# The Jacobian

Juanita Duque-Rosero

**Outline:**

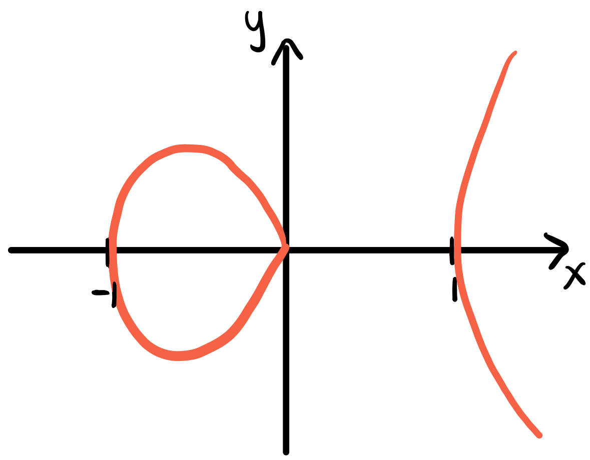
1. Preliminaries: Elliptic Curves, lattices & Riemann surfaces.
2. The Jacobian: Definition.
3. The Abel-Jacobi map: Definition and example.
4. The Abel-Jacobi Theorem: Sketch of the proof.
5. Applications: Rational points.

# Elliptic Curves

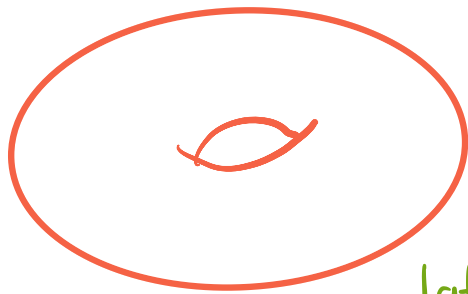
(Curves of genus 1 with a rational point)

Example: $E: y^2 = x^3 - x$

Real glasses $\mathbb{R}$-$\mathbb{R}$



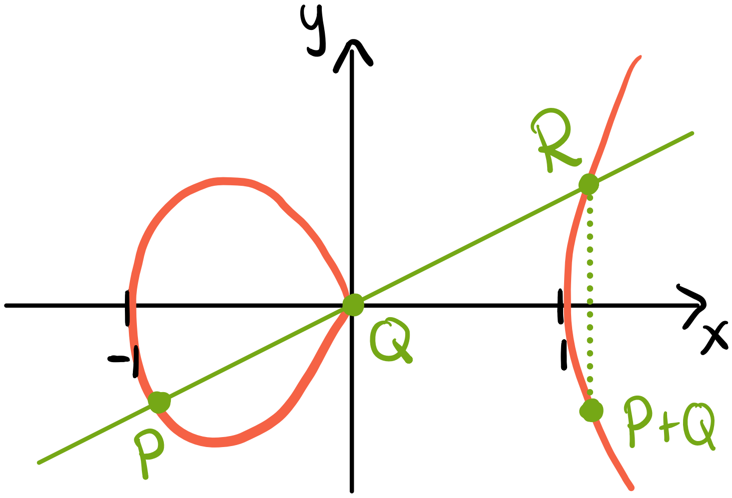

Complex glasses $\mathbb{C}$-$\mathbb{C}$



$\cong \mathbb{C}/L$

lattice

# Abelian Group Structure of $E$




We define

$$P+Q+R=O \leftarrow \text{identity}$$

$$\Updownarrow$$

$P, Q$ and $R$ are colinear

We say that $E$ is an Abelian variety.

Applications: ① Rational points

② Cryptography

# Are Elliptic Curves Special?

Can we define an Abelian group structure on curves of different g?

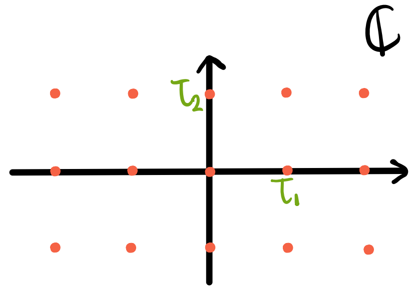
Answer: We cannot. Elliptic curves are special! Projective +compact

Solution: We can define an abstract object where $P+Q$ makes sense: $\left\{ \underbrace{\sum_{i=1}^{n} [P_i]}_{\text{Divisor of } C.} \mid P_i \in C(\mathbb{C}) \right\}$

Better solution: We define the Jacobian of C.

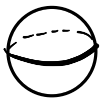
# Lattices

**Def.** A *lattice* is an additive subgroup of $\mathbb{C}^n$, generated over $\mathbb{Z}$ by $2n$ vectors that are linearly independent over $\mathbb{R}$.




# Riemann Surfaces

**Def.** A *Riemann surface* is a one dimensional complex manifold.

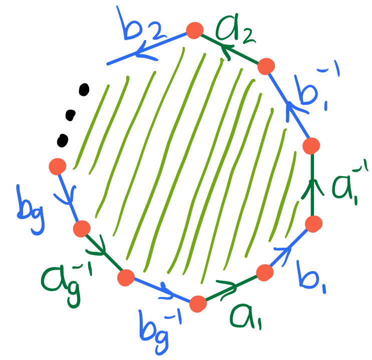
**Examples:** ① $S^2 =$ , using the stereographic projection.

② $C$, a smooth projective plane curve.

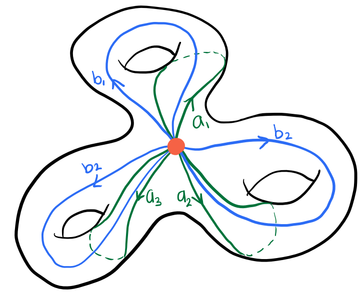
⚠ In this talk, $X$ will be a compact Riemann surface.

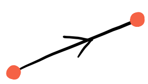
# Topological Structure

$X$ is homeomorphic to $\begin{pmatrix} \text{CW-complex} & \\ 1 & \text{0-cell} \\ 2g & \text{1-cells} \\ 1 & \text{2-cell} \end{pmatrix}$ via



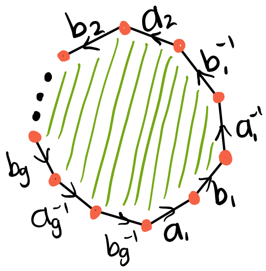

$$H_1(X,\mathbb{Z}) \cong \mathrm{span}_{\mathbb{Z}} \underbrace{\{[a_i],[b_i] \mid 1 \le i \le g\}}_{\text{Basis for } H_1(X,\mathbb{Z})}$$




$a_i$ and $b_i$ are loops on $X$: 

# Topological Structure

$$X \cong \begin{pmatrix} \text{CW-complex} & \\ 1 & \text{0-cell} \\ 2g & \text{1-cells} \\ 1 & \text{2-cell} \end{pmatrix}$$




$$H_1(X,\mathbb{Z}) \cong \text{span}_{\mathbb{Z}} \underbrace{\{[a_i],[b_i]\}}_{\text{Basis}}$$

$a_i$ and $b_i$ are loops on $X$.

# Complex Structure

We can take "derivatives".

$$\Omega^1(X) = \{\underbrace{\text{Holomorphic 1-forms on } X}\}$$

Collection of compatible $\omega_\varphi$, where $\varphi : U \to V$ is a chart of $X$ and $\omega_\varphi = f(z)dz$, with $f(z)$ holomorphic on $V$.

$$\Omega^1(X) \cong \text{span}_{\mathbb{C}}\{\omega_1, \dots, \omega_g\}.$$

# Topological Structure + Complex Structure

We can integrate holomorphic 1-forms over homology classes:

$$\int_{[c]} \omega := \int_c \omega .$$

This is well defined by the Theorem of Stokes.

# The Jacobian

$$\mathrm{Jac}(X) := \frac{\Omega^1(X)^*}{\underbrace{\left\{ \int_{[c]} : \Omega^1(X) \to \mathbb{C} \right\}}_{\text{Period}}} = \Lambda$$

Lattice

Examples: ① $\mathrm{Jac}(S^2) = \{0\}$

② $\mathrm{Jac}(E) = \mathbb{C}/\Lambda \cong E$

# Sanity Check

$$\mathrm{Jac}(X) := \frac{\Omega^1(X)^*}{\left\{\int_{[c]} : \Omega^1(X) \to \mathbb{C}\right\}}$$

① Is $\mathrm{Jac}(X)$ an Abelian group?

Yes:
$$\begin{aligned} \Omega^1(X)^* &\cong \mathbb{C}^g \\ \lambda &\longmapsto (\lambda(\omega_1), \dots, \lambda(\omega_g)) \end{aligned}$$

② Does $\mathrm{Jac}(X)$ tell us how to add $P+Q$, $P, Q \in X(\mathbb{C})$?

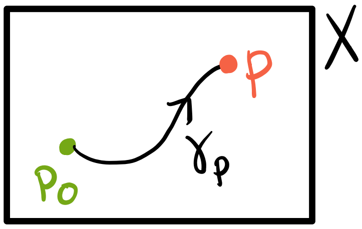
Not yet! How do we represent $P$ and $Q$ in $\mathrm{Jac}(X)$?

$\boxed{\text{We need: } X \hookrightarrow \mathrm{Jac}(X).}$

# Why periods?

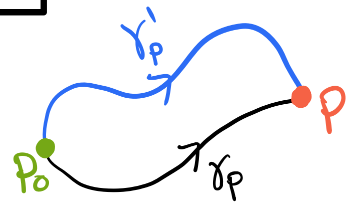
We try to construct a map $X \longrightarrow \Omega^1(X)^*$

Idea:




$$\begin{aligned} X &\longrightarrow \Omega^1(X)^* \\ p &\longmapsto \left(\omega \longmapsto \int_{\gamma_p} \omega\right) \end{aligned}$$

⚠ Not well defined.




Note: $\int_{\gamma_p} \omega - \int_{\gamma_p'} \omega = \int_{\gamma_p - \gamma_p'} \omega$ is a period!

# The Abel-Jacobi Map

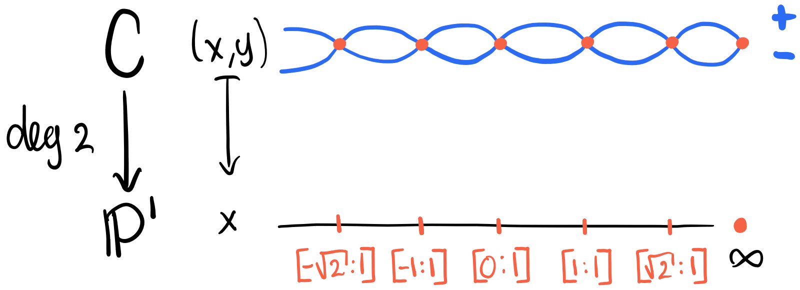
Def. Let $P_0 \in X(\mathbb{C})$. The Abel-Jacobi map $AJ : X \longrightarrow Jac(X)$ with respect to $P_0$ is the map $AJ$ as before, modulo the periods.

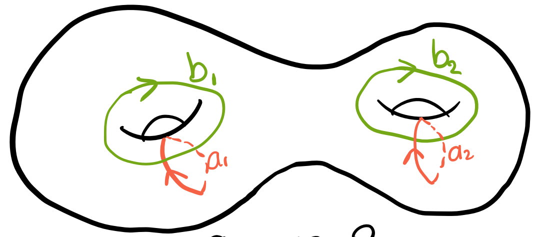
$$\begin{aligned} AJ : X &\longrightarrow Jac(X) \\ P &\longmapsto \left(w \mapsto \int_{\gamma_P} w\right) + \Lambda. \end{aligned}$$

Note: $AJ$ depends on $P_0$.

Question: Is $AJ$ injective?

## Example: $C: y^2 = x(x^2-1)(x^2-2) = f(x)$



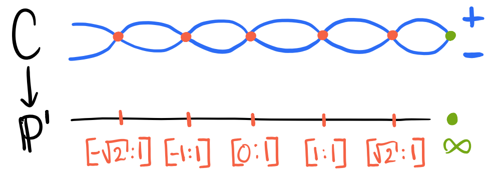



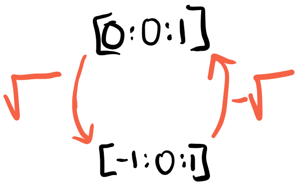

genus 2

$$\Omega^1(C) = \left\langle \frac{dx}{y}, \frac{x\,dx}{y} \right\rangle_{\mathbb{C}}$$

$$\mathrm{Jac}(C) \cong \mathbb{C}^2/\Lambda, \quad \Lambda = \lambda_1\mathbb{Z} \oplus \lambda_2\mathbb{Z} \oplus \lambda_3\mathbb{Z} \oplus \lambda_4\mathbb{Z}.$$

# Example: Finding $\Delta$

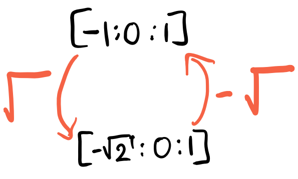



$$\int_0^{-1}\frac{dx}{\sqrt{f(x)}} + \int_{-1}^{0}\frac{dx}{-\sqrt{f(x)}} \approx 4.146i$$

$$\int_0^{-1}\frac{x\,dx}{\sqrt{f(x)}} + \int_{-1}^{0}\frac{x\,dx}{-\sqrt{f(x)}} \approx -2.066i$$

$\lambda_1 = (4.146i, -2.066i)$



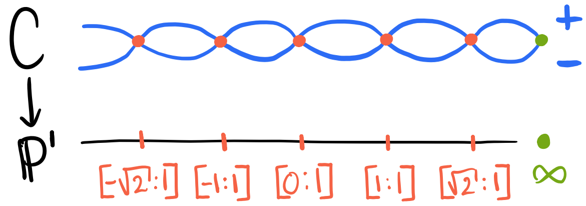

$$\int_{\circlearrowleft}\frac{dx}{y} = -2.409, \quad \int_{\circlearrowleft}\frac{x\,dx}{y} = 2.865$$

$\lambda_2 = (-2.409, 2.865)$

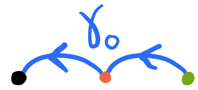
$\lambda_3 = (4.146, 2.066)$

$\lambda_4 = (-2.409i, -2.865i)$

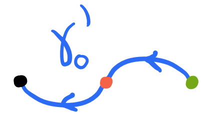
# Example: Computing AJ




$P_0 = \infty = [0:1:0]$




$P = [1:0:1]$




$$\int_{\gamma_0} \frac{dx}{y} = \int_{\infty}^{\sqrt{2}} \frac{dx}{\sqrt{f(x)}} + \int_{\sqrt{2}}^{1} \frac{dx}{\sqrt{f(x)}} \approx -0.869+1.204i, \qquad \int_{\gamma_0} \frac{x\,dx}{y} \approx -2.465+1.432i$$

$$\int_{\gamma_0'} \frac{dx}{y} = \int_{\infty}^{\sqrt{2}} \frac{dx}{\sqrt{f(x)}} + \int_{\sqrt{2}}^{1} \frac{dx}{-\sqrt{f(x)}} \approx -0.869-1.204i, \qquad \int_{\gamma_0'} \frac{x\,dx}{y} \approx -2.465-1.432i$$

$$AJ([1:0:1]) = (-0.869+1.204i, -2.465+1.432i) + \Lambda = (-0.869-1.204i, -2.465+1.432i) - \lambda_4 + \Lambda$$

$$(\lambda_4 = (-2.409i, -2.865i))$$

# Divisors of X

**Def.** The group of divisors of $X$ is:

$$\mathrm{Div}(X) := \left\{ \sum_{i=1}^{r} n_{P_i}[P_i] \,\middle|\, P_i \in X(\mathbb{C}),\ n_{P_i} \in \mathbb{Z},\ r \in \mathbb{Z}_{\geq 0} \right\}$$

**Example:** $3[(1,0,0)] - [(0,-1,0)] \in \mathrm{Div}(S^2)$.

We can extend $AJ$ to $AJ : \mathrm{Div}(X) \longrightarrow \mathrm{Jac}(X)$:

$$AJ\left(\sum_{i=1}^{r} n_{P_i}[P_i]\right) := \sum_{i=1}^{r} n_{P_i} AJ(P_i)$$

# Some Subgroups of Div(X)

**Def.** The subgroup of divisors of degree 0 of $X$ is:

$$\mathrm{Div}^0(X) := \left\{ \sum_{i=1}^{k} n_{p_i}[P_i] \,\middle|\, \sum_{i=1}^{k} n_{p_i} = 0 \right\}$$

**Def.** The subgroup of principal divisors of $X$ is:

$$\mathrm{PDiv}(X) := \left\{ \mathrm{div}(f) \,\middle|\, f : X \to \mathbb{C} \text{ is meromorphic} \right\}$$

**Lemma:** $\mathrm{PDiv}(X) \subseteq \mathrm{Div}^0(X)$.

# The Abel-Jacobi Theorem

We consider the restriction $AJ^0 : \mathrm{Div}^0(X) \subseteq \mathrm{Div}(X) \longrightarrow \mathrm{Jac}(X)$

(Independent of the choice of $P_0$)

**Abel's Theorem.** The kernel of $AJ^0$ is $\mathrm{PDiv}(X)$.

**Jacobi's Inversion Theorem.** The map $AJ^0$ is surjective.

$$AJ^0 : \frac{\mathrm{Div}^0(X)}{\mathrm{PDiv}(X)} \longrightarrow \mathrm{Jac}(X)$$

is an isomorphism of complex manifolds

**Corollary.** Assume $g \geq 1$. Then $AJ: X \longrightarrow Jac(X)$ is injective.

**proof.** $P, Q \in X(\mathbb{C})$. $AJ(P) = AJ(Q) \Rightarrow AJ^{\circ}([P]-[Q]) = 0$

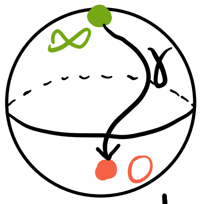
Abel's Theorem $\Rightarrow$ $\exists f: X \to \mathbb{C}$ meromorphic such that
zeros$(f) = P$ (with mult. 1)
poles$(f) = Q$ (with mult. 1)

$$\Rightarrow F: X \longrightarrow \mathbb{C}_\infty \quad \text{s.t} \quad F(x) = \begin{cases} f(x), & x \neq Q, \\ \infty, & x = Q. \end{cases}$$

We know: $\left.\begin{array}{l} \text{- } F \text{ is holomorphic} \\ \text{- } F \text{ has degree } 1 \end{array}\right\}$ $F$ is an isomorphism $\rightarrow\leftarrow$

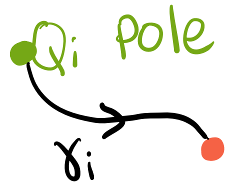
# Abel's Theorem ①: $AJ^0(\mathrm{div}(f)) = \Delta$

Step 1: $F: X \longrightarrow \mathbb{C}_\infty$, $F(x) = \begin{cases} f(x) & x \text{ not a pole of } f, \\ \infty & \text{otherwise.} \end{cases}$

Step 2: 

, $\gamma$ does not pass through any branched pts.

Step 3: $F^*\gamma = \sum_{i=1}^{d} \gamma_i$




$D = \sum_{i=1}^{d} (P_i - Q_i)$

Step 4: $\int_{F^*\gamma} w \overset{\star}{=} \int_\gamma \mathrm{Tr}(w) = 0$

trace of w (is holo. if w is holo.)

# Abel's Theorem ②: $AJ^0(D) = \Lambda \Rightarrow D = \mathrm{div}(f)$.

★ Step 1: $D = \sum_{i=1}^{r} n_i P_i$, $n_i \neq 0$. Find a 1-form $\omega$ such that:

- $\omega$ has simple poles at $P_i$ and no more poles,
- $\mathrm{Res}_{P_i}(w) = n_i$ and $\mathrm{Res}_{P}(w) = 0$ $\forall P \notin \{P_i\}$,
- $\int_{a_i} w$ and $\int_{b_i} w$ are multiples of $2\pi i$.

Step 2: Fix $P_0 \in X(\mathbb{C})$, define $f(P) := \exp\left(\int_{P_0}^{P} w\right)$

Step 3: Near $P_i$, $w = \left(\frac{n_i}{z} + g(z)\right) dz \Rightarrow f(z) = z^{n_i} e^{h(z)}$

holomorphic.

# Jacobi's Inversion Theorem

**Step 1:** Fix $P_0 \in X(\mathbb{C})$. Let $\Phi: X^{(g)} \longrightarrow Jac(X)$

$$(P_1, \dots, P_g) \longmapsto \sum_{i=1}^{g} AJ(P_i - P_0)$$

★ **Step 2:** Use the Implicit Function Theorem: $p \in U \xhookrightarrow{\Phi} V \ni \Phi(p)$.

**Step 3:** For $\lambda \in \Omega^1(X)^* \cong \mathbb{C}^g$, $\exists n \in \mathbb{Z}$ s.t. $\Phi(Q) = \Phi(P) + \frac{\lambda}{n}$.

**Step 4:** $D' := n \sum_{i=1}^{g} (Q_i - P_i) + gP_0 \sim \sum_{i=1}^{g} R_i$ ★ and $AJ^0(D' - gP_0) = \lambda + \Lambda$

Jacobian matrix $\begin{pmatrix} \frac{w_1}{\partial z}(P_1) & \cdots & \frac{w_1}{\partial z}(P_g) \\ \vdots & & \\ \frac{w_g}{\partial z}(P_1) & \cdots & \frac{w_g}{\partial z}(P_g) \end{pmatrix}$

# The Mordell-Weil group

**Goal:** To find rational points on a Jacobian.

<u>Definition</u>. The Mordell-Weil group of $\mathrm{Jac}(X)$ (over $\mathbb{Q}$) is:

$$\mathrm{Jac}(\mathbb{Q}) := \{P \in J \mid P^\sigma = P \quad \text{for all } \sigma \in \mathrm{Gal}_{\overline{\mathbb{Q}}/\mathbb{Q}}\}$$

**Mordell-Weil Theorem (1929).** $\mathrm{Jac}(\mathbb{Q})$ is a F.G. Abelian group.

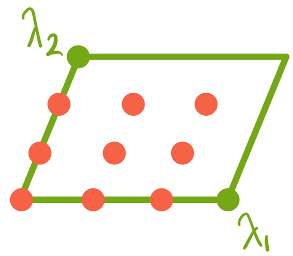
$$\mathrm{Jac}(\mathbb{Q}) \cong \mathrm{Jac}(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^r .$$

# Understanding the Torsion (E)

$E[m] := \{P \in E(\mathbb{C}) \mid mP = 0\}$

$AJ : E \xrightarrow{\sim} \mathrm{Jac}(E) \cong \mathbb{C}/\Lambda$

m=3




Then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

We have the Kummer pairing (if $E[m] \subset E(\mathbb{Q})$)

$$\kappa : E(\mathbb{Q}) \times G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow E[m]$$
$$(P, \sigma) \longmapsto Q^\sigma - Q$$

$mQ = P.$

# Mordell-Weil + Rational Points

$F: x^5+y^5=z^5$, Fermat curve of degree 5 (genus 6).

Theorem (Klassen & Tzermias, '97): Let $K/\mathbb{Q}$, $[K:\mathbb{Q}]=3$.

$$F(K)\setminus F(\mathbb{Q})=\phi.$$

Main tool: $\mathrm{Jac}(F)(\mathbb{Q})\cong(\mathbb{Z}/5\mathbb{Z})^2$.

# Summary:

$X$ compact Riemann surface.

$$\mathrm{Jac}(X) := \Omega^1(X)^* \Big/ \left\{ \int_{[c]} : \omega \longmapsto \int_{[c]} \omega \right\}$$

Abel-Jacobi map: $AJ : X \hookrightarrow \mathrm{Jac}(X)$

$P_0 \xrightarrow{\gamma_p} p \qquad p \longmapsto \left( \omega \mapsto \int_{\gamma_p} \omega \right)$

Abel-Jacobi Theorem: $\dfrac{\mathrm{Div}^0(X)}{\mathrm{PDiv}(X)} \cong \mathrm{Jac}(X)$

# Thank You!