# Teoria d'Honda-Tate

Carlos de Vera Piquero

Departament de Matemàtica Aplicada 2, UPC

STNB 2012 - Varietats abelianes mòdul p
26 de gener

# Índex

# Varietats abelianes sobre un cos finit

- $k = \mathbb{F}_q$, $q = p^a$, $G_k = \mathrm{Gal}(\bar{k}/k)$.
- Si $A/k$ és una varietat abeliana de dimensió $g$, posem

$$\pi_A = \text{endomorfisme de Frobenius de } A\text{, induït per } x \mapsto x^q,$$
$$f_A = \mathrm{charpol}(\pi_A) \in \mathbb{Z}[T],\ \deg(f_A) = 2g.$$

# Varietats abelianes sobre un cos finit

- $k = \mathbb{F}_q$, $q = p^a$, $G_k = \mathrm{Gal}(\bar{k}/k)$.
- Si $A/k$ és una varietat abeliana de dimensió $g$, posem

$$\pi_A = \text{endomorfisme de Frobenius de } A\text{, induït per } x \mapsto x^q,$$
$$f_A = \mathrm{charpol}(\pi_A) \in \mathbb{Z}[T],\ \deg(f_A) = 2g.$$

**Teorema (Tate)**

*Siguin $A, B$ dues varietats abelianes definides sobre $k$. Són equivalents:*

(1) *$B$ és $k$-isògena a una subvarietat abeliana de $A$,*

(2) *$f_B \mid f_A$ en $\mathbb{Q}[T]$.*

*En particular, $A \sim_k B$ si i només si $f_A = f_B$. A més, $A$ és $k$-simple si i només si $f_A = m_A^e$ amb $m_A$ irreductible a $\mathbb{Q}[T]$, $e \geq 1$.*

# $q$-enters de Weil

## Definició

*Un q-enter de Weil és un enter algebraic $\pi$ tal que $|\sigma\pi| = q^{1/2}$ per a tot embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.*

# $q$-enters de Weil

## Definició

*Un q-enter de Weil és un enter algebraic $\pi$ tal que $|\sigma\pi| = q^{1/2}$ per a tot embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.*

Denotarem per $W(q)$ el conjunt dels $q$-enters de Weil, i direm que $\pi, \pi' \in W(q)$ són *conjugats*, $\pi \sim \pi'$, si existeix un isomorfisme

$$\mathbb{Q}(\pi) \xrightarrow{\simeq} \mathbb{Q}(\pi'), \quad \pi \mapsto \pi'.$$

# $q$-enters de Weil

## Definició

*Un q-enter de Weil és un enter algebraic $\pi$ tal que $|\sigma\pi| = q^{1/2}$ per a tot embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.*

Denotarem per $W(q)$ el conjunt dels $q$-enters de Weil, i direm que $\pi, \pi' \in W(q)$ són *conjugats*, $\pi \sim \pi'$, si existeix un isomorfisme

$$\mathbb{Q}(\pi) \xrightarrow{\simeq} \mathbb{Q}(\pi'), \quad \pi \mapsto \pi'.$$

## Exemple

*Associat a una varietat abeliana $A/k$ tenim el $q$-enter de Weil $\pi_A$, determinat llevat de conjugació.*

# El Teorema d'Honda-Tate

L'objectiu és provar el següent:

**Teorema (Honda-Tate, 1968)**

*L'aplicació $A \mapsto \pi_A$ estableix una bijecció*

$$\left\{ \begin{array}{c} \textit{classes d'isogènia de varietats} \\ \textit{abelianes simples sobre } k \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{classes de conjugació de} \\ q\textit{-enters de Weil} \end{array} \right\}$$

# El Teorema d'Honda-Tate

L'objectiu és provar el següent:

**Teorema (Honda-Tate, 1968)**

*L'aplicació $A \mapsto \pi_A$ estableix una bijecció*

$$\left\{ \begin{array}{c} \textit{classes d'isogènia de varietats} \\ \textit{abelianes simples sobre } k \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{classes de conjugació de} \\ q\textit{-enters de Weil} \end{array} \right\}$$

El resultat precís de classificació descriu també l'àlgebra d'endomorfismes $\mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ d'una varietat abeliana simple $A/k$. Per tant, descriu exactament la categoria de varietats abelianes llevat d'isogènia sobre $k$, $\mathrm{Isab}(k)$, definida per:

Objectes($\mathrm{Isab}(k)$): varietats abelianes sobre $k$,

Morfismes($\mathrm{Isab}(k)$): $\mathrm{Mor}(A, B) = \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$.

# Àlgebres centrals simples

Una *àlgebra central simple* sobre un cos $K$ és una $K$-àlgebra $R$ tal que:

(a) $R$ és de dimensió finita sobre $K$,

(b) el centre de $R$ és exactament $K$,

(c) $R$ és un anell simple (no té ideals bilaterals propis no trivials).

# Àlgebres centrals simples

Una *àlgebra central simple* sobre un cos $K$ és una $K$-àlgebra $R$ tal que:

(a) $R$ és de dimensió finita sobre $K$,

(b) el centre de $R$ és exactament $K$,

(c) $R$ és un anell simple (no té ideals bilaterals propis no trivials).

- ▷ Exemple bàsic: l'àlgebra de matrius $\mathrm{M}_r(K)$ (àlgebra escindida).
- ▷ Si $R$ i $S$ són $K$-àlgebres centrals i simples, aleshores $R \otimes S$ també ho és. I per a qualsevol cos $K'/K$, $R \otimes_K K'$ és una $K'$-àlgebra central i simple.

# Àlgebres centrals simples

Una *àlgebra central simple* sobre un cos $K$ és una $K$-àlgebra $R$ tal que:

(a) $R$ és de dimensió finita sobre $K$,

(b) el centre de $R$ és exactament $K$,

(c) $R$ és un anell simple (no té ideals bilaterals propis no trivials).

- ▷ Exemple bàsic: l'àlgebra de matrius $\mathrm{M}_r(K)$ (àlgebra escindida).
- ▷ Si $R$ i $S$ són $K$-àlgebres centrals i simples, aleshores $R \otimes S$ també ho és. I per a qualsevol cos $K'/K$, $R \otimes_K K'$ és una $K'$-àlgebra central i simple.

**Teorema (Wedderburn 1907, Artin 1927)**

*Tota $K$-àlgebra central i simple és isomorfa a $\mathrm{M}_r(D)$ per algun $r \geq 1$ i alguna àlgebra central de divisió $D$ sobre $K$, únicament determinada llevat d'isomorfisme.*

# El grup de Brauer

- Dues $K$-àlgebres centrals simples $R, S$ són equivalents si existeixen enters $m, n \geq 1$ i una $K$-àlgebra central de divisió $D$ tals que $R \simeq \mathrm{M}_n(D)$ i $S \simeq \mathrm{M}_m(D)$. Equivalentment, si $\mathrm{M}_r(R) \simeq \mathrm{M}_s(S)$ per alguns enters $r, s \geq 1$.

# El grup de Brauer

- Dues $K$-àlgebres centrals simples $R, S$ són equivalents si existeixen enters $m, n \geq 1$ i una $K$-àlgebra central de divisió $D$ tals que $R \simeq \mathrm{M}_n(D)$ i $S \simeq \mathrm{M}_m(D)$. Equivalentment, si $\mathrm{M}_r(R) \simeq \mathrm{M}_s(S)$ per alguns enters $r, s \geq 1$.

El conjunt $\mathrm{Br}(K)$ de classes d'equivalència de $K$-àlgebres centrals simples forma un grup amb l'operació $[R][S] := [R \otimes S]$, per a la qual l'element neutre és $[K] = [\mathrm{M}_n(K)]$ i l'invers de $[R]$ és $[R]^{-1} = [R^{op}]$. És el grup de Brauer de $K$.

# El grup de Brauer

- Dues $K$-àlgebres centrals simples $R, S$ són equivalents si existeixen enters $m, n \geq 1$ i una $K$-àlgebra central de divisió $D$ tals que $R \simeq \mathrm{M}_n(D)$ i $S \simeq \mathrm{M}_m(D)$. Equivalentment, si $\mathrm{M}_r(R) \simeq \mathrm{M}_s(S)$ per alguns enters $r, s \geq 1$.

El conjunt $\mathrm{Br}(K)$ de classes d'equivalència de $K$-àlgebres centrals simples forma un grup amb l'operació $[R][S] := [R \otimes S]$, per a la qual l'element neutre és $[K] = [\mathrm{M}_n(K)]$ i l'invers de $[R]$ és $[R]^{-1} = [R^{op}]$. És el grup de Brauer de $K$.

- Cada classe en $\mathrm{Br}(K)$ està representada per una única $K$-àlgebra de divisió, llevat isomorfisme.
- Interpretació cohomològica: es té un isomorfisme

$$\mathrm{H}^2(\mathrm{Gal}(K^s/K), (K^s)^\times) \simeq \mathrm{Br}(K).$$

# Exemples

(1) (Frobenius) L'única àlgebra de divisió no commutativa sobre $\mathbb{R}$ és l'àlgebra

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij = \left(\frac{-1,-1}{\mathbb{R}}\right),\ i^2 = j^2 = -1,\ ij = -ji,$$

dels quaternions de Hamilton. Per tant, $\mathrm{Br}(\mathbb{R}) = \{1 = [\mathbb{R}], [\mathbb{H}]\}$.

# Exemples

(1) (Frobenius) L'única àlgebra de divisió no commutativa sobre $\mathbb{R}$ és l'àlgebra

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij = \left(\frac{-1,-1}{\mathbb{R}}\right),\ i^2 = j^2 = -1,\ ij = -ji,$$

dels quaternions de Hamilton. Per tant, $\mathrm{Br}(\mathbb{R}) = \{1 = [\mathbb{R}], [\mathbb{H}]\}$.

(2) (Wedderburn) Si $F$ és algebraicament tancat i $D$ és una $F$-àlgebra de divisió de dimensió finita, aleshores $D = F$. En particular, $\mathrm{Br}(\mathbb{C}) = 1$.

# Exemples

(1) (Frobenius) L'única àlgebra de divisió no commutativa sobre $\mathbb{R}$ és l'àlgebra

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij = \left(\frac{-1,-1}{\mathbb{R}}\right),\ i^2 = j^2 = -1,\ ij = -ji,$$

dels quaternions de Hamilton. Per tant, $\mathrm{Br}(\mathbb{R}) = \{1 = [\mathbb{R}], [\mathbb{H}]\}$.

(2) (Wedderburn) Si $F$ és algebraicament tancat i $D$ és una $F$-àlgebra de divisió de dimensió finita, aleshores $D = F$. En particular, $\mathrm{Br}(\mathbb{C}) = 1$.

(3) (Wedderburn) Tota àlgebra de divisió finita és un cos. En particular, el grup de Brauer de qualsevol cos finit és trivial.

# Exemples

(1) (Frobenius) L'única àlgebra de divisió no commutativa sobre $\mathbb{R}$ és l'àlgebra

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij = \left(\frac{-1,-1}{\mathbb{R}}\right),\ i^2 = j^2 = -1,\ ij = -ji,$$

dels quaternions de Hamilton. Per tant, $\mathrm{Br}(\mathbb{R}) = \{1 = [\mathbb{R}], [\mathbb{H}]\}$.

(2) (Wedderburn) Si $F$ és algebraicament tancat i $D$ és una $F$-àlgebra de divisió de dimensió finita, aleshores $D = F$. En particular, $\mathrm{Br}(\mathbb{C}) = 1$.

(3) (Wedderburn) Tota àlgebra de divisió finita és un cos. En particular, el grup de Brauer de qualsevol cos finit és trivial.

(4) *Àlgebres cícliques:* $F/K$ extensió cíclica de grau $n$, $\mathrm{Gal}(F/K) = \langle\sigma\rangle$,

$$R = F + uF + \cdots + u^{n-1}F,$$

$$d \cdot u = u \cdot {}^{\sigma}d \text{ per a tot } d \in F,\ u^n = a \in K^{\times}.$$

Denotem aquesta àlgebra per $(F, \sigma, a)$, i $F \subseteq R$ és un subcòs maximal.

# Grup de Brauer d'un cos local

Per als cossos locals:

**Teorema**

*Si $K$ és un cos local, existeix un homomorfisme canònic*

$$\mathrm{inv}_K : \mathrm{Br}(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

*Si $K$ és no arquimedià, aleshores $\mathrm{inv}_K$ és un isomorfisme; en el cas $K = \mathbb{R}$, es té $\mathrm{inv}_{\mathbb{R}}(\mathrm{Br}(\mathbb{R})) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.*

# Grup de Brauer d'un cos local

Per als cossos locals:

**Teorema**

*Si $K$ és un cos local, existeix un homomorfisme canònic*

$$\mathrm{inv}_K : \mathrm{Br}(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

*Si $K$ és no arquimedià, aleshores $\mathrm{inv}_K$ és un isomorfisme; en el cas $K = \mathbb{R}$, es té $\mathrm{inv}_{\mathbb{R}}(\mathrm{Br}(\mathbb{R})) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.*

Exemple: $L/K$ extensió no ramificada de grau $n$, $\mathrm{Gal}(L/K) = \langle\sigma\rangle$, $\sigma$ automorfisme de Frobenius. Si $R = (L, \sigma, \pi_K)$,

$$\mathrm{inv}_K(R) = 1/n.$$

# Grup de Brauer d'un cos de nombres

Si $K$ és un cos de nombres, i $v$ és una plaça de $K$, posem $\mathrm{inv}_v := \mathrm{inv}_{K_v}$.
L'aplicacio $R \mapsto R \otimes_K K_v$ defineix una aplicació natural $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$.

# Grup de Brauer d'un cos de nombres

Si $K$ és un cos de nombres, i $v$ és una plaça de $K$, posem $\mathrm{inv}_v := \mathrm{inv}_{K_v}$.
L'aplicacio $R \mapsto R \otimes_K K_v$ defineix una aplicació natural $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$.

**Teorema (Albert-Brauer-Hasse-Noether)**

*Si $K$ és un cos de nombres, aleshores es té una successió exacta*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0,$$

*on la suma recorre totes les places $v$ de $K$.*

# Grup de Brauer d'un cos de nombres

Si $K$ és un cos de nombres, i $v$ és una plaça de $K$, posem $\mathrm{inv}_v := \mathrm{inv}_{K_v}$. L'aplicacio $R \mapsto R \otimes_K K_v$ defineix una aplicació natural $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$.

**Teorema (Albert-Brauer-Hasse-Noether)**

*Si $K$ és un cos de nombres, aleshores es té una successió exacta*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0,$$

*on la suma recorre totes les places $v$ de $K$.*

- Tota àlgebra de divisió amb centre $K$ ve determinada (llevat isomorfisme) pels seus invariants locals, que sumen zero (mòdul $\mathbb{Z}$).
- $R$ és escindida si, i només si, $R_v := R \otimes_K K_v$ ho és per a tota $v$.

# L'àlgebra de $\mathbb{Q}$-endomorfismes d'una varietat abeliana

Siguin $A, B$ varietats abelianes sobre un cos $k$.

# L'àlgebra de $\mathbb{Q}$-endomorfismes d'una varietat abeliana

Siguin $A, B$ varietats abelianes sobre un cos $k$.

- El grup $\mathrm{Hom}(A, B)$ és un $\mathbb{Z}$-mòdul lliure de rang finit ($\leq 4\dim(A)\dim(B)$).

# L'àlgebra de $\mathbb{Q}$-endomorfismes d'una varietat abeliana

Siguin $A, B$ varietats abelianes sobre un cos $k$.

- El grup $\mathrm{Hom}(A, B)$ és un $\mathbb{Z}$-mòdul lliure de rang finit ($\leq 4\dim(A)\dim(B)$).
- En particular, $\mathrm{End}(A)$ és un $\mathbb{Z}$-mòdul lliure finitament generat, d'on

$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

  és una $\mathbb{Q}$-àlgebra de dimensió finita.

# L'àlgebra de $\mathbb{Q}$-endomorfismes d'una varietat abeliana

Siguin $A, B$ varietats abelianes sobre un cos $k$.

- El grup $\mathrm{Hom}(A, B)$ és un $\mathbb{Z}$-mòdul lliure de rang finit ($\leq 4\dim(A)\dim(B)$).
- En particular, $\mathrm{End}(A)$ és un $\mathbb{Z}$-mòdul lliure finitament generat, d'on
$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$
és una $\mathbb{Q}$-àlgebra de dimensió finita.
- $\mathrm{End}^0(A)$ és l'objecte "natural" per estudiar $A$ llevat d'isogènia: Si $\varphi : A \to B$ és una isogènia, existeix $\psi : B \to A$ tal que $\psi \circ \varphi = n$, i
$$\mathrm{End}^0(A) \longrightarrow \mathrm{End}^0(B),\ \alpha \mapsto \varphi \circ \alpha \circ \psi$$
és un isomorfisme de $\mathbb{Q}$-àlgebres.

# L'àlgebra de $\mathbb{Q}$-endomorfismes d'una varietat abeliana

Siguin $A, B$ varietats abelianes sobre un cos $k$.

- El grup $\mathrm{Hom}(A, B)$ és un $\mathbb{Z}$-mòdul lliure de rang finit ($\leq 4\dim(A)\dim(B)$).
- En particular, $\mathrm{End}(A)$ és un $\mathbb{Z}$-mòdul lliure finitament generat, d'on
$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$
és una $\mathbb{Q}$-àlgebra de dimensió finita.
- $\mathrm{End}^0(A)$ és l'objecte "natural" per estudiar $A$ llevat d'isogènia: Si $\varphi : A \to B$ és una isogènia, existeix $\psi : B \to A$ tal que $\psi \circ \varphi = n$, i
$$\mathrm{End}^0(A) \longrightarrow \mathrm{End}^0(B),\ \alpha \mapsto \varphi \circ \alpha \circ \psi$$
és un isomorfisme de $\mathbb{Q}$-àlgebres.

$\rightsquigarrow$ $\mathrm{End}^0(A)$ només pot capturar propietats d'$A$ llevat d'isogènia!

# Representació en $T_\ell(A)$

- Sigui $\ell \neq \mathrm{char}(k)$, i considerem el mòdul de Tate $T_\ell(A) = \varprojlim A[\ell^n]$.
- $T_\ell(A)$ és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2\dim(A)$, on $G_k$ hi actua.
- Tot homomorfisme $\varphi : A \to B$ defineix un homomorfisme $T_\ell\varphi : T_\ell(A) \to T_\ell(B)$.

# Representació en $T_\ell(A)$

- Sigui $\ell \neq \mathrm{char}(k)$, i considerem el mòdul de Tate $T_\ell(A) = \varprojlim A[\ell^n]$.
- $T_\ell(A)$ és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2\dim(A)$, on $G_k$ hi actua.
- Tot homomorfisme $\varphi : A \to B$ defineix un homomorfisme $T_\ell\varphi : T_\ell(A) \to T_\ell(B)$.

**Teorema (Weil)**

*L'aplicació natural* $\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{G_k}(T_\ell(A), T_\ell(B))$ *és injectiva.*

**Teorema (Tate)**

*Si $k$ és finit, és bijectiva.*

# Representació en $T_\ell(A)$

- Sigui $\ell \neq \mathrm{char}(k)$, i considerem el mòdul de Tate $T_\ell(A) = \varprojlim A[\ell^n]$.
- $T_\ell(A)$ és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2\dim(A)$, on $G_k$ hi actua.
- Tot homomorfisme $\varphi : A \to B$ defineix un homomorfisme $T_\ell\varphi : T_\ell(A) \to T_\ell(B)$.

**Teorema (Weil)**

*L'aplicació natural* $\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{G_k}(T_\ell(A), T_\ell(B))$ *és injectiva.*

**Teorema (Tate)**

*Si $k$ és finit, és bijectiva.*

En particular, si $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, tenim

$$\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_k}(V_\ell(A)).$$

# Representació en $D_p(A)$

Suposem $A/k$, $k = \mathbb{F}_q$.
$W = W(k) =$ anell d'enters de l'extensió $\mathbb{Q}_{p^a}/\mathbb{Q}_p$.
$\sigma =$ automorfisme de $W$ que redueix a $x \mapsto x^p$ en $k$.
$D_k = W[F, V]$ l'anell de Dieudonné, on $F$, $V$ indeterminades satisfent

$$FV = VF = p,\ F\alpha = {}^{\sigma}\alpha F,\ \alpha V = V{}^{\sigma}\alpha \quad (\alpha \in W).$$

# Representació en $D_p(A)$

Suposem $A/k$, $k = \mathbb{F}_q$.
$W = W(k) =$ anell d'enters de l'extensió $\mathbb{Q}_{p^a}/\mathbb{Q}_p$.
$\sigma =$ automorfisme de $W$ que redueix a $x \mapsto x^p$ en $k$.
$D_k = W[F, V]$ l'anell de Dieudonné, on $F$, $V$ indeterminades satisfent

$$FV = VF = p,\ F\alpha = {}^{\sigma}\alpha F,\ \alpha V = V{}^{\sigma}\alpha \quad (\alpha \in W).$$

Associat al grup $p$-divisible $\varinjlim A[p^n]$ tenim el mòdul de Dieudonné $D_p(A)$, que és un $D_k$-mòdul.

# Representació en $D_p(A)$

Suposem $A/k$, $k = \mathbb{F}_q$.
$W = W(k) =$ anell d'enters de l'extensió $\mathbb{Q}_{p^a}/\mathbb{Q}_p$.
$\sigma =$ automorfisme de $W$ que redueix a $x \mapsto x^p$ en $k$.
$D_k = W[F, V]$ l'anell de Dieudonné, on $F$, $V$ indeterminades satisfent

$$FV = VF = p,\ F\alpha = {}^{\sigma}\alpha F,\ \alpha V = V{}^{\sigma}\alpha \quad (\alpha \in W).$$

Associat al grup $p$-divisible $\varinjlim A[p^n]$ tenim el mòdul de Dieudonné $D_p(A)$, que és un $D_k$-mòdul.

**Teorema (Tate)**

*Si $A, B$ són varietats abelianes sobre un cos finit $k$, l'aplicació*

$$\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \mathrm{Hom}_{D_k}(D_p(B), D_p(A)) \text{ és bijectiva.}$$

En particular, $\mathrm{End}^0(A) \otimes \mathbb{Q}_p \simeq \mathrm{End}(D_p(A) \otimes \mathbb{Q}_p)$.

# Reducció al cas simple

- Ja hem vist que si $A \sim B$ aleshores $\mathrm{End}^0(A) \simeq \mathrm{End}^0(B)$.
- D'altra banda, si $A \not\sim B$ es té que $\mathrm{Hom}(A, B) = 0$.

# Reducció al cas simple

- Ja hem vist que si $A \sim B$ aleshores $\mathrm{End}^0(A) \simeq \mathrm{End}^0(B)$.
- D'altra banda, si $A \not\sim B$ es té que $\mathrm{Hom}(A, B) = 0$.
- Per Poincaré-Weil, si $A$ descompon llevat d'isogènia com

$$A \sim A_1^{n_1} \times \cdots \times A_r^{n_r},\ A_i \text{ simples},\ A_i \not\sim A_j \text{ per } i \neq j,$$

aleshores

$$\mathrm{End}^0(A) \simeq \prod_i \mathrm{M}_{n_i}(\mathrm{End}^0(A_i)).$$

# Reducció al cas simple

- Ja hem vist que si $A \sim B$ aleshores $\mathrm{End}^0(A) \simeq \mathrm{End}^0(B)$.
- D'altra banda, si $A \not\sim B$ es té que $\mathrm{Hom}(A, B) = 0$.
- Per Poincaré-Weil, si $A$ descompon llevat d'isogènia com

$$A \sim A_1^{n_1} \times \cdots \times A_r^{n_r},\ A_i \text{ simples},\ A_i \not\sim A_j \text{ per } i \neq j,$$

aleshores

$$\mathrm{End}^0(A) \simeq \prod_i \mathrm{M}_{n_i}(\mathrm{End}^0(A_i)).$$

$\rightsquigarrow$ Bastarà estudiar $\mathrm{End}^0(A)$ per $A$ $k$-simple.

A més, en el cas $A$ $k$-simple, $E = \mathrm{End}^0(A)$ és de divisió, i per tant el seu centre és un cos.

# Descripció de l'àlgebra $E$

## Teorema

*Sigui $A$ una varietat abeliana $k$-simple, $k = \mathbb{F}_q$. Aleshores:*

(1) $f_A = m_A^e$, *amb* $e \geq 1$ *i* $m_A \in \mathbb{Z}[T]$ *mònic irreductible.*

(2) $\pi_A$ *és un $q$-enter de Weil.*

(3) $E = \mathrm{End}^0(A)$ *és una àlgebra de divisió amb centre* $K = \mathbb{Q}(\pi_A)$.

(4) $[E : \mathbb{Q}] = e^2[K : \mathbb{Q}]$ *i* $2\dim(A) = e[K : \mathbb{Q}]$.

(5) *Sigui $v$ una plaça de $K$, i $||\,||_v$ el seu valor absolut normalitzat. Si $||\pi_A||_v = q^{-i_v}$, aleshores $i_v = \mathrm{inv}_v(E)$. Explícitament:*

$$\mathrm{inv}_v(E) = \begin{cases} \frac{1}{2} & si\ v\ és\ real, \\ 0 & si\ v \nmid p, \\ \frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)}[K_v : \mathbb{Q}_p] & si\ v \mid p. \end{cases}$$

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

- Tenim $K = \mathbb{Q}(\pi_A) = \mathbb{Q}$ i $\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2$.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

- Tenim $K = \mathbb{Q}(\pi_A) = \mathbb{Q}$ i $\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2$.
- $E =$ àlgebra de quaternions ramificada en $\infty$ i $p$, $e = 2$.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

- Tenim $K = \mathbb{Q}(\pi_A) = \mathbb{Q}$ i $\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2$.
- $E =$ àlgebra de quaternions ramificada en $\infty$ i $p$, $e = 2$.
- $2\dim(A) = [E : K]^{1/2}[K : \mathbb{Q}] \Rightarrow \dim(A) = 1$.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

- Tenim $K = \mathbb{Q}(\pi_A) = \mathbb{Q}$ i $\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2$.
- $E =$ àlgebra de quaternions ramificada en $\infty$ i $p$, $e = 2$.
- $2\dim(A) = [E : K]^{1/2}[K : \mathbb{Q}] \Rightarrow \dim(A) = 1$.
- $f_A(T) = (T - p^{a/2})^2$, $a_p(A) = 2p^{a/2} \in p\mathbb{Z}$, $A$ supersingular.

# Exemples: cas real (I)

Suposem $\mathbb{Q}(\pi_A) \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Aleshores $\pi_A^2 = \pi_A \overline{\pi}_A = p^a$.

Suposem $a$ parell.

- Tenim $K = \mathbb{Q}(\pi_A) = \mathbb{Q}$ i $\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2$.
- $E =$ àlgebra de quaternions ramificada en $\infty$ i $p$, $e = 2$.
- $2\dim(A) = [E : K]^{1/2}[K : \mathbb{Q}] \Rightarrow \dim(A) = 1$.
- $f_A(T) = (T - p^{a/2})^2$, $a_p(A) = 2p^{a/2} \in p\mathbb{Z}$, $A$ supersingular.
- Per $\mathbb{Q}$-dimensions, $E = End_k^0(A) = \mathrm{End}_{\bar{k}}^0(A \times \bar{k})$.
  $\rightsquigarrow$ Per l'exhaustivitat del Teorema H-T, això ocorre per a tot $k$ !

# Exemples: cas real (II)

Suposem *a* senar.

# Exemples: cas real (II)

Suposem *a* senar.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$

# Exemples: cas real (II)

Suposem *a senar*.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$
- Com que hi ha un únic $\mathfrak{p} \mid p$, $E$ no ramifica en $\mathfrak{p}$.

# Exemples: cas real (II)

Suposem *a* senar.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$
- Com que hi ha un únic $\mathfrak{p} \mid p$, $E$ no ramifica en $\mathfrak{p}$.
- $E$ té ordre 2 en $\mathrm{Br}(K) \Rightarrow [E : K] = 4 \Rightarrow \dim(A) = 2$.

# Exemples: cas real (II)

Suposem *a* senar.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$
- Com que hi ha un únic $\mathfrak{p} \mid p$, $E$ no ramifica en $\mathfrak{p}$.
- $E$ té ordre 2 en $\mathrm{Br}(K) \Rightarrow [E : K] = 4 \Rightarrow \dim(A) = 2$.
- $f_A(T) = (T^2 - p^a)^2$ i el polinomi característic del $q^2$-Frobenius per $A$ en $k'/k$ quadràtica és $(T - p^a)^4$ .

# Exemples: cas real (II)

Suposem *a* senar.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$
- Com que hi ha un únic $\mathfrak{p} \mid p$, $E$ no ramifica en $\mathfrak{p}$.
- $E$ té ordre 2 en $\mathrm{Br}(K) \Rightarrow [E : K] = 4 \Rightarrow \dim(A) = 2$.
- $f_A(T) = (T^2 - p^a)^2$ i el polinomi característic del $q^2$-Frobenius per $A$ en $k'/k$ quadràtica és $(T - p^a)^4$ .
- Pel cas anterior aplicat sobre $k' = \mathbb{F}_{p^{2a}}$, existeix $A_0$ corba el·líptica supersingular amb $f_{A_0} = (T - p^a)^2$.

# Exemples: cas real (II)

Suposem *a* senar.

- Ara $K = \mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\sqrt{p})$ i tenim dues places reals amb
$$\mathrm{inv}_{\infty_1}(E) = \mathrm{inv}_{\infty_2}(E) = 1/2.$$
- Com que hi ha un únic $\mathfrak{p} \mid p$, $E$ no ramifica en $\mathfrak{p}$.
- $E$ té ordre 2 en $\mathrm{Br}(K) \Rightarrow [E : K] = 4 \Rightarrow \dim(A) = 2$.
- $f_A(T) = (T^2 - p^a)^2$ i el polinomi característic del $q^2$-Frobenius per $A$ en $k'/k$ quadràtica és $(T - p^a)^4$ .
- Pel cas anterior aplicat sobre $k' = \mathbb{F}_{p^{2a}}$, existeix $A_0$ corba el·líptica supersingular amb $f_{A_0} = (T - p^a)^2$.
- $A \times k' \sim_{k'} A_0 \times A_0$.

# Exemples: cas totalment imaginari

Suposem $K = \mathbb{Q}(\pi_A) \subseteq \mathbb{C}$ totalment imaginari. $\pi_A \overline{\pi}_A = q \Rightarrow \overline{\pi}_A = q/\pi_A$.

# Exemples: cas totalment imaginari

Suposem $K = \mathbb{Q}(\pi_A) \subseteq \mathbb{C}$ totalment imaginari. $\pi_A \overline{\pi}_A = q \Rightarrow \overline{\pi}_A = q/\pi_A$.

- $K \subseteq \mathbb{C}$ és un cos CM amb $K_0 = \mathbb{Q}(\pi_A + \overline{\pi}_A) \subseteq K$ subcòs real maximal.

# Exemples: cas totalment imaginari

Suposem $K = \mathbb{Q}(\pi_A) \subseteq \mathbb{C}$ totalment imaginari. $\pi_A \overline{\pi}_A = q \Rightarrow \overline{\pi}_A = q/\pi_A$.

- $K \subseteq \mathbb{C}$ és un cos CM amb $K_0 = \mathbb{Q}(\pi_A + \overline{\pi}_A) \subseteq K$ subcòs real maximal.
- $E$ és escindida a les places $v \nmid p$, i per a $v \mid p$ tenim que

$$\mathrm{inv}_v(E) + \mathrm{inv}_{\overline{v}}(E) = 0, \text{ si } \overline{v} \neq v,$$

$$\mathrm{inv}_v(E) = 0, \text{ si } \overline{v} = v.$$

# Exemples: cas totalment imaginari

Suposem $K = \mathbb{Q}(\pi_A) \subseteq \mathbb{C}$ totalment imaginari. $\pi_A \overline{\pi}_A = q \Rightarrow \overline{\pi}_A = q/\pi_A$.

- $K \subseteq \mathbb{C}$ és un cos CM amb $K_0 = \mathbb{Q}(\pi_A + \overline{\pi}_A) \subseteq K$ subcòs real maximal.
- $E$ és escindida a les places $v \nmid p$, i per a $v \mid p$ tenim que
$$\mathrm{inv}_v(E) + \mathrm{inv}_{\overline{v}}(E) = 0, \text{ si } \overline{v} \neq v,$$
$$\mathrm{inv}_v(E) = 0, \text{ si } \overline{v} = v.$$
- Si $k = \mathbb{F}_p$, $E$ escindeix arreu ja que $\mathrm{ord}_v(\pi_A)/\mathrm{ord}_v(p)$ és un múltiple enter de $1/e_v$ i $e_v \mid [K_v : \mathbb{Q}_p]$.
$\Rightarrow E = K$, en particular $\mathrm{End}_k(A)$ és commutatiu.

# Determinació del centre d'$E$

- $E$ de divisió $\Rightarrow Z(E)$ és un cos. Com que $\pi_A$ commuta amb tots els endomorfismes d'$A$, tenim que $K = \mathbb{Q}(\pi_A) \subseteq Z(E)$.

# Determinació del centre d'$E$

- $E$ de divisió $\Rightarrow Z(E)$ és un cos. Com que $\pi_A$ commuta amb tots els endomorfismes d'$A$, tenim que $K = \mathbb{Q}(\pi_A) \subseteq Z(E)$.
- Sigui $\ell \neq p$, $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Pel Teorema d'Isogènia de Tate,
$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_k}(V_\ell(A)).$$

# Determinació del centre d'$E$

- $E$ de divisió $\Rightarrow Z(E)$ és un cos. Com que $\pi_A$ commuta amb tots els endomorfismes d'$A$, tenim que $K = \mathbb{Q}(\pi_A) \subseteq Z(E)$.
- Sigui $\ell \neq p$, $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Pel Teorema d'Isogènia de Tate,
$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_k}(V_\ell(A)).$$
- $G_k$ està generat topològicament pel Frobenius, d'on se segueix que
$$C_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))}(K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = \mathrm{End}_{G_k}(V_\ell(A)) \simeq E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

# Determinació del centre d'$E$

- $E$ de divisió $\Rightarrow Z(E)$ és un cos. Com que $\pi_A$ commuta amb tots els endomorfismes d'$A$, tenim que $K = \mathbb{Q}(\pi_A) \subseteq Z(E)$.
- Sigui $\ell \neq p$, $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Pel Teorema d'Isogènia de Tate,
$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_k}(V_\ell(A)).$$
- $G_k$ està generat topològicament pel Frobenius, d'on se segueix que
$$C_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))}(K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = \mathrm{End}_{G_k}(V_\ell(A)) \simeq E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$
- Pel Teorema del Centralitzador Doble,
$$C_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))}(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell,$$
d'on es dedueix que el centre de $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ és $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, i per tant
$$Z(E) = K = \mathbb{Q}(\pi).$$

# Dimensió de l'àlgebra $E$

- $\deg(f_A) = 2\dim(A)$ i $\deg(m_A) = [K : \mathbb{Q}] \Rightarrow 2\dim(A) = e[K : \mathbb{Q}]$.

# Dimensió de l'àlgebra $E$

- $\deg(f_A) = 2\dim(A)$ i $\deg(m_A) = [K:\mathbb{Q}] \Rightarrow 2\dim(A) = e[K:\mathbb{Q}]$.
- Per provar $[E:\mathbb{Q}] = e^2[K:\mathbb{Q}]$, siguin $A, B/k$. $\pi_A, \pi_B \rightsquigarrow f_A, f_B$.

# Dimensió de l'àlgebra $E$

- $\deg(f_A) = 2\dim(A)$ i $\deg(m_A) = [K:\mathbb{Q}] \Rightarrow 2\dim(A) = e[K:\mathbb{Q}]$.
- Per provar $[E:\mathbb{Q}] = e^2[K:\mathbb{Q}]$, siguin $A, B/k$. $\pi_A, \pi_B \rightsquigarrow f_A, f_B$.
- Sigui $F/\mathbb{Q}$, i considerem les factoritzacions

$$f_A = \prod_h h^{a(h)}, \quad f_B = \prod_h h^{b(h)}$$

en polinomis irreductibles sobre $F$. L'enter

$$r(f_A, f_B) = \sum_h a(h)b(h)\deg(h)$$

no depèn del cos $F$.

# Dimensió de l'àlgebra $E$

- $\deg(f_A) = 2\dim(A)$ i $\deg(m_A) = [K:\mathbb{Q}] \Rightarrow 2\dim(A) = e[K:\mathbb{Q}]$.
- Per provar $[E:\mathbb{Q}] = e^2[K:\mathbb{Q}]$, siguin $A, B/k$. $\pi_A, \pi_B \rightsquigarrow f_A, f_B$.
- Sigui $F/\mathbb{Q}$, i considerem les factoritzacions
$$f_A = \prod_h h^{a(h)}, \quad f_B = \prod_h h^{b(h)}$$
en polinomis irreductibles sobre $F$. L'enter
$$r(f_A, f_B) = \sum_h a(h)b(h)\deg(h)$$
no depèn del cos $F$.
- Prenem $F = \mathbb{Q}_\ell$. $\pi_A, \pi_B$ indueixen endomorfismes en els mòduls semisimples $V_\ell(A), V_\ell(B)$, amb polinomis característics $f_A, f_B$, d'on
$$\dim \mathrm{Hom}_{G_k}(V_\ell(A), V_\ell(B)) = r(f_A, f_B).$$

# Dimensió de l'àlgebra $E$

- $\deg(f_A) = 2\dim(A)$ i $\deg(m_A) = [K:\mathbb{Q}] \Rightarrow 2\dim(A) = e[K:\mathbb{Q}]$.
- Per provar $[E:\mathbb{Q}] = e^2[K:\mathbb{Q}]$, siguin $A, B/k$. $\pi_A, \pi_B \rightsquigarrow f_A, f_B$.
- Sigui $F/\mathbb{Q}$, i considerem les factoritzacions
$$f_A = \prod_h h^{a(h)}, \quad f_B = \prod_h h^{b(h)}$$
en polinomis irreductibles sobre $F$. L'enter
$$r(f_A, f_B) = \sum_h a(h)b(h)\deg(h)$$
no depèn del cos $F$.
- Prenem $F = \mathbb{Q}_\ell$. $\pi_A, \pi_B$ indueixen endomorfismes en els mòduls semisimples $V_\ell(A), V_\ell(B)$, amb polinomis característics $f_A, f_B$, d'on
$$\dim \mathrm{Hom}_{G_k}(V_\ell(A), V_\ell(B)) = r(f_A, f_B).$$
- Aplicant això al cas $A$ simple, $f_A = m_A^e$:
$$\dim_{\mathbb{Q}_\ell}(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = \dim \mathrm{End}_{G_k}(V_\ell(A)) = r(f_A, f_A) = e^2 \deg(m_A),$$
d'on $[E:\mathbb{Q}] = e^2[K:\mathbb{Q}]$.

# Cas $v \nmid p$, $v$ finita

$v$ plaça finita de $K = \mathbb{Q}(\pi_A)$, $v \mid \ell$ amb $\ell \neq p$.

# Cas $v \nmid p$, $v$ finita

$v$ plaça finita de $K = \mathbb{Q}(\pi_A)$, $v \mid \ell$ amb $\ell \neq p$.

- $f_A = m_A^e \Rightarrow V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ és un mòdul lliure de rang $e$ sobre $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

# Cas $v \nmid p$, $v$ finita

$v$ plaça finita de $K = \mathbb{Q}(\pi_A)$, $v \mid \ell$ amb $\ell \neq p$.

- $f_A = m_A^e \Rightarrow V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ és un mòdul lliure de rang $e$ sobre $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
- Pel Teorema de Tate,

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathrm{End}_{G_k}(V_\ell(A)).$$

# Cas $v \nmid p$, $v$ finita

$v$ plaça finita de $K = \mathbb{Q}(\pi_A)$, $v \mid \ell$ amb $\ell \neq p$.

- $f_A = m_A^e \Rightarrow V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ és un mòdul lliure de rang $e$ sobre $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
- Pel Teorema de Tate,

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathrm{End}_{G_k}(V_\ell(A)).$$

- Però $G_k$ està generat topològicament pel Frobenius, d'on

$$\mathrm{End}_{G_k}(V_\ell(A)) \simeq \mathrm{End}_{K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{M}_e(K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell).$$

# Cas $v \nmid p$, $v$ finita

$v$ plaça finita de $K = \mathbb{Q}(\pi_A)$, $v \mid \ell$ amb $\ell \neq p$.

- $f_A = m_A^e \Rightarrow V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ és un mòdul lliure de rang $e$ sobre $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
- Pel Teorema de Tate,

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathrm{End}_{G_k}(V_\ell(A)).$$

- Però $G_k$ està generat topològicament pel Frobenius, d'on

$$\mathrm{End}_{G_k}(V_\ell(A)) \simeq \mathrm{End}_{K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{M}_e(K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell).$$

$\rightsquigarrow$ $E_v = E \otimes_K K_v$ esdevé una àlgebra de matrius, i.e. $\mathrm{inv}_v(E) = 0$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$
- $a$ senar $\Rightarrow K \simeq \mathbb{Q}(\sqrt{p})$ quadràtic real.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$
- $a$ senar $\Rightarrow K \simeq \mathbb{Q}(\sqrt{p})$ quadràtic real.
  - $f_A(T) = (T^2 - q)^e$ per algun $e \geq 1$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$
- $a$ senar $\Rightarrow K \simeq \mathbb{Q}(\sqrt{p})$ quadràtic real.
  - $f_A(T) = (T^2 - q)^e$ per algun $e \geq 1$.
  - Sobre $k'/k$ quadràtica, $A' = A \times k'$, $f_{A'}(T) = (T - q)^{2e}$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$
- $a$ senar $\Rightarrow K \simeq \mathbb{Q}(\sqrt{p})$ quadràtic real.
  - $f_A(T) = (T^2 - q)^e$ per algun $e \geq 1$.
  - Sobre $k'/k$ quadràtica, $A' = A \times k'$, $f_{A'}(T) = (T - q)^{2e}$.
  - $A' \sim_{k'} A_0 \times A_0$, $E' = \mathrm{End}^0_{k'}(A') = \mathrm{M}_2(B_p)$, on $B_p$ àlgebra de quaternions racional ramificada exactament en $\infty$ i $p$.

# Cas $v$ real

Suposem $K = \mathbb{Q}(\pi_A)$ té una plaça real $v$, $\pi_A$ arrel de $T^2 - q = T^2 - p^a$.

- $a$ parell $\Rightarrow K = \mathbb{Q}$, $v = \infty$.
  - Per dimensions, no pot ser $E = K = \mathbb{Q}$.
  - Però $E$ és de divisió, per tant ha de ser
$$\mathrm{inv}_\infty(E) = \mathrm{inv}_p(E) = 1/2.$$
- $a$ senar $\Rightarrow K \simeq \mathbb{Q}(\sqrt{p})$ quadràtic real.
  - $f_A(T) = (T^2 - q)^e$ per algun $e \geq 1$.
  - Sobre $k'/k$ quadràtica, $A' = A \times k'$, $f_{A'}(T) = (T - q)^{2e}$.
  - $A' \sim_{k'} A_0 \times A_0$, $E' = \mathrm{End}^0_{k'}(A') = \mathrm{M}_2(B_p)$, on $B_p$ àlgebra de quaternions racional ramificada exactament en $\infty$ i $p$.
  - $E$ és el centralitzador de $K$ en $E'$, i $E \sim E' \otimes_{\mathbb{Q}} K \sim B_p \otimes_{\mathbb{Q}} K$ en $\mathrm{Br}(K)$, d'on $E$ no escindeix en cap plaça real de $K$.

# Cas $v \mid p$ (I)

- Escrivim $L := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Llavors $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ és un mòdul sobre
$$R = L[F, V] = L[F, (1/p)F^{-1}] = L[F, F^{-1}].$$

# Cas $v \mid p$ (I)

- Escrivim $L := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Llavors $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ és un mòdul sobre
$$R = L[F, V] = L[F, (1/p)F^{-1}] = L[F, F^{-1}].$$
- Podem escriure $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ com a suma directa de $R$-mòduls indescomponibles no isomorfs
$$D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \oplus_i V_i^{n_i}, \qquad V_i^{r_i} \simeq R/m_i(F^a)R,$$
amb els $m_i$ potència d'irreductible.

# Cas $v \mid p$ (I)

- Escrivim $L := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Llavors $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ és un mòdul sobre
$$R = L[F, V] = L[F, (1/p)F^{-1}] = L[F, F^{-1}].$$
- Podem escriure $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ com a suma directa de $R$-mòduls indescomponibles no isomorfs
$$D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \oplus_i V_i^{n_i}, \qquad V_i^{r_i} \simeq R/m_i(F^a)R,$$
amb els $m_i$ potència d'irreductible.
- $\pi_A$ actua en $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ com $F^a$, i el polinomi mínim sobre $\mathbb{Q}_p$ de $F^a$ en $\oplus V_i^{n_i}$ és el mcm dels $m_i$, que divideix $m_A \Rightarrow$ els $m_i$ són irreductibles i sense arrels comunes.

# Cas $v \mid p$ (I)

- Escrivim $L := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Llavors $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ és un mòdul sobre
$$R = L[F, V] = L[F, (1/p)F^{-1}] = L[F, F^{-1}].$$
- Podem escriure $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ com a suma directa de $R$-mòduls indescomponibles no isomorfs
$$D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \oplus_i V_i^{n_i}, \qquad V_i^{r_i} \simeq R/m_i(F^a)R,$$
amb els $m_i$ potència d'irreductible.
- $\pi_A$ actua en $D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ com $F^a$, i el polinomi mínim sobre $\mathbb{Q}_p$ de $F^a$ en $\oplus V_i^{n_i}$ és el mcm dels $m_i$, que divideix $m_A \Rightarrow$ els $m_i$ són irreductibles i sense arrels comunes.
- Suposem que $v$ correspon al factor $m_i$ de $m_A$ sobre $\mathbb{Q}_p$. L'àlgebra $R/m_i(F^a)R$ és simple i central sobre $K_v$, i es pot escriure com $L \otimes K_v[F]$ amb
$$F^a = \pi_A \in K_v,\ F(\alpha \otimes \varphi) = ({}^\sigma\alpha \otimes \varphi)F.$$

# Cas $v \mid p$ (II)

- $f_v = f(K_v/\mathbb{Q}_p)$, $g = (f_v, a)$, $g = [L \cap K_v : \mathbb{Q}_p]$, $a/g = [LK_v : \mathbb{Q}_p]$.

# Cas $v \mid p$ (II)

- $f_v = f(K_v/\mathbb{Q}_p)$, $g = (f_v, a)$, $g = [L \cap K_v : \mathbb{Q}_p]$, $a/g = [LK_v : \mathbb{Q}_p]$.
- Es té un isomorfisme $L \otimes K_v[F] \simeq \mathrm{M}_g(S)$, on

$$S = LK_v[F'] \text{ amb } (F')^{a/g} = \pi_A \in K_v,\ F'(\alpha\varphi) = ({}^{\sigma^g}\alpha\varphi)F'.$$

# Cas $v \mid p$ (II)

- $f_v = f(K_v/\mathbb{Q}_p)$, $g = (f_v, a)$, $g = [L \cap K_v : \mathbb{Q}_p]$, $a/g = [LK_v : \mathbb{Q}_p]$.
- Es té un isomorfisme $L \otimes K_v[F] \simeq \mathrm{M}_g(S)$, on
$$S = LK_v[F'] \text{ amb } (F')^{a/g} = \pi_A \in K_v,\ F'(\alpha\varphi) = ({}^{\sigma^g}\alpha\varphi)F'.$$
- L'àlgebra $S$ és cíclica i
$$\mathrm{inv}_{K_v}(S) = \frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)}[K_v : \mathbb{Q}_p].$$

Però

$$\begin{aligned}
\mathrm{inv}_{K_v}(S) &= \mathrm{inv}_{K_v}(L \otimes K_v[F]) = \mathrm{inv}_{K_v}(R/m_i(F^a)R) = \\
&= -\mathrm{inv}_{K_v}(\mathrm{End}(V_i^{r_i})) = -\mathrm{inv}_{K_v}(\mathrm{End}(V_i^{n_i})) = \\
&= -\mathrm{inv}_v(\mathrm{End}_R(D_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)) = \\
&= \mathrm{inv}_v(E \otimes_{\mathbb{Q}} \mathbb{Q}_p).
\end{aligned}$$

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

- Suposem $A, B$ varietats abelianes amb $\pi_A = \pi_B$ en $W(q)$ mòdul conjugació.

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

- Suposem $A, B$ varietats abelianes amb $\pi_A = \pi_B$ en $W(q)$ mòdul conjugació.
- Com que $A$ és simple, tenim que $f_A = h^n$ amb $h \in \mathbb{Q}[T]$ irreductible.

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

- Suposem $A, B$ varietats abelianes amb $\pi_A = \pi_B$ en $W(q)$ mòdul conjugació.
- Com que $A$ és simple, tenim que $f_A = h^n$ amb $h \in \mathbb{Q}[T]$ irreductible.
- D'altra banda, per ser $B$ simple i $\pi_A = \pi_B$, tenim que $f_B = h^m$.

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

- Suposem $A, B$ varietats abelianes amb $\pi_A = \pi_B$ en $W(q)$ mòdul conjugació.
- Com que $A$ és simple, tenim que $f_A = h^n$ amb $h \in \mathbb{Q}[T]$ irreductible.
- D'altra banda, per ser $B$ simple i $\pi_A = \pi_B$, tenim que $f_B = h^m$.
- Podem suposar $m \leq n$, i llavors $f_B \mid f_A$ i $B$ és isògena a una subvarietat de $A$.

# Injectivitat

La injectivitat de l'aplicació $A \mapsto \pi_A$ se segueix fàcilment del Teorema de Tate a l'inici:

- Suposem $A, B$ varietats abelianes amb $\pi_A = \pi_B$ en $W(q)$ mòdul conjugació.
- Com que $A$ és simple, tenim que $f_A = h^n$ amb $h \in \mathbb{Q}[T]$ irreductible.
- D'altra banda, per ser $B$ simple i $\pi_A = \pi_B$, tenim que $f_B = h^m$.
- Podem suposar $m \leq n$, i llavors $f_B \mid f_A$ i $B$ és isògena a una subvarietat de $A$.
- Però $A$ és simple, d'on $A \sim B$.

# Exhaustivitat: $q$-enters de Weil efectius

## Definició

*Direm que $\pi \in W(q)$ és efectiu si $\pi$ és conjugat a l'endomorfisme de Frobenius $\pi_A$ d'alguna varietat simple definida sobre $k$.*

# Exhaustivitat: $q$-enters de Weil efectius

## Definició

*Direm que $\pi \in W(q)$ és efectiu si $\pi$ és conjugat a l'endomorfisme de Frobenius $\pi_A$ d'alguna varietat simple definida sobre $k$.*

Podem admetre $A$ isotípica ($A \sim A_0^n$) en la definició. El Frobenius $\pi_A$ genera un subcòs central de $\mathrm{End}^0(A)$ i preserva $A_0$, on hi actua com $\pi_{A_0}$.

# Exhaustivitat: $q$-enters de Weil efectius

## Definició

*Direm que $\pi \in W(q)$ és efectiu si $\pi$ és conjugat a l'endomorfisme de Frobenius $\pi_A$ d'alguna varietat simple definida sobre $k$.*

Podem admetre $A$ isotípica ($A \sim A_0^n$) en la definició. El Frobenius $\pi_A$ genera un subcòs central de $\mathrm{End}^0(A)$ i preserva $A_0$, on hi actua com $\pi_{A_0}$.

## Lema

*$N \geq 1$ enter. $\pi^N$ efectiu $\Rightarrow \pi$ efectiu.*

# Exhaustivitat: $q$-enters de Weil efectius

## Definició

*Direm que $\pi \in W(q)$ és efectiu si $\pi$ és conjugat a l'endomorfisme de Frobenius $\pi_A$ d'alguna varietat simple definida sobre $k$.*

Podem admetre $A$ isotípica ($A \sim A_0^n$) en la definició. El Frobenius $\pi_A$ genera un subcòs central de $\mathrm{End}^0(A)$ i preserva $A_0$, on hi actua com $\pi_{A_0}$.

## Lema

*$N \geq 1$ enter. $\pi^N$ efectiu $\Rightarrow \pi$ efectiu.*

Prenem $\pi \in W(q)$. Sigui $E$ l'àlgebra de divisió central sobre $K = \mathbb{Q}(\pi)$ verificant les propietats del Teorema que ens descriu l'àlgebra $\mathrm{End}^0(A)$ en termes de $\pi_A$.

# Exhaustivitat: $q$-enters de Weil efectius

## Definició

*Direm que $\pi \in W(q)$ és efectiu si $\pi$ és conjugat a l'endomorfisme de Frobenius $\pi_A$ d'alguna varietat simple definida sobre $k$.*

Podem admetre $A$ isotípica ($A \sim A_0^n$) en la definició. El Frobenius $\pi_A$ genera un subcòs central de $\mathrm{End}^0(A)$ i preserva $A_0$, on hi actua com $\pi_{A_0}$.

## Lema

*$N \geq 1$ enter. $\pi^N$ efectiu $\Rightarrow \pi$ efectiu.*

Prenem $\pi \in W(q)$. Sigui $E$ l'àlgebra de divisió central sobre $K = \mathbb{Q}(\pi)$ verificant les propietats del Teorema que ens descriu l'àlgebra $\mathrm{End}^0(A)$ en termes de $\pi_A$.

$\rightsquigarrow$ Es tracta de construir $A$ amb $\pi_A \sim \pi$ !

# Varietats abelianes amb CM

**Lema**

*Existeix un cos CM $L \supseteq K$ tal que $L$ escindeix $E$ i $[L : K] = [E : K]^{1/2}$.*

# Varietats abelianes amb CM

## Lema

*Existeix un cos CM $L \supseteq K$ tal que $L$ escindeix $E$ i $[L : K] = [E : K]^{1/2}$.*

## Definició

*Sigui $A$ una varietat abeliana definida sobre un cos $F$, i $L$ un cos de nombres. Direm que $A$ és de tipus $(L)$ si existeix un morfisme d'anells $i : L \to \mathrm{End}_F^0(A)$ i $[L : \mathbb{Q}] = 2\dim(A)$.*
*Quan $L$ és un cos CM també es diu que $A$ té CM per $L$.*

# Varietats abelianes amb CM

## Lema

*Existeix un cos CM $L \supseteq K$ tal que $L$ escindeix $E$ i $[L : K] = [E : K]^{1/2}$.*

## Definició

*Sigui $A$ una varietat abeliana definida sobre un cos $F$, i $L$ un cos de nombres. Direm que $A$ és de tipus $(L)$ si existeix un morfisme d'anells $i : L \to \mathrm{End}_F^0(A)$ i $[L : \mathbb{Q}] = 2\dim(A)$.*
*Quan $L$ és un cos CM també es diu que $A$ té CM per $L$.*

Es tracta de construir una varietat abeliana sobre $\mathbb{C}$ amb CM per $L$, realitzar-la sobre una extensió finita de $\mathbb{Q}_p$ i reduir-la per obtenir una varietat abeliana sobre una extensió de $\mathbb{F}_p$.

# Tipus CM

$L$ cos CM amb $[L:\mathbb{Q}] = 2\dim(A)$, i $\rho$ l'automorfisme de grau 2 induït per la conjugació complexa. $C$ cos algebraicament tancat de característica 0.

# Tipus CM

$L$ cos CM amb $[L:\mathbb{Q}] = 2\dim(A)$, i $\rho$ l'automorfisme de grau 2 induït per la conjugació complexa. $C$ cos algebraicament tancat de característica 0. Un tipus CM per a $L$ és un subconjunt $\Phi \subseteq \mathrm{Hom}(L, C)$ tal que

$$\Phi \cap \Phi\rho = \emptyset, \qquad \Phi \cup \Phi\rho = \mathrm{Hom}(L, C).$$

# Tipus CM

$L$ cos CM amb $[L:\mathbb{Q}] = 2\dim(A)$, i $\rho$ l'automorfisme de grau 2 induït per la conjugació complexa. $C$ cos algebraicament tancat de característica 0. Un tipus CM per a $L$ és un subconjunt $\Phi \subseteq \mathrm{Hom}(L, C)$ tal que

$$\Phi \cap \Phi\rho = \emptyset, \qquad \Phi \cup \Phi\rho = \mathrm{Hom}(L, C).$$

## Definició

*Una varietat abeliana $A$ sobre un subcòs $F \subseteq C$ és de tipus $(L, \Phi)$ si $A$ és de tipus $(L)$ sobre $F$ i la representació de $L$ en l'espai tangent $t_{A_C}$ factoritza per $\prod_{\phi\in\Phi} C_\phi$, on $L$ actua en $C_\phi = C$ via $\phi$.*

# Tipus CM

$L$ cos CM amb $[L:\mathbb{Q}] = 2\dim(A)$, i $\rho$ l'automorfisme de grau 2 induït per la conjugació complexa. $C$ cos algebraicament tancat de característica 0. Un tipus CM per a $L$ és un subconjunt $\Phi \subseteq \mathrm{Hom}(L, C)$ tal que

$$\Phi \cap \Phi\rho = \emptyset, \qquad \Phi \cup \Phi\rho = \mathrm{Hom}(L, C).$$

## Definició

*Una varietat abeliana $A$ sobre un subcòs $F \subseteq C$ és de tipus $(L, \Phi)$ si $A$ és de tipus $(L)$ sobre $F$ i la representació de $L$ en l'espai tangent $t_{A_C}$ factoritza per $\prod_{\phi\in\Phi} C_\phi$, on $L$ actua en $C_\phi = C$ via $\phi$.*

## Lema

*Existeix un esquema abelià de tipus $(L, \Phi)$ definit sobre l'anell d'enters d'un cos de nombres contingut en $C$.*

# Tipus CM

Prenem $C$ una clausura algebraica de $\mathbb{Q}_p$, i sigui $w \mid p$ una plaça de $L$.
Identifiquem $\mathrm{Hom}_{\mathbb{Q}_p}(L_w, C) \xrightarrow{\simeq} H_w \subseteq \mathrm{Hom}(L, C)$, i posem $\Phi_w = \Phi \cap H_w$.
Es té una descomposició $\mathbb{Q}_p \otimes_{\mathbb{Q}} L = \prod_{w|p} L_w$ i particions

$$\mathrm{Hom}(L, C) = \bigcup_{w|p} H_w, \quad \Phi = \bigcup_{w|p} \Phi_w.$$

# Tipus CM

Prenem $C$ una clausura algebraica de $\mathbb{Q}_p$, i sigui $w \mid p$ una plaça de $L$. Identifiquem $\mathrm{Hom}_{\mathbb{Q}_p}(L_w, C) \xrightarrow{\sim} H_w \subseteq \mathrm{Hom}(L, C)$, i posem $\Phi_w = \Phi \cap H_w$. Es té una descomposició $\mathbb{Q}_p \otimes_{\mathbb{Q}} L = \prod_{w|p} L_w$ i particions

$$\mathrm{Hom}(L, C) = \bigcup_{w|p} H_w, \quad \Phi = \bigcup_{w|p} \Phi_w.$$

## Lema (Shimura-Taniyama)

*Sigui $A$ esquema abelià de tipus $(L, \Phi)$ definit sobre l'anell d'enters $\mathcal{O}$ d'una extensió finita de $\mathbb{Q}_p$, i $k_0 = \mathbb{F}_{q_0}$ el cos residual de $\mathcal{O}$. Sigui $A_0$ la reducció de $A$ mòdul l'ideal maximal de $\mathcal{O}$. Existeix un element $\pi_0 \in L$ tal que $i(\pi_0) \in \mathrm{End}(A)$ indueix $\pi_{A_0} \in \mathrm{End}^0_{k_0}(A_0)$, i*

$$\frac{\mathrm{ord}_w(\pi_0)}{\mathrm{ord}_w(q_0)} = \frac{\sharp \Phi_w}{\sharp H_w} = \frac{\sharp \Phi_w}{[L_w : \mathbb{Q}_p]} \quad \textit{per a tota } w \mid p.$$

# Últim pas: escollir un bon tipus CM

Finalment, fent servir que $L \supseteq K$ escindeix $E$ i que coneixem els invariants $\mathrm{inv}_v(E)$ en les places $v \mid p$ de $K$, es prova que es pot escollir $\Phi$ de tal manera que

$$\frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)} = \frac{\sharp\Phi_w}{\sharp H_w} = \frac{\mathrm{ord}_w(\pi_0)}{\mathrm{ord}_w(q_0)}.$$

# Últim pas: escollir un bon tipus CM

Finalment, fent servir que $L \supseteq K$ escindeix $E$ i que coneixem els invariants $\mathrm{inv}_v(E)$ en les places $v \mid p$ de $K$, es prova que es pot escollir $\Phi$ de tal manera que

$$\frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)} = \frac{\sharp\Phi_w}{\sharp H_w} = \frac{\mathrm{ord}_w(\pi_0)}{\mathrm{ord}_w(q_0)}.$$

I d'aquesta igualtat és senzill deduir que $\pi^N = \pi_0^{N_0}$ per alguns enters $N, N_0 \geq 1$, d'on es té que $\pi$ és efectiu.

# Referències


- K. Eisentrager, The theorem of Honda and Tate, http://math.stanford.edu/conrad/hondatate.pdf.
- T. Honda, Isogeny classes of abelian varieties over finite fields, *Journ. Math. Soc. Japan*, **20**, 83-95, (1968).
- D. Mumford, Abelian varieties. With appendices by C. P. Ramanujam and Yuri Manin. Corrected reprint of the second (1974) edition. Tata Institute of Fundamental Research Studies in Mathematics, 5.
- J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.*, **2**, 134-144, (1966).
- J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), *Séminaire Bourbaki*, **21**, 95-110, (1968).
- W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* **2**(4), 521-560, (1969).
- W. C. Waterhouse, J. S. Milne, Abelian varieties over finite fields. 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), 53-64, *Amer. Math. Soc.*, (1971).

# Teoria d'Honda-Tate

Carlos de Vera Piquero

Departament de Matemàtica Aplicada 2, UPC

STNB 2012 - Varietats abelianes mòdul p
26 de gener