Visualizing elements of Sha[3] in genus 2 jacobians

Sander Dahmen

Simon Fraser University

Joint work with Nils Bruin

Consider an elliptic curve E over a number field k.

• the Mordell-Weil group E(k)

- the Mordell-Weil group E(k)
- the Shafarevich-Tate group $\operatorname{III}(E/k)$.

- the Mordell-Weil group E(k)
- the Shafarevich-Tate group III(E/k).

We want to describe elements of III(E/k) explicitly.

 $\operatorname{III}(E/k)$: equivalence classes of principal homogeneous spaces C/k for E/k with points everywhere locally.

 $\operatorname{III}(E/k)$: equivalence classes of principal homogeneous spaces C/k for E/k with points everywhere locally. If C/k corresponds to an elements $\sigma \in \operatorname{III}(E/k)$ of order n > 2, then it can be represented as a curve of degree n in \mathbb{P}^{n-1} . $\operatorname{III}(E/k)$: equivalence classes of principal homogeneous spaces C/k for E/k with points everywhere locally. If C/k corresponds to an elements $\sigma \in \operatorname{III}(E/k)$ of order n > 2, then it can be represented as a curve of degree n in \mathbb{P}^{n-1} . Given an embedding $E \to A$ over k of abelian varieties. III(E/k): equivalence classes of principal homogeneous spaces C/k for E/k with points everywhere locally. If C/k corresponds to an elements $\sigma \in \text{III}(E/k)$ of order n > 2, then it can be represented as a curve of degree n in \mathbb{P}^{n-1} . Given an embedding $E \to A$ over k of abelian varieties. We say that σ is visible in A, if for some $P \in A(\overline{k})$

$$C \simeq_k E + P \subset A.$$

III(E/k): equivalence classes of principal homogeneous spaces C/k for E/k with points everywhere locally. If C/k corresponds to an elements $\sigma \in \text{III}(E/k)$ of order n > 2, then it can be represented as a curve of degree n in \mathbb{P}^{n-1} . Given an embedding $E \to A$ over k of abelian varieties. We say that σ is visible in A, if for some $P \in A(\overline{k})$

$$C \simeq_k E + P \subset A.$$

Equivalently, σ lies in the kernel of $H^1(k, E) \rightarrow H^1(k, A)$.

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Actually, they could be visualized in an abelian surface contained in the new part of $J_0(N_E)$.

Visualizing elements of III in abelian surfaces

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Actually, they could be visualized in an abelian surface contained in the new part of $J_0(N_E)$.

Mazur gave a first theoretical result trying to explain this.

Visualizing elements of III in abelian surfaces

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Actually, they could be visualized in an abelian surface contained in the new part of $J_0(N_E)$.

Mazur gave a first theoretical result trying to explain this.

Theorem (Mazur)

If $\sigma \in \operatorname{III}(E/k)$ has order 3, then σ is visible in an abelian surface.

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Actually, they could be visualized in an abelian surface contained in the new part of $J_0(N_E)$.

Mazur gave a first theoretical result trying to explain this.

Theorem (Mazur)

If $\sigma \in \operatorname{III}(E/k)$ has order 3, then σ is visible in an abelian surface.

How about visibility in jacobians?

Cremona and Mazur found that for surprisingly many elliptic curves E/\mathbb{Q} with nontrivial odd order elements of $\mathrm{III}(E/\mathbb{Q})$, these element can be visualized in $J_0(N_E)$.

Actually, they could be visualized in an abelian surface contained in the new part of $J_0(N_E)$.

Mazur gave a first theoretical result trying to explain this.

Theorem (Mazur)

If $\sigma \in \operatorname{III}(E/k)$ has order 3, then σ is visible in an abelian surface.

How about visibility in jacobians?

Theorem (Bruin & D.)

If $\sigma \in \text{III}(E/k)$ has order 3, then σ is visible in the jacobian of a curve of genus 2.

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ .

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ . If we can construct an elliptic curve E'/k such that

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ . If we can construct an elliptic curve E'/k such that

• there exists an isomorphism of $\operatorname{Gal}(\overline{k}/k)$ -modules

 $\lambda: E[3] \rightarrow E'[3]$

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ . If we can construct an elliptic curve E'/k such that

• there exists an isomorphism of $\operatorname{Gal}(\overline{k}/k)$ -modules

$$\lambda: E[3] \rightarrow E'[3]$$

 $\bullet~\delta$ maps to zero under

$$H^1(k, E[3]) \rightarrow H^1(k, E'[3]) \rightarrow H^1(k, E'),$$

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ . If we can construct an elliptic curve E'/k such that

• there exists an isomorphism of $\operatorname{Gal}(\overline{k}/k)$ -modules

$$\lambda: E[3] \rightarrow E'[3]$$

 $\bullet~\delta$ maps to zero under

$$H^1(k, E[3]) \rightarrow H^1(k, E'[3]) \rightarrow H^1(k, E'),$$

then σ is visible in the abelian surface (over k)

$$A := (E imes E') / \Delta$$

where Δ denotes the graph of λ .

Let $\sigma \in \operatorname{III}(E/k)[3]$ and choose $\delta \in \operatorname{Sel}^{(3)}(E/k)$ mapping to σ . If we can construct an elliptic curve E'/k such that

• there exists an isomorphism of $\operatorname{Gal}(\overline{k}/k)$ -modules

$$\lambda: E[3] \rightarrow E'[3]$$

• δ maps to zero under

$$H^1(k, E[3]) \rightarrow H^1(k, E'[3]) \rightarrow H^1(k, E'),$$

then σ is visible in the abelian surface (over k)

$$A := (E imes E') / \Delta$$

where Δ denotes the graph of λ .

So
$$\Delta(\overline{k}) = \{(P, \lambda(P)) : P \in E[3](\overline{k})\}.$$

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

•
$$E' := \operatorname{Jac}(C')$$
 has $E[3] \simeq E'[3]$

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

• $\operatorname{Flex}(C)$ and $\operatorname{Flex}(C')$ have isomorphic $\operatorname{Gal}(\overline{k}/k)$ -action

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

- $\operatorname{Flex}(C)$ and $\operatorname{Flex}(C')$ have isomorphic $\operatorname{Gal}(\overline{k}/k)$ -action
- C' has a k-rational point.

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

- $\operatorname{Flex}(C)$ and $\operatorname{Flex}(C')$ have isomorphic $\operatorname{Gal}(\overline{k}/k)$ -action
- C' has a k-rational point.

Mazur showed that such a C' can always be constructed.

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

- $\operatorname{Flex}(C)$ and $\operatorname{Flex}(C')$ have isomorphic $\operatorname{Gal}(\overline{k}/k)$ -action
- C' has a k-rational point.

Mazur showed that such a C' can always be constructed. Hence, σ can be visualized in the abelian surface $(E \times E')/\Delta$,

It suffices to construct a smooth cubic curve C'/k in \mathbb{P}^2 such that

- $\operatorname{Flex}(C)$ and $\operatorname{Flex}(C')$ have isomorphic $\operatorname{Gal}(\overline{k}/k)$ -action
- C' has a k-rational point.

Mazur showed that such a C' can always be constructed. Hence, σ can be visualized in the abelian surface $(E \times E')/\Delta$, where Δ denotes the graph of an isomorphism $\lambda : E[3] \rightarrow E'[3]$.

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k.

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

We have a one parameter family of curves

$$C_{(s:t)}: sF + tH = 0.$$

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

We have a one parameter family of curves

$$C_{(s:t)}: sF + tH = 0.$$

Smooth members $C_{(s:t)}$ with $(s:t) \in \mathbb{P}^1(k)$ satisfy:

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

We have a one parameter family of curves

$$C_{(s:t)}: sF + tH = 0.$$

Smooth members $C_{(s:t)}$ with $(s:t) \in \mathbb{P}^1(k)$ satisfy:

•
$$Flex(C_{(s:t)}) = Flex(C) = \{F = H = 0\}$$

Mazur's construction for C'

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

We have a one parameter family of curves

$$C_{(s:t)}: sF + tH = 0.$$

Smooth members $C_{(s:t)}$ with $(s:t) \in \mathbb{P}^1(k)$ satisfy:

•
$$Flex(C_{(s:t)}) = Flex(C) = \{F = H = 0\}$$

•
$$\operatorname{Jac}(C_{(s:t)})[3] \simeq \operatorname{Jac}(C)[3].$$

Mazur's construction for C'

Let C be give by F(x, y, z) = 0 for a ternary cubic form F/k. Consider the Hessian of F

$$H := \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial z \partial x} & \frac{\partial^2 F}{\partial z \partial y} & \frac{\partial^2 F}{\partial z \partial z} \end{vmatrix}.$$

We have a one parameter family of curves

$$C_{(s:t)}: sF + tH = 0.$$

Smooth members $C_{(s:t)}$ with $(s:t) \in \mathbb{P}^1(k)$ satisfy:

•
$$Flex(C_{(s:t)}) = Flex(C) = \{F = H = 0\}$$

•
$$\operatorname{Jac}(C_{(s:t)})[3] \simeq \operatorname{Jac}(C)[3].$$

Now choose C' to be a smooth $C_{(s:t)}$ with a k-rational point.

 $E \times E'$ is principally polarized via the product polarization.

 $((P,P'),(Q,Q'))\mapsto e_E(P,Q)e_{E'}(P',Q').$

$$((P,P'),(Q,Q'))\mapsto e_E(P,Q)e_{E'}(P',Q').$$

The isogeny $E \times E' \rightarrow A := (E \times E')/\Delta$ respect the principal polarization when the Weil paring is trivial on Δ ,

$$((P,P'),(Q,Q'))\mapsto e_E(P,Q)e_{E'}(P',Q').$$

The isogeny $E \times E' \rightarrow A := (E \times E')/\Delta$ respect the principal polarization when the Weil paring is trivial on Δ , i.e.

$$\forall P, Q \in E[3]: e_E(P, Q) = e_{E'}(\lambda(P), \lambda(Q))^{-1}$$

$$((P,P'),(Q,Q'))\mapsto e_E(P,Q)e_{E'}(P',Q').$$

The isogeny $E \times E' \rightarrow A := (E \times E')/\Delta$ respect the principal polarization when the Weil paring is trivial on Δ , i.e.

$$\forall P, Q \in E[3]: e_E(P, Q) = e_{E'}(\lambda(P), \lambda(Q))^{-1}$$

The isomorphism $\lambda : E[3] \rightarrow E'[3]$ coming from Mazur's construction preserves the Weil pairing,

$$((P,P'),(Q,Q')) \mapsto e_E(P,Q)e_{E'}(P',Q').$$

The isogeny $E \times E' \rightarrow A := (E \times E')/\Delta$ respect the principal polarization when the Weil paring is trivial on Δ , i.e.

$$\forall P, Q \in E[3]: e_E(P, Q) = e_{E'}(\lambda(P), \lambda(Q))^{-1}$$

The isomorphism $\lambda : E[3] \rightarrow E'[3]$ coming from Mazur's construction preserves the Weil pairing, i.e.

$$\forall P, Q \in E[3]: e_E(P, Q) = e_{E'}(\lambda(P), \lambda(Q)).$$

• Consider the 9 tangent lines to Flex(C).

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.
- These points are not flex points of a cubic, so there is a unique cubic C'₀ in (P²)* passing through these points (generically).

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.
- These points are not flex points of a cubic, so there is a unique cubic C'₀ in (P²)* passing through these points (generically).
- Using the hessian as before, we construct a one-parameter family of cubics passing through the flex points of C'_0 .

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.
- These points are not flex points of a cubic, so there is a unique cubic C'₀ in (P²)* passing through these points (generically).
- Using the hessian as before, we construct a one-parameter family of cubics passing through the flex points of C'_0 .
- Again, we can pick a curve C' from this family that is smooth and has a k-rational point.

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.
- These points are not flex points of a cubic, so there is a unique cubic C'₀ in (P²)* passing through these points (generically).
- Using the hessian as before, we construct a one-parameter family of cubics passing through the flex points of C'_0 .
- Again, we can pick a curve C' from this family that is smooth and has a k-rational point.

Fisher: $Jac(C')[3] \simeq Jac(C)[3]$ anti-isometrically.

- Consider the 9 tangent lines to Flex(C).
- These lines determine 9 points in $(\mathbb{P}^2)^*$.
- These points are not flex points of a cubic, so there is a unique cubic C'₀ in (P²)* passing through these points (generically).
- Using the hessian as before, we construct a one-parameter family of cubics passing through the flex points of C'_0 .
- Again, we can pick a curve C' from this family that is smooth and has a k-rational point.

Fisher: $Jac(C')[3] \simeq Jac(C)[3]$ anti-isometrically. Some work: Flex(C), Flex(C') have isomorphic $Gal(\overline{k}/k)$ -action.

The genus 2 curve

The genus 2 curve

The genus 2 curve

Make sure that $E := \operatorname{Jac}(C)$ and $E' := \operatorname{Jac}(C')$ are not isogenous, then $A := (E \times E')/\Delta \simeq \operatorname{Jac}(X)$ for a genus 2 Curve X/k. Construction of X:

Consider P² with coordinates (x : y : z) and dual (P²)* with coordinates (u : v : w) describing the line xu + yv + zw = 0.

- Consider P² with coordinates (x : y : z) and dual (P²)* with coordinates (u : v : w) describing the line xu + yv + zw = 0.
- Embed E' in $(\mathbb{P}^2)^*$ such that all tangent lines through $\operatorname{Flex}(E)$ correspond to points on a cubic through $\operatorname{Flex}(E')$.

- Consider P² with coordinates (x : y : z) and dual (P²)* with coordinates (u : v : w) describing the line xu + yv + zw = 0.
- Embed E' in (ℙ²)* such that all tangent lines through Flex(E) correspond to points on a cubic through Flex(E').
- This gives an embedding $E \times E' \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$.

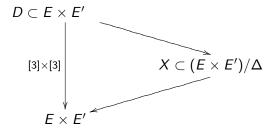
- Consider P² with coordinates (x : y : z) and dual (P²)* with coordinates (u : v : w) describing the line xu + yv + zw = 0.
- Embed E' in (ℙ²)* such that all tangent lines through Flex(E) correspond to points on a cubic through Flex(E').
- This gives an embedding $E \times E' \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$.
- On $E \times E'$ we have the genus 10 curve

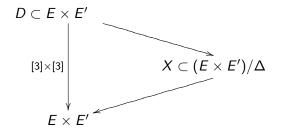
$$D: xu + yv + zw = 0.$$

- Consider P² with coordinates (x : y : z) and dual (P²)* with coordinates (u : v : w) describing the line xu + yv + zw = 0.
- Embed E' in (ℙ²)* such that all tangent lines through Flex(E) correspond to points on a cubic through Flex(E').
- This gives an embedding $E \times E' \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*$.
- On $E \times E'$ we have the genus 10 curve

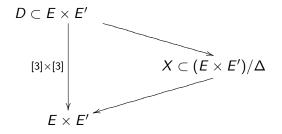
$$D: xu + yv + zw = 0.$$

• Frey and Kani: X is the image of D in $(E \times E')/\Delta$.



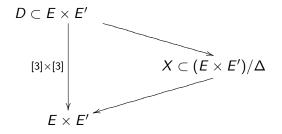


• The map $[3] \times [3]$ is much more accessible.

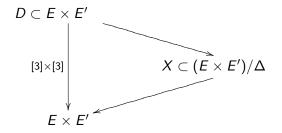


• The map $[3] \times [3]$ is much more accessible.

• The subgroup of $E[3] \times E'[3]$ under which D is invariant is Δ .



- The map $[3] \times [3]$ is much more accessible.
- The subgroup of $E[3] \times E'[3]$ under which D is invariant is Δ .
- Hence a model for X can be found on $E \times E'$ as $([3] \times [3])(D)$.



- The map $[3] \times [3]$ is much more accessible.
- The subgroup of E[3] × E'[3] under which D is invariant is Δ.
- Hence a model for X can be found on E × E' as ([3] × [3])(D).
- This image can easily be computed by interpolation.

Detailed examples:

Detailed examples: See the proceedings

Detailed examples: See the proceedings

Thank you for your attention.