Capítol 3

Galois theory and torsion points on curves

Bernat Plans

Introducció

Aquest capítol és la versió escrita d'una xerrada pronunciada durant el STNB 2008-2009, en la qual vam exposar alguns dels resultats (no tots!) de M. Baker, K. Ribet i A. Tamagawa continguts en [3].

L'objectiu principal és veure com aprofitar el concepte de *punts gairebé racionals* de varietats abelianes, introduït per Ribet anys enrere, per a obtenir noves demostracions de les (ex)conjectures de Manin-Mumford i de Coleman-Kaskel-Ribet.

Aquestes conjectures parlen dels punts de torsió en una corba X de gènere $g \geqslant 2$; un punt de X és "de torsió" si ho és en la jacobiana $J := Jac(X)$, via una immersió d'Albanese $X \hookrightarrow J$. Els *punts gairebé racionals* intervenen perquè, per a un punt de J, "ser gairebé racional" (respecte un cos K) és una condició genèricament necessària per tal de provenir d'un punt de X per alguna $X \hookrightarrow J$ (definida sobre K).

Amb el suport parcial de MTM2006-04895.

3.1 Punts de torsió gairebé racionals en varietats abelianes

L'objectiu d'aquesta secció és provar els Teoremes 3.1.1 i 3.1.4, que seran essencials en les demostracions de les conjectures de Manin-Mumford i de Coleman-Kaskel-Ribet, respectivament.

K sempre denotarà un *cos* i G_K el seu grup de Galois absolut $\mathrm{Gal}(\overline{K}/K)$.

Definició. Donada una varietat abeliana A/K, direm que un punt $a \in A(\overline{K})$ és *gairebé racional* si, per a tot parell $\sigma, \tau \in G_K$, es satisfà:

$$[\sigma a + \tau a = 2a \implies \sigma a = \tau a = a].$$

A partir d'ara abreujarem *gairebé racional(s)* per g.r..

Observació. El subconjunt de $A(\overline{K})$ format pels punts g.r. no és necessàriament un subgrup de $A(\overline{K})$.

3.1.1 Finitud

En tot aquest apartat suposarem que K és de *característica* 0 *amb grau de transcendència finit sobre* $\mathbb{Q}$. L'objectiu és provar el

3.1.1 Teorema. *Si A/K és una varietat abeliana, aleshores només un nombre finit de punts de torsió de $A(\overline{K})$ són g.r..*

Recordem, primer, un resultat enunciat a [18, no. 136] (veure també [18, no. 138]).

3.1.2 Teorema. (Serre) *Sigui A/K una varietat abeliana de dimensió g. Sigui $\rho : G_K \longrightarrow \mathrm{Aut}(\widehat{T}A) \cong \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$ la representació de Galois en el mòdul de Tate adèlic de A. Si $\widehat{\mathbb{Z}}^* \subset \mathrm{Aut}(\widehat{T}A)$ denota el subgrup d'homotècies, aleshores el grup $\widehat{\mathbb{Z}}^*/(\rho(G_K) \cap \widehat{\mathbb{Z}}^*)$ té exponent finit.*

Observació. Una conjectura (no provada) de Lang prediu que, de fet, aquest grup és finit.

Demostració del Teorema 3.1.1:

Sigui $a \in A(\overline{K})^{tors}$ un punt d'ordre m. Veurem que, si m és prou gran, aleshores a no pot ser g.r..

Si e denota l'exponent del grup $\widehat{\mathbb{Z}}^*/(\rho(G_K) \cap \widehat{\mathbb{Z}}^*)$, aleshores

$$((\mathbb{Z}/m\mathbb{Z})^*)^e \subset \rho_m(G_K),$$

on $\rho_m : G_K \to \mathrm{Aut}(A[m])$ és la representació en la m-torsió $A[m]$.

Per tant, donats $x, y \in (\mathbb{Z}/m\mathbb{Z})^*$, existeixen $\sigma, \tau \in G_K$ que actuen en $A[m]$ com les homotècies x^e, y^e. Així, si existeixen x, y satisfent

(i) $x^e + y^e = 2$

(ii) $x^e \neq 1 \neq y^e$,

aleshores a no pot ser g.r., donat que $\sigma a + \tau a = 2a$ i $\sigma a \neq a \neq \tau a$. Això acaba la demostració, gràcies al següent

Lema *Si m és prou gran, aleshores existeixen $x, y \in (\mathbb{Z}/m\mathbb{Z})^*$ que satisfan (i), (ii).*

Demostració: Pel Teorema xinès del residu, si λ és coprimer amb m i la conclusió és vàlida per a m, aleshores també ho és per a $m' = \lambda m$; només cal triar $x' \equiv x \pmod m$ i $y' \equiv y \pmod m$ tals que $x' \equiv y' \equiv 1 \pmod \lambda$. Per tant, és suficient provar el Lema per a $m = p^n$, amb p primer. Recordem que e està fixat.

Cas $n = 1$. Per a $p > e$, l'equació $X^e + Y^e - 2Z^e = 0$ defineix una corba projectiva sobre $\mathbb{F}_p$ que és llisa i de gènere $(e-1)(e-2)/2$. Per les fites de Weil, el nombre de punts sobre $\mathbb{F}_p$ d'aquesta corba és més gran que $p + 1 - (e-1)(e-2)\sqrt{p}$. Per tant, l'equació $x^e + y^e = 2$ té més de $(p + 1 - (e-1)(e-2)\sqrt{p} - e)$ solucions en $\mathbb{F}_p^2$. D'aquestes, menys de $(e+1)^2$ tenen x^e o y^e igual a 0 o 1. La conclusió del Lema es satisfà, doncs, per a $m = p$ prou gran.

Cas $n > 1$. Podem suposar $n > 2r+1$, on r denota la valoració p-àdica de e (això només exclou un nombre finit de casos). En particular, $n - r - 1 > 0$ i $2(n - r - 1) \geqslant n$. En aquest cas, els elements $x := 1 + p^{n-r-1}$, $y := 1 - p^{n-r-1}$ són invertibles en $(\mathbb{Z}/p^n\mathbb{Z})$ i és immediat comprovar que satisfan (i), (ii). □

3.1.2 Acció de la inèrcia en primers de reducció ordinària semiestable

En tot aquest apartat prendrem $K = \mathbb{Q}$ i suposarem/notarem:

- l és un nombre primer fixat.
- $A/\mathbb{Q}$ és una varietat abeliana.
- $I = I_l \subset G_{\mathbb{Q}}$ és "el" subgrup d'inèrcia en l.
- $I(n) := \{\sigma \in I \mid \chi(\sigma) \equiv 1 \pmod{l^n}\}$, on $\chi : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_l^*$ denota el caràcter ciclotòmic l-àdic.

El punt de partida d'aquesta secció és el següent resultat conegut:

3.1.3 Teorema. (SGA7) *Suposem que $A/\mathbb{Q}$ té reducció ordinària semiestable en l. Sigui M un sub-$\mathbb{Z}[I]$-mòdul finit de $A(\overline{\mathbb{Q}})^{tors}$.*

(a') *Si l no divideix l'ordre de M, aleshores $(\sigma-1)^2 M = 0$, $\forall \sigma \in I$.*

(b') *Sempre existeix $0 \to M' \to M \to M'' \to 0$, successió exacta de $\mathbb{Z}[I]$-mòduls, on M' és I-ciclotòmic i M'' és I-trivial.*

(c') *Si A té bona reducció en l, aleshores M_{non-l} és I-trivial.*

Remarques: 1) M_{non-l} és la part l'-primària de M; és a dir, $M = M_l \oplus M_{non-l}$ on M_l és un l-grup i M_{non-l} té ordre coprimer amb l.

2) Que M' sigui I-ciclotòmic vol dir que I actua via $\chi_{|I} : I \twoheadrightarrow \mathbb{Z}_l^*$, a través de l'acció natural de $\mathbb{Z}_l^*$ (trivial en M'_{non-l} i via $\mathbb{Z}_l^* \twoheadrightarrow (\mathbb{Z}/l^n\mathbb{Z})^*$ en M'_l, si l^n és l'exponent de M'_l).

3) (b') s'obté dels resultats de [7]. Veure la prova de [19, Prop. 2.1].

4) (a') és [7, Prop. 3.5] i es pot enunciar dient que l'acció de I en M és *unipotent de rang* 2 (quan $l \nmid \sharp M$). A més, s'obté com a conseqüència directa de (b'): $l \nmid \sharp M \Rightarrow M'$ és I-trivial (remarca 2); com que M'' és I-trivial, es té $(\sigma-1)M \subseteq M'$ i, per tant, $(\sigma-1)^2 M = 0$, $\forall \sigma \in I$.

5) (c') és [7, Cor. 2.2.9] (Criteri de Néron-Ogg-Shafarevich).

L'objectiu d'aquest apartat és combinar el Teorema 3.1.3 amb la condició "g. r.". Després, en la secció 3.3.2, ho aplicarem en situacions en les que alguna de les conclusions del Teorema 3.1.3 és certa, encara que no tinguem "reducció ordinària". Per això introduïm les

Definicions. Direm que un $\mathbb{Z}[I]$-mòdul finit M és *ordinari semiestable* (resp. *ordinari bo*) si es satisfà la conclusió de l'apartat (b') (resp. (b') i (c')) del Teorema 3.1.3.

Observació. Si M és ordinari semiestable (resp. bo), aleshores també ho és tot subquocient de M.

3.1.4 Teorema. (Tamagawa) *Sigui M un sub-$\mathbb{Z}[I]$-mòdul finit de $A(\overline{\mathbb{Q}})^{tors}$. Suposem que M és ordinari semiestable i que està generat per punts g.r..*

(a) Si l no divideix l'ordre de M, aleshores M és I-trivial.

(b) Si $l > 2$, aleshores M és $I(1)$-trivial.

(c) Si $l \geqslant 5$ i M és ordinari bo, aleshores M és I-trivial.

Observació. És immediat comprovar que els conjugats galoisians d'un punt g.r. també són g.r.. Així, si M està generat per punts g.r. com a $\mathbb{Z}[I]$-mòdul, aleshores també ho està com a $\mathbb{Z}$-mòdul.

Demostració del Teorema 3.1.4:

(a) Siguin $\sigma \in I$, $a \in M$. Per la remarca 4, que M sigui ordinari semiestable d'ordre coprimer amb l implica $(\sigma - 1)^2 a = 0$ i, per tant, $0 = \sigma^{-1}(\sigma - 1)^2 a = \sigma a + \sigma^{-1} a - 2a$. Així, si a és g.r., aleshores $\sigma a = a$. Com que estem suposant que M està generat per punts g.r., haurà de ser I-trivial.

(b) Considerem la successió exacta de (b'). Per la remarca 2, que M' sigui I-ciclotòmic (d'exponent finit) fa que sigui $I(n)$-trivial per a n prou gran. Com que M'' també és $I(n)$-trivial, obtenim $(\sigma - 1)^2 M = 0$, $\forall \sigma \in I(n)$, com a la remarca 4. Per tant, M és $I(n)$-trivial, com en la demostració de (a).

D'altra banda, $I(1)/I(n) \cong \mathbb{Z}/l^{n-1}\mathbb{Z}$ i, per tant, haurà de ser $(\sigma^{l^{n-1}} - 1)M = 0$, $\forall \sigma \in I(1)$. Com abans, $(\sigma - 1)^2 M_{non-l} = 0$ per la remarca 4. Com que $\sigma^{l^{n-1}} - 1 \equiv l^{n-1}(\sigma - 1) \pmod{(\sigma-1)^2}$, obtenim $(\sigma - 1)M_{non-l} = 0$. (No podem aplicar directament (a) perquè no sabem que M_{non-l} es pugui generar per punts g.r.; només per múltiples de punts g.r..) En resum, M_{non-l} és $I(1)$-trivial.

Suposem fixat $\sigma \in I(1)$, és a dir, $\sigma \in I$ tal que $\chi(\sigma) \equiv 1 \pmod{l}$. Volem concloure $(\sigma - 1)M = 0$.

Com que $\sigma \in I(1)$ i la restricció $\chi_{|I} : I \to \mathbb{Z}_l^*$ és exhaustiva, existeix $\tau \in I$ tal que $\chi(\sigma) + \chi(\tau) = 2$. Per força $\chi(\tau) \equiv 1 \pmod{l}$, és a dir, $\tau \in I(1)$.

Observem que, si $(\sigma + \tau - 2)M_l = 0$, aleshores $(\sigma + \tau - 2)M = 0$ perquè M_{non-l} és $I(1)$-trivial. Això implicaria $(\sigma - 1)M = 0$ perquè, per hipòtesi, M està generat per punts g.r.. Haurem acabat, doncs, si veiem $(\sigma + \tau - 2)M_l = 0$.

I actua en M a través del grup *abelià* $I/I(n)$. En particular, $(\rho - 1)(\sigma + \tau - 2)M_l = (\sigma + \tau - 2)(\rho - 1)M_l$, per a tot $\rho \in I$. Però $(\rho - 1)M_l \subseteq M_l'$, perquè M_l'' és I-trivial. A més, $(\sigma + \tau - 2)M_l' = 0$, perquè $\chi(\sigma) + \chi(\tau) = 2$ i M_l' és I-ciclotòmic. Per tant, $\forall \rho \in I$, $(\rho - 1)(\sigma + \tau - 2)M_l = 0$. És a dir, $(\sigma + \tau - 2)M_l \subseteq (M_l)^I$.

D'altra banda, $(\sigma + \tau - 2)M_l \subseteq M_l'$ perquè $(\sigma + \tau - 2)M_l'' = 0$. Així, haurà de ser $(\sigma + \tau - 2)M_l \subseteq (M_l')^I$. Però l'acció de I en M_l' és ciclotòmica (l-àdica) i, per tant, els únics elements de I que fixen un element d'ordre l són els de $I(1)$. Com que $I(1) \neq I$ (perquè $l \neq 2$) i M_l' és un l-grup, obtenim $(M_l')^I = 0$.

En resum, $(\sigma + \tau - 2)M_l = 0$ tal com volíem.

(c) Per hipòtesi, M_{non-l} és I-trivial i, per (b), M és $I(1)$-trivial.

Raonant com en la demostració de (b) veiem que, si $\sigma, \tau \in I$ satisfan $\chi(\sigma) + \chi(\tau) = 2$, aleshores $(\sigma - 1)M = 0$. Per tant, haurem acabat si $I/I(1)$ es pot generar per algun $\bar{\sigma}$ amb $\chi(\sigma) \neq 2 \pmod{l}$. Però això és clarament cert perquè $I/I(1) \cong (\mathbb{Z}/l\mathbb{Z})^*$ i estem suposant $l > 3$ (si $\bar{2}$ genera, també ho fa $\bar{2}^{-1} \neq \bar{2}$).

3.2 La (ex)conjectura de Manin-Mumford

En aquesta secció, sempre que no es digui una altra cosa, seran vàlides les següents

Hipòtesis i notacions:

- K és un cos de nombres; $G_K := \mathrm{Gal}(\overline{K}/K)$.
- X és una corba (completa, no singular i geomètricament irreductible) sobre K de gènere $g \geqslant 2$.
- J és la Jacobiana de X i $J(\overline{K})^{tors}$ és el subgrup de torsió de $J(\overline{K})$.
- $P \in X(K)$ és un punt K-racional.
- $i_P : X \to J$ és el morfisme d'Albanese (K-racional) amb punt base P, que envia $Q \in X(\overline{K})$ a la classe del divisor $(Q)-(P)$; es tracta d'una immersió tancada (per ser $g \geqslant 1$).

3.2.1 L'enunciat

Manin i Mumford van conjecturar, de forma independent, el següent resultat que Lang [8] va batejar com la *conjectura de Manin-Mumford* i que finalment Raynaud va demostrar [15].

Teorema MM. *El conjunt $i_P(X(\overline{K})) \cap J(\overline{K})^{tors}$ és finit.*

3.2.2 La demostració

Introduïm primer la següent

Definició. Un punt $Q \in X(\overline{K})$ és *excepcional* si la corba X és hiperel.líptica i Q és punt de ramificació hiperel.líptic.

Com que el conjunt de punts excepcionals és finit, el Teorema MM s'obté com a conseqüència directa del Teorema 3.1.1 i del següent resultat que, en gran part, motiva el concepte de punts g.r..

3.2.1 Lema. *Si un punt $Q \in X(\overline{K})$ no és excepcional, aleshores $i_P(Q)$ és g.r..*

DEMOSTRACIÓ: Com que P és fix per G_K, que $i_P(Q)$ NO sigui g.r. vol dir que existeixen $\sigma, \tau \in G_K$ tals que $Q \notin \{\sigma Q, \tau Q\}$ i

$$(\sigma Q) + (\tau Q) \sim 2(Q).$$

En aquest cas, existeix una funció racional $f \in \overline{K}(X)$ amb zeros en $\{\sigma Q, \tau Q\}$ i un pol doble en Q. Per tant, Q és excepcional (el morfisme no constant $f : X \to \mathbb{P}^1$ és de grau 2 i ramificat en Q). □

3.2.3 Comentaris addicionals

1. El Teorema MM diu que, quan veiem $X(\overline{K})$ dins de $J(\overline{K})$ via la immersió fixada i_P, només un nombre finit de punts de X són de torsió. Quan fem variar el punt base P, però, pot ser que obtinguem infinits *paquets de torsió* $i_P(X(\overline{K})) \cap J(\overline{K})^{tors}$ diferents (i no trivials, és a dir, amb més d'un punt). És conegut que això només pot passar per a $g \leqslant 3$ i, en qualsevol cas (sempre amb $g \geqslant 2$), existeix una fita uniforme per al cardinal de tots els paquets de torsió que només depèn de X. Cf. [2].

2. El Teorema MM és vàlid sobre qualsevol cos K finitament generat de característica 0, donat que el Teorema 3.1.1 ho és. També ho és la següent versió més general provada per Raynaud en [15]:

Teorema. *Per a qualsevol K-immersió tancada $i : X \to A$ en una K-varietat abeliana A, el conjunt $i(X(\overline{K})) \cap A(\overline{K})^{tors}$ és finit.*

Dit d'una altra manera: "dins" d'una varietat abeliana A/K, les úniques corbes X/K que es poden fer passar per infinits punts de torsió són les de gènere 1, és a dir, les traslladades de subvarietats abelianes de dimensió 1 (per un punt de torsió).

Actualment es coneixen diverses demostracions i generalitzacions d'aquest resultat que admeten $\dim X > 1$, A/K varietat semiabeliana, K qualsevol cos de característica 0, ... Veure [20] i les seves referències.

3. Una de les generalitzacions del resultat anterior és l'anomenada *Conjectura de Mordell-Lang*, conjecturada per Lang i finalment

provada per McQuillan [12]. Un cas particular d'aquesta conjectura és el següent:

Teorema. *Sigui $i : X \to A$ una K-immersió tancada en una K-varietat abeliana A. Si Γ és un subgrup finitament generat de $A(\overline{K})$ i $\Gamma' := \{a \in A(\overline{K}) \mid na \in \Gamma$ per algun $n \geqslant 1\}$ és el seu grup de divisió, aleshores el conjunt $i(X(\overline{K})) \cap \Gamma'$ és finit.*

Aquest resultat conté, a la vegada, les conjectures de Manin-Mumford i de Mordell. La primera s'obté amb $\Gamma = \{0\}$ i, per tant, $\Gamma' = A(\overline{K})^{tors}$. La segona s'obté amb $\Gamma = A(K)$ donat que, en aquest cas, $i(X(K)) = i(X(\overline{K})) \cap \Gamma \subseteq i(X(\overline{K})) \cap \Gamma'$.

3.3 La (ex)conjectura de Coleman, Kaskel i Ribet

En tota aquesta secció seran vàlides les següents

Hipòtesis i notacions:

- $X/\mathbb{Q}$ és la corba modular $X := X_0(p)$, amb p primer.
- g és el gènere de X i suposarem $g \geqslant 2$, és a dir, $p \geqslant 23$.
- $0, \infty \in X(\mathbb{Q})$ són les puntes de X.
- $J/\mathbb{Q}$ és la jacobiana $J := J_0(p)$ de X.
- $i := i_\infty : X \hookrightarrow J$ és la immersió standard cuspidal (=Albanese amb punt base $\infty \in X(\mathbb{Q})$).
- $T_\infty := i(X(\overline{\mathbb{Q}})) \cap J(\overline{\mathbb{Q}})^{tors}$.
- w_p és la involució d'Atkin-Lehner de X (permuta 0, ∞). w_p també denota l'endomorfisme induït (functor d'Albanese) en J que envia $[\sum n_i(P_i)]$ a $[\sum n_i(w_p(P_i))]$.
- g^+ és el gènere de $X^+ := X/w_p$.

3.3.1 L'enunciat

La conjectura de Coleman-Kaskel-Ribet [4], demostrada independentment per Baker [1] i Tamagawa [19], afirma:

Teorema CKR.

$$T_\infty = \begin{cases} \{i(0), i(\infty)\} & \text{si } g^+ > 0 \\ \{i(0), i(\infty)\} \cup i(\{\text{punts excepcionals}\}) & \text{si } g^+ = 0 \end{cases}$$

Comentari. Aquest resultat és una versió efectiva de la conjectura de Manin-Mumford per a $X = X_0(p)$. També es coneixen resultats efectius per a d'altres corbes X, incloent-hi les corbes de Fermat. Veure, per exemple, [1], [14], [21].

El que provarem en l'apartat 3.3.2 és:

Teorema CKRbis. *Tot punt gairebé racional de T_∞ és $\mathbb{Q}$-racional. És a dir, el conjunt de punts g.r. en T_∞ és $i(X(\mathbb{Q})) \cap J(\mathbb{Q})^{tors}$.*

Que el Teorema CKR és equivalent al Teorema CKRbis és clar pel Lema 3.2.1 i pels fets següents:

• $\underline{\{i(0), i(\infty)\} \subseteq T_\infty}$, donat que $i(0)$ és de torsió pel Teorema de Manin-Drinfel'd [6].

• $\underline{P \in X(\overline{\mathbb{Q}}) \text{ excepcional} \Rightarrow [i(P) \in T_\infty \Leftrightarrow g^+ = 0]}$.

Això és [4, Prop. 1.1] i és conseqüència de:
· Per un resultat d'Ogg [13], X hiperel.líptica $\Leftrightarrow g^+ = 0$ o bé $p = 37$.
· $g^+ = 0 \Rightarrow w_p = -1$ en J (w_p coincideix amb la inv. hiper.) $\Rightarrow w_p(i(P)) = -i(P), \forall P \in X(\overline{\mathbb{Q}})$. Però $w_p(i(P)) = i(w_p(P)) - i(0)$. Per tant, P excepcional (i $g^+ = 0$) $\Rightarrow 2i(P) = i(0) \in T_\infty \Rightarrow i(P) \in T_\infty$.
· $P \in X_0(37)(\overline{\mathbb{Q}})$ excepcional $\Rightarrow i(P)$ no és de torsió. Veure [11, §5].

• $\underline{i(X(\mathbb{Q})) \cap J(\mathbb{Q})^{tors} = \{i(0), i(\infty)\}}$.

Si $p \notin \{37, 43, 67, 163\}$, aleshores $X(\mathbb{Q}) = \{0, \infty\}$ per un resultat de Mazur [10, Thm. 7.1]. Per als quatre casos restants, veure la prova de [4, Prop. 1.2].

3.3.2 La demostració

A les hipòtesis i notacions anteriors afegim:

- Operadors de Hecke: $T_l \in \mathrm{End}(J)$
- Àlgebra de Hecke: $\mathbf{T} := \mathbb{Z}[\{T_l\}_{l \neq p}, w_p]$
- Ideal d'Eisenstein: $\mathfrak{J} := (\{T_l - (l+1)\}_{l \neq p}, w_p + 1) \subset \mathbf{T}$
- $J[\mathfrak{J}] := \{a \in J(\overline{\mathbb{Q}}) | ta = 0, \forall t \in \mathfrak{J}\}$
- $n := (p-1)/m.c.d(p-1, 12)$

La demostració del Teorema CKRbis combina el Teorema 3.1.4 amb els resultats següents.

Resultat 1. El morfisme $\mathbb{Z} \hookrightarrow \mathbf{T} \twoheadrightarrow \mathbf{T}/\mathfrak{J}$ indueix un isomorfisme $\mathbf{T}/\mathfrak{J} \cong \mathbb{Z}/n\mathbb{Z}$; el $\mathbf{T}/\mathfrak{J}$-mòdul $J[\mathfrak{J}]$ és lliure de rang 2 i, per tant, $J[\mathfrak{J}] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ com a $\mathbb{Z}$-mòduls. Cf. [9, II] i veure [3, p. 26].

Resultat 2. J té reducció ordinària semiestable en p (veure, per exemple, [3, p. 26] o [19, p. 307]). Així, pel Teorema 3.1.3 (b'), tot $\mathbb{Z}[I_p]$-submòdul finit de $J(\overline{\mathbb{Q}})^{tors}$ és ordinari semiestable.

Resultat 3. Si p divideix l'ordre d'un $\mathbf{T}[G_{\mathbb{Q}}]$-submòdul finit $\mathcal{M}$ de $J(\overline{\mathbb{Q}})^{tors}$, aleshores l'acció de I_p en $\mathcal{M}$ és *NO-abeliana*. Cf. [3, pp. 26-27].

Comentari (sobre la dem.): Tot subquocient simple del $\mathbf{T}[G_{\mathbb{Q}}]$-mòdul $J[p]$ és isomorf a un subquocient de $J[\mathfrak{m}]$, per algun ideal maximal $\mathfrak{m} \in Max(\mathbf{T})$ amb $p \in \mathfrak{m}$. Com que $p \nmid n$, $\mathfrak{m}$ és *no-Eisenstein*, i.e. no conté $\mathfrak{J}$. En aquest cas, com a representació de $G_{\mathbb{Q}}$ sobre el cos finit $\mathbf{T}/\mathfrak{m}$ (de característica p), $J[\mathfrak{m}]$ és irreductible i és isomorf a la *representació standard* $\rho_{\mathfrak{m}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbf{T}/\mathfrak{m})$. Cf. [9, Prop. 14.2].

Notem $M := J[\mathfrak{m}]$.
Pel Resultat 2, M és un $\mathbb{Z}[I_p]$-mòdul ordinari semiestable, és a dir, existeix un $\mathbb{Z}[I_p]$-submòdul M' de M tal que M' és I_p-ciclotòmic i $M'' := M/M'$ és I_p-trivial.
Fixem ara un element $\sigma \in I_p$ tal que $\chi_p(\sigma) \equiv 2 \pmod{p}$, on χ_p denota el caràcter ciclotòmic p-àdic; notem que σ existeix perquè $p \neq 2$ i $\chi_{p|I_p} : I_p \to \mathbb{Z}_p^*$ és exhaustiu. Com que p anul.la $M \subseteq J[p]$, resulta que $(\sigma - 1)$ és la identitat en M' i és 0 en M''. Així, $(\sigma - 1)M = M'$ i $(\sigma - 1)^2 = (\sigma - 1)$ en M. D'aquesta manera, com a $\mathbf{T}/\mathfrak{m}$-espai vectorial, $M = M' \oplus M^\sigma$.
Si $\rho_{\mathfrak{m}}(I_p)$ fos abelià, aleshores M^σ seria estable per I_p i, per força, isomorf a M'' com a I_p-mòdul, és a dir, trivial (i, de fet, igual a M^{I_p}). Tindríem, doncs, $M \cong M' \oplus M''$ com a $(\mathbf{T}/\mathfrak{m})[I_p]$-mòduls. Això implicaria que $\rho_{\mathfrak{m}}$ *és finita en* p en el sentit de Serre (veure [19, pp. 307-308]). És conegut, però, que $\rho_{\mathfrak{m}}$ no és finita en p quan $\mathfrak{m}$ és no-Eisenstein. Cf. [17, Prop. 2.2]. En resum, $\rho_{\mathfrak{m}}(I_p)$ és no abelià i això prova el Resultat 3.

Resultat 4. El conjunt de punts de $J(\overline{\mathbb{Q}})^{tors}$ no ramificats en p és $J[\mathfrak{J}]$. Cf. [17, Prop. 3.3].

Resultat 5. $J[\mathfrak{J}]$ admet un subgrup $G_{\mathbb{Q}}$-estable Σ tal que, com a $\mathbb{Z}[G_{\mathbb{Q}}]$-mòduls, $\Sigma \cong \mu_n$ (ciclotòmic) i $J[\mathfrak{J}]/\Sigma \cong \mathbb{Z}/n\mathbb{Z}$ (trivial). Cf. [17, Prop. 3.2]. En particular, per a tot primer l, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari semiestable.

Observació: $\Sigma := \ker(J \to J_1(p))$ és el *subgrup de Shimura* de J.
Per a n senar, el *subgrup de torsió* $C := \langle i(0) \rangle$ és un complement de Σ en $J[\mathfrak{J}]$, és a dir, $J[\mathfrak{J}] \cong \mu_n \oplus \mathbb{Z}/n\mathbb{Z}$ com a $\mathbb{Z}[G_{\mathbb{Q}}]$-mòduls.
Per a una descripció explícita del $\mathbb{Z}[G_{\mathbb{Q}}]$-mòdul $J[\mathfrak{J}]$ quan n és parell, veure [5].

Resultat 6. Per a tot primer $l \mid n$, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari bo. Veure [3, pp. 26-27].

Demostració del Teorema CKRbis:

Sigui $P \in X(\overline{\mathbb{Q}})$ i suposem/notem:

- $a := i(P) \in J(\overline{\mathbb{Q}})$ és de torsió.
- a és g.r..
- M és el $\mathbb{Z}[G_{\mathbb{Q}}]$-submòdul de $J(\overline{\mathbb{Q}})^{tors}$ generat per a.

Clarament, M és finit ($M \subseteq J[m]$ si a és d'ordre m).

Objectiu: I_l actua trivialment en M per a tot primer l. Equivalentment, $a \in J(\mathbb{Q})$.

$l = p$

Pel Resultat 2, M és ordinari semiestable com a $\mathbb{Z}[I_p]$-mòdul. Pel Teorema 3.1.4 (b), M és $I_p(1)$-trivial i, per tant, també ho és el $\mathbf{T}[G_{\mathbb{Q}}]$-mòdul $\mathcal{M}$ generat per a (els elements de $\mathbf{T}$ estan definits sobre $\mathbb{Q}$, i.e., commuten amb els de $G_{\mathbb{Q}}$). Així, I_p actua en $\mathcal{M}$ a través del grup abelià $I_p/I_p(1) \cong (\mathbb{Z}/p\mathbb{Z})^*$. Pel Resultat 3, p ha de ser coprimer amb l'ordre de $\mathcal{M}$ (i de M). Aplicant el Teorema 3.1.4 (a), concloem que I_p actua trivialment en M.

Observació: I_p també actuarà trivialment en $\mathcal{M}$. Pel Resultat 4, $\mathcal{M} \subseteq J[\mathfrak{J}]$. En particular, tot element de $\mathbf{T}$ opera en $\mathcal{M}$ com un enter (per definició de $\mathfrak{J}$) i, per tant, $M = \mathcal{M}$.

$l \nmid n, l \neq p$

Pel Resultat 5, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari semiestable i, per tant, també ho és el $\mathbb{Z}[I_l]$-submòdul $M \subseteq J[\mathfrak{J}]$. Com que l'exponent de M divideix n i estem en el cas $l \nmid n$, el Teorema 3.1.4 (a) garanteix que I_l actua trivialment en M.

$\boxed{l \mid n}$

En aquest cas, el $\mathbb{Z}[I_l]$-mòdul $J[\mathfrak{J}]$ és ordinari bo pel Resultat 6. Per tant, el $\mathbb{Z}[I_l]$-submòdul $M \subseteq J[\mathfrak{J}]$ també és ordinari bo.

Si $l \geqslant 5$, aleshores M és I_l-trivial pel Teorema 3.1.4 (c).

Si $l \in \{2, 3\}$, distingirem dos casos.

⋆ Cas $g^+ = 0$, i.e. $p \in \{23, 29, 31, 41, 47, 59, 71\}$. Tindrem algun $l \in \{2, 3\}$ tal que $l \mid n$ només si $p = 41$, $l = 2$ (i $n = 10$).

Ja hem comentat que el $\mathbb{Z}[I_2]$-mòdul M és ordinari semiestable (de fet, bo), és a dir, tenim una successió exacta de $\mathbb{Z}[I_2]$-mòduls $0 \to M' \to M \to M'' \to 0$, on M' és I_2-ciclotòmic i M'' és I_2-trivial. En la nostra situació, l'exponent de M' divideix $n = 10$ pel Resultat 1. En particular, aquest exponent no és divisible per 4 i, per tant, l'acció ciclotòmica de $I_2 = I_2(1)$ en M' també és trivial. Així, $(\sigma - 1)^2 M = 0$ per a tot $\sigma \in I_2$. Com que M es pot generar amb punts g.r., raonant com a la demostració del Teorema 3.1.4 (a) concloem que M és I_2-trivial.

⋆ Cas $g^+ > 0$. Provarem directament $P \in \{0, \infty\}$.

Considerem l'aplicació $\pi : X \to X^+ = X/w_p$ i notem $\infty^+ := \pi(0) = \pi(\infty)$ (l'única punta de X^+). Per functorialitat d'Albanese, tenim un morfisme $\pi_* : J \to J^+$ tal que $\pi_* \circ i = i^+ \circ \pi$, on $i^+ : X^+ \to J^+$ denota l'aplicació d'Albanese amb punt base ∞^+. Tenint en compte que i^+ és una immersió (perquè $g^+ > 0$), el que volem veure equival a $i(P) \in \ker(\pi_*)$.

Com que $i(P) \in J[\mathfrak{J}] \subset J[1 + w_p]$, existeix una funció racional $g \in \overline{\mathbb{Q}}(X)$ tal que $(g) = (1 + w_p)((P) - (\infty)) = (P) + (w_p(P)) - (\infty) - (0)$. Per tant, o bé $P \in \{0, \infty\}$ o bé X^+ és hiperel.líptica.

Podem suposar, doncs, que X^+ és hiperel.líptica.

Com que estem en el cas $g^+ > 0$, haurà de ser $p = 37$ (cf. [13]). En particular, $i(P) \in J[\mathfrak{J}] \subset J[n] = J[3]$.

D'altra banda, és clar que $\pi_* \circ (1 + w_p) = 2 \circ \pi_*$. Per tant, $\pi_*(i(P)) \in \pi_*(J[1 + w_p]) \subseteq J^+[2]$.

En conclusió, $i(P) \in \ker(\pi_*)$ tal com volíem.

Comentaris.
1) Al final de la demostració hem vist que $i(X(\overline{\mathbb{Q}})) \cap J[\mathfrak{J}] \subset \ker(\pi_*)$, si $g^+ > 0$. Més generalment, és cert (i també ho és quan $g_+ = 0$) que $J[\mathfrak{J}] \subset \ker(\pi_*)$. Cf. [3, p. 28].
2) Part dels arguments donats només fan servir que a pertany al conjunt $J(\overline{\mathbb{Q}})^{tors}_{g.r.} := \{\text{punts g.r. de } J(\overline{\mathbb{Q}})^{tors}\}$, però no que $a \in i(X(\overline{\mathbb{Q}}))$. Així, per exemple, hem provat que $J(\overline{\mathbb{Q}})^{tors}_{g.r.} \subset J[\mathfrak{J}]$ i que aquest conjunt és I_l-trivial per a tot $l \notin \{2,3\} \cap \{\text{divisors de } n\}$.
De fet, és conegut que $J(\overline{\mathbb{Q}})^{tors}_{g.r.} = C \oplus \Sigma[3]$, on C i Σ són els grups de torsió i de Shimura, respectivament. Cf. [16, Thm. 3]. Això estén un resultat de Mazur [9, Thm. 1], conjecturat per Ogg, que estableix $J(\mathbb{Q})^{tors} = C$.

Bibliografia

[1] *M. Baker*, Torsion points on modular curves, Invent. Math. 140 (2000), num. 3, 487–509.

[2] *M. Baker, B. Poonen*, Torsion packets on curves, Compositio Math. 127 (2001), 109–116.

[3] *M. Baker, K. Ribet*, Galois theory and torsion points on curves, J. Théor. Nombres Bordeaux 15 (2003), num. 1, 11–32.

[4] *R. Coleman, B. Kaskel, K. Ribet*, Torsion points on $X_0(N)$, in Automorphic forms, automorphic representations, and arithmetic (Fort Worth, Texas, 1996), Proc. Sympos. Pure Math. 66, Part 1, Amer. Math. Soc., Providence (1999), 27–49.

[5] *J. Csirik*, The kernel of the Eisenstein ideal, J. Number Theory 92 (2002), num. 2, 348–375.

[6] *V. Drinfel'd*, Two theorems on modular curves, Functional Anal. Appl. 7 (1973), 155–156.

[7] *A. Grothendieck*, Modèles de Néron et monodromie (Exposé IX de SGA 7), LNM 288, Springer, 1972, 313–523.

[8] *S. Lang*, Division points on curves, Ann. Mat. Pura Appl. 70 (1965), 229–234.

[9] *B. Mazur*, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[10] *B. Mazur*, Rational isogenies of prime degree, Invent. Math. 44 (1978), 129–162.

[11] *B. Mazur, P. Swinnerton-Dyer*, Arithmetic of Weil curves, Invent. Math. 25 (1974), 1–61.

[12] *M. McQuillan*, Division points on semi-abelian varieties, Invent. Math. 120 (1995), num. 1, 143–159.

[13] *A. Ogg*, Hyperelliptic modular curves, Bull. Soc. Math. France 102 (1974), 449–462.

[14] *B. Poonen*, Computing torsion points on curves, Experiment. Math. 10 (2001), num. 3, 449–465.

[15] *M. Raynaud*, Courbes sur une variété abélienne et points de torsion, Invent. Math. 71 (1983), 207–233.

[16] *K. Ribet, M. Kim*, Torsion points on modular curves and Galois theory, arXiv:math/0305281 (2003).

[17] *K. Ribet*, Torsion points on $J_0(N)$ and Galois representations, in Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math. 1716, Springer, Berlin (1999), 145–166.

[18] *J.-P. Serre*, Œuvres. Collected papers. IV (1985–1998), Springer, 2000.

[19] *A. Tamagawa*, Ramification of torsion points on curves with ordinary semistable Jacobian varieties, Duke Math. J. 106 (2001), 281–319.

[20] *P. Tzermias*, The Manin-Mumford conjecture: a brief survey, Bull. London Math. Soc. 32 (2000), num. 6, 641–652.

[21] *P. Tzermias*, Almost rational torsion points and the cuspidal torsion packet on Fermat quotient curves, Math. Res. Lett. 14 (2007), num. 1, 99–105.

Bernat Plans
Departament de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Av. Diagonal, 647, 08028 Barcelona
bernat.plans@upc.edu

NOTES DEL SEMINARI

MONOGRÀFIC SOBRE TREBALLS DE KENNETH RIBET

Barcelona 2010

19

Notes del Seminari de Teoria de Nombres
(UB-UAB-UPC)

MONOGRÀFIC SOBRE TREBALLS DE KENNETH RIBET

Edició a cura de

M. Alsina N. Vila

Amb contribucions de

X. Guitart L. Terracini B. Plans N. Freitas

M. Alsina
Dept. Matemàtica Aplicada III
E P Superior d'Enginyeria de Manresa
Universitat Politècnica de Catalunya
Agda Bases de Manresa, 61-73
08242 Manresa
montserrat.alsina@upc.edu

N. Vila
Facultat de Matemàtiques,
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
nuriavila@ub.edu

Classificació AMS
Primària: 11G18, 11F33
Secundària: 11D41, 11G05, 11G30, 14G35, 14H25, 14H52

Barcelona, 2010
Amb suport parcial de MTM2006-04895 i MTM2009-07024.
ISBN: 978-84-934244-9-7