Representacions de Galois sobre cossos de mòduli i punts racionals en corbes de Shimura

Carlos de Vera, Víctor Rotger

Departament de Matemàtica Aplicada 2, UPC

STNB 2012
24 de gener

Índex

Corbes de Shimura

B_D àlgebra de quaternions racional i indefinida de discriminant $D > 1$, $\mathcal{O}_D \subseteq B_D$ un ordre maximal. $X_D/\mathbb{Q}$ model canònic de la corba de Shimura associada.

Corbes de Shimura

B_D àlgebra de quaternions racional i indefinida de discriminant $D > 1$, $\mathcal{O}_D \subseteq B_D$ un ordre maximal. $X_D/\mathbb{Q}$ model canònic de la corba de Shimura associada.

- Les corbes X_D generalitzen les corbes modulars clàssiques, que s'obtenen amb $B_D = \mathrm{M}_2(\mathbb{Q})$.

Corbes de Shimura

B_D àlgebra de quaternions racional i indefinida de discriminant $D > 1$, $\mathcal{O}_D \subseteq B_D$ un ordre maximal. $X_D/\mathbb{Q}$ model canònic de la corba de Shimura associada.

- Les corbes X_D generalitzen les corbes modulars clàssiques, que s'obtenen amb $B_D = \mathrm{M}_2(\mathbb{Q})$.
- X_D és solució (*grollera*) al problema de mòduli sobre $\mathbb{Q}$ de classificar parells $(A, \iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A))$, on
  - A superfície abeliana polaritzada,
  - $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ monomorfisme d'anells.

Corbes de Shimura

B_D àlgebra de quaternions racional i indefinida de discriminant $D > 1$, $\mathcal{O}_D \subseteq B_D$ un ordre maximal. $X_D/\mathbb{Q}$ model canònic de la corba de Shimura associada.

- ▷ Les corbes X_D generalitzen les corbes modulars clàssiques, que s'obtenen amb $B_D = \mathrm{M}_2(\mathbb{Q})$.
- ▷ X_D és solució (*grollera*) al problema de mòduli sobre $\mathbb{Q}$ de classificar parells $(A, \iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A))$, on
  - A superfície abeliana polaritzada,
  - $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ monomorfisme d'anells.

  $\rightsquigarrow$ Si $\mathrm{char}(k) = 0$, un punt $P \in X_D(k)$ correspon a la classe d'isomorfisme $[(A, \iota)]$ d'un parell $(A, \iota)/\bar{k}$ que no necessàriament admet un model racional sobre k.

Punts racionals en X_D

(alguns) Antecedents en l'estudi de punts racionals:

- Shimura (1975): $X_D(\mathbb{R}) = \emptyset$ ($\Rightarrow X_D(\mathbb{Q}) = \emptyset$);
- Jordan-Livné (1985): $X_D(L)$, $L/\mathbb{Q}_p$ finita;
- Jordan (1986), Skorobogatov (2005): $X_D(K)$, K quadràtic imaginari.

Punts racionals en X_D

(alguns) Antecedents en l'estudi de punts racionals:

- Shimura (1975): $X_D(\mathbb{R}) = \emptyset$ ($\Rightarrow X_D(\mathbb{Q}) = \emptyset$);
- Jordan-Livné (1985): $X_D(L)$, $L/\mathbb{Q}_p$ finita;
- Jordan (1986), Skorobogatov (2005): $X_D(K)$, K quadràtic imaginari.

Teorema (Jordan, 1986)

Un parell (A, ι) corresponent a un punt $P \in X_D(k)$ admet un model sobre k si, i només si, $B_D \otimes_{\mathbb{Q}} k \simeq \mathrm{M}_2(k)$.

Punts racionals en X_D

(alguns) Antecedents en l'estudi de punts racionals:

- Shimura (1975): $X_D(\mathbb{R}) = \emptyset$ ($\Rightarrow X_D(\mathbb{Q}) = \emptyset$);
- Jordan-Livné (1985): $X_D(L)$, $L/\mathbb{Q}_p$ finita;
- Jordan (1986), Skorobogatov (2005): $X_D(K)$, K quadràtic imaginari.

Teorema (Jordan, 1986)

Un parell (A, ι) corresponent a un punt $P \in X_D(k)$ admet un model sobre k si, i només si, $B_D \otimes_{\mathbb{Q}} k \simeq \mathrm{M}_2(k)$.

- Per a K quadràtic imaginari amb $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, Jordan (1986) dóna condicions suficients explícites perquè $X_D(K) = \emptyset$.
- Skorobogatov (2005): els exemples de Jordan estan explicats per l'obstrucció de Brauer-Manin.

Representacions de Galois

Jordan explota l'estudi de les representacions de Galois associades als parells (A, ι) parametritzats per X_D:

- Suposem $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, $P = [(A, \iota)] \in X_D(K)$, $(A, \iota)/K$.

Representacions de Galois

Jordan explota l'estudi de les representacions de Galois associades als parells (A, ι) parametritzats per X_D:

- Suposem $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, $P = [(A, \iota)] \in X_D(K)$, $(A, \iota)/K$.
- L'acció de $G_K = \mathrm{Gal}\,(\bar{K}/K)$ en $T_p(A)$ i $A[p]$ indueix representacions

$$\varrho_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)), \quad \bar{\varrho}_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A[p])$$

Representacions de Galois

Jordan explota l'estudi de les representacions de Galois associades als parells (A, ι) parametritzats per X_D:

- Suposem $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, $P = [(A, \iota)] \in X_D(K)$, $(A, \iota)/K$.
- L'acció de $G_K = \mathrm{Gal}(\bar{K}/K)$ en $T_p(A)$ i $A[p]$ indueix representacions

$$\varrho_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)), \quad \bar{\varrho}_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A[p])$$

- Si $p \mid D$, $A[p]$ conté un únic $\mathcal{O}_D$-submòdul propi no trivial C_p, isomorf a $\mathbb{F}_{p^2}$, que proporciona una representació

$$\alpha_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

Representacions de Galois

Jordan explota l'estudi de les representacions de Galois associades als parells (A, ι) parametritzats per X_D:

- Suposem $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, $P = [(A, \iota)] \in X_D(K)$, $(A, \iota)/K$.
- L'acció de $G_K = \mathrm{Gal}(\bar{K}/K)$ en $T_p(A)$ i $A[p]$ indueix representacions

$$\varrho_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)), \quad \bar{\varrho}_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A[p])$$

- Si $p \mid D$, $A[p]$ conté un únic $\mathcal{O}_D$-submòdul propi no trivial C_p, isomorf a $\mathbb{F}_{p^2}$, que proporciona una representació

$$\alpha_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

Skorobogatov relaciona $\alpha_{(A,\iota),p}$ amb un recobridor étale de $Y_{D,p} \to X_D$ al qual aplica tècniques de descens.

Representacions de Galois

Jordan explota l'estudi de les representacions de Galois associades als parells (A, ι) parametritzats per X_D:

- Suposem $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$, $P = [(A, \iota)] \in X_D(K)$, $(A, \iota)/K$.
- L'acció de $G_K = \mathrm{Gal}(\bar{K}/K)$ en $T_p(A)$ i $A[p]$ indueix representacions

$$\varrho_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)), \quad \bar{\varrho}_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A[p])$$

- Si $p \mid D$, $A[p]$ conté un únic $\mathcal{O}_D$-submòdul propi no trivial C_p, isomorf a $\mathbb{F}_{p^2}$, que proporciona una representació

$$\alpha_{(A,\iota),p} : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

Skorobogatov relaciona $\alpha_{(A,\iota),p}$ amb un recobridor étale de $Y_{D,p} \to X_D$ al qual aplica tècniques de descens.

Objectiu

Suposem K imaginari quadràtic.

- L'absència o no de punts K-racionals en X_D no sembla que hagi d'estar relacionada amb el fet que K escindeixi B_D o no.
- A més, es conjectura que $X_D(K) = \emptyset$ si $D, \mathrm{disc}(K) \gg 0$.

Objectiu

Suposem K imaginari quadràtic.

- L'absència o no de punts K-racionals en X_D no sembla que hagi d'estar relacionada amb el fet que K escindeixi B_D o no.
- A més, es conjectura que $X_D(K) = \emptyset$ si $D, \operatorname{disc}(K) \gg 0$.

Seguint una idea d'Ellenberg i Skinner, podem eliminar la hipòtesi $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$:

- A un $P = [(A, \iota)] \in X_D(K)$ li podem associar representacions de G_K, independentment de si (A, ι) admet un model racional sobre K o no.

Objectiu

Suposem K imaginari quadràtic.

- L'absència o no de punts K-racionals en X_D no sembla que hagi d'estar relacionada amb el fet que K escindeixi B_D o no.
- A més, es conjectura que $X_D(K) = \emptyset$ si $D, \mathrm{disc}(K) \gg 0$.

Seguint una idea d'Ellenberg i Skinner, podem eliminar la hipòtesi $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$:

- A un $P = [(A, \iota)] \in X_D(K)$ li podem associar representacions de G_K, independentment de si (A, ι) admet un model racional sobre K o no.

$\rightsquigarrow$ Podem donar condicions suficients per tal que $X_D(K) = \emptyset$.
$\rightsquigarrow$ Amb el mateix mètode també podem donar condicions suficients per l'absència de punts $\mathbb{Q}$-racionals en quocients d'Atkin-Lehner de X_D.

Ellenberg, Skinner i les $\mathbb{Q}$-corbes

▷ K cos de nombres, E/K una $\mathbb{Q}$-corba: corba el·líptica sobre K (sense CM) tal que per a tot $\sigma \in G_{\mathbb{Q}}$ existeix una isogènia $\mu_\sigma : {}^\sigma E \to E$.

Ellenberg, Skinner i les $\mathbb{Q}$-corbes

- K cos de nombres, E/K una $\mathbb{Q}$-corba: corba el·líptica sobre K (sense CM) tal que per a tot $\sigma \in G_{\mathbb{Q}}$ existeix una isogènia $\mu_\sigma : {}^\sigma E \to E$.
- La classe $[c_E] \in \mathrm{H}^2(G_{\mathbb{Q}}, \bar{\mathbb{Q}}^\times)$ definida pel 2-cocicle

$$c_E(\sigma,\tau) = \mu_\sigma \cdot {}^\sigma\mu_\tau \cdot \mu_{\sigma\tau}^{-1} \in (\mathrm{Hom}(E,E)\otimes\mathbb{Q})^\times = \mathbb{Q}^\times.$$

és trivial (Tate). Existeix $\alpha : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^\times$ contínua tal que

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

Ellenberg, Skinner i les $\mathbb{Q}$-corbes

- K cos de nombres, E/K una $\mathbb{Q}$-corba: corba el·líptica sobre K (sense CM) tal que per a tot $\sigma \in G_{\mathbb{Q}}$ existeix una isogènia $\mu_\sigma : {}^\sigma E \to E$.
- La classe $[c_E] \in \mathrm{H}^2(G_{\mathbb{Q}}, \bar{\mathbb{Q}}^\times)$ definida pel 2-cocicle

$$c_E(\sigma,\tau) = \mu_\sigma \cdot {}^\sigma\mu_\tau \cdot \mu_{\sigma\tau}^{-1} \in (\mathrm{Hom}(E,E)\otimes\mathbb{Q})^\times = \mathbb{Q}^\times.$$

és trivial (Tate). Existeix $\alpha : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^\times$ contínua tal que

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

- La representació $\phi_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ de G_K en $T_p(E)$ es pot estendre mitjançant

$$\rho_{E,p}(\sigma)(1\otimes x) = \alpha(\sigma)^{-1} \otimes \mu_\sigma({}^\sigma x)$$

a una representació $\rho_{E,p} : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}_p^\times\, \mathrm{GL}_2(\mathbb{Q}_p)$, i $\mathbb{P}\rho_{E,p|G_K} = \mathbb{P}\phi_{E,p}$.

Representacions de Galois associades a varietats abelianes

- A varietat abeliana polaritzada definida sobre L/k.
- R una $\mathbb{Z}$-àlgebra finita, $i : R \hookrightarrow \mathrm{End}(A)$.

Representacions de Galois associades a varietats abelianes

- A varietat abeliana polaritzada definida sobre L/k.
- R una $\mathbb{Z}$-àlgebra finita, $i : R \hookrightarrow \mathrm{End}(A)$.
- Definim

$$C_R(A) := \{\varphi \in \mathrm{End}^0(A) : \varphi \circ i(r) = i(r) \circ \varphi \quad \forall\, r \in R\},$$

$$C_R(T_p(A)) := \{\varphi \in \mathrm{End}(T_p(A)) : \varphi \circ i(r) = i(r) \circ \varphi \quad \forall\, r \in R\},$$

on $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, i posem també

$$G_p := C_R(A)^\times,\ \bar{G}_p := (C_R(T_p(A))/pC_R(T_p(A)))^\times.$$

Representacions de Galois associades a varietats abelianes

- A varietat abeliana polaritzada definida sobre L/k.
- R una $\mathbb{Z}$-àlgebra finita, $i : R \hookrightarrow \mathrm{End}(A)$.
- Definim

$$C_R(A) := \{\varphi \in \mathrm{End}^0(A) : \varphi \circ i(r) = i(r) \circ \varphi \quad \forall\, r \in R\},$$

$$C_R(T_p(A)) := \{\varphi \in \mathrm{End}(T_p(A)) : \varphi \circ i(r) = i(r) \circ \varphi \quad \forall\, r \in R\},$$

  on $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, i posem també

$$G_p := C_R(A)^\times, \; \bar{G}_p := (C_R(T_p(A))/pC_R(T_p(A)))^\times.$$

- L'acció de $G_L = \mathrm{Gal}\,(\bar{L}/L)$ en $T_p(A)$ i $A[p] = T_p(A)/pT_p(A)$ indueix representacions

$$\varrho_{(A,i),p} : G_L \to G_p, \quad \bar{\varrho}_{(A,i),p} : G_L \to \bar{G}_p.$$

Punts en varietats de Shimura (I)

- R una $\mathbb{Z}$-àlgebra finita amb $R \otimes_{\mathbb{Z}} \mathbb{Q}$ semisimple.
- X l'espai de mòduli parametritzant parells (A, i), amb
  - A varietat abeliana polaritzada de dimensió g,
  - $i : R \hookrightarrow \mathrm{End}(A)$ monomorfisme de $\mathbb{Z}$-àlgebres.

Punts en varietats de Shimura (I)

- R una $\mathbb{Z}$-àlgebra finita amb $R \otimes_{\mathbb{Z}} \mathbb{Q}$ semisimple.
- X l'espai de mòduli parametritzant parells (A, i), amb
  - A varietat abeliana polaritzada de dimensió g,
  - $i : R \hookrightarrow \mathrm{End}(A)$ monomorfisme de $\mathbb{Z}$-àlgebres.
- Teoria de varietats de Shimura de tipus PEL:
  - $\rightsquigarrow$ model canònic $X/\mathbb{Q}$, i $P \in X(\bar{k})$ es correspon a la classe d'isomorfisme $P = [(A, i)]$ d'un parell $(A, i)/\bar{k}$.

Punts en varietats de Shimura (I)

- R una $\mathbb{Z}$-àlgebra finita amb $R \otimes_{\mathbb{Z}} \mathbb{Q}$ semisimple.
- X l'espai de mòduli parametritzant parells (A, i), amb
  - A varietat abeliana polaritzada de dimensió g,
  - $i : R \hookrightarrow \mathrm{End}(A)$ monomorfisme de $\mathbb{Z}$-àlgebres.
- Teoria de varietats de Shimura de tipus PEL:
  - $\rightsquigarrow$ model canònic $X/\mathbb{Q}$, i $P \in X(\bar{k})$ es correspon a la classe d'isomorfisme $P = [(A, i)]$ d'un parell $(A, i)/\bar{k}$.

Definició

$(A, i)/\bar{k}$ admet un model racional sobre L/k si existeix $(A', i')/L$ amb $(A' \times \bar{k}, i' \times \bar{k}) \simeq (A, i)$. En tal cas, L és un cos de definició *per a (A, i). El* cos de mòduli *$k_P = k_{(A,i)}$ de (A, i) és la mínima extensió k_P/k tal que per a tot $s \in G_{k_P}$ hi ha un isomorfisme $f_s : {}^s(A, i) \to (A, i)$.*

Punts en varietats de Shimura (I)

- R una $\mathbb{Z}$-àlgebra finita amb $R \otimes_{\mathbb{Z}} \mathbb{Q}$ semisimple.
- X l'espai de mòduli parametritzant parells (A, i), amb
  - A varietat abeliana polaritzada de dimensió g,
  - $i : R \hookrightarrow \mathrm{End}(A)$ monomorfisme de $\mathbb{Z}$-àlgebres.
- Teoria de varietats de Shimura de tipus PEL:
  - $\rightsquigarrow$ model canònic $X/\mathbb{Q}$, i $P \in X(\bar{k})$ es correspon a la classe d'isomorfisme $P = [(A, i)]$ d'un parell $(A, i)/\bar{k}$.

Definició

$(A, i)/\bar{k}$ admet un model racional sobre L/k si existeix $(A', i')/L$ amb $(A' \times \bar{k}, i' \times \bar{k}) \simeq (A, i)$. En tal cas, L és un cos de definició *per a (A, i).*
El cos de mòduli *$k_P = k_{(A,i)}$ de (A, i) és la mínima extensió k_P/k tal que per a tot $s \in G_{k_P}$ hi ha un isomorfisme $f_s : {}^s(A, i) \to (A, i)$.*

$\rightsquigarrow$ k_P és subcòs de qualsevol cos de definició de (A, i).

Punts en varietats de Shimura (II)

- Per a qualsevol extensió L/k, tenim doncs

$$X(L) = \{P \in X(\bar{k}) : k_P \subseteq L\}.$$

(A, i) admet model sobre $L \Rightarrow P = [(A, i)] \in X(L)$.

Punts en varietats de Shimura (II)

- Per a qualsevol extensió L/k, tenim doncs

$$X(L) = \{P \in X(\bar{k}) : k_P \subseteq L\}.$$

(A, i) admet model sobre $L \Rightarrow P = [(A, i)] \in X(L)$.

Fixem $P = [(A, i)] \in X(k)$. Suposem $k_P = k$, i:

(H) $C_R(A)$ és un cos sense arrels de la unitat no trivials ($\neq \pm 1$).

Lema

(H) $\Rightarrow \mathrm{Aut}(A, i) = \{\pm 1\}$.

Punts en varietats de Shimura (II)

- Per a qualsevol extensió L/k, tenim doncs

$$X(L) = \{P \in X(\bar{k}) : k_P \subseteq L\}.$$

(A, i) admet model sobre $L \Rightarrow P = [(A, i)] \in X(L)$.

Fixem $P = [(A, i)] \in X(k)$. Suposem $k_P = k$, i:

(H) $C_R(A)$ és un cos sense arrels de la unitat no trivials ($\neq \pm 1$).

Lema

(H) $\Rightarrow \mathrm{Aut}(A, i) = \{\pm 1\}$.

Demostració.

El grup d'automorfismes d'una varietat abeliana polaritzada és finit, d'on els elements de $\mathrm{Aut}(A, i) \subseteq C_R(A)^\times$ són arrels de la unitat. □

2-cocicle associat a P

- Escollim $\mathbf{f} = \{f_s : {}^s(A,i) \xrightarrow{\simeq} (A,i)\}_{s \in G_k}$, i definim

$$c_P : G_k \times G_k \longrightarrow \mathrm{Aut}(A,i) = \{\pm 1\}, \quad (s,t) \mapsto c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1}.$$

2-cocicle associat a P

- Escollim $\mathbf{f} = \{f_s : {}^s(A,i) \xrightarrow{\simeq} (A,i)\}_{s \in G_k}$, i definim

$$c_P : G_k \times G_k \longrightarrow \mathrm{Aut}(A,i) = \{\pm 1\}, \quad (s,t) \mapsto c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1}.$$

- $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ no depèn de $\mathbf{f}$.

2-cocicle associat a P

- Escollim $\mathbf{f} = \{f_s : {}^s(A,i) \xrightarrow{\simeq} (A,i)\}_{s \in G_k}$, i definim

$$c_P : G_k \times G_k \longrightarrow \mathrm{Aut}(A,i) = \{\pm 1\}, \quad (s,t) \mapsto c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1}.$$

- $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ no depèn de $\mathbf{f}$.

Lema (Weil)

L/k és cos de definició per a (A,i) $\iff$ $[c_{P,L}] = [c_{P|G_L}]$ és trivial en $\mathrm{H}^2(G_L, \{\pm 1\})$.

2-cocicle associat a P

- Escollim $\mathbf{f} = \{f_s : {}^s(A,i) \xrightarrow{\simeq} (A,i)\}_{s \in G_k}$, i definim

$$c_P : G_k \times G_k \longrightarrow \mathrm{Aut}(A,i) = \{\pm 1\}, \quad (s,t) \mapsto c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1}.$$

- $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ no depèn de $\mathbf{f}$.

Lema (Weil)

L/k és cos de definició per a (A,i) $\iff$ $[c_{P,L}] = [c_{P|G_L}]$ és trivial en $\mathrm{H}^2(G_L, \{\pm 1\})$.

Si B_P és l'algebra de quaternions sobre k corresponent a $[c_P]$ per CFT, $[c_{P,L}]$ és trivial $\iff$ $B_P \otimes_k L \simeq \mathrm{M}_2(L)$.

Corol·lari

Hi ha infinites L/k quadràtiques que són cos de definició per (A,i).

Representacions de Galois associades a P

Escollint una col·lecció d'isomorfismes $\mathbf{f}$ com abans, definim

$$\varrho_P = \varrho_{P,p} : G_k \longrightarrow G_p/\{\pm 1\}$$

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k.$$

Representacions de Galois associades a P

Escollint una col·lecció d'isomorfismes $\mathbf{f}$ com abans, definim

$$\varrho_P = \varrho_{P,p} : G_k \longrightarrow G_p/\{\pm 1\}$$

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k.$$

Passant al quocient, definim similarment

$$\bar{\varrho}_P = \bar{\varrho}_{P,p} : G_k \longrightarrow \bar{G}_p/\{\pm 1\}.$$

Lema

ϱ_P i $\bar{\varrho}_P$ són morfismes de grups i no depenen de $\mathbf{f}$.

Representacions de Galois associades a P

Escollint una col·lecció d'isomorfismes $\mathbf{f}$ com abans, definim

$$\varrho_P = \varrho_{P,p} : G_k \longrightarrow G_p/\{\pm 1\}$$

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k.$$

Passant al quocient, definim similarment

$$\bar{\varrho}_P = \bar{\varrho}_{P,p} : G_k \longrightarrow \bar{G}_p/\{\pm 1\}.$$

Lema

ϱ_P i $\bar{\varrho}_P$ són morfismes de grups i no depenen de $\mathbf{f}$.

Si $P = [(A,i)]$ amb (A,i) definida sobre L/k quadràtica, podem prendre $f_s = \mathrm{id}$ per a tot $s \in G_L \subseteq G_k$. Llavors ϱ_P i $\bar{\varrho}_P$ estenen $\varrho_{(A,i)}$ i $\bar{\varrho}_{(A,i)}$.

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).
- $\rho : B_D \to B_D, b \mapsto b^\rho$ (anti)involució positiva.

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).
- $\rho : B_D \to B_D, b \mapsto b^\rho$ (anti)involució positiva.
- Noether-Skolem: $b^\rho = \mu^{-1}\bar{b}\mu$, $\mu \in \mathcal{O}_D^\times$,

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).
- $\rho : B_D \to B_D, b \mapsto b^\rho$ (anti)involució positiva.
- Noether-Skolem: $b^\rho = \mu^{-1}\bar{b}\mu$, $\mu \in \mathcal{O}_D^\times$, $\mathrm{tr}(\mu) = 0, \mathrm{n}(\mu) > 0$.

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).
- $\rho : B_D \to B_D, b \mapsto b^\rho$ (anti)involució positiva.
- Noether-Skolem: $b^\rho = \mu^{-1}\bar{b}\mu$, $\mu \in \mathcal{O}_D^\times$, $\mathrm{tr}(\mu) = 0, \mathrm{n}(\mu) > 0$.
- Una superfície abeliana amb multiplicació quaterniònica (QM) per $(B_D, \mathcal{O}_D, \rho)$ és una tripleta $(A, \iota, \mathcal{L})$, on:
  - A superfície abeliana,
  - $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ monomorfisme,
  - $\mathcal{L}$ polarització feble en A tal que $\iota(b^\rho) = \iota(b)^*$, on $*$ és la involució de Rosati definida per $\mathcal{L}$.

Superfícies abelianes amb QM

- B_D àlgebra de quaternions racional i indefinida, $D > 1$, $\mathcal{O}_D \subseteq B_D$ ordre maximal (únic llevat de conjugació).
- $\rho : B_D \to B_D, b \mapsto b^\rho$ (anti)involució positiva.
- Noether-Skolem: $b^\rho = \mu^{-1}\bar{b}\mu$, $\mu \in \mathcal{O}_D^\times$, $\mathrm{tr}(\mu) = 0, \mathrm{n}(\mu) > 0$.
- Una superfície abeliana amb multiplicació quaterniònica (QM) per $(B_D, \mathcal{O}_D, \rho)$ és una tripleta $(A, \iota, \mathcal{L})$, on:
  - A superfície abeliana,
  - $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ monomorfisme,
  - $\mathcal{L}$ polarització feble en A tal que $\iota(b^\rho) = \iota(b)^*$, on $*$ és la involució de Rosati definida per $\mathcal{L}$.
- Milne (1979): fixat el parell (A, ι), la polarització feble $\mathcal{L}$ està unívocament determinada per μ.

La corba de Shimura X_D

- Fixem $B_D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, i posem $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D : \mathrm{n}(\gamma) = 1\}$.
- $\mathcal{O}_D^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ actua en el semiplà $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ per transformacions de Moebius.

La corba de Shimura X_D

- Fixem $B_D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, i posem $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D : \mathrm{n}(\gamma) = 1\}$.
- $\mathcal{O}_D^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ actua en el semiplà $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ per transformacions de Moebius.
- La superfície de Riemann $V_D := \mathcal{O}_D^1 \backslash \mathfrak{H}$ és compacta ($D > 1$).

La corba de Shimura X_D

- Fixem $B_D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, i posem $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D : \mathrm{n}(\gamma) = 1\}$.
- $\mathcal{O}_D^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ actua en el semiplà $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ per transformacions de Moebius.
- La superfície de Riemann $V_D := \mathcal{O}_D^1 \setminus \mathfrak{H}$ és compacta ($D > 1$).
- Shimura (1967): existeix una corba algebraica projectiva llisa X_D sobre $\mathbb{Q}$ tal que

$$V_D \simeq X_D(\mathbb{C})^{\mathrm{an}}.$$

X_D és la corba de Shimura associada a B_D, i és solució al problema de mòduli de classificar superfícies abelianes amb QM.

La corba de Shimura X_D

- Fixem $B_D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, i posem $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D : \mathrm{n}(\gamma) = 1\}$.
- $\mathcal{O}_D^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ actua en el semiplà $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ per transformacions de Moebius.
- La superfície de Riemann $V_D := \mathcal{O}_D^1 \setminus \mathfrak{H}$ és compacta ($D > 1$).
- Shimura (1967): existeix una corba algebraica projectiva llisa X_D sobre $\mathbb{Q}$ tal que

$$V_D \simeq X_D(\mathbb{C})^{\mathrm{an}}.$$

  X_D és la corba de Shimura associada a B_D, i és solució al problema de mòduli de classificar superfícies abelianes amb QM.

- Parametrització explícita: $\tau \mapsto (A_\tau, \iota_\tau)$, $A_\tau = \mathbb{C}^2/\mathcal{O}_D \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix}$.

Punts racionals en X_D

- $P \in X_D(k)$, $P = [(A, \iota)]$, $(A, \iota)/\bar{k}$ amb cos de mòduli k.
- Existeix col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A, \iota) \overset{\simeq}{\to} (A, \iota)\}_{s \in G_k}$.

Punts racionals en X_D

- $P \in X_D(k)$, $P = [(A, \iota)]$, $(A, \iota)/\bar{k}$ amb cos de mòduli k.
- Existeix col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A, \iota) \xrightarrow{\simeq} (A, \iota)\}_{s \in G_k}$.

Lema

Si A no té CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$, es compleix (H).

Demostració.

Si A no té CM, $\mathrm{End}^0(A) \simeq B_D$ i $C_{\mathcal{O}_D}(A) = \mathbb{Q}$. I si A té CM per M, $\mathrm{End}^0(A) \simeq \mathrm{M}_2(M)$ i $C_{\mathcal{O}_D}(A) = M$. □

Punts racionals en X_D

- $P \in X_D(k)$, $P = [(A, \iota)]$, $(A, \iota)/\bar{k}$ amb cos de mòduli k.
- Existeix col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A, \iota) \xrightarrow{\simeq} (A, \iota)\}_{s \in G_k}$.

Lema

Si A no té CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$, es compleix (H).

Demostració.

Si A no té CM, $\mathrm{End}^0(A) \simeq B_D$ i $C_{\mathcal{O}_D}(A) = \mathbb{Q}$. I si A té CM per M, $\mathrm{End}^0(A) \simeq \mathrm{M}_2(M)$ i $C_{\mathcal{O}_D}(A) = M$. □

- Podem associar representacions de Galois a P, via $[c_P]$.
- Teorema de Jordan *revisited*:

$$B_P = B_D \otimes_{\mathbb{Q}} k \text{ (independentment de } P!).$$

Representacions de Galois

- K quadràtic imaginari, v plaça finita de K, $P_v = [(A_v, \iota_v)] \in X_D(K_v)$ sense CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$.
- Podem prendre (A_v, ι_v) definida sobre L/K_v quadràtica.

Representacions de Galois

- K quadràtic imaginari, v plaça finita de K, $P_v = [(A_v, \iota_v)] \in X_D(K_v)$ sense CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$.
- Podem prendre (A_v, ι_v) definida sobre L/K_v quadràtica.
- Les representacions $\varrho_{(A_v,\iota_v),p}, \bar{\varrho}_{(A_v,\iota_v),p}$ de G_L s'estenen a

$$\varrho_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))/\pm 1 \simeq (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times/\pm 1,$$
$$\bar{\varrho}_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(A_v[p])/\pm 1 \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times/\pm 1.$$

Representacions de Galois

- K quadràtic imaginari, v plaça finita de K, $P_v = [(A_v, \iota_v)] \in X_D(K_v)$ sense CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$.
- Podem prendre (A_v, ι_v) definida sobre L/K_v quadràtica.
- Les representacions $\varrho_{(A_v,\iota_v),p}, \bar{\varrho}_{(A_v,\iota_v),p}$ de G_L s'estenen a

$$\varrho_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))/\pm 1 \simeq (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times/\pm 1,$$
$$\bar{\varrho}_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(A_v[p])/\pm 1 \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times/\pm 1.$$

- Suposem $p \mid D$. $A_v[p]$ té un únic $\mathcal{O}_D$-submòdul propi no trivial,

$$C_p = A_v[I(p)] \simeq \mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2},$$

anomenat subgrup canònic de torsió en p, on
$I(p) = \{\beta \in \mathcal{O}_D : p \mid \mathrm{n}(\beta)\}$ és l'únic $\mathcal{O}_D$-ideal bilateral de norma p.

Representacions de Galois

- K quadràtic imaginari, v plaça finita de K, $P_v = [(A_v, \iota_v)] \in X_D(K_v)$ sense CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$.
- Podem prendre (A_v, ι_v) definida sobre L/K_v quadràtica.
- Les representacions $\varrho_{(A_v,\iota_v),p}, \bar{\varrho}_{(A_v,\iota_v),p}$ de G_L s'estenen a
$$\varrho_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))/\pm 1 \simeq (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times/\pm 1,$$
$$\bar{\varrho}_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(A_v[p])/\pm 1 \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times/\pm 1.$$
- Suposem $p \mid D$. $A_v[p]$ té un únic $\mathcal{O}_D$-submòdul propi no trivial,
$$C_p = A_v[I(p)] \simeq \mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2},$$
anomenat subgrup canònic de torsió en p, on $I(p) = \{\beta \in \mathcal{O}_D : p \mid \mathrm{n}(\beta)\}$ és l'únic $\mathcal{O}_D$-ideal bilateral de norma p.
- La representació $\alpha_{(A_v,\iota_v),p} : G_L \to \mathrm{Aut}_{\mathcal{O}_D}(C_p)$ també s'estén a
$$\alpha_{P_v,p} : G_{K_v} \to \mathrm{Aut}_{\mathcal{O}_D}(C_p)/\pm 1 \simeq \mathbb{F}_{p^2}^\times/\pm 1.$$

Relació amb el recobridor de Shimura

- Considerem el problema de mòduli de classificar tripletes (A, ι, x_p), on
  - (A, ι) és superfície abeliana amb QM,
  - x_p és un generador de C_p com a $\mathcal{O}_D$-mòdul.

Relació amb el recobridor de Shimura

- Considerem el problema de mòduli de classificar tripletes (A, ι, x_p), on
  - (A, ι) és superfície abeliana amb QM,
  - x_p és un generador de C_p com a $\mathcal{O}_D$-mòdul.
- La solució dóna lloc a un recobridor cíclic de Galois $X_{D,p} \to X_D$ amb $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$. El recobridor de Shimura $Z_{D,p} \to X_D$ és el màxim subrecobridor étale de X_D, i té ordre $\frac{p^2-1}{2e}$, $e \mid 6$.

Relació amb el recobridor de Shimura

- Considerem el problema de mòduli de classificar tripletes (A, ι, x_p), on
  - (A, ι) és superfície abeliana amb QM,
  - x_p és un generador de C_p com a $\mathcal{O}_D$-mòdul.
- La solució dóna lloc a un recobridor cíclic de Galois $X_{D,p} \to X_D$ amb $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$. El recobridor de Shimura $Z_{D,p} \to X_D$ és el màxim subrecobridor étale de X_D, i té ordre $\frac{p^2-1}{2e}$, $e \mid 6$.
- Suposant $p \geq 5$ i quocientant per $\mathbb{Z}/6\mathbb{Z} \rightsquigarrow$ Recobridor étale

$$f_p : Y_{D,p} \to X_D, \quad \mathrm{Aut}(Y_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z} \simeq \mathbb{F}_{p^2}^{\times 12}.$$

Relació amb el recobridor de Shimura

- Considerem el problema de mòduli de classificar tripletes (A, ι, x_p), on
  - (A, ι) és superfície abeliana amb QM,
  - x_p és un generador de C_p com a $\mathcal{O}_D$-mòdul.
- La solució dóna lloc a un recobridor cíclic de Galois $X_{D,p} \to X_D$ amb $\mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$. El recobridor de Shimura $Z_{D,p} \to X_D$ és el màxim subrecobridor étale de X_D, i té ordre $\frac{p^2-1}{2e}$, $e \mid 6$.
- Suposant $p \geq 5$ i quocientant per $\mathbb{Z}/6\mathbb{Z} \rightsquigarrow$ Recobridor étale
$$f_p : Y_{D,p} \to X_D, \quad \mathrm{Aut}(Y_{D,p}/X_D) \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z} \simeq \mathbb{F}_{p^2}^{\times 12}.$$
- Per especialització de f_p en $P_v \in X_D(K_v)$, s'obté un caràcter
$$\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$$
que verifica
$$\alpha_{P_v,p}^{12} = \phi_{P_v} \mod \pm 1.$$

Absència de punts K-racionals en X_D

q nombre primer. $P_1(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2q}$, i $\mathcal{B}_1(q)$ el conjunt d'àlgebres de quaternions racionals no escindides per $\mathbb{Q}(\sqrt{-q})$ (i tampoc per $\mathbb{Q}(\sqrt{-1})$ si $q = 2$).

Absència de punts K-racionals en X_D

q nombre primer. $P_1(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2q}$, i $\mathcal{B}_1(q)$ el conjunt d'àlgebres de quaternions racionals no escindides per $\mathbb{Q}(\sqrt{-q})$ (i tampoc per $\mathbb{Q}(\sqrt{-1})$ si $q = 2$).

Teorema (de Vera-Rotger)

K imaginari quadràtic, q ramificat en K. Si $B_D \in \mathcal{B}_1(q)$ i D és divisible per un primer $p \notin P_1(q)$, $p \geq 5$, $(\frac{K}{p}) \neq 1$, aleshores $X_D(K)$ conté només punts CM. Si $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, llavors $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Absència de punts K-racionals en X_D

q nombre primer. $P_1(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2q}$, i $\mathcal{B}_1(q)$ el conjunt d'àlgebres de quaternions racionals no escindides per $\mathbb{Q}(\sqrt{-q})$ (i tampoc per $\mathbb{Q}(\sqrt{-1})$ si $q = 2$).

Teorema (de Vera-Rotger)

K imaginari quadràtic, q ramificat en K. Si $B_D \in \mathcal{B}_1(q)$ i D és divisible per un primer $p \notin P_1(q)$, $p \geq 5$, $(\frac{K}{p}) \neq 1$, aleshores $X_D(K)$ conté només punts CM. Si $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, llavors $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

- ▷ Usant els resultats de Jordan-Livné sobre punts locals en X_D, el Teorema permet obtenir corbes X_D que violen el principi de Hasse sobre K.

Idea de la prova

- $P = [(A, \iota)] \in X_D(K)$ (sense CM) $\rightsquigarrow P_v = [(A_v, \iota_v)] \in X_D(K_v)$, $\forall v$.
- Tenim representacions de Galois $\varrho_{P_v,p}$, $\bar{\varrho}_{P_v,p}$ i $\alpha_{P_v,p}$ estenent les representacions habituals.

Idea de la prova

- $P = [(A, \iota)] \in X_D(K)$ (sense CM) $\rightsquigarrow P_v = [(A_v, \iota_v)] \in X_D(K_v)$, $\forall v$.
- Tenim representacions de Galois $\varrho_{P_v,p}$, $\bar{\varrho}_{P_v,p}$ i $\alpha_{P_v,p}$ estenent les representacions habituals.
- El caràcter $\phi_P : G_K \to \mathbb{F}_{p^2}^{\times 12}$ associat a P restringeix als caràcters locals $\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ associats als P_v.

Idea de la prova

- $P = [(A, \iota)] \in X_D(K)$ (sense CM) $\rightsquigarrow P_v = [(A_v, \iota_v)] \in X_D(K_v)$, $\forall v$.
- Tenim representacions de Galois $\varrho_{P_v,p}$, $\bar{\varrho}_{P_v,p}$ i $\alpha_{P_v,p}$ estenent les representacions habituals.
- El caràcter $\phi_P : G_K \to \mathbb{F}_{p^2}^{\times 12}$ associat a P restringeix als caràcters locals $\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ associats als P_v.
- Explotant la relació $\alpha_{P_v,p}^{12} = \phi_{P_v} \mod \pm 1$, i el fet que $\alpha_{P_v,p}^{12}$ és no ramificada per $v \nmid p$, trobem condicions de congruència mòdul p per a la traça d'un element de Frobenius $\sigma_{\mathfrak{q}}$ en $\mathfrak{q}$ actuant en $T_p(A_{\mathfrak{q}})$, on $qR_K = \mathfrak{q}^2$.

Idea de la prova

- $P = [(A,\iota)] \in X_D(K)$ (sense CM) $\rightsquigarrow P_v = [(A_v,\iota_v)] \in X_D(K_v)$, $\forall v$.
- Tenim representacions de Galois $\varrho_{P_v,p}$, $\bar{\varrho}_{P_v,p}$ i $\alpha_{P_v,p}$ estenent les representacions habituals.
- El caràcter $\phi_P : G_K \to \mathbb{F}_{p^2}^{\times 12}$ associat a P restringeix als caràcters locals $\phi_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ associats als P_v.
- Explotant la relació $\alpha_{P_v,p}^{12} = \phi_{P_v} \mod \pm 1$, i el fet que $\alpha_{P_v,p}^{12}$ és no ramificada per $v \nmid p$, trobem condicions de congruència mòdul p per a la traça d'un element de Frobenius $\sigma_{\mathfrak{q}}$ en $\mathfrak{q}$ actuant en $T_p(A_{\mathfrak{q}})$, on $qR_K = \mathfrak{q}^2$.
- Aplicant la classificació d'Honda-Tate, si $p \notin P_1(q)$ i $B_D \in \mathcal{B}_1(q)$ aquestes congruències no es poden satisfer.

Parells *excepcionals* violant el principi de Hasse

- Seguint Jordan, (B_D, K) és un parell excepcional si K no escindeix B_D i $X_D(K_v) \neq \emptyset$ per a tota plaça v de K.
- Amb el Teorema anterior podem produir parells excepcionals sense punts K-racionals ($\Rightarrow$ violant el principi de Hasse):

$D = 2 \cdot p$	K
$2 \cdot 23$	$\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-119})$, ...
$2 \cdot 31$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, ...
$2 \cdot 43$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-111})$, ...
$2 \cdot 59$	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-119})$, ...
$2 \cdot 67$	$\mathbb{Q}(\sqrt{-55})$, ...
$2 \cdot 71$	$\mathbb{Q}(\sqrt{-119})$, $\mathbb{Q}(\sqrt{-143})$, ...
$2 \cdot 79$	$\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, ...

El grup d'Atkin-Lehner

- El grup $B_{D,+}^{\times} = \{b \in B_D : \mathrm{n}(b) > 0\} \subseteq \mathrm{GL}_2^+(\mathbb{R})$ actua en $\mathfrak{H}$, i indueix una acció del grup d'Atkin-Lehner de $\mathcal{O}_D$,

$$W_D = \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1,$$

en V_D. $W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ si $D = p_1 \cdots p_{2r}$, i un conjunt de representants és qualsevol $\{\mathrm{w}_m\}_{m|D}$ amb $\mathrm{w}_m \in \mathcal{O}_D$, $\mathrm{n}(\mathrm{w}_m) = m$.

El grup d'Atkin-Lehner

- El grup $B_{D,+}^{\times} = \{b \in B_D : \mathrm{n}(b) > 0\} \subseteq \mathrm{GL}_2^+(\mathbb{R})$ actua en $\mathfrak{H}$, i indueix una acció del grup d'Atkin-Lehner de $\mathcal{O}_D$,

$$W_D = \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1,$$

  en V_D. $W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ si $D = p_1 \cdots p_{2r}$, i un conjunt de representants és qualsevol $\{\mathrm{w}_m\}_{m|D}$ amb $\mathrm{w}_m \in \mathcal{O}_D$, $\mathrm{n}(\mathrm{w}_m) = m$.

- En termes modulars, l'acció de $\omega_m = [\mathrm{w}_m] \in W_D$ en X_D és

$$P = [(A, \iota, \mathcal{L})] \mapsto \omega_m(P) = [(A, \iota_{\omega_m}, \mathcal{L}_{\omega_m})],$$

  on $\iota_{\omega_m}(\beta) = \iota(\mathrm{w}_m^{-1}\beta\mathrm{w}_m)$ i $\mathcal{L}_{\omega_m} = \frac{\iota(\mathrm{w}_m)^*(\mathcal{L})}{m}$.

El grup d'Atkin-Lehner

- El grup $B_{D,+}^{\times} = \{b \in B_D : \mathrm{n}(b) > 0\} \subseteq \mathrm{GL}_2^+(\mathbb{R})$ actua en $\mathfrak{H}$, i indueix una acció del grup d'Atkin-Lehner de $\mathcal{O}_D$,

$$W_D = \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1,$$

  en V_D. $W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ si $D = p_1 \cdots p_{2r}$, i un conjunt de representants és qualsevol $\{\mathrm{w}_m\}_{m|D}$ amb $\mathrm{w}_m \in \mathcal{O}_D$, $\mathrm{n}(\mathrm{w}_m) = m$.
- En termes modulars, l'acció de $\omega_m = [\mathrm{w}_m] \in W_D$ en X_D és

$$P = [(A, \iota, \mathcal{L})] \mapsto \omega_m(P) = [(A, \iota_{\omega_m}, \mathcal{L}_{\omega_m})],$$

  on $\iota_{\omega_m}(\beta) = \iota(\mathrm{w}_m^{-1}\beta\mathrm{w}_m)$ i $\mathcal{L}_{\omega_m} = \frac{\iota(\mathrm{w}_m)^*(\mathcal{L})}{m}$.
- $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$.
- Si $\omega_m \in W_D$, posem $X_D^{(m)} := X_D/\langle\omega_m\rangle$ i $\pi_m : X_D \to X_D^{(m)}$.

Interpretació modular de $X_D^{(m)}$

- Suposarem $D = pm$ senar, $(\frac{m}{p}) = -1$. Es pot provar que aleshores $B_D \simeq (\frac{-Dd,m}{\mathbb{Q}})$ per algun enter $d \geq 1$. En particular, hi ha un embedding $R_m \hookrightarrow \mathcal{O}_D$ de l'anell d'enters de $\mathbb{Q}(\sqrt{m})$ en $\mathcal{O}_D$.

Interpretació modular de $X_D^{(m)}$

- Suposarem $D = pm$ senar, $(\frac{m}{p}) = -1$. Es pot provar que aleshores $B_D \simeq (\frac{-Dd,m}{\mathbb{Q}})$ per algun enter $d \geq 1$. En particular, hi ha un embedding $R_m \hookrightarrow \mathcal{O}_D$ de l'anell d'enters de $\mathbb{Q}(\sqrt{m})$ en $\mathcal{O}_D$.
- Si $\mathcal{H}_m$ és la superfície modular de Hilbert classificant superfícies abelianes amb multiplicació real per R_m, tenim una aplicació natural

$$\pi_{R_m} : X_D \to \mathcal{H}_m,\ (A, \iota, \mathcal{L}) \mapsto (A, \iota_{|R_m}, \mathcal{L}).$$

Interpretació modular de $X_D^{(m)}$

- Suposarem $D = pm$ senar, $(\frac{m}{p}) = -1$. Es pot provar que aleshores $B_D \simeq (\frac{-Dd,m}{\mathbb{Q}})$ per algun enter $d \geq 1$. En particular, hi ha un embedding $R_m \hookrightarrow \mathcal{O}_D$ de l'anell d'enters de $\mathbb{Q}(\sqrt{m})$ en $\mathcal{O}_D$.
- Si $\mathcal{H}_m$ és la superfície modular de Hilbert classificant superfícies abelianes amb multiplicació real per R_m, tenim una aplicació natural
$$\pi_{R_m} : X_D \to \mathcal{H}_m,\ (A, \iota, \mathcal{L}) \mapsto (A, \iota_{|R_m}, \mathcal{L}).$$
- De fet, π_{R_m} factoritza per $X_D^{(m)}$ induïnt una aplicació biracional
$$X_D^{(m)} \dashrightarrow \pi_{R_m}(X_D) \subseteq \mathcal{H}_m.$$

Interpretació modular de $X_D^{(m)}$

- Suposarem $D = pm$ senar, $(\frac{m}{p}) = -1$. Es pot provar que aleshores $B_D \simeq (\frac{-Dd,m}{\mathbb{Q}})$ per algun enter $d \geq 1$. En particular, hi ha un embedding $R_m \hookrightarrow \mathcal{O}_D$ de l'anell d'enters de $\mathbb{Q}(\sqrt{m})$ en $\mathcal{O}_D$.
- Si $\mathcal{H}_m$ és la superfície modular de Hilbert classificant superfícies abelianes amb multiplicació real per R_m, tenim una aplicació natural
$$\pi_{R_m} : X_D \to \mathcal{H}_m,\ (A, \iota, \mathcal{L}) \mapsto (A, \iota_{|R_m}, \mathcal{L}).$$
- De fet, π_{R_m} factoritza per $X_D^{(m)}$ induïnt una aplicació biracional
$$X_D^{(m)} \dashrightarrow \pi_{R_m}(X_D) \subseteq \mathcal{H}_m.$$

$\rightsquigarrow$ $X_D^{(m)}$ classifica superfícies abelianes $(A, i, \mathcal{L})$ amb RM per $\mathbb{Q}(\sqrt{m})$ que admeten QM per B_D.

Punts racionals en $X_D^{(m)}$

- $Q \in X_D^{(m)}(k)$, $Q = [(A, i : R_m \hookrightarrow \mathrm{End}(A))]$ on (A, i) té cos de mòduli k i $\mathrm{End}_{\bar{k}}(A) \supseteq \mathcal{O}_D$.

Teorema (Bruin-Flynn-Gonzàlez-Rotger)

Si $Q = [(A, i)] \in X_D^{(m)}(k)$ no és un punt CM i $K = k(\pi_m^{-1}(Q)) = k(\sqrt{\delta})$, $\delta \in k^\times$, aleshores $B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes (\frac{\delta, m}{k})$. És a dir, (A, i) admet un model racional sobre K/k si, i només si, $B_D \otimes_{\mathbb{Q}} K \simeq (\frac{\delta, m}{K})$.

Punts racionals en $X_D^{(m)}$

- $Q \in X_D^{(m)}(k)$, $Q = [(A, i : R_m \hookrightarrow \mathrm{End}(A))]$ on (A, i) té cos de mòduli k i $\mathrm{End}_{\bar{k}}(A) \supseteq \mathcal{O}_D$.

Teorema (Bruin-Flynn-Gonzàlez-Rotger)

Si $Q = [(A, i)] \in X_D^{(m)}(k)$ no és un punt CM i $K = k(\pi_m^{-1}(Q)) = k(\sqrt{\delta})$, $\delta \in k^\times$, aleshores $B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes (\frac{\delta, m}{k})$. És a dir, (A, i) admet un model racional sobre K/k si, i només si, $B_D \otimes_{\mathbb{Q}} K \simeq (\frac{\delta, m}{K})$.

$\rightsquigarrow$ Ara B_Q depèn del punt Q.

Punts racionals en $X_D^{(m)}$

- $Q \in X_D^{(m)}(k)$, $Q = [(A, i : R_m \hookrightarrow \mathrm{End}(A))]$ on (A, i) té cos de mòduli k i $\mathrm{End}_{\bar{k}}(A) \supseteq \mathcal{O}_D$.

Teorema (Bruin-Flynn-Gonzàlez-Rotger)

Si $Q = [(A, i)] \in X_D^{(m)}(k)$ no és un punt CM i $K = k(\pi_m^{-1}(Q)) = k(\sqrt{\delta})$, $\delta \in k^\times$, aleshores $B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes (\frac{\delta, m}{k})$. És a dir, (A, i) admet un model racional sobre K/k si, i només si, $B_D \otimes_{\mathbb{Q}} K \simeq (\frac{\delta, m}{K})$.

$\rightsquigarrow$ Ara B_Q depèn del punt Q.

- Com abans, si A no té CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$, es verifica (H).

Punts racionals en $X_D^{(m)}$

- $Q \in X_D^{(m)}(k)$, $Q = [(A, i : R_m \hookrightarrow \mathrm{End}(A))]$ on (A, i) té cos de mòduli k i $\mathrm{End}_{\bar{k}}(A) \supseteq \mathcal{O}_D$.

Teorema (Bruin-Flynn-Gonzàlez-Rotger)

Si $Q = [(A, i)] \in X_D^{(m)}(k)$ no és un punt CM i $K = k(\pi_m^{-1}(Q)) = k(\sqrt{\delta})$, $\delta \in k^\times$, aleshores $B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes (\frac{\delta, m}{k})$. És a dir, (A, i) admet un model racional sobre K/k si, i només si, $B_D \otimes_{\mathbb{Q}} K \simeq (\frac{\delta, m}{K})$.

$\rightsquigarrow$ Ara B_Q depèn del punt Q.

- Com abans, si A no té CM per $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$, es verifica (H).
- Escollint una col·lecció d'isomorfismes $\mathbf{f} = \{f_s : {}^s(A, i) \xrightarrow{\simeq} (A, i)\}_{s \in G_k}$, podem estendre les representacions de Galois associades a (A, i) via $[c_Q]$.

Absència de punts racionals en $X_D^{(m)}$

q nombre primer. Sigui $P_2(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2\sqrt{q}}$, i $\mathcal{B}_2(q)$ el conjunt d'àlgebres $B \in \mathcal{B}_1(q)$ tals que q no és inert en cap cos quadràtic imaginari no ramificat fora de disc(B).

Absència de punts racionals en $X_D^{(m)}$

q nombre primer. Sigui $P_2(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2\sqrt{q}}$, i $\mathcal{B}_2(q)$ el conjunt d'àlgebres $B \in \mathcal{B}_1(q)$ tals que q no és inert en cap cos quadràtic imaginari no ramificat fora de $\mathrm{disc}(B)$.

Teorema (de Vera-Rotger)

Si $D = pm$ és senar, amb $p \geq 7$ primer, $p \equiv 3 \mod 4$, i existeix un primer q tal que $B_D \in \mathcal{B}_2(q)$ i $p \notin P_2(q)$, aleshores $X_D^{(m)}(\mathbb{Q}) = \emptyset$.

Absència de punts racionals en $X_D^{(m)}$

q nombre primer. Sigui $P_2(q)$ el conjunt de primers dividint algun enter no nul de $\{a^2 - sq, a^4 - 4a^2q + q^2\}_{s=0,1,2,3,4,|a|\leq 2\sqrt{q}}$, i $\mathcal{B}_2(q)$ el conjunt d'àlgebres $B \in \mathcal{B}_1(q)$ tals que q no és inert en cap cos quadràtic imaginari no ramificat fora de disc(B).

Teorema (de Vera-Rotger)

Si $D = pm$ és senar, amb $p \geq 7$ primer, $p \equiv 3 \mod 4$, i existeix un primer q tal que $B_D \in \mathcal{B}_2(q)$ i $p \notin P_2(q)$, aleshores $X_D^{(m)}(\mathbb{Q}) = \emptyset$.

Alguns parells (p, m) amb $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ i $X_{pm}^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$:

(23, 17), (31, 17), (31, 29), (31, 37), (31, 53), (31, 61), (47, 13), (47, 41), (59, 13), (71, 13), (71, 17), (79, 17), (83, 5), (83, 13), (103, 5), (107, 5), (107, 17), (127, 5), (151, 13), (167, 5), ...

Comentaris

- La idea de la prova és similar a la del cas de X_D, considerant un recobridor étale $Y_{D,p}^{(m)} \to X_D^{(m)}$ construït a partir de $Y_{D,p} \to X_D$.

Comentaris

- La idea de la prova és similar a la del cas de X_D, considerant un recobridor étale $Y_{D,p}^{(m)} \to X_D^{(m)}$ construït a partir de $Y_{D,p} \to X_D$.
- A nivell "global", ens cal controlar els cossos $K = \mathbb{Q}(\pi_m^{-1}(Q))$, $Q \in X_D^{(m)}(\mathbb{Q})$:

Lema

Si $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D, aleshores K és no ramificat fora de D.

Comentaris

- La idea de la prova és similar a la del cas de X_D, considerant un recobridor étale $Y_{D,p}^{(m)} \to X_D^{(m)}$ construït a partir de $Y_{D,p} \to X_D$.
- A nivell "global", ens cal controlar els cossos $K = \mathbb{Q}(\pi_m^{-1}(Q))$, $Q \in X_D^{(m)}(\mathbb{Q})$:

Lema

Si $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D, aleshores K és no ramificat fora de D.

- La condició $B_D \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-m}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-m}))$ equival a que ω_m no tingui punts fixos ($\iff$ π_m no ramificada).
- Tanmateix, sota les hipòtesis del Teorema, si $\mathbb{Q}(\sqrt{-m})$ no escindeix B_D llavors $X_D^{(m)}(\mathbb{A}_{\mathbb{Q}}) = \emptyset$.

Bonus track

El Lema anterior pot usar-se, juntament amb [Rotger, 2008], per provar l'absència de punts racionals en certs quocients d'Atkin-Lehner:

Teorema (de Vera-Rotger)

Siguin p i m dos primers amb $p \equiv m \equiv 3 \bmod 4$, $\left(\frac{m}{p}\right) = -1$ i $p \neq 3, 7, 11, 19, 43, 67, 163$. Si existeix un primer senar q tal que $p \notin P_0(q)$, $\left(\frac{q}{p}\right) = 1$ i $\left(\frac{q}{m}\right) = -1$, llavors $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$.

Alguns parells (p, m) amb $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ i $X_{pm}^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$:

(23, 7), (23, 11), (23, 19), (23, 43), (31, 3), (31, 11), (31, 23), (31, 31), (31, 43), (47, 11), (47, 19), (47, 23), (47, 31), (47, 43), (59, 11), (59, 23), (59, 31), (59, 43), (59, 47), (71, 7), (71, 11), (71, 23), (71, 31), (71, 31), (71, 47), (79, 3), (79, 7), (79, 43), ...

Qüestions obertes

- El fet que en el cas de $X_D^{(m)}$ no puguem explicar l'absència de punts racional mitjançant l'obstrucció de Brauer-Manin rau en el fet que B_Q depèn del punt Q.

- Més en general, suposem que l'espai de mòduli X d'una família de varietats abelianes, equipada amb alguna estructura addicional, admet un model canònic sobre $\mathbb{Q}$, i suposem també que (H) es verifica per a tot punt $P \in X_D(k)$.
  - És l'àlgebra B_P independent de P?
  - És més fàcil tractar amb el conjunt $\{B_P : P \in X(k)\}$ que amb el propi $X(k)$?
  - Existeix una àlgebra de quaternions B sobre $\mathbb{Q}$ tal que $B_P = B \otimes_{\mathbb{Q}} k$ (per a tot P)?

Representacions de Galois sobre cossos de mòduli i punts racionals en corbes de Shimura

Carlos de Vera, Víctor Rotger

Departament de Matemàtica Aplicada 2, UPC

STNB 2012
24 de gener