Esplicitando il gruppo di Mordell-Weil della Jacobiana di una curva

Guido Lido

Per applicare il teorema di Chabauty-Coleman ad una data curva C definita su un campo di numeri K, dobbiamo verifiacare che il rango del gruppo $Jac(C)(K)$ sia strettamente minore del genere della curva C. Questo fornisce un po' di motivazione a queste note in cui ci proponiamo di dimostrare il teorema di Mordell-Weil per varietà abeliane seguendo la linea dimostrativa in [2] e descrivere dei metodi per calcolare il gruppo di Mordell-Weil di una varietà abeliana, soffermandoci sul caso delle Jacobiane di curve iperellittiche.

Il teorema di Mordell-Weil

Teorema 1 (Mordell-Weil debole)**.** *Sia K un campo di numeri, sia A una varietà abeliana definita su K e sia m un intero positivo. Allora il gruppo di $A(K)/mA(K)$ è un gruppo finito*

Dimostriamo questo teorema.

Innanzitutto guardiamo al gruppo $A(K)$ come al sottogruppo dei punti di $A(\overline{K})$ che sono invarianti rispetto a $\mathrm{Gal}(\overline{K}/K)$. In altre parole guardiamo $A(K)$ come un H^0 di Galois e utilizziamo la coomologia di Galois. Sia quindi $G = \mathrm{Gal}(\overline{K}/K)$ e consideriamo la sequenza esatta di G-moduli

$$0 \longrightarrow A[m](\overline{K}) \longrightarrow A(\overline{K}) \xrightarrow{\cdot m} A(\overline{K}) \longrightarrow 0$$

Prendendo le G-coomologie otteniamo la sequenza esatta

$$A(K) \xrightarrow{\cdot m} A(K) \xrightarrow{\delta} H^1(K, A[m]) \xrightarrow{i} H^1(K, A(\overline{K}))[m] \xrightarrow{\cdot m} H^1(K, A(\overline{K}))[m]$$

da cui deduciamo la sequenza di nostro interesse

$$0 \longrightarrow \frac{A(K)}{AJ(K)} \xrightarrow{\delta} H^1(K, A[m]) \xrightarrow{i} H^1(K, A(\overline{K}))[m] \longrightarrow 0 \qquad (1)$$

Ne deduciamo che ci basta dimostrare la finitezza di $\mathrm{Ker}\, i$ e lo faremo guardando delle proprietà locali dei cocicli in questo sottogruppo di $H^1(K, A[m])$. La sequenza 1 è vera per qualsiasi campo su cui la varietà abeliana A è definita quindi possiamo scrivere la stessa sequenza per qualsiasi campo contenente K

ed in particolare per un qualsiasi completamento K_v di K. Inoltre considerando $\mathrm{Gal}(\overline{K_v}/K_v)$ come un sottogruppo di G e considerando $A(\overline{K})$ come un sottogruppo di $A(\overline{v})$ abbiamo le naturali mappe di restrizione in coomologia che compaiono nel seguente diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{A(K)}{A(K)} & \xrightarrow{\delta} & H^1(K, A[m]) & \xrightarrow{i} & H^1(K, A(\overline{K}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}'_v} & & \\ 0 & \longrightarrow & \frac{A(K_v)}{A(K_v)} & \xrightarrow{\delta_v} & H^1(K_v, A[m]) & \xrightarrow{i_v} & H^1(K_v, A(\overline{K}_v)[m] & \longrightarrow & 0 \end{array} \tag{2}$$

La commutatività del diagramma di sopra ci dice che $\mathrm{Ker}\, i = \mathrm{Im}\, \delta$ è contenuto in $\mathrm{res}_v^{-1}(\mathrm{Ker}\, i_v) = \mathrm{res}_v^{-1}(\mathrm{Im}\, \delta_v)$. In particolare possiamo definire il *gruppo di Selmer $m-$esimo*

$$\mathrm{Sel}^{(m)}(A/K) = \{\xi \in H^1(K, A[m]) : \quad \mathrm{res}_v(\xi) \in \mathrm{Im}\, \delta_v \quad \forall v\} = \bigcap_v \mathrm{Ker}(i_v \,\mathrm{res}_v)$$

e dedurre che $\mathrm{Ker}\, i$ è contenuto nel gruppo di Selmer.

Per dimostrare la finitezza del gruppo di Selmer stimiamo la ramificazione dei cocicli di nostro interesse, ed in particolare ci serve la defininizione di "cociclo non ramificato"

Definizione. Dato L un campo completo e M un $\mathrm{Gal}(\overline{L}/L)$-modulo, diciamo che $\xi \in H^1(L, M)$ è *non ramificato* se la restrizione di ξ a $H^1(L^{unr}, M)$ è banale, dove L^{unr} è la massima estensione non ramificata di L

Definizione. Dato L un campo, v una valutazione su L e M un $\mathrm{Gal}(\overline{L}/L)$-modulo, diciamo che $\xi \in H^1(L, M)$ è *non ramificato inv* se la restrizione di ξ a $H^1(L_v, M)$ è banale.

Osservazione. La seconda definizione di non-ramificazione è ben posta in quanto non dipende dall'immersione di $\mathrm{Gal}(\overline{L_v}/L_v)$ in $\mathrm{Gal}(\overline{L}/L)$.

Osservazione. Sarebbe equivalente dire che un cociclo ξ è non ramificato in v se esiste un cociclo η che rappresenta ξ tale che $\overline{L}^{\mathrm{Ker}\,\eta}$ è un'estensione di L in cui v non ramifica.

Date queste definizioni, la finitezza del gruppo di Selmer discende dai seguenti lemmi.

Lemma 1. *Siano A, m, K come nel teorema e sia v una valutazione non-archimedea su K tale che v non divide m e A ha buona riduzione in v. Allora un cociclo $\xi \in H^1(K_v, A[m])$ è nell'immagine di δ_v se e solo se ξ non è ramificato.*

Corollario 1. *Siano A, m, K come nel teorema e sia $S = S(A, m, K) \subset M_K^0$ l'insieme delle valutazioni K tali che A ha cattiva riduzione in v oppure v divide $m \cdot \infty$. Allora il gruppo di Selmer m-esimo è contenuto nel gruppo $H^1(G, E[m], S)$ degli omomorfismi incrociati che non ramificano al di fuori di S*

Lemma 2. *Sia K un campo di numeri, G il suo gruppo di Galois assoluto, M un G-modulo finito e S un insieme finito di primi di K. Allora $H^1(G, M, S)$ è finito.*

Dimostrazione del lemma 1. Partiamo dal "solo se". Sia $F : G_v \mapsto E[m]$ un cociclo che rappresenta ξ. Ci basta dimostrare che se τ è nel gruppo di inerzia, allora $F(\tau) = 0$. Lo dimostreremo fondamendalmente con un'argomento di riduzione $\pmod v$. In particolare come notazione scriviamo $\widetilde{A}$ per indicare la riduzione della varietà abeliana e indichiamo $\widetilde{P}$ per indicare la riduzione di un punto $P \in A(\overline{K}_v)$.

Per definizione esiste un punto $P \in A(\overline{K}_v)$ tale che $F(\sigma) = \sigma(P) - P$ per ogni $\sigma \in G_v$ e consideriamo L un'estensione normale di K su cui sono definiti P e $E[m]$.

Consideriamo la riduzione $\widetilde{A}$ di A modulo v. La buona riduzione e il fatto che v non divida m implica che la mappa di riduzione $A[m] \mapsto \widetilde{A}[m]$ è una bigezione. Sia τ nel gruppo di inerzia: per definizione si ha che $\tau(P)$ è congruo a P modulo v ovvero che la riduzione di $\tau P - P$ è un punto di torsione banale su $\widetilde{A}$; per quanto appena detto sulla riduzione modulo v della m-torsione ne deduciamo che in realtà $\tau P = P$. Abbiamo dimostrato ciò che volevamo a proposito di τ e per l'arbitrarietà di τ abbiamo dimostrato la prima freccia.

Supponiamo ora che $\xi \in H^1(K_v, A[m])$ sia un cociclo non ramificato. In particolare possiamo supporre che $\xi = [\eta]$ dove η è un cociclo banale sul gruppo di inerzia. In particolare η è completamente determinato da $\eta(\Phi)$, dove Φ è un Froboenius di K_v; dunque per dimostrare che $i_v(\xi) = 0$ ci basta trovare un punto $P \in A(K_v^{unr})$ tale che $\Phi(P) - P = \eta(\Phi)$: infatti una volta trovato un tale punto si ha che η coincide con il cociclo $\sigma \mapsto \sigma(P) - P$, che è banale in $H^1(K_v, A(\overline{K}_v))$.

Per trovare un tale punto consideriamo la riduzione $\widetilde{A}$ di A e consideriamo l'omomorfismo di Froboenius $\phi : \widetilde{A} \mapsto \widetilde{A}$. La mappa algebrica $\phi - (Id) : \widetilde{A} \mapsto \widetilde{A}$ è una mappa fra varietà abeliane con Kernel finito, dunque deve essere surgettiva. In particolare esiste un punto $P_0 \in \widetilde{A}(\overline{k(v)})$ tale che $\phi(P_0) - P_0 = \widetilde{\eta(\Phi)}$; visto che $\widetilde{\eta(\Phi)}$ è di m-torsione ne deduciamo che il punto $Q_0 = [m]P_0$ è un punto $k(v)$-razionale. Prendiamo ora un punto $Q \in A(K_v)$ che si riduca a Q_0 e sia P un punto tale che $[m]P = Q$ e tale che P si riduca a P_0: allora si può verificare che un tale P è proprio quello che cercavamo. □

Dimostrazione del lemma 2. Sia m l'esponente di M. Consideriamo prima il caso in cui K contiene le radici m-esime dell'unità e l'azione di G su M è banale. In tal caso $H^1(G, M) = \mathrm{Hom}(G, M)$. Sia L la massima estensione abeliana di K di esponente m e non ramificata fuori da S: allora ogni elemento di $H^1(G, M, S)$ è banale su $\mathrm{Gal}(\overline{K}/L)$ per definizione degli oggetti in gioco. Questo dimostra che $H^1(G, M, S) \subset \mathrm{Hom}(\mathrm{Gal}(L/K), M)$ e anzi vale l'uguaglianza.Basta dimostrare che L/K è un'estensione finita di K e questa è vera per Kummer theory oppure è vera in generale. UN modo facile di dimostrarlo è fare il caso in cui O_S è un

UFD.

Trattiamo ora il caso generale. Sia K' un'estensione di K tale che $\mathrm{Gal}(\overline{K}/L)$ agisce banalmente su M e contenente le radici m-esime dell'unità. Sia $\widetilde{S}$ l'insieme dei primi in K' che stanno sopra un primo in S e consideriamo la mappa

$$H^1(\mathrm{Gal}(\overline{K}/K), M) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K'), M)$$

data dalla restrizione degli omomorfismi crociati al sottogruppo $\mathrm{Gal}(\overline{K}/K')$. Questa mappa induce

$$H^1(\mathrm{Gal}(\overline{K}/K), M, S) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K'), M, \tilde{S})$$

e il membro di destra lo conosciamo. In particolare ne deduciamo che tutti gli omomorfismi crociati a sinistra sono banali su $\mathrm{Gal}(\overline{K}/K''$ per una certa K'' estensione finita di $\tilde{K}$ e dunque estensione finita di K. Questo implica che se prendiamo la chiusura normale di K'' e la chiamiamo K''' allora $H^1(\mathrm{Gal}(\overline{K}/K), M, S)$ è un sottoinsieme dell'insieme delle mappe da $\mathrm{Gal}(K'''/K)$ in M. Questo termina. □

Il corollario 1 ed il lemma 2 implicano la finitezza del gruppo di Selmer e quindi il teorema 1. Partendo dal teorema di Mordell-Weil debole, utilizzando un argomento di altezze, si può mostrare che il *gruppo di Mordell-Weil* di una varietà Abeliana su un campo di numeri, ovvero $A(K)$, è finitamente generato. In particolare servono le seguenti definizioni.

Osservazione. Se normalizziamo che le valutazioni su $\mathbb{Q}$ in modo tale che $|p|_p = p^{-1}$ e $|10|_\infty = 10$ allora per ogni razionale q abbiamo una *formula di prodotto*

$$\prod_{v \in M_{\mathbb{Q}}} |q|_v = 1$$

Prendiamo ora K un campo di numeri e rinormalizziamo le valutazioni su K in maniera tale che, se v è una valutazione normalizzata su $\mathbb{Q}$ e w la induce su $\mathbb{Q}$ la stessa topologia, allora $w|_{\mathbb{Q}} = v^{e(w/v)}$. Allora la formula di prodotto su $\mathbb{Q}$ implica che per ogni $k \in K$

$$\prod_{v \in M_K} |k|_v = 1$$

Definizione. Dato $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ definiamo l'*altezza di Weil* di questo punto

$$h([x_0 : \cdots : x_n]) = \sum_{v \in M_L} \log(\max_i |x_i|_v)^{\frac{1}{[L:K]}}$$

La formula di prodotto su K implica che questa è una buona definizione su $\mathbb{P}^n(K)$. Dalla formula $\sum(e_i f_i) = [K : \mathbb{Q}]$ si può dedurre che queste a dimostrare che queste altezze si incollano ad una funzione altezza su $\mathbb{P}^n(\overline{Q})$.

Ora che abbiamo una nozione di "complessità" dei punti in nel proettivo possiamo affrontare il

Teorema 2 (Mordell-Weil forte)**.** *Sia K un campo di numeri e sia A una varietà abeliana definita su K. Allora il gruppo di $A(K)$ è un gruppo finitamente generato.*

La dimostrazione utilizza la seguente

Proposizione 1 (Regola del quasi-parallelogramma)**.** *Sia A una varietà abeliana definita su $\overline{\mathbb{Q}}$ e sia i un'immersione di A in $\mathbb{P}^n$ tramite un line bundle simmetrico*[1]*. Allora per ogni coppia di punti $P, Q \in A(\overline{\mathbb{Q}})$ si ha*

$$2h\big(i(P+Q)\big) + 2h\big(i(P-Q)\big) = h\big(i(2P)\big) + h\big(i(2Q)\big) + O(1)$$

dove h denota l'altezza logaritmica di Weil e $O(1)$ dipende da A.

Tralasciamo la dimostrazione della proposizione (chi vuole la può trovare nel secondo capitolo di [1]) e dedichiamoci alla dimostrazione del teorema di Mordell-Weil.

Sketch di dimostrazione del teorema 2. Iniziamo con un lemma facile. Come notazione consideriamo A fissato e indichiamo negli O la dipendenza da tutti i parametri (ad eccezione al più di A).

Lemma 3. *1. Per ogni m intero esiste C_m tale che $h(mP) \geq m^2 h(P) - C_m$ per ogni P.*

2. Per ogni Q esiste una costante C_Q tale che $h(P-Q) \leq 2h(P) + O_Q(1)$ per ogni P

La prima parte viene per induzione usando la regola del quasi-parallelogramma e la seconda utilizzando la prima parte con $m = 2$ e la regola del quasi-parallelogramma.

Fatto questo fissiamo un qualsiasi m e $G = \{P_1, \ldots, P_n\}$ un insieme di punti che rappresentano tutto $J(K)/mJ(K)$. Definiamo $C = \max\{C_{P_1}, \ldots, C_{P_n}\}$ e C_m, utlizzando le notazioni del lemma 3. Allora se $P \in A(K)$ ha altezza maggiore di $C + C_m$ esiste un punto $P' \in A(K)$ tale che $h(P') \leq \frac{3}{4}h(P)$ e tale che $P \in \langle P_1, \ldots, P_n, P' \rangle$: questo perché per definizione di G allora sappiamo che esiste un k ed un P' tale che

$$P_k - P = [m]P' \quad \Rightarrow \quad m^2 h(P') \leq C_m + h(P_k - P) = C_m + C + h(P)$$

che implica quello che vogliamo. Ne ricaviamo facilmente che l'insieme

$$\{P \in A : \quad h(P) \leq C + C_m\}$$

genera J(K), e questo insieme è finito per il teorema di Northcott. □

[1] Un line bundle L su una varietà Abeliana è detto simmetrico se $[-1]^* L = L$

Calcolabilità del gruppo di Mordell-Weil

Supponiamo che ci abbiano "dato" (in che modo?) una varietà abeliana A definita su un campo di numeri K e ci abbiano chiesto di trovare il rango di $A(K)$. Per tale scopo ci basta calcolare $A(K)/mA(K)$ e $A[m](K)$. La dimostrazione del teorema 1 ci suggerisce la seguente procedura (la notazione è quella del diagramma commutativo)

1. Fissiamo un intero positivo m e calcoliamo l'insieme S delle valutazioni che sono di cattiva riduzione per A o che dividono $m \cdot \infty$ (insomma le valutazioni del lemma 1).

2. Calcoliamo un'estensione $L \supset K$ tale che $H^1(K, A[m], S) \subset H^1(\mathrm{Gal}(L/K), A[m])$; come suggerito dalla dimostrazione del lemma 2 ci basta prendere $L_0 = K(A[m])$ e poi prendere L come la massima estesione abeliana di L_0 di esponente m e non-ramificata fuori da(ll' estensione in L_0 di) S.

3. Calcolare $H^1(K, A[m], S) \subset H^1(\mathrm{Gal}(L/K), A[m])$ (se L è quello di sopra allora c'è uguaglianza).

4. Per ogni $v \in S$ calcolare $\mathrm{Im}\,\delta_v \subset H^1(K_v, A[m])$.

5. Calcolare il gruppo di Selmer m-esimo

$$Sel^{(m)}(A/K) = \{\xi \in H^1(K, A[m], S) : \quad \mathrm{res}_v(\xi) \in \delta_v \quad \forall \quad v \in S\}$$

6. Per ogni elemento del gruppo di Selmer verificare se è nell'immagine di δ.

7. Calcolare $A[m](K)$. Infatti $A[m]$ è uno schema di dimensione zero e calcolare i suoi punti razionali è analogo a calcolare la decomposizione primaria dell'ideale che lo definisce, ce su un campo di numeri è fattibile; in modo più concreto questo si traduce nel calcolare la fattorizzazione in irriduducibili di un po' di polinomi in $K[x]$ o al più in $K'[x]$ per qualche estensione finita di $K' \supset K$.

8. Calcolare il rango r: esso è quell'intero r tale che

$$m^r = \frac{\#\,\mathrm{Im}\,\delta}{\#A[m](K)}$$

Alcuni degli step elencati spero siano sufficientemente chiari, mentre gli step 4 e 6 hanno bisogno di un' ulteriore spiegazione.

Lo step 6

Supponiamo che L sia il campo suggerito nel secondo step e supponiamo di avere in mano un cociclo $\eta \in Z^1(\mathrm{Gal}(L/K), A[m])$. Domandarsi se $[\eta]$ sia nell'immagine di δ è equivalente a domandarsi se η è un cobordo quando lo consideriamo in $Z^1(\mathrm{Gal}(L(K), A(L))$. In altre parole, per rispondere alla domanda

dello step 6 dobbiamo cercare un punto $P \in A(L)$ tale che $\sigma(P) - P = \eta(\sigma)$ per tutti gli elementi $\sigma \in \mathrm{Gal}(L/K)$; inoltre se scegliamo $\alpha_1, \ldots, \alpha_n$ di L/K e scriviamo un generico numero in L come $a_1\alpha_1 + \ldots a_n\alpha_n$ con gli $a_i \in K$ allora trovare un tale punto P corrisponde a trovare una soluzione K-razionale ad un po' di equazioni polinomiali.

Questo ragionamento si può applicare per qualsiasi estensione di campi L/K e qualsiasi cociclo η: capire se un cociclo è banale in $Z^1(\mathrm{Gal}(L(K), A(L))$ equivale a capire se una certa varietà ha un punto K-razionale. Questo si può spiegare sporcandosi meno le mani, in quanto $H^1(K, A(\overline{K}))$ parametrizza gli spazi omogenei di A, che sono dei twist di A.

In particolare, non essendo noto nessun algoritmo per determinare se una varietà algebrica su un campo di numeri, non esiste nessun algoritmo per eseguire con certezza lo step 6. Si può però sperare che la mappa δ sia surgettiva sul gruppo di Selmer m-esimo per qualche m primo eventualmente grande; allora con questa speranza possiamo sostituire lo step 6 con

6' Scegliere un bound $B >> 0$ e calcolare tutti i punti di $A(K)$ di altezza minore di B. Se l'immagine di questi punti tramite la mappa δ genera il gruppo di Semer allora siamo soddisfatti, altrimenti ricominciamo l'algoritmo da capo a con un m primo più grande ed un B più grande.

Comunque l'ipotesi che la mappa δ sia surgettiva nel Selmer n-esimo per m primo sufficientemente grande è implicata da una congettura "standard". Diamo una definizione ed enunciamo tale congettura.

Definizione. Data A una varietà su un campo di numeri K definiamo il gruppo di Tate-Shafarevich

$$(A/K) = \{\xi \in H^1(K, A(\overline{K})) : \quad \mathrm{res_v}'(\xi) = 0 \ \ \forall \ \ v\}$$

La definizione del gruppo di Selmer e l'esattezza delle righe del diagramma commutativo implicano che possiamo scrivere la seguente sequenza esatta:

$$0 \longrightarrow \frac{A(K)}{mA(K)} \xrightarrow{\delta} Sel^{(m)}(A/K) \longrightarrow (A/K)[m] \longrightarrow 0.$$

Quindi sapessimo che il gruppo di Tate-Shafarevich è finito, allora per m primo abbastanza grande $[m] = 0$ e quindi se anche B è abbastanza grande lo step 6' finisce con un successo. In particolare se è finito allora l'algoritmo descritto, a cui sostituiamo lo step 6' allo step 6, prima o poi termina dando il risultato giusto. Per questo motivo è conveniente sperare che

Congettura. *Per ogni varietà Abeliana A definita su un campo di numeri K il gruppo (A/K) è finito.*

Lo step 4

Un modo per eseguire questo step potrebbe essere il seguente: per ogni elemento $\xi \in H^1(K, A[m], S)$ e per ogni $v \in S$ controlliamo se $i_v \circ \mathrm{res}_v(\xi) = 0$. Come visto

a proposito dello step 6, controllare questa condizione equivale a testare se una certa varietà ha un punto K_v razionale: se $K_v = \mathbb{C}$ o $\mathbb{R}$ il problema si riduce al Nullstellensatz (reale), se invece v è una valutazione non-archimedea associata ad un primo P grazie al lemma di Hensel il problema si riduce a cercare punti in O_K/P^N per qualche $N >> 0$.

Alternativamente si possono calcolare punti su $A(K_v)$ e quindi la loro immagine tramite δ_v. E' di aiuto la seguente

Proposizione 2. *Sia A una varietà abeliana di dimensione g su un campo di numeri K, sia v una valutazione su K e m un'intero positivo. Allora*

- $\frac{A(K_v)}{mA(K_v)} = 1$ *se* $K_v \cong \mathbb{C}$
- $\frac{A(K_v)}{mA(K_v)} = \frac{\#A[2](K_v)}{m^g}$ *se* $K_v \cong \mathbb{R}$
- $\frac{A(K_v)}{mA(K_v)} = \#A[2](K_v) \cdot m^g$ *se v è una valutazione non archimedea che divide m.*
- $\frac{A(K_v)}{mA(K_v)} = \#A[2](K_v)$ *se v è una valutazione non archimedea che non divide m.*

Proof. Il primo caso è ovvio. Nel secondo caso $A(K_v)$ è un gruppo di Lie compatto di dimensione g, quindi ha una componente dell'identità isomorfa ad un toro complesso di dimensione g, mentre il gruppo delle componenti è un gruppo finito F. In particolare abbiamo il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S_1^g & \longrightarrow & A(K_v) & \xrightarrow{i} & F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \\ 0 & \longrightarrow & S_1^g & \longrightarrow & A(K_v) & \longrightarrow & F & \longrightarrow & 0 \end{array}$$

Applicando lo snake lemma e prendendo le cardinalità otteniamo che

$$1 = \frac{m^g \cdot F[m] \cdot \#\big(A(K_v)/mA(K_v)\big}{A[m](K_v) \cdot \#(F/mF)} = \frac{m^g \cdot \#\big(A(K_v)/mA(K_v)\big}{A[m](K_v)}$$

la cui si deduce l'uguaglianza voluta. Occupiamoci degli ultimi due casi. In questi casi non ha utilità andare a guardare le componenti connesse di $A(K_v)$, visto che è totalmente disconnesso, ma si può trovare un sottogruppo aperto di $A(K_v)$ che abbia una struttura semplice, ovvero che è isomorfo a O_K^g con la struttura di gruppo dato dall'addizione. Nel caso in cui v sia un primo di buona riduzione questo sottogruppo è il Kernel della mappa di riduzione $\pmod v$. In particolare il quoziente di $A(K_v)$ per questo sottogruppo è sempre un gruppo

finito ed otteniamo il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & O_K^g & \longrightarrow & A(K_v) & \xrightarrow{i} & F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \\ 0 & \longrightarrow & O_K^g & \longrightarrow & A(K_v) & \longrightarrow & F & \longrightarrow & 0 \end{array}$$

Come prima applicando lo snake lemma e prendendo le cardinalità otteniamo quanto voluto. □

Guardando la dimostrazione qui sopra scopriamo che, a meno di avere una descrizione esplicita del sottogruppo "semplice" di $A(K_v)$ e del gruppo quoziente F, è possibile calcolare dei generatori di $A(K_v)/mA(K_v)$. Abbiamo anche un altro modo di sfruttare la proposizione precedente per calcolare $\delta_v(A(K_v))$: cercare punti in $A(K_v)$ in maniera casuale e calcolarne la loro immagine tramite δ_v; quando la cardinalità dell'immagine trovata eguaglia il numero dato dalla proposizione allora abbiamo calcolato *tutta* l'immagine di δ_v.

Jacobiane di curve iperellittiche

Vediamo ora come semplificare i calcoli nel caso nel caso in cui la varietà Abeliana sia la Jacobiana di una curva iperellittica e $m = 2$. In questo caso, infatti il gruppo $H^1(K, A[2])$ ha una descrizione abbastanza esplicita.

Fissiamo una curva iperellittica C proiettiva di genere g definita su un campo K da un 'equazione del tipo

$$y^2 = F(x) = a_{2g+1}x^{2g+1} + \cdots + a_0$$

dove f è un polinomio libero da quadrati. Indichiamo con J la Jacobiana di C, di cui vorremmo calcolare il rango del gruppo di Mordell-Weil, o almeno il secondo gruppo di Selmer. Indichiamo inoltre con ∞ l'unico punto di C che non è nella carta affine data. Ci siamo implicitamente ristretti al caso in cui F è un polinomio di grado disparin ma si possono ottenere risultati dalla forma simile anche nel caso in cui F ha grado pari.

Definiamo l'algebra finita étale su K

$$L = K[T]/F(T)$$

ed indichiamo con $N = N_{L/K}$ la norma di L come K-algebra.

Ciò che ci interessa in questa sezione è mostrare che esiste un isomorfismo

$$\lambda : H^1(K, J[2]) \xrightarrow{\sim} \{l \in L^*(L^*)^2 : \quad N(l) = (K^*)^2\} \quad \subset \quad \frac{L^*}{(L^*)^2}$$

ed inoltre che usando questo isomorfismo la mappa delta si scrive in modo "facile", ovvero che se prendiamo un po' di punti $P = (x_i, y_i) \in C(\overline{K})$ tali che

$y_i = 0$, allora

$$\lambda \circ \delta : \frac{J(K)}{2J(K)} \mapsto \frac{L^*}{(L^*)^2} \qquad \lambda \circ \delta \left(\sum_i n_i P_i \right) = \prod_i ([x_i - T])^{n_i}$$

in particolare se consideriamo un qualsiasi punto $(x, y) \in C(K)$ con $y = 0$ allora

$$\lambda \circ \delta(P - \infty) = [x - T].$$

Questa cosa è vera per qualsiasi campo ed è anche funtoriale. In particolare nel caso in cui K è un campo di numeri possiamo riparafrasare la parte sinistra del diagramma nel seguente modo:

$$\begin{array}{ccc} \frac{J(K)}{J(K)} & \xrightarrow{\lambda \circ \delta} & \frac{L^*}{(L^*)^2} \\ \downarrow & & \downarrow \\ \frac{J(K_v)}{J(K_v)} & \xrightarrow{\lambda_v \circ \delta_v} & \frac{(L \otimes_K K_v)^*}{(L \otimes_K K_v)^{*2}} \end{array}$$

Anche la caratterizzazione del sottogruppo $H^1(K, J[2], S) \subset H^1 K, J[2]$ è semplice in quanto

$$\lambda(H^1(K, J[2], S)) = \{l \in L^*(L^*)^2 : \quad N(l) = (K^*)^2 \text{ e per ogni } v \notin S$$

$$\text{e per ogni estensione di } v \text{ a } L^* \text{ si ha } w(l) = 2\mathbb{Z}\}$$

Quindi possiamo riparafrasare tutto l'algoritmo visto nella sezione precedente, sostituendo la mappa δ con la mappa $\lambda \circ \delta$, semplificando i calcoli.

Per dimostrare l'esistenza di una tale mappa λ abbiamo bisogno di due ingredienti: il pairing di Weil ed una descrizione esplicita di $J[2]$

Il pairing di Weil

Si tratta di una mappa bilineare, antisimmetrica non-degenere e Galois-covariante $J[2] \times J[2] \mapsto \mu_2(K)$. Definiamo innanzitutto una mappa definita al livello di divisori

Definizione. Siano $D = \sum_P n_P P$ e $E = \sum_Q m_Q Q$ due divisori con di grado 0 che hanno supporto disgiunto e ordine 2 nel gruppo delle classi. Allora definiamo

$$W(D, E) = \frac{f_D(E)}{f_E(D)} = \frac{\prod_Q f_D(Q)^{m_Q}}{\prod_P f_E(P)^{n_P}}$$

dove f_D è una funzione razionale il cui divisore di zeri e poli e $2D$ e f_E è definito analogamente.

E' immediato mostrare che l 'accoppiamento fra divisori appena definito è una mappa in K^* alternante, Galois-equivariante e bilineare (nei casi in cui è definito). Inoltre la *reciprocità di Weil* implica che se $D = \operatorname{div} f$, allora $W(D, E) = 1$ e quindi la definizione di $W(\cdot, \cdot)$ passa modulo equivalenza lineare; inoltre visto che due classi di equivalenza possono essere sempre rappresentati da divisori con supporto disgiunto allora W è definito su tutto $J[2] \times J[2]$. Questo, insieme alla bilinearità implica che l'immagine di W è in $\mu_2(K)$.

La reciprocità di Weil è il seguente teorema, sulla cui dimostrazione non ci soffermiamo

Teorema. *Sia C una curva liscia e siano f, g funzioni razionali tali che* $\operatorname{div} f = \sum n_p P$ *e* $\operatorname{div} g = \sum m_Q Q$ *abbiano supporto disgiunto. Allora*

$$\prod_Q f(Q)^{m_Q} = f(\operatorname{div} g) = g(\operatorname{div} f) = \prod_P g(P)^{n_P}.$$

Inoltre l'accoppiamento di Weil è non degenere e si può dimostrare calcolandolo su dei generatori di $J[2]$ come quelli nel prossimo paragrafo.

Una descrizione di $J[2]$ e l'algebra L

Siano $\alpha_0, \ldots, \alpha_{2g}$ le radici del polinomio F e consideriamo i divisori $D_0 = (\alpha_0, 0) - \infty, \ldots, D_{2g} = (\alpha_{2g}, 0) - \infty$. Visto che $\operatorname{div}(x - \alpha_i) = 2D_i$ allora i $[D_i]$ sono punti di due torsione della Jacobiana, quindi esiste una mappa

$$\mathbb{F}_2 \cdot D_0 \oplus \cdots \oplus \mathbb{F}_2 \cdot D_{2g} \mapsto J[2] \tag{3}$$

Possiamo in realtà dimostrare che tale mappa è surgettiva e che

Proposizione 3.

$$J[2] \cong \frac{\mathbb{F}_2 \cdot D_0 \oplus \cdots \oplus \mathbb{F}_2 \cdot D_{2g}}{D_0 + \cdots + D_{2g}}$$

Proof. Visto che $\operatorname{div} y = D_0 + \cdots + D_{2g}$ allora è chiaro che nel kernel della mappa c'è questa relazione. Se dimostriamo il kernel non contiene altre relazioni allora ne deduciamo che il membro destro della proposizione si immerge in $J[2]$ e visto che entrambi hanno dimensione $2g$ su $\mathbb{F}_2$ ne deduciamo che sono isomorfi.

Supponiamo per assurdo che esista un'altra relazione, allora possiamo supporre che la relazione sia $D_0 + \cdots D_r = \operatorname{div} f$ per qualche $r < 2g$. Guardando ai poli di f scopriamo che $f = a(x) + yb(x)$ per certi polinomi a, b. Inoltre prendendo la norma otteniamo che

$$a(x)^2 - F(x)b(x)^2 = (x - \alpha_1) \cdots (x - \alpha_r)$$

e visto che F ha grado dispari, confrontando i gradi deduciamo che $b = 0$, a visto che il polinomio $(x - \alpha_1) \cdots (x - \alpha_r)$ non è un quadrato otteniamo un assurdo. Quindi non ci possono altre relazioni. □

Possiamo identificare in modo canonico $L(\overline{K})$ con l'insieme dei D_i, e questa identificazione è in realtà un'isomorfismo come moduli di Galois. Questo ci dice che $\overline{L} = L \otimes_K \overline{K}$ è identificabile con le funzioni $\{D_0, \dots, D_{2g}\} \mapsto \overline{K}$ e L è identificabile con il sottoinsiemi delle funzioni equivarianti rispetto alla naturale azione del gruppo di Galois. Questa identificazione manda una funzione ϕ nella classe di un polinomio f tale che $f(\alpha_i) = \phi(D_i)$.

Questa corrispondenza in paricolare ci dà una mappa

$$J[2] \mapsto \mu_2^{\{D_0,\dots,D_{2g}\}} \mapsto \mu_2(\overline{L})$$

$$[D] \mapsto \Big(\phi : D_i \mapsto W(D, D_i)\Big) \mapsto ...$$

Questa mappa è iniettiva per la non-degeneratezza di $W(\cdot,\cdot)$ e, visto che $[D_1 + \dots D_{2g}] = 0$, in realtà atterra negli elementi di norma 1. Per questioni di cardinalità otteniamo un isomorfismo

$$J[2] \cong \{\zeta \in \mu_2(\overline{L}) : \quad N(\zeta) = 1\}.$$

Visto che questo è un isomorfismodi moduli di Galois, abbiamo anche un'isomorfismo

$$H^1(K, J[2]) \cong H^1\big(K, \{\zeta \in \mu_2(\overline{L}) : \quad N(\zeta) = 1\}\big) \subset H^1(K, \mu_2(\overline{L})) \qquad (4)$$

Ora guardiamo la sequenza esatta di moduli di Galois

$$1 \longrightarrow \mu_2(\overline{L}) \longrightarrow \overline{L}^* \xrightarrow{\cdot 2} \overline{L}^* \longrightarrow 1$$

Prendendo la sequenza esatta lunga in coomologia e utilizzando il fatto che $H^1(K, \overline{L}^*) = 0$ (questo si può dimostrare allo stesso modo del teorema 90 di Hilbert) otteniamo che

$$H^1(K, \mu_2(\overline{L})) \cong \frac{L^*}{(L^*)^2}$$

e analogamente che

$$H^1\big(K, \{\zeta \in \mu_2(\overline{L}) : \quad N(\zeta) = 1\}\big) \cong \{l \in L^*(L^*)^2 : \quad N(l) = (K^*)^2\} \qquad (5)$$

Da (4) e (5) otteniamo l'isomorfismo λ voluto. Inoltre se scriviamo esplicitamente gli isomorfismi intermedi (sono tutti "mappe δ" in coomologia) possiamo dimostrare che $\lambda \circ \delta$ è descritta dalla formula detta.

References

[1] [Ser] Serre JP. (1997), Lectures on the Mordell-Weil Theorem. Aspects of Mathematics, vol 15. Vieweg+Teubner Verlag, Wiesbaden.

[2] [Sil] Silverman J.H. (2009), The arithmetic of elliptic curves. Vol. 106. Springer Science and Business Media.