NOTES DEL SEMINARI

Representacions de Galois de dimensió 2:
Conjectures d’Artin, de Serre i de Fontaine-Mazur

Barcelona 2005

11

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

Comitè editorial
P. Bayer E. Nart J. Quer

Representacions de Galois de dimensió 2:
Conjectures d'Artin, de Serre i de Fontaine-Mazur

Edició a cura de

L.V. Dieulefait, N. Vila

Amb contribucions de

A. Arenas   F. Bars   P. Bayer   L.V. Dieulefait
J. Fernández   J. Quer   V. Rotger   N. Vila

L. V. Dieulefait, N. Vila
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
08007 Barcelona
Espanya

Comitè editorial

P. Bayer
Fac. de Matemàtiques
Univ. de Barcelona
Gran Via de les Corts
Catalanes, 585
08007 Barcelona
Espanya

E. Nart
Dep. de Matemàtiques
Edifici C
Univ. Autònoma de
Barcelona
08193 Bellaterra
Espanya

J. Quer
Fac. de Matemàtiques
i Informàtica
Univ. Politècnica de
Catalunya
Pau Gargallo, 5
08228 Barcelona
Espanya

Classificació AMS
Primària: 11F80, 11F11, 14K15
Secundària: 11F41, 11G40

Barcelona, 2005
Amb suport parcial de MCYT BFM2003-01898

ISBN: 84-934244-1-2

Índex

Introducció

Aquestes notes contenen les exposicions sobre el tema: *Representacions de Galois de dimensió 2: Conjectures d'Artin, de Serre i de Fontaine-Mazur*, corresponents a la divuitena edició del SEMINARI DE TEORIA DE NOMBRES (UB-UAB-UPC), celebrat a Barcelona del 19 al 23 de gener de 2004. El programa general d'aquest tema va ser elaborat per L. Dieulefait i N. Vila, i les exposicions van ser presentades per persones del seminari. La seva gentilesa en fer-nos arribar el contingut de les exposicions ha fet possible l'edició del present volum.

L'objectiu d'aquest tema va ser conèixer l'estat actual de les conjectures d'Artin, de Serre i de Fontaine-Mazur i copsar les idees i tècniques més importants que han permès els avenços espectaculars produïts els darrers anys. Si bé les representacions de Galois complexes, ℓ-àdiques i mòdul p, així com les conjectures d'Artin i de Serre, han estat tractades i estudiades en diverses edicions de l'STNB, es dedica els tres primers capítols a presentar cada una de les conjectures, donar breument el llenguatge necessari per plantejar-les i presentar alguns resultats previs sobre elles. El quart capítol està dedicat a explicar l'estratègia fonamental que ha permès els avenços recents, la qual té l'origen en els treballs de Wiles i Taylor-Wiles, que van conduir a la prova de la conjectura de Shimura-Taniyama-Weil. Recentment, Taylor ha explotat i exportat aquesta estratègia en situacions més generals. En els dos capítols següents s'entrarà en els treballs de Taylor relatius a la conjectura de Fontaine-Mazur (dimensió 2 i cristal·lina) on s'obté un resultat sobre modularitat potencial de representacions de Galois ℓ-àdiques que té importants conseqüències i corol·laris. En el setè capítol es presenten resultats relatius a les proves de la conjectura de Serre sobre cossos petits: $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$ i $\mathbb{F}_9$. El darrer capítol es dedica a la conjectura d'Artin en el cas icosaèdric.

L. Dieulefait i N. Vila

Barcelona, 15 de gener de 2005.

Capítol 1

La conjectura d'Artin

Núria Vila

En aquest capítol introduirem la funció L d'Artin associada a una representació de Galois complexa, donarem les seves propietats fonamental i formularem la conjectura d'Artin. Definirem la funció L d'Artin estesa, veurem la seva meromorfia i donarem la seva equació funcional. Centrat-nos en representacions de Galois complexes dos dimensionals estudiarem el seu caràcter modular i donarem les idees clau en la prova de la conjectura d'Artin per aquestes representacions en els casos cíclic, dièdric, tetraèdric i octaèdric.

1.1 Representacions de Galois

Sigui K un cos de nombres, $\overline{K}$ una clausura galoisiana de K i $G_K = \mathrm{Gal}(\overline{K}/K)$ el grup de Galois absolut de K. Una **representació de Galois** és un morfisme continu

$$\rho : G_K \longrightarrow \mathrm{GL}(V) = \mathrm{GL}(n, F),$$

Amb el suport parcial de MCYT BFM2003-01898.

on F és un cos topològic i V és un F-espai vectorial de dimensió n. Considerem G_K com a grup topològic amb la topologia de Krull, segons el cos topològic F tenim:

a) Representacions complexes: $F = \mathbb{C}$ amb la topologia discreta.

b) Representacions mòdul p: $F = \overline{\mathbb{F}}_p$ o $\mathbb{F}_q$, cos finit, amb la topologia discreta.

c) Representacions ℓ-àdiques: $F = \mathbb{Q}_\ell$ o una extensió finita de $\mathbb{Q}_\ell$ amb la topologia ℓ-àdica.

En els casos a) i b) tenim

ρ continua $\Leftrightarrow$ $\mathrm{Ker}(\rho)$ obert $\Leftrightarrow$ $\mathrm{Ker}(\rho) \lhd G_K$ d'index finit $\Leftrightarrow$ $\mathrm{Im}(\rho) \simeq \mathrm{Gal}(\overline{K}^{\ker\rho}/K)$ finita.

Així, en aquests casos, una representació de Galois ρ és, de fet, una representació d'un grup finit, doncs factoritza a traves del seu nucli. És a dir, la representació ρ es realitza en una extensió de Galois finita del cos K, tenim:

$$\rho : G(N/K) \longrightarrow \mathrm{GL}(V) = \mathrm{GL}(n, F),$$

on $N = \overline{K}^{\ker\rho}$.

1.2 Funció L d'Artin d'una representació de Galois complexa

Sigui

$$\rho : G_K \longrightarrow \mathrm{GL}(V) = \mathrm{GL}(n, \mathbb{C}),$$

una representació de Galois complexa. Com hem comentat, podem pensar que ρ és una representació d'un grup finit, per tant es tracta d'una representació lineal semisimple, tal que el caràcter traça

$$\chi = \chi_\rho = \mathrm{tr}\,\rho$$

individua la representació ρ.

Si v és un primer (finit) de K i $\overline{v}$ un primer de $\overline{K}$ sobre v, denotem per $G_{\overline{v}}$ i per $I_{\overline{v}}$ els grups de descomposició i d'inèrcia de $\overline{v}$. Denotem per $\mathrm{Frob}_{\overline{v}}$ l'automorfisme de Frobenius de $G_{\overline{v}}/I_{\overline{v}}$ i per Frob_v qualsevol dels $\mathrm{Frob}_{\overline{v}}$ per a $\overline{v}|v$. Notem que tots ells són conjugats. Sigui q_v el cardinal del cos residual a v. Per cada primer v, el quocient $G_{\overline{v}}/I_{\overline{v}}$ actua sobre $V^{I_{\overline{v}}}$. Notem que el polinomi característic de l'endomorfisme $\mathrm{Frob}_{\overline{v}}$ de $V^{I_{\overline{v}}}$ només depèn del primer v. Si v és un primer arquimedià (infinit) i $\overline{v}$ un primer de $\overline{K}$ sobre v, posem $G_{\overline{v}} = \{1\}$, si són tots dos reals o tots dos complexos; si v és real i $\overline{v}$ complex, posem $G_{\overline{v}} = I_{\overline{v}}$ el grup d'ordre 2, generat per l'unic element $\mathrm{Frob}_{\overline{v}} \in G_K$ (conjugació complexa) que canvia els dues immersions complexes corresponents a $\overline{v}$.

Amb aquestes notacions, definim **la funció L d'Artin** de ρ com el producte d'Euler:

$$L(\chi, s) := \prod_v L_v(\chi, s),$$

on

$$L_v(\chi, s) := \det(1 - \mathrm{Frob}_{\overline{v}}\, q_v^{-s} | V^{I_{\overline{v}}})^{-1},$$

és el factor d'Euler a v, per a cada primer v de K.

Notem que el grau del factor $L_v(\chi, s)$ com a polinomi en q_v^{-s} és la dimensió de $V^{I_{\overline{v}}}$. Així, per a quasi tot primer v, aquest grau és el grau de la representació ρ, doncs $V^{I_{\overline{v}}} = V$.

1.2.1 Propietats de la funció L d'Artin

Enunciem a continuació les primeres propietats de la funció L d'Artin. Per a la demostració d'aquestes propietats podeu confrontar, per exemple, [Ne 99].

1. La funció L d'Artin és una **funció analítica** en el semiplà $\mathrm{Re}(s) > 1$: convergeix absolutament i uniformement en el semiplà $\mathrm{Re}(s) \geq 1 + \delta$, per a tot $\delta > 0$.

2. La funció L d'Artin de la representació trivial és la funció **zeta de Dedekind**

$$L(1,s) = \zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}.$$

3. **Additivitat:** Si χ_1, χ_2 són els caràcters de dues representacions de G_K, es té

$$L(\chi_1+\chi_2,s) = L(\chi_1,s)L(\chi_2,s).$$

4. **Inducció:** Si $K \subset K'$, χ és el caràcter d'una representació de $H = G_{K'} \subset G = G_K$ i $\chi^* = \mathrm{Ind}_H^G \chi$ és el caràcter induït, es té

$$L(\chi^*,s) = L(\chi,s).$$

5. **Inflació:** Si χ és el caràcter d'una representació de $\mathrm{Gal}(N/K)$, $N' \supset N \supset K$ amb $N' \supset K$ de Galois i χ' és el caràcter de $\mathrm{Gal}(N'/K)$ obtingut composant la projecció a $\mathrm{Gal}(N/K)$ amb el caràcter χ, es té

$$L(\chi',s) = L(\chi,s).$$

1.2.2 Conjectura d'Artin

El caràcter induït del caràcter trivial del subgrup $\{1\} \subset \mathrm{Gal}(N/K)$ és el caràcter r_G de la representació regular de $G = \mathrm{Gal}(N/K)$. Aquest caràcter és

$$r_G = \sum_{\chi} \chi(1)\chi,$$

on χ són els caràcters irreductibles de $\mathrm{Gal}(N/K)$. Com a conseqüència de les propietats (2), (3) i (4), obtenim:

$$\zeta_N(s) = \zeta_K(s) \prod_{\chi \neq 1} L(\chi,s)^{\chi(1)}.$$

El punt de partida de les investigacions d'Artin sobre L-series va ser la qüestió de si, donada una extensió de Galois N/K, el quocient de les seves funcions zeta $\zeta_N(s)/\zeta_K(s)$ és una funció entera, és a dir, és una funció holomorfa en tot el pla complex. Això es deduiria de la seva famosa conjectura:

CONJECTURA D'ARTIN: Per a tot caràcter irreductible $\chi \neq 1$, la funció L d'Artin $L(\chi, s)$ defineix una funció entera.

• **Cas ABELIÀ:** Notem en primer lloc que la conjectura d'Artin és certa per a extensions abelianes. En efecte, com a conseqüència de la teoria de cossos de classe, la funció L d'Artin per a N/K abeliana coincideix amb una funció L de Hecke. Això vol dir que les propietats de les series de Hecke, en particular la seva equació funcional, es transfereix a la funció L d'Artin, en el cas abelià. Dit en poques paraules, si N/K una extensió abeliana amb conductor $\mathfrak{f}$ i $\chi : \mathrm{Gal}(N/K) \longrightarrow \mathbb{C}^*$, és un caràcter (morfisme) irreductible del grup de Galois $\mathrm{Gal}(N/K)$, composant amb el símbol d'Artin es defineix un caràcter sobre $J^{\mathfrak{f}}$, el grup d'ideals fraccionaris primers amb $\mathfrak{f}$,

$$\widetilde{\chi} : J^{\mathfrak{f}} \longrightarrow \mathbb{C}^*,$$

que és un *Grössencharacter* primitiu mod $\mathfrak{f}$. Es té

$$L(\chi, s) = L(\widetilde{\chi}, s).$$

Per a una demostració detallada podeu confrontar, per exemple, [Ne 99].

1.3 Funció L d'Artin estesa

Sigui ρ una representació de Galois complexa de G_K amb caràcter traça χ. Volem definir una funció L estesa

$$\Lambda(\chi, s) = A(\chi)^{s/2}\gamma(\chi, s)L(\chi, s),$$

de manera que tingui prolongació meromorfa a tot el pla complex i satisfaci una equació funcional del tipus

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 1 - s),$$

per a $W(\chi)$ una certa constant de valor absolut 1, tal i com passa en el cas abelià. Ens cal però abans definir els factors que hem d'afegir:

• **El conductor d'Artin:** És un ideal de K que mesura el nivell de la ramificació de la representació ρ. És divisible exactament per tots els primers que ramifiquen a ρ.

Per a cada primer (finit) v de K, sigui

$$I_{\overline{v}} = G_0 \supset G_1 \supset G_2 \supset \cdots$$

la successió de grups de ramificació superior de $\overline{v}|v$. Sigui

$$f(\chi, v) = (\sharp G_0)^{-1} \sum_{i=0}^{\infty} \sharp G_i \operatorname{codim} V^{G_i}.$$

El ideal

$$\mathfrak{f}(\chi) := \prod_{v} v^{f(\chi,v)},$$

s'anomena **el conductor d'Artin** de la representació ρ.

El factor corresponent al conductor és la constant

$$A(\chi) := |d_K|^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}(\chi)),$$

on d_K denota el discriminant absolut de K.

• **Els factors gamma:** Els factors de l'infinit seran

$$\gamma(\chi, s) := \prod_{v|\infty} \gamma_v(\chi, s).$$

Posem

$$\Gamma_{\mathbb{R}}(s) = \pi^{s/2}\Gamma(s/2),$$

$$\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = 2(2\pi)^{-s}\Gamma(s).$$

Denotem $\Gamma_v(s)$, $\Gamma_{\mathbb{R}}(s)$ o $\Gamma_{\mathbb{C}}(s)$ segons v sigui real o complex. Aleshores definim

$$\gamma_v(\chi, s) := \Gamma_v(s)^{n_+(\chi,v)}\Gamma_v(s+1)^{n_-(\chi,v)},$$

on $n_+(\chi, v) = \dim V^{G_{\overline{v}}}$ i $n_-(\chi, v) = \dim V/V^{G_{\overline{v}}}$, és a dir, les dimensions dels subespais de V de vectors propis de valor propi $+1$ i -1, respectivament, per l'automorfisme de Frobenius $\mathrm{Frob}_{\overline{v}} \in G_K$ (conjugació complexa).

Així tenim definida la **funció L d'Artin estesa**

$$\Lambda(\chi, s) := A(\chi)^{s/2}\gamma(\chi, s)L(\chi, s).$$

Els factors $A(\chi)$, $\gamma(\chi, s)$ i la funció L d'Artin estesa tenen les propietats functorials anàlogues a les de la funció L d'Artin: additivitat, inducció i inflació. A més, si χ és un caràcter 1-dimensional, es té

$$\Lambda(\chi, s) = \Lambda(\widetilde{\chi}, s),$$

on $\widetilde{\chi}$ és el Hecke Grössencharacter corresponent.

1.3.1 Teorema. *(Artin-Brauer)*
La funció L estesa $\Lambda(\chi, s)$ té prolongació meromorfa a tot el pla complex i satisfà l'equació funcional

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 1 - s),$$

on $W(\chi)$ s'anomena Artin root number i és una constant de valor absolut 1.

Artin va conjecturar aquest resultat que fou provat per Brauer l'any 1947, per reducció al cas 1-dimensional. De fet, el punt essencial per tenir aquesta reducció és un teorema de Brauer sobre representacions de grups finits.

1.3.2 Teorema. *(Brauer)*
Tot caràcter d'un grup finit G és combinació $\mathbb{Z}$-lineal de caràcters monomials, és a dir, induïts per caràcters de grau 1 de subgrups

$$\chi = \sum_{i=1}^{n} n_i \chi_i^*,$$

on $n_i \in \mathbb{Z}$, χ_i caràcter de grau 1 de $H_i \subset G$.

Aleshores, la prova del Teorema d'Artin-Brauer se segueix de les propietats de la funció L d'Artin estesa. En efecte,

$$\Lambda(\chi, s) = \prod_i \Lambda(\chi_i^*, s)^{n_i} = \prod_i \Lambda(\chi_i, s)^{n_i} = \prod_i \Lambda(\widetilde{\chi_i}, s)^{n_i}.$$

La Teoria de Cossos de Classes ens dóna l'equació funcional

$$\Lambda(\widetilde{\chi_i}, s) = W(\widetilde{\chi_i})\Lambda(\overline{\widetilde{\chi_i}}, 1-s),$$

per a cada caràcter de Hecke $\widetilde{\chi_i}$.

Així, si definim l'Artin root number

$$W(\chi) := \prod_i W(\widetilde{\chi_i}).$$

Clarament té mòdul 1 i obtenim l'equació funcional

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 1-s).$$

Remarquem que la conjectura d'Artin la podem formular ara:

CONJECTURA D'ARTIN: Si χ és un caràcter de G_K que no conté el caràcter trivial $\chi \neq 1$, $\Lambda(\chi, s)$ defineix una funció **entera** en tot el pla complex.

És clar que, a part de per a representacions 1-dimensionals, la conjectura d'Artin és certa per a les representacions monomials, això és, induïdes per una representació 1-dimensional d'un subgrup. És a dir, la conjectura d'Artin és certa per a les representacions complexes amb caràcters del tipus

$$\chi = \sum_{i=1}^{n} n_i \chi_i^*,$$

on $0 < n_i \in \mathbb{Q}, \quad \chi_i$ és una representació 1-dimensional, no trivial, de $H_i \subset G$. Per exemple, si el grup de Galois $G = \mathrm{Gal}(N/K)$ és un grup nilpotent, tot caràcter irreductible és induït per una representació de grau 1 d'un subgrup de G. A més, donat que la representació augmentació d'un grup G, és a dir, la representació regular menys la trivial, és monomial, tenim que si N/K és de Galois, el quocient $\zeta_N(s)/\zeta_K(s)$ és una funció entera. Remarquem que el resultat corresponent per a extensions N/K no galoisianes és obert. Afegim que la conjectura d'Artin està actualment incorporada en el programa general de Langlands i es segueix de les conjectures generals de Langlands.

A partir d'aquest moment en centrem en representacions de Galois complexes dos dimensionals.

1.4 Representacions de Galois complexes associades a formes modulars de pes 1

En aquesta secció fixem el cos $K = \mathbb{Q}$. Tot seguit posarem de manifest que la conjectura d'Artin i la "modularitat" de les representacions de Galois son qüestions equivalents per a representacions complexes 2-dimensional senars, és a dir, tals que el seu determinant envia la conjugació complexa a -1.

En primer lloc, comentem el celebre teorema de Deligne-Serre (1974) sobre les representacions associades a formes modulars de pes 1 i les seves funcions L.

1.4.1 Teorema. *(Deligne-Serre)*
Sigui $f = \Sigma_{n=1}^{\infty} a_n q^n$ una forma modular nova, normalitzada, sobre $\Gamma_0(N)$ de pes 1 i caràcter ϵ. Aleshores existeix una representació irreductible $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V) = \mathrm{GL}(2, \mathbb{C})$ amb conductor N, determinant ϵ i funció L d'Artin

$$L(\rho, s) = L(f, s) = \Sigma_{n=1}^{\infty} a_n n^{-s}$$

Com a conseqüència la representació ρ associada a la forma modular f satisfà la conjectura d'Artin, doncs $L(f, s)$ té continuació analítica en tot el pla complex.

Resumim a continuació els punts més importants de la prova d'aquest teorema (cf. [DS 74])

• Multiplicant f per una serie d'Eisenstein de pes 1 convenient, s'obté una forma modular pròpia de pes 2, congruent amb f mòdul ℓ.

• Per reducció mòdul ℓ de la representació ℓ-àdica associada, s'obté una "aproximació mòdul ℓ", és a dir, $\overline{\rho}_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \mathbb{F}_\ell)$ amb $\mathrm{Tr}(\overline{\rho}_\ell)(\mathrm{Frob}_p) = a_p \pmod{\ell}$ i $\det(\overline{\rho}_\ell)(\mathrm{Frob}_p) = \epsilon(p) \pmod{\ell}$.

• Això ho fem per a infinits ℓ.

• Hi ha una cota uniforme per a la imatge de $\overline{\rho}_\ell$: Rankin (els a_p's són finits en nombre, a menys d'un conjunt de primers p de densitat petita)

• "Enganxant" les $\overline{\rho}_\ell$, s'obté una representació $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \mathcal{O}_E)$ que redueix a $\overline{\rho}_\ell$ per a infinits ℓ, on $\mathcal{O}_E$ és un anell d'enters.

En l'altra direcció tenim el que es coneix com teorema convers de Weil (1967)

1.4.2 Teorema. *(Weil-Langlands)*
Sigui ρ una representació de Galois complexa 2-dimensional de $G_{\mathbb{Q}}$ irreductible i senar amb conductor N i determinant imparell ϵ. Suposem que existeix un M tal que per a tot caràcter de Dirichlet χ de conductor primer amb M, la funció L d'Artin $L(\rho \otimes \chi, s)$ és entera en tot el pla complex. Aleshores, existeix una forma modular f nova, normalitzada, de pes 1 i caràcter ϵ sobre $\Gamma_0(N)$ tal que

$$L(\rho, s) = L(f, s).$$

Si $L(\rho, s) = \sum_{n=1}^{\infty} a_n n^{-s}$, el fet que per torçament la funció L d'Artin $L(\rho \otimes \chi, s)$ és entera en tot el pla complex, permet provar que es compleixen les hipòtesis del teorema de Weil que assegura que $f(z) = \sum_{n=1}^{\infty} a_n q^n$, $q = e^{2\pi i z}$, és una forma nova normalitzada de $\Gamma_0(N)$ amb pes 1 i caràcter ϵ. Per a una demostració detallada confronteu [Og 69].

Així, la conjectura d'Artin i la modularitat de representacions de Galois son qüestions equivalents per a representacions complexes 2-dimensional senars. Demanar que ρ sigui modular, és a dir, provenint d'una forma modular, s'anomena **Conjectura d'Artin forta**.

1.5 La conjectura d'Artin 2-dimensional

Els subgrups G finits de $\mathrm{GL}(2,\mathbb{C})$ es classifiquen per la seva imatge $\widetilde{G}$ a $\mathrm{PGL}(2,\mathbb{C})$. Aquesta imatge $\widetilde{G}$ pot ser:

- un grup cíclic C_n,
- un grup diedral D_{2n},
- isomorfa al grup alternat A_4 (grup tetraèdric),
- isomorfa al grup simetric S_4 (grup octaèdric) o
- isomorfa al grup alternat A_5 (grup icosaèdric).

Així, les representacions de Galois dos dimensionals complexes es classifiquen segons aquestes imatges en tipus: cíclic, diedral, tetraèdric, octaèdric o icosaèdric.

Sabem que, en particular, la conjectura d'Artin i la conjectura d'Artin forta en el cas senar, són certes per a representacions de Galois complexes dos dimensionals de tipus cíclic o diedral, doncs es tracta de representacions abelianes o monomials. Els celebres teoremes de Langlands [La 80] i de Tunnell [Tu 81] proven la conjectura d'Artin per a representacions de Galois complexes dos dimensionals de tipus tetraèdric o octaèdric. A continuació donarem un esbós de les demostracions d'aquests resultats. D'altra banda, recentment, s'han produït avenços molt significatius en l'únic cas en que la conjectura d'Artin dos dimensional està oberta: pel tipus icosaèdric. El capítol 8 estarà dedicat a presentar l'estat actual de la conjectura d'Artin en el cas icosaèdric.

1.5.1 El cas tetraèdric

Destacarem els punts clau de la demostració de Langlands [La 80] de la conjectura d'Artin per a representacions de Galois complexes dos dimensionals de tipus tetraèdric.

Sigui

$$\rho : G_K \rightarrow \mathrm{GL}(2, \mathbb{C}) \rightarrow \mathrm{PGL}(2, \mathbb{C})$$

amb imatge A_4.

Notem, en primer lloc, que el grup alternat A_4 és resoluble i la successió

$$1 \rightarrow D_{2.2} \rightarrow A_4 \rightarrow C_3 \rightarrow 0$$

és exacta.

Considerem les inclusions de cossos $K \subset E \subset L$ associades, és a dir, tals que $\mathrm{Gal}(E/K) = C_3$, $\mathrm{Gal}(L/K) = A_4$ i $\rho|G_E$ amb imatge diedral.

Com que $\rho|G_E$ te imatge diedral, és monomial, i per tant es correspon amb una representació automorfa cuspidal π_E de $\mathrm{GL}(2, \mathbb{A}_E)$, doncs les conjectures de Langlands són certes, en aquest cas.

L'acció de C_3 a $D_{2.2}$ és per automorfismes interns i tenim que $\pi_E = \pi_E^\sigma$, per a tot $\sigma \in C_3$.

Ara, donat que l'extensió E/K és galoisiana i cíclica podem aplicar el teorema de canvi de base de Langlands [La 80].

Es demostra que existeix una única representació cuspidal π_K de $\mathrm{GL}(2, \mathbb{A}_K)$, amb caràcter central $\det \rho_K$, tal que restringeix a π_E.

Un estudi dels factors locals i de les representacions 3-dimensionals monomials globals, permet provar que

$$L(\rho_K, s) = L(\pi_K, s),$$

per a Re(s) gran. Donat que la funció $L(\pi_K, s)$ associada a una representació automorfa cuspidal és entera, obtenim la conjectura d'Artin en aquest cas.

1.5.2 El cas octaèdric

Destacarem ara els punts clau de la demostració de la conjectura d'Artin per a representacions de Galois complexes dos dimensionals de tipus octaèdric. Aquesta prova donada per Tunnell a [Tu 81], utilitza els mètodes de Langlands [La 80] i un resultat analític de Jacquet, Piatetskii-Shapiro i Shalika [JPS 81].

Mirem primer de fer com en el cas tetraèdric. Sigui

$$\rho : G_K \to \mathrm{GL}(2, \mathbb{C}) \to \mathrm{PGL}(2, \mathbb{C})$$

amb imatge S_4.

De nou el grup simètric S_4 és resoluble. Considerem la successió exacta següent:

$$1 \to A_4 \to S_4 \to C_2 \to 0.$$

Siguin $K \subset E \subset L$ les extensions de cossos associades, és a dir, tals que $\mathrm{Gal}(E/K) = C_2$, $\mathrm{Gal}(L/K) = S_4$ i $\rho|G_E$ amb imatge tetraèdrica.

Ara $\rho|G_E$ es correspon amb una representació automorfa cuspidal π_E de $\mathrm{GL}(2, \mathbb{A}_E)$ (Langlands), invariant per l'acció de $\mathrm{Gal}(E/K)$.

Donat que E/K és galoisiana i cíclica, podem aplicar el teorema de canvi de base de Langlands [La 80]. Existeixen dues representacions cuspidals π_1, π_2 de $\mathrm{GL}(2, \mathbb{A}_K)$, tals que per canvi de base a E ens dóna $\rho|G_E$, però ull!!, ara, el caràcter central no distingeix.

Tunnell [Tu 81] considera N el cos fix pels elements de $\mathrm{Gal}(L/K)$ del 2-subgrup de Sylow (d'ordre 8) de S_4. L'extensió N/K és cúbica, no normal. Ara $\rho|G_N$ és monomial, per tant es correspon amb una representació automorfa cuspidal π_N de $\mathrm{GL}(2, \mathbb{A}_N)$. Utilitzant els resultats [La 80] i de [JPS 81] prova que hi ha un únic índex i tal que π_i, per canvi de base a N és la representació cuspidal π_N. Així, sigui π la representació automorfa π_i de $\mathrm{GL}(2, \mathbb{A}_K)$ que per canvi de base dóna d'una banda ρ_N i d'altra ρ_E. Aquesta representació automorfa π és l'associada a ρ i en conseqüència la funció $L(\rho, s)$ és entera.

Bibliografia

[DS 74] Deligne, P., Serre, J-P.: Formes modulaires de poids 1, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 507-530; “Serre, J-P.: Oeuvres”, vol. III, 1972–1984. Springer-Verlag, Berlin, 1986.

[JPS 81] Jacquet, H., Piatetskii-Shapiro, I.I., Shalika, J.: Relèvement cubique non normal, *C. R. Acad. Sci. Paris* **292** (1981), 567-579.

[La 80] Langlands, R.: Base change for GL(2), *Annals of Mathematics Studies,* **96**. Princeton University Press, Princeton, N.J., 1980.

[Ne 99] Neukirch, J.: Algebraic Number Theory , Grundlehren der Mathematischen Wissenchaften, 322. Springer-Verlag, Berlin, 1999.

[Og 69] Ogg A.: Modular forms and Dirichlet series, Benjamin, 1969.

[Se 77] Serre, J-P.: Modular forms and Galois representations, in Algebraic Number Fields, Academic Press, (1977), 193-268; “Serre, J-P. : Oeuvres”, vol. III, 1972–1984. Springer-Verlag, Berlin, 1986.

[Tu 81] Tunnell, J.: Artin’s conjecture for representations of octahedral type, *Bull. Amer. Math. Soc.* **5** (1981), no. 2, 173–175.

N. Vila
Facultat de Matemàtiques
Universitat de Barcelona

Gran Via de les corts Catalanes 585, E-08007 Barcelona,
nuriavila@ub.edu

Capítol 2

Les conjectures de Serre

Víctor Rotger

2.1 Formes modulars mod p

2.1.1 Formes modulars en característica 0

Sigui $\mathcal{H} = \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$ l'hiperplâ superior de Poincaré. Dotat amb la mètrica Riemanniana hiperbòlica, $\mathcal{H}$ és una superfície de Riemann simplement connexa amb grup d'automorfismes $\mathrm{Aut}(\mathcal{H}) \simeq \mathrm{PSL}_2(\mathbb{R})$. L'acció de $\mathrm{PSL}_2(\mathbb{R})$ s'estén de manera natural a l'hiperplà superior de Poincaré compactificat $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Per qualsevol enter positiu $N \geq 1$, sigui

$$\Gamma_1(N) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} mod N\},$$

el grup modular de nivell N. Es tracta d'un subgrup discret de $\mathrm{SL}_2(\mathbb{R})$ i per tant actua en $\mathcal{H}^*$.

Amb el suport parcial de MCYT BFM2003-06768-C02-02

Donat un enter positiu k i una matriu $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, utilitzem la notació

$$F(z)_{|\gamma} = \det(\gamma)^{k/2} \cdot (cz+d)^{-k} \cdot F(\frac{az+b}{cz+d}).$$

2.1.1 Definició

1. Una funció holomorfa $F : \mathcal{H} \longrightarrow \mathbb{C}$ és una forma modular de nivell N i pes k sobre $\mathbb{C}$ si:
   - $F_{|\gamma} = F \quad \forall\, \gamma \in \Gamma_1(N)$
   - $F_{|\gamma}$ és holomorfa en $i\infty$, $\forall\, \gamma \in \mathrm{SL}_2(\mathbb{Z})$:
     Admet $\quad F_{|\gamma} = \sum_{n \geq 0} A_n e^{\frac{2\pi i}{N} \cdot n}$
2. F és paràbolica si $A_0 = 0$, $\forall\, \gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Els espais de formes modulars i parabòliques de *nivell* N i *pes* k són

$$\bullet \quad M_k(N)_{\mathbb{C}} = M_k(N)_{\mathbb{C}}$$

i

$$\bullet \quad S_k(N)_{\mathbb{C}} = S_k(N)_{\mathbb{C}},$$

respectivament.

Finalment, diem que una forma $F = \sum_{n \geq 0} A_n q^n$, $q = e^{2\pi i}$ està definida sobre un subanell $R \subset \mathbb{C}$ si $A_n \in R$, $\forall n \geq 0$. De manera anàloga als anteriors espais de formes modulars, denotem per

$$\bullet M_k(N)_R \text{ amb } M_k(N)_R \otimes \mathbb{C} = M_k(N)_{\mathbb{C}}$$

i

$$\bullet S_k(N)_R \text{ amb } S_k(N)_R \otimes \mathbb{C} = S_k(N)_{\mathbb{C}}$$

els R-mòduls de formes modulars i parabòliques.

2.1.2 Formes modulars sobre una $\mathbb{Z}[1/N]$-àlgebra

Sigui $X_1(N)/\mathbb{Z}[\frac{1}{N}]$ el model enter de Deligne-Rappoport de la corba modular de nivell $N \geq 5$. Amb les estructures respectives de superfícies de Riemann, tenim un isomorfisme

$$X_1(N)(\mathbb{C}) \simeq \mathcal{H}^*/\Gamma_1(N).$$

La corba $X_1(N)$ és l'espai de mòduli fi de corbes el·líptiques (E, P) amb un punt P de N-torsió marcat. Associada al problema de mòduli, existeix la corba el.líptica universal

$$\mathcal{E} \xrightarrow{\pi} X_1(N)$$

amb la $\Gamma_1(N)$-estructura de nivell

$$\iota : (\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathcal{E}[N].$$

Denotem per

$$0 : X_1(N) \longrightarrow \mathcal{E}$$

la secció 0 de la corba el.líptica universal $\mathcal{E}$ i per

$$\Omega^1_{\mathcal{E}/X_1(N)}$$

el feix de diferencials relatives. Finalment, considerem el feix invertible sobre $X_1(N)$

$$\underline{\omega} := 0^*(\Omega^1_{\mathcal{E}/X_1(N)}).$$

2.1.2 Definició (Katz) Sigui R una $\mathbb{Z}[1/N]$-àlgebra. El R-mòdul de formes modulars de nivell N i pes k sobre R és

$$M_k(N)_R = H^0(X_1(N) \otimes R, \underline{\omega}^{\otimes k})$$

En el que segueix, denotarem per

$$M_k(N)_{\bar{\mathbb{F}}_p}$$

el R-mòdul de les formes modulars mod p segons Katz.

Sigui $f \in M_k(N)_R$,

$$f = a_0 + a_1 q + a_2 q^2 + ... \in R[[q]]$$

el desenvolupament en sèrie de potències al voltant d'un punt cuspidal c de $X_1(N)(R)$, on q és un uniformitzant de c. Denotarem per

$$S_k(N)_R = \{f \in M_k(N)_R : a_0 = 0 \, \forall c\}$$

el R-mòdul de les formes parabòliques mod p segons Katz.

2.1.3 Formes modulars mod p segons Serre

Sigui $\bar{\mathbb{Q}}_p$ una clausura algebraica del cos $\mathbb{Q}_p$ de nombres p-àdics. Sigui $\bar{\mathbb{Z}}_p$ l'anell d'enters de $\bar{\mathbb{Q}}_p$ i $\wp$ l'ideal maximal de $\bar{\mathbb{Z}}_p$.

2.1.3 Definició (Serre) Una sèrie formal

$$f = \sum_{n \geq 0} a_n q^n, a_n \in \bar{\mathbb{F}}_p$$

és una forma modular mod p de Serre de nivell N i pes k si existeix $F \in M_k(N)_{\bar{\mathbb{Z}}_p}$ tal que $F \, mod \, \wp = f$.

Denotem per

$$M_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p}$$

el $\bar{\mathbb{F}}_p$-espai vectorial de formes modulars mod p de Serre de nivell N i pes k. Tenim un isomorfisme natural

$$M_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p} \simeq M_k(N)_{\bar{\mathbb{Z}}_p} \otimes \bar{\mathbb{F}}_p.$$

2.1.4 Proposició. (Edixhoven) *Siguin $k \geq 1$ i $(p, N) = 1$. Aleshores*

1. $S_k^{Serre}(N)_{\bar{\mathbb{F}}_p} \subseteq S_k(N)_{\bar{\mathbb{F}}_p}$
2. *Si $k \geq 2$, $S_k^{Serre}(N)_{\bar{\mathbb{F}}_p} = S_k(N)_{\bar{\mathbb{F}}_p}$, a no ser que $N = 1, p = 2$ o 3.*

En general, per $k = 1$, no tota $f \in S_1(N)_{\bar{\mathbb{F}}_p}$ es pot aixecar a característica 0 i per tant $S_k^{\text{Serre}}(N)_{\bar{\mathbb{F}}_p} \subsetneq S_k(N)_{\bar{\mathbb{F}}_p}$.

2.1.5 Exemple. L'invariant de Hasse $E/\bar{\mathbb{F}}_p \mapsto \text{inv}(E)$ és una forma modular de pes $p-1$. En característica $p = 2$ no es pot aixecar a $\bar{\mathbb{Z}}_2$.

2.1.4 L'àlgebra de Hecke

Sigui $N \geq 1$. L'àlgebra de Hecke de nivell N és

$$\mathbb{T} = \langle T_\ell, \ell \nmid N, < d >, d \in (\mathbb{Z}/N\mathbb{Z})^* \rangle_{\mathbb{Z}}$$

on T_ℓ, $< d >$ es defineixen com a operadors que actuen

- En $X_1(N)$ com a correspondències,
- En $J(X_1(N))$ com a endomorfismes de varietats abelianes,
- En $M_k((N))_R$ i $S_k((N))_R$ com a endomorfismes lineals.

2.1.5 Formes noves

Sigui $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow R^*$ un homomorfisme de grups tal que $\varepsilon(-1) = (-1)^k$.

Diem que una forma modular $f \in M_k(\Gamma_1(N))_R$ té caràcter ε si

$$< d > (f) = \varepsilon(d)f, \quad \forall d \in (\mathbb{Z}/N\mathbb{Z})^*.$$

Obtenim unes descomposicions naturals:

$$M_k(\Gamma_1(N))_R = \bigoplus_{\varepsilon} M_k(\Gamma_1(N), \varepsilon)_R$$

i

$$S_k(\Gamma_1(N))_R = \bigoplus_{\varepsilon} S_k(\Gamma_1(N), \varepsilon)_R.$$

Diem que una forma parabòlica $f = \sum a_n q^n$ de tipus (N, k, ε) és *nova* si:

1. $a_0 = 0, a_1 = 1$
2. $T_\ell(f) = a_\ell f$
3. $\nexists g \in S_k(M, \varepsilon)$ per $M \mid N$ amb 1) i 2)

Denotem per $S_k^{new}(N, \varepsilon)$ el R-submòdul de $S_k(N, \varepsilon)$ de rang finit generat per les formes noves.

2.1.6 Aixecaments de formes modulars mod p

2.1.6 Proposició. *Sigui* $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*$ *un homomorfisme de grups. Aleshores existeix un únic caràcter* $\varepsilon_N : (\mathbb{Z}/N\mathbb{Z})^* \to \bar{\mathbb{Z}}_p^*$ *tal que* $\varepsilon_N \equiv \varepsilon$ *mod* p.

2.1.7 Definició El caràcter de Teichmuller és l'homomorfisme

$$\chi_p : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_p^*$$

definit per

$$\chi_p(n) \equiv n \bmod p, \forall n \in \mathbb{Z}, (n,p) = 1.$$

2.1.8 Teorema. (Serre, Gross) *Sigui* $f = \sum a_n q^n$ *una forma* nova *definida sobre* $\bar{\mathbb{F}}_p$ *de tipus* (N, k, ε).

1. *Si* f *és de tipus* $(N, 2, \varepsilon)$, *existeix una forma nova* F *de tipus* $(N, 2, \varepsilon_N)$ *sobre* $\bar{\mathbb{Z}}_p$ *tal que* $F \equiv f$ *mod* $\wp$.
2. *Si* f *és de tipus* (N, k, ε), $2 < k \leq' p + 1$, *existeix una forma nova* F *de tipus* $(Np, 2, \varepsilon_N \chi_p^{k-2})$ *sobre* $\bar{\mathbb{Z}}_p$ *tal que* $F \equiv f$ *mod* $\wp$.

En el segon apartat del teorema, per $k \leq' p + 1$ volem significar $k < p + 1$ o $k = p + 1$ sota una condició tècnica que no precisarem en aquestes notes.

2.2 Representacions de Galois associades a formes modulars

Sigui V un espai vectorial sobre $\bar{\mathbb{F}}_p$ i sigui

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

una representació del grup absolut de Galois $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ en el grup de transformacions lineals de V.

Diem que la representació ϱ és:

1. *contínua*, si Ker $\varrho = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ per algun cos de nombres K, $[K : \mathbb{Q}] < \infty$.

   Les representacions contínues indueixen una representació

$$\varrho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}(V).$$

2. *irreductible*, si no existeixen subespais propis $W \subset V$ invariants per l'acció de $\varrho(G_{\mathbb{Q}})$.

3. *semisimple*, si $V = \bigoplus_{i=1}^{k}$ és la suma directa de $G_{\mathbb{Q}}$-subespais irreductibles W_i.

4. *parell*, si $\det(\varrho(c)) = 1$, *senar* si $\det(\varrho(c)) = -1$.

2.2.1 Teorema. (Shimura, Deligne) *Sigui $f = \sum a_n q^n$ una forma nova definida sobre $\mathbb{F}_q$ de tipus (N, k, ε).*

Aleshores existeix una única representació de Galois contínua i semisimple

$$\varrho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$$

tal que:

1. *+s no ramificada en $\ell \nmid Np$*

2. *Per tot $\ell \nmid Np$:*

$$\mathrm{tr}(\varrho_f(Frob_\ell)) = a_\ell,$$

$$\det(\varrho_f(Frob_\ell)) = \varepsilon(\ell)\ell^{k-1}.$$

Demostració.

- Ens reduïm a $2 \leq k \leq' p+1$ mitjançant la derivació de Ramanujan-Katz.

- Per Serre i Gross, aixequem f a una forma nova $F = \sum A_n q^n$ nova de pes 2 i nivell N o Np.
- Associada per Shimura a la forma nova F, considerem la varietat abeliana $A_F/\mathbb{Q}$, que satisfà les següents propietats:

  (i) A_F és isògena a una subvarietat de $J(X_1(N))$

  (ii) El cos $E = \mathbb{Q}(A_N)$ generat pels coeficients de Fourier de F és un cos de nombres: $\mathcal{O}_E = \mathrm{End}_{\mathbb{Q}}(A_F)$.

  (iii) $\dim(A_F) = [E : \mathbb{Q}]$.

- $T_p(A_F) \simeq \mathcal{O}_{E_\wp} \bigoplus \mathcal{O}_{E_\wp}$, per qualsevol ideal primer $\wp$ a sobre de p.
- En considerar l'acció de Galois sobre la torsió de A_F, obtenim una representació $\varrho_F : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{E_\wp})$.
- Reduïnt mod $\wp$, obtenim $\varrho_f : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_q)$.
- La representació ϱ_f és no ramificada en $\ell \nmid Np$. Pel criteri de Serre-Tate, obtenim que A_F tè bona reducció fora de N.
- Les relacions d'Eichler-Shimura demostren que els valors de $\mathrm{tr}(\varrho_f(Frob_\ell))$ i $\det(\varrho_f(Frob_\ell))$ són els enunciats en el teorema. □

2.2.2 Definició Diem que una representació de Galois

$$\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

és modular si $\varrho = \varrho_f$ per alguna forma modular nova mod p.

2.2.3 Conjectura (La conjectura dèbil de Serre) *Totes les representacions de Galois*

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

contínues, irreductibles i senars són modulars.

2.3 La conjectura forta de Serre

Donada una representació de Galois $\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$, Serre n'associa uns invariants N_ϱ, ε_ϱ i k_ϱ que ara introduïrem.

Destaquem però que N_ϱ depèn del comportament dels grups de descomposició $D_\ell = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \subset \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ per $\ell \neq p$.

En canvi, la definició del pes de Serre k_ϱ depèn de $D_p \subset \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Finalment, ε_ϱ s'introdueix a partir del caràcter. $\det(\varrho) : G_{\mathbb{Q}} \to \bar{\mathbb{F}}_p^*$.

2.3.1 Els invariants de Serre

Sigui

$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

una representació de Galois en un espai vectorial sobre $\bar{\mathbb{F}}_p$ de dimensió $\dim_{\bar{\mathbb{F}}_p}(V) = 2$.

El conductor N_ϱ de Serre

Sigui $\bar{v}_\ell$ una extensió a $\bar{\mathbb{Q}}$ de la valoració ℓ-àdica de $\mathbb{Q}_\ell$ i sigui

$$G = \varrho(G_{\mathbb{Q}}) \subseteq \mathrm{GL}(V)$$

el subgrup finit imatge de la representació ϱ.

Considerem la cadena

$$G_0 \supset G_1 \supset G_2 \supset ...$$

de grups de ramificació associats a $\bar{v}_\ell$ i siguin

$$V^{G_i} = \{v \in V : v^g = v, g \in G_i\} \subseteq V$$

els subespais invariants de V per l'acció de G_i.

2.3.1 Definició

$$N_\varrho = \prod_{\ell \neq p} \ell^{n(\ell)}$$

on $n(\ell) = \sum_{i=0}^{\infty} \frac{1}{(G_0:G_i)} \mathrm{codim}_{\bar{\mathbb{F}}_p} V^{G_i} \geq 0.$

Remarquem que de la pròpia definició, tenim que

$$n(\ell) = 0 \Leftrightarrow \varrho \text{ no ramifica en } \ell$$

i que N_ϱ és coprimer amb p.

El caràcter ε_ϱ de Serre

Serre defineix el caràcter ε_ϱ com segueix. El homomorfisme

$$\det(\varrho) : G_{\mathbb{Q}} \to \bar{\mathbb{F}}_p^*$$

és continu i té per imatge un subgrup cíclic de $\bar{\mathbb{F}}_p^*$. A més, el conductor del homomorfisme divideix $N_\varrho p$.

D'aquí obtenim un caràcter

$$\det(\varrho) : (\mathbb{Z}/N_\varrho p\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*$$

que al seu torn n'indueix dos, un dels quals és el que ens interessa:

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*$$

i

$$\varepsilon_\varrho : (\mathbb{Z}/N_\varrho\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*,$$

amb $\det \varrho(Frob_\ell) = \varphi(\ell) \cdot \varepsilon_\varrho(\ell)$ per $\ell \nmid N_\varrho p$.

El pes k_ϱ de Serre

Considerem les extensions de cossos

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{nr} \subset \mathbb{Q}_p^t \subset \bar{\mathbb{Q}}_p$$

i els grups galoisians

- $D_p \simeq \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$,

- $I_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$,
- $D_p/I_p \simeq \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$,
- $I_s = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^t)$,
- $I_t = I_p/I_s = \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p^{nr}) \simeq \lim \mathbb{F}_{p^n}^*$

El grup d'homomorfismes continus de I_t en $\bar{\mathbb{F}}_p^*$ es pot descriure com segueix:

$$\hat{I}_t = \mathrm{Hom}_{cont}(I_t, \bar{\mathbb{F}}_p^*) \overset{inv}{\simeq} (\mathbb{Q}/\mathbb{Z})' = \{[\frac{a}{d}], p \nmid d\}$$

D'entre els elements de $\hat{I}_t$, en destaquem els següents:

- $\chi : I_t \to \mathbb{F}_p^*$ amb $\mathrm{inv}(\chi) = \frac{1}{p-1}$, el caràcter ciclotòmic,
- $\psi : I_t \to \mathbb{F}_{p^2}^*$ amb $\mathrm{inv}(\psi) = \frac{1}{p^2-1}$,
- $\psi' : I_t \to \mathbb{F}_{p^2}^*$ amb $\mathrm{inv}(\psi') = \frac{p}{p^2-1}$

Considerem la restricció de la representació al grup de descomposició en p:

$$\varrho : D_p \longrightarrow \mathrm{GL}(V) \simeq \mathrm{GL}_2(\bar{\mathbb{F}}_p).$$

El subgrup d'inèrcia I_s opera trivialment sobre la semisimplificació V^{ss} de V i l'acció de I_t sobre V^{ss} diagonalitza:

$$I_t \xrightarrow{\varrho} \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}.$$

Hi ha dues possibilitats:

- Nivell 1: $\varphi, \varphi' : I_t \to \mathbb{F}_p^*$ o
- Nivell 2: $\varphi, \varphi' : I_t \to \mathbb{F}_{p^2}^*$ amb $\varphi' = \varphi^p$.

2.3.2 Definició El pes k_ϱ és l'enter en $[1, p^2-1]$:

1. Si φ, φ' són de nivell 2, aleshores
$$\varphi = \psi^a \psi'^b, \varphi' = \psi^b \psi'^a$$
per $0 \le a < b \le p-1$. Definim
$$k_\varrho := 1 + pa + b.$$

2. Si φ, φ' són de nivell 1, tenim:

   (a) Si $\varrho_{|I_p} \simeq \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$, $0 \le a \le b \le p-2$, definim
   $$k_\varrho := 1 + pa + b.$$

   (b) Si $\varrho_{|I_p} \simeq \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$, $0 \le \alpha \le p-2, 1 \le \beta \le p-1$, siguin $a = \min(\alpha, \beta)$ i $b = \max(\alpha, \beta)$. Definim
   $$k_\varrho := 1 + pa + b \text{ o } 1 + pa + b + p - 1.$$

2.3.3 Conjectura (Conjectura forta de Serre) *Sigui*
$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$
una representació contínua, irreductible i senar.

Aleshores existeix una forma nova $f \in S_{k_\varrho}(N_\varrho, \varepsilon_\varrho)_{\bar{\mathbb{F}}_p}$ *tal que*
$$\varrho \simeq \varrho_f.$$

2.3.4 Teorema. (Serre, Mazur, Ribet, Carayol, Jordan, Livné, Gross, Edixhoven, Diamond) *Sigui*
$$\varrho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p), p > 2$$
una representació contínua, irreductible i senar. Aleshores

1. *Si ϱ és modular, ϱ satisfà la conjectura forta de Serre.*

2. *Si $\varrho = \varrho_f, f \in M_k(N, \epsilon)_{\bar{\mathbb{F}}_p}$, $(N, p) = 1$, aleshores*
$$N_\varrho \mid N, k_\varrho \le k$$
i
$$\epsilon : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N_\varrho\mathbb{Z} \xrightarrow{\epsilon_\varrho} \bar{\mathbb{F}}_p^*.$$

2.4 Conseqüències

2.4.1 Comportament per twists

Sigui $\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ una representació contínua, irreductible i senar.

Per cada $i \geq 0$, siguin

$$\varrho(i) = \varrho \otimes \chi^{-i} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

les representacions torçades de ϱ.

2.4.1 Proposició. (Atkin-Serre-Tate, Lario)

$$N_{\varrho(i)} = N_{\varrho}, \epsilon_{\varrho(i)} = \epsilon_{\varrho}, \forall i$$

Existeix $0 \leq i \leq p-1 :\ k_{\varrho(i)} \leq p+1$

ϱ *és modular* $\Leftrightarrow$ $\varrho(i)$ *és modular per algun* $0 \leq i \leq p-1$.

La Conjectura Forta de Serre implica la següent

2.4.2 Conjectura 1. *Si* $\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ *és no-ramificada fora de* p*, aleshores* $\exists f \in S_k(SL_2(\mathbb{Z})), k \leq p+1$ *tal que* $\varrho = \varrho_f$.

2. *Si* $p = 2, 3, 5$ *o 7, aleshores* $S_k(SL_2(\mathbb{Z})) = \emptyset$ *per* $k \leq p+1$ *i per tant no existeixen representacions* $\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ *no ramificades fora de* p.

La conjectura ha estat provada per $p = 2$ (Tate), $p = 3$ (Serre), $GRH \Rightarrow p = 5$ (Brueggeman)

2.4.2 El teorema de Fermat.

2.4.3 Teorema. (Serre) *Si la conjectura forta de Serre és certa,*

$$a^p + b^p + c^p = 0, \quad p \geq 5$$

no té solució amb $a, b, c \in \mathbb{Z}$, $abc \neq 0$.

Demostració.

- Ens podem reduir amb arguments elementals al cas en què a, b, c són primers entre ells, b és parell i $a \equiv 3 \bmod 4$.
- Sigui $E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$ la corba el.líptica de Frey.
- Sigui $\varrho_{a,b,c} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ la representació associada a la p-torsió de $E_{a,b,c}$.
- $N_{\varrho_{a,b,c}} = 2, \epsilon_{\varrho_{a,b,c}} = 1$ i $k_{\varrho_{a,b,c}} = 2$.
- $\exists\, f \in S_2(2) = H^0(X_0(2), \Omega^1_{X_0(2)}) : \varrho_{a,b,c} = \varrho_f$.
- Però $X_0(2) \simeq \mathbb{P}^1_{\mathbb{Q}}$!!!

2.4.3 Conjectura de Shimura-Taniyama-Weil generalitzada.

Serre va demostrar també que si la conjectura forta de Serre és certa, la següent conjectura és certa.

2.4.4 Conjectura (Shimura-Taniyama-Weil generalitzada) *Sigui* $A/\mathbb{Q}$ *una varietat abeliana de dimensió* $n \geq 1$*. Si* $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ *és un cos de nombres de grau* n*, aleshores* A *és isògena a una subvarietat abeliana de* $J(X_1(N))$ *per algun* N*.*

Bibliografia

[Ed] Edixhoven, B.: Serre's conjectures, *Modular Forms and Fermat's Last Theorem*, G. Cornell, J. H. Silverman, G. Stevens (eds.), Springer-Verlag (1991), 209-242.

[La] Lario, J-C.: Representacions de Galois i corbes el·líptiques, Ph. D Thesis, Universitat de Barcelona (1991).

[Se] Serre, J-P.: Sur les representations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), *Duke Math. J.* **54** (1987), 179-230.

V. Rotger
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú
Universitat Politècnica de Catalunya
Av. Victor Balaguer s/n, E-08800 Vilanova i la Geltrú,
vrotger@mat.upc.es

Capítol 3

La conjectura de Fontaine-Mazur

Francesc Bars

Exposició: 20 de Gener 2004.

3.1 Introducció

Aquesta exposició únicament intenta introduir els ingredients bàsics pel plantejament de la conjectura Fontaine-Mazur formulada en [11]. La conjectura formula de manera precisa la següent idea: representacions del grup de Galois $Gal(\overline{K}/K)$ amb K un cos de nombres que venen de les representacions locals d'un tros d'un motiu sobre K amb coeficients amb un altre cos de nombres E tenen unes propietats algebraiques fixes i que a més aquestes propietats algebraiques caracteritzen que vinguin de la geometria algebraica aritmètica, és a dir d'un tros d'un motiu sobre un cos de nombres K amb coeficients en E.

Sota el support econòmic de DGI, BFM2003-06092.

Notacions i comentaris

En la §3.2, K denota un cos de nombres i E un altre cos de nombres. En la secció posterior §3.3 K denota un cos local amb cos residual de característica p amb E un cos local extensió finita de $\mathbb{Q}_l$. Usualment denotem λ per a un primer de K i per β un primer de E. Igualment G_K denotarà el grup de Galois absolut de K, és a dir $Gal(\overline{K}/K)$ on $\overline{F}$ sempre denota clausura algebraica del cos F, i igualment F_γ amb $\gamma \in Spec(F)$ denota el cos completat de F per l'ideal γ de F.
L denota una extensió finita de $\mathbb{Q}_l$ dins la clausura algebraica de $\mathbb{Q}_l$ i L^0 una extensió de L dins $\overline{\mathbb{Q}_l}$. Denotem per $\kappa(\lambda)$ el cos residual de K_λ, i $\kappa(F)$ pel cos residual d'un cos local F.
Observació: Les notes d'aquesta exposició difereixen de la exposició realitzada en el seu dia en el seminari STNB 2004, ja que en aquella exposició ens vam restringir a presentar la conjectura amb $E = \mathbb{Q}$ (és dir consideràvem motius sense coeficients!) i igualment no es va poder explicar res sobre la teoria referent a mòduls de Deligne, que si que escriurem breument en aquestes notes (§3.3) (no obstant tota aquesta teoria de mòduls de Deligne i filtrats ho escriurem únicament per a l-representacions, és a dir "$E = \mathbb{Q}$, $L = L^0 = \mathbb{Q}_l$").

3.2 Enunciat de la conjectura de Fontaine-Mazur

Anem primer a definir que vol dir que una representació de G_K, amb K cos de nombres, ve de la geometria algebraica (aritmètica).
Recordem que una representació L^0-àdica és un morfisme continu

$$\rho : Gal(\overline{K}/K) \to GL(V)$$

amb V un L^0-espai vectorial.(Una representació l-adica, significa una representació $\mathbb{Q}_l$-àdica)
Donada una varietat algebraica X sobre K llissa i projectiva, obtenim de manera natural molts espais vectorials V associats amb estructura addicional (realitzacions), nosaltres ens interessa que tingui una acció continua lineal per al grup de Galois G_K, considerem la realització

l-adica étale associada a X;

$$\oplus_{i=0}^{2dim(X)} H_{et}^i(X \times_K \overline{K}, \mathbb{Q}_l) \otimes_{\mathbb{Q}} E \tag{3.1}$$

amb acció de G_K (observem que la categoria que presentem correspon a $Ch_{\mathbb{Q}}(K, E)$ que és isomorfa a la categoria de $Ch_E(K)$ per aquesta equivalència veieu Deligne 2.1 [6]) Ens interessa usualment restringirnos a un $H_{et}^i(\overline{X}, \mathbb{Q}_l) \otimes E$ (informació parcial de X en la realització l-àdica a coeficients en E). Les anteriors representacions són un cas concret de representacions provinents de la geometria algebraica considerant els objectes $M = (X, proj, r)$ dins la categoria de motius de Chow sobre K amb coeficients en E on $proj$ denota un projector i r un enter (Tate twist) i obtenim una realització l-àdica,

$$\oplus_{i=0}^{2dim(X)} proj^* H_{et}^i(X \times_K \overline{K}, \mathbb{Q}_l(r)) \otimes_{\mathbb{Q}} E \tag{3.2}$$

En general triar un sumand d'aquesta descomposició correspondria a representacions de la geometria "pures"(correspondria sol agafar un d'aquests factors en la suma directa que té un únic pes, recordem per X varietat projectiva el motiu $proj^* H_{et}^i(X \times_K \overline{K}, \mathbb{Q}_l(r))$ és pur de pes $w = i - 2r$). Més en general en geometria algebraica podem considerar objectes geomètrics (X sense ser projectiva com fins ara) i considerar la realització l-àdica de X però ara X és una varietat algebraica qualsevol, on les components irreductibles de la seva realització en grups de cohomologia ètale poden tenir pesos mixtes (veieu Deligne en [7](complement d'una varietat amb creuament normal,...)). Obtenim així el que podríem anomenar representacions de la geometria "mixtes".

Escrivim

$$\rho_l = \prod_{\beta | l} \rho_\beta : G_K \to GL(V \otimes_{\mathbb{Q}_l} E_\beta),$$

com GL lineal amb E_β, és a dir E_β-representacions de G_K, amb V la realització l-àdica d'un objecte geomètric sobre K. Restringim-nos a ρ_β irreductible, i observeu que si V és simple i prové d'un subquocient d'algun grup de cohomologia étale a coeficients en E, llavors és una peça de $proj^* H_{et}^m(\overline{X}, \mathbb{Q}_l(r)) \otimes E_\beta$ amb X projectiva (cas pur).

D'aquestes consideracions es proposa la següent definició.

3.2.1 Definició Sigui ρ una L^0-representació irreductible de G_K, és a dir una representació irreductible continua

$$\rho : G_K \to GL(V)$$

on V és un L^0-espai vectorial i GL és lineal en L^0. Diem que ρ ve de la geometria algebraica (aritmètica) si és isomorfa a un subquocient d'algun grup de cohomologia étale provinent de la realització l-àdica d'alguna varietat X sobre K amb coeficients en un E, diem-li M on existeix $\beta \in Spec(E)$ amb $E_\beta \cong L$ i que $V \cong M \otimes_L L^0$ com $L^0[G_K]$-representacions.

Anem a estudiar les propietats de la representació de G_K en $H^i_{et}(X \times_K \overline{K}, \mathbb{Q}_l)$, que passin a subquocients. Ens restringim amb X/K és projectiva i llisa sobre K (és a dir el cas de representacions "pures", bàsicament doncs estudiarem representacions irreductibles simples de la geometria algebraica).

Considerem la representació:

$$\rho : G_K \to GL(H^i_{et}(\overline{X}, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} L).$$

Recordem que una representació L-àdica s'anomena no ramificada en el primer λ de K si el grup d'inèrcia de λ en G_K, I_λ, actua de manera trivial.
Com X és una varietat, fora d'un conjunt finit S de places de K tenim que X té bona reducció i per tant per tot $\lambda \notin (S \cup \{\lambda' | l\})$ finit, el grup d'inèrcia I_λ es conegut que actua de manera trivial en la realització l-àdica de X (és a dir en cada component de (3.1)) i per tant en qualsevol subquocient d'una component, per tant s'obté;

3.2.2 Lema. *Una representació de G_K de la geometria algebraica és no ramificada fora d'un conjunt finit de places finites de K. És a dir la representació factoritza a traves de $G_{K,S} = Gal(K_S/K)$ on K_S denota la extensió maximal de K no ramificada fora del conjunt S.*

Hi ha aquí la pregunta natural següent,

3.2.3 Questió Existeix una representació local irreductible semi-simple de G_K ($\rho : G_K \to GL_L(V)$) de manera que no existeix cap conjunt finit S de $Spec(K)$ on la representació ρ factoritzi a través de $G_{K,S}$? (La resposta és que si, hi ha exemples amb V no provinents de la geometria on ramifica a un numero no finit de primers, veieu [14] i §5 en [13]. Agrair aquí a en Luis Dieulefait per comentarme aquestes referències).

Restringim la nostra representació

$$\rho : G_K \to GL(H^i_{et}(\overline{X}, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} L)$$

al grup de descomposició G_λ de G_K en una plaça finita $\lambda \in Spec(K)$. Denotem per $p = car(\kappa(\lambda))$ on $\kappa(\lambda)$ és el cos residual de λ. L'estudi d'aquesta representació local de $G_\lambda \cong G_{K_\lambda}$ (elegint immersió) té un comportament diferent per a $l \neq p$ i per a $l = p$ "tota la informació").
Estudi per a $l \neq p$
Considerem una representació local

$$\rho_\lambda : G_\lambda \to GL_L(V),$$

amb $\kappa(\lambda) = p$ amb L extensió finita de $\mathbb{Q}_l$ dins $\overline{\mathbb{Q}}_l$.

Si ens restringim a V com un tros (pur) d'una realització l-àdica per una v.a. X projectiva i llissa sobre K ($H^i_{et}(\overline{X}, \mathbb{Q}_l(r)) \otimes_{\mathbb{Q}_l} L$), llavors si $X \times_{K_\lambda} \overline{K_\lambda}$ té bona reducció en λ la inèrcia I_λ actua de manera trivial en cadascun dels grups de cohomologia étale de la seva realització l-àdica, si tè potencialment bona reducció llavors en una extensió finita $K'_{\lambda'}$ de K_λ obtenim $I_{\lambda'}(\subset G_{K'_{\lambda'}})$ actua de manera trivial sobre cada peça de la realització l-adica associada a $(X, proj, r)$ i en particular en $proj^* H^i_{et}(\overline{X}, \mathbb{Q}_l(r)) \otimes L$.

3.2.4 Definició Diem que ρ_λ una representació local arbitrària L-àdica ($\rho_\lambda : G_\lambda \to GL_L(V)$) s'anomena de bona reducció si I_λ es troba en el nucli de ρ_λ (condició que també es diu que és no-ramificada en λ).
Diem que ρ_λ és potencialment de bona reducció si existeix un subgrup obert de I_λ que actua de manera trivial (és a dir hi ha una extensió finita $K'_{\lambda'}$ de K_λ dins $\overline{K_\lambda}$ on $I_{\lambda'} \subset Ker(\rho_\lambda | G_{K'_{\lambda'}})$).

En quan a l'estudi general de representacions amb $l \neq p$ tenim el següent resultat de Grothendieck (veieu 1 en [5]),

3.2.5 Proposició. *Sigui $\rho_\lambda : G_\lambda \to GL_L(V)$, com abans amb $l \neq p$. Imposem a més que cap extensió finita de $\kappa(\lambda)$ contingui totes les arrels l^n-èssimes de la unitat $\forall n$ (aquesta condició es compleix per exemple quan $\kappa(\lambda)$ és finit). Llavors existeix un obert H de I_λ de manera que $\rho(h)$ és unipotent per a tot $h \in H$.*

Demostració:[sketch] Reduïm-nos cas $L = \mathbb{Q}_l$. Via una extensió finita de K_λ podem suposar que tot element $x \in I_{\lambda'}$ compleix que $\rho(x)$ és una matriu a coeficients en $\mathbb{Z}_l$ i congruent amb la matriu Id mòdul l^2, denotem igualment per K_λ aquesta extensió. Amb aquestes condicions tenim $\rho(I_\lambda)$ és un pro-l-grup. Per veure que $\rho(x)$ és unipotent argumentem de la forma següent;
sigui K_{nr} l'extensió maximal no ramificada de K_λ, $I_\lambda = Gal(K_\lambda^{sep}/K_{nr})$; K_l la l-part de l'extensió maximal moderadament ramificada de K (és a dir és l'extensió de K_{nr} generada per les l^m-arrels d'un uniformitzant a K_{nr}). Es prova llavors que l'ordre de $Gal(K_\lambda^{sep}/K_l)$ com nombre supernatural és primer amb l, i per tant si $x \in Gal(K_\lambda^{sep}/K_l)$, $\rho(x)$ és una potencia de l; per tant $\rho(Gal(K_\lambda^{sep}/K_l)) = \{1\}$. Per estudiar llavors l'acció en la inèrcia ens restringim a la imatge del grup de Galois,

$$Gal(K_l/K_{nr}) \cong \varprojlim \mu_{l^n} = T_l(\mu)$$

compatible amb $Gal(\overline{\kappa(\lambda)}/\kappa(\lambda)) \cong Gal(K_{nr}/K_\lambda)$ per automorfismes interns. Considerem el caracter

$$\chi : G_\kappa := Gal(\overline{\kappa(\lambda)}/\kappa(\lambda)) \to \mathbb{Z}_l^*$$

donat per l'acció de G_κ sobre $T_l(\mu)$. Donat $x \in Gal(K_l/K_{nr})$ tenim x i $x^{\chi(t)}$ conjugats en $Gal(K_l/K_\lambda)$ per qualsevol $t \in G_\kappa$.
Considerem $X = log\rho(x)$ el logaritme l-adic. De $log(\rho(x)^{\chi(t)}) = \chi(t)X$, tenim que X i $\chi(t)X$ son matrius conjugades $\forall t \in G_\kappa$. Sigui $a_i(X)$ la funció i-simètrica de les arrels característiques de X, de la igualtat anterior obtenim: $a_i(X) = \chi(t)^i a_i(X)$, com no conté totes les arrels l-èssimes de la unitat la imatge de χ es un subgrup infinit de $\mathbb{Z}_l^*$, triem t complint que $\chi(t)$ no és una arrels de la unitat, obtenint

$a_i(X) = 0$ per tot $i > 0$, i per tant X és una matriu nilpotent.
Com $\rho(x) \equiv 1 (mod\ l^2)$ obtenim

$$\rho(x) = exp(log(\rho(x))) = exp(X) \text{ és unipotent.}$$

□

3.2.6 Definició Sigui ρ una L-representació de G_{K_λ} del L-espai vectorial V amb $car(\kappa(\lambda)) = p \neq car(L)$.
Diem que ρ és semiestable si l'acció de I_{K_λ} opera de manera unipotent.
Diem que ρ és potencialment semiestable si existeix una extensió finita F/K_λ ($F \subset \overline{K_\lambda}$) on $\rho|Gal(\overline{K_\lambda}/F)$ és semiestable (equivalentment existeix un subgrup obert H de I_{K_λ} on ρ actua de manera unipotent en H).

3.2.7 Corol·lari. *La L-representació local de G_{K_λ} amb V igual a $H^m_{et}(\overline{X}, \mathbb{Q}_l(r)) \otimes_{\mathbb{Q}_l} L$ és potencialment semiestable $\forall \lambda \nmid l$, és a dir tota representació simple de la geometria algebraica és potencialment semiestable $\forall \lambda \nmid l$.*

Denotem per $Rep_{L,l}(G_{K_\lambda})$ amb $l = car(\kappa(L)) \neq p = car(\kappa(\lambda))$ la categoria tannakiana de les L-representacions de G_{K_λ}. Podem considerar les representacions amb bona reducció que formen una subcategoria (de $Rep_{L,l}(G_{K_\lambda})$) tannakiana que denotem per $Rep_{L,l,f}(G_{K_\lambda})$ (si considerem les representacions que són potencialment bona reducció, el seu conjunt el denotem per $Rep_{L,l,pf}(G_{K_\lambda})$) i si considerem les representacions que són semiestable tenim llavors la categoria $Rep_{L,l,st}(G_{K_\lambda})$, i finalment denotem per $Rep_{L,l,pst}(G_{K_\lambda})$ per a la categoria de representacions potencialment semiestables. Hem demostrat en 3.2.5 per $K_\lambda/\mathbb{Q}_p$ finita(la nostra situació) $Rep_{L,l}(G_{K_\lambda}) = Rep_{L,l,pst}(G_{K_\lambda})$ (*). Tenim el següent diagrama on totes les inclusions son estrictes a excepció de la igualtat (*) per $K_\lambda/\mathbb{Q}_p$ finita:

$$\begin{tikzcd}
 & Rep_{L,l,pf}(G_{K_\lambda}) \arrow[dr] & & \\
Rep_{L,l,f}(G_{K_\lambda}) \arrow[ur] \arrow[dr] & & Rep_{L,l,pst}(G_{K_\lambda}) \arrow[r] & Rep_{L,l}(G_{K_\lambda}) \\
 & Rep_{L,l,st}(G_{K_\lambda}) \arrow[ur] & &
\end{tikzcd}$$

Estudi per a $l = p$

Considerem ara que $l = p$, i centrem-nos en les representacions de motius purs de Chow a $\mathbb{Q}$-coeficients, més concretament amb les representacions G_{K_λ} amb $\lambda | l$ de $V = H^m_{et}(\overline{X}, \mathbb{Q}_l)$, amb X projectiva i llisa sobre K, recordem que tenim els següents resultats de comparació que ens donen certa forma d'estudiar aquest G_{K_λ}-representacions d'algun altre punt de vista.
Comencem amb el següent resultat de comparació (per una altra exposició més extensa de teoremes de comparació i anells Fontaine veieu [17]):

$$(Faltings)\ H^m_{et}(\overline{X}, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \mathbb{C}_l \cong \oplus_{o+q=m}(H^o(X, \Omega^q_{X/K_\lambda}) \otimes_{K_\lambda} \mathbb{C}_l(-o))$$

que respecta l'acció de Galois G_{K_λ}, on $\mathbb{C}_l = \hat{\overline{\mathbb{Q}_l}}$ i $\Omega^\cdot$ és el complex de cadenes de diferencials de X/K_λ.
Reescrivim l'anterior isomorfisme de comparació entre una cohomologia de diferencials amb una topològica via un anell de Fontaine $B_{HT,l} := \oplus_{j \in \mathbb{Z}} \mathbb{C}_l(j)$ d'una altra manera. Recordeu que la cohomologia diferencial de Hodge-Tate es defineix via $H^i_{Hod}(X/K_\lambda) := \oplus_{o+q=i} H^o(X, \Omega^q_{X/K_\lambda})$ i així el morfisme de comparació és;

$$H^m_{et}(\overline{X}, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} B_{HT,l} \cong (H^m_{Hod}(X/K_\lambda) \otimes_{K_\lambda} B_{HT,l}.$$

3.2.8 Observació. (d'en X.Xarles) La B dels anells de Fontaine es probablement en honor a Barsotti, i aquests anells han estat també anomenats anells de Barsotti-Tate [8]. Barsotti va introduir anells d'aquest tipus al estudiar com es relacionaven les diferencials d'una varietat abeliana sobre els p-adics amb bona reducció amb certs objectes cohomològics associats a la reducció (e.g. el mòdul de Dieudonné), veieu [1].

Fixem-nos que si considerem la cohomologia de Rham $H^m_{dR}(X/K_\lambda)$ tenim un K_λ-espai vectorial que té una filtració natural, si volem comparar amb la cohomologia étale que té una estructura de G_{K_λ}-mòdul i volem que aquest isomorfisme sigui canònic i mantingui les propietats d'aquests grups cohomològics, necessitem un altre anell de

Fontaine però ara amb acció de Galois i una filtració, és l'anell $B_{dR,l}$. Tenim l'isomorfisme,

$$(Faltings\ 1988)\quad H^m_{et}(\overline{X},\mathbb{Q}_l)\otimes_{\mathbb{Q}_l} B_{dR,l}\cong H^m_{dR}(X/K_\lambda)\otimes_{K_\lambda} B_{dR,l}$$

que és compatible amb l'acció de G_{K_λ} que actua per $\sigma\otimes\sigma$ en l'esquerra i per $id\otimes\sigma$ en el terme de la dreta, compatible amb les filtracions, és a dir $id\otimes Fil^q\leftrightarrow\sum_{a+b=q}Fil^a\otimes Fil^b$, dualitat de Poincaré,...

3.2.9 Observació. Recordeu que $Gr_{Fil}H^m_{dR}(X/K_\lambda)=H^m_{Hod}(X/K_\lambda)$, i per tant el la cohomologia de Hodge-Tate perdem aquesta filtració, i deixem escrit aquí que $Gr_{Fil}B_{dR,l}=B_{HT,l}$.

Anem ara a endinsar-nos sobre quin tipus de reducció té la varietat X/K_λ en l'unic primer tancat de K_λ, especialitzant-nos obtenim que varietats amb cert tipus de reducció tenen de manera natural una topologia de Grothendieck amb més propietats com son un Frobenius, una monodromia,... Anem a escriure-hi un parell de cosetes.
Suposem que X té bona reducció en λ, tenim la cohomologia cristal.lina que es compara amb la de de Rham (veieu p.9 [17]), que ens associa un $K_{0,\lambda}$-e.v. ($K_{0,\lambda}$ és la subextensió maximal no ramificada dins K_λ) junt amb un Frobenius i una filtració.
Tenim l'isomorfisme (Fontaine,Messing,Faltings,Kato,Tsuji):

$$H^m_{et}(\overline{X},\mathbb{Q}_l)\otimes_{\mathbb{Q}_l} B_{cris,l}\cong H^m_{cris}(Y_X/K_{0,\lambda})\otimes_{K_{0,\lambda}} B_{cris,l};$$

compatible amb G_{K_λ}, Frobenius i filtració.
En cas que X no té bona reducció en λ (ni potencialment bona reducció), però té reducció semiestable en λ (és a dir existeix un model propi $\mathcal{X}/\mathcal{O}_{K_\lambda}$ on localment per la topologia ètale és $\mathcal{O}_{K_\lambda}[t_1,\dots,t_n]/(t_1\cdot\ldots\cdot t_r-\pi)$, π uniformitzant de l'anell enters $\mathcal{O}_{K_\lambda}$) tenim una cohomologia de Grothendieck (cohomologia log-cristalina) que té una monodromia N, filtració, frobenius; (i també tenim un isomorfisme amb la cohomologia de de Rham $H^m_{log-cris}(\mathcal{X})\otimes_{K_{0,\lambda}}K\cong H^m_{dR}(X/K_\lambda)$ (com en el cas cristal.lí)), i obtenim un altre anell de Fontaine $B_{st,l}$ que ens la compara amb la cohomologia étale compatible amb aquestes estructures:
(Kato, Tsuji, Faltings)

$$H^m_{et}(\overline{X},\mathbb{Q}_l)\otimes_{\mathbb{Q}_l} B_{st,l}\cong H^m_{log-cris}(\mathcal{X})\otimes_{K_{0,\lambda}} B_{st,l},$$

isomorfisme compatible amb N, φ(Frobenius), G_{K_λ} i amb filtracions després de tensorialitzar $B_{dR,l} \otimes B_{st,l}$.
Per entendre millor necessitem dir alguna cosa sobre els anells de Fontaine B, (veieu la subsecció posterior §3.3.1) diem aquí que $B_{cris,l} \subset B_{st,l}$ i fixant uniformitzant $B_{st,l} \subset B_{dR,l}$ i la filtració en $B_{st,l}$ prové d'aquesta inclusió.
Denotem per B, si no es diu el contrari, a qualsevol dels anells de Fontaine amb $p = l$ $B_{cris,l}, B_{st,l}, B_{dR,l}$ o $B_{HT,l}$.

3.2.10 Lema. *1. Sigui V una representació p-àdica de G_{K_λ}. Llavors:*

$$dim_{K_B}(B \otimes_{\mathbb{Q}_l} V)^{G_{K_\lambda}} \leq dim_{\mathbb{Q}_l} V,$$

$$on\ K_B = \begin{cases} K_\lambda \text{ per a } B = B_{dR,l} \text{ o } B_{HT,l} \\ K_{0,\lambda} \text{ per a } B = B_{cris,l} \text{ o } B_{st,l} \end{cases}$$

2. Si tenim $dim_{K_B}(B \otimes_{\mathbb{Q}_l} V)^{G_{K_\lambda}} = dim_{\mathbb{Q}_l} V$, llavors el morfisme natural:

$$B \otimes_{K_B} (B \otimes_{\mathbb{Q}_l} V)^{G_{K_\lambda}} \to B \otimes_{\mathbb{Q}_l} V$$

és un isomorfisme.

3.2.11 Definició 1. Una representació p-àdica V de G_{K_λ} s'anomena B-admissible si $dim_{K_B}(B \otimes_{\mathbb{Q}_p} V)^{G_{K_\lambda}} = dim_{\mathbb{Q}_p} V$.
Si $B = B_{cris}$ s'anomena representació cristal.lina. Si $B = B_{st}$ s'anomena representació semiestable. Si $B = B_{dR}$ s'anomena representació de de Rham. Si $B = B_{HT}$ s'anomena representació de Hodge-Tate.

2. Una representació p-àdica V de G_{K_λ} s'anomena potencialment B-admissible si $dim_{K_B}(B \otimes_{\mathbb{Q}_p} V)^{G_{K'_\lambda}} = dim_{\mathbb{Q}_p} V$; amb K'_λ una extensió finita de K_λ dins $\overline{K_\lambda}$.
Si $B = B_{cris}$ s'anomena representació potencialment cristal.lina.
Si $B = B_{st}$ s'anomena representació potencialment semiestable.

3.2.12 Observació. Les nocions de potencialment Hodge-Tate i potencialment de Rham no existeixen ja que directament són aquestes representacions de Hodge-Tate i de de Rham respectivament.

Del lema 3.2.10 i dels teoremes de comparació obtenim que la representació p-adica amb $V = H^m_{et}(\overline{X}, \mathbb{Q}_l)$ és de Rham i de Hodge-Tate. A més si X té reducció semiestable és semiestable la G_{K_λ}-representació p-àdica V. I si X té bona reducció llavors V és cristal.lina. Si X té potencialment bona reducció llavors V és una representació potencialment cristal.lina, i si X té potencialment reducció semiestable, llavors V és potencialment semiestable.

3.2.13 Observació. El twist de Tate va bé amb els isomorfismes de comparació per tant provem que $H^m_{et}(\overline{X}, \mathbb{Q}_l)(r)$ és sempre de Rham i segons la seva reducció pot ser cristal.lina o semiestable. No obstant un gran resultat de l'any 2002 de Laurent Berger prova que no hi haurà diferencies entre representacions potencialment semiestables i de Rham ([2]).

3.2.14 Observació. Per simplificar la notació hem fet els isomorfismes de comparació per motius purs i a coeficients en $\mathbb{Q}$, amb això volem dir per $V = H^m_{et}(\overline{X}, \mathbb{Q}_p(r))$.

Si volem a coeficients en E enlloc de $\mathbb{Q}$, i per tant no treballar en $\mathbb{Q}_l$-representacions sinó en $L \cong E_\beta$-representacions de G_{K_λ} també hauriem d'obtenir els resultats anteriors sobre aquestes representacions amb la mateixes definicions (prenent aquest V E-espai vectorial com a $\mathbb{Q}_l$-espai vectorial en les definicions) i resultats anteriors, no obstant no ho he vist explícitament escrit.

3.2.15 Questió Considereu una varietat projectiva sobre un cos local K arbitrari i considerem la $l = p$-representació de G_K donada en $V = H^m(\overline{X}, \mathbb{Q}_l(r))$. Podeu trobar els anells de Fontaine per a obtenir els morfismes de comparació amb bona reducció i reducció semiestable? (Veieu §1 [12] per a la construcció de B_{cris} per a cossos locals amb cos residual no perfecte).

Denotem per $Rep_B(G_{K_\lambda})$ (o $Rep_{pB}(G_{K_\lambda})$) la categoria (tannakiana) formada per les representacions L-àdiques B-admissibles (o respectivament potencialment B-admissibles) tenim llavors el següent diagrama:

$$
\begin{tikzcd}
 & & & & Rep(G_{K_\lambda}) \\
 & Rep_{st}(G_{K_\lambda}) \arrow[dr] & & & Rep_{HT}(G_{K_\lambda}) \arrow[u] \\
Rep_{cris}(G_{K_\lambda}) \arrow[ur] \arrow[dr] & & Rep_{pst}(G_{K_\lambda}) & = & Rep_{dR}(G_{K_\lambda}) \arrow[u] \\
 & Rep_{pcris}(G_{K_\lambda}) \arrow[ur] & & &
\end{tikzcd}
$$

on $Rep(G_{K_\lambda})$ denota totes les representacions L-àdiques de G_{K_λ}, i cada $\rightarrow$ és estricta a excepció de la igualtat entre ser potencialment semiestable amb de Rham (Berger [2]).

3.2.16 Definició Una representació L^0-àdica de G_K que anomenem V, amb K un cos de nombres ($car(\kappa(L^0)) = l$), s'anomena geomètrica si existeix L i una L-representació de G_K, diem-li W, on $W \otimes_L L^0 \cong V$ com $L^0[G_K]$-representacions i la representació W compleix les dues condicions següents:

1. és no ramificada fora d'un conjunt finit de places de K (és a dir I_λ actua de manera trivial en la L-representació per tot λ a excepció d'un conjunt finit de $\lambda' s$).
2. La restricció de la L-representació a G_{K_λ} (λ no arquimediana) és potencialment semiestable (tan si $\kappa(\lambda) = p \neq l$ com $\kappa(\lambda) = l = p$).

3.2.17 Proposició. *Una L^0-representació simple (i irreductible) de la geometria algebraica és geomètrica.*

DEMOSTRACIÓ: Una L^0-representació de la geometria algebraica simple prové d'una L-representació de la geometria algebraica per un L-espai vectorial, per força ve d'un motiu pur (pel fet de ser simple la representació), per tant s'inclou $V \subset H^m_{et}(\overline{X}, \mathbb{Q}_l(r)) \otimes_{\mathbb{Q}_l} L$ per certa varietat llissa i projectiva X sobre $\mathbb{Q}$, amb certs m, r que ens donen el pes $w = m - 2r$ (és a dir prové dels motius purs de Chow amb pes w i amb multiplicació E on existeix $\beta \in \mathrm{Spec}(E)$ on $E_\beta \cong L$).

Per tant ens podem restringir a estudiar l'enunciat per la L-representació $V = H^m_{et}(\overline{X}, \mathbb{Q}_l(r)) \otimes_{\mathbb{Q}_l} L$. Ja sabem que fora de les places on X té mala reducció és no ramificada, per tant compleix la primera condició per tal de ser una representació geomètrica.
Restringim la representació a G_{K_λ}, si $\lambda \nmid \kappa(L) = l$ tenim pel corol.lari 3.2.7, és semiestable. Si $\lambda \mid \kappa(L) = l$, tenim que és de Rham pel teorema de comparació i pel resultat de Berger [2] que és semiestable. Per tant es compleix la segona propietat per ser una representació geomètrica. □

3.2.18 Observació. Podriem considerar la categoria tanakiana generada per totes les representacions de motius purs, són les que anomenem representacions semisimples, és la categoria de representacions semisimples i que provenen de la geometria algebraica. Aquesta categoria és subcategoria tanakiana de les representacions que provenen de la geometria algebraica (aquestes inclouen els motius mixtos). La proposició anterior prova que aquesta categoria es troba dins la categoria formada per representacions geomètriques. Per a extendre aquest resultat (proposició anterior) per a representacions irreductibles però no simples de la geometria algebraica (i.e. per a motius mixtes) s'estén l'argument anterior però pensant que la representació ens dona submòduls simples purs i escrivint-ho com Ext's de motius purs podem atacar-ne la semiestabilitat ($p = l$) obtenint que són representacions geomètriques.

Per tant hem provat que una representació L-àdica (mòdul conjectures bones en motius mixtes) de la geometria algebraica és llavors una representació L-àdica geomètrica.

3.2.19 Conjectura (Fontaine-Mazur, 1993) *Una representació irreductible L-àdica és geomètrica si i només si és de la geometria algebraica.*

3.2.20 Observació. Si la L-representació és potencialment abeliana, és a dir existeix un subgrup obert de G_K que opera en V a través d'un grup quocient abelià, llavors la condició de ser geomètrica, usant teoria de classes ens permet obtenir un caracter de Hecke i d'aquest una varietat abeliana CM amb el mòdul de Tate ($m = 1$ en cohomologia étale per la varietat) junt amb un twist de Tate convenient provant que és de la geometria algebraica (no obstant la construcció no és molt explícita i estaria bé escriure-ho amb més detall i més explícitament). Aquest és el primer cas en que podem provar la conjectura de Fontaine-Mazur.

3.2.21 Observació. El treball de Wiles [16] (i de Taylor-Wiles [15]) sobre el teorema de Fermat, permet associar una forma modular a certes representacions geomètriques de dimensió 2, i en particular veure que provenen de la geometria algebraica per a certa corba el.líptica amb $m = 1$ i $K = \mathbb{Q}$.

En general falten idees per a poder demostrar que una representació geomètrica és de la geometria algebraica i fins i tot centrant-nos en representacions simples irreductibles. No obstant el pes que hauria de tenir està determinat.

Fixem-nos que una representació irreductible V que sigui geomètrica de les propietats locals, són interessants únicament per a $\lambda \mid l = p$ (per al cas $l \neq p$, el resultat del Grothendieck (3.2.5), no tenim cap restricció, recordem K és en aquesta secció un cos de nombres). Ser semiestable per $\lambda \mid l = p = car(\kappa(L))$ implica que és de Hodge-Tate i es poden associar de manera fàcil els pesos de Hodge-Tate. Abans d'associar-los anem a definir el pes de V que denotem per $w(V)$. Si V és 1-dimensional existeix un únic enter i complint que l'acció de G_K és finita en $V(i)$ (això succeeix quan el pes és zero i com $w(V(i)) = w(V) - 2i$), definim llavors $w(V) := 2i$. Si V té dimensió N definim $w(V) := \frac{w(\wedge^N V)}{N}$ (si V és simple i de la geometria algebraica, serà un enter (cas motiu pur), si és geomètrica i és simple, per la conjectura de Fontaine-Mazur tindria que ser un enter).
A la representació V irreductible i geomètrica, per ser de Hodge-Tate li associem els pesos de Hodge Tate:

$$h(\lambda) := (h_r(\lambda))_r \; amb \; h_r(\lambda) := dim_L(\hat{\overline{L}}(r) \otimes_L V)^{G_{K_\lambda}},$$

per cada $\lambda | l = p = \kappa(L)$ i $r \in \mathbb{Z}$, usualment s'escriu $h_r(\lambda) = h_{r,s}(\lambda)$ amb $r, s \in \mathbb{Z}$ complint $r + s = w$. (Observem que per a qualsevol representació podem associar-li aquests pesos de Hodge-Tate).
Denotem per: $Geom(K, S, h)$ el conjunt de les L-representacions irreductibles de $G_{K,S}$ (i.e. representacions de G_K no ramificades fora

de S) amb pes h de Hodge-Tate fixats per cada $\lambda \mid \kappa(L) = l = p$ mòdul isomorfisme.

3.2.22 Conjectura *(Fontaine-Mazur) Per a qualsevol conjunt de places S amb $l = p = \kappa(L) \in S$, el conjunt $Geom(K, S, h)$ és finit.*

3.3 Estudi de representacions locals semiestables

Recordem que en aquesta secció K denota un cos local extensió finita de $\mathbb{Q}_p$ (tot i que alguns resultats són més genereals). Ens restringim a $\mathbb{Q}_l$-representacions enlloc de L-representacions.

3.3.1 Una pinzellada dels anells de Fontaine.

Considerem K un cos local extensió finita de $\mathbb{Q}_p$,(tot i que es possible fer-ho per cossos locals K amb cos residual no perfecte [12]).
Anem a introduir primer una noció vaga i no del tot precisa de que serà els cossos que nosaltres volem (anomenats anells de Fontaine).
Els volem obtenir com un anell de periodes, és a dir d'un pairing:

$$H^m_{dR}(X/\tilde{K}) \times H^m_{Betti}(X(\mathbb{C}), \mathbb{Q}) \to B$$

$$< \omega, \gamma > \mapsto b = \int_\gamma \omega$$

per tota X una varietat algebraica projectiva llisa sobre un cos de nombres $\tilde{K}$ (on K és la completació de $\tilde{K}$ en un plaça finita) de cert tipus aritmètic que estem interessats a estudiar, B és l'anell de comparació d'una cohomologia de diferencials amb una cohomologia provinent de la topologia de X.
Tensorialitzem la cohomologia de Betti per $\otimes_{\mathbb{Q}} \mathbb{Q}_l$ obtenint que és isomorfa a la cohomologia étale (Grothendieck) i preguntem-nos sobre aquest anell de períodes necessari per a comparar després d'aquesta tensorialització.
Si té bona reducció la varietat X/K, tenim que podem triar com anell de períodes l'anell $\mathbb{Q}_l$ si $l \neq p$ i l'anell de Fontaine anomenat

B_{cris} si $l = p$. Si X és varietat projectiva qualsevol tenim que quan $l = p$ l'anell de períodes és B_{dR}. Aquests anells de Fontaine (B's) ja han sortit en el seminari durant alguna edició per tant, solament en farem un breu resum i introduírem els anells corresponent a varietats semiestables tan en el cas $l = p$ com $l \neq p$ (aquest últim cas, pel resultat de Grothendieck 3.2.5, correspon també, llevat d'una extensió finita, amb els períodes de totes les varietats algebraiques projectives).

Anem a recordar breument la construcció de $B_{cris,p}$ (denotem per $B_{cris,l} = \mathbb{Q}_l$ quan $l \neq p$), i $B_{dR,p}$ cas $l = p$. Per a una exposició més extensa d'aquests anells podeu consultar la lectura 2 en [3].

Denotem per $\mathbb{C}_p \cong \hat{\overline{K}}$ i $\mathcal{O} := \mathcal{O}_{\mathbb{C}_p}$ el seu anell d'enters, obtenim l'anell integre de característica p i perfecte següent:

$$R_{\mathcal{O}} := \lim_{\leftarrow}(\mathcal{O}/p \leftarrow \mathcal{O}/p \leftarrow \ldots)$$

amb morfismes elevar a p, és a dir $a \mapsto a^p$. Considerem el morfisme de Teichmuller $[\ ] : R_{\mathcal{O}} \to W(R_{\mathcal{O}})$, ($W$ denota l'anell de Witt) i sigui $\underline{p} := (p^{(n)}) \in R_{\mathcal{O}}$ sistema compatible de p^n-arrels de p, i $\underline{\epsilon} := (\epsilon^{(n)}) \in R_{\mathcal{O}}$ format per sistema arrels p^n-èssimes de 1. Definim per

$$A_{cris,p} := \{\sum w_n \frac{(p - [\underline{p}])^n}{n!},\ w_n \to 0,\ w_n \in W(R_{\mathcal{O}})\}$$

considerem l'element de $A_{cris,p}$ següent

$$t = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{([\underline{\epsilon}] - 1)^n}{n} = \sum_{n=1}^{\infty} (n-1)!(-1)^{n+1} \frac{([\underline{\epsilon}] - 1)^n}{n!} \in A_{cris,p},$$

s'obté de σ el Frobenius en l'anell de Witt s'estén a $A_{cris,p}$, denotem per $B^+_{cris,p} := A_{cris,p}[1/p]$ i $B_{cris,p} := B_{cris,p}[1/t]$, l'element t dona la filtració en el cos $B_{cris,p}$ on $B^+_{cris,p}$ és anell de valoració discreta $val(t) = 1$. Tenim doncs que $B_{cris,p}$ és un anell amb filtració i amb un Frobenius φ provinent de σ i una acció de G_K. Compleix $B^{G_K}_{cris,p} = K_0$ (maxima subextensió de K no ramificada enlloc)

Anem a definir $B_{dR,p}$. Definim $B^+_{dR,p} := \lim\limits_{\longleftarrow} \dfrac{W(R_{\mathcal{O}})[1/p]}{(p - [\underline{p}])^n}$ que és un anell de valoriació discreta complet amb maximal $\mathfrak{m} = (p - [\underline{p}])$, i $B_{dR,p} := Quot(B^+_{dR,p})$. Tenim que $t \in (p - [\underline{p}])$ i és uniformitzant,

dona així una filtració on $Fil^m B_{dR,m}/Fil^{m+1}B_{dR,p} = \mathbb{C}_p(m)$. A més $B_{dR,p}$ té acció natural de G_K complint $B_{dR,p}^{G_K} = K$, i tenim de manera natural $B_{cris,p} \subset B_{dR,p}$.
Després d'aquest repàs d'aquests dos anells de Fontaine anem a introduir el B_{st}.
L'anell B_{st}.
Escrivim per $B_l = \begin{cases} \mathbb{Q}_l & si\ l \neq p\ amb\ G_K - acció\ trivial \\ B_{cris,p} & si\ l = p \end{cases}$
elegim $q \in K$ que no sigui 0 ni una unitat. Anem a definir $B_{st,l,q}$ una B_l-àlgebra amb G_K-acció i una derivació $N : B_{st,l,q} \to B_{st,l,q}$ de nucli B_l.
Sigui $T_{l,q} := \varprojlim_{n\in\mathbb{N}} (\overline{K}/q^{\mathbb{Z}})_{l^n}$ i $W_{l,q} := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_{l,q}$. Considerem $a = (a_n) \in T_{l,q}$, elegim $\tilde{a_n}$ de a_n en $\overline{K}$ compleix que existeixen $r_n \in \mathbb{Z}$ tal que $\tilde{a_n}^{l^n} = q^{r_n}$ amb $r_n \overset{n\to\infty}{\longrightarrow} v(a) \in \mathbb{Z}_l$ on aquest element és independent d'aquests aixecaments elegits de a, aquest v s'estén a $W_{l,q}$ amb linealitat, és G_K-equivariant i té nucli $\mathbb{Q}_l(1)$, és a dir tenim (tensoriatitzant per $\otimes_{\mathbb{Q}_l}\mathbb{Q}_l(-1)$):

$$0 \to \mathbb{Q}_l \to W_{l,q}(-1) \to \mathbb{Q}_l(-1) \to 0.$$

Considerem la $\mathbb{Q}_l$-àlgebra $Sym_{\mathbb{Q}_l} W_{l,q}(-1)$ que és isomorfa a l'àlgebra de polinomis en dues indeterminades. Denotem per

$$B_{l,q} := Sym_{\mathbb{Q}_l} W_{l,q}(-1)/(''1\ en\ grau\ 0 = 1\ en\ grau\ 1'')$$

que denota a un anell de polinomis a coeficients en $\mathbb{Q}_l$ en indeterminada u amb $u \in W_{l,q}(-1)$, $u \notin \mathbb{Q}_l$ amb acció de G_K. Definim en $B_{l,q}$ una derivació,

$$N : B_{l,q} \to B_{l,q}(-1)$$

la $\mathbb{Q}_l$-derivació que a $u \in V_{l,q}(-1)$ va a $1 \otimes v(u) \in V_{l,q}(-1) \otimes \mathbb{Q}_l(1)$. Anem doncs a definir els anells de Fontaine semiestables per,

$$\begin{cases} B_{st,l,q} := B_{l,q}\ si\ l \neq p \\ B_{st,l,q} := B_{cris,p} \otimes_{\mathbb{Q}_p} B_{p,q}\ si\ l = p \end{cases}$$

En el cas $l = p$ tenim en $B_{st,l,q}$ una G_K-acció via $g(b \otimes c) = gb \otimes gc$, acció Frobenius φ:$\varphi(b \otimes c) = \varphi(b) \otimes c$, d'una derivació $N(b \otimes c) = b \otimes N(c)$ on $b \in B_{cris}$ i $c \in B_{st,p,q}$. Es comprova que φ i N commuten amb G_K (i si fem actuar φ sobre $B_{st,p,q}(-1)$ per $\varphi(b \otimes c) = \varphi(b) \otimes c$ llavors N commuta amb φ).

3.3.1 Observació. Usualment el $B_{st,p,q}$ pel teorema de comparació que hem vist en la secció anterior es pren q un uniformitzant de K i a més té un operador $N : B_{st,p,q} \to B_{st,p,q}$ (i a més una filtració però que encara no li hem introduït!!!). Per relacionar la nostra definició amb aquesta, observem que $\mathbb{Q}_p(1) \subset B_{cris,p}$ on si t generador de $\mathbb{Q}_p(1)$ va al t definit anteriorment en $B_{cris,p}$,

$$\begin{aligned} i : B_{st,p,q}(-1) &\to B_{st,p,q} \\ b \otimes t^{-1} &\mapsto bt^{-1}, \end{aligned}$$

i es defineix l'operador de monodromia per $N_{mon} := i \circ N$ (si $val(q) \geq 0$ que és el cas de triar q un uniformitzant).

3.3.2 Observació. Referent a la dependència de q. Si $l = p$ tenim un isomorfisme canònic entre $B_{st,p,q} \cong B_{st,p,q'}$ compatible amb G_K i φ, però no sempre amb N, únicament és compatible en N si q/q' és una unitat de K.
Si $l \neq p$ tenim iso canònic si $\overline{q}$ i $\overline{q}'$ generen el mateix s.e.v en $Kum_l(K) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \varprojlim_n (K^*/K^{*l^n}) = H^1(K, \mathbb{Q}_l(1))$ (que sempre es compleix si el cos residual de K és finit).

Podriem pensar $B_{st,p,q} = B_{cris,p}(u)$ amb u una indeterminada. Si volem introduir-hi una filtració i pensar com l'anell de periodes (és anell de comparació), és a dir u com un període, estem pensant aquest anell dins de $B_{dR,p}$ i aquesta inclusió ens dona la filtració en $B_{st,p,q}$ però depèn fortament de q aquesta inclusió!!!

$$B_{cris,p} \to B_{st,p,q} \to B_{dR,p}$$

on $u \mapsto log(b) \in B_{dR,p}$, aquest b es construeix usant el q triat ($val(q) = 1$ ara) que prové d'un període concret en una corba el.líptica de Tate, veieu la construcció explicíta del període $log(b)$ en la pàgina 13-14, exemple 12 [17].

3.3.2 Mòduls de Deligne ($l \neq p$ i $l = p$)

Sigui V una representació l-àdica de G_K, anem a associar-hi uns mòduls que ens donen informació de V. Deixeu-me escriure que les proves dels resultats següents les trobeu en [10].

3.3.3 Definició (Mòdul de Deligne)

1. Suposem $l \neq p$. Un l-mòdul de Deligne (relatiu a $\overline{K}/K$) es donar un $\mathbb{Q}_l$-espai vectorial Δ junt amb una acció lineal de G_K i una aplicació $\mathbb{Q}_l$-lineal G_K-equivariant
$$N : \Delta \to \Delta(-1).$$

2. Suposem $l = p$. Sigui $\overline{k}$ el cos residual de $\overline{K}$ i denotem per $P_0 = Quot(W(\overline{k}))$ el cos de fraccions de l'anell de Witt $W(\overline{k})$; P_0 té acció natural de G_K (amb I_K actuant trivialment) i un Frobenius σ.
Un p-mòdul de Deligne és donar un P_0-espai vectorial Δ junt amb una acció semi-lineal de G_K, un frobenius
$$\varphi : \Delta \to \Delta$$
σ-lineal, injectiu i commutant amb l'acció de Galois i d'una aplicació P_0-lineal, G_K-equivariant:
$$N : \Delta \to \Delta$$
verificant $N\varphi = p\varphi N$

S'anomena la dimensió d'un mòdul de Deligne a la dimensió com espai vectorial (com $\mathbb{Q}_l$-e.v. si $l \neq p$ o bé com P_0-e.v. si $l = p$).

Els mòduls de Deligne formen una categoria tannakiana, on els morfismes son aplicacions lineals ($\mathbb{Q}_l$ si $l \neq p$, P_0 si $l = p$), commuta l'acció de G_K i de N i amb φ si $l = p$. Denotem per $\underline{Del}_*(G_K)$ la subcategoria plena dels $*$-mòduls de Deligne amb $dim\Delta < \infty$ complint:

1. l'acció de G_K és contínua i I_K actua a traves d'un quocient finit.

2. l'operador de monodromia N és nilpotent (per $l \neq p$ denotem per N també a $N \otimes id(-i) : \Delta(-i) \to \Delta(-i-1)$).

(Observeu que la segona condició es satisfà directament per $l = p$ ja que no hi ha aplicació P_0-lineal on $N\varphi = p^r\varphi N$ per $r >> 0$, i per $l \neq p$ també es compleix si el cos residual és finit).
Anem a construir un mòdul de Deligne a partir d'una representació. Considerem doncs V una representació l-àdica de G_K i considerem

$$V \otimes_{\mathbb{Q}_l} B_{st,l}$$

és un l-mòdul de Deligne (a partir d'ara l pot ser $= p$ o $\neq p$ si no s'especifica) amb:

$$g(v \otimes b) = gv \otimes gb,\ g \in G_K,\ v \in\ V,\ b \in B_{st,l}$$

$$N(v \otimes b) = v \otimes Nb,$$

$$(si\ l = p\ exigim)\ \varphi(v \otimes b) = v \otimes \varphi(b).$$

Recordem que localment donar representacions per $l \neq p$ correspon a donar una acció de N i de G_K(és una cosa coneguda pels especialistes en el camp, veieu per exemple lemma 3.1.1. en lecture 3 de Breuil en [3], i observeu aquí que la restricció que posa en la lecture 3 per la potència en p de commuta frobenius de G_K amb N prové del twist de com aquí definim l'operador de monodromia en els mòduls de Deligne per a $l \neq p$) , amb aquesta idea i per caracteritzar les representacions potencialment amb certes propietats, considerem el l-mòdul de Deligne:

$$\underline{\hat{D}}_{pst,q}(V) := \varinjlim_{H \in \mathcal{H}} (B_{st,l} \otimes_{\mathbb{Q}_l} V)^H,$$

on $\mathcal{H}$ té per elements els subgrups oberts de I_K.

3.3.4 Teorema. *Sigui V una representació l-àdica de G_K i $\Delta = \underline{\hat{D}}_{pst,q}(V)$. Llavors:*

1. *$dim\Delta \leq dim_{\mathbb{Q}_l} V$ i $\Delta \in \underline{Del}_l(G_K)$.*
2. *L'aplicació natural,*

$$\alpha_V : B_{st,l,q} \otimes \Delta \to B \otimes_{\mathbb{Q}_l} V$$

és injectiva.

3. *Les següents afirmacions són equivalents:*

   (a) $dim(\Delta) = dim_{\mathbb{Q}_l} V$

   (b) α_V *és isomorfisme,*

   (c) V *és potencialment semiestable,*

   (d) *existeix* K'/K *finita on* Δ *com element de* $\underline{Del}_l(G_{K'})$ *tenim que* I_L *actua trivialment.*

D'aquí obtenim una manera via moduls de Deligne com saber si una representació local és semiestable, de bona reducció,...

3.3.5 Corol·lari. *Denotem per* B_l *el cos* $\mathbb{Q}_l$ *si* $l \neq p$ *i pel cos* B_{cris} *si* $l = p$. *Donada* V *una representació* l*-àdica denotem per:*

$$\hat{\underline{D}}_{st,q}(V) := (B_{st,q} \otimes_{\mathbb{Q}_l} V)^{I_K},\ \hat{\underline{D}}_f(V) := (B_l \otimes V)^{I_K},\ \hat{\underline{D}}_{pf}(V) := \varinjlim_{H \in \mathcal{H}} (B_l \otimes V)^H.$$

Sigui V *una representació potencialment semiestable de* G_K *i* $\Delta = \hat{\underline{D}}_{pst,q}(V)$. *Llavors:*

1. V *semiestable* $\Leftrightarrow$ I_K *opera trivialment sobre* Δ *i* $\Delta = \hat{\underline{D}}_{st}(V)$.

2. V *potencialment bona-reducció* $\Leftrightarrow$ $N = 0$ *sobre* Δ *i llavors* $\Delta = \hat{\underline{D}}_{pf}(V)$.

3. V *bona reducció* $\Leftrightarrow$ $N = 0$ *i* I_K *actua trivialment en* Δ.

Preguntem-nos si donat un mòdul de Deligne $\underline{Del}$ un pot obtenir la representació, la resposta és NO per a $l = p$ i SI per a $l \neq p$:

3.3.6 Proposició. *Sigui* $p \neq l$. *Sigui* $\Delta \in \underline{Del}_l(G_K)$, *definim per*

$$\underline{V}_{pst}(\Delta) := \{v \in B_{st,q} \otimes \Delta | Nv = 0\}.$$

Llavors;

1. $\underline{V}_{pst}(\Delta) \in Rep_{\mathbb{Q}_l,pst}(G_K)$,

2. $\underline{V}_{pst}$ *indueix una* $\otimes$*-equivalència entre* $\underline{Del}_l(G_K)$ *i* $Rep_{\mathbb{Q}_l,pst}(G_K)$ *on* $\hat{\underline{D}}_{pst}$ *és el quasi-invers.*

3.3.7 Observació. Quan $l = p$, necessitem posar una filtració en $\underline{\hat{D}}_{pst}(V)$ per a poder retrobar V del mòdul de Deligne, per fer això de com triem el logaritme q obtenim

$$B_{st,p,q} \subset B_{dR}$$

i això ens permet identificar $(\overline{K} \otimes_{K_0} \underline{D}_{pst}(V))^{G_K}$ amb $D_{dR}(V)$ i per tant una filtració. Fontaine proposa en [10] posar aquesta filtració en els mòduls de Deligne per a obtenir l'equivalència de categories.

3.3.8 Observació. Crec que es pot fer una modificació per L-representacions definint L-mòduls de Deligne i obtenir el resultat anteriors, no obstant falta comprovar-ho en detall (exercici).

3.3.3 Mòduls amb Frobenius i monodromia. Afegim-hi filtració.

Anem a introduir una noció equivalent de mòduls de Deligne posant-hi en aquest llenguatge la filtració que comentàven que necessitem per $p = l$ (en l'acabament de la subsecció anterior). **Aquí durant tota aquesta subsecció imposem que** $l = p$. Deixem escrit que les proves dels resultats següents i/o indicacions amb referències per les proves les podeu trobar a [10] i [3].

Sigui K' una extensió de K.

3.3.9 Definició Un $(\varphi, N, G_{K'/K})$-mòdul és un K_0'-espai vectorial D (recordem si M és un cos local M_0 és la maxima subextensió de M no ramificada) amb:

1. $\varphi : D \to D$ σ-lineal (σ és el Frobenius de K_0')
2. aplicació K_0'-lineal $N : D \to D$,
3. acció semilineal de $G_{K'/K}$ complint
   (a) $N\varphi = p\varphi N$
   (b) $\forall g \in G_{K'/K}$ $g\varphi = \varphi g$ i $gN = Ng$.

3.3.10 Definició Diem que un $(\varphi, N, G_{K'/K})$-mòdul és discret si $\{g \in G_{K'/K} | gd = d, \ \forall d \in D\}$ és un obert a $G_{K'/K}$.

Considerem,

$$\underline{Mod}(\varphi, N, G_{K'/K})$$

la subcategoria plena dels $(\varphi, N, G_{K'/K})$-mòduls on els seus objectes són '$(\varphi, N, G_{K'/K})$-mòduls discrets de dimensió finita on es defineix la dimensió d'un $(\varphi, N, G_{K'/K})$-mòdul per $dimD := dim_{K'_0} D$. Denotem els $(\varphi, N, 1)$-mòduls com (φ, N)-mòduls.

3.3.11 Proposició. *Considerem el següent funtor:*

$$\underline{Co} : \underline{Mod}(\varphi, N, G_K) \to \underline{Del}_p(G_K)$$

$$D \mapsto P_0 \otimes_{K_0^{nr}} D.$$

És una $\otimes$-equivalència de categories.

Prenem $K' = K$ i per tant (φ, N)-mòduls (aquesta simplificació fa que ens restringim en aquesta secció a trobar una categoria de mòduls equivalent a representacions semi-estables sobre K enlloc de potencialment semiestables, veieu observació 3.3.18).

3.3.12 Definició Un (φ, N)-mòdul filtrat és un (φ, N)-mòdul D amb una filtració decreixent en $D_K := D \otimes_{K_0} K$, $(Fil^i D_K)_{i \in \mathbb{Z}}$ per K-espais vectorials on $Fil^i D_K = D_K$ per $i << 0$ i $Fil^i D_K = 0$ per $i >> 0$.

Considerem D un (φ, N)-mòdul filtrat, $d = dimD = dim_{K_0} D$, obtenim que $\otimes_{K_0}^d D$ és un (φ, N)-mòdul filtrat amb $\varphi := \otimes^d \varphi$ i $N := N \otimes \ldots \otimes 1 + 1 \otimes N \otimes 1 \otimes \ldots \otimes 1 + 1 \otimes \ldots \otimes 1 \otimes N$, i filtració $Fil^i(\otimes^d D_K) := \sum_{i_1 + \ldots + i_d = i} Fil^{i_1} D_K \otimes \ldots \otimes Fil^{i_d} D_K$. Igualment podem considerar $\wedge_{K_0}^d D$ com un (φ, N)-mòdul filtrat amb l'estructura provinent de $\otimes D$. Del fet que $dim_{K_0}(\wedge_{K_0}^d D) = 1$ existeix un únic $i_0 \in \mathbb{Z}$ complint,

$$Fil^i(\wedge^d D_K) = \begin{cases} \wedge^d{}_K D_K \ per \ i \leq i_0 \\ 0 \ per \ i > i_0 \end{cases}$$

Igualment obtenim que existeix un únic $\alpha_0 \in \mathbb{Z}$ on $e_1 \in \wedge_{K_0}^d D \setminus \{0\}$ $\varphi(e_1) = \lambda_0 e_1$ amb $val(\lambda_0) = \alpha_0$.
Es defineix $t_H(D) := i_0$ i $t_N(D) := \alpha_0$.

3.3.13 Definició Donat D un (φ, N)-mòdul filtrat. Diem que D' és un (φ, N)-submòdul filtrat de D, si és un (φ, N)-mòdul amb $D' \hookrightarrow D$ commutant amb φ i N i complint $Fil^i(D'_K) = D'_K \cap Fil^i(D_K)$.

Anem a definir els mòduls pels quals obtindrem una equivalència de categories amb les representacions semiestables pel cas $p = l$.

3.3.14 Definició Sigui D un (φ, N)-mòdul filtrat. D s'anomena dèbilment admissible (=:w.a.=weak admissible) si compleix que $t_H(D) = t_N(D)$ i a més $t_H(D') \leq t_N(D')$ per a qualsevol (φ, N)-submòdul filtrat D' de D.

Fent la immersió de B_{st} en B_{dR} (triant així un uniformitzant concret) obtenim una filtració en $B_{st,p,q}$ donada per $Fil^m(B_{st,p,q}) := B_{st,p,q} \cap Fil^m(B_{dR})$.

3.3.15 Lema. *Sigui V una representació l-àdica de G_K (recordeu $l = p$). Sigui $D_{st}(V) := (B_{st,q} \otimes_{\mathbb{Q}_p} V)^{G_K}$ i definim en $D_{st}(V)$ el frobenius per $\varphi := \varphi_{B_{st,q}} \otimes Id$, $N = N_{B_{st,q}} \otimes Id$ i $Fil^i D_{st}(V)_K := (Fil^i B_{st,q} \otimes V) \cap D_{st}(V)_K$. Llavors;*
$D_{st}(V)$ és un (φ, N)-mòdul filtrat dèbilment admissible.

Denotem per

$$\underline{MF}^f_{K/K}$$

la categoria dels (φ, N)-mòduls filtrats discrets de dimensió finita que són dèbilment admissibles.

3.3.16 Teorema. (Colmez-Fontaine,[4]) *El functor,*

$$D_{st} : Rep_{st,\mathbb{Q}_p}(G_K) \to \underline{MF}^f_{K/K}(\varphi, N)$$

$$V \mapsto (B_{st,q} \otimes_{\mathbb{Q}_p} V)^{G_K}$$

és una equivalència de categories. S'obté V mitjançant,

$$V \cong \underline{V}_{st}(D_{st}(V)) = Hom_{\varphi,N,Fil^\cdot,K_0-lineal}(D^*_{st}(V), B^+_{st,q}).$$

3.3.17 Observació. Observeu que si $N = 0$ en el (φ, N)-mòdul debilment admissible, llavors correspon a una representació cristal.lina.

3.3.18 Observació. Per a obtenir l'anterior resultat per a potencialment semiestables, tindriem que obtenir una inclusió de mòduls filtrats admissibles per extensions finites i prendre després limit inductiu.
Treballant amb $N = 0$ en aquests limit inductius de mòduls dèbilment admissibles trobariem l'equivalència amb les representacions potencialment cristal.lines.

Si enlloc de treballar amb $\mathbb{Q}_p$-representacions volem treballar amb L-representacions cal introduir algunes modificacions en la definició de (φ, N)-mòduls i la filtració, com per exemple treballar en $K_0 \otimes_{\mathbb{Q}_p} L$-mòduls enlloc de K_0-espai vectorial, per veure les generalitzacions en detall consulteu [4].

3.3.19 Observació. Per a veure exemples concrets d'aquest mòduls filtrats i fer-ne la llista completa en dimensió 2 en alguns casos i llegir-ne les cristal.lines, consulteu §11 i §12 en [11].

Bibliografia

[1] *Barsotti, I.*: Varietà abeliane su corpi p-adici. I. Symposia Mathematica (INDAM, Rome, 1967/68),Vol.1 (1969), 109–173.

[2] *Berger, L.*: Représentations p-adiques et équations différentielles. Inv.Math. 148 (2002), 219-284.

[3] *Breuil,C.*: p-adic Hodge theory, deformations and local Langlands. In Advanced course on Modular forms and p-adic Hodge theory. Quaderns num. 20 (july 2001) in CRM (Barcelona), pp.7-82.

[4] *Colmez, P., Fontaine, J.-M.*: Construction des représentations p-adiques semi-stables. Inv.Math.140, 2000, 1-43.

[5] *Deligne, P.*: Résumé des premiers exposés de A. Grothendieck, 1–24 I, SGA 7, Exposé I. LNM 288 Groupes de Monodromie en Géométrie Algébrique, 1972. 1995.

[6] *Deligne, P.*: Valeurs de fonctions L et periodes d'integrals. Proc.Symp. Pure Math. 33 (2), 1979.

[7] *Deligne, P.*:La conjecture de Weil: II. Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), 137–252.

[8] *Fontaine, J.M.*: Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate. Journées de Géométrie Algébrique de Rennes (Rennes, 1978). Astérisque 65(1979) Vol.III, 3–80.

[9] *Fontaine, J.M.*: Représentations p-adiques semi-stables. Exposé III in Périodes p-adiques (Bures-sur-Yvette, 1998). Astérisque 223(1994), 113-184.

[10] *Fontaine, J.M.*: Représentations l-adiques potentiellement semi-stables. Exposé VIII in Périodes p-adiques (Bures-sur-Yvette, 1998). Astérisque 223(1994), 321-347.

[11] *Fontaine, J.M. i Mazur, B.*: Geometric Galois Representations. Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[12] *Kato, K.*: Generalized explicit reciprocity laws. Adv. Stud. Contemp. Math.1(1999),57–126.

[13] *Khare, Ch. i Ramakrishna, R.*: Finiteness of Selmer groups and deformation rings. Invent.math.154 (2003), 179-198.

[14] *Ramakrishna, R.*: Infinitely ramified Galois representations. Ann.Math.(2)151 (2000), 793–815.

[15] *Taylor, R. i Wiles, A.*: Ring theoretic properties of certain Hecke algebras. Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[16] *Wiles, A.*: Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443–551.

[17] *Xarles, X.*: Comparison theorems between crystalline and ètale cohomology: a short introduction. Publicat en la pàgina web personal d'en X.Xarles a http://mat.uab.es/∼xarles/articles.htm

Francesc Bars Cortina
Depart. Matemàtiques, Edifici C,
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona,
Catalunya. Spain.
e-mail: francesc@mat.uab.es

Capítol 4

El mètode de Taylor-Wiles

P. Bayer

Introducció

Wiles [Wi1995] i Taylor-Wiles [Ta-Wi1995] demostraren la modularitat sobre $\mathbb{Q}$ de representacions p-àdiques residualment modulars sotmeses a certes condicions sobre la irreductibilitat i la ramificació de la representació residual. Els seus resultats permeteren demostrar la conjectura de Shimura-Taniyama-Weil per a una àmplia classe de corbes el·líptiques definides sobre $\mathbb{Q}$, que inclou les corbes el·líptiques $E/\mathbb{Q}$ semiestables. El seu mètode de demostració de la modularitat consisteix en identificar un anell de deformació universal amb una àlgebra de Hecke, que és una intersecció completa.

Diversos autors han intentat millorar els resultats de Wiles i de Taylor-Wiles afeblint les condicions exigides per aquests autors a la representació de partida. En particular, un avenç degut a Diamond [Di1996] permeté obtenir la modularitat de les corbes el·líptiques $E/\mathbb{Q}$ amb reducció semiestable en $p = 3$ i en $p = 5$.

Skinner i Wiles [Sk-Wi1999] demostraren la modularitat sobre un cos de nombres totalment real de representacions p-àdiques potencial-

---

Amb finançament parcial de MCYT BFM2003-01898.

ment ordinàries en p i residualment reductibles. El seu resultat avala la conjectura de Fontaine-Mazur. El seu mètode no identifica un anell de deformació amb una àlgebra de Hecke, com en el cas de Wiles i de Taylor-Wiles, sinó que restringeix el problema de deformació a un cos totalment real F escaient, a fi de fer més gran la codimensió del lloc de les deformacions reductibles en l'espai de les deformacions de la representació residual restringida a F. El cos F pot ésser escollit resoluble sobre $\mathbb{Q}$, amb la qual cosa el resultat final s'obté per un canvi de base realitzat d'acord amb la teoria de Langlands.

Skinner i Wiles [Sk-Wi2001] demostraren la modularitat sobre un cos de nombres F totalment real de representacions p-àdiques, gairebé ordinàries en les places que divideixen p, residualment modulars i residualment irreductibles. En el cas $F = \mathbb{Q}$, els seus resultats milloren els de Wiles i de Taylor-Wiles esmentats abans.

Altres millores obtingudes posteriorment en proves de modularitat (cf. els treballs de Breuil) han permès demostrar la conjectura de Shimura-Taniyama-Weil per a totes les corbes el·líptiques $E/\mathbb{Q}$.

Notacions

En tot el treball emprarem les notacions que segueixen:

$p \neq 2$, un nombre primer fixat;

$p^* := (-1)^{\frac{p-1}{2}} p$;

$\ell \neq p$, un nombre primer;

F, un cos totalment real;

$d := [F : \mathbb{Q}]$;

$\overline{F} \hookrightarrow \overline{F}_v$, $v|p$, una immersió fixada de clausures algebraiques;

$z_1, \ldots, z_d$, les conjugacions complexes de F;

Σ, un conjunt finit de places de F;

F_Σ, una extensió maximal de F no ramificada fora de Σ i de $v|\infty$;

$\{v_1, \ldots, v_t\}$, el conjunt de les places de F dividint p;

E, una extensió finita de $\mathbb{Q}_p$;

$\mathcal{O}_E$, l'anell d'enters de E;

λ, l'ideal maximal de $\mathcal{O}_E$;

$k := \mathcal{O}_E/\lambda$, el cos residual de $\mathcal{O}_E$.

4.1 El teorema de Wiles i de Taylor-Wiles

El teorema següent és un dels resultats clau de [Wi1995] i [Ta-Wi1995].

4.1.1 Teorema. *Suposem donada una representació*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathcal{O}_E)$$

contínua, irreductible i no ramificada fora d'un conjunt finit de primers. Suposem que se satisfan les condicions següents:

(i) *La representació residual* $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}(2, k)$ *prové d'una forma modular. És a dir,* ρ *és residualment modular.*

(ii) $\det\rho = \varepsilon$, *on* ε *denota el caràcter ciclotòmic.*

(iii) *La representació* $\overline{\rho}$ *restringida a* $\mathbb{Q}(\sqrt{p^*})$ *és absolutament irreductible.*

(iv) *La representació* $\overline{\rho} \otimes \overline{\mathbb{F}}_p$ *restringida al grup de descomposició en* p, D_p, *i al grup d'inèrcia en* p, I_p, *es comporta com*

$$\overline{\rho}_{|D_p} \simeq \begin{bmatrix} \psi_1 & * \\ 0 & \psi_2 \end{bmatrix}, \quad \overline{\rho}_{|I_p} \simeq \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}.$$

És a dir, ρ *és residualment ordinària.*

(v) *Per a cada nombre primer* $\ell \equiv -1 (\mathrm{mod}\, p)$, *o bé la representació* $\overline{\rho}_{|I_\ell}$ *és absolutament irreductible, o bé la representació* $\overline{\rho}_{|D_\ell}$ *és reductible sobre la clausura algebraica.*

Aleshores, la representació ρ *és modular.*

En la resta de la secció donarem algunes indicacions sobre la demostració del teorema 4.1.1. Comencem per considerar:

$\mathcal{D} = (\mathcal{O}, \Sigma, \mathcal{M})$, $\mathcal{M} \subseteq \Sigma$, una dada de deformació;

$R_{\mathcal{D}}$, l'anell universal de les deformacions de ρ de dada $\mathcal{D}$;

$\mathbb{T}_{\mathcal{D}}$, l'anell de les deformacions de ρ que són modulars.

L'estratègia de Wiles consisteix en veure que la modularitat és un tret que s'encomana. Més concretament, es tracta de provar que l'existència d'un cert epimorfisme

$$R_{\mathcal{D}} \to \mathbb{T}_{\mathcal{D}}$$

permet deduir l'existència d'un isomorfisme

$$R_{\mathcal{D}} \simeq \mathbb{T}_{\mathcal{D}},$$

per a una dada de deformació $\mathcal{D}$ convenient.

Wiles [Wi1995] procedeix de la manera següent: donat un conjunt finit de primers, Q, es consideren dades de deformació ampliades, $\mathcal{D}_Q$, que provenen d'aixecaments de nivells, i es procedeix per inducció. Es defineix una dada de deformació minimal, ϕ, en la qual Σ és igual a $\mathcal{M} \cup \{p\}$. La demostració del teorema es redueix al cas minimal. La prova en aquest cas es realitza sota el supòsit que $\mathbb{T}_{\phi}$ és un anell d'intersecció completa. Aquestes demostracions utilitzen el treball de molts altres autors en relació a la conjectura de Serre [Se1987], (3.2.4?). La demostració que $\mathbb{T}_{\phi}$ és, efectivament, un anell d'intersecció completa és donada a Taylor-Wiles [Ta-Wi1995].

4.1.1 Deformacions de tipus Q

A una representació residual $\overline{\rho}$, com abans, li associarem una sèrie de dades de deformació. Prèviament cal definir:

$$Q, \quad N_Q, \quad \chi_Q, \quad R_Q, \quad \mathfrak{m}_Q, \quad \mathbb{T}_Q.$$

El conjunt Q. És un conjunt finit de primers q que satisfan les condicions següents:

(i) La representació $\overline{\rho}$ és no ramificada en q.

(ii) Per a tot $q \in Q$, és $q \equiv 1 \pmod{p}$.

(iii) $\overline{\rho}(\mathrm{Frob}_q) \otimes \overline{\mathbb{F}}_q = \begin{bmatrix} \alpha_q & 0 \\ 0 & \beta_q \end{bmatrix}, \quad \alpha_q \neq \beta_q.$

El nivell N_Q. D'acord amb un teorema de Carayol, el nivell es defineix com

$$N_Q = N(\overline{\rho}) \prod_{q \in Q} q\, p^{\delta},$$

on $N(\overline{\rho})$ denota el conductor de $\overline{\rho}$. Aquí $\delta = 0$ si $\overline{\rho}$ és plana i $\delta = 1$, altrament.

El caràcter χ_Q. Per a cada $q \in Q$, sigui Δ_q el p-subgrup de Sylow de $(\mathbb{Z}/q\mathbb{Z})^*$. Denotem per $\chi_q : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^* \to \Delta_q$. Aleshores,

$$\chi_Q := \prod_{q \in Q} \chi_q.$$

Notem que l'ordre del caràcter χ_Q és una potència de p.

L'anell R_Q. Aquest anell prové d'una deformació universal de tipus Q. En parlem tot seguit.

4.1.2 Definició Sigui A una $\mathcal{O}$-àlgebra noetheriana, completa i local. Designem per $\mathfrak{m}_A$ el seu ideal maximal. Una representació contínua

$$\widetilde{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}(2, A)$$

és diu que és una deformació de $\overline{\rho}$ de tipus Q si satisfà les condicions següents:

(i) La reducció de $\widetilde{\rho}$ mòdul $\mathfrak{m}_A$ és igual a $\overline{\rho}$.

(ii) El caràcter $\varepsilon^{-1} \det \widetilde{\rho}$ és d'ordre finit i primer amb p.

(iii) Si $\ell \notin Q \cup \{p\}$ i $\overline{\rho}_{|I_\ell}$ és semisimple, aleshores $\widetilde{\rho}(I_\ell) \simeq \overline{\rho}(I_\ell)$.

(iv) Si $\ell \notin Q \cup \{p\}$ i $\overline{\rho}_{|I_\ell} \simeq \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$, aleshores $\widetilde{\rho}_{|I_\ell} \simeq \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$.

(v) Si $\overline{\rho}$ és plana i si $\det\overline{\rho}_{|I_p} = \varepsilon$, aleshores $\widetilde{\rho}$ és plana.

(vi) Si $\overline{\rho}$ no és plana, o bé $\det\overline{\rho}_{|I_p} \neq \varepsilon$, aleshores $\widetilde{\rho}_{|D_p} \simeq \begin{bmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{bmatrix}$, essent φ_2 un caràcter no ramificat tal que $\varphi_2 \pmod{\mathfrak{m}_A} = \psi_2$.

El teorema següent garanteix l'existència de l'anell R_Q.

4.1.3 Teorema. *Sigui ρ una representació que satisfaci les condicions del teorema 4.1.1. Aleshores,*

(i) *Existeix una deformació de $\overline{\rho}$,*

$$\rho_Q^{\mathrm{univ}} : G_{\mathbb{Q}} \to \mathrm{GL}(2, R_Q),$$

que és universal de tipus Q.

(ii) $\mathrm{Hom}_k(\mathfrak{m}_{R_Q}/(\lambda, \mathfrak{m}_{R_Q}^2), k) \simeq \mathrm{H}^1_Q(\mathbb{Q}, \mathrm{ad}^o\overline{\rho})$.

(iii) *Si E' és una extensió finita de E, es té que*

$$R_{E',Q} = \mathcal{O}_{E'} \otimes_{\mathcal{O}_E} R_{E,Q}. \square$$

El significat del teorema 4.1.3 es resumeix en l'existència d'un isomorfisme

$$\mathrm{Hom}_{\mathcal{O}-\mathrm{Alg}}(R_Q, A) \simeq \mathrm{Def}_Q(\overline{\rho}, A).$$

Una primera versió del teorema 4.1.3 fou obtinguda per Mazur l'any 1982 fent ús del criteri de representabilitat de Schlessinger. En la prova de 4.1.3 Wiles necessita que la representació residual sigui absolutament irreductible sobre $\mathbb{Q}(\sqrt{p^*})$.

Construccions explícites d'anells de deformació universal R_Q foren donades en casos particulars per Fontaine-Mazur [Fo-Ma1995] i per Smit-Lenstra [Sm-Le1997].

L'ideal $\mathfrak{m}_Q$. Considerem la projecció natural $\lambda : \Gamma_0(N_Q) \to (\mathbb{Z}/N_Q\mathbb{Z})^*$ i sigui

$$\Gamma_Q := \lambda^{-1}\left(\mathrm{Sylow}_p(\mathbb{Z}/N(\overline{\rho})\mathbb{Z})^* \times \prod_{q\in Q} \mathrm{Hall}_{p'}(\mathbb{Z}/q\mathbb{Z})^*\right).$$

Introduïm l'àlgebra de Hecke

$$\mathbb{T}(\Gamma_Q) := \mathbb{Z}[T_\ell, \langle \ell \rangle, \ell \nmid pN_Q;\ U_q, q \in Q;\ U_p\,],$$

interpretada com a subàlgebra de l'àlgebra dels $\mathbb{C}$-endomorfismes de $S_2(\Gamma_1(N_Q) \cap \Gamma_Q)$.

Prenem $\mathcal{O}$ prou gran a fi que els valors propis de tots els elements de $\overline{\rho}(G_{\mathbb{Q}})$ siguin racionals sobre k. L'ideal $\mathfrak{m}_Q$ de $\mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ es defineix per

$$\begin{aligned} \mathfrak{m}_Q := \quad & \langle \lambda;\ \operatorname{tr} \overline{\rho}\,(\mathrm{Frob}_\ell) - T_\ell,\ \det \overline{\rho}\,(\mathrm{Frob}_\ell) - \ell \langle \ell \rangle, \ell \nmid N_Q p; \\ & U_q - \alpha_q, q \in Q;\ U_p - \psi_2(\mathrm{Frob}_p), p \rangle. \end{aligned}$$

En el treball [Ta-Wi1995], p. 555, s'afirma que aquest ideal és maximal:

> *It is a deep result following from the work of many mathematicians that* $\mathfrak{m}_Q$ *is a proper ideal (see [D]), and thus maximal.*
>
> Taylor-Wiles [Ta-Wi1995].

Havíem suposat que la representació residual $\overline{\rho}$ era modular. Ara se'ns diu que prové d'una forma modular de $S_2(\Gamma_1(N_Q) \cap \Gamma_Q)$; és a dir, d'una forma modular d'un nivell i d'un pes concrets, i d'un caràcter amb propietats de ramificació específiques.

Esmentarem breument els teoremes de Ribet i de Diamond en què es basa l'afirmació anterior. Per a tal fi, sigui $X_1(N, dq)$ el model de Deligne-Rapoport sobre $\mathbb{Z}_q$ de la corresponent corba modular. Considerem el component connex J^0 de la fibra especial del model de Néron sobre $\mathbb{Z}_q$ de la jacobiana $J_1(N, dq)$. Tenim una successió exacta

$$0 \to T \to J^0 \to J_1(N, dq) \times J_1(N, dq) \to 0,$$

on T és un tor. Designem per X el seu grup de caràcters.

Considerem ara la corba modular

$$X_1(N, pq) = X(\Gamma_1(N) \cap \Gamma_0(pq)),$$

on p, q són primers que no divideixen N. Considerem els dos morfismes de degeneració naturals

$$\alpha_p, \beta_p : X_1(N, pq) \to X_1(N, q)$$

definits per

$$\alpha_p(E, P, C) = (E, P, 0); \quad \beta_p(E, P, C) = (E/C, P \pmod{C}, 0),$$

d'acord amb la interpretació modular d'aquestes corbes.

Siguin L_q el grup de caràcters X definit per a $d = p$; X_q dues còpies del grup de caràcters X definit per a $d = 1$. Les aplicacions de degeneració produeixen una aplicació

$$\delta_p : L_q \to X_q.$$

Sigui

$$Y := \ker(\delta_q).$$

D'altra banda, sigui B l'àlgebra de quaternions sobre $\mathbb{Q}$ de discriminant $D = pq$. Siguin $\mathcal{O}_B$ un ordre maximal de B i $W \subseteq \mathcal{O}_B/N\mathcal{O}_B$ un submòdul d'exponent N i d'ordre N^2. Considerem el grup fuchsià aritmètic

$$\Gamma = \{g \in \mathcal{O}_B : \ \mathrm{nr}(g) = 1, \ xg = x \text{ per a tot } x \in W\}.$$

Sigui $X(\Gamma)$ el model sobre $\mathbb{Q}$ de la corba de Shimura que té per punts complexos $\Gamma\backslash\mathcal{H}$. Siguin $\mathcal{C}/\mathbb{Z}_p$ el model de Čerednik-Drinfeld de $X(\Gamma)$ en p i $\widetilde{J}(X(\Gamma))/\mathbb{Z}_p$ el model de Néron de la seva jacobiana. Denotem per Y_p el grup de caràcters del component connex de la seva fibra especial. Aleshores, Diamond afirma que:

4.1.4 Teorema. (cf. [Di1997], [Ri1990]) *Existeix un isomorfisme*

$$Y_p \xrightarrow{\sim} Y$$

que és compatible amb l'acció dels operadors de Hecke.

L'anell $\mathbb{T}_Q$. Atès que $\mathfrak{m}_Q \neq \mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O}$, podem considerar el completat de $\mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ en $\mathfrak{m}_Q$ i obtenir l'anell local

$$\mathbb{T}_Q := (\mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O})_{\mathfrak{m}_Q}.$$

El teorema següent és degut, essencialment, a Carayol [Ca1994].

4.1.5 Teorema. *Existeix una representació contínua*

$$\rho_Q^{\text{mod}} : G_{\mathbb{Q}} \to \text{GL}(2, \mathbb{T}_Q)$$

que satisfà les condicions següents:

(i) $\rho_Q^{\text{mod}} \pmod{\mathfrak{m}_Q} = \overline{\rho}$. *És a dir,* ρ_Q^{mod} *és una deformació modular de* $\overline{\rho}$.

(ii) *Si* $q \in Q$, *aleshores*

$$\rho_{Q|D_q}^{\text{mod}} = \begin{bmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{bmatrix}, \ \varphi_2(\text{Frob}_q) = U_q; \quad \rho_{Q|I_q}^{\text{mod}} = \begin{bmatrix} 1 & 0 \\ 0 & \chi_q \end{bmatrix}.$$

(iii) *Si* $\ell \notin Q \cup \{p\}$, *i o bé* $\overline{\rho}_{|I_\ell} = \chi \oplus 1$, *o bé* $\overline{\rho}_{|D_\ell}$ *és absolutament irreductible, aleshores*

$$\rho_Q^{\text{mod}}(I_\ell) \simeq \overline{\rho}(I_\ell).$$

(iv) $\det \rho_Q^{\text{mod}} = \varepsilon \chi_Q \varphi$, *essent* φ *un caràcter d'ordre primer amb* p.

(v) *La restricció* $\rho_{Q|D_q}^{\text{mod}}$ *és plana.*

4.1.6 Corol·lari. . *Existeix un homomorfisme* $R_Q \to \mathbb{T}_Q$ *tal que el diagrama següent és commutatiu*

$$\begin{tikzcd} & \text{GL}(2, R_Q) \arrow[dr] & \\ G_Q \arrow[ur, "\rho_Q^{\text{univ}}"] \arrow[rr, "\rho_Q^{\text{mod}}"] & & \text{GL}(2, \mathbb{T}_Q). \end{tikzcd}$$

4.1.2 El criteri numèric de Wiles

Si $\overline{\rho}$ admet una deformació modular de tipus $\mathcal{D} = (\mathcal{O}, \Sigma, \mathcal{M})$, disposem d'homomorfismes

$$\varphi_{\mathcal{D}} : R_{\mathcal{D}} \to \mathbb{T}_{\mathcal{D}}, \quad \pi_{\mathcal{D}} : \mathbb{T}_{\mathcal{D}} \to \mathcal{O},$$

el primer dels quals és un epimorfisme.

4.1.7 Teorema. *Suposem que $\overline{\rho}$ admet una deformació modular de tipus $\mathcal{D} = (\mathcal{O}, \Sigma, \mathcal{M})$. Sigui $\eta = \mathrm{Ann}(\ker \pi_{\mathcal{D}})$. Si $\sharp\mathcal{O}/\pi_{\mathcal{D}}(\eta) \geq \sharp\mathfrak{p}_R/\mathfrak{p}_R^2$, aleshores:*

(i) $\varphi_{\mathcal{D}_1} : R_{\mathcal{D}_1} \simeq \mathbb{T}_{\mathcal{D}_1}$*, per a tot tipus* $\mathcal{D}_1 \supseteq \mathcal{D}$*.*

(ii) *Per a tots els tipus $\mathcal{D}_1 \supseteq \mathcal{D}$, l'anell $\mathbb{T}_{\mathcal{D}_1}$ és un anell d'intersecció completa.*

Demostració. Fets generals i les hipòtesis del teorema impliquen que

$$\sharp\mathcal{O}/\pi_{\mathcal{D}}(\eta) \leq \sharp\mathfrak{p}_\pi/\mathfrak{p}_\pi^2 \leq \sharp\mathfrak{p}_R/\mathfrak{p}_R^2 \leq \sharp\mathcal{O}/\pi_{\mathcal{D}}(\eta).$$

Alhora, les igualtats que en resulten impliquen que l'anell $\mathbb{T}_{\mathcal{D}}$ és d'intersecció completa sobre $\mathcal{O}$.

Demostració del teorema 4.1.1. Es tracta de veure que si ρ és residualment modular i se satisfan les condicions del teorema, aleshores ρ és modular. Es comença per considerar el cas

$$Q = \phi; \quad \mathbb{T} := \mathrm{T}_\phi \subseteq \mathrm{End}(S_2(\Gamma_1(N(\overline{\rho})p^\delta))).$$

Aleshores, $\Gamma_1(N(\overline{\rho})p^\delta) \subseteq \Gamma_\phi$. Es defineix $\mathbb{T}_\phi = (\mathbb{T}(\Gamma_\phi) \otimes_{\mathbb{Z}} \mathcal{O})_{\mathfrak{m}}$.

Donat un conjunt Q qualsevol, podem considerar homomorfismes

$$\pi_Q : \mathbb{T}_Q \to \mathbb{T}_\phi \to \mathcal{O}, \quad T_\ell \mapsto T_\ell, \quad \langle\ell\rangle \to \langle\ell\rangle, \quad U_q \to B_q,$$

on $B_q \in \mathbb{T}$ és l'única arrel de l'equació $U^2 - T_q U + q\langle q\rangle$ que es projecta en α_q. En definir

$$\mathcal{P}_Q = \ker \pi_Q = \langle T_\ell - A_\ell; \langle\ell\rangle - \chi\langle\ell\rangle; U_q - B_q\rangle,$$

$$\eta_Q = \pi_Q(\mathrm{Ann}_{\mathbb{T}_Q}(\mathcal{P}_Q)),$$

es té el resultat següent:

4.1.8 Teorema. (i) $\sharp\mathcal{O}/\eta_Q \leq \sharp\mathcal{P}_Q/\mathcal{P}_Q^2 < \infty$.

(ii) $\sharp\mathcal{O}/\eta_Q = \sharp\mathcal{P}_Q/\mathcal{P}_Q^2 < \infty$ *si, i només si, $\mathbb{T}_Q$ és un anell d'intersecció completa.*

El teorema 4.1.8 permet demostrar el teorema 4.1.1 per inducció. El raonament de Wiles és: si $\mathbb{T}_Q$ és una intersecció completa per a un cert Q, aleshores $\mathbb{T}_\phi$ és una intersecció completa i, per tant, $\mathbb{T}_Q$ esdevé una intersecció completa per a tot Q. Taylor-Wiles [Ta-Wi1995] demostren que $\mathbb{T}_Q$ és intersecció completa per a un cert Q. $\square$

4.2 El criteri de Diamond

Una millora obtinguda per Diamond [Di1997] consisteix en establir l'existència d'un isomorfisme

$$R_{\mathcal{D}} \simeq \mathbb{T}_{\mathcal{D}}$$

sense fer ús de la condició Gorenstein que empra Wiles. El seu treball aplega resultats de Fujiwara, Lenstra, de Smit, Schoof i del propi Diamond. El criteri més important en aquesta direcció és el següent.

4.2.1 Teorema. *Siguin k un cos finit i $r \geq 0$ un nombre enter. Siguin*

$$A := k\,[[S_1, \dots, S_r]]\,, \quad B := k[[X_1, \dots, X_r]].$$

Considerem donats una k-àlgebra R i un R-mòdul $H \neq 0$ tal que $\dim_k H < \infty$.

Suposem que per a cada $n \geq 1$ tenim un diagrama commutatiu

$$\begin{array}{ccc} A & \xrightarrow{\phi_n} & B \\ \downarrow & & \downarrow \psi_n \\ k & \to & R, \end{array}$$

un B-mòdul H_n i un homomorfisme $\pi_n : H_n \to H$ tal que H_n és lliure sobre $A/\mathfrak{m}_A^n$, i $k \otimes_A H_n \simeq H$, mitjançant π_n.

Aleshores, H és lliure sobre R i R és una intersecció completa.

En el cas concret que ens ocupa, el teorema s'aplica de la forma següent. Es pren

$$A = \lim\operatorname{proj} k[\Delta_Q], \quad \Delta_Q = \Pi(\mathbb{Z}/q\mathbb{Z})_p^*, \quad q \equiv 1 \pmod{p^n},$$

$$B = \lim\operatorname{proj}\ k \otimes_{\mathcal{O}} R_Q, \quad R = k \otimes_{\mathcal{O}} R_\phi.$$

Els mòduls H, H_n provenen de l'homologia de corbes modulars.

4.3 Representacions ordinàries modulars

La conjectura següent és un cas particular de la conjectura de Fontaine-Mazur [Fo-Ma1995].

Conjectura. Suposem donada una representació

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(2, \overline{\mathbb{Q}}_p)$$

contínua, irreductible i no ramificada fora d'un conjunt finit de primers que inclou el primer de l'infinit. Suposem que se satisfan les condicions:

(i) La representació ρ és ordinària en p: $\rho_{|I_p} \simeq \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$.

(ii) $\det(\rho) \simeq \psi\varepsilon^{k-1}$, és senar, on ε denota el caràcter ciclotòmic, $k \geq 2$ un enter, i ψ un caràcter finit.

Aleshores, la representació ρ és modular. $\square$

En aquesta secció explicarem algunes propietats de les representacions ordinàries en relació a la seva probable modularitat. Suposem que F és un cos de nombres totalment real, de grau d. Els autors consideren dades de deformació $\mathcal{D} = (\mathcal{O}, \Sigma, c, \mathcal{M})$ donada per un cocicle

$$0 \neq c \in \ker \left\{ H^1(\mathrm{Gal}(F_\Sigma/F), k(\chi^{-1})) \to \bigoplus_{i=1}^{t} H^1(D_i, k(\chi^{-1})) \right\}.$$

Denotem per $\rho_c : \mathrm{Gal}(F_\Sigma/F) \to \mathrm{GL}(2, k)$, $\rho_c = \begin{bmatrix} 1 & * \\ 0 & \chi \end{bmatrix}$ una representació tal que

$$\rho_c(z_i) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \rho_c(\sigma) = \begin{bmatrix} 1 & c(\sigma) \\ 0 & -1 \end{bmatrix}, \quad \rho_{c|D_i} \simeq \begin{bmatrix} 1 & 0 \\ 0 & \chi \end{bmatrix},$$

on $\sigma \in \mathrm{Gal}(F_\Sigma/F)$, i els grups D_i, $1 \leq i \leq t$, provenen de les places que divideixen p.

El resultat següent proporciona l'estructura de l'anell $R_{\mathcal{D}}$ associat a les deformacions de ρ_c de tipus $\mathcal{D}$.

4.3.1 Teorema. *Sigui $R_{\mathcal{D}}$ l'anell de deformació universal de tipus $\mathcal{D}$. Aleshores,*

$$R_{\mathcal{D}} \simeq \mathcal{O}[[x_1, \dots, x_g]]/(f_1, \dots, f_r),$$

on $g - r \geq d + \delta_F - 2t - 3\sharp\mathcal{M}$, i δ_F denota el $\mathbb{Z}_p$-rank del grup de Galois de l'extensió pro-abeliana maximal de F no ramificada fora de les places $v_1, \dots, v_t$ de F que divideixen p.

En la demostració del teorema anterior, els autors consideren dades de deformació de tipus Q, $\mathcal{D}_Q$, dades de tipus minimal $\mathcal{D}_Q^{\min}$, i pseudo dades de deformació, $\mathcal{D}_Q^{\mathrm{ps}}$, que proporcionen anells universals i homomorfismes

$$r_{\mathcal{D}} : R_{\mathcal{D}_Q^{\mathrm{ps}}} \to R_{\mathcal{D}_Q}.$$

Àlgebra de Hecke gairebé ordinària. Designem per $\mathbb{T}_k(U_a)$ l'àlgebra de Hecke operant a $S_k(U_a)$, on $U_a = U \cap U(p^a)$ denota un nivell. El límit

$$e = \lim T_0(p)^{p^n(p^m-1)} \quad (n \to \infty)$$

no depèn de m. Es defineixen les àlgebres

$$\mathbb{T}_k(U_a, \mathcal{O}) = e\mathbb{T}_k(U_a, \mathcal{O}), \quad \mathbb{T}_\infty(U_a, \mathcal{O}) = \lim\operatorname{proj} \mathbb{T}_2(U_a, \mathcal{O}).$$

Donat un homomorfisme algebraic

$$\lambda : \mathbb{T}_\infty(U_a, \mathcal{O}) \to \overline{\mathcal{O}}_p,$$

el seu nucli, $\ker\lambda = \varphi$, s'anomena un primer algebraic. El conjunt

$$\{\varphi : \ \varphi \text{ primer algebraic}\}$$

és dens per a la topologia de Zariski en $\operatorname{Spec}(\mathbb{T}_\infty(U_a, \mathcal{O})/Q)$, quan Q és un conjunt minimal de primers.

Les representacions ordinàries $\pi \in \Pi_2^{\mathrm{ord}}(U_a)$ estan en correspondència bijectiva amb els ideals primers algebraics $\lambda \in \mathbb{T}_2(U_a, \mathcal{O})$. Un teorema de Wiles associa aleshores a aquests primers representacions galoisianes

$$\rho_\pi : \operatorname{Gal}(\overline{F}/F) \to \operatorname{GL}(2, \overline{\mathbb{Q}}_p),$$

de conductor $\mathfrak{n}$, que satisfan les condicions següents:

(i) $\rho_\pi(z_1) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

(ii) ρ_π és no ramificada fora de $\mathfrak{n}p$.

(iii) Per a tot primer $\ell \nmid \mathfrak{n}p$, es té que $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_\ell)) = \lambda(T(\ell))$.

(iv) Per a tot primer $\ell \nmid \mathfrak{n}p$, es té que
$\det(\rho_\pi(\mathrm{Frob}_\ell)) = \lambda(S(\ell))\mathrm{Nor}(\ell)$.

(v) $\rho_{\pi|D_i} \simeq \begin{bmatrix} \psi_1^{(i)} & * \\ 0 & \psi_2^{(i)} \end{bmatrix}$, per a $1 \leq i \leq t$.

Skinner i Wiles demostren que $R_{\mathcal{D}}$ és un mòdul sobre una àlgebra d'Iwasawa

$$\Lambda_{\mathcal{O}} = \mathcal{O}[[T_1, \dots T_{\delta_F}, Y_1^{(1)}, \dots, Y_{d_t}^{(t)}]].$$

Defineixen un tipus d'ideals $\mathfrak{m}$ en l'àlgebra de Hecke que anomenen permissibles. Per a aquests demostren que

$$\mathbb{T}_\infty(U_a, \mathcal{O})_{\mathfrak{m}}$$

és un $\Lambda_{\mathcal{O}}$-mòdul i que existeix un epimorfisme

$$R_{\mathcal{D}^{\mathrm{ps}}} \to \mathbb{T}_\infty(U_a, \mathcal{O})_{\mathfrak{m}},$$

atès que $\rho_{\mathfrak{m}}^{\mathrm{mod}}$ és de tipus $\mathcal{D}^{\mathrm{ps}}$.

La pregunta clau esdevé: existeixen ideals permissibles? La proposició següent proporciona una condició suficient per a la seva existència.

4.3.2 Proposició. *Sigui π un uniformitzant de $\mathcal{O}$. Si*

$$\mathrm{ord}_\pi(L_p(F, -1, \chi\omega)) \geq 0,$$

aleshores l'àlgebra de Hecke $\mathbb{T}_\infty(U_a^\chi, \mathcal{O})$ admet ideals maximals permissibles.

La idea de la demostració és la següent: la condició imposada al valor especial de la funció L ocasiona l'existència d'una forma modular, f, tal que la representació automorfa associada, π_f, és un element de $\Pi_2^{\mathrm{ord}}(U_a^\chi)$.

4.4 El teorema de Skinner-Wiles en el cas residualment reductible

Estem ara en condicions d'esmentar els conceptes més importants necessaris per portar a terme la demostració de la modularitat sobre cossos totalment reals de certes representacions residualment reductibles i ordinàries.

Bones dades de deformació. Partim d'un parell $(F, \mathcal{D})$, essent $\mathcal{D} = (\mathcal{O}, \Sigma, c, \mathcal{M})$ una dada de deformació. Es diu que $\mathcal{D}$ és bona si satisfà les condicions següents:

(i) $[F : \mathbb{Q}] = d$ és un nombre parell.

(ii) $L_p(F, -1, \chi\omega) \in \mathcal{O}, \quad L_p(F, -1, \chi\omega) \notin \mathcal{O}^*$.

(iii) $d \geq 2 + \delta_F + 8(\sharp\Sigma + \dim_k H_{\Sigma_0}(F, k))$.

(iv) Per a cada $v_i|p$, és té que

$$d_{v_i} > 2 + 2t + 7(\sharp\Sigma + \dim_k H_{\Sigma_0}(F, k)), \quad d_{v_i} = [F_{v_i} : \mathbb{Q}_p].$$

(v) Si $\rho_{c|I_w} \neq 1,\ w \nmid p$, aleshores o bé $\chi_{|I_w} \neq 1$, o bé $\chi_{|D_w} = 1$.

Primers gentils. Donada una dada de deformació $\mathcal{D}$, un ideal primer $\mathfrak{p} \subseteq \mathbb{T}_{\mathcal{D}}$ es diu que és gentil si satisfà les condicions següents:

(i) La dimensió de $\mathfrak{p}$ és 1.

(ii) La representació $\rho_{\mathfrak{p}}$ és irreductible.

(iii) $\mathfrak{p}$ és la imatge inversa d'un ideal primer de $\mathbb{T}_{\mathcal{D}_c}$, on $\mathcal{D}_c = (\mathcal{O}, \Sigma_c, c, \mathcal{M})$.

(iv) Alguna conjugada de la representació ρ és una deformació gentil de tipus $(\mathcal{O}', \Sigma_c, c, \mathcal{M})$.

Primers promodulars per a un tipus $\mathcal{D}$. Un ideal primer $\mathfrak{q} \subseteq R_{\mathcal{D}}$ s'anomena promodular quan la projecció natural

$$\varphi_{\mathfrak{q}} : R_{\mathcal{D}^{\mathrm{ps}}} \to R_{\mathcal{D}}/\mathfrak{q}$$

factoritza segons un diagrama commutatiu

$$\begin{array}{ccccc} & & \mathbb{T}_{\mathcal{D}} & & \\ & \pi_{\mathcal{D}} \nearrow & & \searrow \theta_{\mathfrak{q}} & \\ R_{\mathcal{D}^{\mathrm{ps}}} & & \xrightarrow{\varphi_{\mathfrak{q}}} & & R_{\mathcal{D}}/\mathfrak{q}. \end{array}$$

Considerem les hipòtesis

(P1): Si $\mathfrak{p} \subseteq \mathbb{T}_{\mathcal{D}}$ és un primer gentil per a $\mathcal{D}$, aleshores tot primer Q tal que $Q \subseteq \mathfrak{p}_{\mathcal{D}} \subseteq R_{\mathcal{D}}$ és promodular.

(P2): Existeix un ideal primer $\mathfrak{q} \subseteq R_{D_c}$ promodular tal que la deformació ρ_q és gentil.

La proposició següent és clau en la prova del teorema de Skinner-Wiles.

4.4.1 Proposició. *Si* $(F, \mathcal{D})$ *és un parell format per un cos totalment real i una deformació, les hipòtesis* (P1) *i* (P2) *se satisfan per a* $\mathcal{D}$ *i per a* $\mathcal{D}_c$*, aleshores tot ideal primer* $\mathfrak{q} \subseteq R_{\mathcal{D}}$ *és promodular.*

En relació a la hipòtesi (P2), es té el criteri següent:

Criteri per a (P2): Si $(F, \mathcal{D})$ és un parell bo i la hipòtesi (P1) se satisfà per a cada dada de deformació $(\mathcal{O}', \Sigma', c', \mathcal{M}')$, on $\Sigma' \subseteq \Sigma$, $\mathcal{O}' \supseteq \mathcal{O}$, aleshores la hipòtesi (P2) se satisfà per a la dada $\mathcal{D}$.

Arribem ara al resultat principal de Skinner-Wiles [Sk-Wi1999].

4.4.2 Teorema. *Sigui* $\mathcal{D} = (\mathcal{O}, \Sigma, c, \mathcal{M})$ *una dada de deformació. Sigui*

$$\rho : \mathrm{Gal}(F_\Sigma/F) \to \mathrm{GL}(2, \mathcal{O})$$

una deformació de $\overline{\rho}$ *de tipus* $\mathcal{D}$ *tal que*

(i) ρ *és irreductible;*

(ii) $\det(\rho) = \psi\varepsilon^\mu$*, és senar, on* $\mu \geq 1$ *és un enter, i* ψ *és un caràcter d'ordre finit; i*

(iii) $\rho_{|D_i} \simeq \begin{bmatrix} \widetilde{\chi}\psi_1^{(i)} & * \\ 0 & \psi_2^{(i)} \end{bmatrix}$*, amb* ${\psi_2^{(i)}}_{|I_i}$ *d'ordre finit per a* $1 \leq i \leq t$*.*

Suposem que existeix una extensió L/F de cossos totalment reals tal que

(i) *la clausura galoisiana de L sobre F és resoluble;*

(ii) *el grau $[L:\mathbb{Q}]$ és parell;*

(iii) *L és permissible per a $\mathcal{D}$; i*

(iv) *el parell $(L, \mathcal{D}_L)$ és bo.*

Aleshores $\rho \otimes \overline{\mathbb{Q}}_p$ és la representació associada a una forma modular de Hilbert, nova.

El teorema següent és l'aplicació més important del teorema anterior.

4.4.3 Teorema. *Sigui $F/\mathbb{Q}$ una extensió abeliana i totalment real. Sigui $p \neq 2$ un nombre primer. Suposem donada una representació*

$$\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}(2, \overline{\mathbb{Q}}_p)$$

contínua, irreductible, no ramificada fora d'un conjunt finit de places de F. Suposem que se satisfan les condicions següents:

(i) $\overline{\rho}^{\mathrm{ss}} \simeq \chi_1 \oplus \chi_2$ *i l'extensió $F(\chi_1/\chi_2)/\mathbb{Q}$ és abeliana.*

(ii) $(\chi_1/\chi_2)(z) = -1$, *per a cada conjugació complexa z.*

(iii) $(\chi_1/\chi_2)_{D_v} \neq 1$, *per a cada plaça $v|p$.*

(iv) $\rho_{|D_v} \simeq \begin{bmatrix} \psi_1^{(v)}\widetilde{\chi_1} & * \\ 0 & \psi_2^{(v)}\widetilde{\chi_2} \end{bmatrix}$, *on $\psi_2^{(v)}$ factoritza per un pro-p-grup de F_v i $\psi_2^{(v)}{}_{|I_v}$ és d'ordre finit, per a cada $v|p$.*

(v) $\det(\rho) = \psi\varepsilon^{k-1}$, *on $k \geq 2$, i ψ és d'ordre finit.*

Aleshores ρ és la representació associada a una forma modular de Hilbert, nova.

El teorema següent, de la teoria d'Iwasawa i degut a Washington, és un ingredient destacat en la prova del teorema 4.4.3.

4.4.4 Teorema. *Sigui L/K una extensió abeliana i finita. Sigui L_∞/L la $\mathbb{Z}_\ell$-extensió ciclotòmica de L. Aleshores la p-part del nombre de classes resta fitada. És a dir, si $L_\infty = \lim\operatorname{ind} L(\mu_{\ell^n})$, existeix una constant c tal que*

$$p^c \parallel h(L(\mu_{\ell^n})), \qquad \textit{per a tot } n \gg 0.$$

4.5 El teorema de Skinner-Wiles en el cas residualment irreductible

Considerem en aquesta secció el teorema provat per Skinner-Wiles a [Sk-Wi2001].

4.5.1 Teorema. *Sigui $E/\mathbb{Q}_p$ una extensió finita. Sigui*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(2, E)$$

una representació contínua, irreductible i no ramificada fora d'un conjunt finit de primers. Suposem que se satisfan les condicions següents:

(i) $\overline{\rho}^{\mathrm{ss}}$ *és irreductible. És a dir, ρ és residualment irreductible.*

(ii) $\overline{\rho}^{\mathrm{ss}}_{|D_p} \simeq \begin{bmatrix} \chi_1 & * \\ 0 & \chi_2 \end{bmatrix}, \quad (\chi_1|\chi_2)_{|D_p} \neq 1.$

(iii) $\overline{\rho}^{\mathrm{ss}}$ *prové d'una forma modular. És a dir, ρ és residualment modular.*

(iv) $\rho_{|I_p} \simeq \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}.$

(v) $\det(\rho) = \psi\varepsilon^{k-1}$ *és senar i $k \geq 2$.*

Aleshores la representació ρ prové d'una forma modular.

La demostració de la modularitat en el cas irreductible que estem considerant és més fàcil que en el cas reductible considerat a la secció anterior. En aquest cas disposem de les àlgebres $R_{\mathcal{D}}, \mathbb{T}_{\mathcal{D}}$; se'ns diu que $\overline{\rho}^{\mathrm{ss}}$ admet una deformació a $\mathrm{GL}(2, \mathbb{T}_{\mathcal{D}})$. Per tant, existeix un epimorfisme

$$R_{\mathcal{D}} \to \mathbb{T}_{\mathcal{D}}.$$

En el treball, els autors donen també una versió del teorema anterior per a cossos totalment reals. Per a tal fi, cal fer les hipòtesis següents:

(H1): El grau $[F : \mathbb{Q}]$ és parell.

(H2): Existeix un tipus de deformació minimal $\mathcal{D}_0 = (\mathcal{O}, \Sigma_0, \mathcal{M}_0)$. L'àlgebra $\mathbb{T}_\infty(U_{\mathcal{D}_0}, \mathcal{O})$ posseeix un ideal maximal permissible, amb la qual cosa disposem d'una representació contínua

$$\rho^{\mathrm{mod}}_{\mathcal{D}_Q} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}(\mathbb{T}_{\mathcal{D}_Q}).$$

Sota aquestes hipòtesis, tècniques de canvi de base permeten demostra el teorema següent.

4.5.2 Teorema. *Suposem donada una representació*

$$\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}(2, \overline{\mathbb{Q}}_p)$$

contínua, irreductible, no ramificada fora d'un conjunt finit de primers, que satisfà les condicions següents:

(i) $\overline{\rho}^{\mathrm{ss}}$ *és irreductible.*

(ii) $\overline{\rho}^{\mathrm{ss}}_{|D_i} \simeq \begin{bmatrix} \chi_1^{(i)} & * \\ 0 & \chi_2^{(i)} \end{bmatrix}, \quad \chi_1^{(i)} \neq \chi_2^{(i)}.$

(iii) *Existeix una representació automorfa i gairebé ordinària,* π_0, *de* $\mathrm{GL}_{2|F}$ *tal que* ρ_{π_0} *és una bona* χ_2*-deformació de* $\overline{\rho}^{\mathrm{ss}}$.

Aleshores, $\rho \simeq \rho_\pi$ *per a alguna representació automorfa* π.

Bibliografia

[Ca1994] Carayol, H.: Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 213–237, *Contemp. Math.*, 165, Amer. Math. Soc., Providence, RI, 1994. MR1279611 (95i:11059).

[Di1996] Diamond, F.: The refined conjecture of Serre. *Elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), 22–37, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995. MR1363493 (97b:11065).

[Di1996-2] Diamond, F. On deformation rings and Hecke rings. *Ann. of Math.* (2) 144 (1996), no. 1, 137–166. MR1405946 (97d:11172).

[Di1997] Diamond, F.: The Taylor-Wiles construction and multiplicity one. *Invent. Math.* 128 (1997), no. 2, 379–391. MR1440309 (98c:11047).

[Fo-Ma1995] Fontaine, J-M.; Mazur, B.: Geometric Galois representations. *Elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995. MR1363495 (96h:11049).

[Ri1990] Ribet, K. A.: On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.* 100 (1990), no. 2, 431–476. MR1047143 (91g:11066).

[Se1987] Serre, J-P.: Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). *Duke Math. J.* 54 (1987), no. 1, 179–230. MR0885783 (88g:11022).

[Sk-Wi1997] Skinner, C. M.; Wiles, A. J.: Ordinary representations and modular forms. *Proc. Nat. Acad. Sci. U.S.A.* 94 (1997), no. 20, 10520–10527. MR1471466 (98h:11068)

[Sk-Wi1999] Skinner, C. M.; Wiles, A. J.: Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.* No. 89, (1999), 5–126 (2000). MR1793414 (2002b:11072).

[Sk-Wi2001] Skinner, C. M.; Wiles, A. J.: Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math.* (6) 10 (2001), no. 1, 185–215. MR1928993 (2004b:11073).

[Sm-Le1997] de Smit, B.; Lenstra, H. W., Jr.: Finite complete intersection algebras and the completeness radical. *J. Algebra* 196 (1997), no. 2, 520–531. MR1475123 (98j:13010).

[Ta-Wi1995] Taylor, R.; Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* (2) 141 (1995), no. 3, 553–572. MR1333036 (96d:11072).

[Wi1995] Wiles, A.: Modular forms, elliptic curves, and Fermat's last theorem. *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Zürich, 1994), 243–245, Birkhäuser, Basel, 1995. MR1403925 (97f:11041).

P. Bayer

Facultat de Matemàtiques,

Universitat de Barcelona.

Gran Via de les Corts Catalanes 585. E-08007, Barcelona

bayer@ub.edu

Capítol 5

Formes modulars de Hilbert i representacions λ-àdiques associades.

Àngela Arenas

Aquestes notes són la transcripció de les transparencies presentades el dimecres 21 de gener de 2004 a la primera part de la xerrada intitulada: Modularitat Potencial I.

5.1 Grup modular de Hilbert

Sigui $F|\mathbb{Q}$ un cos de nombres totalment real de grau $[F:\mathbb{Q}] = g > 1$, i sigui $\mathcal{O}$ el seu anell d'enters. Denotarem per $h = h^+(F)$ el nombre de classes de F en sentit estricte i per ∂ la diferent de F (relativa a $\mathbb{Q}$). La immersió canònica $\sigma : F \hookrightarrow \mathbb{R}^g$ indueix una immersió obvia de $GL^+(2,F)$ en $\big(GL^+(2,\mathbb{R})\big)^g$. Per tant $GL^+(2,F)$ es pot considerar actuant en $\mathbb{H}^g$: si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL^+(2,F)$, $z = (z_1,\dots,z_g) \in \mathbb{H}^g$

Amb el suport parcial de MCYT BFM 2003-01898.

i a_i, b_i, c_i, d_i denoten els conjugats de a, b, c, d en $\mathbb{R}$, $i = 1, \dots, g$, aleshores $\gamma(z) = \left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \dots, \frac{a_g z_g + b_g}{c_g z_g + d_g}\right)$.

$SL(2, \mathcal{O})$ és un subgrup discret de $SL(2, \mathbb{R})^g$ ja que $\sigma(\mathcal{O})$ és una xarxa de $\mathbb{R}^g$ (cf.[Ar 00]). $SL(2, \mathcal{O})$ s'anomena grup modular de Hilbert. Donats $\mathbf{b}$ un ideal fraccionari i $\mathbf{n}$ un ideal enter de F considerem el grup d'unitats $\Gamma = \Gamma(\mathbf{b}, \mathbf{n})$ donat per

$$\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL^+(2, F) \mid a, d \in \mathcal{O}\,,\ b \in \mathbf{b}^{-1}, c \in \mathbf{bn},\, ad - bc \in \mathcal{O}^* \right\}.$$

Remarca

$SL(2, \mathcal{O}) = \Gamma(\mathcal{O}, \mathcal{O})_1 \subset \Gamma(\mathcal{O}, \mathcal{O})$.

Teorema

L'espai quocient $X_\Gamma = \Gamma \backslash \mathbb{H}^g \cup F \cup \{\infty\}$ és compacte (compactificació de Satake). X_Γ té un nombre finit de classes de punts parabòlics i de classes de punts el·líptics. Aquestes classes són els punts singulars de X_Γ considerada com a varietat analítica de dimensió complexa g. (Els punts parabòlics són altament singulars). En el cas particular $\Gamma = SL(2, \mathcal{O})$, el nombre de classes de Γ-punts parabòlics és h.

X_Γ és una varietat algebraica projectiva complexa (compactificació de Baily- Borel). X_Γ és l'espai analític complex associat al $Proj(\mathcal{M}(\Gamma))$ de l'anell graduat de formes modulars de Hilbert respecte de Γ. X_Γ s'anomena varietat modular de Hilbert. Les varietats modulars de Hilbert són espais de moduli d'esquemes abelians amb multiplicació real.

Cas $g = 2$. X_Γ superfície modular de Hilbert. F. Hirzebruch (1970) resol explícitament les singularitats, (veure [Hi 73]).

5.2 Formes modulars de Hilbert (punt de vista clàssic)

Donades una funció holomorfa $f : \mathbb{H}^g \to \mathbb{C}$, una g-tupla d'enters positius parells $\mathbf{k} = (k_1, \dots, k_g)$, i una matriu $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL^+(2, F)$ escrivim, $(f|_{\mathbf{k}}\,\gamma)(z) := (\det\gamma)^{k/2}(cz{+}d)^{-k}\, f\big(\gamma(z)\big) = j_k(\gamma,z)^{-1} f\big(\gamma(z)\big)$, $j_k(\gamma,z)^{-1} = (\det\gamma)^{k/2}(cz+d)^{-k}$, $(\det\gamma)^{k/2} = \prod_{i=1}^{g}\, (a_i d_i - b_i c_i)^{k_i/2}$, $(cz+d)^{-k} = \prod_{i=1}^{g}(c_i z_i + d_i)^{-k_i}$.

Considerem un conjunt de representants $\mathbf{c}_1, \ldots, \mathbf{c}_h$ de les classes estrictes d'ideals de F. Obviament els representants es poden triar de manera que siguin primers amb $\mathbf{n}\,\partial$. Considerem ara $\Gamma_j(\mathbf{n}) := \Gamma(\mathbf{c}_j\partial, \mathbf{n})$, $j = 1, \ldots, h$.

Una forma modular de Hilbert de pes $\mathbf{k} = (k_1, \ldots, k_g)$ i nivell $\mathbf{n}$ és una h-tupla $\mathbf{f} = (f_1, \ldots, f_h)$ de funcions holomorfes $f_j : \mathbb{H}^g \to \mathbb{C}$, $j = 1, \ldots, h$, satisfent $f_j|_{\mathbf{k}}\ \gamma = f_j$, $\gamma \in \Gamma_j(\mathbf{n})$,

Les formes modulars de Hilbert de pes $\mathbf{k}$ i nivell $\mathbf{n}$ constitueixen un $\mathbb{C}$-espai vectorial $\mathcal{M}_{\mathbf{k}}(\mathbf{n})$ de dimensió finita. A tota $\mathbf{f} = (f_1, \ldots, f_h)$ $\in \mathcal{M}_{\mathbf{k}}(\mathbf{n})$ li correspon una única"successió de coeficients de Fourier" indexats pels ideals enters de $\mathcal{O}$. Més concretament si $\mathbf{m}$ és un ideal enter de F, aleshores existeix una única j tal que $\mathbf{m}$ pertany a la classe estricta de $\mathbf{c}_j^{-1}$, i.e. $\mathbf{m} = \xi\ \mathbf{c}_j^{-1}$ per a cert ξ totalment positiu. (ξ es troba necessariament en $\mathbf{c}_j$ i a més no és únic, es pot modificar amb qualsevol unitat totalment positiva de $\mathcal{O}^*$).

Com que $\Gamma_j(\mathbf{n})$ obviament conté translacions definides per elements de $(\mathbf{c}_j\ \partial)^{-1}$, f_j es pot desenvolupar en sèrie de Fourier

$f_j(z) = \sum_\zeta\ c_j(\zeta)\ \exp\left(2\pi\sqrt{-1}\,\zeta{\cdot}z\right)$, on $z = (z_1, \ldots, z_g)$, ζ recorre tots els elements totalment positius de la xarxa dual de $(\mathbf{c}_j\ \partial)^{-1}$ que és $\mathbf{c}_j$, i $\zeta \cdot z = \zeta_1 z_1 + \cdots + \zeta_g z_g$ $(\zeta_1, \ldots, \zeta_g$ són tots els conjugats de $\zeta = \zeta_1$ en $\mathbb{R})$. Amb aquestes notacions posem

$$c\,(\mathbf{m}\,, \mathbf{f}) = c_j(\xi)\ \xi^{-\mathbf{k}/2}\,,\quad \text{si}\ \ \mathbf{m} = \xi\,\mathbf{c}_j^{-1},\ \text{amb}\ \xi^{-\mathbf{k}/2} = \prod_{j=1}^{g} \xi_j^{-k_j/2}.$$

El $\mathbf{m}$-èssim coeficient de Fourier no depen de ξ, ja que $f_j(\epsilon z)\epsilon^{k/2} = f_j(z)$, per a tot unitari totalment positiu ϵ.

$f_j(z)$ s'anomena forma parabòlica si s'anul·la a les cusps de $\Gamma_j(\mathbf{n})$.

$\mathbf{f} \in \mathcal{M}_{\mathbf{k}}(\mathbf{n})$ s'anomena forma parabòlica de Hilbert si cada f_j és parabòlica, $j = 1, \ldots, h$.

$\mathcal{S}_{\mathbf{k}}(\mathbf{n})$ espai de formes parabòliques de Hilbert és un $\mathbb{C}$- espai vectorial de dimensió finita.

Remarca.

$\mathcal{M}_{\mathbf{k}}(\mathbf{n}) = \bigoplus_{\psi_0} \mathcal{M}_{\mathbf{k}}(\mathbf{n}, \psi_0)$,
amb $\mathcal{M}_{\mathbf{k}}(\mathbf{n}, \psi_0) = \prod_{j=1}^{h} \mathcal{M}_{\mathbf{k}}(\Gamma(\mathbf{c}_j\partial, \mathbf{n}), \psi_0)$, on ψ_0 recorre tots els caràcters de $(\mathcal{O}/\mathbf{n})^*$.

5.3 Formes modulars de Hilbert (punt de vista adèlic)

Siguin $F_{\mathbf{A}}$ l'anell d'adèles de F, $F_{\mathbf{A}}^*$ el grup d'idèles de F, $G_F = GL(2,F)$, $G_{\mathbf{A}} = GL(2,F_{\mathbf{A}})$ l'adelització de G_F, $(G_{\mathbf{A}})_\infty$ la part infinita de $G_{\mathbf{A}}$, $G_{\mathbf{A}_+}$ el subgrup d'elements de $G_{\mathbf{A}}$ tals que la seva part arquimediana cau en la component connexa de l'identitat de $(G_{\mathbf{A}})_\infty$, i.e., en $\left(GL^+(2,\mathbb{R})\right)^g$. Com que F és totalment real, es té $G_{F_+} = G_F \cap G_{\mathbf{A}_+}$.

Denotem per $G_{\mathbf{p}} = GL(2, F_{\mathbf{p}})$, on $\mathbf{p}$ denota una plaça (finita o no) de F i $F_{\mathbf{p}}$ denota la seva corresponent completació. Pel teorema d'aproximació forta $G_{\mathbf{A}}$ es pot expressar com una unió disjunta finita

$G_{\mathbf{A}} = \bigsqcup_{j=1}^{h} G_F\ x_j\ W$, per a certs $x_j \in G_{\mathbf{A}}$ que es poden triar com $x_j = \left(\begin{smallmatrix} t_j^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$, on les $t_j \in F_{\mathbf{A}}^*$ es poden considerar tenint ∞-components trivials i tals que els seus $\mathcal{O}$-ideals associats constitueixen un sistema complet de representants per a les classes estrictes d'ideals, $W = W(\mathbf{n})$ és el subgrup de $G_{\mathbf{A}_+}$ definit per

$W = \prod_{\mathbf{p}}\ W_{\mathbf{p}}\ \times (G_{\mathbf{A}})_{\infty_+}$, amb $W_{\mathbf{p}}$, $\mathbf{p}$ primer finit, igual a

$$\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL(2, F_{\mathbf{p}}) \mid a, d \in \mathcal{O}_{\mathbf{p}}\,,\ b \in \partial_{\mathbf{p}}^{-1}, c \in \mathbf{n}_{\mathbf{p}}\, \partial_{\mathbf{p}}, ad - bc \in \mathcal{O}_{\mathbf{p}}^* \right\}.$$

Aleshores, si posem

$\Gamma_j(\mathbf{n}) := x_j\ W x_j^{-1} \cap G_F$, observem que

$\Gamma_j(\mathbf{n}) = \Gamma\,(t_j\partial\,, \mathbf{n})$.

En aquest marc, podem associar a una forma parabòlica de Hilbert $\mathbf{f} = (f_1, \ldots, f_h)$ una aplicació $\Phi : G_{\mathbf{A}} \longrightarrow \mathbb{C}$ per mitjà de la fòrmula

$\Phi\,(\alpha\ x_j\ w) = (f_j\ |_k\ w_\infty)\left(\underbrace{\sqrt{-1},\ldots,\sqrt{-1}}_{g}\right), \alpha \in G_F, w \in W$, la qual té sentit, i.e. $w_\infty(\sqrt{-1},\ldots,\sqrt{-1}) \in \mathbb{H}^g$, ja que $w_\infty \in (G_{\mathbf{A}})_{\infty+}$.

Aquestes funcions complexes definides a $G_{\mathbf{A}}$ satisfan certes condicions, entre les quals cal destacar

$\Phi(\alpha x_j^{-\iota} w) = \psi(w^\iota)(f_j|_{\mathbf{k}} w_\infty)(\mathbf{i}),\ \alpha \in G_{\mathbb{Q}},\ w \in W,$

on ι denota la involució principal de $M(2,F)$. Recíprocament, podem associar a qualsevol $\Phi : G_{\mathbf{A}} \longrightarrow \mathbb{C}$, satisfent certes condicions, una h-tupla $(f_1,\ldots,f_h)$ de funcions $f_j : \mathbb{H}^g \longrightarrow \mathbb{C}$ definides de la següent manera: per a tot $z = (z_1,\ldots,z_g) \in \mathbb{H}^g$ podem triar w en W tal que $w_\infty(\sqrt{-1},\ldots,\sqrt{-1}) = (z_1,\ldots,z_g)$, aleshores, si

$$w_\infty = \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix},\ldots,\begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}\right),$$

posant

$f_j(z) = \prod_{i=1}^g \left(a_i\, d_i - b_i\, c_i\right)^{-k_i/2} \prod_{i=1}^g \left(c_i(\sqrt{-1}) + d_i\right)^{k_i}\ \Phi\,(x_j\, w)$

es veu fàcilment que està ben definida i que satisfà totes les condicions, (cf. [Sh 78]).

5.4 Operadors de Hecke

Per a ideals enters $\mathbf{q}$ i $\mathbf{n}$ de $\mathcal{O}$ tenim $\mathbb{C}$-homomorfismes $T(\mathbf{q}), S(\mathbf{q}) : \mathcal{S}_{\mathbf{k}}(\mathbf{n}) \longrightarrow \mathcal{S}_{\mathbf{k}}(\mathbf{n})$. La seva acció sobre els "coeficients de Fourier "ve donada per

$c\,(\mathbf{m},\, T(\mathbf{q})\,\mathbf{f}) = \sum_{\mathbf{a}\supseteq\mathbf{m}+\mathbf{q}}\ N(\mathbf{a}^{-1}\mathbf{q})\ c\,(\mathbf{a}^{-2}\mathbf{m}\,\mathbf{q}\,,\,\mathbf{f})\,,$

$c\,(\mathbf{m},\, S(\mathbf{q})\,\mathbf{f}) = N(\mathbf{q})^{k_0-2} c\,(\mathbf{m},\,\mathbf{f}),\ \text{si}\ (\mathbf{q},\mathbf{n}) = \mathcal{O},$

$c\,(\mathbf{m},\, S(\mathbf{q})\,\mathbf{f}) = 0,\ \text{si}\ (\mathbf{q},\mathbf{n}) \neq \mathcal{O},$

on N denota la norma de l'ideal, i k_0= max $(k_1,\ldots,k_g)$.

Teorema

Sigui $\mathbf{q} \subset \mathcal{O}$ ideal primer. L'àlgebra de Hecke

$$\mathbb{T}(W, Y) = \mathbb{Z}[T(\mathbf{q}), S(\mathbf{q})]$$

és commutativa i amb els $T(\mathbf{q}), S(\mathbf{q})$ algebraicament independents.

Amb les següents lleis de multiplicació:

$T(\mathbf{m}_1\mathbf{m}_2) = T(\mathbf{m}_1)T(\mathbf{m}_2)$, si $(\mathbf{m_1}, \mathbf{m_2}) = \mathcal{O}$.

$T(\mathbf{q}^r)T(\mathbf{q}) = T(\mathbf{q}^{r+1}) + N(\mathbf{q})S(\mathbf{q})T(\mathbf{q}^{r-1})$.

El teorema anterior equival a dir que la sèrie formal de Dirichlet $\sum_{\mathbf{m}} T(\mathbf{m})N(\mathbf{m})^{-s}$ ($\mathbf{m}$ recorre els ideals enters de $\mathcal{O}$), té producte d'Euler $\prod_{\mathbf{q}}(1 - T(\mathbf{q})N(\mathbf{q})^{-s} + S(\mathbf{q})N(\mathbf{q})^{1-2s})^{-1}$, ($\mathbf{q}$ recorre els ideals primers de $\mathcal{O}$).

5.5 Producte escalar de Petersson

Donades dues formes parabòliques de Hilbert $\mathbf{f} = (f_1, \ldots, f_h), \mathbf{g} = (g_1, \ldots, g_h) \in \mathcal{S}_{\mathbf{k}}(\mathbf{n})$, es defineix el seu producte escalar de Peterssson per $< \mathbf{f}, \mathbf{g} >= \sum_{j=1\ldots,h} < f_j, g_j >$, on $< f_j, g_j >$ ve donat per

$$\mu(\Gamma\backslash\mathbb{H}^g)^{-1} \int_{\Gamma\backslash\mathbb{H}^g} \overline{f_j(z)} g_j(z) d\mu(z),$$

on $d\mu(z) = \prod_{\nu=1}^{g} y_\nu^{-2} dx_\nu dy_\nu$, $z_\nu = x_\nu + i\, y_\nu$,i $\mu(\Gamma\backslash\mathbb{H}^g)$ és la mesura d'un domini fonamental de $\Gamma\backslash\mathbb{H}^g$ respecte de $d\mu(z)$.

Remarca (Siegel).

$\mu(\Gamma_j(\mathbf{n})\backslash\mathbb{H}^g) = 2\pi^{-g} D_F^{3/2} \zeta_F(2)\ [\mathcal{O}_+^* : \mathcal{O}^{*2}] \prod_{\mathbf{p}|\mathbf{n}}(1 + N(\mathbf{p})^{-1})$.

Teorema

Si $\mathbf{f}, \mathbf{g} \in \mathcal{S}_{\mathbf{k}}(\mathbf{n})$, $(\mathbf{m}, \mathbf{n}) = \mathcal{O}$, es té $< \mathbf{f}|_{\mathbf{k}} T(\mathbf{m}), \mathbf{g} >=< \mathbf{f}, \mathbf{g}|_{\mathbf{k}} T(\mathbf{m}) >$.

L'espai $\mathcal{S}_{\mathbf{k}}(\mathbf{n})$ té una base de funcions pròpies respecte de tots els operadors de Hecke $T(\mathbf{m})$ amb $(\mathbf{m}, \mathbf{n}) = \mathcal{O}$.

5.6 Sèries L

Si $\mathbf{f} \in \mathcal{S}_{\mathbf{k}}(\mathbf{n})$, es defineix $L(s, \mathbf{f}) = \sum c(\mathbf{m}, \mathbf{f}) N(\mathbf{m})^{-s}$, on $\mathbf{m}$ recorre tots els ideals enters de F.

$L(s, \mathbf{f})$ convergeix per a $Re(s) > \frac{k_0}{2} + 1$ i es pot perllongar a una funció meromorfa en tot el pla.

Una forma parabòlica $\mathbf{f} \in \mathcal{S}_{\mathbf{k}}(\mathbf{n})^{new}$ s'anomena nova si és (normalitzada i) vector propi respecte de tots els $T(\mathbf{m})$ amb $(\mathbf{m}, \mathbf{n}) = \mathcal{O}$. Per un resultat de Miyake [Mi 71], també ho és respecte de la resta d'operadors de Hecke. Si

$\mathbf{f}|T(\mathbf{m}) = \theta(T(\mathbf{m}))\mathbf{f}, \quad \mathbf{f}|S(\mathbf{m}) = \theta(S(\mathbf{m}))\mathbf{f}$, es té

$L(s, \mathbf{f}) = \prod_{\mathbf{p}}(1 - \theta(T(\mathbf{p}))N(\mathbf{p})^{-s} + \theta(S(\mathbf{p}))N(\mathbf{p})^{1-2s})^{-1}$

Els valors propis dels $T(\mathbf{p})$ són nombres algebraics. Si $k_1 = \cdots = k_g$, són enters algebraics.

Si $k_1 \equiv \cdots \equiv k_g \pmod 2$, aleshores $L_{\mathbf{f}} = \mathbb{Q}(\theta(T))$ és un cos de nombres. Denotem per $\mathcal{O}_{\mathbf{f}}$ el seu anell d'enters.

5.7 Representacions λ-àdiques

Sigui $\lambda \subset \mathcal{O}_{\mathbf{f}}$ un ideal primer, designem per $\mathcal{O}_{\mathbf{f},\lambda}$ la completació de $\mathcal{O}_{\mathbf{f}}$ a λ. Per a $\mathbf{q} \subset \mathcal{O}$ ideal primer, $Frob\,\mathbf{q}$ designa l'automorfisme de Frobenius en $Gal(\overline{F}/F)$

Teorema

Per a tot $\lambda \subset \mathcal{O}_{\mathbf{f}}$ ideal primer, $\lambda \cap \mathbb{Z} = \ell$, existeix una representació contínua

$\rho_{\mathbf{f},\lambda} : Gal(\overline{F}/F) \longrightarrow GL(2, \mathcal{O}_{\mathbf{f},\lambda})$

no ramificada fora dels primers $\mathbf{q} \subset \mathcal{O}$ amb $\mathbf{q}$ no dividint $\mathbf{n}\ell$ i tal que

$tr\rho_{\mathbf{f},\lambda}(Frob\,\mathbf{q}) = \theta(T(\mathbf{q}))$, $det\rho_{\mathbf{f},\lambda}(Frob\,\mathbf{q}) = \theta(S(\mathbf{q}))N\mathbf{q}$.

La següent remarca recull diverses aportacions a la prova d'aquest teorema.

Remarca

a)Si $F = \mathbb{Q}$

$k = 2$, Eichler-Shimura. $k > 2$, Deligne. $k = 1$, Serre-Deligne.

b) Si $[F : \mathbb{Q}] > 1$, i $k_j \geq 2$, $j = 1, \ldots, h$, el teorema està provat si:

1. $[F : \mathbb{Q}]$ imparell.

2. $[F : \mathbb{Q}]$ parell i $\mathbf{f}$ correspon a una representació automorfa cuspidal de $GL(2, F_{\mathbf{A}})$, $\pi_{\mathbf{f}} = \bigotimes \pi_{\mathbf{f},v}$, tal que per a certa plaça finita $v, \pi_{\mathbf{f},v}$ és especial o supercuspidal. (1)+(2) Ohta, Rogawski i Tunnell.

3. ℓ és un primer ordinàri per a $\mathbf{f}$ (i.e. ℓ és primer a $\theta(T(\mathbf{q}))$ per a tot primer $\mathbf{q}$ de F sobre ℓ), Wiles.

4. $[F : \mathbb{Q}]$ parell, Taylor.

Proposició ([Wi 88])

Si $\mathbf{f} \in \mathcal{S}_2(\mathbf{n})$, $\mathbf{n} \subset \mathcal{O}$, $[F : \mathbb{Q}] = 2$, aleshores, existeixen infinits primers $\lambda \subset \mathcal{O}_{\mathbf{f}}$, pels quals $\mathbf{f}$ és ordinària en λ. En particular existeixen les corresponents $\rho_{\mathbf{f},\lambda}$.

Teorema (Deligne, Langlands, Carayol, Wiles, Taylor)

Si $\mathbf{q} \subset \mathcal{O}$ ideal primer amb $\mathbf{q}|\mathbf{n}$, $(\mathbf{q}, \ell\mathcal{O}) = \mathcal{O}$,

$\theta(T(\mathbf{q})) \neq 0$ i si $\sigma \in D_{\mathbf{q}}$ sobre $Frob\ \mathbf{q}$, aleshores

$tr\rho(\sigma) = \theta(T(\mathbf{q})) + \chi(\sigma)(N\mathbf{q})\theta(T(\mathbf{q}))^{-1}$,

$det\rho(\sigma) = \chi(\sigma)N\mathbf{q}$.

χ caràcter de Galois continu que estèn l'aplica-

ció, $Frob\ \mathbf{q} \longrightarrow \theta(S(\mathbf{q}))$, $\mathbf{q}$ primer i $(\mathbf{q}, \mathbf{n}\ell) = \mathcal{O}$.

Proposició ([Ta 93])

Per a totes les λ's, $\lambda|\ell$,llevat d'un nombre finit,les representacions λ-àdiques són cristal·lines.

5.8 Formes modulars associades a àlgebres de quaternions

Per la correspondència de Jacquet-Langlands es poden associar a les formes noves de Hilbert, formes modulars relatives a àlgebres de quaternions.

B un àlgebra de quaternions sobre un cos totalment real F , G_B l'adelització de B^* (també anomenat grup d'idèles de B). $(G_B)_\infty$ la part arquimediana de G_B, $(G_B)_{\infty+}$ la component connexa de l'identitat de $(G_B)_\infty$ i.e., llevat d'ordre, $(G_B)_{\infty+} \simeq \left(GL^+(2,\mathbb{R})\right)^t \times (\mathcal{H}^*)^{g-t}$ si B ramifica en exactament $(g-t)$ places infinites , i $(G_B)_0$ per a la part finita de G_B. Per a qualsevol plaça $\mathbf{p}$ (finita o no) de F, $(G_B)_\mathbf{p}$ denotará la $\mathbf{p}$ component de G_B.

El cas més simple $B = M(2,F)$ és essencialment el que correspon a les formes modulars de Hilbert $(t = g)$.

B indefinida (i.e. amb $t > 0$) F-algebra de divisió quaterniònica. B totalment definida $(t = 0)$, Hida + Taylor.

5.9 Formes modulars Λ-àdiques

$\mathcal{O}_L$ una extensió finita de $\Lambda = \mathbb{Z}_p[[T]]$.

Es consideren q-desenvolupaments formals $\mathcal{F}$ amb coeficients en $\mathcal{O}_L$ i amb els exponents de q pertanyent al conjunt d'elements totalment positius de $\mathcal{O}_L$ amb el 0.

$\mathcal{F}$ és una forma Λ-àdica si mòdul cada un dels ideals primers d'un conjunt infinit $\{P_\nu\}$ de $\mathcal{O}_L$, $\mathcal{F}$ redueix a un q-desenvolupament d'una forma modular de Hilbert "de veritat" $\mathbf{f}_\nu$ sobre F.

Si $h > 1$, $\mathcal{F}$ serà un vector format per h sèries de potències.

Bibliografia

[Ar 00] Arenas, A.: *Formes modulars de Hilbert* . Varietats abelianes amb multiplicació complexa. Notes del Seminari de Teoria de Nombres (UB-UAB-UPC) (2000), 161-173.

[Hi 73] Hirzebruch, F.: Hilbert modular surfaces. *L'Ens. Math.* **19** (1973), 183-281.

[Mi 71] Miyake, T.: On automorphic forms on GL_2 and Hecke operators. *Ann. of Math.* **94** (1971), 174-189.

[Sh 78] Shimura, G.: The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.* **45** No.3 (1978), 637-697.

[Ta 89] Taylor, R.: On Galois representations associated to Hilbert modular forms. *Invent. Math.* **98** (1989), 265-280.

[Ta 93] Taylor, R.: *On Galois representations associated to Hilbert modular forms II.* Elliptic Curves, Modular Forms,and Fermat's Last Theorem. International Press (1993), 185-191.

[Wi 88] Wiles, A.: On ordinary λ-adic representations associated to modular forms. *Invent. Math.* **94** (1988), 529-573.

A. Arenas
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les corts Catalanes 585, E-08007 Barcelona,
angelaarenas@ub.edu

Capítol 6

Modularitat potencial de representacions de Galois

Luis V. Dieulefait, Núria Vila

Aquestes notes contenen la transcripció de les transparències presentades per N. Vila a la segona part de la xerrada *Modularitat Potencial I* i un resum del contingut de la xerrada de L. Dieulefait, amb títol *Modularitat Potencial II.*

6.1 Enunciat del teorema de modularitat potencial i les seves conseqüències

En primer lloc enunciarem el teorema de modularitat potencial i les seves conseqüències, teorema B de Taylor a [Ta]). A continuació donarem un esbós de la prova de les bones propietats de la funció L i de la prova de la conjectura de Fontaine-Mazur en casos 2-dimensionals, assumint el punt 1 del teorema B de [Ta] que serà discutit a la secció següent.

Amb el suport parcial de MCYT BFM2003-01898.

TEOREMA B (Taylor)
Sigui $\ell > 3$ primer, $2 \leq k \leq (\ell+1)/2$ enter.
Sigui $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \overline{\mathbb{Q}_\ell})$ representació continua irreductible tal que:
• ρ ramifica només un nombre finit de primers.
• $\det \rho(c) = -1$.
• $\rho | G_\ell$ és cristal.lina amb nombres de Hodge-Tate: 0 i 1-k.
Aleshores,

1. Existeix $F/\mathbb{Q}$ totalment real Galois finita tal que ℓ no ramifica a F, una representació automorfa π cuspidal regular algebraica de $\mathrm{GL}(2, \mathbb{A}_F)$ i un primer λ en el cos de racionalitat M de π ($M_\lambda \hookrightarrow \overline{\mathbb{Q}_\ell}$) tal que:
   • $\rho_{\pi,\lambda} \sim \rho | G_F$
   • π_x és no ramificada per a totes les places x sobre ℓ i
   • π_∞ té pes k.

2. Si ρ és no ramificada en un primer p i α és un valor propi de $\rho(\mathrm{Frob}_p)$ aleshores $\alpha \in \overline{\mathbb{Q}}$ i per a tot isomorfisme $i : \overline{\mathbb{Q}_\ell} \simeq \mathbb{C}$ és té:
$$|i\alpha| = p^{(k-1)/2}.$$

3. Fixem un isomorfisme $i : \overline{\mathbb{Q}_\ell} \simeq \mathbb{C}$. Existeix una funció racional $L_{\ell,i}(X) \in \mathbb{C}(X)$ tal que el producte:
$$L(i\rho, s) = L_{\ell,i}(\ell^{-s})^{-1} \prod_{p \neq \ell} i \det(1 - \rho_{I_p}(\mathrm{Frob}_p) p^{-s})^{-1}$$
   convergeix per $\Re s > (k+1)/2$ i s'estén a una funció meromorfa a tot el pla complex que satisfà l'equació funcional:
$$(2\pi)^{-s}\Gamma(s)L(i\rho, s) = WN(\rho)^{k/2-s}(2\pi)^{s-k}\Gamma(k-s)L(i(\rho^\vee \otimes \epsilon^{k-1}), k-s),$$
   on ϵ és el caràcter ciclotòmic,
   $N(\rho)$ és el conductor de ρ (primer amb ℓ),
   W és un nombre complex de norma 1.

4. Si $k = 2$, suposem a més que, per algun primer $p \neq \ell$ tenim:
$$\rho | G_p \sim \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}.$$

Aleshores ρ es realitza en la cohomologia ℓ-àdica (amb coeficients en un twist de Tate del feix constant) d'una varietat sobre $\mathbb{Q}$.

De fet, veurem a la secció següent:
TEOREMA (M P)
Sigui $\ell > 3$ primer, $2 \leq k \leq \ell - 1$ enter, $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \overline{\mathbb{Q}}_\ell)$ representació continua irreductible senar, que ramifica només un nombre finit de primers i $\rho|G_\ell$ és cristal.lina amb nombres de Hodge-Tate: 0 i 1-k. Si la representació reduïda $\overline{\rho}$ és irreductible, suposem que resta irreductible quan la restringim a $\mathbb{Q}_\ell(\sqrt{(-1)^{(\ell-1)/2}\ell})$ (això es automàtic si $2k \neq \ell + 3$). Aleshores, existeix $F/\mathbb{Q}$ totalment real Galois finita en el que ℓ no ramifica tal que:
Per cada subcos $E \subset F$ amb $\mathrm{Gal}(F/E)$ soluble existeix una una representació automorfa π_E cuspidal regular algebraica de $\mathrm{GL}(2, \mathbb{A}_E)$ i una immersió λ del cos de coeficients de π_E en $\overline{\mathbb{Q}}_\ell$, tal que:
- $\rho_{\pi_E,\lambda} \sim \rho|G_E$
- $\pi_{E,x}$ és no ramificada per a totes les places x de E sobre ℓ i
- $\pi_{E,\infty}$ té pes k.

6.1.1 "Prova" de les bones propietats de la funció L ((2)+(3)) a partir de M P

Per (1) i el Th 3.4.6 de Brylinski-Labesse [BL 84] tenim (2): $|i\alpha| = p^{(k-1)/2}$.

Com a conseqüència:
- $|i(\mathrm{tr}\,\rho(\mathrm{Frob}_p))| \leq 2p^{(k-1)/2}$.
- Si $L_p(i\rho, X) := i\det(1 - \rho_{I_p}(\mathrm{Frob}_p)X) \in \mathbb{C}(X)$,

$$L^\ell(i\rho, s) = \prod_{p \neq \ell} L_p(i\rho, p^{-s})^{-1}$$

defineix una funció meromorfa a $\Re s > (k+1)/2$.

Sigui
$$L(i\rho, s) = L^\ell(i\rho, s) L_\ell(i\rho, \ell^{-s})^{-1}$$

Pel teorema de Brauer, la representació trivial de $\mathrm{Gal}(F/\mathbb{Q})$, és

$$\sum_j n_j \,\mathrm{Ind}_{G_{F_j}}^{G_\mathbb{Q}} \chi_j,$$

on F_j/F amb $\mathrm{Gal}(F/F_j)$ és resoluble, $\chi_j : \mathrm{Gal}(F/F_j) \to \overline{\mathbb{Q}}^\times$.
Per cada j hi ha una representació automorfa π_j cuspidal, regular i algebraica de $\mathrm{GL}_2(\mathbb{A}_{F_j})$ tal que $\rho|G_{F_j} \sim \rho_{\pi_j,\ell}$. Aleshores,

$$\rho = \sum_j n_j \,\mathrm{Ind}_{G_{F_j}}^{G_\mathbb{Q}} \chi_j \otimes \rho_{\pi_j,\ell}.$$

En conseqüència,

$$L(i\rho, s) = \prod_j L(\pi_j \otimes (\chi_j \circ \det), s)^{n_j},$$

d'on s'obté la continuació meromorfa a tot el pla complex i l'equació funcional.

Escollim un caràcter additiu no trivial $\Psi = \Psi_p : \mathbb{A}_F/\mathbb{Q} \to \mathbb{C}^\times$ amb $\mathrm{Ker}\Psi_\ell = \mathbb{Z}_\ell$ i $\Psi_\infty = e^{2\pi\sqrt{-1}x}$
Escollim una mesura de Haar $dx = \prod dx_p$ a $\mathbb{A}_F$, amb
dx_∞ la mesura usual a $\mathbb{R}$, $dx_\ell(\mathbb{Z}_\ell) = 1$ i $dx(\mathbb{A}_F/F) = 1$
Si $p \neq \ell$, sigui $\mathrm{WD}(\rho|G_p)$ la representació de Weil-Deligne associada a $\rho|G_p$. Definim a la Tate:

$$\epsilon(i\rho, s) = \sqrt{-1}^k \prod_{p\neq\ell} \epsilon(i\,\mathrm{WD}(\rho^\vee|G_p) \otimes |\,\mathrm{Art}^{-1}|_p^{-s}, \Psi_p, dx_p).$$

Tenim, $\epsilon(i\rho, s) = WN^{k/2-s}$, on W és independent de s i N és el conductor de ρ.

6.1.2 "Prova" de (4) (conjectura de Fontaine-Mazur) a partir de M P

De (1), resultats motívics de Blasius i Rogawski [BR 93] i restricció d'escalars, tenim que ρ es realitza en la cohomologia ℓ-àdica d'una varietat sobre $\mathbb{Q}$.

És més, veiem que si $k = 2$ existeix un cos de nombres M, un primer λ de M sobre ℓ, una varietat abeliana $A/\mathbb{Q}$ de dimensió $[M : \mathbb{Q}]$ i una immersió $\mathcal{O}_M \hookrightarrow \mathrm{End}(A/\mathbb{Q})$ tal que $\rho_{A,\lambda} \sim \rho$.

De (1) i per [Hi 81], existeix F cos totalment real, N un cos de nombres, λ' primer de N sobre ℓ, B/F varietat abeliana de dimensió $[N : \mathbb{Q}]$ i una immersió $\mathcal{O}_N \hookrightarrow \mathrm{End}(B/F)$ tal que

$$\rho_{B,\lambda'} \sim \rho | G_F.$$

Sigui C la restricció d'escalars de F a $\mathbb{Q}$ de B. Tenim

$$\mathrm{End}_{\mathcal{O}_N}(C/\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq P \oplus \bigoplus_{i=1}^{r} M_i,$$

On M_i/N finita. A menys d'isogènies dóna:
$C \sim A_P \oplus \bigoplus_{i=1}^{r} A_i$, amb $\mathcal{O}_{M_i} \simeq \mathrm{End}_{\mathcal{O}_N}(A_i/\mathbb{Q})$.
Ara $V_{\lambda'} C \simeq \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} V_{\lambda'} B \simeq X \oplus Y$, amb $X \sim \rho$.
Per Faltings, a $(\mathrm{End}_{\mathcal{O}_N}(C/\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q})_{\lambda'}$ li correspon una descomposició $P_X \oplus P_Y$. Per tant, podem escollir $i = 1, \cdots, r$ i un primer λ_i de M_i sobre λ' tal que $V_{\lambda_i} A_i = X$.
En conseqüència:
$M = M_i$, $\lambda = \lambda_i$ sobre ℓ, $A = A_i$, dóna

$$\rho_{A,\lambda} \sim \rho.$$

COROL.LARI
Si $\ell > 3$ primer, $\overline{\rho} : G_\mathbb{Q} \longrightarrow \mathrm{GL}(2, \overline{\mathbb{F}}_\ell)$ representació continua irreductible imparell i

$$\overline{\rho} | G_\ell \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

amb $\chi_1 | I_\ell \neq \chi_2 | I_\ell$. Aleshores existeix un cos de nombres M, un primer λ de M sobre ℓ, una varietat abeliana $A/\mathbb{Q}$ de dimensió $[M : \mathbb{Q}]$ i una immersió $\mathcal{O}_M \hookrightarrow \mathrm{End}(A/\mathbb{Q})$ tal que $\overline{\rho}$ és equivalent a la representació de Galois associada a la λ torsió de A.

Utilitzant la generalització del resultats de Ramakrishna [Ra 02] de Taylor a [Ta 03], hi ha l'aixecament ℓ-àdic, satisfent les condicions.

6.2 Bosquejo de la demostración del teorema de modularidad potencial

Nos proponemos dar algunas ideas de la demostración de R. Taylor (cf. [Ta 02] y [Ta]) del resultado de modularidad potencial llamado Teorema M P en la sección previa, o equivalentemente, del apartado (1) del Teorema B.
La demostración se divide en dos casos, dependiendo de si la representación ρ es ordinaria (localmente en ℓ) o es cristalina pero no ordinaria. Llamemos (a) al primer caso y (b) al segundo. El caso (b) difiere del (a) en algunos aspectos técnicos, y fundamentalmente en lo siguiente:
En ambos casos se prueba primero que la representación residual $\bar{\rho}$ cumple $\bar{\rho}|_{G_F}$ es modular (si la representación residual es irreducible). Luego, se precisa un resultado "tipo Wiles"sobre el cuerpo F para concluir a partir de esta modularidad residual (o reducibilidad residual) que toda "buena deformación", y en particular $\rho|_{G_F}$, es modular. En el caso ordinario, sendos resultados (que cubren tanto el caso residualmente reducible como el residualmente modular) de Skinner y Wiles (cf. [SW 99] y [SW 01]) pueden aplicarse para concluir la modularidad de $\rho|_{G_F}$. En el caso no-ordinario, caso (b), Taylor demuestra (generalizando resultados anteriores de Taylor-Wiles y Diamond) el resultado requerido, que enunciaremos luego.
Observación: es sabido que en el caso (b) la restricción de $\bar{\rho}$ al grupo de inercia en ℓ actúa a través de caracteres fundamentales de nivel 2, y esto implica que $\bar{\rho}$ es necesariamente irreducible en el caso (b).

Veamos ahora la estrategia que utiliza R. Taylor para probar que sobre un cierto cuerpo F totalmente real es $\bar{\rho}|_{G_F}$ modular. Por simplicidad seguiremos en esta parte su primera demostración, que es la del caso (a), efectuada en [Ta 02].
Si $\bar{\rho}$ tiene imagen soluble, por resultados de Langlands y Tunnell se sabe que es modular (cambio de base soluble). Luego, podemos asumir que la imagen residual es un grupo insoluble.
Por simplicidad asumamos que el determinante de $\bar{\rho}$ es simplemente el caracter ciclotómico ϵ. La idea es probar que existen cuerpos totalmente reales E y M, un primo p y una variedad abeliana A definida

sobre E cumpliendo:
· p y ℓ no ramifican en E
· la dimensión de A es igual al grado de M sobre $\mathbb{Q}$
· El anillo de enteros algebraicos $\mathcal{O}$ de M está contenido en $\mathrm{End}(A/E)$
· Para un primo $\lambda \mid \ell$ de $\mathcal{O}$ la representación de Galois asociada a $A[\lambda](\bar{E})$ es equivalente a $\bar{\rho}|_{G_E}$
· A tienen reducción buena ordinaria en todos los primos que dividen a p
· Existe un primo $\mathcal{P}$ de $\mathcal{O}$ dividiendo a p tal que el G_E-modulo $A[\mathcal{P}](\bar{E})$ es de la forma $\mathrm{Ind}_{\mathrm{Gal}(\bar{L}/L)}^{\mathrm{Gal}(\bar{E}/E)} \omega$ para una extensión cuadrática L de E no contenida en $E(\zeta_p)$ y un caracter ω de $\mathrm{Gal}(\bar{L}/L)$

La clave para establecer la modularidad residual de $\rho|_{G_E}$ es la existencia de una tal variedad abeliana A, pues por construcción esta variedad es de tipo GL_2 y la representación de Galois asociada a su $\mathcal{P}$ torsión es dihedral, luego modular, por lo que si tenemos a nuestra disposición un resultado de tipo Wiles concluimos que como $\bar{\rho}_{A,\mathcal{P}}$ es modular, $\rho_{A,\mathcal{P}}$ es modular, es decir A es modular, y por lo tanto $\rho_{A,\lambda}$ y la representación residual correspondiente $\bar{\rho}_{A,\lambda}$ son modulares, y como esta última por construcción coincide con $\bar{\rho}|_{G_E}$ esta también es modular, de donde aplicando nuevamente resultados tipo Wiles se concluye que $\rho|_{G_E}$ es modular.

Pasemos ahora a discutir como probar, una vez adecuadamente elejidos M y p, la existencia de un cuerpo E y una variedad abeliana A/E que cumpla las propiedades deseadas. Esto equivale a la construcción de puntos de cierta variedad modular de Hilbert-Blumenthal sobre un cuerpo totalmente real E en el que ni ℓ ni p ramifiquen.

Este problema, debido al siguiente principio local-global de Moret-Bailly, equivale a una tal construcciòn localmente en ℓ, p e ∞.

TEOREMA (M B): Sea K cuerpo de números y S conjunto finito de primos de K (tanto no-arquimedeanos como arquimedeanos). Sea K_S la máxima extensión de K en la que los primos de S descomponen

totalmente.
Sea $X/Spec\ K$ esquema quasi-proyectivo genéricamente irreducible tal que, para todo v en S, $X(K_v)$ es no vacío (donde K_v denota la completación v-adica de K). Entonces $X(K_S)$ es Zariski denso en X.

En virtud de este resultado, la existencia de un cuerpo E y una variedad A/E como la que buscamos se reduce a un problema mucho más simple de existencia sobre cuerpos locales, en nuestro caso sobre $\mathbb{Q}_\ell$, $\mathbb{Q}_p$ y $\mathbb{R}$.

Por ejemplo, la existencia sobre $\mathbb{Q}_\ell$ de una variedad de Hilbert-Blumenthal con las propiedades que buscamos, es decir, tal que la representación de Galois asociada a su λ torsión coincida con la restricciòn de $\bar{\rho}$ al grupo de descomposición D_ℓ en ℓ y la asociada a su $\mathcal{P}$ torsión con la restricción de una dihedral a D_ℓ, se deduce de resultados de Rapaport en el caso ordinario de peso 2 y de resultados de Honda-Tate (para establecer la existencia sobre $\mathbb{F}_\ell$) y de Serre-Tate (para clasificar las deformaciones a $\mathbb{Z}_\ell$, como grupos de Barsotti-Tate, via ciertas extensiones).
La existencia sobre $\mathbb{R}$ es trivial, basta tomar una curva elíptica E sobre $\mathbb{R}$ y considerar $A = E \otimes_{\mathbb{Z}} \mathcal{O}$.

Por lo tanto, dada la existencia local de una variedad abeliana con las propiedades deseadas sobre $\mathbb{Q}_p$, $\mathbb{Q}_\ell$ y $\mathbb{R}$, por el teorema (M B) se concluye que sobre un cuerpo E totalmente real en el que ℓ y p descomponen totalmente existe una variedad A de Hilbert-Blumenthal con multiplicación real por $\mathcal{O}$ con $\bar{\rho}_{A,\lambda} \cong \bar{\rho}|_{G_E}$ y $\bar{\rho}_{A,\mathcal{P}}$ dihedral. Como ya comentamos, de esto se sigue la modularidad de $\rho|_{G_E}$, si se dispone de resultados tipo Wiles sobre E.

En el caso ordinario, el resultado de tipo Wiles necesario: "residualmente modular (o reducible) implica modular"es un teorema de Skinner y Wiles. Para el caso no-ordinario (b), Taylor demuestra un resultado similar, generalizando resultados de Taylor-Wiles y Diamond al caso de cuerpos de nùmeros totalmente reales:

TEOREMA: Sea $\ell > 3$, $2 \leq k \leq \ell - 1$.
Sea F totalmente real de grado par en el que ℓ descompone totalmente. Sea

$$\rho : G_F \to \mathrm{GL}_2(\bar{\mathbb{Q}}_\ell)$$

representación irreducible que solo ramifica en un conjunto finito de primos tal que para cada primo x de F dividiendo a ℓ ρ es cristalina localmente en x con números de Hodge-Tate 0 y $1 - k$. Supongamos que $\bar{\rho}$ restringida a $F(\sqrt{\pm\ell})$ (el signo tal que sea una extensión cuadrática no-ramificada fuera de ℓ) es irreducible y que existe una forma de Hilbert f sobre F tal que:
· $\bar{\rho}_{f,\lambda} \cong \bar{\rho}$ (para algun primo $\lambda \mid \ell$ en el cuerpo generado por los coeficientes de f)
· f es no ramificada en todo primo finito x de F (nivel minimal)
· f es de peso (paralelo) k

Entonces existe una forma de Hilbert f' sobre F tal que $\rho \cong \rho_{f',\lambda'}$ y f' tiene peso paralelo k.

Observaciones:
(1) La condición de nivel minimal puede parecer demasiado restrictiva, pues en general $\bar{\rho}$ puede ramificar en uno o más primos. De todos modos, siguiendo una estrategia de bajada de nivel via cambio de base soluble (creada por Skinner y Wiles) se sabe que elijiendo adecuadamente una extensión soluble de un cuerpo dado E siempre podemos reducirnos a un caso de "conductor 1"donde la condición de nivel minimal (que es precisa para probar el teorema de tipo Wiles anterior) se satisface.
(2) Una vez establecida la modularidad de la restricciòn de ρ a un cuerpo totalmente real F, para todo subcuerpo K de F tal que $\mathrm{Gal}(F/K)$ sea soluble, se deduce de los teoremas de cambio de base soluble automorfos que también sobre K se tiene el resultado de modularidad de la restricción de ρ.

6.2.1 Otras aplicaciones de la modularidad potencial

Además de las consecuencias mencionadas en la primera sección, Taylor también demuestra, utilizando propiedades conocidas de las familias compatibles de representaciones de Galois asociadas a formas de Hilbert (en particularidad la compatibilidad Langlands global - Langlands local) y argumentos que utilizan el teorema de Brauer para relacionar una representación ℓ-adica con ciertas restricciones (a algunos subcuerpos de F) donde se sabe que es modular (véase en la sección 1 una descripción de este tipo de argumento, aplicado a probar las buenas propiedades de la función L) que dada una familia compatible de representaciones de Galois contínuas, irreducibles, dos-dimensionales, e impares, tal que genéricamente (o sea para todo ℓ suficientemente grande) cumple las condiciones de aplicabilidad del teorema (B), de la modularidad potencial de una de las representaciones de la familia se deduce automáticamente la modularidad potencial de toda la familia, y de esto se deduce que la familia cumple una propiedad de compatibilidad local que Taylor denomina "fuertemente compatible", propiedad que a priori se sabía solo en el caso de una familia de representaciones asociada a una forma modular. Esta propiedad viene a decir que dos representaciones ρ_ℓ y $\rho_{\ell'}$ cualesquiera de la familia ramifican en el mismo conjunto S (sin contar a ℓ ni a ℓ') y más aún que el tipo de ramificación en cada uno de estos primos es el mismo (cf. [Ta]), o sea que esencialmente para p fijo el comportamiento local $\rho_\ell|_{D_p}$ no depende de ℓ, si $\ell \neq p$.

Una consecuencia aún más fuerte, probada por el primer autor en [Di 04], es que, dada una representación ℓ-adica ρ que cumple las condiciones del teorema (B), entonces siempre se puede incluir en una familia compatible de representaciones de Galois cuyo conjunto de ramificación S coincide con el conjunto de ramificación de ρ (sin incluir ℓ) y tales que para todo primo impar ℓ' fuera de S la representación ℓ'-adica de la familia también será cristalina. Las técnicas para demostrar este resultado incluyen una vez más la utilización del teorema de Brauer y de propiedades conocidas de las representaciones de Galois asociadas a formas de Hilbert, incluyendo resultados de Breuil que garantizan que estas representaciones son cristalinas con gran generalidad, para primos fuera del nivel.

Recordemos que hay casos donde el apartado 4 del teorema B no puede aplicarse por ser $k = 2$ y no cumplirse la condición local (ver Teorema B, 4) (condición necesaria para que los resultados de Blasius-Rogawski o Hida que implican que las representaciones de Galois asociadas a formas de Hilbert son motívicas puedan aplicarse). Por ejemplo, si $k = 2$ (en este caso se dice que la representación es Barsotti-Tate) y la representación es semiestable en todos los primos donde ramifica, entonces la condición local del teorema B - 4 no se cumple y no podemos concluir, a pesar de ser potencialmente modular, que la representación provenga de la geometría.
Sin embargo, a partir del resultado de existencia de familias mencionado en el párrafo anterior, en algunos casos donde $k = 2$, incluso si la representación es semiestable, es posible demostrar la conjetura de Fontaine-Mazur y además la modularidad de la representación utilizando el truco de transladar el problema a un problema similar pero cambiando la caracteristica residual a un valor suficientemente pequeño, donde la modularidad puede establecerse utilizando las técnicas de Wiles. Este argumento funciona por ejemplo para probar la conjetura de Fontaine-Mazur en el caso $k = 2$ y conductor 1, y también en el caso $k = 2$ y coeficientes enteros (este último es el caso de representaciones que tienen el mismo aspecto que las asociadas a curvas elípticas).
En el caso $k = 2$ y conductor 1, de la modularidad de la representación se concluye su no existencia, pues no hay formas modulares de peso 2 y nivel 1. Para una demostración de estos casos de Fontaine-Mazur y otras aplicaciones de la modularidad potencial, ver [Di 04].

Para terminar, comentemos que también pueden aplicarse los resultados de modularidad potencial para establecer casos de la conjetura de Serre: recientemente dos trabajos independientes, uno del primer autor y otro de Khare y Wintenberger (ver [Di] y [KW]), utilizando la "existencia de familias" y la no-existencia de representaciones ℓ-adicas cristalinas con $k = 2$ y conductor 1 probadas en [Di 04], combinadas con un resultado de existencia de levantamiento minimal para representaciones residuales, que también se deduce de la modularidad potencial (y de resultados de bajada de nivel para formas de Hilbert); prueban la conjetura de Serre en el caso de peso 2 y nivel 1 (y otros casos de baja ramificación).

Bibliografia

[BL 84] Brylinski J.-L., Labesse, J.-P.: Cohomologie d'intersection et fonctions L de certaines variétés de Shimura, *Ann. Sci. ENS* **17** (1984), 361-412.

[BR 93] Blasius, D., Rogawski, J.: Motives for Hilbert modular forms, *Invent. Math.* **114** (1993), 55-87.

[Di 04] Dieulefait, L.: Existence of families of Galois representations and new cases of the Fontaine-Mazur conjecture, *J. Reine Angew. Math.* **577** (2004), 147-151.

[Di] Dieulefait, L.: The level 1 weight 2 case of Serre's conjecture, preprint disponible a: http://front.math.ucdavis.edu/math.NT

[Hi 81] Hida, H.: On abelian varieties with complex multiplications as factors of the Jacobian of Shimura curves, *Amer. J. Math.* **103** (1981), no. 4, 727–776.

[KW] Khare, C., Wintenberger, J-P.: On Serre's reciprocity conjecture for 2-dimensional mod p representations of the Galois group of Q , preprint disponible a: http://front.math.ucdavis.edu/math.NT

[Ra 02] Ramakrishna, R.: Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur, *Ann. of Math. (2)* **156** (2002), no. 1, 115–154.

[SW 99] Skinner, C., Wiles, A.: Residually reducible representations and modular forms, *Inst. Hautes Études Sci. Publ. Math.* **89** (1999), 5-126.

[SW 01] Skinner, C., Wiles, A.: Nearly ordinary deformations of irreducible residual representations, *Ann. Fac. Sci. Toulouse Math. (6)* **10** (2001), 185-215.

[Ta 02] Taylor, R.: Remarks on a conjecture of Fontaine and Mazur, *J. Inst. Math. Jussieu* **1** (2002), no. 1, 125-143.

[Ta 03] Taylor, R.: On icosahedral Artin representations. II, *Amer. J. Math.* **125** (2003), no. 3, 549-566.

[Ta] Taylor, R.: On the meromorphic continuation of degree two L-functions, preprint disponible a: http://abel.math.harvard.edu/∼rtaylor/.

L. Dieulefait, N. Vila
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les corts Catalanes 585, E-08007 Barcelona,
ldieulefait@ub.edu, nuriavila@ub.edu

Capítol 7

Alguns casos resolts de la conjectura de Serre

Julio Fernández

En aquest capítol presentem alguns dels resultats apareguts fins ara en relació a la versió feble de la conjectura de Serre sobre la modularitat d'una representació

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_q)$$

senar i absolutament irreductible, on $G_{\mathbb{Q}}$ i $\mathbb{F}_q$ designen, respectivament, el grup de Galois absolut de $\mathbb{Q}$ i el cos finit de q elements. Per raons d'ús posterior, notem d'entrada que, si q és senar, la irreductibilitat absoluta de la representació (senar) ρ equival simplement a la seva irreductibilitat (cf. Lemma 5 de [Ru 97]).

Després de revisar com es dedueix la modularitat de ρ per a $q = 3$ a partir dels resultats de Langlands i Tunnell que completen la demostració de la conjectura d'Artin en el cas resoluble, tractem tres altres casos de la conjectura de Serre per a valors de q *petits* que han estat abordats en els darrers anys. Concretament, passem revista a una part dels treballs [ST 97], [Ma 01] i [Ell 02], en els quals es demostra la conjectura per a $q = 5$, $q = 7$ i $q = 9$, respectivament, sempre sota certes condicions locals imposades a la representació ρ.

El *leitmotif* general d'aquests tres treballs és *fer ús de la geometria*, i ho és en un sentit doble. D'una banda, la tàctica emprada per demostrar la modularitat de ρ consisteix a realitzar aquesta representació a partir de l'acció de Galois sobre la torsió d'alguna varietat abeliana: una corba el·líptica definida sobre $\mathbb{Q}$ en el cas $q = 5$, una corba el·líptica definida sobre un cos de nombres totalment real i resoluble en el cas $q = 7$, i una superfície abeliana amb multiplicació real (RM) sobre un cos de nombres totalment real i resoluble en el cas $q = 9$. D'una altra banda, això s'assoleix trobant punts racionals en certs espais de moduli associats a la representació ρ. Al cas el·líptic, que és el que veurem amb una mica de detall, aquests espais de moduli són *corbes torçades*, o *twists*, de la corba modular $X(p)$.

Aquesta aproximació geomètrica al problema ve motivada pel coneixement que es té de les representacions de Galois p-àdiques associades als mòduls de Tate d'una varietat abeliana, així com per la *bona propagació* de la modularitat entre elles. En tots tres casos, l'*espurna* de la modularitat prové sempre dels resultats de Langlands i Tunnell aplicats a una representació de Galois 2-dimensional sobre $\mathbb{F}_3$.

Hem dividit el capítol en cinc seccions. La Secció 7.1 recull els ingredients de la modularitat de representacions galoisianes que necessitem per a la resta del capítol. La Secció 7.2 tracta el cas bàsic $q = 3$ de la conjectura, mentre que la Secció 7.3 és un interludi geomètric sobre certs models racionals de la corba modular $X(p)$ amb una aplicació directa al cas $q = 5$. Finalment, les Seccions 7.4 i 7.5 estan dedicades, respectivament, als casos $q = 7$ i $q = 9$.

7.1 Representacions p-àdiques i mòdul p

Fixem d'ara endavant un primer senar p. En aquesta secció repassem el concepte de modularitat per a representacions de Galois 2-dimensionals p-àdiques i mòdul p. Enunciem també dos resultats que són fonamentals per a les dues darreres seccions del capítol. El primer, degut essencialment a Ramakrishna, és un teorema d'existència de *bons* aixecaments p-àdics per a una representació mòdul p de $G_{\mathbb{Q}}$ *de tipus ordinari en p*. El segon, degut a Skinner i Wiles, tracta la *propagació* de la modularitat entre representacions p-àdiques, també sota certes condicions de tipus ordinari en p.

Per una *representació mòdul p* entenem un morfisme continu (d'un subgrup) de $G_{\mathbb{Q}}$ en el grup de matrius $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$, on $\overline{\mathbb{F}}_p$ designa una clausura algebraica del cos finit de p elements. La continuïtat del morfisme equival en aquest cas a demanar que tingui imatge finita; en particular, la representació només ramifica en un nombre finit de primers. La conjectura de Serre prediu la modularitat de tota representació mòdul p

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

senar i irreductible. El camí que sovint es pren per abordar aquesta conjectura consisteix a intentar demostrar la modularitat d'un aixecament p-àdic qualsevol de ρ.

Per una *representació p-àdica* entenem un morfisme continu (d'un subgrup) de $G_{\mathbb{Q}}$ en el grup de matrius $\mathrm{GL}_2(\overline{\mathbb{Q}}_p)$, on $\overline{\mathbb{Q}}_p$ designa una clausura algebraica de $\mathbb{Q}_p$. Sempre suposem, a més, que la representació només ramifica en un nombre finit de primers. De la seva continuïtat, se'n dedueix que, mòdul conjugació, té imatge a $\mathrm{GL}_2(\overline{\mathbb{Z}}_p)$, on $\overline{\mathbb{Z}}_p$ és l'anell d'enters de $\overline{\mathbb{Q}}_p$. Si denotem per $\mathcal{P}$ l'ideal maximal de $\overline{\mathbb{Z}}_p$, el cos residual $\overline{\mathbb{Z}}_p/\mathcal{P}$ s'identifica amb $\overline{\mathbb{F}}_p$. Així doncs, una representació p-àdica

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$$

dóna lloc a una (única, mòdul conjugació) representació mòdul p

$$\overline{\phi} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p).$$

Diem que ϕ és un *aixecament p-àdic* de ρ, i també que ρ és la *reducció mòdul p* de ϕ, si $\overline{\phi} = \rho$. El mateix concepte es pot estendre a representacions p-àdiques i mòdul p de dimensió n qualsevol. El següent teorema és una adaptació deguda a Taylor [Ta 03] d'un resultat de Ramakrishna [Ra 02] sobre deformacions de representacions mòdul p. Denotem per χ_p el caràcter p-àdic donat per l'acció galoisiana sobre les arrels de la unitat de $\overline{\mathbb{Q}}$ d'ordre potència de p.

7.1.1 Teorema. *Sigui* $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{p^r})$ *una representació senar amb imatge no-resoluble i tal que*

$$\rho_{|D_p} \;\sim\; \begin{pmatrix} \overline{\chi}_p\,\varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix},$$

amb $\overline{\chi}_p\,\varepsilon_1 \neq \varepsilon_2$*. Sigui* $W(\mathbb{F}_{p^r})$ *l'anell de vectors de Witt de* $\mathbb{F}_{p^r}$*. Aleshores, existeix un aixecament* p*-àdic*

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2\left(W(\mathbb{F}_{p^r})\right)$$

de ρ *tal que el caràcter* $(\det\phi)\,\chi_p^{-1}$ *té ordre finit i tal que*

$$\phi_{|D_p} \;\sim\; \begin{pmatrix} \chi_p\,\psi_1 & * \\ 0 & \psi_2 \end{pmatrix},$$

on ψ_i *és un aixecament* p*-àdic moderadament ramificat de* ε_i*.*

7.1.2 Remarca. Donat que el subgrup de matrius triangulars superiors de $\mathrm{GL}_2(\mathbb{F}_{p^r})$ és resoluble, la irreductibilitat de ρ ve garantida per la hipòtesi de no-resolubilitat de la seva imatge.

Del concepte de modularitat introduït al Capítol 2, en revisem ara tant la seva formulació *à la Deligne-Serre*, que fa ús de formes modulars de pes arbitrari (no necessàriament 2), com la seva formulació *à la Shimura*, de caire més geomètric. Una representació p-àdica irreductible

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$$

és *modular* si se satisfan les dues condicions equivalents següents:

- Existeix una forma (parabòlica) de Hecke g (per a algun pes, algun nivell i algun caràcter) tal que

  $$\mathrm{tr}\,\phi\,(\mathrm{Frob}_l) \;=\; a_l(g)$$

  per a tot primer l llevat d'un nombre finit, on $a_l(g)$ és el valor propi de g per l'operador de Hecke l-èsim.

- Existeix una varietat abeliana modular $A_{/\mathbb{Q}}$ tal que ϕ és (conjugada a) la representació p-àdica $\phi_{A,\mathcal{P}}$ associada a A.

Perquè la primera definició tingui sentit, cal haver fixat per a cada primer l una immersió $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_l$. Quant a la segona definició, recordem que A és la varietat abeliana associada per Shimura a una forma nova f de pes 2. Aquesta varietat abeliana està definida mòdul $\mathbb{Q}$-isogènia, i el seu anell de $\mathbb{Q}$-endomorfismes es pot identificar amb l'anell d'enters $\mathcal{O}$ del cos de nombres de grau $\dim(A)$ generat pels coeficients de Fourier de f. Si abusem de la notació $\mathcal{P}$ per referir-nos també a l'ideal primer de $\mathcal{O}$ donat per la immersio $\overline{\mathbb{Z}} \hookrightarrow \overline{\mathbb{Z}}_p$ i designem per $\mathcal{O}_{\mathcal{P}}$ el completat de $\mathcal{O}$ en $\mathcal{P}$, el mòdul de Tate $T_pA \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathcal{P}}$ té rang 2 sobre $\mathcal{O}_{\mathcal{P}}$ i l'acció de Galois sobre ell dóna lloc a una representació p-àdica

$$\phi_{A,\mathcal{P}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{\mathcal{P}}).$$

Denotem per $\rho_{A,\mathcal{P}}$ la reducció mòdul p de $\phi_{A,\mathcal{P}}$.

Considerem el cas particular en què $\dim(A) = 1$. Gràcies als treballs [Wi 95], [TW 95], [Di 96], [BCDT], avui sabem que la conjectura de Shimura-Taniyama és certa: tota corba el·líptica E definida sobre $\mathbb{Q}$ és modular. En aquest cas, l'àlgebra de $\mathbb{Q}$-endomorfismes és isomorfa a $\mathbb{Z}$, de forma que $\phi_{E,\mathcal{P}}$ és simplement la representació p-àdica

$$\phi_{E,\,p} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$$

associada al mòdul de Tate T_pE. Aquesta representació $\phi_{E,\,p}$ té una importància clau: la seva modularitat (per a un primer p qualsevol) equival a la de la corba el·líptica E.

De forma anàloga al cas p-àdic, es defineix la modularitat d'una representació mòdul p

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

irreductible. Així, ρ és *modular* si se satisfan les dues condicions equivalents següents:

- Existeix una forma de Hecke g tal que

  $$\mathrm{tr}\,\rho\,(\mathrm{Frob}_l) \;=\; a_l(g) \mod \mathcal{P}$$

  per a tot primer l llevat d'un nombre finit.

- Existeix una varietat abeliana modular $A_{/\mathbb{Q}}$ tal que ρ és (conjugada a) la representació mòdul p $\rho_{A,\mathcal{P}}$ associada a A.

Per exemple, la representació

$$\rho_{E,p} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

associada a la p-torsió d'una corba el·líptica E definida sobre $\mathbb{Q}$ és modular: en efecte, $\phi_{E,p}$ és un aixecament p-àdic modular de $\rho_{E,p}$.

Al següent teorema de Skinner i Wiles [SW 01], els conceptes de *senaritat* i *modularitat* per a una representació p-àdica ϕ del grup de Galois absolut d'un cos de nombres F totalment real generalitzen els del cas $F = \mathbb{Q}$. La representació ϕ és *senar* si, per a tota immersió $F \hookrightarrow \mathbb{R}$, la imatge per ϕ de la corresponent conjugació complexa té dos valors propis diferents. La representació ϕ és *modular* si prové d'una forma modular de Hilbert (cf. Capítol 5).

7.1.3 Teorema. *Sigui F un cos de nombres totalment real i siguin ϕ_1, ϕ_2 dues representacions p-àdiques senars del grup de Galois absolut de F. Suposem que les reduccions mòdul p $\overline{\phi}_1, \overline{\phi}_2$ són conjugades i irreductibles, i que tant ϕ_1 com ϕ_2 satisfan les següents condicions:*

(1) *El caràcter $(\det \phi_i)\, \chi_p^{-1}$ té ordre finit.*

(2) *Per a tot primer $\mathfrak{p}$ de F sobre p,*

$$\phi_{i|D_{\mathfrak{p}}} \sim \begin{pmatrix} \gamma_{\mathfrak{p},i} & * \\ 0 & \delta_{\mathfrak{p},i} \end{pmatrix},$$

on el caràcter $\delta_{\mathfrak{p},i}$ és finitament ramificat.

(3) *Per a tot primer $\mathfrak{p}$ de F sobre p, a la condició (2) es pot suposar, a més, que $\overline{\delta}_{\mathfrak{p},1} = \overline{\delta}_{\mathfrak{p},2}$ i que $\overline{\delta}_{\mathfrak{p},i} \neq \overline{\gamma}_{\mathfrak{p},i}$.*

Aleshores, ϕ_1 és modular si i només si ϕ_2 és modular.

7.1.4 Remarca. Si E és una corba el·líptica definida sobre F amb bona reducció potencial ordinària o reducció potencialment multiplicativa a tot primer $\mathfrak{p}$ de F sobre p, aleshores la representació $\phi_{E,p}$ satisfà la condició (2) del Teorema 7.1.3.

7.2 La conjectura de Serre a $\mathrm{GL}_2(\mathbb{F}_3)$

Al mateix article [Se 87] on formula la seva conjectura, Serre estudia el següent cas particular, per al qual verifica l'anomenada versió forta de la conjectura.

7.2.1 Teorema. *Tota representació $\rho : \mathbb{G}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ senar i irreductible és modular.*

DEMOSTRACIÓ: El teorema es prova aixecant ρ a un representació complexa

$$\rho' : \mathbb{G}_Q \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

contínua, senar, irreductible i amb imatge resoluble a $\mathrm{PGL}_2(\mathbb{C})$. La conjectura d'Artin, demostrada en els casos tetraèdric i octaèdric gràcies als treballs de Langlands [La 80] i Tunnell [Tu 81], és certa per a una representació ρ' satisfent aquestes hipòtesis; és a dir, existeix una forma de Hecke g de pes 1 tal que $\operatorname{tr}\rho'(\mathrm{Frob}_l) = a_l(g)$ per a tot primer l llevat d'un nombre finit. La representació ρ' que ens interessa s'obté composant ρ amb la representació fidel de $\mathrm{GL}_2(\mathbb{F}_3)$ en $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}\,])$ definida, per exemple, així:

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \longmapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \longmapsto \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}.$$

La reducció de ρ' mòdul l'ideal primer $(1+\sqrt{-2}\,)$ de norma 3 és precisament ρ, de forma que $\operatorname{tr}\rho = \operatorname{tr}\rho' \bmod (1+\sqrt{-2}\,)$ i la modularitat de ρ' implica la de ρ. Així doncs, només cal comprovar que ρ' satisfà les hipòtesis necessàries per poder aplicar la conjectura d'Artin. Donat que $\det\rho = \det\rho' \bmod 3$, tenim que ρ' és senar perquè ρ ho és. D'altra banda, si ρ' fos reductible, llavors seria la suma directa de dos caràcters i, en particular, la imatge de ρ seria abeliana; pel lema de Schur, això entraria en contradicció amb el fet que ρ és absolutament irreductible. Finalment, la imatge de ρ' és clarament resoluble, perquè $\mathrm{GL}_2(\mathbb{F}_3)$ és una extensió d'índex 2 del grup simètric $\mathcal{S}_4$. $\square$

7.2.2 Remarques. (1) Serre també prova la seva conjectura per a una representació amb imatge $\mathrm{GL}_2(\mathbb{F}_2)$, i fa notar que arguments semblants serveixen per demostrar-la anàlogament per a una representació mòdul p senar amb imatge projectiva diedral.

(2) El Teorema 7.2.1 també és cert per a un cos de nombres totalment real en lloc de $\mathbb{Q}$.

7.3 Twists de la corba modular $X(p)$

En aquesta secció estudiem certs models sobre $\mathbb{Q}$ per a $X(p)$, la corba modular associada al subgrup de congruència $\Gamma(p)$ definit com el nucli de la reducció $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{F}_p)$. Després apliquem un resultat de [ST 97] sobre el cas racional $X(5)$ a la demostració de la conjectura de Serre per a una representació amb imatge a $\mathrm{GL}_2(\mathbb{F}_5)$ i determinant ciclotòmic.

Fixem una representació $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ amb determinant igual al caràcter ciclotòmic $\overline{\chi}_p$. Això equival a fixar un $\mathbb{F}_p[G_{\mathbb{Q}}]$-espai vectorial V_ρ de dimensió 2 juntament amb un $G_{\mathbb{Q}}$-isomorfisme

$$\eta : \wedge^2 V_\rho \longrightarrow \mu_p \,,$$

on μ_p designa el grup de les arrels p-èsimes de la unitat de $\overline{\mathbb{Q}}$. Un exemple típic és el dels punts de p-torsió d'una corba el·líptica E definida sobre $\mathbb{Q}$, amb $G_{\mathbb{Q}}$-isomorfisme

$$e_{E,p} : \wedge^2 E[p] \longrightarrow \mu_p$$

donat per l'aparellament de Weil.

Existeix una corba (llisa, irreductible, no-compacta) $Y_\rho(p)$ definida sobre $\mathbb{Q}$ tal que, per a tot cos K de característica zero, el punts K-racionals de $Y_\rho(p)$ estan en bijecció amb les classes d'isomorfisme de parelles (E, φ), on E és una corba el·líptica definida sobre K i $\varphi : E[p] \longrightarrow V_\rho$ és un G_K-isomorfisme *simplèctic*, és a dir, tal que l'isomorfisme $\wedge^2 E[p] \longrightarrow \wedge^2 V_\rho$ induït per φ fa commutatiu el següent diagrama:

$$
\begin{tikzcd}
\wedge^2 E[p] \arrow[rr, "\varphi"] \arrow[dr, "e_{E,p}"'] & & \wedge^2 V_\rho \arrow[dl, "\eta"] \\
& \mu_p &
\end{tikzcd}
$$

En particular, un punt $\mathbb{Q}$-racional de $Y_\rho(p)$ dóna lloc a una corba el·líptica definida sobre $\mathbb{Q}$ tal que la representació $\rho_{E,p}$ associada als punts de p-torsió de E és conjugada a ρ. Denotem per $X_\rho(p)$ la compactificació de la corba $Y_\rho(p)$. Es tracta d'un model $\mathbb{Q}$-racional de la corba modular $X(p)$.

Denotem per X_p el model *canònic* corresponent al $\mathbb{F}_p[G_\mathbb{Q}]$-espai vectorial $V_p = \mathbb{F}_p \times \mu_p$ amb aparellament $\eta_p : \wedge^2 V_p \longrightarrow \mu_p$ definit per $(1,1) \wedge (0, \zeta_p) \mapsto \zeta_p$, on ζ_p és una arrel p-èsima primitiva de la unitat fixada. Els punts algebraics de X_p estan en bijecció amb les classes d'isomorfisme de parells $(E, [P,Q])$, on $E_{/\overline{\mathbb{Q}}}$ és una corba el·líptica i $[P,Q]$ és una base de la p-torsió de E tal que $e_{E,p}(P \wedge Q) = \zeta_p$. Una bijecció alternativa ve donada pel conjunt de classes d'isomorfisme de tripletes (E, P, C), on $E_{/\overline{\mathbb{Q}}}$ és una corba el·líptica, P és un punt de E d'ordre p i C és un subgrup cíclic de $E[p]$ que no conté P. Un punt $\mathbb{Q}$-racional de X_p dóna lloc a una corba el·líptica E definida sobre $\mathbb{Q}$ tal que

$$\rho_{E,p} \sim \begin{pmatrix} 1 & 0 \\ 0 & \chi_p \end{pmatrix}.$$

Per a $p = 3, 5$, la corba de gènere zero X_p té punts $\mathbb{Q}$-racionals. De fet, el següent resultat ens diu que aquesta és una propietat general per a qualsevol model $X_\rho(p)$ de gènere zero.

7.3.1 Teorema. *Per a $p = 3, 5$, la corba $X_\rho(p)$ és isomorfa a $\mathbb{P}^1$ sobre $\mathbb{Q}$. En particular, existeixen infinites corbes el·líptiques $E_{/\mathbb{Q}}$ tals que $\rho_{E,p}$ és conjugada a ρ.*

Demostració (Idea): Existeix un $G_\mathbb{Q}$-morfisme natural

$$\mathrm{Aut}_{\eta_p}(V_p) \longrightarrow \mathrm{Aut}(X_p),$$

on $\mathrm{Aut}_{\eta_p}(V_p)$ designa el grup de $G_\mathbb{Q}$-automorfismes de V_p que són simplèctics respecte de l'aparellament η_p. Donat qualsevol isomorfisme simplèctic $\varphi : V_p \longrightarrow V_\rho$, l'aplicació

$$\begin{array}{ccc} G_{\mathbb{Q}} & \longrightarrow & \mathrm{Aut}_{\eta_p}(V_p) \\ \sigma & \longmapsto & \varphi^{-1}\, {}^{\sigma}\varphi \end{array}$$

defineix a $H^1\left(G_{\mathbb{Q}}, \mathrm{Aut}(X_p)\right)$ un element ξ_ρ que no depèn de l'isomorfisme φ triat. La corba X_ρ resulta ser el twist de X_p associat a ξ_ρ. Es demostra llavors que ξ_ρ és trivial per a $p = 3, 5$. $\square$

7.3.2 Remarques. (1) El Teorema 7.3.1 es pot enunciar prenent com a cos base un cos de característica zero qualsevol.

(2) La demostració per a $p = 5$ es pot trobar a [ST 97]. L'esbòs de demostració que donem aquí segueix [Ru 97].

(3) La segona part de l'enunciat per a $p = 3$ és un resultat de [LR 95], on els mètodes que es fan servir no són modulars.

7.3.3 Corol·lari. *Si* $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_5)$ *té determinant ciclotòmic, aleshores* ρ *és modular.*

7.3.4 Remarca. A [ST 97] figura una versió més feble del Corol·lari 7.3.3 en què es requereix també una certa condició local en el primer 3, perquè fins llavors només s'havia pogut demostrar la conjectura de Shimura-Taniyama per a corbes el·líptiques sobre $\mathbb{Q}$ semiestables en 3 i en 5.

7.4 La conjectura de Serre a $\mathrm{GL}_2(\mathbb{F}_7)$

El resultat principal de [Ma 01] és el següent:

7.4.1 Teorema. *Sigui* $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_7)$ *una representació senar i irreductible que satisfà les següents condicions:*

- $\rho(I_3)$ *té ordre senar a* $\mathrm{PGL}_2(\mathbb{F}_7)$,
- $\rho_{|D_7} \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$,

- $\det \rho(I_7)$ *té ordre parell.*

Aleshores, ρ *és modular.*

7.4.2 Remarques. (1) Donat que la modularitat de ρ és equivalent a la de qualsevol representació torçada de ρ amb imatge a $\mathrm{GL}_2(\mathbb{F}_7)$, i donat que la primera i la tercera condicions del Teorema 7.4.1 es mantenen per torçament, la segona condició es pot afeblir demanant només que $\rho_{|D_7}$ sigui reductible.

(2) La tercera condició del Teorema 7.4.1 se satisfà, per exemple, si el determinant de ρ és ciclotòmic.

La demostració del Teorema 7.4.1 es pot dividir en tres parts ben diferenciades quant al tipus de resultats que s'utilitzen:

(A) L'existència d'un aixecament

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_7)$$

de ρ *à la Ramakrishna*. Aquest aixecament ϕ s'obté aplicant una variant del Teorema 7.1.1 en què no es requereix la no-resolubilitat de la imatge de ρ. El caràcter $(\det \phi)\, \chi_7^{-1}$ té ordre finit, i se sastisfà

$$\phi_{|D_7} \sim \begin{pmatrix} \chi_7\, \psi_1 & * \\ 0 & \psi_2 \end{pmatrix},$$

on el caràcter ψ_2 és no-ramificat.

(B) La modularitat de la restricció de ϕ al grup de Galois absolut G_F d'un cert cos de nombres F totalment real i resoluble. Notem que la restricció $\rho_{|G_F}$ continua sent senar i irreductible.

(C) La modularitat de ϕ, que s'obté a partir de resultats de canvis de base cíclics de Langlands [La 80] i Khare [Ka 00].

L'article [Ma 01] està consagrat a la part (B) de la demostració. A més del Teorema 7.1.3, l'eina més important que es fa servir és la corba modular X_7 introduïda a la Secció 7.3. Aquesta corba té gènere 3 i no és hiperel·líptica. Per tant, admet un model quàrtic a $\mathbb{P}^2$ donat de forma canònica per les diferencials regulars. Concretament, a [Elk 98] es mostra que un model projectiu pla per a X_7 sobre $\mathbb{Q}$ ve donat per la quàrtica de Klein $X^3Y + Y^3Z + X^3Z = 0$.

Donat un primer p, considerem la reducció $\pi : X_{7/\mathbb{Z}_p} \longrightarrow X_{7/\mathbb{F}_p}$. A [Ma 01] es demostra el resultat que reproduïm a continuació; la seva aplicació en aquelles places on la corba twistada $X_\rho(7)$ admet la quàrtica de Klein com a model local és fonamental per a la demostració del Teorema 7.4.1.

7.4.3 Lema. *Existeix un subconjunt finit S de $X_{7/\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ tal que, si una tripleta $(E_{/\overline{\mathbb{Q}}_p}, P, C)$ representa un punt de $X_{7/\mathbb{Z}_p}(\overline{\mathbb{Q}}_p) \setminus \pi^{-1}(S)$, aleshores la corba el·líptica E té bona reducció ordinària.*

A les places sobre 7 on la corba $X_\rho(7)$ no és (localment) isomorfa a X_7, no es pot aplicar el Lema 7.4.3. Se'n proposa llavors a [Ma 01] la següent versió, corresponent al cas de reducció potencialment multiplicativa.

7.4.4 Lema. *Sigui K una extensió finita de $\mathbb{Q}_7$ i considerem una representació $\rho' \colon G_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_7)$ tal que*

$$\rho' \sim \begin{pmatrix} \overline{\chi}_7 & * \\ 0 & 1 \end{pmatrix}.$$

Fixem per a $X_{\rho'}(7)_{/K}$ un model quàrtic a $\mathbb{P}^2$. Aleshores, existeix una recta $L_{/K}$ a $\mathbb{P}^2$ que talla $X_{\rho'}(7)$ en quatre punts diferents, definits sobre una extensió galoisiana finita K' de K amb índex de ramificació senar, cadascun dels quals correspon a una certa corba el·líptica sobre K' amb reducció potencialment multiplicativa.

La prova de la modularitat de ρ passa per una *bona* realització el·líptica de la restricció de ρ al grup de Galois absolut d'un cert cos de nombres F totalment real i resoluble. Com a primera aproximació a aquest cos de nombres, es comença prenent

$$F' = \overline{\mathbb{Q}}^{\ker(\overline{\chi}_7^{-1}\ \det\rho)}(\zeta_7 + \zeta_7^{-1})$$

i definint ρ' com la restricció de ρ al grup de Galois abolut de F'. Donat que el determinant de ρ' és ciclotòmic, podem considerar la corba twistada $X_{\rho'}(7)$ i un model quàrtic $X_{/F}$ a $\mathbb{P}^2$ per a aquesta corba.

Fent servir llavors els Lemes 7.4.3 i 7.4.4, així com les condicions del Teorema 7.4.1 imposades a la representació ρ, per a tot primer $\mathfrak{q}$ de F' sobre 3 o 7 s'obté l'existència de

- una extensió galoisiana finita $K_{\mathfrak{q}}$ del completat $F'_{\mathfrak{q}}$ amb índex de ramificació senar,
- una recta $L_{\mathfrak{q}}$ a $\mathbb{P}^2$ definida sobre $K_{\mathfrak{q}}$

tals que els quatre punts d'intersecció de $L_{\mathfrak{q}}$ amb $X_{/K_{\mathfrak{q}}}$ corresponen a corbes el·líptiques $E_{/K_{\mathfrak{q}}}$ amb bona reducció ordinària o reducció potencialment multiplicativa i amb 7-torsió simplècticament isomorfa al $G_{K_{\mathfrak{q}}}$-mòdul subjacent a ρ. Quant a les places a l'infinit, existeix també una recta (explícita) L_∞ a $\mathbb{P}^2_{/\mathbb{R}}$ tal que la seva intersecció amb la quàrtica $X_{/\mathbb{R}}$ consta de quatre punts reals diferents.

Tenint en compte que l'espai de rectes de $\mathbb{P}^2$ és una varietat racional, es fa servir llavors un argument de tipus *local-global*, i també d'irreductibilitat de Hilbert, per concloure l'existència d'una extensió totalment real i resoluble F de F' i d'una recta $L_{/F}$ a $\mathbb{P}^2$ que *aproxima* les rectes locals $L_{\mathfrak{q}/K_{\mathfrak{q}}}$ i $L_{\infty/\mathbb{R}}$ en el sentit que la intersecció de L amb $X_{/F}$ dóna lloc a quatre corbes el·líptiques definides sobre F, cadascuna de les quals satisfà les propietats de la següent proposició.

7.4.5 Proposició. *Sigui ρ com al Teorema 7.4.1. Aleshores, existeix una corba el·líptica E definida sobre un cos de nombres F totalment real i resoluble que satisfà les següents propietats:*

(1) *La representació $\rho_{E,3} : G_F \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ és exhaustiva.*

(2) *La corba el·líptica E té bona reducció ordinària en tot primer de F sobre 3.*

(3) *Per a tot primer $\mathfrak{q}$ de F sobre 3,*

$$\rho_{E,3|D_{\mathfrak{q}}} \sim \begin{pmatrix} \overline{\gamma}_{\mathfrak{q}} & * \\ 0 & \overline{\delta}_{\mathfrak{q}} \end{pmatrix},$$

amb $\overline{\gamma}_{\mathfrak{q}} \neq \overline{\delta}_{\mathfrak{q}}$.

(4) *La representació* $\rho_{E,7}$ *és conjugada a* $\rho_{|G_F}$.

(5) *Si* $\rho_{|I_7}$ *descompon en suma directa de dos caràcters, aleshores* E *té bona reducció ordinària en tot primer de* F *sobre* 7.
Si $\rho_{|I_7}$ *no descompon, aleshores* E *té reducció potencialment multiplicativa en tot primer de* F *sobre* 7.

(6) *Per a tot primer* $\mathfrak{p}$ *de* F *sobre* 7,

$$\rho_{E,7_{|I_{\mathfrak{p}}}} \sim \begin{pmatrix} \overline{\gamma}_{\mathfrak{p}} & * \\ 0 & \overline{\delta}_{\mathfrak{p}} \end{pmatrix},$$

amb $\overline{\gamma}_{\mathfrak{p}} \neq \overline{\delta}_{\mathfrak{p}}$.

Finalment, la part (B) de la demostració del Teorema 7.4.1 es dedueix de la Proposició 7.4.5 de la següent forma, que esquematitzem al final d'aquest paràgraf fent servir un diagrama extret de [Ell 02]. Sigui

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_7)$$

un aixecament 7-àdic de ρ *à la Ramakrishna*, i siguin F i E el cos de nombres i la corba el·líptica donats per la proposició. El Teorema 7.2.1 dóna l'existència d'un aixecament 3-àdic modular

$$\phi' : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}}_3)$$

de la representació $\rho_{E,3}$. Per provar que $\phi_{|G_F}$ és modular, s'aplica el Teorema 7.1.3 dues vegades. Primer, a les representacions ϕ' i $\phi_{E,3}$ fent servir les propietats (1), (2) i (3) de la proposició. Després, a les representacions $\phi_{E,7}$ i $\phi_{|G_F}$ fent servir les propietats (4), (5) i (6) de la proposició. La modularitat de $\phi_{E,7}$ es dedueix de la de $\phi_{E,3}$ per compatibilitat de les representacions p-àdiques associades als mòduls de Tate d'una corba el·líptica.

$$\begin{tikzcd}
\phi' \arrow[dr, dotted, "\mathbf{7.2.1}"'] & & \phi_{E,3} \arrow[r, dotted] & \phi_{E,7} \arrow[dr, dotted] & & \phi_{|G_F} \\
& \rho_{E,3} \arrow[ur, dotted, "\mathbf{7.1.3}"] & & & \rho_{E,7} \simeq \rho_{|G_F} \arrow[ur, dotted, "\mathbf{7.1.3}"] &
\end{tikzcd}$$

7.5 La conjectura de Serre a $\mathrm{GL}_2(\mathbb{F}_9)$

El resultat principal de [Ell 02] és el següent:

7.5.1 Teorema. *Sigui* $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_9)$ *una representació senar i amb imatge no-resoluble que satisfà les següents condicions:*

- $\rho_{|D_3} \sim \begin{pmatrix} \gamma & * \\ 0 & \delta \end{pmatrix}$, *amb* $\gamma_{|I_3} = \overline{\chi}_3$ *i* $\delta_{|I_3}$ *trivial,*
- $\rho(I_5)$ *té ordre senar i determinant trivial.*

Aleshores, ρ *és modular.*

La demostració d'aquest teorema es divideix també en les mateixes parts (A), (B) i (C) que el Teorema 7.4.1, essent de nou la part (B) l'essencial de les tres. Aquesta vegada, en lloc d'una realització el·líptica, i donat que $\mathrm{GL}_2(\mathbb{F}_9)$ és isomorf a $\mathrm{GL}_4(\mathbb{F}_3)$, el que es busca és realitzar (alguna restricció convenient de) la representació ρ fent servir l'acció galoisiana sobre la 3-torsió d'una superfície abeliana. Les superfícies abelianes que es fan servir amb aquest propòsit tenen *multiplicació real* (RM), la qual cosa permet obtenir de forma natural representacions de Galois 2-dimensionals associades als seus mòduls de Tate.

De forma més general, es diu que una varietat abeliana A definida sobre un cos de nombres F té RM (sobre F) per un ordre $\mathcal{O}$ d'un cos de nombres K totalment real de grau $\dim(A)$ si existeix una immersió de $\mathcal{O}$ en l'anell d'endomorfismes de A definits sobre F. Per a una tal varietat abeliana, la construcció de la representació p-àdica

$$\phi_{A,\mathcal{P}} : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$$

associada al mòdul de Tate T_pA i a la immersió $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, així com la de la seva reducció mòdul p $\rho_{A,\mathcal{P}}$, és completament anàloga a la del cas d'una varietat abeliana modular sobre $\mathbb{Q}$ (cf. Secció 7.1). A [Ell 02] es demostra que, si A és principalment polaritzada i té bona reducció ordinària o reducció multiplicativa en un primer $\mathfrak{p}$ de F sobre p amb índex de ramificació senar, llavors la representació $\phi_{A,\mathcal{P}}$

satisfà la següent propietat, que forma part de les hipòtesis del Teorema 7.1.3 :

$$\phi_{A,\mathcal{P}|D_\mathfrak{p}} \sim \begin{pmatrix} \gamma_\mathfrak{p} & * \\ 0 & \delta_\mathfrak{p} \end{pmatrix}, \quad \text{amb } \overline{\delta}_\mathfrak{p} \neq \overline{\gamma}_\mathfrak{p}.$$

El següent resultat és l'anàleg a la Proposició 7.4.5 per al cas que estem considerant en aquesta secció. Notem que, si F és un cos de nombres com a l'enunciat, llavors la restricció $\rho' = \rho_{|G_F}$ té determinant ciclotòmic. La superfície abeliana A es troba a [Ell 02] mostrant l'existència de punts F-racionals adients en la superfície modular de Hilbert twistada $X_{\rho'}\big(3, \mathbb{Z}[(1+\sqrt{5}\,)/2]\big)$, els punts no-cuspidals de la qual parametritzen les classes d'isomorfisme de superfícies abelianes principalment polaritzades amb RM per l'ordre $\mathbb{Z}[(1+\sqrt{5}\,)/2]$ i amb un isomorfisme simplèctic de la seva 3-torsió al $\mathbb{F}_3[G_F]$-espai vectorial subjacent a ρ'. D'altra banda, així com a la Secció 7.4 es fan servir twists de la corba modular $X(7)$, la corba el·líptica E de l'enunciat de la proposició es troba en aquest cas fent servir la corba modular twistada $X_{\rho_{A,\sqrt{5}}}(5)$.

7.5.2 Proposició. *Sigui ρ com al Teorema 7.5.1. Aleshores, existeixen un cos de nombres F totalment real i resoluble, una corba el·líptica E definida sobre F i una superfície abeliana $A_{/F}$ principalment polaritzada amb RM sobre F per $\mathbb{Z}[(1+\sqrt{5}\,)/2]$ que satisfan les següents propietats:*

(1) *La representació $\rho_{E,3}$ és irreductible.*

(2) *La corba el·líptica E té reducció multiplicativa en tot primer de F sobre 3 o 5.*

(3) *Per a tot primer $\mathfrak{q}$ de F sobre 3,*

$$\rho_{E,3|I_\mathfrak{q}} \sim \begin{pmatrix} \overline{\chi}_3 & 0 \\ 0 & 1 \end{pmatrix}.$$

(4) *Tot primer de F sobre 3 o 5 té índex de ramificació senar.*

(5) *La representació $\rho_{E,5}$ és exhaustiva i conjugada a $\rho_{A,\sqrt{5}}$.*

(6) *La superfície abeliana A té bona reducció ordinària o reducció multiplicativa en tot primer de F sobre* 3 *o* 5.

(7) *La representació $\rho_{A,3}$ és conjugada a $\rho_{|G_F}$.*

Vegem com obtenir el Teorema 7.5.1 a partir de la Proposició 7.5.2. Sigui

$$\phi : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2\,(W(\mathbb{F}_9))$$

un aixecament 3-àdic de ρ com al Teorema 7.1.1, i siguin F, E i A el cos de nombres, la corba el·líptica i la superfície abeliana donats per la proposició. La modularitat de $\phi_{|G_F}$ es dedueix de la següent forma, que esquematitzem amb un diagrama anàleg al de la Secció 7.4. El Teorema 7.2.1 dóna l'existència d'un aixecament 3-àdic modular ϕ' de la representació $\rho_{E,3}$. Apliquem llavors el Teorema 7.1.3 tres vegades. Primer, a les representacions ϕ' i $\phi_{E,3}$ fent servir les propietats (1), (2) i (3) de la proposició. Després, a les representacions $\phi_{E,5}$ i $\phi_{A,\sqrt{5}}$ fent servir les propietats (4), (5) i (6) de la proposició. Finalment, a les representacions $\phi_{A,3}$ i $\phi_{|G_F}$ fent servir les propietats (6) i (7) de la proposició. De nou, la modularitat de $\phi_{E,5}$ i la de $\phi_{A,3}$ s'obtenen per compatibilitat de les representacions p-àdiques associades als mòduls de Tate.

$$\begin{tikzcd}
\phi' \arrow[dr, dotted, "\mathbf{7.2.1}"'] & & \phi_{E,3} \arrow[r, dotted] & \phi_{E,5} \arrow[dr, dotted] & & \phi_{A,\sqrt{5}} \arrow[r, dotted, no head] & {} \\
& \rho_{E,3} \arrow[ur, dotted, "\mathbf{7.1.3}"] & & & \rho_{E,5} \simeq \rho_{A,\sqrt{5}} \arrow[ur, dotted, "\mathbf{7.1.3}"] & &
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[r, dotted, no head] & \phi_{A,\sqrt{5}} \arrow[r, dotted] & \phi_{A,3} \arrow[dr, dotted] & & \phi_{|G_F} \\
& & & \rho_{A,3} \simeq \rho_{|G_F} \arrow[ur, dotted, "\mathbf{7.1.3}"] &
\end{tikzcd}$$

Tanquem el capítol amb una aplicació d'aquesta secció a la conjectura generalitzada de Shimura-Taniyama inclosa a [Ell 02]. Així com el Teorema 7.2.1 és d'on prové en última instància la modularitat en la prova d'aquesta conjectura per a corbes el·líptiques sobre $\mathbb{Q}$, el Teorema 7.5.1 permet demostrar el següent resultat.

7.5.3 Corol·lari. *Tota superfície abeliana amb RM sobre* $\mathbb{Q}$ *i amb bona reducció ordinària o reducció multiplicativa en* 3 *i* 5 *és modular.*

Bibliografia

[BCDT] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), 843-939.

[Di 96] Diamond, F.: On deformation rings and Hecke rings. *Ann. of Math.* **144** (1996), 137-166.

[Elk 98] Elkies, N. D.: The Klein quartic in Number Theory. *The eightfold way*, 51-101. MSRI Publications **35**, 1998.

[Ell 02] Ellenberg, J.: Serre's conjecture over $\mathbb{F}_9$. *Preprint*, 2002.

[Ka 00] Khare, C.: Mod p descent for Hilbert modular forms. *Math. Res. Lett.* **7** (2000), 455-462.

[La 80] Langlands, R.: Base change for GL(2). *Annals of Math. Studies* **96**, Princeton University Press, Princeton, NJ, 1980.

[LR 95] Lario, J-C., Rio, A.: An octahedral-elliptic type equality in $\mathrm{Br}_2(k)$. *C. R. Acad. Sci. Paris Sér. I Math.*, **321** (1995), no. 1, 39-44.

[Ma 01] Manoharmayum, J.: On the modularity of certain $\mathrm{GL}_2(\mathbb{F}_7)$ Galois representations. *Math. Res. Lett.* **8** (2001), 703-712.

[Ra 02] Ramakrishna, R.: Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. *Ann. of Math.* **156** (2002), 115-154.

[Ru 97] Rubin, K.: Modularity of mod 5 representations. *Modular forms and Fermat's Last Theorem*, Springer-Verlag, New York, 1997.

[Se 87] Serre, J-P.: Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). *Duke Math. J.* **54** (1987), no. 1, 179-230.

[ST 97] Shepherd-Barron, N. I., Taylor, R.: Mod 2 and mod 5 icosahedral representations. *J. Amer. Math. Soc.* **10** (1997), no. 2, 283-298.

[SW 01] Skinner, C., Wiles, A.: Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math.* **10** (2001), no. 1, 185-215.

[Ta 03] Taylor, R.: On icosahedral Artin representations II. *Amer. J. Math.* **125** (2002), no. 3, 549-566.

[TW 95] Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* **141** (1995), 553-572.

[Tu 81] Tunnell, J.: Artin's conjecture for representations of octahedral type. *Bull. Amer. Math. Soc.* **5** (1981), no. 2, 173-175.

[Wi 95] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.* **141** (1995), 443-551.

J. Fernández
Département de Mathématiques
Université de Franche-Comté
16 route de Gray, F-25030 Besançon
julio@math.univ-fcomte.fr
julio.fernandez-gonzalez@upc.es

Capítol 8

La conjectura d'Artin en el cas icosaèdric

Jordi Quer

Aquest capítol conté les transparències presentades a la xerrada del seminari.

Conjectura d'Artin icosaedral

STNB 2004

Conjectura d'Artin

Siguin F un cos de nombres i

$$\rho\colon G_F \to \mathrm{GL}_n(\mathbb{C})$$

una representació contínua (imatge finita). La **conjectura d'Artin** diu que

$$L(\rho, s) \qquad \text{és } \textbf{entera}$$

(excepte si ρ conté la representació trivial, que té un pol a $s = 1$).

La **conjectura forta** (ρ irreductible) diu que ρ és **automorfa**: existeix una representació automorfa cuspidal π de $\mathrm{GL}_n(\mathbb{A}_F)$ tal que

$$L(\rho, s) = L(\pi, s)$$

Resultats coneguts

Si $n = 1$ la conjectura forta és conseqüència de la Teoria de Cossos de Classes.

Si ρ és induida d'una representació 1-dimensional ρ_L de G_L amb L/F finita,

- La conjectura d'Artin és certa $(L(\rho, s) = L(\rho_L, s))$,
- La conjectura forta és certa sempre que L/F és resoluble (canvi de base cíclic).

Si $n = 2$ les representacions irreductibles es classifiquen en tipus segons que

$$\operatorname{Proj} \rho(G_F) \quad \simeq \quad D_{2n}, \quad A_4, \quad S_4, \quad A_5$$

i la conjectura forta està provada per tipus diedral (induida de L/F quadràtica), i per tipus tetraedral (Langlands) i tipus octaedral (Langlands-Tunnell), fent servir que $\rho(G_F)$ és un grup resoluble.
El tipus icosaedral equival a $\rho(G_F)$ no resoluble.

Conjectura d'Artin icosaedral (forta, sobre $\mathbb{Q}$, senar)

Sigui $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ una representació icosaedral senar, o sigui, amb

$$\operatorname{Proj}\rho(G_{\mathbb{Q}}) \simeq A_5 \quad \text{i} \quad \det\rho(c) = -1.$$

Aleshores existeix una forma $f \in S_1^{\mathrm{new}}(\Gamma_1(N))$ tal que $L(\rho, s) = L(f, s)$.

- Depèn només de l'extensió $K/\mathbb{Q}$ fixa pel nucli de $\operatorname{Proj}\rho$, amb $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_5$.
- El teorema de Deligne-Serre associa a cada $f \in S_1^{\mathrm{new}}(\Gamma_1(N))$ una representació ρ_f amb $L(\rho_f, s) = L(f, s)$. Per tant la conjectura d'Artin és el recíproc.
- El teorema de Weil redueix la conjectura d'Artin forta a la prolongació analítica.

Resultats: exemples particulars vía computació numèrica

- **Buhler (1978)** Un exemple, amb conductor $N = 800$,
- **Frey et al. (1994)** Set exemples, de conductors

$$2083, \quad 2^2 \cdot 487, \quad 2^2 \cdot 751, \quad 2^2 \cdot 887, \quad 2^2 \cdot 919, \quad 2^5 \cdot 73, \quad 2^5 \cdot 193,$$

- **Jehanne-Müller (2000)** Un exemple, amb conductor $N = 5203 = 11^2 \cdot 43$.
- **Buzzard-Stein (2002)** Vuit exemples, de conductors

$$2^5{\cdot}43, \quad 2^4{\cdot}151, \quad 2^4{\cdot}199, \quad 2^2{\cdot}7{\cdot}127, \quad 2^2{\cdot}3{\cdot}313, \quad 2^2{\cdot}13{\cdot}79, \quad 2^6{\cdot}67, \quad 3^3{\cdot}199,$$

Mètode de Buhler (LNM 654) i Frey et al. (LNM 1585)

1) Es calcula $\dim S_1^{\mathrm{new}}(\Gamma_1(N))$ vía

$$f \mapsto (f \cdot 2E_p, f \cdot \theta_2^8)\colon \qquad S_1(N,\varepsilon) \to S_2(N,\varepsilon\chi_{-p}) \times S_5(N,\varepsilon)$$

on $E_p \in M_1(N,\chi_{-p})$ i $\theta_2^8 \in M_4(N,1)$ amb imatge formada pels parells (f_1, f_2) de $S_2(N,\varepsilon\chi_{-p}) \times S_5(N,\varepsilon)$ tals que $f_1 \cdot \theta_2^8 = f_2 \cdot 2E_p \in S_6(N,\varepsilon\chi_{-p})$.

2) Es calcula el nombre $d(N)$ de $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ (contínues, irreductibles i senars) de conductor $N_\rho = N$. Per fer-ho cal determinar els conductors de tots els aixecaments lineals d'una projectiva (Kiming) i calcular totes les extensions (no reals) de $\mathbb{Q}$ amb grup de Galois D_{2n}, A_4, S_4, A_5 no ramificades fora dels $p \mid N$.

3) Es comprova que

$$\dim S_1^{\mathrm{new}}(\Gamma_1(N)) = d(N)$$

Mètode de Jehanne-Müller (JNT Bordeaux 2000)

Es calcula $L(\rho, s)$ i es considera la transformada de Mellin $f = \sum a_n q^n$.

Es troben formes $\theta \in S_1(N, \chi)$ (diedral: partir de funcions theta de formes quadràtiques) i $g_1, g_2 \in S_2(N, \chi^2)$ (símbols modulars) tals que

$$\theta f \equiv g_1 \pmod{q^{1+\psi(N)/3}}, \qquad f^2 \equiv g_2 \pmod{q^{1+\psi(N)/3}}$$

La identitat $\theta^2 g_2 \equiv g_1^2 \pmod{q^{\psi(N)/3}}$ a $S_4(N, \chi^4)$ assegura la igualtat com a formes. Aleshores $g = g_1/\theta$ és holomorfa cuspidal ja que $(g_1/\theta)^2 = g_2$ ho és. Per tant,

$$g \in S_1(\Gamma_1(N))$$

Es comprova que ρ_g és icosaedral (simplement mirant els coeficients) i que K és el cos fix de $\operatorname{Proj} \rho_g$ (a partir d'una llista d'extensions icosaedrals). Per tant ρ és un twist de la representació ρ_g de Deligne-Serre.

Resultats: condicions locals

- **Buzzard-Dickinson-Shepherd–Barron-Taylor (2001)** Condicions en 2 i 5:
  1. $\mathrm{Proj}\,\rho$ és no ramificada en 2 i $\mathrm{Proj}\,\rho(\mathrm{Frob}_2)$ té ordre 3, i
  2. $\mathrm{Proj}\,\rho$ és no ramificada en 5

- **Taylor (2003)** Condicions en 3 i 5:
  1. $\mathrm{Proj}\,\rho(I_3)$ té ordre senar, i
  2. $\mathrm{Proj}\,\rho(D_5)$ té ordre 2 i l'homomorfisme $\mathbb{Q}_5^* \to \{\pm 1\}$ envía 5 a -1

- **Goins (2004?)** Familia infinita salvatgement ramificada en 5 dels K

  cos de descomposició de $f(X) = X^5 + BX + C$ amb $75C^2/\sqrt{D_f} \in \mathbb{Q}^* \cap \mathbb{Z}_5^{*2}$

Tots tres resultats s'apliquen a infinites extensions icosaedrals $K/\mathbb{Q}$.

Mètode de demostració d'aquests resultats

Es fixa un primer ℓ i es considera un isomorfisme $\mathbb{C} \simeq \overline{\mathbb{Q}}_\ell$. Llevat d'equivalència la representació $\rho\colon G_\mathbb{Q} \to GL_2(\overline{\mathbb{Q}}_\ell)$ pren valors a l'anell d'enters $\mathcal{O}$ d'una extensió finita de $\mathbb{Q}_\ell$, amb ideal maximal λ i es té una reducció

$$\overline{\rho}\colon G_\mathbb{Q} \to \mathrm{GL}_2(k), \qquad k = \mathcal{O}/\lambda \simeq \mathbb{F}_{\ell^u}$$

Aleshores:

1) Es demostren resultats d'aixecament que asseguren que $\overline{\rho}$ modular $\Rightarrow$ ρ modular (de pes 1). Les formes de pes 1 s'obtenen especialitzant formes Λ-àdiques de Hida.

2) Es demostra la modularitat de la representació residual $\overline{\rho}$. El mètode és sempre el mateix: contagi de la modularitat a través de la família compatible de representacions ℓ-àdiques associades a punts de torsió de varietats abelianes modulars.

Resultats d'aixecament de representacions residuals modulars a representacions d'Artin modulars (de pes 1)

Siguin ℓ un primer, $\mathcal{O}$ l'anell d'enters d'una extensió finita de $\mathbb{Q}_\ell$ amb ideal maximal λ, i $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ una representació contínua. Les condicions següents es demanen sempre:

1) ρ és no ramificada fora d'un conjunt finit de primers,

2) $\overline{\rho}|_{G_M}\colon G_M \to \mathrm{GL}_2(\mathcal{O}/\lambda)$ és absolutament irreductible, on $M = \mathbb{Q}(\sqrt{\ell^*})$ si $\ell \neq 2$ i $M = \mathbb{Q}(i)$ si $\ell = 2$,

3) $\overline{\rho}$ és modular.

afegint certes condicions locals (que sempre inclouen $\rho(I_\ell)$ finit) aleshores s'assegura que ρ és modular de pes 1, o sigui, que $L(\rho, s) \sim L(f, s)$ per una forma $f \in S_1^{\mathrm{new}}(\Gamma_1(N))$. En particular, això prova que ρ té imatge finita (conjectura de Fontaine-Mazur).

Representacions no ramificades amb $\ell \geqslant 5$

Teorema (Buzzard-Taylor, *Companion forms and weight one forms*, Ann. of Math., 1999) Per primers $\ell \geqslant 5$ amb condició en ℓ

4) ρ és no ramificada en ℓ i $\rho(\mathrm{Frob}_\ell)$ té valors propis diferents mòdul λ.

Extensió al cas $\ell = 2$

Teorema (Buzzard-Dickinson-Shepherd–Barron-Taylor, *On icosahedral Artin representations*, Duke Math. J., 2001) Pel primer $\ell = 2$ amb condicions

4) $\overline{\rho}(G_{\mathbb{Q}}) \simeq \mathrm{SL}_2(\mathbb{F}_4) \quad (\simeq A_5)$,

5) $\overline{\rho}(c) \neq 1$,

6) $\overline{\rho}$ és no ramificada en 5,

7) ρ és no ramificada en 2 i $\rho(\mathrm{Frob}_2)$ té valors propis diferents mòdul λ,

Generalització a representacions moderadament ramificades en ℓ

Teorema (Buzzard, *Analytic continuation of overconvergent eigenforms*, J. Amer. Math. Soc., 2003) Tots els primers amb

4) $\rho|_{D_\ell} \simeq \alpha \oplus \beta$ amb $\alpha(I_\ell), \beta(I_\ell)$ caràcters d'ordre finit amb $\alpha \not\equiv \beta \pmod{\lambda}$.

i, si $\ell = 2$, suposi's a més que $\overline{\rho}(c) \neq 1$, que $\mathrm{Proj}\,\overline{\rho}$ no és un grup diedral i que

5) $\overline{\rho}$ és doblement modular provinent de $\overline{f}_\alpha$ i de $\overline{f}_\beta$

Generalització a representacions salvatgement ramificades en ℓ

Teorema (Goins, *On the modularity of wildly ramified galois representations*, preprint) Per $\ell \neq 2$. Si

4) $\overline{\rho}$ és salvatgement ramificada en ℓ,

5) $\rho(D_\ell)$ és finit i $\mathrm{Proj}\,\rho(D_\ell)$ és cíclic d'ordre potència de ℓ.

Idea de la demostració

Formes modulars de Hida. $\Lambda = \mathcal{O}[[X]]$, $\varphi_k \colon \Lambda \to \mathcal{O}$, $\varphi_k(A(X)) = A((1+\ell)^k - 1)$,

$$F = \sum A_n(X) q^n \quad \text{tal que} \quad \varphi_k(F) = \sum \varphi_k(A_n(X)) q^n \in S_k(\Gamma_1(N))$$

per gairebé tot $k \geqslant 1$. Les especialitzacions de formes de Hida són formes modulars ℓ-àdiques "overconvergents" i s'interprenten en termes de geometria rígida sobre la corba modular $X_1(N)$.

1) Utilitzant (i generalitzant) resultats de Gross es construeixen dues formes modulars $\overline{f}_\alpha, \overline{f}_\beta \in S_2(\Gamma_1(N\ell); \mathcal{O}/\lambda)$ amb $\ell \nmid N$ corresponents a $\overline{\rho}$ amb $U_\ell \overline{f}_\alpha = \overline{\alpha}\overline{f}_\alpha, U_\ell \overline{f}_\beta = \overline{\beta}\overline{f}_\beta$, on α, β són els dos valors propis de $\overline{\rho}(\mathrm{Frob}_\ell)$.

2) Utilitzant i generalitzant Wiles i Diamond s'aixequen a formes Λ-àdiques de Hida F_α, F_β: l'anell de deformació universal és isomorf a una àlgebra de Hecke Λ-àdica.

3) Especialitzant F_α, F_β en pes $k = 1$ s'obtenen formes modulars ℓ-àdiques overconvergents no clàssiques $f_\alpha, f_\beta \in \mathcal{M}_1^{-p/(p+1)}(N)$ tals que

$T_p f_\alpha = \operatorname{Tr} \rho(\operatorname{Frob}_p) f_\alpha, \quad T_p f_\beta = \operatorname{Tr} \rho(\operatorname{Frob}_p) f_\beta$ si $p \nmid N\ell$

$\langle p \rangle f_\alpha = \det \rho(\operatorname{Frob}_p) f_\alpha, \quad \langle p \rangle f_\beta = \det \rho(\operatorname{Frob}_p) f_\beta$ $U_p f_\alpha = U_p f_\beta = 0$ si $p \mid N$,

$U_\ell f_\alpha = \alpha f_\alpha, U_\ell f_\beta = \beta f_\beta$.

4) Aquestes formes s'enganxen per obtenir una forma de pes 1 clàssica

$$f = (\alpha f_\alpha - \beta f_\beta)/(\alpha - \beta) \in S_1^{\mathrm{new}}(\Gamma_1(N); \mathcal{O})$$

(en el cas de Goins és lleugerament diferent, i una mica més fàcil: les formes que surten ja són clàssiques elles mateixes).

Exemples de Buzzard-Stein (Pacific J. Math, 2003)

Donada una representació icosaedral senar $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ amb $K/\mathbb{Q}$ cos fix de $\operatorname{Proj}\rho$, es calculen uns quants $\operatorname{Tr}\rho(\mathrm{Frob}_p)$ i

1) Es busca una forma $f = a_n q^n \in S_5(N_\rho, \varepsilon_\rho)$ a coeficients a $\overline{\mathbb{F}}_5$ tal que a_p coincideixi amb $\operatorname{Tr}\rho(\mathrm{Frob}_p)$ per uns quants primers,

2) Es torça f i s'obté g amb coeficients a $\mathbb{F}_5$, per simplificar calculs,

3) Es demostra que ρ_g és no ramificada en 5,

4) Es demostra que $\operatorname{Proj}\rho_g(G_{\mathbb{Q}}) \simeq A_5$,

5) Es demostra que el cos fix de $\operatorname{Proj}\rho_g$ ha de ser K usant una llista d'extensions icosaedrals de discriminant petit, per tant ρ té una reducció mòdul 5 que és modular,

6) S'aplica Buzzard-Taylor obtenint-se la modularitat de ρ.

Demostracions de modularitat mòdul ℓ per contagi

Donada $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$

1) Es busca una varietat abeliana $A/\mathbb{Q}$ de tipus GL_2 amb $\mathrm{End}_{\mathbb{Q}}(A) \simeq R$ anell d'enters d'un cos de nombres de grau $\dim A$ tal que

$$\overline{\rho} \sim \overline{\rho}_{A,\mathfrak{l}} \qquad \text{corresponent a } A[\mathfrak{l}]$$

per un primer $\mathfrak{l}$ de R de característica ℓ.

2) Per a cada primer $\mathfrak{p}$, de característica p, l'acció de $G_{\mathbb{Q}}$ sobre $A[\mathfrak{p}^n]$ proporciona representacions

$$\rho_{A,\mathfrak{p}}\colon G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_p), \qquad \overline{\rho}_{A,\mathfrak{p}}\colon G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_p).$$

3) Hi ha un primer $\mathfrak{p}_0$ tal que es sap demostrar que $\overline{\rho}_{A,\mathfrak{p}_0}$ és modular (per exemple, amb imatge diedral, A_4 o S_4) i tal que

4) amb tècniques de deformació (Wiles, Taylor-Wiles, Diamond, etc.) es pot demostrar la modularitat de $\rho_{A,\mathfrak{p}_0}$.

5) Aleshores totes les $\rho_{A,\mathfrak{p}}$ són modulars (sistema compatible) i, per tant, ho són

$$\rho_{A,\mathfrak{l}}\colon G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_\ell), \qquad \overline{\rho}_{A,\mathfrak{l}}\colon G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell).$$

Per tant, la varietat A ha de tenir un comportament local prefixat en dos primers:

- en $\mathfrak{p} = \ell$ la representació $\overline{\rho}$ correspon a l'acció sobre $A[\ell]$,

- en $\mathfrak{p} = \mathfrak{p}_0$ l'acció galoisiana sobre $A[\mathfrak{p}_0]$ ha de ser tal que les tècniques conegudes permeten demostrar que és modular i que la deformació corresponent a l'acció sobre el mòdul de Tate $T_{\mathfrak{p}_0}A$ també ho és.

Teorema de Buzzard-Dickinson-Shepherd–Barron-Taylor

Teorema (*On icosahedral Artin representations*, Duke Math. J. 2001).

Sigui $K/\mathbb{Q}$ una extensió amb $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_5$ que no és totalment real, tal que

1) 2 no ramifica a K i $\mathrm{Frob}_2 \in \mathrm{Gal}(K/\mathbb{Q})$ té ordre 3, i

2) 5 no ramifica a K.

Aleshores tota representació $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ tal que $\mathrm{Proj}\,\rho$ té cos fix K és modular.

Mètode: demostrar la modularitat de la reducció $\overline{\rho}$ mòdul 2 i aplicar la generalització a $\ell = 2$, feta al mateix article a partir de resultats de Dickinson, del teorema de Buzzard-Taylor.

Llevat d'equivalència i de twist hi ha una representació $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ amb $\mathcal{O}$ l'anell d'enters d'una extensió finita de $\mathbb{Q}_2$ amb ideal maximal λ tal que $\det\rho$ té ordre potència de 2, ρ és no ramificada en 2 i 5 i $\rho(\mathrm{Frob}_2)$ té ordre 3.

Aleshores la seva reducció $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ satisfà

1) $\overline{\rho}$ té imatge $\mathrm{SL}_2(\mathbb{F}_4) \simeq A_5$,

2) $\overline{\rho}(c) \neq 1$,

3) $\overline{\rho}$ és no ramificada en 5, i

4) ρ és no ramificada en 2 i $\rho(\mathrm{Frob}_2)$ té valors propis diferents α, β mòdul λ.

i aquestes condicions, més la modularitat de $\overline{\rho}$ en el sentit següent,

5) Existeix $f \in S_2(\Gamma_1(N); \mathbb{F}_4)$ tal que $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_p) = a_p$ per $p \nmid 2N$, $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_p) = 0$ per $p \mid N$ i $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_p) = \alpha$ per $p = 2$.

són les de la generalització de Buzzard-Taylor per assegurar la modularitat de ρ.

Modularitat de representacions mòdul 2

Proposició. Sigui $\overline{\rho}\colon GL_2(\mathbb{Q}) \to \mathrm{SL}_2(\mathbb{F}_4)$ no ramificada en 2 tal que $\rho(\mathrm{Frob}_2)$ té valors propis diferents $\alpha, \beta \in \mathbb{F}_4^*$. Aleshores existeix una superficie abeliana $A/\mathbb{Q}$ de tipus GL_2 amb multiplicació per l'anell d'enters de $\mathbb{Q}(\sqrt{5})$ tal que

1) la representació $\overline{\rho}$ és la corresponent a l'acció de $G_{\mathbb{Q}}$ en $A[2] \simeq \mathbb{F}_4^2$,

2) l'acció de $G_{\mathbb{Q}}$ en $A[\sqrt{5}] \simeq \mathbb{F}_5^2$ dona lloc a un epimorfisme $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_5)$.

La conjectura Serre per representacions mòdul 5 amb determinant ciclotòmic garanteix la modularitat per $\overline{\rho}_{A,\sqrt{5}}$.

Aplicant els resultats de Wiles s'obté la modularitat de $\rho_{A,\sqrt{5}}$. Per contagi $\rho_{A,2}$ és modular i per tant $\overline{\rho}_{A,2} \simeq \rho$ també.

La varietat A es construeix demostrant que la superfície de mòduli corresponent té un punt.

Teorema de Taylor

Teorema (*On icosahedral Artin representations II*, Amer. J. Math. 2003).

Si $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ és icosaedral senar tal que

1) $\mathrm{Proj}\,\rho(I_3)$ és d'ordre senar, i

2) $\mathrm{Proj}\,\rho(D_5)$ és d'ordre 2 i l'aplicació corresponent $\mathbb{Q}_5^* \to \{\pm 1\}$ envía 5 a -1

aleshores ρ és modular.

Prova: llevat conjugació es pot considerar $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ amb $\mathcal{O}$ anell d'enters d'una extensió finita de $\mathbb{Q}_5$. Gràcies al teorema de Buzzard (o de Buzzard-Taylor si s'aplica) n'hi ha prou a demostrar que la reducció mòdul 5 és modular. O sigui, que

Si $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ és icosaedral senar tal que

1) $\mathrm{Proj}\,\overline{\rho}(I_3)$ és d'ordre senar, i

2) $\mathrm{Proj}\,\overline{\rho}(D_5)$ és d'ordre 2 i l'aplicació corresponent $\mathbb{Q}_5^* \to \{\pm 1\}$ envía 5 a -1

aleshores $\overline{\rho}$ és modular (Observació: $\det \rho$ no pot ser el caràcter ciclotòmic).

Lema En les condicions anteriors existeixen $F/\mathbb{Q}$ resoluble totalment real i E/F corba el·líptica tal que

1) $\mathbb{Q}(\sqrt{5}) \subseteq F$ i $\sqrt{5}$ descompon completament a F,

2) $\overline{\rho}_{E,5}\colon G_F \to \mathrm{GL}_2(\mathbb{F}_5)$ és equivalent a un twist de $\overline{\rho}|_{G_F}$,

3) $\overline{\rho}_{E,3}\colon G_F \to \mathrm{GL}_2(\mathbb{F}_3)$ és exhaustiva,

4) E té bona reducció ordinaria en 3 i bona reducció ordinaria potencial en 5,

5) Per a tot primer $\mathfrak{p} \mid 3$ és $\overline{\rho}_{E,3}|_{D_{\mathfrak{p}}} \sim \chi_{1,\mathfrak{p}} \oplus \chi_{2,\mathfrak{p}}$ amb $\chi_{1,\mathfrak{p}} \neq \chi_{2,\mathfrak{p}}$.

$\textsc{Prova}$: La obstrucció a la existència d'un lifting de $\mathrm{Proj}\,\overline{\rho}|_{G_{\mathbb{Q}(\sqrt{5})}}: G_{\mathbb{Q}(\sqrt{5})} \to A_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ amb determinant el caràcter ciclotòmic de $\mathbb{Q}(\sqrt{5})$ és un element de

$$H^2(G_{\mathbb{Q}(\sqrt{5})}, \{\pm 1\})$$

que té components trivials a $3, \sqrt{5}$ i les places Arquimedianes, per tant hi ha una extensió biquadràtica totalment real $F_1/\mathbb{Q}$ tal que

1) $\mathbb{Q}(\sqrt{5}) \subset F_1$ i tan 3 com $\sqrt{5}$ descomponen a F_1,

2) Existeix una representació $\widetilde{\rho}$: $G_{F_1} \to \mathrm{GL}_2(\mathbb{F}_5)$ amb determinant ciclotòmic tal que $\mathrm{Proj}\,\widetilde{\rho} = \mathrm{Proj}\,\overline{\rho}|_{F_1}$.

Sigui F_2/F_1 totalment real on $\sqrt{5}$ descompon completament tal que $\widetilde{\rho}$ és trivial a tots els grups de descomposició dels primers de característica 3, i tal que els índexos de ramificació de cada primer per damunt de 3 són senars. Sigui F la clausura galoisiana de F_2.
Aleshores el twist $X_{\widetilde{\rho}}/F$ de la corba modular X_5 té un punt a F amb tal que la 3-torsió de la corba el·líptica corresponent genera una extensió de grau 24.

PROVA del Teorema de Taylor. Siguin F i E com al lema.

1) Automorfa mòdul 3. Com que $\overline{\rho}_{E,3}$ és octaedral, pel teorema de Langlands-Tunnell existeix π''' de $\mathrm{GL}_2(\mathbb{A}_F)$ i una plaça μ del seu cos de coeficients tal que

$$\overline{\rho}_{E,3} \sim \overline{\rho}_{\pi''',\mu}$$

2) Aixecament a automorfa 3-àdica. Aplicant els teoremes d'aixecament de Skinner-Wiles a la representació $\rho_{E,3}$ existeix π'' de $\mathrm{GL}_2(\mathbb{A}_F)$ amb cos de coeficients $\mathbb{Q}$ tal que

$$\rho_{E,3} \simeq \rho_{\pi'',3}$$

3) Contagi a automorfa ℓ-àdica. Aleshores per a tot primer racional ℓ, en particular per $\ell = 5$, és

$$\rho_{E,\ell} \sim \rho_{\pi'',\ell}$$

4) Reducció mòdul 5. Torçant π'' (per passar de $\overline{\rho}_{E,5}$ a $\overline{\rho}$) s'obté π' de $\mathrm{GL}_2(\mathbb{A}_F)$ i una plaça λ' del seu cos de coeficients, de característica residual 5 tal que

$$\overline{\rho} \sim \overline{\rho}_{\pi',\lambda'}$$

5) Deformació de Ramakrishna. Existeix una representació contínua $\rho' \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_5^*)$ tal que

- $\overline{\rho}' \sim \overline{\rho}$,
- $\rho'|_{D_5} \sim \begin{pmatrix} \chi_1\varepsilon_5 & * \\ 0 & \chi_2 \end{pmatrix}$ amb χ_1, χ_2 caràcters d'ordre finit moderadament ramificats.

6) Aixecament a automorfa 5-àdica. Aplicant els teoremes d'aixecament de Skinner-Wiles existeix π de $\mathrm{GL}_2(\mathbb{A}_F)$ i un plaça λ del seu cos de coeficients tal que

$$\rho'|_{G_F} \sim \rho_{\pi,\lambda}$$

7) Canvi de base. Aplicant canvi de base cíclic a una cadena $F = F_1 \supset F_2 \supset F_3 \supset \cdots \supset F_n = \mathbb{Q}$ s'obtenen π_i de $\mathrm{GL}_2(\mathbb{A}_{F_i})$ tals que

$$\rho'|_{G_{F_i}} \sim \rho_{\pi_i,\lambda_i}$$

El cas $i = n$ assegura que ρ' és automorfa i, per tant, $\overline{\rho}' \sim \overline{\rho}$ és modular.

Teorema de Goins

Teorema. Sigui $K/\mathbb{Q}$ el cos de descomposició d'un polinomi $f(X) = X^5 + BX + C$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_5$ i

$$75C^2/\sqrt{D_f} \in \mathbb{Q}^* \cap \mathbb{Z}_5^{*2}$$

Aleshores tota representació $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ que tingui K com a cos fix de $\mathrm{Proj}\,\rho$ és modular.

$\textsc{Prova}$: es construeix una $\mathbb{Q}$-corba quadràtica E de grau 2 sobre $\mathbb{Q}(\sqrt{5})$ amb

$$\overline{\rho}_{E,\sqrt{5}} \simeq \overline{\rho}$$

que és modular (Ellenberg-Skinner, per contagi de $\overline{\rho}_{E,3}$).

Es comprova que la representació $\overline{\rho}$ satisfà les condicions del teorema de Goins sobre aixecament de representacions icosaedrals senars.

Proposició. Per a cada $t \in \mathbb{Q}^*$ es consideren

$$q_t(X) = X^5 + \frac{9-5t^2}{t^2}X + \frac{4(9-5t^2)}{5t^2}, \qquad E_t\colon Y^2 = X^3 + 2X^2 + \frac{3+t\sqrt{5}}{2t\sqrt{5}}$$

i sigui $K/\mathbb{Q}$ el cos de descomposició de $q_t(X)$. Aleshores:

1) $\mathrm{Gal}(K/\mathbb{Q}) \subseteq A_5$, amb igualtat si $t \in \mathbb{Q}^{*2}$,

2) si $t \in \mathbb{Z}_5^{*2}$ aleshores $D_5 = I_5 = I_5^w \simeq C_5$,

3) E_t és una $\mathbb{Q}$-corba de grau 2 amb isogènia definida sobre $\mathbb{Q}(\sqrt{5}, \sqrt{-2})$,

4) per a tota quíntica $X^5 + AX + B$ amb $t = 75C^2/\sqrt{\mathrm{Disc}}$, en particular $q_t(X)$, el seu cos de descomposició és el cos $\mathbb{Q}(\{P + 2P\})$ per $P \in E_t[5]$.

Teorema (Ellenberg-Skinner). Les $\mathbb{Q}$-corbes E_t són modulars.