Capítol 1

Varietats abelianes sobre Q i formes modulars

Xavier Guitart

Aquestes notes són la versió redactada d'una xerrada d'una hora dedicada a explicar l'article [Ri92]. L'objectiu de la presentació era enunciar els dos teoremes més rellevants de l'article i donar una noció de les idees que utilitza Ribet per a demostrar aquests resultats principals, fent a la vegada un sumari de la teoria necessària per tal de fer l'exposició el més autocontinguda possible. Aquest és, també, l'objectiu d'aquest text; òbviament, la millor referència per a una demostració completa, rigurosa i elegant dels resultats que descriurem (a part de molts altres) és l'article original de Ribet.

1.1 Introducció

La conjectura de Shimura-Taniyama, també coneguda com a Teorema de Modularitat des de la seva demostració completa l'any 2001, admet diversos enunciats equivalents. Per exemple, considerem $X_1(N)/\mathbf{Q}$ la corba modular associada a la classificació de parells (E,P), on E és una corba el·líptica i P és un punt de E d'ordre N. Denotem per

Amb el suport parcial de MTM2009-13060-C02-01.

$J_1(N)$ la jacobiana de $X_1(N)$. Aleshores podem enunciar Shimura-Taniyama de la manera següent:

1.1.1 Teorema *Sigui* C *una corba el·líptica definida sobre* $\mathbf{Q}$*. Aleshores existeix un morfisme exhaustiu* $J_1(N) \to C$ *definit sobre* $\mathbf{Q}$ *per a algun* $N \geqslant 1$*. És a dir,* C *és un quocient de* $J_1(N)$*.*

Una possible interpretació d'aquest enunciat és com a una caracterització de les varietats abelianes de dimensió 1 que són quocient d'alguna $J_1(N)$: són totes les corbes el·líptiques definides sobre $\mathbf{Q}$. En vista d'aquesta interpretació, dues preguntes apareixen de manera molt natural portant a possibles generalitzacions de Shimura-Taniyama en dues direccions diferents. La primera elimina la restricció de considerar quocients de dimensió 1; és a dir, ens podem preguntar per quines són les varietats abelianes sobre $\mathbf{Q}$ que apareixen com a quocient de les varietats $J_1(N)$. La segona, considera quocients no necessàriament sobre $\mathbf{Q}$; més concretament, ens podem preguntar sobre quines són les corbes el·líptiques sobre $\overline{\mathbf{Q}}$ que apareixen com a quocients de les diferents $J_1(N)_{\overline{\mathbf{Q}}}$.

A l'article [Ri92] (del qual se'n pot trobar una nova reimpressió a [Ri04]), Ribet utilitza la conjectura de Serre [Se87, 3.2.4?] sobre representacions de Galois per a donar una resposta a les dues qüestions anteriors. La resposta a la primera pregunta són unes varietats que Ribet anomenà *de tipus* GL_2, i la resposta a la segona són les corbes el·líptiques que anomenà (manllevant un terme utilitzat prèviament per Gross) $\mathbf{Q}$-*corbes*. Així doncs, Ribet demostrà que la conjectura de Serre implica els resultats següents, que són als que dediquem les seccions 1.2 i 1.3 respectivament:

1. Una varietat simple $A/\mathbf{Q}$ és quocient d'alguna $J_1(N)$ si i només si és de tipus GL_2; és a dir, si i només si la seva àlgebra d'endomorfismes $\mathbf{Q}$-definits $\mathrm{End}_{\mathbf{Q}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ és un cos de nombres de grau sobre $\mathbf{Q}$ igual a la dimensió de A.

2. Una corba el·líptica $C/\overline{\mathbf{Q}}$ és quocient d'alguna $J_1(N)_{\overline{\mathbf{Q}}}$ si i només si és una $\mathbf{Q}$-corba; és a dir, si i només si per a tot $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ la corba ${}^{\sigma}C$ és isògena a C.

Observem que en el moment en què Ribet va escriure l'article la conjectura de Serre no estava demostrada i que, per tant, aquests resultats eren conjecturals. Actualment la conjectura de Serre ja ha estat provada, amb la qual cosa 1 i 2 ja són teoremes. Conseqüentment, hem optat per enunciar-los com a tals, i no en la versió conjectural amb què apareixen a [Ri92]. Finalment, remarquem també que l'article de Ribet tingué un cert caràcter fundacional, en el sentit que arran dels seus resultats es va despertar un gran interès per a les varietats de tipus GL_2 i les $\mathbf{Q}$-corbes. Per exemple, al volum que conté [Ri04] s'hi pot trobar un recull d'articles dedicats a l'estudi d'aquestes varietats, amb especial èmfasi en la seva relació amb les formes modulars.

1.2 Varietats de tipus GL_2

Comencem definint les varietats que, com ja hem comentat, acabaran apareixent en la caracterització dels factors simples de les jacobianes de corbes modulars.

1.2.1 Definició *Una varietat abeliana $A/\mathbf{Q}$ es diu que és de tipus GL_2 si la seva àlgebra d'endomorfismes $\mathbf{Q}$-definits, $\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_{\mathbf{Q}}(A)$, és isomorfa a un cos de nombres de grau sobre $\mathbf{Q}$ igual a la dimensió de A.*

Les varietats abelianes de tipus GL_2 de dimensió 1 són les corbes el·líptiques sobre $\mathbf{Q}$. En efecte, si $C/\mathbf{Q}$ és un corba el·líptica, la seva àlgebra d'endomorfismes $\mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(C)$ és isomorfa a $\mathbf{Q}$ o a un cos quadràtic imaginari K. Observem però, que fins i tot en aquest segon cas es compleix que l'àlgebra d'endomorfismes $\mathbf{Q}$-definits $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(C)$ és isomorfa a $\mathbf{Q}$: altrament K actuaria en l'espai de vectors tangents $\mathrm{Lie}(C/\mathbf{Q})$, que té dimensió 1 sobre $\mathbf{Q}$.

Una altra font d'exemples de varietats de tipus GL_2 són les associades a formes modulars de pes 2. Sigui $f = \sum a_n q^n$ una forma modular cuspidal de pes 2 per a un subgrup de $\mathrm{SL}_2(\mathbf{Z})$ de la forma $\Gamma_1(N)$, i que és forma pròpia normalitzada pels operadors de Hecke. Aleshores una construcció de Shimura associa a f una varietat abeliana A_f de tipus GL_2. Aquesta A_f és, per construcció, un quocient de $J_1(N)$, i $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A_f)$ és isomorf a $\mathbf{Q}(\dots,a_n,\dots)$ que té grau igual a la dimensió de A_f. Per tant, $J_1(N)$ té quocients que són varietats de tipus GL_2; de fet, Ribet provà a [Ri80] el següent resultat.

1.2.2 Teorema *La varietat* $J_1(N)$ *és isògena sobre* $\mathbf{Q}$ *a un producte de varietats de la forma* A_f*.*

Així doncs, tot quocient simple de $J_1(N)$ sobre $\mathbf{Q}$ és isogen a una varietat de tipus GL_2. Un dels teoremes principals de [Ri92] és el recíproc d'aquest fet.

1.2.3 Teorema *Sigui* $A/\mathbf{Q}$ *una varietat de tipus* GL_2*. Aleshores* A *és isògena sobre* $\mathbf{Q}$ *a un factor* $\mathbf{Q}$*-simple de* $J_1(N)$ *per a algun* $N\geqslant 1$.

En la resta de secció indicarem, sense entrar en els detalls, quins són els passos que condueixen a la prova d'aquest enunciat. Els dos ingredients principals que hi intervenen són, d'una banda la conjectura de Serre, i de l'altra el teorema de la isogènia de Faltings. Abans d'enunciar la conjectura de Serre, fem un breu repàs de les representacions associades a les varietats abelianes i a les formes modulars.

Representacions associades a varietats de tipus GL_2

Sigui A una varietat abeliana de tipus GL_2 i sigui $E=\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)$. Fixem un nombre primer ℓ i sigui $T_\ell(A)=\varprojlim A[\ell^n]$ el mòdul de Tate ℓ-àdic de A; considerem també $V_\ell(A)=T_\ell(A)\otimes_{\mathbf{Z}}\mathbf{Q}$, que és un $\mathbf{Q}_\ell$-mòdul lliure de rang $2\dim A=2[E:\mathbf{Q}]$. A més, $V_\ell(A)$ és un $E\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$-mòdul lliure de rang 2, i com que E actua sobre A com endomorfismes definits sobre $\mathbf{Q}$, el grup de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ actua en $V_\ell(A)$ de manera $E\otimes\mathbf{Q}_\ell$-lineal. Això dóna lloc a la representació ℓ-àdica

$$\rho_\ell:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\longrightarrow\mathrm{Aut}_{E\otimes\mathbf{Q}_\ell}(V_\ell(A))\simeq\mathrm{GL}_2(E\otimes\mathbf{Q}_\ell).$$

En general la representació ℓ-àdica associada a una varietat abeliana pren valors en $\mathrm{GL}_{2d}(\mathbf{Q}_\ell)$, on d és la dimensió de la varietat. El fet que les varietats de tipus GL_2 tinguin com a àlgebra d'endomorfismes $\mathbf{Q}$-definits un cos de nombres de grau igual a la dimensió de la varietat fa que, tal com acabem de veure, aquesta representació es pugui pensar prenent valors a $\mathrm{GL}_2(E \otimes \mathbf{Q}_\ell)$; aquesta és l'explicació de perquè aquestes varietats s'anomenen de tipus GL_2.

L'anell $E \otimes \mathbf{Q}_\ell$ no és un cos en general, sinó un producte de cossos. Tenim que $E \otimes \mathbf{Q}_\ell \simeq \prod_{\lambda|\ell} E_\lambda$, on el producte recorre tots els primers λ de E que divideixen ℓ, i E_λ és el completat de E respecte de la topologia induïda per λ. Així doncs, per a cada primer λ de E dividint ℓ tenim una representació λ-àdica

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(E_\lambda).$$

Una propietat fonamental d'aquesta representació λ-àdica és que si p és un primer diferent de ℓ i en el qual A té bona reducció, aleshores ρ_λ és no ramificada en p. A més, si Frob_p denota un element de Frobenius per p en $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, resulta que el polinomi característic de $\rho_\lambda(\mathrm{Frob}_p)$ té coeficients a E i no depèn de λ.

Per a poder aplicar la conjectura de Serre cal considerar la reducció d'aquestes representacions. Sigui $\mathcal{O}$ l'anell d'enters de E. Sempre existeix una varietat $\mathbf{Q}$-isògena a A que té anell d'endomorfismes $\mathbf{Q}$-definits isomorf a $\mathcal{O}$. Com que l'enunciat del teorema 1.2.3 no canvia si reemplacem A per una varietat $\mathbf{Q}$-isògena, podem suposar (i suposem) que $\mathrm{End}_{\mathbf{Q}}(A) \simeq \mathcal{O}$. Així doncs, amb un argument anàleg a l'anterior podem prensar que les representacions λ-àdiques tenen coeficients a $\mathcal{O}_\lambda$:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes\mathbf{Z}_\ell}(T_\ell(A)) \simeq \mathrm{GL}_2(\mathcal{O} \otimes \mathbf{Z}_\ell) \simeq \prod_{\lambda \mid \ell} \mathrm{GL}_2(\mathcal{O}_\lambda),$$

i per tant podem reduir mòdul λ cada representació λ-àdica, obtenint una representació amb coeficients al cos finit $\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda \subseteq \overline{\mathbf{F}}_\ell$:

$$\overline{\rho}_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda) \subseteq \mathrm{GL}_2(\overline{\mathbf{F}}_\ell).$$

Representacions associades a formes modulars

Hem vist que a cada varietat abeliana de tipus GL_2 li podem associar representacions que prenen valors en $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$; tot seguit veiem que també podem associar representacions d'aquest estil a formes modulars. El resultat principal és el següent.

1.2.4 Teorema *Sigui $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ una forma pròpia pels operadors de Hecke, i sigui $E_f = \mathbf{Q}(\ldots, a_n, \ldots)$ i $\mathcal{O}_f$ l'anell d'enters d'E_f. Existeix una representació*

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_f \otimes \mathbf{Z}_\ell) \simeq \prod_{\tilde{\lambda} \mid \ell} \mathrm{GL}_2(\mathcal{O}_{f,\tilde{\lambda}})$$

associada a f, és a dir, tal que per a tot $p \nmid \ell N$ es compleix que

- *ρ_ℓ és no ramificada en p,*
- *$\mathrm{tr}(\rho_{f,\ell}(\mathrm{Frob}_p)) = a_p$,*
- *$\det \rho_{f,\ell}(\mathrm{Frob}_p) = \varepsilon(p) \cdot p^{k-1}$, on ε és el caràcter de f.*

Per a cada $\tilde{\lambda} \mid \ell$ tenim la reducció mòdul $\tilde{\lambda}$:

$$\overline{\rho}_{f,\tilde{\lambda}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_{f,\tilde{\lambda}}/\tilde{\lambda}\mathcal{O}_{f,\tilde{\lambda}}) \subseteq \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$$

que és contínua, irreductible (quasi per a tot λ) i senar.

En el cas $k = 2$, la representació no és més que l'associada a la varietat A_f pel procediment que hem descrit a 1.2. Per a pes $k \geqslant 2$ l'existència de $\rho_{f,\ell}$ fou provada per Deligne a [De71], i per a pes $k = 1$ ho fou per Deligne i Serre a [DS74].

La conjectura de Serre és en certa manera un recíproc del teorema anterior.

1.2.5 Teorema (Conjectura de Serre) *Sigui $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ una representació contínua, irreductible i senar. Aleshores existeix una forma modular $f \in S_k(\Gamma_1(N))$ i un primer $\tilde{\lambda} \subseteq \mathcal{O}_f$ tal que*

$$\rho \simeq \overline{\rho}_{f,\tilde{\lambda}}.$$

A més, la conjectura dóna una fórmula per a calcular a partir de la representació un pes $k = k(\rho)$ i un nivell $N = N(\rho)$ per a una forma f que resol el problema.

Demostració del teorema 1.2.3

Sigui $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2. Per a poder aplicar la conjectura de Serre a les representacions $\overline{\rho}_\lambda$, Ribet prova que $\overline{\rho}_\lambda$ és senar i absolutament irreductible quasi per a tot λ. Per a aquests λ la conjectura de Serre implica doncs que $\overline{\rho}_\lambda$ és modular. Així doncs, existeixen enters k_λ i N_λ, una forma modular $f_\lambda \in S_{k_\lambda}(N_\lambda)$ i un primer $\tilde{\lambda}$ de $\mathcal{O}_{f_\lambda}$ tal que

$$\overline{\rho}_\lambda \simeq \overline{\rho}_{f_\lambda,\tilde{\lambda}}.$$

El que es vol demostrar és que existeix una forma f de pes 2 tal que A és $\mathbf{Q}$-isògena a A_f. El següent pas que fa Ribet és trobar una forma f candidata a complir que A_f sigui isògena a A. Per a fer-ho, considera Λ el conjunt *infinit* de primers λ tals que $\overline{\rho}_\lambda$ és absolutament irreductible i tals que A té bona reducció en el primer racional que hi ha per sota de λ. Per a tot primer $\lambda \in \Lambda$, es té que $k_\lambda = 2$; això ho dedueix de certes propietats del determinant de $\overline{\rho}_\lambda$ que ha demostrat prèviament, i que li permeten aplicar un teorema de Serre que directament implica $k_\lambda = 2$. En segon lloc, els nivells N_λ estan acotats quan λ recorre Λ. Això és perquè en la definició de N_λ que apareix en la conjectura de Serre s'observa que N_λ divideix el conductor de ρ_λ, i aquest és un divisor del conductor de ρ_ℓ; però el conductor de ρ_ℓ no depèn de ℓ (i és per definició el conductor de A). Com que k_λ sempre és igual a 2 i hi ha un nombre finit de possibles N_λ, es dedueix que hi ha un nombre finit de formes modulars de pes 2 que donen lloc a infinites representacions ρ_λ. Per tant, existeix almenys una forma f de pes 2 que dóna lloc a infinites de les ρ_λ. Aquesta és la forma f candidata, i ara només falta provar que A_f és isògena sobre $\mathbf{Q}$ a A. És en aquest punt on apareix el segon ingredient important de la demostració, el teorema de la isogènia de Faltings.

Sigui $B/\mathbf{Q}$ una varietat abeliana i fixem ℓ un primer de bona reducció; si $p \neq \ell$ és un primer de bona reducció aleshores denotem per $L_p(B,s) = \det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(B))^{-1}$ el factor local en p de la seva L-sèrie.

1.2.6 Teorema (Faltings) *Dues varietats abelianes $B/\mathbf{Q}$ i $C/\mathbf{Q}$ són isògenes sobre $\mathbf{Q}$ si i només si $L_p(B,s) = L_p(C,s)$ quasi per a tot primer p.*

Continuant amb la demostració, veiem ara que A i A_f són $\mathbf{Q}$-isògenes. Sigui $\lambda \in \Lambda$ i p un primer de bona reducció de A. Sabem que existeix un primer $\tilde{\lambda}$ de $\mathcal{O}_\lambda$ tal que $\overline{\rho}_\lambda \simeq \overline{\rho}_{A_f,\tilde{\lambda}}$. En particular, el polinomi característic de $\overline{\rho}_\lambda(\mathrm{Frob}_p)$, que és

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A)) \bmod \lambda, \tag{1.1}$$

coincideix amb el polinomi característic de $\overline{\rho}_{A_f,\tilde{\lambda}}(\mathrm{Frob}_p)$, que és

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f)) \bmod \tilde{\lambda}. \tag{1.2}$$

Podem pensar que els polinomis $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A))$ i $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A_f))$ tenen coeficients a la composició $E \cdot E_f$. La igualtat entre (1.1) i (1.2) implica que existeix un primer λ' de $E \cdot E_f$ que divideix λ i tal que

$$\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A)) \equiv \det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A_f)) \mod \lambda'.$$

Com que aquest raonament és vàlid per a tot $\lambda \in \Lambda$, veiem que $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A))$ i $\det(1-p^{-s}\cdot\mathrm{Frob_p} \mid T_\ell(A_f))$ són congruents mòdul *infinits* primers. Però dos polinomis amb coeficients en un cos de nombres que són congruents mòdul infinits primers necessàriament són iguals, i per tant

$$\det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A)) = \det(1 - p^{-s} \cdot \mathrm{Frob_p} \mid T_\ell(A_f)).$$

En definitiva, hem vist que $L_p(A,s) = L_p(A_f,s)$ quasi per a tot p, i pel teorema de Faltings això implica que A i A_f efectivament són $\mathbf{Q}$-isògenes.

1.3 Q-corbes

En aquesta secció descriurem la caracterització dels quocients de dimensió 1 del conjunt de varietats de la forma $J_1(N)_{\overline{\mathbf{Q}}}$.

1.3.1 Definició *Una corba el·líptica $C/\overline{\mathbf{Q}}$ és una $\mathbf{Q}$-corba si és isògena a cadascuna de les seves conjugades de Galois ${}^\sigma C$ amb $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.*

El segon teorema principal de l'article de Ribet és el següent.

1.3.2 Teorema *Una corba el·líptica $C/\overline{\mathbf{Q}}$ és un quocient de $J_1(N)_{\overline{\mathbf{Q}}}$ per a algun $N \geqslant 1$ si i només si C és una $\mathbf{Q}$-corba.*

Fixem-nos que gràcies als teoremes 1.2.2 i 1.2.3 n'hi ha prou amb caracteritzar els quocients de dimensió 1 sobre $\overline{\mathbf{Q}}$ de les varietats de tipus GL_2. I encara més, gràcies al resultat següent de Shimura n'hi ha prou amb considerar varietats de tipus GL_2 sense CM (multiplicació complexa).

1.3.3 Teorema (Shimura) *Sigui $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2 i suposem que $A_{\overline{\mathbf{Q}}}$ té alguna subvarietat amb CM. Aleshores $A_{\overline{\mathbf{Q}}}$ és isògena a una potència d'una corba el·líptica amb CM.*

És un fet conegut que les corbes el·líptiques amb CM són $\mathbf{Q}$-corbes, i a més Shimura també havia demostrat que tota corba el·líptica amb CM és quocient d'alguna $J_1(N)_{\overline{\mathbf{Q}}}$. Així doncs, el resultat que de fet va provar Ribet a [Ri92] i que implica el teorema 1.3.2 és el següent.

1.3.4 Teorema *Una corba el·líptica $C/\overline{\mathbf{Q}}$ sense CM és un quocient d'una varietat de tipus GL_2 si i només si C és una $\mathbf{Q}$-corba.*

En el que queda de secció indicarem els passos principals que duen a la demostració de 1.3.4. Notem que 1.3.2 era conjectural en el moment en què Ribet publicà l'article (ja que 1.2.3 depenia de la conjectura de Serre), però en canvi 1.3.4 no era conjectural, sinó un teorema pròpiament dit.

Prenem $A/\mathbf{Q}$ una varietat abeliana de tipus GL_2 i sigui E la seva àlgebra d'endomorfismes $\mathbf{Q}$-definits. Una de les implicacions de 1.3.4 es dedueix de la següent

1.3.5 Proposició *Si $A_{\overline{\mathbf{Q}}}$ no té cap subvarietat amb CM, aleshores $A_{\overline{\mathbf{Q}}}$ és isògena a la potència d'una varietat $\overline{\mathbf{Q}}$-simple.*

PROVA: En principi sabem que $A_{\overline{\mathbf{Q}}}$ té una descomposició en producte de varietats absolutament simples de la forma $A_{\overline{\mathbf{Q}}} \sim B_1^{n_1} \times \cdots \times B_r^{n_r}$. Com que E és un cos que actua en $A_{\overline{\mathbf{Q}}}$, de fet actua en cada factor $B_i^{n_i}$, i per tant actua en $H_1(B_i^{n_i}(\mathbf{C}),\mathbf{Q})$ que és un $\mathbf{Q}$-espai vectorial de dimensió $2\dim B_i^{n_i}$. Així doncs $[E:\mathbf{Q}]$ ha de dividir $2\dim B_i^{n_i}$. Però d'altra banda $[E:\mathbf{Q}] = \dim(A) \geqslant \dim B_i^{n_i}$, i això només deixa lloc a dues opcions: o bé $[E:\mathbf{Q}] = \dim B_i^{n_i}$ o bé $[E:\mathbf{Q}] = 2\dim B_i^{n_i}$. Aquesta darrera no és possible, ja que aleshores $A_{\overline{\mathbf{Q}}}$ tindria una subvarietat amb CM. Per tant ha de ser $[E:\mathbf{Q}] = \dim B_i^{n_i}$, la qual cosa implica que $\dim(A) = \dim(B_i^{n_i})$ i per tant $A_{\overline{\mathbf{Q}}} \sim B_i^{n_i}$. □

Si una corba el·líptica $C/\overline{\mathbf{Q}}$ és un quocient de $A_{\overline{\mathbf{Q}}}$, necessàriament la descomposició de $A_{\overline{\mathbf{Q}}}$ és doncs de la forma $A_{\overline{\mathbf{Q}}} \sim C^n$. Per $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ tenim que ${}^\sigma C^n \sim {}^\sigma A_{\overline{\mathbf{Q}}} = A_{\overline{\mathbf{Q}}} \sim C^n$. Ara, per la unicitat de la descomposició de varietats abelianes com a producte de varietats simples forçosament ${}^\sigma C \sim C$, amb la qual cosa veiem que C és una $\mathbf{Q}$-corba.

Veiem ara com es prova l'altra implicació de 1.3.4. Sigui doncs $C/\overline{\mathbf{Q}}$ una $\mathbf{Q}$-corba sense multiplicació complexa. Hem de veure que existeix una varietat abeliana $A/\mathbf{Q}$ de tipus GL_2 tal que $A_{\overline{\mathbf{Q}}} \sim C^n$. En particular, si això és cert, una certa potència de C serà de fet isògena a una varietat definida sobre $\mathbf{Q}$. El problema d'identificar quan una varietat sobre $\overline{\mathbf{Q}}$ és isògena a una varietat definida sobre $\mathbf{Q}$, és anàleg al problema de descens del cos de definició de varietats algebraiques. La solució d'aquest problema per al cas de varietats algebraiques quasiprojectives és un teorema clàssic de Weil.

1.3.6 Teorema (Teorema del descens de Weil) *Sigui L/K una extensió de de Galois i B/L una varietat algebraica quasiprojectiva. Existeix una varietat A/K isomorfa a B sobre L si i només si per a tot $\sigma \in \mathrm{Gal}(L/K)$ existeix un isomorfisme $\phi_\sigma : {}^\sigma B \to B$ i es satisfà que*

$$\phi_\sigma \circ {}^\sigma\phi_\tau \circ \phi_{\sigma\tau}^{-1} = 1.$$

Ribet prova, com un dels passos en la seva demostració de 1.3.4, l'anàleg d'aquest teorema en la categoria de varietats abelianes llevat d'isogènia, i de fet l'enuncia a [Ri92, teorema 8.2] de la forma següent.

1.3.7 Teorema *Sigui B/L una varietat abeliana. Existeix una varietat A/K isògena a B sobre L si i només si per a tot $\sigma \in \mathrm{Gal}(L/K)$*

existeix un isomorfisme de la categoria de varietats abelianes llevat d'isogènia $\nu_\sigma : {}^\sigma B \to B$ i es satisfà que

$$\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} = 1.$$

Per a cada $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, sigui $\mu_\sigma : {}^\sigma C \to C$ una isogènia, que sabem que existeix pel fet que C és **Q**-corba. Per a cada parella d'elements $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ la composició $\mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ és un element no nul de $\mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(C) \simeq \mathbf{Q}$ (aquest isomorfisme és degut a que estem suposant que C no té CM). Una senzilla comprovació ens mostra que l'aplicació

$$\begin{array}{rccl} c: & \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \times \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) & \longrightarrow & \mathbf{Q}^\times \\ & (\sigma, \tau) & \longmapsto & c(\sigma,\tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} \end{array}$$

satisfà la condició de 2-cocicle (considerant $\mathbf{Q}^\times$ com un $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-mòdul amb l'acció trivial). La seva classe de cohomologia $[c]$ és un element de $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{Q}^\times)$ que no depèn de la classe d'isogènia de C, i 1.3.7 ens diu que C és isògena a una varietat definida sobre **Q** si i només si $[c] = 1$. En general $[c] \neq 1$, però recordem que el que cal veure no és que C és isògena a una varietat definida sobre **Q**, sinó que una certa potència de C ho és. El punt clau per a veure-ho és el teorema següent:

1.3.8 Teorema (Tate) *Si considerem $\overline{\mathbf{Q}}^\times$ com un $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-mòdul amb l'acció trivial, aleshores $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \overline{\mathbf{Q}}^\times) = \{1\}$.*

Per tant, la imatge de $[c]$ en $H^2(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \overline{\mathbf{Q}}^\times)$ és trivial; és a dir, existeix una aplicació contínua $\alpha : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{Q}}^\times$ tal que

$$c(\sigma, \tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}.$$

Sigui E el cos que obtenim adjuntant a **Q** els valors de α. Observem que $E/\mathbf{Q}$ és finita ja que α és contínua, i posem $n = [E : \mathbf{Q}]$. Fixant una immersió

$$E \hookrightarrow \mathrm{M}_n(\mathbf{Q}) \simeq \mathbf{Q} \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(C^n)$$

podem identificar els $\alpha(\sigma)$ amb endomorfismes de C^n llevat d'isogènia. Denotem per $\hat{\mu}_\sigma$ la isogènia ${}^\sigma C^n \to C^n$ que és μ_σ en cada coordenada, i definim $\nu_\sigma = \alpha(\sigma)\circ\mu_\sigma \in \mathbf{Q}\otimes \mathrm{Hom}_{\overline{\mathbf{Q}}}({}^\sigma C^n, C^n)$. El càlcul

$$\begin{aligned}\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} &= \alpha(\sigma)^{-1}\circ\hat{\mu}_\sigma\circ{}^\sigma\alpha(\tau)^{-1}\circ{}^\sigma\hat{\mu}_\tau\circ\hat{\mu}_{\sigma\tau}^{-1}\circ\alpha(\sigma\tau)\\ &= \alpha(\sigma)^{-1}\circ\alpha(\tau)^{-1}\circ\alpha(\sigma\tau)\circ\hat{\mu}_\sigma\circ{}^\sigma\hat{\mu}_\tau\circ\hat{\mu}_{\sigma\tau}^{-1}\\ &= c(\sigma,\tau)^{-1}\circ c(\sigma,\tau) = 1,\end{aligned}$$

juntament amb 1.3.7 ens diu que existeix una varietat abeliana $A/\mathbf{Q}$ definida sobre $\mathbf{Q}$ tal que $A_{\overline{\mathbf{Q}}} \sim C^n$. Així doncs, hi ha un isomorfisme

$$\mathbf{Q}\otimes\mathrm{End}_{\overline{\mathbf{Q}}}(A) \simeq \mathrm{M}_n(\mathbf{Q}).$$

Amb una versió una mica més refinada de 1.3.7 es pot veure que sota aquest isomorfisme, si $\varphi \in \mathbf{Q}\otimes\mathrm{End}_{\overline{\mathbf{Q}}}(A)$ es correspon amb una matriu $X \in \mathrm{M}_n(\mathbf{Q})$, aleshores ${}^\sigma\varphi$ es correspon amb la matriu $\alpha(\sigma)X\alpha(\sigma)^{-1}$ (on identifiquem $\alpha(\sigma)$ amb una matriu via la immersió $E \hookrightarrow \mathrm{M}_n(\mathbf{Q})$). Els elements φ de $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)$ són aquells que ${}^\sigma\varphi = \varphi$, i per tant es corresponen amb les matrius X tals que $\alpha(\sigma)X\alpha(\sigma)^{-1} = X$. Com que les matrius $\alpha(\sigma)$ generen la imatge de E dins $\mathrm{M}_n(\mathbf{Q})$, això ens diu que $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A)$ es correspon amb el centralitzador de E en $\mathrm{M}_n(\mathbf{Q})$. Com que $[E:\mathbf{Q}] = n$ i $\mathrm{M}_n(\mathbf{Q})$ és una $\mathbf{Q}$-àlgebra central simple de dimensió n^2 sobre $\mathbf{Q}$, resulta que E és un subcòs maximal de $\mathrm{M}_n(\mathbf{Q})$ i és el seu propi centralitzador. Per tant $\mathbf{Q}\otimes\mathrm{End}_{\mathbf{Q}}(A) \simeq E$, i la igualtat $[E:\mathbf{Q}] = n = \dim A$ ens diu que efectivament A és de tipus GL_2.

Bibliografia

[De71] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki, Lecture Notes in Math., vol. 355, 1971, pp. 136–172.

[DS74] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) 7 (1974), 507–530 (1975).

[Ri92] K. A. Ribet, *Abelian varieties over Q and modular forms.* Algebra and topology 1992 (Taejo(n), 53–79, Korea Adv. Inst. Sci. Tech., Taejo(n, 1992.

[Ri04] K. A. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms.* Modular curves and abelian varieties, 241–261, Progr. Math., 224, Birkhäuser, Basel, 2004. Edited by J. Cremona, J.-C. Lario, J. Quer and K. Ribet.

[Ri80] K. A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

[Se87] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J., 54 (1987), 179–230.

Xavier Guitart
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Jordi Girona 1-3, 08034 Barcelona
xevi.guitart@gmail.com

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