Torelli's Theorem

Remarks on Sections III.12–13 of Milne's *Abelian Varieties*

University of Freiburg

28th July 2020

Assumptions, notation and recollections

- k is an algebraically closed field.

Assumptions, notation and recollections

- k is an algebraically closed field.
- C is a smooth complete curve over k of genus $g \geqslant 2$.

Assumptions, notation and recollections

- k is an algebraically closed field.
- C is a smooth complete curve over k of genus $g \geqslant 2$.
- J is its Jacobian, which is an abelian variety representing

$$T \mapsto \{\mathcal{L} \in \operatorname{Pic}(C \times T) \mid \deg(\mathcal{L}_t) = 0 \text{ for all } t \in T\} / \operatorname{Pic}(T).$$

Assumptions, notation and recollections

- k is an algebraically closed field.
- C is a smooth complete curve over k of genus $g \geqslant 2$.
- J is its Jacobian, which is an abelian variety representing

$$T \mapsto \{\mathcal{L} \in \operatorname{Pic}(C \times T) \mid \deg(\mathcal{L}_t) = 0 \text{ for all } t \in T\} / \operatorname{Pic}(T).$$

- In particular, we may and will identify $J(k) = \operatorname{Pic}^0(C)$.

Assumptions, notation and recollections

- k is an algebraically closed field.
- C is a smooth complete curve over k of genus $g \geqslant 2$.
- J is its Jacobian, which is an abelian variety representing

$$T \mapsto \{\mathcal{L} \in \operatorname{Pic}(C \times T) \mid \deg(\mathcal{L}_t) = 0 \text{ for all } t \in T\} / \operatorname{Pic}(T).$$

- In particular, we may and will identify $J(k) = \operatorname{Pic}^0(C)$.
- Fix $P \in C(k)$ once and for all. Then we get a canonical map

$$f \colon C \to J, \quad Q \mapsto [Q - P].$$

Assumptions, notation and recollections

- k is an algebraically closed field.
- C is a smooth complete curve over k of genus $g \geqslant 2$.
- J is its Jacobian, which is an abelian variety representing

$$T \mapsto \{\mathcal{L} \in \operatorname{Pic}(C \times T) \mid \deg(\mathcal{L}_t) = 0 \text{ for all } t \in T\} / \operatorname{Pic}(T).$$

- In particular, we may and will identify $J(k) = \operatorname{Pic}^0(C)$.
- Fix $P \in C(k)$ once and for all. Then we get a canonical map

$$f\colon C \to J, \quad Q \mapsto [Q - P].$$

- For all $1 \leqslant r \leqslant g$ we get an induced map

$$f\colon C^{(r)} \to J, \quad P_1 \cdot \ldots \cdot P_r \mapsto [P_1 + \cdots + P_r - rP]$$

birational onto its image $W^r \subseteq J$, which is a closed subvariety.

Canonical polarization

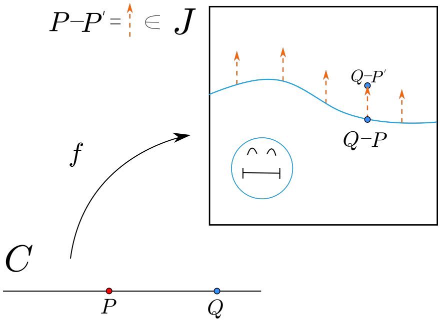
- For $r = g - 1$ we get a divisor $\Theta = W^{g-1} \subseteq J$, the image of

  $f\colon C^{(g-1)} \to J, \quad P_1 \cdot \ldots \cdot P_{g-1} \mapsto [P_1 + \cdots + P_{g-1} - (g-1)P].$

Canonical polarization

- For $r = g-1$ we get a divisor $\Theta = W^{g-1} \subseteq J$, the image of

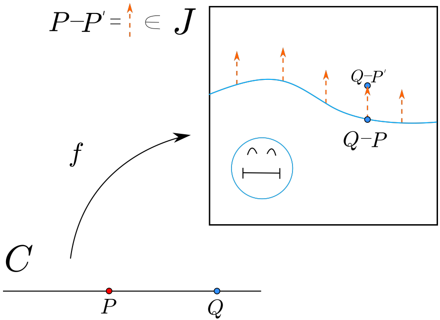
  $f\colon C^{(g-1)} \to J, \quad P_1 \cdot \ldots \cdot P_{g-1} \mapsto [P_1 + \cdots + P_{g-1} - (g-1)P]$.



Canonical polarization

- For $r = g - 1$ we get a divisor $\Theta = W^{g-1} \subseteq J$, the image of

  $f\colon C^{(g-1)} \to J, \quad P_1 \cdot \ldots \cdot P_{g-1} \mapsto [P_1 + \cdots + P_{g-1} - (g-1)P].$



- The induced $\lambda\colon J \to J^\vee$ is an isomorphism, so Θ gives us a principal polarization of J called the *canonical polarization*.

Statement — Existence

Let C and C' be curves as before and let $\beta\colon (J,\lambda) \xrightarrow{\sim} (J',\lambda')$ be an isomorphism such that $\lambda' \circ \beta = \beta^\vee \circ \lambda$.

Statement — Existence

Let C and C' be curves as before and let $\beta\colon (J,\lambda) \xrightarrow{\sim} (J',\lambda')$ be an isomorphism such that $\lambda' \circ \beta = \beta^\vee \circ \lambda$.

Then there exists an isomorphism $\alpha\colon C \xrightarrow{\sim} C'$ such that

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\alpha"'] & J \arrow[d, "\beta"] \\ C' \arrow[r, "f'"'] & J' \end{tikzcd}$$

commutes up to a sign and a translation by some $c \in J'(k)$.

Statement — Uniqueness

A curve C as before is called *hyperelliptic* if there is a (unique) $2:1$ branched covering $\pi\colon C \to \mathbb{P}^1$.

Statement — Uniqueness

A curve C as before is called *hyperelliptic* if there is a (unique) $2:1$ branched covering $\pi\colon C \to \mathbb{P}^1$. From Hartshorne's exercises:

- A curve of genus 2 is always hyperelliptic.
- There are hyperelliptic curves of any genus $g \geqslant 2$.
- A plane curve of degree 4 (thus $g = 3$) is not hyperelliptic.

Statement — Uniqueness

A curve C as before is called *hyperelliptic* if there is a (unique) $2:1$ branched covering $\pi\colon C \to \mathbb{P}^1$. From Hartshorne's exercises:

- A curve of genus 2 is always hyperelliptic.
- There are hyperelliptic curves of any genus $g \geqslant 2$.
- A plane curve of degree 4 (thus $g = 3$) is not hyperelliptic.

We can now state uniqueness distinguishing two cases:

- If C is not hyperelliptic, then the sign, α and c are uniquely determined by β, P and P'.
- If C is hyperelliptic, then the sign can be chosen arbitrarily, and α and c are uniquely determined by β, P, P' and the chosen sign.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2) \colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f' \colon C' \to J'$.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2)\colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f'\colon C' \to J'$.
- Hence $(\alpha_1 - \alpha_2)(Q_1) \sim (\alpha_1 - \alpha_2)(Q_2)$ and

$$(*) \quad \alpha_1(Q_1) + \alpha_2(Q_2) \sim \alpha_2(Q_1) + \alpha_1(Q_2) \quad (\forall Q_1, Q_2).$$

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2)\colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f'\colon C' \to J'$.
- Hence $(\alpha_1 - \alpha_2)(Q_1) \sim (\alpha_1 - \alpha_2)(Q_2)$ and

$$(*) \quad \alpha_1(Q_1) + \alpha_2(Q_2) \sim \alpha_2(Q_1) + \alpha_1(Q_2) \quad (\forall Q_1, Q_2).$$

- Suppose $\alpha_1 \neq \alpha_2$. Then $\exists Q_1 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_2(Q_1)$. Since α_1 is an isomorphism, there are also plenty $Q_2 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_1(Q_2)$, hence $\alpha_1(Q_1) \notin \{\alpha_2(Q_1), \alpha_1(Q_2)\}$.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2)\colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f'\colon C' \to J'$.
- Hence $(\alpha_1 - \alpha_2)(Q_1) \sim (\alpha_1 - \alpha_2)(Q_2)$ and

$$(*) \quad \alpha_1(Q_1) + \alpha_2(Q_2) \sim \alpha_2(Q_1) + \alpha_1(Q_2) \quad (\forall Q_1, Q_2).$$

- Suppose $\alpha_1 \neq \alpha_2$. Then $\exists Q_1 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_2(Q_1)$. Since α_1 is an isomorphism, there are also plenty $Q_2 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_1(Q_2)$, hence $\alpha_1(Q_1) \notin \{\alpha_2(Q_1), \alpha_1(Q_2)\}$.
- So the degree 2 linear system given by $(*)$ contains at least two divisors, which implies that it is of dimension at least 1.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2)\colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f'\colon C' \to J'$.
- Hence $(\alpha_1 - \alpha_2)(Q_1) \sim (\alpha_1 - \alpha_2)(Q_2)$ and

$$(*) \quad \alpha_1(Q_1) + \alpha_2(Q_2) \sim \alpha_2(Q_1) + \alpha_1(Q_2) \quad (\forall Q_1, Q_2).$$

- Suppose $\alpha_1 \neq \alpha_2$. Then $\exists Q_1 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_2(Q_1)$. Since α_1 is an isomorphism, there are also plenty $Q_2 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_1(Q_2)$, hence $\alpha_1(Q_1) \notin \{\alpha_2(Q_1), \alpha_1(Q_2)\}$.
- So the degree 2 linear system given by $(*)$ contains at least two divisors, which implies that it is of dimension at least 1.
- Varying Q_1 we obtain more such linear systems, and curves of general type can have at most one such linear system.

Proof — Uniqueness (modulo case distinctions for signs)

- Suppose α_1, α_2, c_1 and c_2 were such that $f' \circ \alpha_i = \beta \circ f + c_i$.
- Then $f' \circ (\alpha_1 - \alpha_2)\colon C \to J'$ is constant, so $\alpha_1 - \alpha_2$ sends every pair of points in C to the same fibre of $f'\colon C' \to J'$.
- Hence $(\alpha_1 - \alpha_2)(Q_1) \sim (\alpha_1 - \alpha_2)(Q_2)$ and

$$(*) \quad \alpha_1(Q_1) + \alpha_2(Q_2) \sim \alpha_2(Q_1) + \alpha_1(Q_2) \quad (\forall Q_1, Q_2).$$

- Suppose $\alpha_1 \neq \alpha_2$. Then $\exists Q_1 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_2(Q_1)$. Since α_1 is an isomorphism, there are also plenty $Q_2 \in C(k)$ s.t. $\alpha_1(Q_1) \neq \alpha_1(Q_2)$, hence $\alpha_1(Q_1) \notin \{\alpha_2(Q_1), \alpha_1(Q_2)\}$.
- So the degree 2 linear system given by $(*)$ contains at least two divisors, which implies that it is of dimension at least 1.
- Varying Q_1 we obtain more such linear systems, and curves of general type can have at most one such linear system.
- This contradiction shows that $\alpha_1 = \alpha_2$, thus $c_1 = c_2$.

Corollary — Torelli over a perfect field $F \subseteq k$

If C, C' and β are defined over F, then α is defined over F as well. In particular, $C \cong C'$ over F.

Corollary — Torelli over a perfect field $F \subseteq k$

If C, C' and β are defined over F, then α is defined over F as well. In particular, $C \cong C'$ over F.

Sketch of proof (choose a sign if C hyperelliptic):

(1) α is characterized by: $\exists c \in J(k)$ s.t. $f^{P'} \circ \alpha = \pm\beta \circ f^{P} + c$.

Corollary — Torelli over a perfect field $F \subseteq k$

If C, C' and β are defined over F, then α is defined over F as well. In particular, $C \cong C'$ over F.

Sketch of proof (choose a sign if C hyperelliptic):

(1) α is characterized by: $\exists c \in J(k)$ s.t. $f^{P'} \circ \alpha = \pm\beta \circ f^P + c$.

(2) Replacing P by Q we get $f^Q = f^P + d$, resp. for $(-)'$. Hence

$$f^{Q'} \circ \alpha = f^{P'} \circ \alpha + d' = \pm\beta \circ f^P + c + d' = \pm\beta \circ f^Q \mp \beta(d) + c + d'.$$

Corollary — Torelli over a perfect field $F \subseteq k$

If C, C' and β are defined over F, then α is defined over F as well. In particular, $C \cong C'$ over F.

Sketch of proof (choose a sign if C hyperelliptic):

(1) α is characterized by: $\exists c \in J(k)$ s.t. $f^{P'} \circ \alpha = \pm\beta \circ f^P + c$.

(2) Replacing P by Q we get $f^Q = f^P + d$, resp. for $(-)'$. Hence

$$f^{Q'} \circ \alpha = f^{P'} \circ \alpha + d' = \pm\beta \circ f^P + c + d' = \pm\beta \circ f^Q \mp \beta(d) + c + d'.$$

(3) Hence α is independent of the chosen k-points P and P'.

Corollary — Torelli over a perfect field $F \subseteq k$

If C, C' and β are defined over F, then α is defined over F as well. In particular, $C \cong C'$ over F.

Sketch of proof (choose a sign if C hyperelliptic):

(1) α is characterized by: $\exists c \in J(k)$ s.t. $f^{P'} \circ \alpha = \pm\beta \circ f^P + c$.

(2) Replacing P by Q we get $f^Q = f^P + d$, resp. for $(-)'$. Hence

$$f^{Q'} \circ \alpha = f^{P'} \circ \alpha + d' = \pm\beta \circ f^P + c + d' = \pm\beta \circ f^Q \mp \beta(d) + c + d'.$$

(3) Hence α is independent of the chosen k-points P and P'.

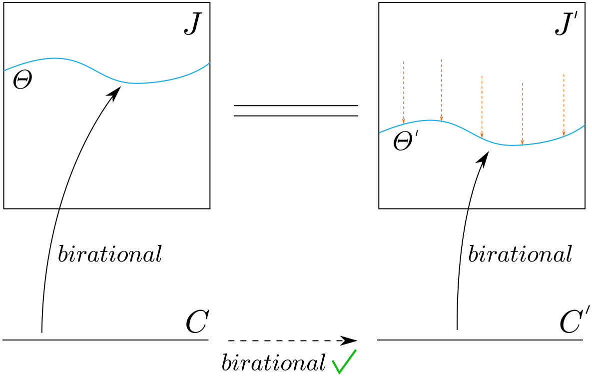
(4) For $\sigma \in \mathrm{Gal}(k/F)$ we have $\sigma f^P = f^{\sigma P}$, resp. for $(-)'$. Hence

$$f^{\sigma P'} \circ \sigma\alpha = \sigma f^{P'} \circ \sigma\alpha = \pm\sigma\beta \circ \sigma f^P + \sigma c = \pm\beta \circ f^{\sigma P} + \sigma c.$$

Point (3) implies then $\sigma\alpha = \alpha$.

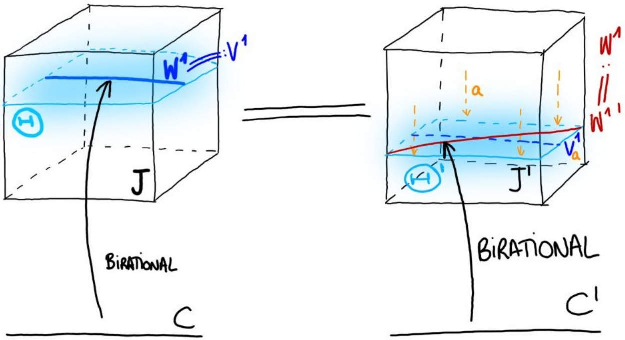
Idea of the existence proof for $g = 2$

Suppose $g = 2$ as in the previous picture. If we identify J with J' via β, the fact that β is a polarized isomorphism guarantees the following situation:



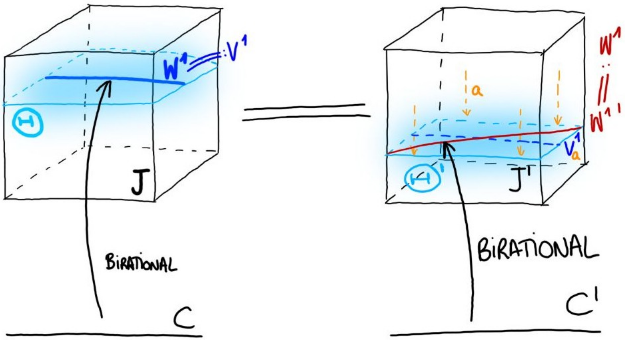
Idea of the existence proof for $g > 2$

If $g > 2$, the fact that β is a polarized isomorphism guarantees a priori only that Θ' is a translation Θ_a of Θ by some $a \in J(k)$:



Idea of the existence proof for $g > 2$

If $g > 2$, the fact that β is a polarized isomorphism guarantees a priori only that Θ' is a translation Θ_a of Θ by some $a \in J(k)$:



Is $V^1_a = W^1_b$ for some $b \in J(k)$?
[Yes! Modulo replacing W^1 by its image under $x \mapsto -x$.]

Thanks for listening!