Isogeny classes of rational squares of CM elliptic curves

Francesc Fité[1] (UPC/BGSMath) and Xavier Guitart (UB)

BIRS, Banff, 31st May 2017.

[1]Funded by Maria de Maeztu Grant (MDM-2014-0445)

A conjecture

- F is a number field.
- A/F is an abelian variety
- Call $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ the *endomorphism algebra* of $A_{\overline{\mathbb{Q}}}$.
- For any $g, d \geq 1$, set

$$\mathcal{L}_{g,d} = \{\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \,|\, \dim(A) = g \text{ and } [F:\mathbb{Q}] = d\}/\simeq\ .$$

Conjecture

For every $g, d \geq 1$, the set $\mathcal{L}_{g,d}$ is finite.

(Attributed to Coleman; for example in a paper of Bruin-Flynn-González-Rotger.)

A conjecture

- F is a number field.
- A/F is an abelian variety
- Call $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ the *endomorphism algebra* of $A_{\overline{\mathbb{Q}}}$.
- For any $g, d \geq 1$, set

$$\mathcal{L}_{g,d} = \{\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \mid \dim(A) = g \text{ and } [F:\mathbb{Q}] = d\}/\simeq \ .$$

Conjecture

For every $g, d \geq 1$, the set $\mathcal{L}_{g,d}$ is finite.

(Attributed to Coleman; for example in a paper of Bruin-Flynn-González-Rotger.)

A conjecture

- F is a number field.
- A/F is an abelian variety
- Call $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ the *endomorphism algebra* of $A_{\overline{\mathbb{Q}}}$.
- For any $g, d \geq 1$, set

$$\mathcal{L}_{g,d} = \{\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \,|\, \dim(A) = g \text{ and } [F:\mathbb{Q}] = d\}/\simeq \, .$$

Conjecture

For every $g, d \geq 1$, the set $\mathcal{L}_{g,d}$ is finite.

(Attributed to Coleman; for example in a paper of Bruin-Flynn-González-Rotger.)

A conjecture

- F is a number field.
- A/F is an abelian variety
- Call $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ the *endomorphism algebra* of $A_{\overline{\mathbb{Q}}}$.
- For any $g, d \geq 1$, set

$$\mathcal{L}_{g,d} = \{\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \mid \dim(A) = g \text{ and } [F : \mathbb{Q}] = d\}/\simeq \ .$$

Conjecture

For every $g, d \geq 1$, the set $\mathcal{L}_{g,d}$ is finite.

(Attributed to Coleman; for example in a paper of Bruin-Flynn-González-Rotger.)

A conjecture

- F is a number field.
- A/F is an abelian variety
- Call $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ the *endomorphism algebra* of $A_{\overline{\mathbb{Q}}}$.
- For any $g, d \geq 1$, set

$$\mathcal{L}_{g,d} = \{\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \,|\, \dim(A) = g \text{ and } [F : \mathbb{Q}] = d\}/\simeq \ .$$

Conjecture

For every $g, d \geq 1$, the set $\mathcal{L}_{g,d}$ is finite.

(Attributed to Coleman; for example in a paper of Bruin-Flynn-González-Rotger.)

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M)$$

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}$$

Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}\,.$$

Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}\,.$$

Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}\,.$$

Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}\,.$$

Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

An open question

Example: $g = d = 1$

$$\#\mathcal{L}_{1,1} = 10\,.$$

Indeed:

- $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ is $\mathbb{Q}$ if A does not have CM.
- If $A/\mathbb{Q}$ has CM by M, then

$$\mathrm{Cl}(M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Gal}(M(j_A)/M) \simeq \{1\}\,.$$

  Thus there are 9 possibilities for M.

Problem

What is the set $\mathcal{L}_{2,1}$?

Endomorphism algebras of abelian surfaces

Let A be an abelian surface over $\mathbb{Q}$.

Dec. of $A_{\overline{\mathbb{Q}}}$	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\#$Possibilities
$A_{\overline{\mathbb{Q}}}$ is simple	$\mathbb{Q}$ real quad. field indef. div. quat. alg./$\mathbb{Q}$ quartic CM field	1 ? ? 13 (Murabayashi-Umegaki, Bisson-Kilicer-Streng)
$A_{\overline{\mathbb{Q}}} \sim E \times E'$ and $E \not\sim E'$	$\mathbb{Q} \times \mathbb{Q}$ $\mathbb{Q} \times M_1$, M_i quad. imag. $M_1 \times M_2$	1 9, since $\#\mathrm{Cl}(M_i) = 1$ 36
$A_{\overline{\mathbb{Q}}} \sim E^2$	$\mathrm{M}_2(\mathbb{Q})$ $\mathrm{M}_2(M)$, M quad. imag.	

Endomorphism algebras of abelian surfaces

Let A be an abelian surface over $\mathbb{Q}$.

Dec. of $A_{\overline{\mathbb{Q}}}$	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\#$Possibilities
$A_{\overline{\mathbb{Q}}}$ is simple	$\mathbb{Q}$ real quad. field indef. div. quat. alg./$\mathbb{Q}$ quartic CM field	1 ? ? 13 (Murabayashi-Umegaki, Bisson-Kilicer-Streng)
$A_{\overline{\mathbb{Q}}} \sim E \times E'$ and $E \not\sim E'$	$\mathbb{Q} \times \mathbb{Q}$ $\mathbb{Q} \times M_1$, M_i quad. imag. $M_1 \times M_2$	1 9, since $\#\mathrm{Cl}(M_i) = 1$ 36
$A_{\overline{\mathbb{Q}}} \sim E^2$	$\mathrm{M}_2(\mathbb{Q})$ $\mathrm{M}_2(M)$, M quad. imag.	

Endomorphism algebras of abelian surfaces

Let A be an abelian surface over $\mathbb{Q}$.

Dec. of $A_{\overline{\mathbb{Q}}}$	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\#$Possibilities
$A_{\overline{\mathbb{Q}}}$ is simple	$\mathbb{Q}$ real quad. field indef. div. quat. alg./$\mathbb{Q}$ quartic CM field	1 ? ? 13 (Murabayashi-Umegaki, Bisson-Kilicer-Streng)
$A_{\overline{\mathbb{Q}}} \sim E \times E'$ and $E \not\sim E'$	$\mathbb{Q} \times \mathbb{Q}$ $\mathbb{Q} \times M_1$, M_i quad. imag. $M_1 \times M_2$	1 9, since $\#\mathrm{Cl}(M_i) = 1$ 36
$A_{\overline{\mathbb{Q}}} \sim E^2$	$\mathrm{M}_2(\mathbb{Q})$ $\mathrm{M}_2(M)$, M quad. imag.	1 ?, since $\#\mathrm{Cl}(M) = 1, 2, \dots$

Endomorphism algebras of abelian surfaces

Let A be an abelian surface over $\mathbb{Q}$.

Dec. of $A_{\overline{\mathbb{Q}}}$	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\#\mathrm{Possibilities}$
$A_{\overline{\mathbb{Q}}}$ is simple	$\mathbb{Q}$ real quad. field indef. div. quat. alg./$\mathbb{Q}$ quartic CM field	1 ? ? 13 (Murabayashi-Umegaki, Bisson-Kilicer-Streng)
$A_{\overline{\mathbb{Q}}} \sim E \times E'$ and $E \not\sim E'$	$\mathbb{Q} \times \mathbb{Q}$ $\mathbb{Q} \times M_1$, M_i quad. imag. $M_1 \times M_2$	1 9, since $\#\mathrm{Cl}(M_i) = 1$ 36
$A_{\overline{\mathbb{Q}}} \sim E^2$	$\mathrm{M}_2(\mathbb{Q})$ $\mathrm{M}_2(M)$, M quad. imag.	1 N_2

The goal of the talk is to find an upper bound for

$$N_2 = \#\{\text{ab. surf. } A/\mathbb{Q} \text{ such that } A_{\overline{\mathbb{Q}}} \sim E^2, \text{ where } E \text{ has CM}\}/ \sim_{\overline{\mathbb{Q}}} .$$

Endomorphism algebras of abelian surfaces

Let A be an abelian surface over $\mathbb{Q}$.

Dec. of $A_{\overline{\mathbb{Q}}}$	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\#\mathrm{Possibilities}$
$A_{\overline{\mathbb{Q}}}$ is simple	$\mathbb{Q}$ real quad. field indef. div. quat. alg./$\mathbb{Q}$ quartic CM field	1 ? ? 13 (Murabayashi-Umegaki, Bisson-Kilicer-Streng)
$A_{\overline{\mathbb{Q}}} \sim E \times E'$ and $E \not\sim E'$	$\mathbb{Q} \times \mathbb{Q}$ $\mathbb{Q} \times M_1$, M_i quad. imag. $M_1 \times M_2$	1 9, since $\#\mathrm{Cl}(M_i) = 1$ 36
$A_{\overline{\mathbb{Q}}} \sim E^2$	$\mathrm{M}_2(\mathbb{Q})$ $\mathrm{M}_2(M)$, M quad. imag.	1 N_2

Actually, for any prime g, we will find an upper bound for

$$N_g = \#\{\text{ab. var. } A/\mathbb{Q} \text{ such that } A_{\overline{\mathbb{Q}}} \sim E^g, \text{ where } E \text{ has CM}\}/ \sim_{\overline{\mathbb{Q}}} .$$

Main result

Theorem 1 (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ such that $A_{\overline{\mathbb{Q}}} \sim E^g$, where $E/\overline{\mathbb{Q}}$ is an elliptic curve with CM by M. Then:

i) The class group $\mathrm{Cl}(M)$ has exponent dividing g.

ii) If moreover g is prime, then

$$\mathrm{Cl}(M) = \begin{cases} 1,\ \mathrm{C}_2,\ \mathrm{C}_2 \times \mathrm{C}_2 & \text{if} g = 2, \\ 1,\ \mathrm{C}_g & \text{otherwise.} \end{cases}$$

Main result

Theorem 1 (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ such that $A_{\overline{\mathbb{Q}}} \sim E^g$, where $E/\overline{\mathbb{Q}}$ is an elliptic curve with CM by M. Then:

i) The class group $\mathrm{Cl}(M)$ has exponent dividing g.
ii) If moreover g is prime, then

$$\mathrm{Cl}(M) = \begin{cases} 1,\ \mathrm{C}_2,\ \mathrm{C}_2 \times \mathrm{C}_2 & \text{if} g = 2, \\ 1,\ \mathrm{C}_g & \text{otherwise.} \end{cases}$$

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\dots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\dots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \le \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,,$$
$$N_g \le \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \ge 3\,.$$

- On the other hand: $N_g \ge \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \ge 2$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\ldots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\ldots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$
$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\dots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\dots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$

$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$. Indeed, for $M \in \mathcal{M}^g$, take $E/\mathbb{Q}(j_E)$ with CM by M. Then

$$A = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(j_E)}(E)$$

satisfies $\dim(A) = [\mathbb{Q}(j_E):\mathbb{Q}] = \#\mathrm{Cl}(M) = g$ and $A_{\overline{\mathbb{Q}}} \sim E^g_{\overline{\mathbb{Q}}}$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\ldots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\ldots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$
$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$. Indeed, for $M \in \mathcal{M}^g$, take $E/\mathbb{Q}(j_E)$ with CM by M. Then

$$A = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(j_E)}(E)$$

satisfies $\dim(A) = [\mathbb{Q}(j_E):\mathbb{Q}] = \#\mathrm{Cl}(M) = g$ and $A_{\overline{\mathbb{Q}}} \sim E^g_{\overline{\mathbb{Q}}}$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\ldots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\ldots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$
$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$. Indeed, for $M \in \mathcal{M}^g$, take $E/\mathbb{Q}(j_E)$ with CM by M. Then

$$A = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(j_E)}(E)$$

satisfies $\dim(A) = [\mathbb{Q}(j_E) : \mathbb{Q}] = \#\mathrm{Cl}(M) = g$ and $A_{\overline{\mathbb{Q}}} \sim E^g_{\overline{\mathbb{Q}}}$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\ldots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\ldots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$
$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$. Indeed, for $M \in \mathcal{M}^g$, take $E/\mathbb{Q}(j_E)$ with CM by M. Then

$$A = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(j_E)}(E)$$

satisfies $\dim(A) = [\mathbb{Q}(j_E):\mathbb{Q}] = \#\mathrm{Cl}(M) = g$ and $A_{\overline{\mathbb{Q}}} \sim E^g_{\overline{\mathbb{Q}}}$.

Open question

Is $N_2 > 9 + 18$?

An upper bound

- Write:

$$\mathcal{M}^{g,\overset{i}{\dots},g} := \{M \text{ quad. imag. field} \mid \mathrm{Cl}(M) \simeq \mathrm{C}_g \times \overset{i}{\dots} \times \mathrm{C}_g\}.$$

- Theorem 1 implies:

$$N_2 \leq \#\mathcal{M}^1 + \#\mathcal{M}^2 + \#\mathcal{M}^{2,2} = 9 + 18 + 24 = 51\,.$$
$$N_g \leq \#\mathcal{M}^1 + \#\mathcal{M}^g\,, \qquad \text{for } g \geq 3\,.$$

- On the other hand: $N_g \geq \#\mathcal{M}^1 + \#\mathcal{M}^g$ for $g \geq 2$. Indeed, for $M \in \mathcal{M}^g$, take $E/\mathbb{Q}(j_E)$ with CM by M. Then

$$A = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(j_E)}(E)$$

satisfies $\dim(A) = [\mathbb{Q}(j_E) : \mathbb{Q}] = \#\mathrm{Cl}(M) = g$ and $A_{\overline{\mathbb{Q}}} \sim E^g_{\overline{\mathbb{Q}}}$.

Open question

Is $N_2 > 9 + 18$?

Proof of Theorem 1

Definition

Let B/F be an abelian variety. The minimal extension K/F over which

$$\mathrm{End}(B_K) \simeq \mathrm{End}(B_{\overline{\mathbb{Q}}})$$

is called the *endomorphism field of* B.

- K/F is finite and Galois.
- Recast of the setting of Theorem 1:

  (H) $A/\mathbb{Q}$ is an abelian variety of dimension $g \geq 1$ such that $A_K \sim E^g$, where E/K is an elliptic curve with CM by M.

  Here $K/\mathbb{Q}$ is the endomorphism field of A.

Proof of Theorem 1

Definition

Let B/F be an abelian variety. The minimal extension K/F over which

$$\mathrm{End}(B_K) \simeq \mathrm{End}(B_{\overline{\mathbb{Q}}})$$

is called the *endomorphism field of* B.

- K/F is finite and Galois.
- Recast of the setting of Theorem 1:

  (H) $A/\mathbb{Q}$ is an abelian variety of dimension $g \geq 1$ such that $A_K \sim E^g$, where E/K is an elliptic curve with CM by M.

  Here $K/\mathbb{Q}$ is the endomorphism field of A.

Proof of Theorem 1

Definition

Let B/F be an abelian variety. The minimal extension K/F over which

$$\mathrm{End}(B_K) \simeq \mathrm{End}(B_{\overline{\mathbb{Q}}})$$

is called the *endomorphism field of* B.

- K/F is finite and Galois.
- Recast of the setting of Theorem 1:
  (H) $A/\mathbb{Q}$ is an abelian variety of dimension $g \geq 1$ such that $A_K \sim E^g$, where E/K is an elliptic curve with CM by M.

  Here $K/\mathbb{Q}$ is the endomorphism field of A.

Proof of Theorem 1

Theorem 2 (F.-Guitart)

Under (H), there exist a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Part i) of Theorem 1 follows from Theorem 2

$$\mathrm{Gal}(L/M) \twoheadrightarrow \mathrm{Gal}(M(j_{E'})/M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Cl}(M)\,.$$

Theorem 3 (After Guralnick-Kedlaya)

Suppose that (H) holds and g is prime. If v_g denotes the g-adic valuation, then:

- $v_2(\#\,\mathrm{Gal}(K/M)) \leq 2$.
- For $g > 2$, we have $\#\mathrm{Cl}(M) = 1$ or $v_g(\#\,\mathrm{Gal}(K/M)) \leq 1$.

- Part ii) of Theorem 1 follows from Theorem 3.

Proof of Theorem 1

Theorem 2 (F.-Guitart)

Under (H), there exist a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Part i) of Theorem 1 follows from Theorem 2

$$\mathrm{Gal}(L/M) \twoheadrightarrow \mathrm{Gal}(M(j_{E'})/M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Cl}(M)\,.$$

Theorem 3 (After Guralnick-Kedlaya)

Suppose that (H) holds and g is prime. If v_g denotes the g-adic valuation, then:

- $v_2(\#\,\mathrm{Gal}(K/M)) \leq 2$.
- For $g > 2$, we have $\#\mathrm{Cl}(M) = 1$ or $v_g(\#\,\mathrm{Gal}(K/M)) \leq 1$.

- Part ii) of Theorem 1 follows from Theorem 3.

Proof of Theorem 1

Theorem 2 (F.-Guitart)

Under (H), there exist a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Part i) of Theorem 1 follows from Theorem 2

$$\mathrm{Gal}(L/M) \twoheadrightarrow \mathrm{Gal}(M(j_{E'})/M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Cl}(M)\,.$$

Theorem 3 (After Guralnick-Kedlaya)

Suppose that (H) holds and g is prime. If v_g denotes the g-adic valuation, then:

- $v_2(\#\,\mathrm{Gal}(K/M)) \leq 2$.
- For $g > 2$, we have $\#\mathrm{Cl}(M) = 1$ or $v_g(\#\,\mathrm{Gal}(K/M)) \leq 1$.

- Part ii) of Theorem 1 follows from Theorem 3.

Proof of Theorem 1

Theorem 2 (F.-Guitart)

Under (H), there exist a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Part i) of Theorem 1 follows from Theorem 2

$$\mathrm{Gal}(L/M) \twoheadrightarrow \mathrm{Gal}(M(j_{E'})/M) \simeq \mathrm{Gal}(H_M/M) \simeq \mathrm{Cl}(M)\,.$$

Theorem 3 (After Guralnick-Kedlaya)

Suppose that (H) holds and g is prime. If v_g denotes the g-adic valuation, then:

- $v_2(\#\,\mathrm{Gal}(K/M)) \leq 2$.
- For $g > 2$, we have $\#\mathrm{Cl}(M) = 1$ or $v_g(\#\,\mathrm{Gal}(K/M)) \leq 1$.

- Part ii) of Theorem 1 follows from Theorem 3.

A refined version of Theorem 1 for $g = 2$

Theorem 1* (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian surface such that $A_{\overline{\mathbb{Q}}} \sim E^2$, where $E/\overline{\mathbb{Q}}$ is an elliptic curve with CM by M. Then, the set of possibilities for M provided that $\mathrm{Gal}(K/M) \simeq G$ is contained in $\mathcal{M}(G)$, where

$\mathrm{Gal}(K/M)$	$\mathcal{M}(\mathrm{Gal}(K/M))$
C_1	$\mathcal{M}^1$
C_2	$\mathcal{M}^1 \cup \mathcal{M}^2$
C_3	$\mathcal{M}^1$
C_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2$
C_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2$
D_2	$\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_3	$\mathcal{M}^1 \cup \mathcal{M}^2$
D_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
A_4	$\mathcal{M}^1 \setminus \{\mathbb{Q}(\sqrt{-7})\}$
S_4	$\{\mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \setminus \{\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-115})\}$

Proof of Theorem 2: abelian F-varieties

Definition (Ribet)

Let $B/\overline{\mathbb{Q}}$ be an abelian variety and F a number field.
We say that B is an *(abelian) F-variety* if for every $\sigma \in G_F$:

1. There exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$,
2. For every $\varphi \in \mathrm{End}(B)$, the following diagram commutes

$$\begin{tikzcd} {}^\sigma B \arrow[r, "\mu_\sigma"] \arrow[d, "{}^\sigma\varphi"] & B \arrow[d, "\varphi"] \\ {}^\sigma B \arrow[r, "\mu_\sigma"] & B \end{tikzcd}$$

- If $\dim(B) = 1$, then B is called an *(elliptic) F-curve.*
- If $\dim(B) = 1$, observe that
  - If B does not have CM, then 2) is always satisfied.
  - If B has CM (by M), then 1) automatic and 2) amounts to $M \subseteq F$.

Proof of Theorem 2: abelian F-varieties

Definition (Ribet)

Let $B/\overline{\mathbb{Q}}$ be an abelian variety and F a number field.
We say that B is an *(abelian) F-variety* if for every $\sigma \in G_F$:

1. There exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$,
2. For every $\varphi \in \mathrm{End}(B)$, the following diagram commutes

$$\begin{tikzcd} {}^\sigma B \arrow[r, "\mu_\sigma"] \arrow[d, "{}^\sigma\varphi"] & B \arrow[d, "\varphi"] \\ {}^\sigma B \arrow[r, "\mu_\sigma"] & B \end{tikzcd}$$

- If $\dim(B) = 1$, then B is called an *(elliptic) F-curve*.
- If $\dim(B) = 1$, observe that
  - If B does not have CM, then 2) is always satisfied.
  - If B has CM (by M), then 1) automatic and 2) amounts to $M \subseteq F$.

Proof of Theorem 2: abelian F-varieties

Definition (Ribet)

Let $B/\overline{\mathbb{Q}}$ be an abelian variety and F a number field.
We say that B is an *(abelian) F-variety* if for every $\sigma \in G_F$:

1. There exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$,
2. For every $\varphi \in \mathrm{End}(B)$, the following diagram commutes

$$\begin{tikzcd} {}^\sigma B \arrow[r, "\mu_\sigma"] \arrow[d, "{}^\sigma\varphi"] & B \arrow[d, "\varphi"] \\ {}^\sigma B \arrow[r, "\mu_\sigma"] & B \end{tikzcd}$$

- If $\dim(B) = 1$, then B is called an *(elliptic) F-curve*.
- If $\dim(B) = 1$, observe that
  - If B does not have CM, then 2) is always satisfied.
  - If B has CM (by M), then 1) automatic and 2) amounts to $M \subseteq F$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for* B, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define
- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define
- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

$$c_B\colon G \times G \to (\mathrm{End}(B) \otimes \mathbb{Q})^\times$$
$$(\sigma, \tau) \mapsto \mu_\sigma \circ {}^\sigma\mu_\tau \circ (\mu_{\sigma\tau})^{-1}$$

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

$$c_B\colon G \times G \to Z(\mathrm{End}(B) \otimes \mathbb{Q})^\times$$
$$(\sigma, \tau) \mapsto \mu_\sigma \circ {}^\sigma\mu_\tau \circ (\mu_{\sigma\tau})^{-1}$$

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \stackrel{\mathrm{res}}{\to} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

$$c_B \colon G \times G \to Z(\mathrm{End}(B) \otimes \mathbb{Q})^\times = R^\times$$
$$(\sigma, \tau) \mapsto \mu_\sigma \circ {}^\sigma\mu_\tau \circ (\mu_{\sigma\tau})^{-1}$$

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \stackrel{\mathrm{res}}{\to} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for B*, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

$$c_B\colon G \times G \to Z(\mathrm{End}(B) \otimes \mathbb{Q})^\times = R^\times$$
$$(\sigma, \tau) \mapsto \mu_\sigma \circ {}^\sigma\mu_\tau \circ (\mu_{\sigma\tau})^{-1}$$

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \overset{\mathrm{res}}{\to} H^2(\mathrm{Gal}(K/L), R^\times)),$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Weil's descent criterion

- Let B be a F-variety.
- We may assume B/K, where K is a number field.
- We may assume that K is a *field of complete definition for* B, i.e.:
  - K/F is finite and Galois,
  - All the isogenies μ_σ are defined over K.
- Set $G = \mathrm{Gal}(K/F)$ and define

$$c_B \colon G \times G \to Z(\mathrm{End}(B) \otimes \mathbb{Q})^\times = R^\times$$
$$(\sigma, \tau) \mapsto \mu_\sigma \circ {}^\sigma\mu_\tau \circ (\mu_{\sigma\tau})^{-1}$$

- Denote by $\gamma_B = [c_B] \in H^2(G, R^\times)$.

Weil's descent criterion (Ribet)

If $F \subseteq L \subseteq K$ is such that

$$\gamma_B \in \mathrm{Ker}(H^2(G, R^\times) \stackrel{\mathrm{res}}{\to} H^2(\mathrm{Gal}(K/L), R^\times))\,,$$

then there exists B'/L such that $B'_{\overline{\mathbb{Q}}} \sim B_{\overline{\mathbb{Q}}}$.

Recall the setting of Theorem 2

Theorem 2 (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ such that:

- $A_K \sim E^g$
- E/K has CM by M.

Here, K the endomorphism field of A.
Then, there exists a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$,
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Key observation:
  E is a an M-curve and K is a field of complete definition for E.

$$\forall \sigma \in G_M : \quad {}^{\sigma}E^g \sim {}^{\sigma}A_K \sim A_K \sim E^g \qquad \rightsquigarrow \qquad \mu_\sigma : {}^{\sigma}E \to E\,.$$

Recall the setting of Theorem 2

Theorem 2 (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ such that:

- $A_K \sim E^g$
- E/K has CM by M.

Here, K the endomorphism field of A.
Then, there exists a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$,
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Key observation:
  E is a an M-curve and K is a field of complete definition for E.

$$\forall \sigma \in G_M: \quad {}^\sigma E^g \sim {}^\sigma A_K \sim A_K \sim E^g \qquad \rightsquigarrow \qquad \mu_\sigma : {}^\sigma E \to E\,.$$

Recall the setting of Theorem 2

Theorem 2 (F.-Guitart)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ such that:

- $A_K \sim E^g$
- E/K has CM by M.

Here, K the endomorphism field of A.
Then, there exists a subextension $M \subseteq L \subseteq K$ and an elliptic curve E'/L such that:

- $E'_{\overline{\mathbb{Q}}} \sim E_{\overline{\mathbb{Q}}}$,
- L/M is Galois and $\mathrm{Gal}(L/M)$ has exponent dividing g.

- Key observation:
  E is a an M-curve and K is a field of complete definition for E.

$$\forall \sigma \in G_M: \quad {}^{\sigma}E^g \sim {}^{\sigma}A_K \sim A_K \sim E^g \qquad \rightsquigarrow \qquad \mu_\sigma : {}^{\sigma}E \to E\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have
- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows ‘Ribet’s strategy’:

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have
- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have
- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have

$$H^2(G, M^\times) \simeq H^2(G, U) \times H^2(G, P)$$

- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have

$$H^2(G, M^\times)[g] \simeq H^2(G, U)[g] \times H^2(G, P)[g]$$

- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have

$$H^2(G, M^\times)[g] \simeq H^2(G, U)[g] \times H^2(G, P)[g]$$
$$\gamma_E \mapsto (\gamma_U, \overline{\gamma})$$

- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

It follows 'Ribet's strategy':

- One shows that $\gamma_E \in H^2(G, M^\times)[g]$, where $G = \mathrm{Gal}(K/M)$ (by relating γ_E, γ_{E^g}, and γ_A).
- Write $P = M^\times/U$, where $U \subseteq M^\times$ denotes the roots of unity in $M^\times$.
- We have

$$\begin{aligned} H^2(G, M^\times)[g] &\simeq H^2(G, U)[g] \times H^2(G, P)[g] \\ \gamma_E &\mapsto (\gamma_U, \overline{\gamma}) \end{aligned}$$

- For any subgroup $H \subseteq G$, one shows that

$$\mathrm{res}^G_H(\overline{\gamma}) = 1 \qquad \Rightarrow \qquad \mathrm{res}^G_H(\gamma_U) = 1\,.$$

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

- Take $H = \langle a^g \mid a \in G \rangle \triangleleft G$. Then clearly

$$\mathrm{res}^G_H(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
  - There is a model of E over $L = K^H$, and
  - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

$$H^1(G,P) \to H^1(G,P/P^g) \to H^2(G,P)[g] \to 1$$

- Take $H = \langle a^g \mid a \in G \rangle \lhd G$. Then clearly

$$\mathrm{res}_H^G(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
  - There is a model of E over $L = K^H$, and
  - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

$$\mathrm{Hom}(G, P) \to \mathrm{Hom}(G, P/P^g) \to H^2(G, P)[g] \to 1$$

- Take $H = \langle a^g \mid a \in G \rangle \lhd G$. Then clearly

$$\mathrm{res}^G_H(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
    - There is a model of E over $L = K^H$, and
    - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

$$1 \to \mathrm{Hom}(G, P/P^g) \xrightarrow{\simeq} H^2(G,P)[g] \to 1$$

- Take $H = \langle a^g \mid a \in G \rangle \lhd G$. Then clearly

$$\mathrm{res}^G_H(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
  - There is a model of E over $L = K^H$, and
  - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

$$1 \to \mathrm{Hom}(G, P/P^g) \xrightarrow{\simeq} H^2(G,P)[g] \to 1$$

- Take $H = \langle a^g \mid a \in G \rangle \triangleleft G$. Then clearly

$$\mathrm{res}^G_H(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
  - There is a model of E over $L = K^H$, and
  - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Sketch of proof of Theorem 2

- Consider the map

$$P \to P$$
$$x \mapsto x^g$$

- It induces an exact sequence in cohomology

$$1 \to \mathrm{Hom}(G, P/P^g) \xrightarrow{\simeq} H^2(G, P)[g] \to 1$$

- Take $H = \langle a^g \mid a \in G \rangle \triangleleft G$. Then clearly

$$\mathrm{res}_H^G(\overline{\gamma}) = 1, \qquad \text{as } \overline{\gamma} \in \mathrm{Hom}(G, P/P^g)\,.$$

- By Weil's descent criterion:
  - There is a model of E over $L = K^H$, and
  - $\mathrm{Gal}(L/F) \simeq G/H$ is killed by g.

Final comments

Theorem (Elkies-Ribet)

Let $E/\overline{\mathbb{Q}}$ be an F-curve *without CM*. Then E admits a model over a polyquadratic extension of F.

- Ribet shows that
$$\gamma_E \in H^2(G, \mathbb{Q}^\times)[2]\,,$$
(for different reasons as ours). The other steps of the proof are analogous.

Corollary

Let A be an abelian variety over F such that $A_{\overline{\mathbb{Q}}} \sim E^g$, where E is an elliptic curve *without CM* and g is *odd*. Then E admits a model over F.

$$\left.\begin{array}{l} \gamma_E^g = 1 \\ \gamma_E^2 = 1 \end{array}\right\} \Rightarrow \gamma_E = 1 \Rightarrow E \text{ admits a model over } F\,.$$