $\overline{a}$ e $v_\mathfrak{P} = v_\mathfrak{p}$ perché l'estensione è non ramificata.

Osservazione 2.11. [Interazione tra inv e norm residue symbol] *Siano* $\overline{a} \in K_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*)$ *e* $\chi \in G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}^{\vee}$*, allora* $\delta(\chi) \in H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \mathbb{Z})$ *e l'accoppiamento di dualità (cup product)*

$$\cup : H^0(G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}, L_{\mathfrak{P}}^*) \times H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, \mathbb{Z}) \longrightarrow H^2(G_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}, L_{\mathfrak{P}}^*)$$

consente di definire $\mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ *su ogni elemento del tipo* $\overline{a} \cup \delta(\chi)$*. In particolare, la compatibilità tra le varie mappe in coomologia fornisce la formula*

$$\begin{aligned} \mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\overline{a} \cup \delta(\chi)) &= (\varphi_{\mathfrak{P}} \circ \delta^{-1} \circ \overline{v}_{\mathfrak{P}})(\overline{a} \cup \delta(\chi)) \\ &= \varphi_{\mathfrak{P}}(v_{\mathfrak{P}}(a) \cdot \chi) = \chi(\mathrm{Frob}_{\mathfrak{p}}^{v_{\mathfrak{P}}(a)}) \\ &= \chi((\overline{a}, L_{\mathfrak{P}}/K_{\mathfrak{p}})). \end{aligned} \tag{4}$$

2.2.2. *Coomologia attraverso le estensioni cicliche ciclotomiche.*

Proposizione 2.12.

$$\mathrm{Br}(K) = \bigcup_{L/K \text{ ciclica ciclotomica}} H^2(L/K, L^*)$$

e

$$\bigoplus_{\mathfrak{p}} \mathrm{Br}(K_{\mathfrak{p}}) = \bigcup_{M/K} \bigoplus_{\mathfrak{p}} H^2(M_{\mathfrak{q}}/K_{\mathfrak{p}}, M_{\mathfrak{q}}^*) = \bigcup_{M/K} H^2(M/K, \mathbb{I}_M) = \bigcup_{L/K \text{ ciclica ciclotomica}} H^2(L/K, \mathbb{I}_L).$$

Dimostrazione. Sia $c \in H^2(L'/K, \mathbb{I}_{L'})$ per qualche estensione normale L'/K e sia $o(c) = m$. Dato che $c \in \bigoplus_{\mathfrak{p}} H^2(L'_{\mathfrak{q}}/K_{\mathfrak{p}}, (L'_{\mathfrak{q}})^*)$ possiamo definire S come l'insieme (finito) di primi di K per cui le componenti locali $c_{\mathfrak{p}}$ di c sono non nulle. Prendiamo L/K ciclica ciclotomica come nel Lemma 2.7 rispetto a S e m. Per Hilbert 90 le mappe di inflazione

$$H^2(L/K, \mathbb{I}_L) \longrightarrow H^2((LL')/K, \mathbb{I}_{LL'}) \quad \text{e} \quad H^2(L'/K, \mathbb{I}_{L'}) \longrightarrow H^2((LL')/K, \mathbb{I}_{LL'})$$

sono iniettive. Abbiamo il seguente diagramma

$$\begin{array}{ccccc} H^2(L/K, \mathbb{I}_L) & \hookrightarrow & H^2((LL')/K, \mathbb{I}_{LL'}) & \xrightarrow{\mathrm{res}_{LL'/L}} & H^2((LL')/L, \mathbb{I}_{LL'}) \\ & & \uparrow & & \\ & & H^2(L'/K, \mathbb{I}_{L'}). & & \end{array}$$

Dunque $c \in H^2(L/K, \mathbb{I}_L)$ se e solo se $\mathrm{res}_{LL'/L}(c) = 0$.
Per ogni primo $\mathfrak{p} \in S$ consideriamo il seguente diagramma commutativo

$$\begin{array}{ccc} H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*) & \xrightarrow{\mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}} & \mathbb{Z}/([L_{\mathfrak{P}} : K_{\mathfrak{p}}]) \\ \downarrow & & \downarrow \\ H^2((LL')_{\mathfrak{Q}}/K_{\mathfrak{p}}, (LL')_{\mathfrak{Q}}^*) & \xrightarrow{\mathrm{inv}_{(LL')_{\mathfrak{Q}}/K_{\mathfrak{p}}}} & \mathbb{Z}/([(LL')_{\mathfrak{Q}} : K_{\mathfrak{p}}]) \\ \downarrow{\scriptstyle \mathrm{res}_{(LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}}} & & \downarrow{\scriptstyle [L_{\mathfrak{P}}:K_{\mathfrak{p}}]} \\ H^2((LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}, (LL')_{\mathfrak{Q}}^*) & \xrightarrow{\mathrm{inv}_{(LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}}} & \mathbb{Z}/([(LL')_{\mathfrak{Q}} : L_{\mathfrak{P}}]) \end{array}$$

(dove le mappe orizzontali sono definite grazie all'Osservazione 2.9). Abbiamo

$$(\mathrm{inv}_{(LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}} \circ \mathrm{res}_{(LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}})(c_{\mathfrak{p}}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]\, \mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(c_{\mathfrak{p}})$$

e, dato che $o(c) = m \mid [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ e le mappe inv sono isomorfismi, si ottiene $\mathrm{res}_{(LL')_{\mathfrak{Q}}/L_{\mathfrak{P}}}(c_{\mathfrak{p}}) = 0$ per ogni $\mathfrak{p} \in S$, i.e. $c \in H^2(L/K, \mathbb{I}_L)$.
La dimostrazione per $\mathrm{Br}(K)$ è analoga. □

2.3. **Dimostrazione per le estensioni cicliche ciclotomiche.**

Teorema 2.13. *Sia L/K un'estensione ciclica ciclotomica, allora la successione*

$$H^2(L/K, L^*) \xhookrightarrow{\text{res}} \bigoplus_{\mathfrak{p}\in\mathcal{P}_K} H^2(L_{\mathfrak{P}}/K_{\mathfrak{p}}, L_{\mathfrak{P}}^*) \xrightarrow{\text{inv}_{L/K}} \mathbb{Z}/([L:K])$$

è esatta (con $\text{inv}_{L/K} = \sum_{\mathfrak{p}} \text{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$*).*

Dimostrazione. Ci interessa in particolare la dimostrazione del fatto che $\text{inv}_{L/K}(c) = 0$ per ogni $c \in H^2(L/K, L^*)$.

Step 1. Possiamo supporre $K = \mathbb{Q}$.
Infatti nel caso generale basta prendere $M/\mathbb{Q}$ ciclica ciclotomica contenente L e utilizzare il diagramma commutativo

$$\begin{array}{ccccc} H^2(L/K, L^*) & \hookrightarrow & H^2(M/K, M^*) & \xrightarrow{\text{inv}_{M/K}} & \mathbb{Z}/([M:K]) \\ & & \downarrow \text{cor} & & \downarrow \\ & & H^2(M/\mathbb{Q}, M^*) & \xrightarrow{\text{inv}_{M/\mathbb{Q}}} & \mathbb{Z}/([M:\mathbb{Q}]) \end{array}$$

per vedere che è sufficiente dimostrare $\text{inv}_{M/\mathbb{Q}}(H^2(M/\mathbb{Q}, M^*)) = 0$.

Step 2. Dimostrazione per $L/\mathbb{Q}$ ciclica ciclotomica.
Sia $\omega \in G_{L/\mathbb{Q}}^\vee = H^1(L/\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$ un generatore, allora $\delta(\omega) \in H^2(L/\mathbb{Q}, \mathbb{Z})$ è un generatore (l'analogo globale della classe fondamentale). Il Teorema di Tate (e le proprietà dei gruppi di coomologia di L^*, cf. [2, Theorem I.7.3]) implica che il cup product con $\delta(\omega)$ fornisce un isomorfismo

$$\cup\delta(\omega) : H^0(L/\mathbb{Q}, L^*) \longrightarrow H^2(L/\mathbb{Q}, L^*),$$

dunque possiamo scrivere ogni elemento di $H^2(L/\mathbb{Q}, L^*)$ nella forma $\overline{a} \cup \delta(\omega)$ per qualche $\overline{a} \in \mathbb{Q}^*/N_{\mathbb{Q}}^L(L^*)$.
Quindi (cf. Osservazione 2.11)

$$\text{inv}_{L/\mathbb{Q}}(\overline{a} \cup \delta(\omega)) = \sum_p \text{inv}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(\overline{a} \cup \delta(\omega))_p \tag{5}$$

$$= \sum_p \omega((\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p)) = \omega\left(\prod_p (\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p)\right), \tag{6}$$

ed è sufficiente dimostrare $\prod_p (\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p) = \text{Id}$ (dove il prodotto/composizione di automorfismi è su tutti i posti di $\mathbb{Q}$, quindi include anche $p = \infty$). Per fare questo possiamo supporre $L \subset \mathbb{Q}(\zeta_n)$ con $n = \ell_1^{e_1} \cdots \ell_r^{e_r}$ e dimostrare che tale prodotto di norm residue symbols è l'identità su ognuna delle radici $\ell_i^{e_i}$-esime dell'unità. Dato che il norm residue symbol (e le altre mappe coinvolte) sono compatibili con le restrizioni, è sufficiente controllare tale proprietà per ogni $L \subset \mathbb{Q}(\zeta_{\ell_i^{e_i}})$ per ottenere poi il risultato sulla composizione. Quindi da ora in poi supponiamo $L \subset \mathbb{Q}(\zeta_{\ell_i^{e_i}})$.
Per semplicità fissiamo $\ell = \ell_i$ con $e = e_i$ e fissiamo anche un rappresentante a di $\overline{a}$. Le componenti locali sono date da

- se $p = \infty$ allora $N_{\mathbb{Q}_p}^{L_{\mathfrak{P}}}(L_{\mathfrak{P}}^*) = N_{\mathbb{R}}^{\mathbb{C}}(\mathbb{C}^*) = \mathbb{R}_{>0}$, dunque

$$(\overline{a}, \mathbb{C}/\mathbb{R})(\zeta_{\ell^e}) = \left\{ \begin{array}{ll} \zeta_{\ell^e} & \text{se } a > 0 \\ \\ \zeta_{\ell^e}^{-1} & \text{se } a < 0 \end{array} \right\} = \zeta_{\ell^e}^{\text{sgn}(a)};$$

- se $p \neq \infty$ e $p \neq \ell$, allora p non è ramificato in $L/\mathbb{Q}$ e dunque $(a, L_{\mathfrak{P}}/\mathbb{Q}_p) = \mathrm{Frob}_p$, i.e.
$$(\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p)(\zeta_{\ell^e}) = \zeta_{\ell^e}^{p^{v_p(a)}};$$
- se $p = \ell$ allora l'estensione locale è totalmente ramificata (e la mappa inv locale deve essere calcolata su un'estensione non ramificata dello stesso grado, cf. Osservazione 2.9), se scriviamo $a = u\ell^s$ con $v_p(u) = 0$ e definiamo $r \equiv u^{-1} \pmod{\ell^e}$ si ha (cf. [2, Part II §7], dato che l'estensione è totalmente ramificata, ℓ è una norma quindi è logico che il norm residue symbol non dipenda da ℓ ma solo da u...sul perché dell'esponente -1 non posso fare altro che rimandare alle dimostrazioni complete con la teoria di Lubin-Tate)
$$(\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p)(\zeta_{\ell^e}) = \zeta_{\ell^e}^{r}.$$

Riunendo tutte le componenti locali e osservando che $u = \prod_{p\neq\ell} p^{v_p(a)}$, si ottiene

$$\prod_p (\overline{a}, L_{\mathfrak{P}}/\mathbb{Q}_p)(\zeta_{\ell^e}) = \zeta_{\ell^e}^{\mathrm{sgn}(a)\prod_{p\neq\ell,\, p\neq\infty} p^{v_p(a)}\cdot r} = \zeta_{\ell^e},$$

perchè $\mathrm{sgn}(a) \prod_{p\neq\ell,\ p\neq\infty} p^{v_p(a)} \cdot r \equiv 1 \pmod{\ell^e}$ per definizione di r.

Step 3. La surgettività di $\mathrm{inv}_{L/K}$ dipende dall'esistenza di almeno un primo $\mathfrak{p}$ di K inerte in L.

Step 4. Il fatto che il nucleo di $\mathrm{inv}_{L/K}$ è esattamente $H^2(L/K, L^*)$ dipende da considerazioni sulla cardinalità dei gruppi di coomologia coinvolti (inclusi i gruppi di coomologia del gruppo delle classi di ideli C_K).
Per una dimostrazione degli ultimi due step cf. [2, Proposition III.5.6] o [3, Proposition 8.1.15]. □

3. Goal 2: Proposition 8.2 di Gross

Sia $d(n) \in H^1(K, E)[p]$ una delle classi di coomologia definite nelle lezioni precedenti, che è l'immagine di una classe $c(n) \in H^1(K, E[p])$.

Teorema 3.1. [1, Proposition 8.2] *Sia $s \in \mathrm{Sel}_p(E/K)$ e sia $\langle\ ,\ \rangle$ l'accoppiamento di dualità di Tate. Sia λ l'unico primo di K sopra ℓ (con le solite ipotesi richieste su p ed ℓ), allora*
$$\langle d(\ell)_\lambda, s_\lambda\rangle := \langle c(\ell)_\lambda, s_\lambda\rangle = 0.$$
In particolare, almeno una delle due componenti locali $d(\ell)_\lambda$ e s_λ deve essere nulla.

3.1. **I gruppi di Selmer.** Per definire il gruppo di Selmer di una curva ellittica E definita su un campo K, consideriamo la successione esatta della n-torsione ($n \in \mathbb{N}$)
$$E[n] \hookrightarrow E(\overline{K}) \xrightarrow{\ n\ } E(\overline{K})$$
e prendiamo la coomologia rispetto a $G_K := \mathrm{Gal}(\overline{K}/K)$ per ottenere una mappa iniettiva (di Kummer)
$$\kappa_n : E(K)/nE(K) \hookrightarrow H^1(K, E[n]).$$
La definizione è analoga alla mappa di Kummer classica $K^*/(K^*)^n \hookrightarrow H^1(K, \mu_n)$, infatti $\kappa_n(P + nE(K))(\sigma) = \sigma(Q) - Q$ per ogni $\sigma \in G_K$, dove $Q \in E(\overline{K})$ è tale che $nQ = P$.
Analogamente, per i campi locali otteniamo mappe
$$\kappa_{n,\mathfrak{p}} : E(K_\mathfrak{p})/nE(K_\mathfrak{p}) \hookrightarrow H^1(K_\mathfrak{p}, E[n]).$$

Dato che $G_{K_\mathfrak{p}}$ è un sottogruppo di G_K, possiamo considerare le mappe di restrizione e le ovvie mappe indotte dall'inclusione $E(K) \hookrightarrow E(K_\mathfrak{p})$ per ottenere un diagramma commutativo

$$\begin{array}{ccc} E(K)/nE(K) & \xhookrightarrow{\kappa_n} & H^1(K, E[n]) \\ \downarrow & & \downarrow \mathrm{res}_\mathfrak{p} \\ E(K_\mathfrak{p})/nE(K_\mathfrak{p}) & \xhookrightarrow{\kappa_{n,\mathfrak{p}}} & H^1(K_\mathfrak{p}, E[n]). \end{array}$$

Definizione 3.2. *La n-parte del gruppo di Selmer di E su K è data da*

$$\mathrm{Sel}_n(E/K) := \{\alpha \in H^1(K, E[n]) : \mathrm{res}_\mathfrak{p}(\alpha) \in \mathrm{Im}(\kappa_{n,\mathfrak{p}}) \quad \forall \mathfrak{p} \in \mathcal{P}_K\}.$$

Passando al limite diretto su n otteniamo una mappa

$$\kappa : E(K) \otimes \mathbb{Q}/\mathbb{Z} \xhookrightarrow{} H^1(K, E_{tors})$$

e le sue analoghe $\kappa_\mathfrak{p}$ per i campi locali. Possiamo quindi definire

Definizione 3.3. *Il gruppo di Selmer di E su K è*

$$\mathrm{Sel}(E/K) := \{\alpha \in H^1(K, E_{tors}) : \mathrm{res}_\mathfrak{p}(\alpha) \in \mathrm{Im}(\kappa_\mathfrak{p}) \quad \forall \mathfrak{p} \in \mathcal{P}_K\}.$$

Osservazioni 3.4.

1. *Dalla definizione e dal diagramma commutativo*

$$\begin{array}{ccc} E(K) \otimes \mathbb{Q}/\mathbb{Z} & \xhookrightarrow{\kappa} & H^1(K, E_{tors}) \\ \downarrow & & \downarrow \mathrm{res}_\mathfrak{p} \\ E(K_\mathfrak{p}) \otimes \mathbb{Q}/\mathbb{Z} & \xhookrightarrow{\kappa_\mathfrak{p}} & H^1(K_\mathfrak{p}, E_{tors}), \end{array}$$

   segue immediatamente un inclusione naturale

$$E(K) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}(E/K).$$

   Lo studio del gruppo di Selmer, ed in particolare del suo rango (o, più precisamente, dello $\mathbb{Z}$-rango del suo duale di Pontrjagin), consente quindi di trovare un limite superiore per il rango di $E(K)$.
2. *Per definizione il gruppo di Tate-Shafarevich di E su K, indicato con $Ш(E/K)$ è il nucleo della mappa*

$$H^1(K, E(\overline{K})) \xrightarrow{\mathrm{res}} \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E(\overline{K_\mathfrak{p}}))$$

   (il prodotto di tutte le mappe di restrizione, notare come sia Sel *che* Ш *rappresentino le ostruzioni a dei problemi di tipo locale-globale). La mappa di coomologia*

$$\eta : H^1(K, E_{tors}) \longrightarrow H^1(K, E(\overline{K}))$$

   (indotta dall'inclusione $E_{tors} \hookrightarrow E(\overline{K})$) ha conucleo contenuto in $H^1(K, E(\overline{K})/E_{tors})$ e quest'ultimo gruppo è nullo perché $E(\overline{K})/E_{tors}$ è divisibile. Dunque η è surgettiva e si può dimostrare (o usare come definizione alternativa) che

$$\mathrm{Sel}(E/K) = \eta^{-1}(Ш(E/K)).$$

   Abbiamo una successione esatta

$$E(K) \otimes \mathbb{Q}/\mathbb{Z} \xhookrightarrow{} \mathrm{Sel}(E/K) \xrightarrow{\eta} Ш(E/K).$$

   La congettura di Birch e Swinnerton-Dyer prevede (tra le altre cose) che $Ш(E/K)$ sia finito e quindi, almeno congetturalmente, il rango del gruppo di Selmer coincide con il rango di $E(K)$.

3.2. **Dimostrazione della Proposition 8.2.** Abbiamo bisogno del seguente risultato preliminare che riguarda gli autospazi rispetto all'azione del coniugio τ.

Proposizione 3.5. [1, Proposition 8.1] *Gli autospazi* $(E(K_\lambda)/pE(K_\lambda))^\pm$ *e* $H^1(K_\lambda, E(\overline{K_\lambda}))[p]^\pm$ *sono* $\mathbb{Z}/(p)$*-spazi vettoriali di dimensione 1.*
Inoltre la dualità di Tate induce un pairing non degenere

$$(E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(K_\lambda, E(\overline{K_\lambda}))[p]^\pm \longrightarrow \mathbb{Z}/(p).$$

Dimostrazione. Abbiamo isomorfismi di $G_{K_\lambda/\mathbb{Q}_\ell}$-moduli (visti lezioni precedenti ?)

$$E(K_\lambda)[p] \simeq E(K_\lambda)/pE(K_\lambda) \quad \text{e} \quad \mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p]) \simeq H^1(K_\lambda, E(\overline{K_\lambda}))[p],$$

che valgono anche per i relativi spazi $\pm$ (visto che τ è un generatore di $G_{K_\lambda/\mathbb{Q}_\ell}$ per le ipotesi su ℓ). Il campo residuo di λ è $\mathbb{F}_{\ell^2}$. Dato che $\ell + 1 \equiv 0 \pmod p$, si ha $\mu_p \subset K_\lambda$. Però $\ell - 1 \not\equiv 0 \pmod p$ implica $\mu_p \notin \mathbb{Q}_\ell$, quindi l'azione di $G_{K_\lambda/\mathbb{Q}_\ell}$ su μ_p è per inversione, i.e. $\mu_p(K_\lambda) = \mu_p(K_\lambda)^-$. Dunque l'azione su $\mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p])$ è opposta a quella su $E(K_\lambda)[p]$.
Inoltre non è possibile avere $E(K_\lambda) = E(K_\lambda)^+$ o $E(K_\lambda) = E(K_\lambda)^-$, altrimenti il Weil pairing (compatibile con l'azione del coniugio) implicherebbe $\mu_p \subset \mathbb{Q}_\ell$. Quindi entrambi gli autospazi $E(K_\lambda)^\pm$ sono $\mathbb{Z}/(p)$-spazi vettoriali di dimensione 1.
Ne seguono gli isomorfismi

$$(E(K_\lambda)/pE(K_\lambda))^\pm \simeq E(K_\lambda)[p]^\pm \simeq \mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p])^\mp,$$

e tutti questi sono $\mathbb{Z}/(p)$-spazi vettoriali di dimensione 1.
Per l'ultima affermazione basta adesso vedere che gli autospazi relativi a diversi autovalori sono ortogonali. Questo segue immediatamente dalla compatibilità della dualità di Tate con l'azione del coniugio e dal fatto che $H^2(K_\lambda, \mu_p) \simeq \mathbb{Z}/(p)$ è un modulo banale. Dunque

$$\langle a, b\rangle_\lambda = \langle a, b\rangle_\lambda^\tau = \langle \tau(a), \tau(b)\rangle_\lambda = \langle \pm a, \mp b\rangle_\lambda = -\langle a, b\rangle_\lambda$$

implica $\langle a, b\rangle_\lambda = 0$. □

Possiamo ora concludere con la dimostrazione della [1, Proposition 8.2].

Dimostrazione. [Teorema 3.1] Prendiamo $c(\ell) \in H^1(K, E[p])$ e ricordiamo che la sua immagine in $H^1(K, E(\overline{K}))[p]$ è esattamente $d(\ell)$. Il cup product e il Weil pairing definiscono mappe

$$H^1(K, E[p]) \times H^1(K, E[p]) \xrightarrow{\cup} H^1(K, E[p] \otimes E[p]) \longrightarrow H^2(K, \mu_p) = \mathrm{Br}(K)[p].$$

Localmente questo corrisponde alla dualità di Tate

$$H^1(K_\mathfrak{p}, E[p]) \times H^1(K_\mathfrak{p}, E[p]) \xrightarrow{\langle\,,\rangle_\mathfrak{p}} H^2(K_\mathfrak{p}, \mu_p) = \mathrm{Br}(K_\mathfrak{p})[p].$$

Per calcolare $\langle d(\ell), s\rangle = \prod_\mathfrak{p} \langle d(\ell)_\mathfrak{p}, s_\mathfrak{p}\rangle_\mathfrak{p}$, ricordiamo che $s_\mathfrak{p} \in E(K_\mathfrak{p})/pE(K_\mathfrak{p})$ per definizione e che $E(K_\mathfrak{p})/pE(K_\mathfrak{p}) = E(K_\mathfrak{p})/pE(K_\mathfrak{p})^\perp$ nella dualità di Tate. Dunque, dato che due qualsiasi sollevamenti di $d(\ell)$ in $H^1(K, E[p])$ differiscono per elementi di $E(K)/pE(K)$, possiamo definire

$$\langle d(\ell)_\mathfrak{p}, s_\mathfrak{p}\rangle_\mathfrak{p} := \langle c(\ell)_\mathfrak{p}, s_\mathfrak{p}\rangle_\mathfrak{p} \quad \text{per ogni } \mathfrak{p},$$

i.e. il calcolo avviene tramite il diagramma

$$\begin{array}{ccc} H^1(K_\mathfrak{p}, E[p]) & \times & H^1(K_\mathfrak{p}, E[p]) \xrightarrow{\langle\,,\rangle_\mathfrak{p}} \mathbb{Z}/(p) \\ \downarrow \quad \nwarrow & & \uparrow \\ d(\ell)_\mathfrak{p} \in H^1(K_\mathfrak{p}, E(\overline{K_\mathfrak{p}}))[p] & & s_\mathfrak{p} \in E(K_\mathfrak{p})/pE(K_\mathfrak{p}). \end{array}$$

Dato che per ogni $\mathfrak{p} \neq \lambda$ (dove λ è l'unico primo di K sopra ℓ) si ha $d(\ell)_\mathfrak{p} = 0$ (cf. [1, Proposition 6.2]), otteniamo

$$\langle d(\ell), s\rangle = \prod_\mathfrak{p} \langle d(\ell)_\mathfrak{p}, s_\mathfrak{p}\rangle_\mathfrak{p} = \langle d(\ell)_\lambda, s_\lambda\rangle_\lambda.$$

Dal diagramma commutativo

$$\begin{array}{ccc} H^1(K,E[p])\times H^1(K,E[p]) & \xrightarrow{\langle\,,\,\rangle} & \mathrm{Br}(K)[p] \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow \\ \oplus_{\mathfrak{p}}\left(H^1(K_{\mathfrak{p}},E[p])\times H^1(K_{\mathfrak{p}},E[p])\right) & \xrightarrow{\oplus_{\mathfrak{p}}\langle\,,\,\rangle_{\mathfrak{p}}} & \oplus_{\mathfrak{p}}\mathrm{Br}(K_p)[p] \\ & & \downarrow{\scriptstyle \mathrm{inv}_K} \\ & & \mathbb{Z}/(p) \end{array}$$

e dal Teorema 2.1, ricaviamo

$$0 = \mathrm{inv}_K(\langle d(\ell), s\rangle) = \mathrm{inv}_K(\langle d(\ell)_\lambda, s_\lambda\rangle_\lambda) = \mathrm{inv}_{K_\lambda}(\langle d(\ell)_\lambda, s_\lambda\rangle_\lambda).$$

Dato che inv_{K_λ} è iniettiva, deve essere $\langle d(\ell)_\lambda, s_\lambda\rangle_\lambda = 0$. □

Meaning: dato che la dualità di Tate induce un pairing non degenere

$$H^1(K_\lambda, E(\overline{K_\lambda}))[p]^{\pm} \times (E(K_\lambda)/pE(K_\lambda))^{\pm} \longrightarrow \mathbb{Z}/(p)$$

e che i due sono spazi vettoriali di dimensione 1 su $\mathbb{Z}/(p)$ (cf. [1, Proposition 8.1]), deve essere $d(\ell)_\lambda = 0$ oppure $s_\lambda = 0$. Ma

$$d(\ell)_\lambda = 0 \iff P_1 \in pE(K_\lambda)$$

(cf. [1, Proposition 6.2]), mentre $s_\lambda = 0$ significa, per definizione,

$$s_\lambda \in pE(K_\lambda).$$

Quindi, in ogni caso si trova un p-multiplo di un punto K_λ-razionale.

References

[1] B.H. Gross *Kolyvagin's work on modular elliptic curves.*

[2] J. Neukirch *Class Field Theory - The Bonn Lectures*, edited by A. Schmidt, Springer (2013).

[3] J. Neukirch - A. Schmidt - K. Wingberg *Cohomology of number fields*, Second edition, GMW 323, Springer (2008).